



# NetBackup™ and vRanger Pro™ Integration

**Vizioncore Inc.  
975 Weiland Road  
Buffalo Grove, IL 60089**

## Introduction

Events ranging from terrorism to natural disasters have forced the issue of Business Continuity and Disaster Recovery (DR) to the forefront of IT Management, and for good reason. Businesses are becoming increasingly dependent on information systems, and even a brief outage can have a significant impact. Major disasters carry a greater penalty, with most unprotected companies failing within two years of an event.

Implementing a comprehensive backup and DR plan requires a combination of protection methods tailored to each workload's requirements. There are three common protection methods used to satisfy the various availability needs of a given application:

- Continuous Availability
- Off-Site Replication
- Backup and Restore

While each of these methods has a place in a modern DR plan, Backup and Restore is the foundation of any data protection effort.

This paper will focus on Backup and Restore; in particular, how to combine two Best of Breed solutions (Symantec® NetBackup™ and Vizioncore's® vRanger Pro™) to create a complete Backup and Restore solution for today's enterprises.

## Backup and Restore Benefits of Virtualization

The case for virtualization has been widely made and well received; in part due to the advantages that virtualization offers DR. To fully appreciate the value of integrating NetBackup and vRanger Pro, it is important to discuss their different approaches in protecting virtual servers.

On a basic level, a VM is a collection of encapsulated files that represent a physical machine—Operating System (OS), patches, configurations, applications, and data. These files can be backed up, restored, and moved around more efficiently than a typical physical server. They can be protected from outside the guest, eliminating the need for costly file-level agents. Once backed up, these VM archives can be restored quickly and easily, without pre-installing the OS.

## NetBackup and vRanger Pro Overview

Recent estimates place NetBackup as the clear leader in the Enterprise backup market, with as much as 45 percent of customers using it. With NetBackup introducing advanced features such as disk-to-disk backup and deduplication, their position in the physical server backup market can only improve. While NetBackup has set the bar for physical servers, their feature set for virtual servers is less advanced, relying exclusively on a basic integration with VMware Consolidated Backup (VCB). While this integration can extend the back-end functionality of NetBackup to VMs, it lacks VMware-specific functions that a “built for virtualization” solution would offer.

Vizioncore's vRanger Pro, on the other hand, is the leading Backup and Restore solution for VMware Virtual Infrastructure. Designed from the start for VMware, vRanger Pro offers agentless, image-level backups taken from outside the guest, without disrupting the running VM. vRanger Pro clearly differentiates itself in the virtualized backup space with VMware-specific functions such as: file-level restores from image-level backups; the ability to skip VMDKs (virtual hard drives) for a given VM; and an advanced VCB integration with a network failsafe option.

With two clear leaders in their respective markets, how can customers know which solution is better for their environments? In most cases, the answer is to integrate both products for a complete

solution.

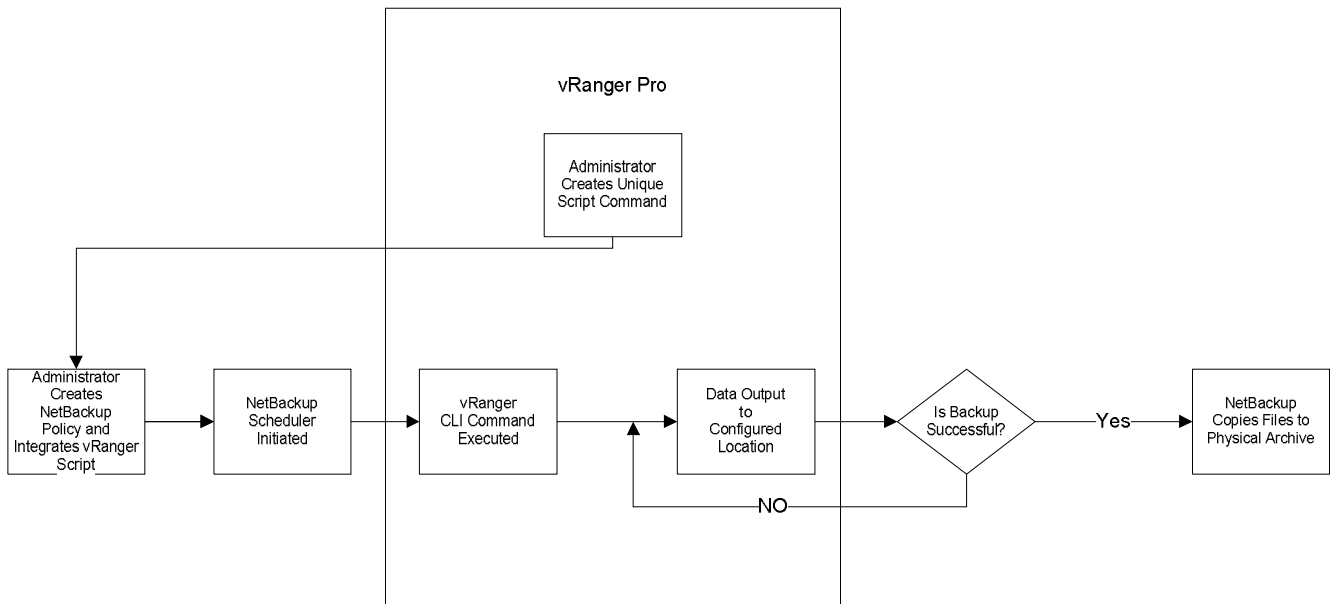
## How NetBackup and vRanger Pro Work Together

Working together, NetBackup and vRanger Pro provide a powerful backup and restore solution, which makes running and managing backup and restore tasks easier. The vRanger Pro CLI Output area ensures process consistency and automation by activating jobs through scripting. NetBackup works as a facilitator, copying compressed files quickly to disk or tape. Once a backup is complete, NetBackup deletes the files from the mount point and archives them. From the archive location, NetBackup moves the files to a local destination from which vRanger Pro can restore them.

During job configuration, vRanger Pro builds a CLI command to capture the required parameters of the backup job. Rather than scheduling or saving the job, the administrator copies the CLI command to build the NetBackup policy. For more information on CLI commands, see the *vRanger Pro User Manual*.

In NetBackup, an administrator creates a policy and schedules it to execute. This policy directs NetBackup to locate and move the backup files to a mount point. Each policy name must be unique, based on the task that the corresponding script runs. For example, a policy that runs a web server backup should be named differently than a policy that backs up email. All policies share a common structure. There is no limit to the number of policies that can be executed. To back up several VMs running on the same host, an administrator must create separate policies for each VM.

This is the basic process flow for the combined solution:



## NetBackup and vRanger Pro Integration

Integrating NetBackup and vRanger Pro is as simple as confirming proper installation of all components. After completing installation, there are a few minor configurations that must be made within NetBackup and vRanger Pro. Step-by-step instructions are included below.

## Implementation

To complete a full backup of a VM and save it to tape, an administrator must:

- Confirm that all pre-requisites have been met.
- Complete the set-up process.
- Confirm the successful installation of vRanger Pro.
- If using VCB, confirm successful installation of the VCB plug-in.
- Complete the configuration process.

### Pre-requisites

The administrator who completes this process should have an advanced knowledge of vRanger Pro and NetBackup as well as a basic knowledge of scripting.

This procedure assumes:

- NetBackup has been installed.
- The virtual infrastructure includes only one VirtualCenter (VC), which can feature multiple domains.
- The backup files will be copied to a mount point that is either a SAN or a local Windows destination.
- Off-host backups (via VCB) are desired for some or all VMs.

### Set Up

These steps must be completed before beginning the configuration process.

- vRanger Pro must be installed properly.
- If running a LAN-free backup, the VCB plug-in must be installed properly.
- If restoring an individual file, the File-Level Restore plug-in must be installed properly.
- If running a LAN-free backup, vRanger Pro, VCB, and NetBackup must be installed on the same server. This server should be connected to the SAN using fiber-optic cable. The target VM's ESX Server must be connected to the same SAN using fiber-optic cable.
- The SAN must be zoned to see the Virtual Machine File System Logical Unit Numbers (VMFS LUNs) that the target VM's ESX Server uses. LUNs must be aligned so that the storage is presented to the proxy server with the same numbering system as it is presented to the ESX Hosts.

In the target VM, mount point, and destination tape drives, there must be sufficient free space to accommodate the decompressed/compressed backup files, including snapshots.

- For the target VM location, confirm that there is a minimum of 6GB of free space. Recommended: At least 10GB or 10 percent of the VMFS, whichever is greater.
- For the mount point location, the drive should have enough free space to accommodate the compressed backup files, including snapshots.
- For the destination tape drive, confirm that there is sufficient space to store the compressed archive files.
- If the ultimate goal is restoration, confirm that the ESX Server or VM restore destination has enough free disk space to accommodate the decompressed backup files.

## Installation

The vRanger Pro installation must be completed before the VCB and File-Level Restore plug-ins can be installed. Detailed installation instructions are in the *vRanger Pro User Manual*, which can be accessed through [www.vizioncore.com](http://www.vizioncore.com).

1. Install vRanger Pro.
2. (Optional) Install VCB plug-in.
3. (Optional) Install File-Level Restore plug in.

## Configuration

### Configure vRanger Pro

1. Identify the target machine.
2. Enable (or disable) the compression option.
3. Establish how frequently the backup should be run.
4. Assign the mount point location.
5. Set additional options as desired.

### Configure NetBackup

1. Access the NetBackup Administration Console.
2. In the left pane, select NetBackup Management→Host Properties→Clients. The Client Properties dialog displays.
3. In the left pane of the Client Properties dialog, select Timeouts.
4. Set the Client read timeout spin box to 1,200 seconds (minimum). Click Apply.
5. Select Windows Client→Client Settings. The Client Properties dialog displays.
6. In the Archive Bit/Incrementals section, select the Use Change Journal in incrementals checkbox. Click Apply. Click OK.

### Create New Policy

1. Access the NetBackup Administration Console.
2. In the left pane, right-click NetBackup Management→Policies→Add New Policy. The Add a New Policy dialog displays.
3. Enter a name for the policy and click OK.
4. Right-click Policies→Properties.
5. On the Attributes tab, select MS-Windows-NT in the Policy type dropdown.
6. Select the Cross mount points checkbox.
7. Clear the Collect disaster recovery information for Bare Metal Restore checkbox. Click OK.
8. On the Schedules tab, click New. The Add New Schedule dialog displays.
9. On the Add New Schedule dialog, enter a name for the schedule.
10. In the Type of backup dropdown, select Full Backup.
11. In the Schedule Type section, select a radio button—either Calendar or Frequency.
12. In the Destination section, select the Snapshots and copy snapshots to a storage unit radio button.

### Configure Script and Run bpstart\_notify.bat

Using vRanger Pro's GUI interface, select target, destination, timeframe, and other options as desired. Notice that as options are selected, a CLI command builds in the lower portion of the screen. This command will be used to pass the job parameters from NetBackup to vRanger Pro at run-time using the "bpstart\_notify.bat" configured for each NetBackup policy.

**Warning:** After completing this process, do not click Run Backup or Schedule Backup. Instead, select Copy. Instead of running the program from vRanger Pro, we will take advantage of the powerful CLI interface that is created by cutting and pasting the command into NetBackup rather than using the task scheduler found within vRanger Pro, this is actually the power of the combination since both products do what they are designed to and leverage the strengths of both of the products.

#### Sample script:

```
If "%2" == "backup_web" goto backup_web
If "%2" == "backup_email"goto backup_email
If "%2" == "backup_front_end"goto backup_front_end

    Goto end

:backup_web

REM (Insert vRanger Pro call here.)

CALL "c:\program files\vizioncore\vRangerProCli.exe" -virtualcenter vc2://Folder=group-v8959 -
copylocal F:\VZ_BACKUP\MOE-SVG -drives:db -vmnotes -vcb -totalvcbasync 2 -diffratio 50 -
maxfullage 14 -retendays 31 -zipname [config]_[year][month][day][hour][minute][second] -onlyon

    Goto end

:end
```

### vRanger Pro commands are run in the background.

For each policy, the vRanger Pro commands in the script are run. Within the VCB framework, vRanger Pro takes a snapshot of the pending changes to the .VMDK. Then, the VCB mounts the .VMDK, compresses the files, and applies the snapshot. The compressed files are copied to the mount point.

### NetBackup copies the files to tape.

After each bpstart\_notify.bat script completes, NetBackup copies the compressed files from the mount point to tape, where they are archived.

### The files are archived.

If the backup is successful, the files are deleted from the mount point within a few minutes. The archived files can be restored only after NetBackup moves them to a location where vRanger Pro can access them.

## Archiving

When the compressed backup files are saved to tape, they are—essentially—archived. The data is stored there for a duration configured by the administrator. vRanger Pro plays no role in archiving.

## Restoring

vRanger Pro does the majority of the work during the restore process. However, before vRanger Pro can restore an archive, NetBackup must move the files from the archive location to a local restore destination.

vRanger Pro offers several restoration methods, all of which are easy to complete. Restores can be done in normal mode (full-image restore), from the .info file, by individual file, or P2V to a VM. Details on two of these processes—full-image and file-level restore—are included in this paper. vRanger Pro can restore from its own local database or from a backup completed using a previous installation of the software. In general, configuring a restore is as simple as selecting the archive or file to restore, selecting the restore destination, and setting a few attributes.

Before vRanger Pro restores an archive, it verifies that the destination drive has sufficient free space

to accommodate the decompressed files. The data is then copied in blocks and decompressed as it is copied.

<b>Restore a VM</b>	
1.	Use NetBackup to move the archive to the restore destination.
2.	Access vRanger Pro. In the left pane of the Restore window, click the Restore VM icon.
3.	On the Restore Archive tab, select the checkbox of the archive that you want to restore.
4.	On the Restore To tab, click to highlight the location to which you want to restore the data.
5.	On the Options tab, select the checkboxes for the flags that you want to set. Select the Enable vRanger enhanced write speeds checkbox.
6.	Click one of the buttons—Schedule Restore or Run Restore.
7.	If you clicked Run Restore, a command prompt displays and vRanger Pro completes the restore in the background.
8.	If you clicked Schedule Restore, the Schedule Task dialog displays. <ol style="list-style-type: none"> <li>a. On The Schedule Task dialog, select a timeframe, enter your password, and click Add. Windows Task Manager creates a restore task.</li> <li>b. Select Control Panel→Scheduled Tasks to confirm that the restore request was saved.</li> </ol>
<b>Restore an Individual File</b>	
1.	Use NetBackup to move the archive to the restore destination.
2.	Access vRanger Pro. In the left pane of the Restore window, click the Restore VM icon.
3.	On the Restore Archive tab, select the checkbox of the file that you want to restore.
4.	On the Restore To tab, click to highlight the location to which you want to restore the data.
5.	On the Options tab, select the checkboxes for the flags that you want to set. Select the Enable vRanger enhanced write speeds checkbox.
6.	Click one of the buttons—Schedule Restore or Run Restore.
7.	If you clicked Run Restore, a command prompt displays and vRanger completes the restore in the background.
8.	If you clicked Schedule Restore, the Schedule Task dialog displays. <ol style="list-style-type: none"> <li>a. On The Schedule Task dialog, select a timeframe, enter your password, and click Add. Windows Task Manager creates a restore task.</li> <li>b. Select Control Panel→Scheduled Tasks to confirm that the restore request was saved.</li> </ol>

## Best Practices

This section includes some hints for installing, integrating, and configuring NetBackup and vRanger Pro. Tips for completing the backup, archive, and restore processes are also included.

### Installation

- For optimal performance, do not install vRanger Pro or NetBackup on a VM.
- Install the VCB and the File-Level Restore plug-ins only after vRanger Pro's installation is complete.

### Configuration

- It is useful, based on the needs of your organization, to create some generic policies in NetBackup. These policies can be rerun or copied for reuse later. This will save time and effort.
- It is best to name each policy based on the task to be completed. For example, to back up a

set of front end servers, name the policy “frnt\_end\_srvrs”.

- vRanger Pro offers enhanced write speed for restores. On the Options tab of the Restore window, select Enable vRanger enhanced write speeds. A driver is installed on the ESX Server. This driver is only active during the restoration process and is removed without requiring a reboot.
- Be careful when setting expirations and rerunning backups. The Restore Grid information remains in vRanger Pro’s internal database for all archived files that have not been overwritten or have not expired.

### **Backup Process**

- Before starting a backup or restore process, test to confirm connections and adequate disk space.
- In the event that the target virtual machine is a transactional virtual machine requiring special quiescing, it may be necessary to run an application specific program to perform the quiescing before taking the backup.
- If the Schedule Backup or Run Backup buttons on vRanger Pro’s Option tab are disabled, there is either conflicting or insufficient information for completing the backup process. This information must be provided (or corrected) before the administrator can proceed.
- Before implementing a larger backup and restore, it is a good idea to test the processes on a smaller scale. For example, before backing up a group of VMs hosted on the same ESX Server, identify one VM to be the basis of your test. Follow the steps to back it up and confirm that the process completes as expected. Then, use NetBackup to archive the files to disk or tape. Finally, use NetBackup to move the files to a location from which vRanger Pro can restore it. If any of these processes do not execute as expected, adjust to suit need.

### **Archive Process**

- It is best to archive backup files to removable media such as tape. Doing so offers the flexibility and portability to save the files to a remote DR site. At that location, the files will have a greater measure of protection against corruption and system failure.
- For P2V backups, the free space on the destination drive should be twice that of the target machine. That is, if the physical machine has a 40GB hard drive, the destination drive for the archive file should have 80GB of free space.

### **Restore Process**

- Simultaneous restores should be limited to no more than two to an individual host and no more than ten to a VMFS.
- A complete restoration can only be done from a full backup or a combination of differentials and the machine’s last full backup. To perform a complete restore using differential backups, select both the archive of the last full backup and any archived differential backup files as well.

### **General**

- Organize hosts and VMs in a thoughtful, logical way. Doing so will make it easier to group them for backup and restore.