Realtime publishers

Managing Your Virtualized Environment: Migration Tools, Backup and Disaster Recovery

The Essentials Series

sponsored by

Dan Sullivan

Copyright Statement

Ongoing Operations: Backup, Disaster Recovery, and Data Protection

Maintaining your virtualized environment will require attention to backup, disaster recovery, and data protection. Although there are many similarities between these operations in non-virtualized and virtualized environments, there are significant differences as well. This concluding article on managing virtualized environments will examine:

- The need for virtualization-aware backups
- Key features of backup solutions
- Disaster recovery and data protection considerations
- Management concerns related to backup, disaster recovery, and data protection

The purpose of this article is to help you understand how to choose and deploy a backup solution that will meet your particular requirements.

Need for Virtualization-Aware Backups

A typical backup solution for non-virtualized servers includes a software agent that runs on the server and transfers data to a backup server, which in turn, writes data to a backup device. In theory, this setup might appear to work for a virtualized environment, however, this process can cause challenges in a virtual environment. To deal with these challenges, you need a virtualization-aware technology so that you can save on resource consumption, whether storage or network related.

If your backup solution is licensed on a per-agent basis, the cost of licensing your backup solution could increase dramatically. Before you deploy an agent-based backup solution in a virtualized environment, consider the licensing structure; site-licensing or physical server-based licensing will not constrain your ability to deploy additional virtual machines as needed.

Key Technical Features to Consider

Virtualization-awareness is just one of the features that a backup solution should provide. In today's enterprise, backup solutions have to support heterogeneous environments, provide features required for regulation compliance, and help control costs of backup storage. When evaluating backup solutions, consider:

- Support for multiple virtualization solutions
- The ability to perform live snapshots
- Support for migration
- Compliance issues, especially encryption
- Support for data compression

These features will affect both the cost and efficiency of backup operations.

Support for Multiple Virtualization Solutions

Enterprises have long supported multiple operating systems (OSs) so it is no surprise that they would also deploy multiple virtualization platforms. Organizations choose virtualization platforms and OSs based on different sets of requirements, availability of applications, cost, and other factors. Enterprises rarely have a wide range of disparate backup requirements. A single comprehensive backup solution should be sufficient for most organizations. That is, as long as the backup solution supports multiple virtualization environments.

Perform Live Snapshots

There was a time when you could assume that most of the demand on your applications would occur during "business hours." This situation left the night as the ideal time to perform backups. Those days are gone. Applications are used continuously. The amount of data requiring backup continues to grow to the point where traditional nightly backup windows are not long enough to complete backups. Another approach is needed.

With live snapshots, you can quiesce the VMs and make snapshots at any time. Creating a snapshot happens quickly, so there is minimal impact on VM performance. This ability to make live snapshots is essential to allowing VMs to continue operations while ensuring that sufficiently frequent backups are always available.

Support for Migration

Backups are primarily used to protect systems in the event of a failure, but there are other uses as well. A backup of a VM can be used to migrate a VM to other physical servers running a hypervisor or to a physical server. This capability makes VM backups a useful tool for supporting migration—that is, as long as the backup solution supports restoring a VM to a device or hypervisor different from it source device or hypervisor.

Support for Compliance

Businesses in healthcare, financial services, and government as well as publically-traded companies are subject to a number of regulations designed to protect the confidentiality and integrity of business and personal information. Many such regulations require security controls to mitigate the risk of disclosing private and personal information. These typically require that data is encrypted both when it is stored on devices and when it is transmitted over networks. If a backup tape or drive were lost or stolen, it could constitute a data breach under regulations. Backups that provide the ability to encrypt data as it is backed up can reduce and virtually eliminate the risk of a lost backup tape leading to the disclosure of private information.

Support for Compression

VMs must keep all of their state information and data uncompressed when executing. When stored on a backup device, however, the VM can be compressed. This setup can save substantial amounts of storage and ultimately reduce the cost of operating and protecting your virtualized environment.

Backups are essential in virtualized environments just as they are in non-virtualized environments. An appropriate backup solution should include support for multiple virtualization platforms and rapid backups using snapshots as well as support for migration, compliance, and compression.

Disaster Recovery and Data Protection Considerations

Backups are a basic building block of disaster recovery, but disaster recovery brings additional demands on how you use those backups. Imagine your data center is lost to a fire, flood, or other natural disaster. You have backups of all of your virtualized servers at an offsite location. You've secured a disaster recovery site with a mix of hardware. Now comes the real test. Can you restore your operations with full VMs restored to the same hardware configuration, full VMs restored to different hardware configurations, or selectively restore files from VM backups? These are all scenarios you could encounter during a recovery operation. In fact, unless you have an identically configured recovery site, you will probably find yourself restoring to a different set of hardware.

When selecting a backup solution, be sure to consider the range of possible options you might need in a disaster recovery situation. You would not want to find out during a restore operation that your backup solution does not restore to dissimilar hardware or requires you to restore a full VM just to restore a few files.

Management Considerations

When it comes to backups, disaster recovery, and data protection, there is no shortage of management considerations. In some cases, there is overlap between technical and management considerations. Some of the most important features to assess in a backup solution, at least from a management perspective, include:

- Cost and licensing model
- Support for centralized management
- Support for existing storage media
- Deduplication of data
- Policy-based backup
- Support for hybrid virtual-physical environments

These factors all have the potential to impact the cost and efficiency of operations.

Cost and Licensing Model

As with virtualization platforms, there are many ways to price a backup solution. Site licenses and per-physical server licenses are probably the easiest to plan around. When license charges are based on the number of VMs using the backup system, estimates are more difficult. For example, would you pay per backup agent deployed to a running VM? Or perhaps by backup agent deployed to a VM image regardless of whether it is running? Be sure to understand the licensing model as part of your evaluation to avoid unexpected surprises down the road.

Centralized Management

Centralized management features can streamline backup operations. Look for backup systems that support:

- Remote agent installation
- Centralized backup plans
- Monitoring and reporting

Each of these features can help reduce the administrative overhead associated with performing and managing backups.

Support for Existing Storage Media

Do not overlook the fact that your business might have a substantial investment in backup storage media. If you have to invest in a different media in order to use a new backup solution, be sure to factor that cost into your decision.

Policy-Based Backups

Not all data or applications are equally valuable. Some data and systems should be backed up more frequently than others. Consider the plight of a systems administrator who has to code a script with exceptions to the rules for backups. As new VMs are deployed, the systems administrator will have to add the new VM to the proper script. As users change their requirements for backup, the systems administrator will have to delve into scripts again to make changes. A more efficient method is to define policies that describe the backups that are to be performed based on characteristics of the target systems.

Deduplication of Data

Data is often redundant. Backing up every block of data, even if an identical block has already been backed up, is a costly option. Backup vendors have implemented deduplication technologies that detect duplicate data blocks within a backup. When a duplicate is detected, a reference to the first copy of that block of data is inserted into the backup instead of inserting another copy of the data block. Substituting a reference to a block of data for a block of data itself can substantially reduce the volume of storage required for backups.

Support for Hybrid Virtual-Physical Environments

Organizations might find that they need to support a combination of virtualized and physical servers. For example, they might license enterprise software that is supported only when running on physical servers. In such a scenario, it's reasonable to deploy applications to VMs only when there are no restrictions on virtualization. Ideally, the business should not need two backup solutions, one for their virtual servers and one for their physical servers.

Summary

Backup, disaster recovery, and data protection are critical considerations in virtualized and physical server environments. When assessing the right backup solution for your organization, remember the need for virtualization-aware backups as well as key technical and management features of the solution. Also keep in mind the additional requirements imposed by disaster recovery and other data protection considerations.