Realtime publishers

The Essentials Series: The Evolving Landscape of Enterprise Data Protection

Leveraging Your Existing Infrastructure for Enterprise Data Protection

sponsored by

syncsort

by Dan Sullivan

Copyright Statement

Leveraging Your Existing Infrastructure for Enterprise Data Protection

Comprehensive and efficient enterprise data protection should not require substantial changes to your existing infrastructure. If you were to find that your company needed to deploy new operating systems (OSs) or make changes to database processes to implement a data protection strategy, it might be time to reconsider your strategy. This, the third and final article in the *Essential Series: The Evolving Landscape of Enterprise Data Protection*, discusses evaluation criteria for selecting an appropriate solution for your business.

Before delving into detailed evaluation criteria, it is worth noting two overarching principles. First, enterprise data protection should not require changes to core components of the IT environment, such as OSs, databases, email systems, or storage hardware. A second principle is that data protection methods should seamlessly support changes to OSs, storage hardware, and so on. The business environment is already dynamic and subject to many influences; data protection should not add another driver to that dynamic situation.

Evaluation Criteria for Enterprise Data Protection

To meet the flexibility requirements outlined in the two overarching principles, a data protection solution should support several features:

- Ability to redeploy to different disk configurations
- Source server flexibility
- Database-specific support
- Email-specific support
- Single point of management

Together, these criteria help to distinguish data protection solutions that can function within the constraints of dynamic IT environments from those that introduce more constraints on that environment.

Ability to Redeploy to Different Disk Configurations

You do not always have the luxury of restoring a backup image to the same device from which it was made. For example, a hardware failure on a server might require you to restore an application to another server with a different configuration. In particular, you should be able to restore to a device independent of:

- Disk manufacturer because you do not want to limit your options with future hardware purchases to a single manufacturer because some elements of the current collection of backups cannot be restored to a different manufacturer's device
- Disk quality because failover devices, particularly with disaster recovery, may not of the same quality level. Under disaster recovery scenarios, the business may be able to tolerate lower performance; IT should not artificially introduce the need for higher-quality disks in a disaster recovery center to support a limited backup application. In disk-to-disk data protection, the destination disks should be flexible in terms of manufacturer and quality.

This kind of necessary flexibility extends beyond disks.

Source Server Flexibility

As much as IT professionals try to leverage the benefits of standardization, it is not always possible to maintain a homogeneous environment. IT departments may have to support servers running a combination of Microsoft Windows and Linux OSs, for example. Even within these broad families of OSs, there are multiple versions and distributions that support a number of different file systems.

Database-Specific Support

Just as there are a variety of OSs found in midsized and large organizations, there is often a mix of databases. It is not unusual to find a combination of Oracle, Microsoft SQL Server, MySQL, and IBM DB2 running in the same business. Databases, though, present particular challenges because of the way they use files and write data blocks.

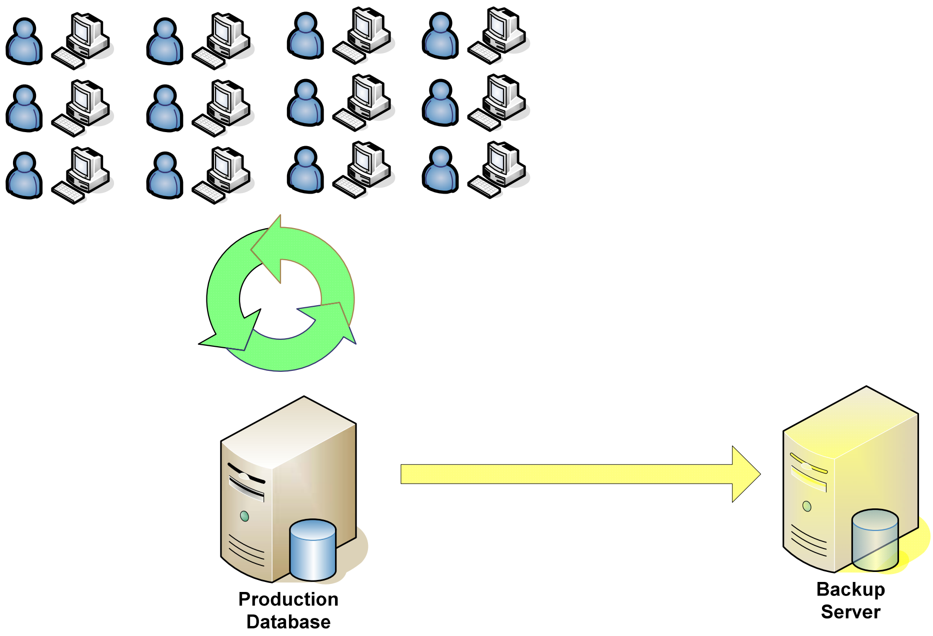

Figure 1: Database backups may have to be performed while users are actively updating the database. Such "hot backups" require special attention to transaction-level details to ensure a consistent state of the database is captured.

Databases are designed to provide logically consistent transactions. If you try to transfer funds from a savings account to a checking account and the system goes down before the transaction completes, during recovery, the database removes partially completed actions; you will never find the funds removed from your savings account but not added to your checking account. In a similar way, a backup should not represent a snapshot of a database in the middle of executing a transaction; it should represent a valid business state.

When restoring database objects from backups, it is helpful to be able to select subsets of the entire database to restore. For example, if an application programming error is discovered shortly after it is deployed, it may require restoring the database to a previous state. The erroneous program may have only affected a single table in the database. Ideally, you could restore just that table, not the entire database, from a known-good point. (Of course, this assumes that the other tables in the database are in a logically consistent state with the restored data.)

Email servers are another application with idiosyncratic backup and restore requirements.

Email-Specific Support

Although databases house the crown jewels of business operational data, email servers store vast amounts of communication records that can be just as essential to business operations. Email applications have developed to offer a wide range of personally customizable features, such as personal mailboxes and individual folders, as well as the ability to store and archive large volumes of email messages. An enterprise data protection system should include email protection features such as:

- Block-level recovery to allow email administrators to restore entire email systems in the case of a disaster or server hardware failure
- Fine-grained recovery options, including the ability to restore a single mailbox, personal folder, or individual message
- Rollback recovery to a specific point in time to eliminate, for example, a malware compromise on the email server
- Ability to create backups of email servers and email databases without shutting down the email server

Both databases and email servers are core service providers in the IT infrastructure. Data protection strategies should accommodate the way these systems function and should not require you to restrict their services in order to accommodate backup and recovery services.

Single Point of Management and Reporting

Ideally, all backup and recovery functions are accessible from a single console. When evaluating management and reporting features, look for the ability to:

- Monitor backup and restore operations from the console
- Perform log analysis and exception handling
- Optimize performance by analyzing bottlenecks and points of under-utilization
- Generate reports on historical trends
- Consolidate aggregate, enterprise-level reporting for upper management
- Provide both predefined reports for common requirements as well as custom reporting solutions for individual needs

The requirements outlined earlier—such as the ability to deploy to different disk configurations, support different source servers, provide application-specific support, and provide reporting and management features—are all technical evaluation criteria. The most commonly used measure of business value for technologies such as this is the return on investment (ROI).

The Most Common Evaluation Criteria: ROI

For all the technical features a data protection system may provide, the ultimate question that must be answered is: will it be worth the investment? To answer that question, you must take into the account the initial product cost and the time and resources required to install and configure the system. Perhaps more importantly, though, you must consider the additional costs or savings that may be realized during the life of the product deployment. These include considerations such as whether the system

- Supports minimal changes to infrastructure to support backup and disaster recovery
- Adapts to changes in OSs, databases, and email systems
- Reduces management and labor costs
- Optimizes configuration with information from comprehensive management reporting
- Uses a single backup for multiple uses, ranging from file restore to site disaster recovery

The ROI is closely tied to the technical criteria outlined earlier. In the case of enterprise data protection, what is good by IT professionals' standards is good for the bottom line.

Summary

When evaluating and selecting data protection products and services, it pays to ensure the selected systems account for the flexibility required by business operations. ROI can be significantly influenced by:

- The ability to reduce the amount of data copied from source systems, such as that found in source-side deduplication systems
- How well the data protection system exploits the advantages of virtualized servers for data protection
- The ability to leverage and accommodate existing infrastructure

Although no two businesses or organizations are exactly the same, shared patterns and practices are common. The best data protection solutions recognize and accommodate those common requirements.