Keeping it Simple: How to Protect Growing VMware Environments

Good News for Backup Administrators – Put the Power of Simplicity to Work on VMware Backup and Recovery

ACHIEVING ADEQUATE DATA PROTECTION FOR EACH VIRTUAL MACHINE CAN BE EITHER A STRAIGHT-FORWARD OR DECIDEDLY COMPLEX PROCESS.

IT teams that make the move to VMware are often thrilled by how much easier it is to provision and manage their previously cumbersome and costly server environments. Yet, as virtual machines proliferate and more ESX Servers are added to these environments, administrators who are tasked with protecting their growing virtual data centers often face added layers of complexity. Depending on the third-party backup application in use, achieving adequate data protection for each virtual machine (or a whole VirtualCenter environment) can be either straight forward or a decidedly complex process. A few guidelines can help today's administrators focus on keeping it simple while still ensuring robust, automated backup and recovery for VMware.

This whitepaper will show you how. ▶

BakBone®

Keeping it Simple: How to Protect Growing VMware Environments
Backup Administrators – Put the Power of Simplicity to Work on VMware Backup and Recovery

Avoiding Extra Work When Protecting Virtual Machines

As VMware evolved to meet the needs of its growing customer base, the company built an excellent foundation for data protection. Designed to work in conjunction with third-party backup software applications, VMware engineered its own point-in-time snapshot functionality to appropriately quiesce and reconvene operations of one or more virtual machines. This has allowed VMware to produce consistent disk-based backup images without undue disruption to end-user operations.

To help centralize and further streamline its backup/recovery operations, VMware developed its own VMware Consolidated Backup (VCB) set of utilities to back up virtual machines (VMs) from each ESX Server to a centralized VCB Proxy Server.

Such foundational moves have paved the way for faster protection of virtual environments. But, they represent only half of the story for automated backup of VMware environments. The other half of the equation relates to how smoothly your third-party backup software application picks up where VMware leaves off – ensuring automated, successful backups and easy restores with minimal impact on staff time.

While most data protection solutions now claim integration with VMware, a closer look often leads to a few uncomfortable realities. The following tips can help you avoid adding more work to an already busy IT schedule:

1. Automate Discovery of the Current Status of Your Virtual Machines
Due to the dynamic nature of VMware environments, administrators may add or remove many virtual machines, move them to resource-free servers, power up one set or power down others. Such moves impact backup operations and should be automatically reflected by the backup software within its own discovery process.

2. Avoid Using Old Ways to Back Up a New Architecture
Many backup and recovery applications still rely on old-fashioned command line interfaces and non-intuitive steps to back up virtual machines and work with VCB. Instead, look for an intuitive user interface with point-and-click operations.

3. Avoid Writing and Updating Scripts
VCB offers data protection vendors the ability to work with specific pre- and post-processing backup scripts and commands so the system knows when to quiesce certain VM operations, when to create snapshots and when to clean up after backups are completed. Such VMware communications are a useful function of your backup software. What's not useful, however, is when the backup software passes the increasingly complex job of pre- and post-command scripting onto the backup administrator. This now requires administrators to spend time mastering the VCB Proxy Server's own language, along with writing/updating scripts for key backup jobs. Instead, look for backup software that automates and offloads scripting from the backup administrator. This can make it easier for less-experienced IT staffers to perform basic backup/restore functions.

4. When It Comes to Backup, Think Big and Small
Some backup administrators may want to perform image-level backups of only certain VMs. Others may want to back up all VMs on multiple ESX Servers. Still, others may want to back up (and restore) individual Microsoft Windows-based files in key VMs. It's a good idea to understand how easy (or hard) it is to accomplish backups and restores from within the backup vendor's software interface.

WHILE MOST DATA PROTECTION SOLUTIONS NOW CLAIM INTEGRATION WITH VMWARE, A CLOSER LOOK OFTEN LEADS TO A FEW UNCOMFORTABLE REALITIES.

BakBone®

Keeping it Simple: How to Protect Growing VMware Environments
Backup Administrators – Put the Power of Simplicity to Work on VMware Backup and Recovery

Letting the 'GUI' Simplify VMware Backup and Recovery

Backup software integration with VMware means different things to different vendors. With Release 8.1 of its award-winning NetVault®: Backup software, BakBone Software applied the following tenets to help define its own levels of VMware integration offered to backup administrators. Such best practices have since been realized within BakBone's fully integrated NetVault: Backup VMware Plugin:

1. Make VM environment discovery a seamless process.
2. Simplify and empower the backup administrator's experience.
3. Replace scripting with automation.
4. Make it easy to restore individual files or virtual machines.

The NetVault: Backup VMware Plugin hides its rich data protection functions and complete integration behind an intuitive graphical user interface (GUI). The result: Automation and time-savings for daily backup administration.

Best Practice #1: Make VM Environment Discovery a Seamless Process

Backup administrators do not need to take time to manually update the backup software in order to reflect the latest changes to their VMware environment. As simple as refreshing the screen, NetVault: Backup's rich GUI automatically displays the hierarchical relationship between various ESX Servers and their VMs, including the current state of each VM. After being connected to the Virtual Infrastructure, NetVault: Backup naturally discovers and graphically depicts the current status of each VM within an individual ESX Server or in a complete VirtualCenter environment. Whether your VMware environment hosts Microsoft Windows or Linux guest operating systems, NetVault: Backup uses its VMware plugin to automatically discover and protect all your VMs.

ALL RESTORES —
FROM INDIVIDUAL
FILES TO FULL VM
IMAGES — CAN
BE PERFORMED
BY THE BACKUP
ADMINISTRATOR
USING A BASIC, POINT-
AND-CLICK PROCESS.

Auto-Discovery of Your VMware Environment

**Icons for Instant
Visual Identification**

A standalone ESX Server

A data center

A cluster of hosts

An ESX host

A VM

A VM (currently inaccessible)

A powered off VM

A suspended VM

A mounted VM
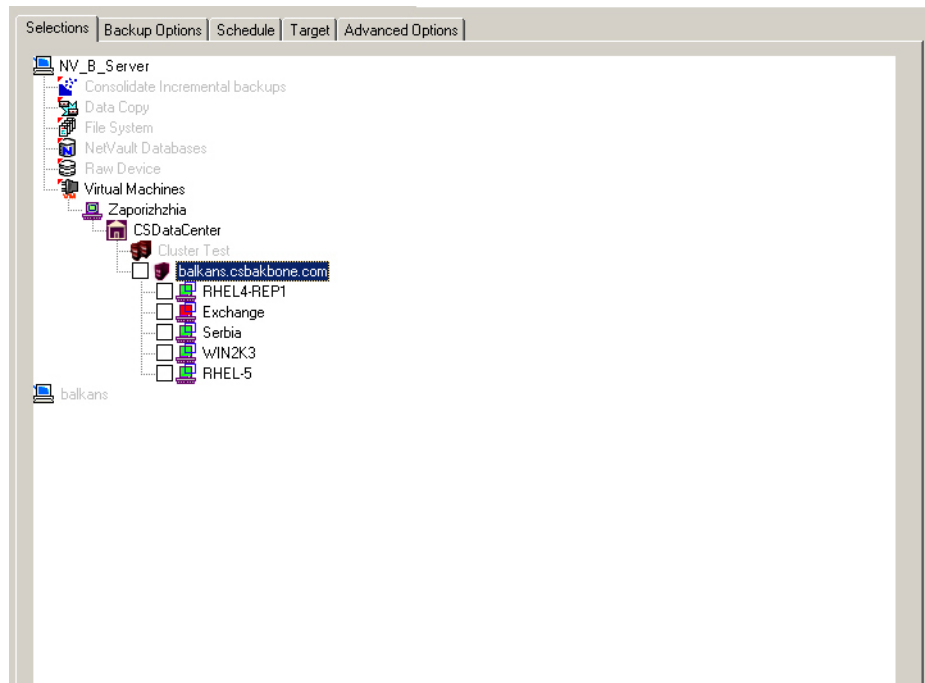
Best Practice #2: Simplify and Empower the Backup Administrator's Experience

Instead of relying on awkward command-line functions, NetVault: Backup allows administrators to use a simple point-and-click process right from within its own GUI to set backup policies and select VMs for specific backup or restore.

Five Steps to Back Up Your VMs

1. Within the Backup window, locate and open the **Virtual Machines** plugin.

2. Open one of the following nodes:
   - **localhost node** (for administrators performing backup from an ESX Server)
   - **VirtualCenter Server** node (for administrators performing backup from the VCB Proxy Server)

3. Expand the hierarchy tree to view individual virtual machines. Now place a check mark in each box representing the virtual machine(s) you want to back up.

4. Set other options on the Schedule, Target or Advanced Options Tab.

5. Name the job, then click the **Submit** button.

(This process creates an image-level backup of each VM.)
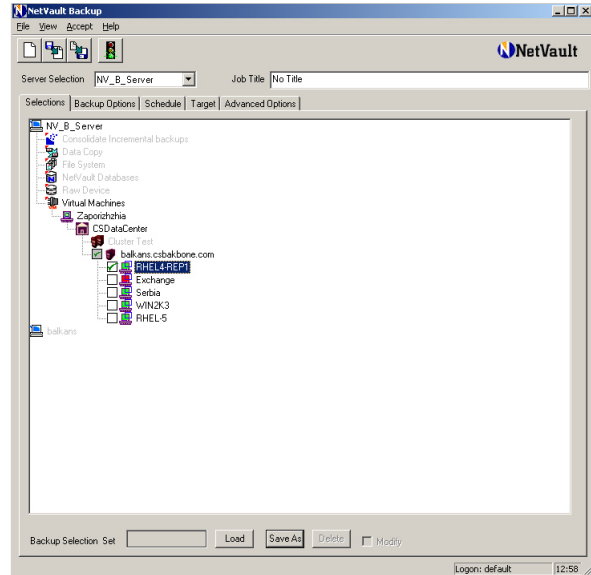
In just a few steps, administrators can see their latest backup and restore operations take effect.

Quick VM Image Restores

1. Within the Restore window, following Steps 1 and 2 above.

2. Locate and select the appropriate VMware image listed in the saveset.

3. Finalize the job, using the Source, Target Client, Schedule or Advanced Options tabs.

4. Name the job, then click **Submit** to complete the restore process.
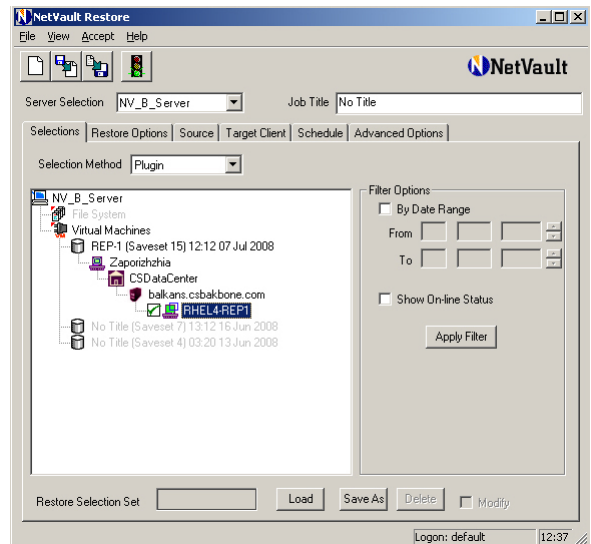
Best Practice #3: Replace Scripting with Automation

Administrators looking to use VCB Proxy Server can comfortably set and schedule backup jobs and policies all from within NetVault: Backup's rich GUI. There's no need to perform pre- and post-processing commands. Such automation leads to significant reductions in time administering and updating backup jobs, as well as a reduction in the risk of manual errors.

Best Practice #4: Make It Easy to Restore Individual Files or a Full VirtualCenter

NetVault: Backup is designed to protect the VM contents of both individual VMware ESX Servers as well as entire ESX Server clusters. Administrators can perform full-image backups of each VM from either the ESX Server or the VCB Proxy Server.

Administrators using VCB to protect VMs running the Microsoft Windows guest operating system can also use NetVault: Backup to perform file-level backups or restores within these VMs.
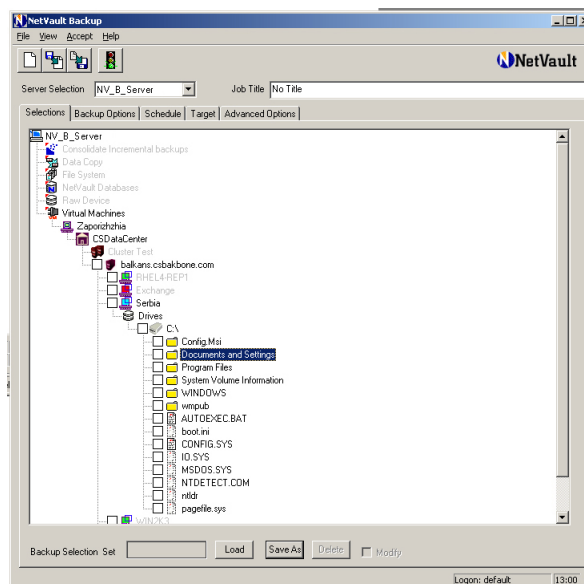
Restoring Image-Level Backups
NetVault: Backup lets you choose either of the following methods to restore the image-level backups:

- Restoring Image Backups Using VCB – This method is also known as COS-less restore as it does not use the Service Console Operating System to restore data. To use this method you must install the VMware Converter on the VCB Proxy Server. The VMware Converter can be downloaded from the VMware website at http://www.vmware.com/download/converter/. This method gives you the flexibility to restore to either the original ESX host or to an alternate ESX Host.

- Restoring Image Backups Using Service Console – This method is also known as COS-based restore. To use this method, an instance of the VMware Plugin must be running on the ESX Server. You will then be restoring the image to the original ESX host.

Easy File-Level Backup of a VM via VCB

1. Within the Backup window, locate and open the **Virtual Machines** plugin.

2. Open the **VirtualCenter Server** node (for administrators performing backup from the VCB Proxy Server)

3. Expand the hierarchy tree to view individual virtual machines. Right-click on the specific Microsoft Windows VM whose files you want access. Then, select **Mount**. (This mounts a snapshot of the VM to a temporary area on the VCB Proxy Server.)

4. You should now be able to see the VM's specific disk drives, files and folders. Place a check mark in each box representing the files or folders you want to back up.

5. Use the Backup Options Tab to define whether or not you want a full backup, incremental backup or differential backup.

6. Set other options on the Schedule, Target or Advanced Options Tab.

7. Name the job, then click the **Submit** button.

❄️BakBone®

Keeping it Simple: How to Protect Growing VMware Environments
Backup Administrators – Put the Power of Simplicity to Work on VMware Backup and Recovery

Restoring File-Level Backups

The NetVault: Backup VMware Plugin provides the following two methods to restore file-level backups:

- Using Shared Network Drives – This method does not require an instance of NetVault: Backup Client to run locally on the VMware machine. File-level restores are performed to the shared network drives on the virtual machines using the Filesystem Plugin installed on the VCB Proxy Server. Since the Filesystem Plugin is automatically installed with a NetVault: Backup Client, no additional software is required for this type of restore.
- Using Native Filesystem Plugin – This method is suitable if an instance of NetVault: Backup Client is already running on the virtual machine for backup and recovery of other data. The virtual machine is treated as any other physical NetVault: Backup Client for the file system restores.

This is truly scalable data protection, capable of spanning from individual files up to a complete VirtualCenter environment.

Ensuring Flexible Restores –
For the Present and for the Future

IT organizations seeking to continue growing their virtual server infrastructures don't just care about backup. They really need to know that the backup software will deliver when it matters most with flexible restores that can be manipulated as the situation's needs arise:

- COS-based or COS-less Restores – A choice of COS-based or COS-less Image restores, along with a selection of individual file recovery techniques make it easy to restore VMs or individual files from either an ESX Server or from the VCB Proxy Server.
- Alternate Restore Location – Restoring to another location is a must for VMware disaster recovery. NetVault: Backup makes it easy to restore data sets remotely to another ESX Server.
- A wide range of restores available – NetVault: Backup supports restoring from the smallest files to a large VirtualCenter environment with multiple ESX Server clusters.
- Application-aware restores – Administrators can take advantage of NetVault: Backup's integrated Application Plugin Modules, which are especially helpful in VMware environments that need a more granular, application-specific backup for applications like Oracle or Microsoft Exchange.

Making Life Simpler and Easier

Administrators also benefit in other ways from using NetVault: Backup with VMware:
- Single-Entry Updates – There's no need to re-script a single entry point for each VM. Ideally, a single entry point can propagate automatically to other VMs. If administrators need to move any of these, they can now make just one update, instead of multiple script changes.

- Global Identifier for Streamlined VM Migration – Since NetVault: Backup can track virtual machines by global identifier (instead of just their individual names), administrators don't need to worry about losing the VM location after using VMotion to move or migrate one or more VMs. In contrast, some backup systems track virtual machines by name only, which can cause the VM location to be lost.

- Data Protection Visibility for Better Coverage – NetVault: Backup offers visibility of the entire VI tree. This helps administrators ensure that their VM data is fully incorporated into their organization's data protection strategy.

- Backup Support for Various Network/Storage Topologies – NetVault: Backup gives administrators greater flexibility by allowing them to back up to a variety of storage systems, including direct-attached storage (DAS), SAN and LAN.

- File-Level Restores without Unnecessary Agent Costs per VM – To help keep costs down, NetVault: Backup allows users to make file-level restores directly to virtual machines without requiring an agent on each VM.

Conclusion

NetVault: Backup and its VMware Plugin are built with full support for today's growing VMware environments. For BakBone, full integration means just that – integration that makes the process of backing up or restoring your virtual machines as transparent and painless as possible.

Why struggle with scripting and awkward interfaces when you don't have to? Why waste more time than you need on the backup process? NetVault: Backup has perfected its simple, yet powerful centralized interface to back up everything from common file shares to highly complex VMware environments. Regardless of your needs, you are a point-and-click away from managing your backups from one central location with NetVault: Backup. To test the software, visit www.bakbone.com/downloads for a free trial download. ▪

BakBone®
The Power of Simplicity™

BakBone Global Headquarters
9540 Towne Centre Drive, Suite 100
San Diego, CA 92121
Toll Free Phone: 877-939-2663
Phone: 858-450-9009
Fax: 858-450-9929
Email: sales@bakbone.com

Asia Pacific Headquarters
Shinjuku Dai-ichi-Seimei Bldg.11th Floor
2-7-1 Nishi Shinjuku, Shinjuku-ku
Tokyo, Japan 163-0711
Phone: 81-3-5908-3511
Fax: 81-3-5908-3512
Email: sales@bakbone.co.jp

Europe Headquarters
100 Longwater Avenue
Green Park
Reading
RG2 6GP
United Kingdom
Phone: 44 (0)1189-224-800
Fax: 44 (0)1189-224-899
Email: sales_europe@bakbone.com

About BakBone

BakBone is committed to making data protection a simple, straightforward process while delivering its Integrated Data Protection (IDP) strategy through an award-winning product suite. Thousands of users worldwide leverage BakBone's IDP approach to simplify the management of multi-platform environments with a portfolio of backup, disaster recovery, replication and storage reporting solutions for Linux, Windows, Unix and Mac OS X environments. BakBone's products offer a single point of control for managing resources across all platforms, providing improved operational efficiency, reduced system downtime, improved availability and enhanced security to support the business growth of enterprise environments. BakBone is headquartered in San Diego, Calif. For more information about BakBone, visit www.bakbone.com or email info@bakbone.com.

61297_070108