White Paper

Business Continuity

Protecting Mission-Critical Application Environments

The Top 5 Challenges and Solutions for Backup and Recovery

MICRO FOCUS

Table of Contents

page

Executive Summary 1

Key Facts About Mission-Critical Application Backup and Recovery 1

Top Five Challenges and Solutions 2

Protecting Mission-Critical Applications with the Micro Focus Data Protection Suite 7

Executive Summary

The number one job of today's IT organizations is to protect applications, their data, and the entire infrastructure from the risk of data loss, corruption, and application malfunction—and to do so in an integrated manner, with minimal disruption. Mission-critical application environments are comprised of the software and hardware essential to the survival of an organization. This means that when a critical environment fails, is interrupted, or experiences data corruption, the business operations are significantly affected.

While most organizations combine hardware, hypervisor, and applications such as SAP, Oracle, Microsoft Exchange, Microsoft SQL Server, the tendency is to have a data protection strategy that looks solely at the data. However, to handle this complexity more effectively, it's important to shift to a more intelligent, flexible and scalable backup and recovery framework—one that looks beyond just data recovery and incorporates application awareness, storage integration, and operational analytics.

This white paper identifies the top five backup and recovery challenges in mission-critical environments and offers key considerations and solutions for your backup and recovery strategy. It closes with a list of advanced capabilities offered by the Micro Focus Data Protection Suite for protecting mission critical applications.

Key Facts About Mission-Critical Application Backup and Recovery

Protecting and recovering application data is different from protecting unstructured data (such as documents, emails, instant messages, video, and audio files). Here are key things you need to know about application data:

- Application files are referred to as open files because they are frequently updated and accessed. The backup process must coordinate with the application before performing a backup of its data.
- An application can consist of a set of files; for example data files, redo/transaction logs, control files, and cache files. All of these files need to be captured in a consistent manner because failure to do so can lead to backup data corruption and restore inconsistencies.

- Each application has a unique architecture and method to read and write data files. This also applies to the backup and restore process; each application needs to be backed up and restored in a unique way.

Top Five Challenges and Solutions

The following outlines key challenges for protecting your mission-critical workloads:

Challenges

1. Protecting Varying and Complex Application Workloads

You rely on multiple applications for day-to-day operations. Regardless of how they are classified independently (mission-critical, operational, supportive, and so on), they each have their own level of importance and must be protected in a manner that matches their value to the organization. For those classified as critical to the business, with little to no tolerance for performance degradation and downtime, you must take a more strategic approach to setting application recovery objectives. The reality is that traditional backup and recovery solutions and procedures fail to meet this challenge and often result in an attempt to apply a "one-size-fits-all" approach.

2. Protecting Virtualized Applications

Today, virtualization is just as commonplace as servers, storage, and networking. With many application vendors supporting virtualization platforms, it is not uncommon for organizations to virtualize their mission-critical applications. But protecting virtualized applications adds an additional layer of complexity to the backup process, requiring the backup and recovery solution to work in tandem with the hypervisor to ensure that none of the workloads are resource-starved in the process. Traditional backup and recovery approaches, however, are not practical for virtual environments, offering minimal support and burdening the virtual machine administrator with complex restore processes. Because traditional approaches are not designed for virtualized applications, attempting them proves costly with complex scripting, inconsistent backups, data corruption/loss, and more importantly, an unstable virtual infrastructure.

3. Inconsistent and Complex Application Recovery

Application owners define backup and recovery needs in terms of service level agreements (SLAs). Administrators use Recovery Time Objectives (RTOs) to marry the SLA to a backup configuration that matches the targeted duration of time the application is restored. During a recovery operation, the complexity of the process and the number of staff involved are the key inhibitors to meeting RTOs. In environments with distributed responsibilities (for example, application, virtual machine, backup, and infrastructure administrators) restore operations require multiple roles, with each administrator capable of completing only a partial restore operation. This results in a time-consuming and complex approach that leads to inconsistent recovery operations and failure to meet aggressive SLAs.

4. Dynamic and Agile Data Center Infrastructure

As IT organizations continue to rely on a combination of physical, virtual, cloud (private, public, and hybrid), and distributed data centers, the boundaries of IT are increasingly transparent. This means that there is not always a need for an application to reside in the same place and on the same infrastructure: with some applications remaining on physical servers, some virtualized, and others that can operate outside the core data center. With this kind of application mix and mobility, a traditional data protection approach results in a complex collection of backup and recovery tools that are specialized for the application and/or infrastructure it runs on. Having multiple backup and recovery tools at each location results in a heavy OPEX cost and equally complex and costly restore operations.

5. Infrastructure Saturation from Application Performance and Growth Requirements

Traditional backup and recovery solutions provide the level of infrastructure management required to balance the resource demands of the infrastructure and the performance requirements of the mission-critical applications being protected. However, attempting to force-fit a traditional solution often means the transmission of redundant information, underutilization of the backup infrastructure, and inefficient capacity management for backup operations. Data protection solutions that lack the ability to effectively schedule, balance resource loads, compress information, deduplicate redundant data, and offer intelligent insight and forecasting often result in mission-critical application disruptions, unreliable recovery efforts, inconsistent backup operations, and failure to effectively plan for future infrastructure needs.

Solutions

The increased business risks in mission-critical environments can seem daunting, but when you utilize today's advanced technologies and backup and recovery techniques, you can reduce your risk and enable the success, integrity, and security of your end-to-end business processes.

Here are five elements of a consistent, efficient, and policy-based approach to data protection for mission-critical environments:

1. Protecting Varying and Complex Application Workloads

Because each application has its own unique characteristics and importance to the business, the backup and recovery strategy should be just as unique and aligned to the application's criticality to the business. The more expensive the loss of data, the higher the rate of change; and for more critical applications, the backup and recovery policy should be more aggressive. This means the backup and recovery solution must provide support for non-disruptive backup and instant recovery, regardless of the complexity of the application. Achieving this requires a solution that is not only application-aware, but also integrated with the infrastructure.

Integrating with the infrastructure enables the backup and recovery solution to balance resource utilization by offloading certain aspects of the process to the device best suited to complete the task. For example, non-disruptive backups can be achieved when the solution relies on integration with the primary storage array to create snapshots—or space-efficient, point-in-time copies of the production data—as the source for the backup operation. This reduces the operational impact on the application while still providing a means to manage how aggressive the backup and recovery policy should be.

2. Protecting Virtualized Applications

Application-aware, hypervisor-integrated, and capable of utilizing the advanced features of the physical infrastructure are key to protecting your virtualized applications. Hardware and software vendors offer application programming interfaces (APIs) that cooperatively work with external applications to complete a joint task; for example, backup and recovery. However, to ensure optimum protection for current and future mission-critical applications you will require flexible protection approaches that include:

- **Agentless:** Backups coordinated via the hypervisor APIs
- **Agent:** Guest-level services for application and operating system combinations that do not support hypervisor utilities

- **A combination of the two:** A lightweight agent to prep the application and operating system, and agentless approach to offload the backup operation to underlying infrastructure

3. Inconsistent and Complex Application Recovery

Simplifying recovery operations should begin with instituting a data protection solution that offers application-awareness and provides application owners with direct visibility and ownership over the backup and recovery process. This enables your IT staff to focus on infrastructure tasks and places the responsibility of backup management and granular recovery in the hands of the application owner.

With the owner's specialized application knowledge and access to application-aware protection tools, the backup and recovery process greatly reduces the time-consuming and error-prone conditions that occur when multiple IT roles are required to complete the restore operation. Additionally, your IT staff can focus on building the data protection infrastructure to meet the aggressive SLAs and be assured that the actions taken by the application owner are within the scope of the greater data protection strategy.

4. Dynamic and Agile Data Center Infrastructure

Transparent IT boundaries and the fluid characteristics of the data center mean point-based backup and recovery solutions will only address the data protection challenges you currently face. More importantly, narrowing the data protection solution to a specific fit criteria increases the need to adopt multiple solutions. Instead, IT should be enabled to build a service-defined, rather than hardware-specific, backup infrastructure. With a service-defined approach, the focus is placed on the workload being protected, with the data protection solution managing the physical and virtual requirements (storage, backup target, network load, and so on) as resource pools. This approach allows you to align your SLA and RPO requirements with the data protection resource pool that has the features and capability mix to meet the requirements.

5. Infrastructure Saturation from Application Performance and Growth Requirements

The goal for meeting this challenge is to create a data protection solution capable of scaling in lock step with both the data growth characteristics of the organization and the aggressiveness of the backup and recovery strategy. This enables maximum infrastructure utilization while addressing the performance and growth requirements of mission-critical applications.

Combining a scalable and application-aware solution with the use of operational analytics is the key to transitioning data protection from a reactive IT operation into a strategic system that facilitates data-driven decision-making. When your data protection solution uses real-time analytics and monitoring, you can:

- Narrow the issue scope to improve resolution speed
- Provide recommendations to achieve maximum utilization
- Introduce corporate foresight to understand future mission-critical application needs based on how the infrastructure is being used

But What About…

- **High availability:** Using high availability (HA) as a means to protect mission-critical applications and have them readily available in the event of disruption improves RPO. However, the tradeoff is that HA creates a vulnerability by requiring continual replication of the application data to support a restart. If the application becomes corrupted, the corruption is replicated to the HA pair. Without the ability to restore the application to the point-in-time before the corruption occurred, the organization is at risk. Combining HA with an application-aware data protection solution delivers the best of both worlds.
- **Application clustering:** Application clustering is a technique that aims to reduce downtime to zero by instituting an automatic response to failure without the need for intervention when a node fails and can be used to increase the scalability of an application. Clustering and HA are often used in tandem, and like HA, without a data protection solution that understands the application cluster, the restore operation will be both time-consuming and error prone.
- **Distributing applications:** By distributing applications, you can select specific and group-specific parts of an application to run in different locations and divide tasks or resources among the groups. While this approach addresses application scale and resilience, like clustering and HA, the approach does not address the long-term data restoration needs that are required in the event of data corruption or loss. So it's essential that the backup solution be aware of HA, clustering, and distributed application configurations to ensure both success and integrity in the backup and restore operations.

Protecting Mission-Critical Applications with the Micro Focus Data Protection Suite

Micro Focus® Data Protection Suite enables a comprehensive, centrally managed data centric backup and recovery solution for critical data in the data center, in remote offices and across platforms. The Suite combines backup, restore, and disaster recovery capabilities with real-time monitoring and operational analytics to meet the scale and flexibility requirements of your most challenging data protection needs. It manages and protects data at all phases of the data protection cycle, all data formats—structured and unstructured, applications, and databases, and environments—physical or virtualized for a flexible, scalable data protection solution for the most demanding environments.

With a robust architecture that enables the offloading of data protection processing to different points in the infrastructure, along with an automated storage tiering across disk, tape, and cloud targets, the Data Protection Suite optimizes backup and restore for the often resource-constrained data protection process found in mixed environments.

The result is a data protection solution that gives your administrators the capability to organize, manage, schedule, and execute protection strategies by SLAs, without being tied to the physical or virtual components the workload is running on. The solution ensures business continuity and resiliency for mission-critical environments.

The Data Protection Suite offers advanced capabilities for protecting mission-critical environments:

- **Comprehensive integrations** enable backup, restore, and disaster recovery responsibilities to extend into the data protection process. Application-awareness allows backup and restore operations to focus on restorability. Hypervisor extensions support low-level interface integrations to enhance the backup operation and extend protection operations into virtual environment management tools. Hardware-acceleration means the management and orchestration of snapshots accelerate the backup and restore process. Granular options provide the ability to instantly restore single items, objects, or whole images.

- **Distributed granular recovery** enables administrators and application owners to recover single items directly from the application console, without requiring assistance from the backup administrator. The single-item recovery process is streamlined to allow application administrators to recover from disk or tape backups.
- **Operational analytics, reporting, and monitoring of data** helps in tracking and managing SLAs by identifying protection gaps, running rapid root-cause analysis for issues, and planning for future backup resources. Administrators can proactively identify issues before they cascade into outages and data loss, and run rapid root-cause analysis that provides trends and scenario-based modeling to discover potential scheduling conflicts, enabling better management and future planning of backup resources—all critical tasks in effectively running mission critical applications.
- **Enhanced automated disaster recovery**, also known as bare metal recovery, is the ability to centrally recover virtual or physical servers from a single backup. Unique to the Data Protection Suite, this recovery option enables you to create disaster recovery images from an existing file system or image backup, including object copies, without the need to create a separate backup for system recovery. The Data Protection Suite automatically rebuilds the application, the system, and the underlying infrastructure provisioning.
- **Federated deduplication,** when used with storage systems such as HPE StoreOnce Catalyst or Dell EMC Data Domain, ensures that only unique information is transferred from point-to-point using a deduplication algorithm prioritized by the backup target in use. This enables optimal capacity utilization and manageable network bandwidth consumption at varying levels of the backup infrastructure—at the source, the backup server, or the backup target.

Learn More At

www.microfocus.com/dataprotector

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com