Software

Superior VMware® Protection for Limited IT Budgets

Introduction

How server virtualization is complicating backup, replication and recovery strategies

Server virtualization is having a profound impact on IT departments. According to Gartner, the majority of new server workloads became virtualized in 2011, and that trend has accelerated since. In some data centers today, 80 to 90 percent of the applications are running on virtual machines (VMs).

The impact of virtualization on other aspects of data center operations is also accelerating, especially in the area of data protection. Server virtualization requires changes to backup, replication and recovery strategies, as well as to the organization's disaster recovery and business continuity plans.

For example, recovering virtual servers that host multiple VMs, each with its own data images, can take significantly longer—upwards of several hours or more. This need not be the case, but satisfying stringent recovery point objectives (RPOs) and recovery time objectives (RTOs) in a virtualized environment requires greater granularity and other changes in backup, replication and recovery capabilities.

Data protection is being further complicated by other forms of virtualization involving data storage in both private and public clouds. Gone are the days when administrators could identify the physical disk where every file was stored. Now an organization's data might be scattered throughout a hybrid cloud consisting of a variety of internal and outsourced applications and data warehouses, each of which requires a suitable backup, replication and recovery strategy.

The situation is not all negative, of course. Indeed, some backup, replication and recovery solutions take advantage of virtualization and cloud architectures to enhance capabilities or simplify operations. Dell™ vRanger™, for example, is able to replicate VMs between primary and secondary data centers in a private cloud to facilitate rapid failover and recovery. And Dell™

A typical organization has a range of applications with different RPO and RTO requirements.

AppAssure™ uses "hot standby" VMs with near-continuous block-level updates from the source server to enhance disaster recovery preparedness.

About this document

This white paper, intended for IT administrators and managers, is organized into two sections followed by a brief conclusion. The first section assesses the four key criteria in a data protection strategy for a VMware environment. The second section highlights how two solutions from Dell Software, AppAssure and vRanger, together provide comprehensive data protection for VMware environments more cost-effectively than any single solution could.

Data protection in a VMware environment

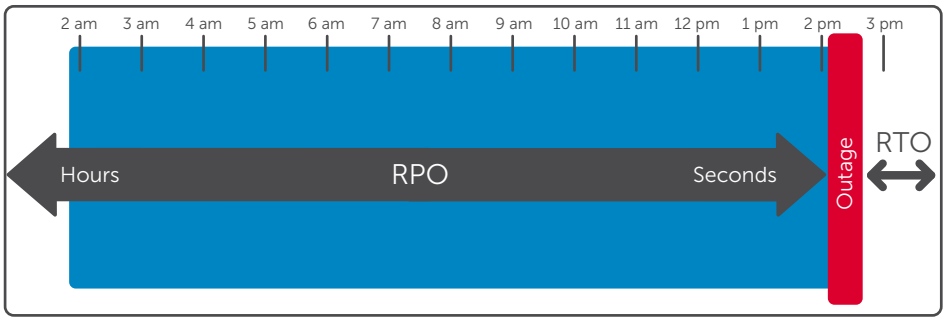
A robust VMware data protection strategy should satisfy the following four criteria, each of which is discussed in turn in this section:

- Support a broad range of recovery point objectives and recovery time objectives
- Be simple to install, operate and manage
- Ensure high performance, scalability and integrity
- Provide granular backup and recovery for both virtual and physical servers

Support for a broad range of RPOs and RTOs

The recovery point objective is the point in time to which data must be recovered after an outage or failure. The RPO is determined for each application by a combination of how frequently the data is updated and how much data loss is tolerable. For applications where the data rarely changes or that have a high tolerance for data loss, the RPO can be quite high: a day, a week or even longer. For applications where data loss can cause substantial financial losses or other major problems, the RPO can be as short as minutes, thereby requiring near-continuous data protection (near-CDP).

The recovery time objective is the amount of time between detecting a loss or failure and being fully restored to normal operations. The RTO must take into account the number and sizes of files required for a full recovery, which is often dependent upon the RPO. For example, a critical application with a short RPO can require three files during the recovery: a full backup, an incremental backup (all changes since the most recent full backup), and the transaction log (all transactions since the most recent incremental backup). By contrast, static or archival data can



Nightly image-based backups for less critical applications

Minutes between backups for more critical applications

Replication with rapid failover for the most critical applications

Figure 1. The RPO for an application depends on how critical it is to the organization's operations.

normally be restored from a single full backup file. In either case, granular recovery capabilities (discussed below) can dramatically decrease recovery times for many applications.

A typical organization has a range of applications with different RPO and RTO requirements, as illustrated in Figure 1. It is also common to use different data protection solutions that have been optimized for different needs. For example, one solution might be designed specifically for nightly backups of less critical applications, while another is needed to provide near-CDP operation or other capabilities to accommodate mission-critical needs.

Why should the data for some applications be protected with only a nightly backup when solutions exist that support much shorter RPOs with more frequent and even near-continuous data protection? The reason is that the additional protection requires additional effort and cost, which cannot be justified for many, if not most, applications. For example, some applications use archival data that changes only on a weekly, monthly, quarterly or annual basis, making even a nightly backup unnecessary. And solutions that automatically discover and backup VMs nightly without requiring the installation of special agents afford considerable savings of time, money and effort, while providing adequate data protection for most applications.

Another consideration for RPOs is the ability to recover to a backup other than the most recent one. This need usually occurs when data becomes corrupted somehow, such as by a virus or an incorrectly coded SQL statement, but the corruption is not immediately detected. Naturally, this ability requires retaining backups for an extended period of time, and more frequent backups require proportionally more storage space to retain. The optimal retention period for each application depends on how much time might pass until corruption is likely to be detected, the size of the backup file sets (preferably after being deduplicated and compressed), and, of course, the storage space available, potentially made much larger by archiving to tape.

Simplicity of installation, operation and management

Backup, replication and recovery solutions vary widely in how easy they are to install, operate and manage in virtualized environments. And as is often the case, there may be tradeoffs involved. For example, a solution that requires an agent would be more difficult to install, but agents are needed to provide advanced functionality, such as near-CDP, global deduplication, and granular recovery capabilities that require reading data block-by-block.

The architecture of a solution often affects its ease of installation and use. Some are software-only solutions capable of running on ordinary virtualized or dedicated servers. Others are configured as dedicated appliances with specialized hardware that might perform advanced functions like deduplication and compression. The latter affords better performance, and can also simplify certain procedures. For example, limited storage space often makes backup file management a constant task, while the much smaller deduplicated or compressed files alleviate the need to constantly be deleting "old" files—some of which might not be so old and might be needed to recover from data corruption some day!

The best backup and recovery solutions have capabilities purpose-built for specific environments—in this case, VMware. These solutions are able to leverage various VMware features or application programming interfaces to minimize and possibly eliminate duplicate effort. Examples of VMware APIs useful in data protection include those for Changed Block Tracking (CBT), vStorage and vCenter.

Backup, replication and recovery solutions vary widely in how easy they are to install, operate and manage in virtualized environments.

Job parallelism is one of the best ways to accommodate shrinking nightly backup windows.

High performance, scalability and integrity

Backup windows are shrinking and many applications now operate 24x7, especially in multi-national organizations. So regardless of the RPO, backup and replication operations must complete quickly and in a non-intrusive manner. This is particularly true for applications with a stringent RPO, where backups are being taken quite frequently or nearly continuously. A good way to ensure non-intrusive operation is to employ real-time resource governing, which allocates server resources (particularly CPU) to the backup job only when doing so will have little or no adverse impact on application-level performance.

LAN-free backups using a separate fiber optic or other network, although more expensive, are an option for those backup jobs that tend to consume too much bandwidth. The separate network enables the backup jobs to complete faster (especially on ultra-fast optical fiber), and removing the backup traffic from the data center LAN preserves its full capacity for production application workloads.

Scalability has two dimensions, time and space, both of which are familiar to administrators. As for time, backup job parallelism is one of the best ways to accommodate shrinking nightly backup windows, and the larger the data center, the more likely this is to be a necessity. Virtual appliance capabilities also help by enabling backup operations to be spread across the virtual infrastructure.

Similar relief is possible in the space dimension through deduplication and compression. The smaller files not only reduce storage space requirements—perhaps dramatically—but they also enable longer retention periods, which can improve data integrity by affording at least partial recovery from data corruption. Deduplication and compression also reduce the time it takes to replicate backup files across the WAN.

Granularity for virtual and physical servers

That extraordinarily rare but awful screeching sound of a hard disk drive head crashing makes it certain the server will require a full, bare metal recovery. Various other failures might also make it necessary to fully restore the hypervisor and all of the virtual machine images on a physical server. But the damage caused by most problems is often limited to only a single VM, or a single folder or file.

The key to greater granularity is the ability to search deep within the entire set of backup files. The best searches are also fast, based on having a complete catalog, and permit both specific and "wildcard" searches to afford greater flexibility. The ability to find and restore individual files with file-level recovery (FLR) helps satisfy stringent RTOs and can save administrators a considerable amount of time and grief.

VMware data protection solutions from Dell Software

No single backup and recovery solution could possibly be optimal for all of the broad range of applications normally found in a virtualized environment. The more sophisticated solutions are "overkill" for most applications, while solutions that emphasize simplicity often lack the advanced capabilities needed to protect mission-critical applications adequately.

For this reason, Dell offers two software-based backup, replication and recovery solutions for VMware: AppAssure and vRanger. Together, they provide comprehensive and cost-effective data protection for the full range of virtualized applications, as shown in Figure 2. A third product, the Dell™ DR4100 Disk Backup Appliance, provides optional hardware-based deduplication and compression to minimize storage space requirements.

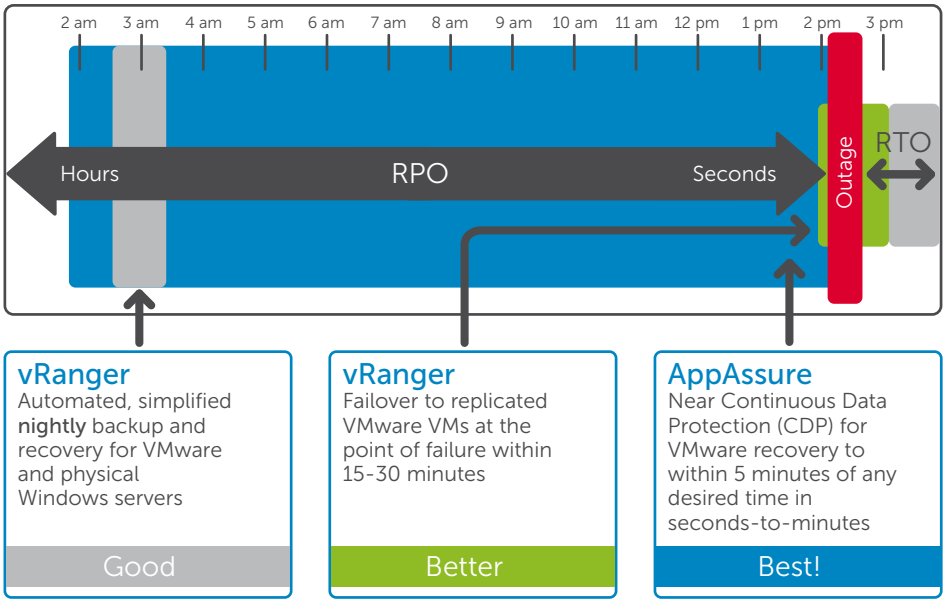


Figure 2. Together, AppAssure and vRanger provide complete and cost-effective data protection in virtualized environments.

AppAssure features near-continuous data protection with built-in replication to a secondary site or the cloud.

AppAssure

Designed for virtual, physical and cloud environments, AppAssure is backup and recovery software that features near-continuous data protection with built-in replication to a secondary site or the cloud. The no-impact "hot" backups require no downtime, providing near-continuous protection with no adverse impact on application performance. Support for near-zero RPOs, with snapshots taken as frequently as every five minutes, provides up to 288 recovery points in a 24-hour period. And support for near-zero RTOs is afforded by a Live Recovery™ feature capable of getting applications up and running again in 15 minutes or less after a failure.

In addition to these basic capabilities, AppAssure offers several additional capabilities that are beneficial in most environments. The use of "hot standby" VMs with continuous block-level updates from the source server enhances disaster recovery preparedness. The size of backup files is reduced by as much as 80 percent with built-in data deduplication and compression. And a granular, message-level search and restore capability for Microsoft Exchange and SharePoint make it easier to recover from many common problems more easily and quickly.

vRanger

vRanger software is designed for simple and affordable backup, replication and recovery in virtual VMware and physical Windows Server® environments. The agentless design simplifies data protection for the entire virtualized environment by detecting and backing up VMs automatically via VMware APIs, and the virtual appliance architecture scales to support even the largest VMware installations.

Scalability is further enhanced by the Direct-to-Target architecture and job parallelism that dramatically reduce backup, replication and recovery times, while Resource Governing ensures that applications are not adversely impacted during backup operations. Patented Active Block Mapping (ABM), with only the active blocks being read and written, improves backup performance and reduces storage space requirements by up to one-third. And combining vRanger's ABM with the DR4100 Disk Backup Appliance delivers industry-leading backup storage savings.

vRanger's agentless design simplifies data protection for the entire virtualized environment by detecting and backing up VMs automatically via VMware APIs.

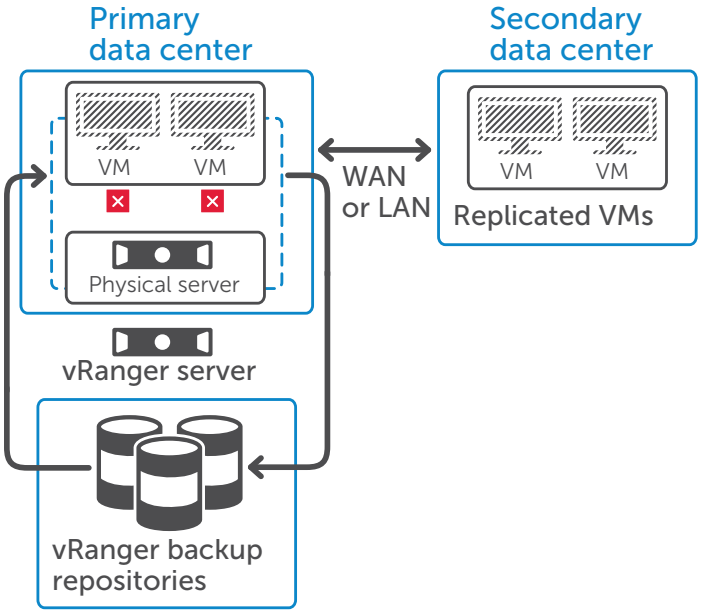


Figure 3. Replication of VMs between primary and secondary data centers (and vice-versa) enables rapid failover and recovery.

Productivity is enhanced by vRanger's integrated backup catalog, which enables administrators to locate individual files and folders quickly using keyword and wildcard searches, and restore them just as quickly with a single click. vRanger also provides a very cost-effective way to replicate VMs. Replicating VMs both locally and remotely, as shown in Figure 3, enhances disaster recovery preparedness by enabling rapid VM failover and recovery at all sites, whether primary or secondary.

Dell DR4100 Disk Backup Appliance

The DR4100 provides target-based deduplication and compression, and is certified for use with vRanger and many other backup solutions, including Dell™ NetVault™ Backup. By removing redundant data in-line from the backup work stream and compressing the results prior to storing and replicating the files, the DR4100 dramatically reduces both disk space and WAN bandwidth requirements. The DR4100 also offers a cost-effective way to support multiple backup workloads, as well as to consolidate and optimize data protection for multiple remote offices with a single, easy-to-manage solution.

The high-performance, disk-based DR4100 appliance is easy to deploy and manage, and affords a low total cost of ownership. The DR4100 is a 2U-high, rack-mountable appliance available in a range of RAID-protected logical capacities—from 40TB to over 400TB based on a 15:1 reduction ratio—making it ideal for small enterprise, remote office and multi-site environments. The system supports both 1GbE and 10GbE interfaces, and the 12 integral disk drives are protected against individual failures in a robust RAID6 configuration.

Summary

Server virtualization and cloud architectures are having an urgent and profound impact on data protection strategies. A complete VMware data protection strategy should meet four criteria: support for a broad range of RPOs and RTOs; simplicity of installation, operation and management; high performance, scalability and integrity; and granular backup and recovery for both virtual and physical servers.

No single backup and recovery solution could possibly satisfy all four criteria in an optimal and cost-effective way.

For this reason, Dell recommends a combination of AppAssure for near-continuous data protection for mission-critical applications, and vRanger for automating nightly backup and replication functions.

To learn more about how your organization can benefit from using AppAssure and vRanger backup, replication and recovery solutions, please visit software.dell.com/products/appassure and software.dell.com/products/vranger, where you will also find links to additional informative resources and free trial versions of the software.

Dell recommends a combination of AppAssure for near-continuous data protection for mission-critical applications, and vRanger for automating nightly backup and replication functions.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.