Industry Trends and Technology Perspective White Paper

Enabling comprehensive data protection for VMware environments using FalconStor Software solutions

Issues and solutions to enable complete data protection and application availability for virtual server and storage environments

By Greg Schulz

Founder and Senior Analyst, the StorageIO Group

October 10, 2007

Server and storage virtualization are complementary technologies that support day-to-day business along with high-availability, business continuity (BC) and disaster recovery (DR) needs in a virtual data center environment. This paper looks at the issues and requirements for comprehensive data protection beyond simple server "crash consistent" restart in a VMware environment and addresses the importance of application-aware enabling data protection technologies.

Introduction

Server virtualization continues to gain popularity as a proven tool to improve resource utilization and simplify server management with server consolidation (Figure-1). However, along with benefits of consolidation come new challenges for high availability, business continuity (BC), and disaster recovery (DR). VMware Version 3 Infrastructure (VI3) has addressed some of these challenges through its baseline HA product for maintenance, dynamic workload changes, and load-balancing along with basic BC/DR in the form of crash consistent server restart.

To elevate VMware environments to the next level of high resiliency, many storage-minded organizations are beginning to explore storage virtualization and advanced application-aware data protection solutions such as offerings from FalconStor Software. This combination provides a powerful mechanism for implementing tiered application data storage and BC/DR to align with business needs and service requirements.

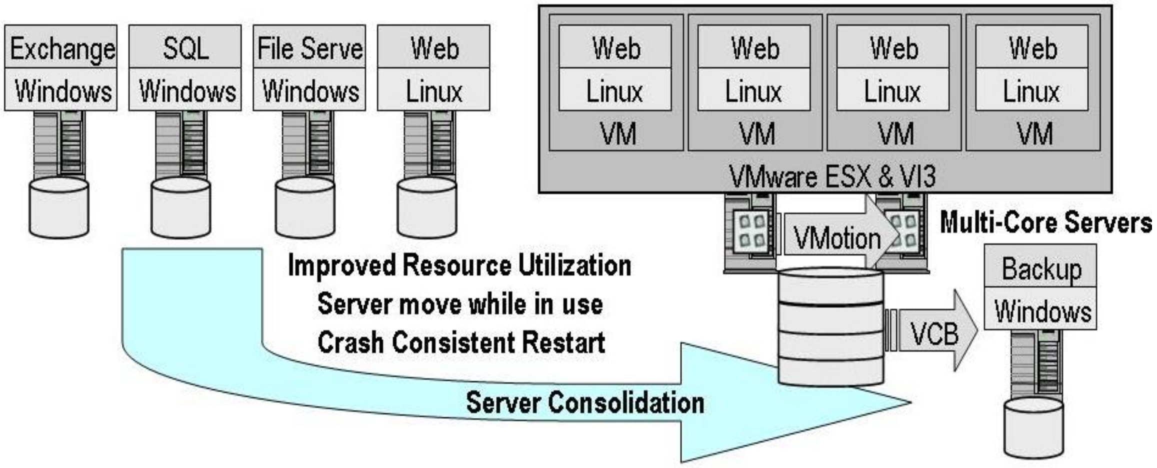

Figure-1: Server consolidation using VMware server virtualization and data protection

Server virtualization data protection challenges

The business and technology benefits of server virtualization are becoming increasingly apparent. In addition to supporting server consolidation to increase resource utilization and reduce costs, VMware VI3 powered server virtualization provides flexible deployment and movement of VMs, enabling baseline data protection and ongoing availability.

The flexibility of VMware enables consistent, simplified management to reduce application downtime due to infrastructure changes. A by-product of server consolidation is the collection of multiple applications that may or may not require high availability; however, the underlying infrastructure needs to be continuously available and resilient. Similarly, workloads in and of themselves may not be critical, top-tier priorities, but when VMware server virtualization enables tiered data protection across applications and servers, all workloads become critical and require enhanced BC/DR capabilities. Because of the aggregation of servers, these applications become reliant on server virtualization, data protection, and high availability. Consequently, there are now multiple “eggs” to protect in one “basket”. The net result of consolidating multiple servers is that multiple workloads can constitute a single point of failure.

Server virtualization business issues and impacts

The associated risks of a consolidated environment can now have a greater impact on more users should a disruption – planned or unplanned – occur. The virtual environment needs to be more resilient with extensible data protection for rapid restart and prevention of data loss. To support rapid application restart and avoid the extended delays associated with application data restoration and recovery, complete and application-aware data protection is needed to ensure that all data is copied in its current state.

Without application-aware data protection, the data essential for rapid application restart may be missing, forcing a time-consuming and disruptive data recovery and restoration process with possible data loss. Furthermore, without application-aware and context-based data protection, your virtual servers may restart; however, your applications may be missing critical data to resume or rollback processing as of the time of the failure. This further delays return to service.

What does application-aware mean?

- ✓ Collects the-data not yet written to disk
- ✓ Application context data protection
- ✓ Leverage application backup APIs
- ✓ Capture buffered data
- ✓ Maintain transactional integrity
- ✓ Preserve data state and consistency

Application-aware data protection is a feature that helps transform and move VI3 technology into the realm of a mission-critical, enterprise-essential enabling tool such as those traditionally associated with IBM Mainframe class computing and storage. Key to providing data consistency is the ability to leverage popular application integration agents and APIs for Oracle, Microsoft SQL, and Exchange, among others, for complete and comprehensive data protection.

VI3 environments with enhanced data protection capabilities such as those discussed in this paper are laying the foundation for mission-critical tier-one applications to be deployed with confidence on VMware-enabled platforms on a local and wide area basis. The primary objective is to eliminate data loss, maintain application-state and transaction coherency, reduce restoration and recovery time for BC/DR, and remove the complexity associated with traditional DR approaches.

Essential to a complete VMware BC/DR strategy is an architecture that can reduce or even eliminate restore, restart, and recovery time while minimizing the impact of backup processes. This will require the use of advanced protection capabilities such as the integration of application-aware snapshots, data replication, server and LAN free backup, and VI3 baseline server failover and restart capabilities.

Traditional server and application data protection

In addition to incurring server and operating system recovery time, organizations are faced with the challenge of restoring, recovering, rolling back, and restarting applications, along with corresponding data loss and application downtime. Another challenge with system recovery, particularly for traditional bare metal restoration, is the need to restore to a like physical application server that is the same make and model of what was backed-up. Furthermore, there is a financial and overall business impact of the time and resource consumption (CPU, memory, network and storage I/O performance) required to protect data from disaster through traditional backup methodologies.

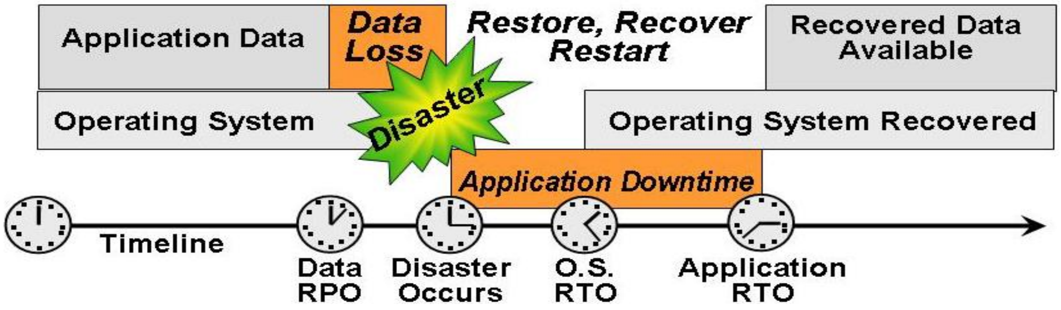

Figure-2: Standard VMware data protection using scheduled backups or snapshots

To help illustrate this point, Figure-2 shows a traditional application and server configuration and data protection model relying on direct or network-based backup. Data is protected up to the most recent backup or recovery point objective (RPO). However, any data that is added or changed between the RPO and time of failure is lost.

Baseline VMware and VMotion for rapid operating system restart

Leveraging the inherent capabilities of VMware VI3, VMs can be dynamically moved across different physical servers in a VMware ESX environment (locally or remotely) to support services maintenance or load balancing to meet changing workload requirements. Another ability of VMware VI3 environments is support for crash consistent automatic restart or "virtual" reboot, which is similar to a traditional server rebooting after a crash or failure. Thus, in Figure-3 by using VM and virtual re-boot, there is a slight improvement in availability by reducing the amount of time for operating system restart.

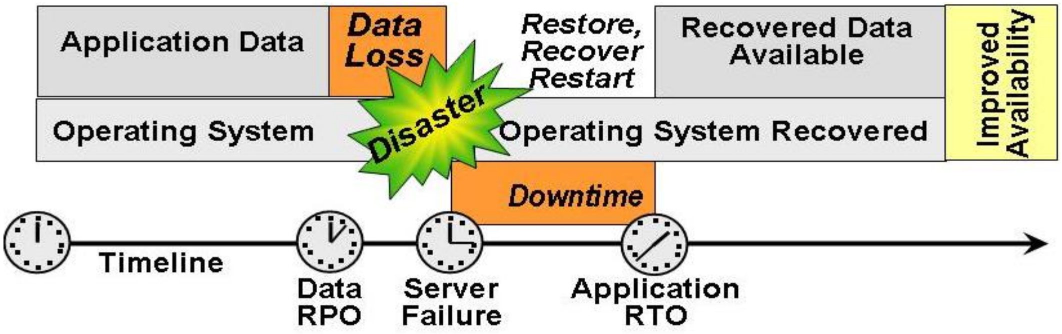

Figure-3: Leveraging VMware VI3 VMotion for rapid operating system restart

On the surface, this is a powerful capability; however, there are some caveats and pitfalls to be aware of, including the context of a crash consistent reboot, the RPO of application data, and associated RTO for systems and applications. There is still a time delay and associated downtime to recover application data to a known recovery point as well as possible data loss.

In other words, the virtual servers may reboot, but is 100% of the data in the correct state to restart and resume application service delivery from the point of failure? In most cases, the data is not consistent; therefore it needs to be re-built – a lengthy process.

VI3 enhanced with advanced data protection and replication

Since VMs are stored in files on disk, they can be backed up similarly to an open file and moved (VMotion) locally or across ESX implementations. While VMs provide crash-consistent recovery for reboot, application-state and changed data is not captured without using third-party advanced data protection tools. VMware provides for rapid server restart in the event of a server failure or crash. However, without integration of third-party technology, including application-aware snapshots and data replication, application and data recovery is dependent on the recovery point of when the last good known backup was performed and the timely restoration to that point.

To enhance a VI3 environment, Figure-4 shows how third-party data replication combined with application-aware data protection, such as the protection offered by the VMware-certified FalconStor® Continuous Data Protection (CDP) Virtual Appliance for VMware Virtual Infrastructure and FalconStor® Snapshot Director for VMware, eliminates data loss and minimizes the downtime due to lengthy recovery as compared to simple server crash recovery and reboot.

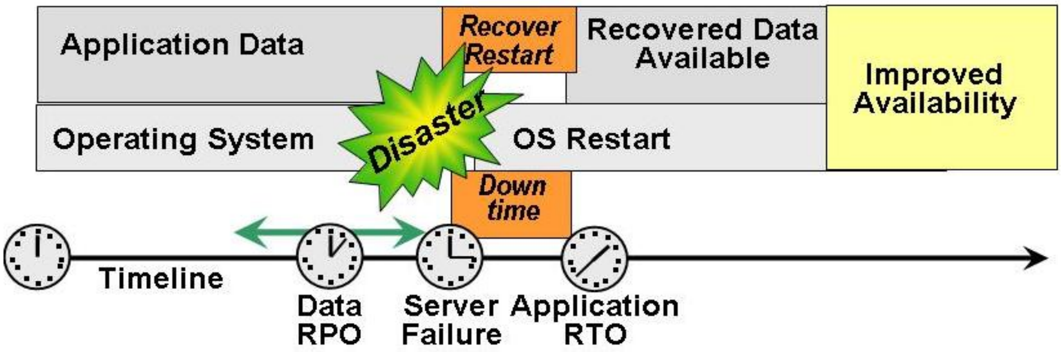

Figure-4: VI3 Application aware data protection to minimize data loss and downtime

In Figure-4 a VI3 environment with third-party application-aware technology, such as FalconStor CDP Virtual Appliance for VMware Virtual Infrastructure and Snapshot Director for VMware, ensures that all application data is captured in its current state and is replicated to a remote location to facilitate rapid application restart which minimizes the time required for recovery and eliminates data loss.

Another consideration pertaining to VMware based backup and DR is how bare metal restore to various models of physical servers will be handled as well as virtual-to-virtual (V2V), physical-to-virtual (P2V), and physical-to-physical (P2P) based data protection configuration scenarios.

FalconStor DiskSafe™ technology resides on application servers to capture all critical application data with full data consistency while enabling rapid bare metal restore to the physical servers. In addition to being able to leverage various application servers for rapid recovery and application restart, the flexibility to use any set of existing physical servers with an easy-to-use VM data protection solution makes DR testing more practical.

For example, FalconStor CDP Virtual Appliance running in either a VI3 VM or on a standalone server integrates with DiskSafe agents to capture all application state and transaction data while storing the data in a VM recoverable image format for rapid recovery based on dynamic recovery points. The result is rapid restore by accessing a loadable VM image on any available physical server with an available VI3 VM.

Enabling VI3 HA

VMotion is a tool for dynamically moving running VMs and their applications in a predicable manner for maintenance, load-balancing, or automated failover and restart due to loss of a physical server in a VI3 environment assuming the VMs have access to shared storage. Table-1 shows various baseline VMware

VI3 data protection capabilities to enable high availability and BC/DR along with enhancing overall data availability and application consistency with third-party solutions like those from FalconStor.

HA Functionality Components	What this means to an organization
Move VMs - VMotion • Move active VM to other server • Simple VM failover / restart	✓ Application-aware capabilities require 3rd party solution ✓ Data movers (replication and backup) are needed ✓ Provides for VM movement and basically failover restart
Distributed Resource Scheduler (DRS) • Resource monitor and dispatcher • VMotion for load balancing and HA	✓ Combine with VCB and snapshots for data protection ✓ Schedule VMotion movements for planned maintenance ✓ Automate planned downtime and scheduled maintenance
VMware enabled snapshots • Reduce backup window • Point-in-time crash consistency	✓ Lack application awareness for complete data capture ✓ Integrate with 3rd party data movers and protection tools ✓ Rapid file restoration from accidental deletion

Table-1: VI3 HA functionality and components

Enabling VI3 application-aware data protection for BC/DR

VI3 enables a simple backup called VMware Consolidated Backup (VCB) that provides a centralized facility for LAN-free and server backup of VMs. VCB is a mechanism by which third-party backup and data protection software interface to off-load backups from VMs. VCB consists of pre-processing scripts to quiesce the virtual disks so that a snapshot can be taken, and then un-quiesce to restore the VM back to normal running operations. The VCB scripts also make the snapshot accessible to a backup server where a third-party backup or data protection agent performs the actual data backup, copy, or replication. The net result is that VMs are off-loaded from CPU and I/O intensive backup processing and backup data traffic is removed from LAN networks. Building on the functionally components in Table-1 for VI3 HA, Table-2 shows components for implementing BC/DR.

BC/DR Functionality Components	What this means to an organization
VMware Consolidated Backup (VCB) • Combine with 3rd party backup tools • Off-load server and LAN of backup	✓ Requires 3rd party data backup tools to move data to tape ✓ Integrates with existing tools for investment protection ✓ Add application-aware support for complete protection
3rd party data replication required • Server, appliance, or storage system based • WAN-friendly and efficient data movement	✓ Provide data replication capabilities not present in VI3 ✓ Integrate with application-aware agents to capture all data ✓ Simplified management and reduced complexity
FalconStor Snapshot Director for VMware • Appliance-based heterogeneous replication	✓ Provides heterogeneous application-aware data replication ✓ Off-load servers and storage system replication overhead
FalconStor CDP Virtual Appliance for VMware Virtual Infrastructure • Application awareness • Deploy on a physical or virtual server • Data safe streamlines VM recovery • Variable and dynamic recovery points	✓ Enables bare metal restoration to unlike servers ✓ Facilitate rapid application restart with data integrity ✓ Supports rapid and simplified DR testing capabilities ✓ V2V, P2P, P2V data protection and recovery

Table-2: VI3 and 3rd party components to enable application-aware BC/DR data protection

Building on the baseline data protection provided by VCB and third-party data protection integration, application-aware agents ensure that all current data is written to disk in sequence with the virtual disk backup. Where a VCB backup of a virtual disk captures 100% of what is on the disk, only application-aware snapshots ensure that 100% of the data is on disk and completely protected. The benefit is that all data is captured and protected, including data in buffers as well as data on disk at the time of the VCB snapshot.

Therefore, an effective strategy to enable rapid restart and application resumption for BC/DR in a VMware environment needs to include application-aware data protection. Application-aware data protection, including snapshots and replication that capture an application's current data state, is needed for data consistency and coherency. This means that all data, including application state information with memory buffers, is written to disk and captured for snapshots, replication, and off-line LAN free backups.

VI3 data protection checklist:

- ✓ Enhance underlying VI3 capabilities
- ✓ Application-aware data protection
- ✓ Eliminate backup scan overhead
- ✓ Off-load LAN backup traffic
- ✓ Heterogeneous data replication
- ✓ Variable "virtual" recovery points
- ✓ Leverage disk-based VTL technology
- ✓ V2V, P2V, P2P recovery capabilities
- ✓ Bare metal restore to unlike servers
- ✓ Transfer data back to primary server

In cases where 100% of captured data has been replicated as of a specific RPO, essential data for application and transactional integrity may still be missing, resulting in a lack of consistency. Only application-aware data protection can eliminate lost or corrupt data in such instances.

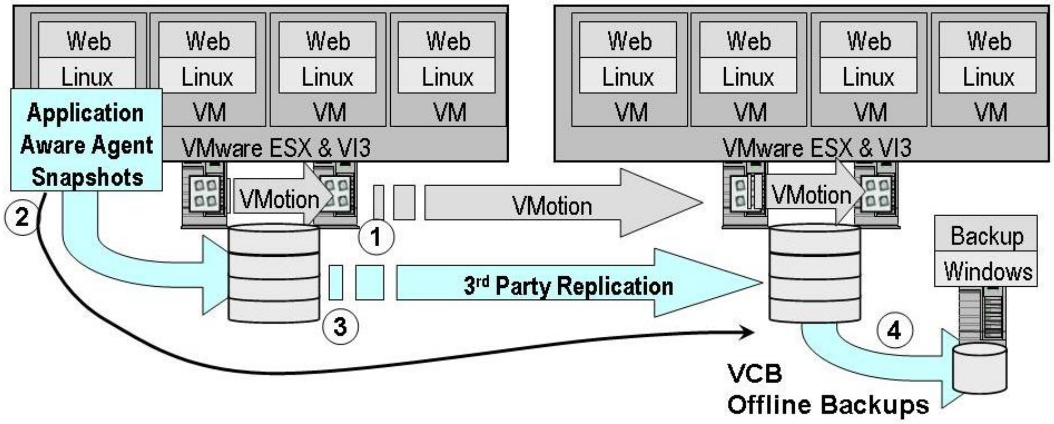

Figure-5: Steps for application-aware VMware VI3 data protection for HA, BC, and DR

The recommended solution (Figure-5) is to use a snapshot director, such as FalconStor Snapshot Director for VMware, that can interface with known and field-proven agents and APIs to perform hot application and complete data capture by quiescing applications so that data can be flushed to disk and protected using replication and VCB enabled backup.

With application-aware snapshots like those enabled by FalconStor Snapshot Director for VMware, applications are put into a hot backup mode. Unlike traditional backups, there is no extended downtime or disruption while data is replaced and backed up, which eliminates the backup window to improve application availability and reduce data exposure.

The enhanced VMware VI3 environment shown in Figure-5 combines baseline VI3 functionalty (VMotion and VCB) with third-party data protection technology to provide application-aware data consistency and coherency for BC/DR. In Figure-5, VMotion **(1)** is used to dynamically and proactively move VMs around in a VI3 environment while also providing operating system crash consistency. Crash-consistent recovery of VMware-hosted operating systems means that guest operating systems running in VMs have the ability for rapid restart after a crash; however, additional third-party protection is required to protect application data.

For example, combining third-party application-aware **(2)** snapshot capabilities with VMware enables all application data to be captured and written to disk in a coherent and consistent state to facilitate rapid application restart in the event of a server crash. In order to protect applications and their data from site-wide failures and disasters, organizations need to leverage third-party replication **(3)** such as FalconStor CDP Virtual Appliance for VMware and/or provisioning from FalconStor® Network Storage Server (NSS)-series Appliances with application-aware snapshot functionality to provide complete and consistent data protection.

The final piece of a complete data protection strategy for VI3 environments is to protect replicated data using off-line, LAN, and server free **(4)** VCB backups to disk, tape, or a combination of disk and tape with a virtual tape library (VTL) such as FalconStor® VirtualTape Library (VTL). VCB off-loads LANs and servers from backup data movement to improve performance and resource utilization in a VI3 environment.

Conclusion

The use of VMware to enable server consolidation and basic server crash-consistent server reboot, combined with heterogeneous data protection, reduces data loss and speeds restoration and application restart following outages and disasters. FalconStor Software offers advanced application-aware data protection solutions that ensure complete protection and integrity for virtual and physical system data, optimizing high availability and BC/DR in a VMware environment.

About the author:

Greg Schulz is founder and Senior Analyst of the StorageIO group and the author of the book “*Resilient Storage Networks - Designing Flexible Scalable Data Infrastructures*” (Elsevier).

All trademarks are the property of their respective companies and owners. The StorageIO group makes no expressed or implied warranties in this document relating to the use or operation of the products and techniques described herein. The StorageIO group in no event shall be liable for any indirect, inconsequential, special, incidental or other damages arising out of or associated with any aspect of this document, its use, reliance upon the information, recommendations, or inadvertent errors contained herein. Information and recommendations made by the StorageIO group are based upon public information believed to be accurate, reliable, and subject to change.