QUEST SOFTWARE®

Five Tips for Effective Backup and Recovery in Virtual Environments

Written by
Daniel Lord
Sr. Product Marketing Manager
Quest Software, Inc.

WHITE PAPER

Contents

Abstract

In this white paper, Quest's virtual data protection experts offer five tips that will dramatically increase the effectiveness of backup and recovery in your virtual environment.

Introduction

Virtualization is being rapidly adopted, particularly in small to mid-sized businesses (SMBs) where time and money are always at a premium. It brings significant time, money and labor savings in a variety of areas, including procurement, administration, deployment, operation, reliability and recoverability. Virtualization can radically simplify management of the entire environment and enable the SMB administrator to "do more with less." Moreover, disaster recovery becomes significantly easier once a business has virtualized, provided the administrator adopts newer, more efficient technologies that are designed to work with the virtual infrastructure.

However, like any technology, virtualization brings challenges that can erode its cost benefits and leave the infrastructure less protected than before. In this paper, Quest's data protection experts offer five tips for effective backup and recovery to help you avoid the challenges that might keep you from fully protecting your virtual assets and infrastructure. You will discover how simple and affordable effective virtual data protection can be, and maximize your investment in your virtualized infrastructure.

Our Five Tips

Tip #1: Minimize the amount of data you protect

You can reduce the amount of data you back up while ensuring 100 percent recovery by using technologies that filter out unchanged and deleted data.

While tools that utilize VMware CBT (Changed Block Tracking) eliminate the backup of some unnecessary data, CBT does not prevent the backup and restore of deleted data. The Windows operating system uses the unused free space that is allocated, but not used, for data to store deleted files. That deleted data is never removed until it is overwritten to make space for new data. VMs that host applications with frequently changing data can have gigabytes of deleted data. Unfortunately, those files are seen as changed data blocks, and backup tools using only CBT will back up that deleted data. That stretches backup times, lengthens restore times, and overloads your network.

Our tip is to select a tool that does not back up deleted data. That way, you can back up often and with greater granularity. You'll also save substantially on storage space, backup time, bandwidth and recovery time, enabling you to have better recovery point objectives (RPOs) and shorter recovery time objectives (RTOs).

Tip #2: Maximize backup speed and throughput

Many backup administrators manage data protection for their virtual systems as if they were protecting physical systems; this can seriously reduce the efficiency of virtual asset data protection. For example, administrators often put multiple VMs on a server that would have previously hosted only one physical application. This creates increased contention for network resources—particularly when backups and restores are being performed.

Virtualized systems are different and need different techniques for optimal protection. We recommend you use a tool that allows simultaneous backup and restore to avoid bottlenecks. In addition, use a tool that provides flexible backup methods (proxy, direct-to-target, LAN-free) to fit your environment and minimize workload impact.

To further increase network and system efficiency, choose a tool that eliminates the need for a backup server by sending backup images directly to target storage. This approach reduces network load by eliminating intermediate steps.

Tip #3: Keep your recovery options flexible

While agent-based systems have their benefits, they aren't always most efficient or cost effective for small organizations. When you back up virtual systems with agent-based systems, you typically have to pre-stage your VMs to restore an entire VM. This means you have to spawn a new VM via clone or template, size the memory and disks correctly, name it correctly, and create the appropriate number of virtual disks. Once this is up and running, you must then install an agent, connect to the target, and restore the VM. One alternative to an agent-based system is bare-metal restore routines. However, these are challenging to implement at best, and you may have to maintain duplicate hardware with this option as well.

Fortunately, virtualization brings many simpler and more powerful recovery options. Use a tool that allows you to simply click on a VM to restore it, with no need for pre-staging. Find one that allows you to easily restore files at the file level and to restore application objects. Set up your disaster recovery scheme so you can fail over to a VM on a remote server (either on campus or offsite) with a single click of a button, and ensure the replication is automatically reversed so that once the source site comes back up, you can simply synchronize the changes and failback to source.

What about physical boxes? Almost every virtual environment has some servers that just can't be virtualized yet. Consider companion tools that work with your virtual data protection tool to offer continuous protection for physical servers. Using continuous protection, you can image physical systems into VMs, which can be then restored to a VM

or a physical server. This approach gives you the flexibility to get your systems restored and your business back on line fast.

What about long term tape-based retention? Most organizations already have investments in agent-based software and tape systems. All you need is a single agent with visibility to an archive repository to sweep the archives off to tape. Consider a tool that offers sweep-to-tape integration that can be used with a traditional backup tool. Then if you ever need to recover an old archive, you can simply restore it to the repository, import the manifest, and start restoring files or VMs as you please.

Tip #4: Minimize performance drains

As mentioned earlier, many backup administrators manage data protection for virtual machines as if they were managing separate individual physical systems. Another example of this is deploying backup agents on each VM and running backup jobs in defined backup windows in order to avoid hurting the performance of business operations on the system. Often backups are run during off-peak hours, usually at night.

Unfortunately, this approach has a significant impact on the virtual machine host and VMs. The host system must take on the extra processing load and absorb latency increases due to I/O contention during the entire backup window, slowing all VMs on the host until all scheduled backups are complete. Adding to this impact is increased network traffic and latency due to the increased volume of data traveling to the backup server.

Our tip is to use dynamic resource management to free unneeded resources; when resources are taken only when needed, limited or scarce resources can be shared among processes. You can also reduce performance impact by simplifying your backup infrastructure with a flexible tool that can adapt to your network layout (LAN, WAN, or storage network), shifting the load of data protection operations away from the networks critical to business performance. For even greater benefits, choose a tool that provides flexible backup methods (proxy, direct-to-target, LAN-free).

Reducing the impact of backups on your network, servers and applications will enable you to save on hardware and infrastructure costs. It will also help your current infrastructure perform better so you have room for growth without spending more money. In other words, with the right tools, you can do even more with less.

Tip #5: Protect to fit your needs and SLAs

You have different SLAs and infrastructure for different applications and data. Your data protection solution needs to adapt to fit your needs—not the other way around. Your data protection tool shouldn't force you to conduct your data protection operations in a way that interferes with your production systems and networks. You should back up only as often as you need to meet your SLAs, in order to minimize effort and load on your production systems and networks.

Therefore, choose a flexible tool that offers a choice of networks and a method to be used for data protection: LAN, WAN, server-less. We recommend an image-based data protection tool because images are very portable, allowing you to recover when, where and how you need to for the greatest efficiency. We also advise choosing a tool with flexible licensing to provide the best fit for your environment while costing as little as possible.

Most of all, choose an architecture that fits the SLAs for your organization. The correct architecture for your business depends on the hardware and setup you have today; *there is no one-size-fits-all*. Understanding the options here is arguably the most important part of the equation when designing a virtualized disaster recovery system. Regardless of which image-based tool you are using, you need to configure it correctly, which includes, among other things, choosing the correct source method and understanding data flow and proper positioning of targets.

Finally, choose a tool that offers a variety of architectural options for deployment: network-based, direct-to-target, iSCSI, fiber and both ESX and ESXi backups. This will ensure you can set up your backup regime in a way that makes sense for your environment.

Conclusion

Following these five tips will dramatically increase the effectiveness of backup and recovery in your virtual environment, but to implement them you'll need a powerful and flexible virtual environment data protection tool. Quest vRanger Pro makes VMware virtual machine backup, restore and replication simple, fast, affordable and scalable.

Quest vRanger Pro from Quest Software includes all the features you need to fully implement these five tips, protect your data, and minimize the size of your backups.

vRanger adds Active Block Management (ABM—patent pending) which skips over deleted data, unlike VMware's API for Changed Block Tracking (CBT) alone. In continually changing environments, this reduces the size of your backups by eliminating many gigabytes of pointless extra backup. vRanger reduces space requirements, network bandwidth and backup and restore time, without sacrificing data protection.

vRanger maximizes speed and throughput for backup and restore operations. It:

- Allows simultaneous backup and restore to avoid bottlenecks
- Offers flexible backup methods (proxy, direct-to-target, LAN-free) to fit your environment and minimize workload impact
- Eliminates the need for a backup server by sending backup images directly to target storage

vRanger offers great flexibility in recovery options. It:

- Restores with one-click – there's no need for pre-staging
- Restores files at the file level as well as application objects
- Restores to a VM or a physical server
- Offers sweep-to-tape integration that can be used with a traditional backup tool—simply restore it to the repository, import the manifest, and start restoring files or VMs as you please

vRanger minimizes performance drains. It:

- Uses dynamic resource management to free unneeded resources; when resources are taken only when needed, limited or scarce resources can be shared among processes
- Adapts to your network layout (LAN, WAN or storage network), shifting the load of data protection operations away from the networks critical to business performance
- Provides flexible backup methods (proxy, direct-to-target, LAN-free)

vRanger enables you to backup only as often as needed to meet your SLAs. It:

- Offers a choice of network and method to be used for data protection: LAN, WAN, server-less
- Allows you to recover when, where and how you need to for the greatest efficiency using its image-based data protection tool
- Has flexible licensing to provide the best fit for your environment while minimizing costs
- Offers a variety of architectural options for deployment: network-based, direct-to-target, iSCSI, fiber, and both ESX and ESXi backups

Quest vRanger provides ESX and ESXi image-based VMware backup, replication and recovery that's simple, fast, affordable and scalable.

The Quest® vRanger product family speeds VMware backup and replication while dramatically reducing storage requirements. Choose the solution that best meets your needs:

- **vRanger Standard Edition (SE)**: simple, fast, affordable **VMware backup** and restore
- **vRanger Pro**: all SE features, plus VMware replication for comprehensive VMware data protection in one simple interface.

Simplify your disaster recovery plans for vSphere with one-pass **ESX / ESXi backup** that includes granular restore capabilities across files, objects and applications. Improve disaster recovery plans on site or at a remote site with efficient **VMware** replication and easier access during data protection efforts.

Quest also offers free online training resources to help you make informed decisions regarding proper setup. And there is a free training portal where you and your staff can take advantage of training offered for all Quest products, *all at no additional cost to your business.*

No one makes obtaining efficient, affordable and powerful disaster recovery tools easier than Quest. Quest Software ensures simplicity at work.

About the Author

Daniel Lord, senior product marketing manager for the Quest Server Virtualization Group, brings to market data protection products, including vRanger. Daniel has more than a decade of experience in product marketing, product management, and systems engineering at Oracle, Veritas and Sun MicroSystems, focusing on backup and recovery, storage, and systems management technologies. Daniel has earned a B.S. in Engineering from San Francisco State University and an MBA from Santa Clara University.

Quest Software, Inc.
Attn: Legal Department
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: **legal@quest.com**

Trademarks

UPDATED: February, 2011

About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for application management, database management, Windows management, virtualization management, and IT management, go to **www.quest.com**.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

E-MAIL **sales@quest.com**

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at **https://support.quest.com**.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.

QUEST SOFTWARE®

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.