Realtime publishers

Protecting Data with a Unified Platform

The Essentials Series

sponsored by

Acronis

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Unified Platform for Data Protection

Data is an increasingly valuable asset to businesses, governments, and other organizations; protecting this asset is an increasingly complex challenge. An essential requirement of any data protection operation is to ensure data can be recovered in the event of accidental loss or intentional destruction.

IT professionals have been creating backups as a routine course of business for decades. Unfortunately, practices that have worked well in the past might be insufficient to meet the needs of today's highly-distributed, heterogeneous computing and storage infrastructure. There is also growing complexity in the types and volume of data generated and used in today's business. Some data, such as documents, are stored in files that are well served by a basic model of backing up the entire file if there has been any change since the last backup. Other data, such as database records and emails, are stored in large, highly structured data stores that require specialized backup procedures. Backing up an entire database to capture the change of a single item is impractical, disruptive, and can lead to data loss. In addition, IT professionals must protect not only various data types but also multiple storage device types.

Protecting the full range of business data can become costly and time consuming unless a unified approach is applied to data protection regardless of platform, data type, or location. This guide outlines the benefits of a unified data protection solution and how a unified approach can be used to protect business data, ensure availability, and streamline business operations.

This guide examines five topics that span the range of issues IT professionals face today with regards to data protection:

- Employing backup, recovery, and data protection
- Addressing data protection in dynamic environments
- Ensuring data availability
- Streamlining data migration
- Considering issues with data protection in the cloud

Let's begin with a discussion of today's data protection challenges, what these trials require of IT professionals, and how you can leverage a unified data protection platform to address them.

Challenges to Data Protection

Data protection is a multifaceted problem that includes ensuring data is available, that it is kept confidential, and that its integrity is not compromised. The focus here, and in the articles in that follow, is on ensuring data availability and the role of backup and recovery strategies in that effort.

Backing up and restoring data is more challenging today than it has been in the past for multiple reasons:

- Increasing use of multiple platforms
- Increasing volumes of data
- Growing importance of unstructured and structured data
- Changing business drivers that shape IT strategy

Any one of these issues alone is enough to test the capabilities of your backup applications and procedures; it is not uncommon for a business to face multiple issues at the same time.

Increasing Use of Multiple Platforms

Organizations are adopting multiple computing platforms to meet their IT needs. It was not that long ago that a "heterogeneous environment" meant some combination of Microsoft Windows, Linux, and Apple Mac OS operating systems (OSs) were in use. It is still common to run multiple OSs, but that is just the beginning of a heterogeneous platform.

Virtualization is widely used to improve the efficiency and cost effectiveness of servers. Instead of running one application on one server, you can now run several applications, each in their own virtual machine, on the same server. With the advantages of virtualization come the challenges of managing another layer in the application stack. Backing up virtual machines presents new challenges that did not exist before. For example, should you backup the physical server as a single device without regard to the number and types of virtual machines? It sounds like a simple, straightforward option but this setup can run into a number of problems. Best practices for virtual machine backup suggests virtual machine–specific backups that take advantage of the virtualization platform's backup-related functionality is a better option.

As they do with OSs, organizations might find themselves running multiple virtualization platforms or hypervisors. The Linux administrators may prefer VMware's platform while the Windows server administrators find Hyper-V is a good fit for their needs. Ideally, IT administrators avoid the down-in-the-weeds implementation details of backing up these different platforms by using a unified backup platform designed to work with commonly used hypervisors.

The increasing use of cloud computing introduces another set of difficulties. Many organizations use public cloud providers for computing and storage services. Cloud providers typically offer redundancy in data storage to mitigate the risk of data loss, but that is no substitute for performing and maintaining your own backups.

Mobile devices, both company owned and employee owned, are increasingly popular for business and personal use. These devices can become ad hoc repositories of business data as employees draft documents, collect data in apps, and maintain their own data sets. The difficulties presented by protecting data on a diverse array of platforms are compounded by another issue: data growth.

Increasing Volumes of Data

In 2011, an estimated 1.8 trillion gigabytes of data was generated, and the rate of growth will continue to the point where we will have to manage 50 times our current data volumes by 2020. (Source: http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X_in_next_decade_IDC_study_predicts). This data will come from a variety of sources with varying levels of importance. The data generated by mission-critical applications must of course be protected, but large amounts of data are being generated in less obvious ways. Server logs can capture low-level details about events related to performance and security. Desktop devices can similarly generate data useful for diagnosing problems. Third-party data vendors can provide valuable marketing information derived from demographic and social networking resources. Business partners may share data to better integrate operations. These are just several examples of the wide range of potential data sources that contribute to the increasing volumes of data that need protection.

Growing Importance of Unstructured as well as Structured Data

Unstructured data, such as text, audio, and video, is another contributor to data protection complexity. These types of data can be especially valuable when automated techniques can extract pieces of information and map them to a more structured format. For example, a business that can collect customer surveys and opinions from sponsored surveys and Web sites and use text mining techniques to extract customer sentiment, complaints, and discussed features of products might find valuable information that is unavailable from other sources.

Changing Business Drivers that Shape IT Strategy

As businesses adapt to changing market conditions and long-term opportunities, the businesses sometimes have to change their IT operations. These changes can be relatively minor; for example, more closely integrating two existing applications. Other times the changes are more dramatic and require the introduction of new applications or processes, such as creating a new analytics group to consolidate and analyze data about operations and sales. These kinds of changes can have ripple effects on how data is used, updated, and shared. These effects, in turn, impact how we implement backup and restore operations.

There are clearly a number of challenges to data protection. As we start to address each of these, it can become clear that there are common requirements to meeting the challenges.

Common Requirements to Meeting Data Protection Challenges

Data protection challenges stem from the diversity of data types and platforms as well as the volume of data. It is not surprising then to realize that the common requirements for meeting these challenges tend to center on creating a unified perspective on that data.

IT professionals need a comprehensive view of data and backups. It is not efficient to use multiple backup systems to understand the status of your backup and restore operations. Doing so can require more time and training than is necessary. A single unified backup system can help reduce unproductive time, improve your ability to detect problems, and allow you to scale backup operations to meet the demands of growing data volumes.

A single backup system should also provide a single point of access to data regardless of the platform used. Ideally, a systems administrator could use a single interface to determine the backup status of a mission-critical application. Such should be the case even if that application consists of a Web application running on a Windows server, an application server running on a Linux server, and a database server running on another Linux server.

Ease of use is another common requirement. You do not want to deploy a large number of features in a way that becomes difficult for systems administrators to find the functions they need. There is a need to balance the right amount and types of functionality with the ability for users to access those functions efficiently.

Benefits of a Unified Platform

When you consider the challenges to protecting data and the need for common requirements, the advantages of a unified data protection solution come to light. The following list highlights just some of the advantages and benefits of a unified data protection system:

- **Fragmentation avoidance—**Multiple devices and application types make it is easy to create backup silos tied to different backup systems. This setup prevents the ability to have a single unified view of your data protection status.
- **Ease of use—**IT professionals often have multiple responsibilities and backup and recovery is just one of them. Applications that are easy to use can reduce the time and training required to effectively perform systems administration tasks.
- **Cost savings—**Licensing multiple backup applications can incur higher costs associate with the initial purchase price, ongoing support contracts, and training for each application. A unified solution can help avoid redundant costs.
- **Rapid, less complex recovery—**If multiple components of an application or database need to be restored, the restoration can require coordination across multiple backup systems. For example, a database may be restored with one system while the application services are restored with another.

- **Single platform training—**Applications and systems are important, but human resources are the most valuable part of a business. IT professionals can learn to manage multiple systems for data protection, but training on a single platform can save time and possibly reduce frustration for your most valuable resource.
- **Reduced administration overhead—**IT support applications, such as backup and recovery systems, are managed assets. They need to be installed, configured, upgraded, and patched. All systems require some degree of maintenance, so reducing the number of applications required for data protection can help reduce administrative overhead.
- **Scalability and flexibility—**Data volumes are growing. A backup solution will need to scale to meet your needs in the future. Keep in mind that you might be using additional platforms in the future, such as public cloud providers. Will your backup solution work with those additional platforms?

Summary

IT professionals are facing a range of challenges to protecting their organization's data. The complexity of IT systems coupled with growing data volumes and dynamic business environments are driving the development and deployment of unified data protection solutions. Unified solutions will not eliminate the challenges, but they can help mitigate the effects of the changing IT environment by providing a comprehensive, single point of access application for addressing a wide range of data protection needs.