

Simplifying Disaster Recovery (DR):

One-Button Failover/Failback for Combined Physical/Virtual Data Centers

Abstract: Having a disaster recovery (DR) plan is mandatory. Most organizations recognize this — particularly those that have learned the hard way, when a disaster caught them unprepared. DR procedures have always been complicated for the physical server infrastructure, and the introduction of server virtualization has only made matters worse. VMware created vCenter Site Recovery Manager to streamline virtual server DR, but physical infrastructure DR procedures have remained difficult and time-consuming.

The FalconStor[®] Continuous Data Protector (CDP) solution can be deployed in conjunction with VMware vCenter Site Recovery Manager to empower the solution to automate and manage the DR process (both failover and failback) between entire heterogeneous physical and virtual infrastructures. This unique implementation dramatically speeds both processes and reduces costs while ensuring achievement of recovery time objectives (RTO).

Background

Standard disaster recovery (DR)

Reliable DR and failover procedures are crucial for the survival of any business today. The inability to fail over or recover from a disaster has driven numerous companies out of business due to delayed restarts, loss of transactions, and loss of customer trust. As a result, many organizations depend on snapshots and remote replication to a secondary site to fail over their business operations in case of an outage.

Failing over a physical infrastructure is an extremely complicated and time-consuming process, involving many tedious manual tasks in order to even test a DR implementation. In order to perform a failover, the following steps must occur:

- > Each server must be shut down
- > Data must be synchronized and replicated to a remote site
- > Replica volumes must be mounted and enabled at the DR site for each host
- > DR standby servers must be rebooted in the correct order, requiring constant monitoring
- > IP addresses and domain name servers must be remapped

The complexity makes testing impractical as it impacts the production environment and requires significant management. For this reason, many companies avoid DR testing altogether.

There are other requirements as well — including an even more complex and time-consuming process to fail back to the production site following an actual disaster. The generally accepted physical-to-physical (P2P) failover time for a site is about nine hours. These tasks are prone to error, and since they are not easily monitored or tracked, testing records are insufficient for compliance purposes.

Furthermore, in order to have sufficient failover capacity, there must be a one-to-one mapping of primary site hardware to secondary site hardware. This is extremely costly.

Enterprise data center environments

Large data centers today are gaining the cost and management benefits of server virtualization using applications such as VMware ESX Server. By consolidating multiple virtual machines (VMs) onto fewer physical machines, organizations can increase server utilization rates and reduce the number of servers required to run the business. Many organizations today operate “hybrid” data centers that use both physical and virtual servers. Some servers cannot be virtualized due to support and warranty requirements, while others cannot be virtualized because of the potential impact on process, management, and performance. A common practice is to virtualize Tier 2 applications, while keeping high-performance, high availability (HA), business-driving Tier 1 applications such as Oracle, IBM DB2, and Microsoft Exchange on separate physical servers. These physical and virtual environments must be managed separately, making DR processes even more complicated.

Virtualization at the DR site

In addition to consolidating primary data center servers, VMware ESX provides the opportunity to consolidate storage capacity at the

DR site. The virtual infrastructure at the primary site can be replicated to a consolidated virtual infrastructure at the secondary site, offering tremendous hardware and management savings. In addition, most organizations carefully consider the number of VMs they will host on a physical server at the primary site in order to ensure optimal functioning. However, at the secondary site they often increase the ratio of virtual to physical machines, since the failover site is expected to be a temporary solution. While a company may host four or five VMs on each primary physical server, they may consolidate 20 or 30 on each physical machine at the remote site. This type of consolidation makes a DR infrastructure much more affordable.

VMware vCenter Site Recovery Manager to the rescue

Still, the actual failover process from the primary virtual infrastructure to the secondary virtual infrastructure is complex. For this reason, VMware created vCenter Site Recovery Manager to streamline and automate the DR process for virtualized servers. VMware vCenter Site Recovery Manager works with virtual servers managed by VMware vCenter and VMware ESX, and leverages the storage vendor’s replication engine to automate both testing and actual recovery at the click of a button. VMware vCenter Site Recovery Manager delivers complete DR reporting for compliance and corporate governance, and simplifies the virtual server DR process, alleviating the burden on staff, resources, and productivity. VMware vCenter Site Recovery Manager can reduce the virtual-to-virtual (V2V) failover time from 12 to 24 hours, to about four hours. The development of VMware vCenter Site Recovery Manager enables IT managers to breathe a tremendous sigh of relief when it comes to failing over their virtual infrastructure.

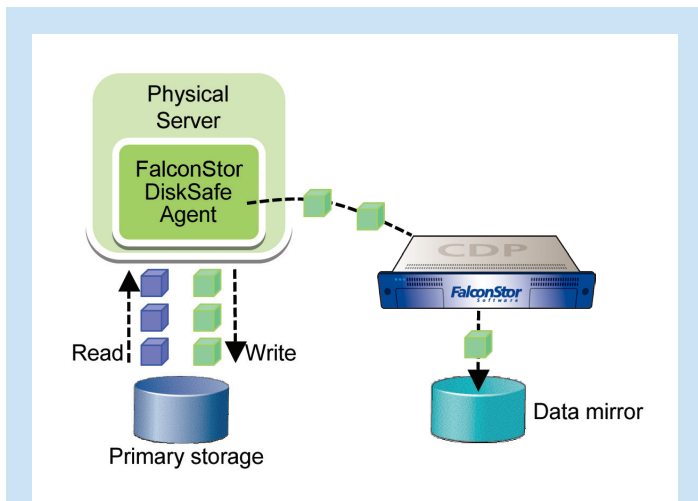
However, the physical servers must also have a DR plan and an effective set of recovery procedures. Unfortunately, the only option thus far has been a resource-intensive, complicated, error-prone set of manual steps. Tier 2 virtualized applications can be brought back in about four hours, but users still have to wait another five hours for the business-driving applications to return to functionality.

Failback is not automated with VMware vCenter Site Recovery Manager. When the outage has been resolved, data must be manually failed back by reversing replication roles and failing over from the remote site to the production site. VMware vCenter Site Recovery Manager must then be returned to its initial configuration.

FalconStor CDP with VMware vCenter Site Recovery Manager

There had to be a better way to recover data, and FalconStor Software developed it. By using the FalconStor® Continuous Data Protector (CDP) solution with VMware vCenter Site Recovery Manager, organizations can manage entire physical and virtual failover and failback processes together. This is a tremendous advantage that saves time and money, makes RTOs achievable, and delivers proof of compliance.

FalconStor CDP combines local snapshots and remote replication for fast, reliable recovery of both physical and virtual servers. In this joint deployment, FalconStor CDP software takes a snapshot of the storage LUNs in physical servers to create corresponding VMs based



The FalconStor DiskSafe® agent copies newly written data blocks to the FalconStor CDP server, where a mirror of the production physical server data is kept. Data is copied continuously, with minimal impact to production processing.

on the exact same LUN images. These VMs can be continuously or periodically replicated to a remote site just like other VMs, and can be managed by VMware vCenter Site Recovery Manager. For example, an IT staff can run a complete VMware vCenter Site Recovery Manager recovery plan at the touch of a button for testing or complete failover, including all physical and virtual servers at the primary site. Unlike other solutions, the FalconStor CDP solution lets users complete DR testing functions without interrupting storage replication and protection activities.

By combining these two applications, companies can execute both virtual-to-virtual (V2V) and physical-to-virtual (P2V) failover, all automated and managed by VMware vCenter Site Recovery Manager. In addition, FalconStor CDP can be used to present replicated disks to a physical standby server on the remote site. If that server is configured to boot from the SAN, VMware vCenter Site Recovery Manager can then automatically power on the physical machine, enabling P2P failover as well.

Automated failback process

When the time comes to return to the production site, the FalconStor Auto-failback Manager for VMware vCenter Site Recovery Manager solution can discover site configurations, reverse the replication roles between the secondary and production sites, and automate the failback process once the outage or disaster has ended. This relieves administrators from having to manually adjust storage arrays, reconfigure VMware vCenter Site Recovery Manager, complete the replication, and then return VMware vCenter Site Recovery Manager to its original configuration.

Cost and Management Benefits

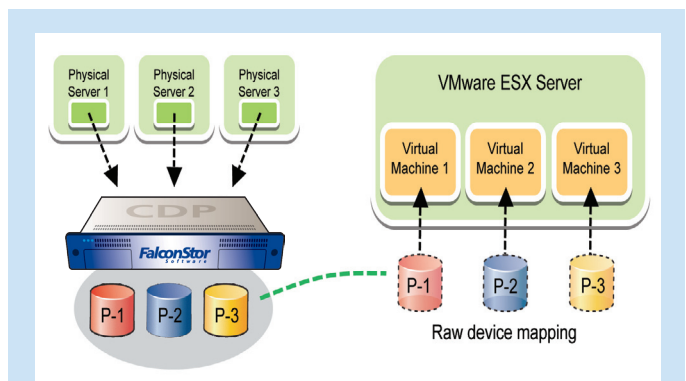
The most obvious benefit of this combined solution is that users have a unified tool with which to automatically fail over their entire physical and virtual infrastructure to a DR site, and fail back again to the production site. Failover and failback are now single processes,

rather than separate processes for physical and virtual servers. This simplifies management and reduces costs. Application-specific FalconStor snapshot agents enable FalconStor CDP to replicate data with 100% transactional integrity so that data is ready for immediate use once the failover is complete. The agents quiesce each application prior to capturing a data point; as a result, data replicated by FalconStor CDP isn't subject to lengthy data integrity checks. FalconStor CDP enables organizations to quickly resume business operations. Other solutions have no method of securing data integrity, so the data is copied in a crash-consistent state during replication.

Since protection and replication operations take place on FalconStor CDP appliances, limited server resources are used for data protection. FalconStor CDP replication can run continuously or periodically without interrupting production operations, making it much easier to achieve and improve upon recovery point objectives (RPOs). Because replication can occur more frequently, many more transactionally-consistent recovery points are available.

By linking VMware vCenter Site Recovery Manager with FalconStor CDP, users experience the benefits of both technologies, including:

- > **WAN-optimized replication.** Patented FalconStor MicroScan® technology and built-in data compression reduce replication bandwidth utilization by up to 90% or more. Because less data travels across the WAN to be stored remotely, FalconStor technology reduces the expense of both bandwidth and hardware for replication.
- > **Three-fold infrastructure savings.** 1) With VMware vCenter Site Recovery Manager and FalconStor CDP, customers can use any storage array certified by both FalconStor and VMware. Users can purchase the array that offers the right features, capacity, and price for them rather than a vendor-specified storage device. 2) WAN optimization and data compression technologies reduce DR site hardware requirements. 3) Failing over to a virtual infrastructure eliminates the need for one-to-one mapping of physical equipment between primary and remote sites; therefore, less hardware is needed.



The FalconStor CDP server maintains up-to-date mirror images of physical server storage. Snapshots of these images are mounted to a VMware ESX server, which uses raw device mapping to create VMs that correspond to each protected physical server but remain inactive.

- > **One-button management.** With VMware vCenter Site Recovery Manager, users gain one-button efficiency for DR tasks including failover, failback, recovery, and testing. This simplification of management dramatically lowers the cost of DR implementations.
- > **Automated failback.** FalconStor Auto-failback Manager is integrated with the VMware vCenter Site Recovery Manager single management interface, enabling immediate failback once a disaster is over. Automation eliminates manual errors and dramatically speeds return to operations at the production site.
- > **Instantly usable data.** Regardless of the type of workload, data is 100% transactionally consistent, so it is instantly usable upon failover instead of requiring file system checks and database repairs.
- > **Achievement and improvement of RTOs.** The synergy of VMware vCenter Site Recovery Manager automation for both physical and virtual servers, FalconStor CDP application agents for data consistency, and the replication speed of FalconStor CDP dramatically improves the speed of data recovery, helping to minimize RTOs.
- > **Proof of compliance.** This combined solution makes reporting of DR testing just as accurate for physical machines as virtual machines, making it easier to achieve corporate and regulatory compliance.
- > **Better data protection.** Combining FalconStor CDP with VMware vCenter Site Recovery Manager reduces costly downtime, minimizes the risk of losing business or customers due to a failure, and enables a fast return to operations.

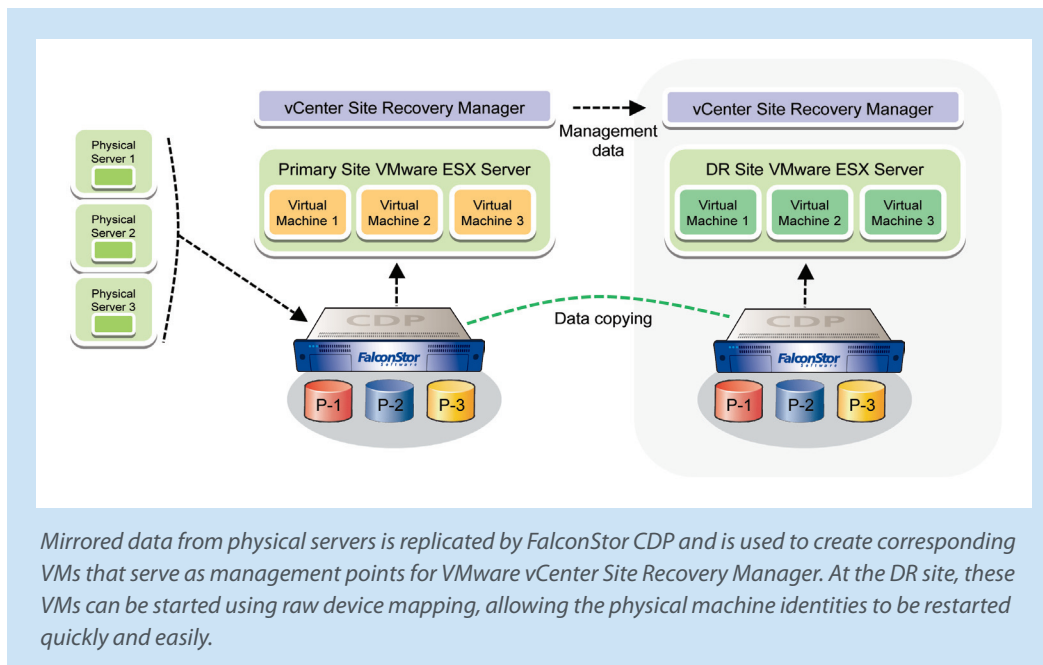
- > **Flexibility.** Users can implement iSCSI or Fibre Channel (FC) protocols, leverage thick-to-thin disk replication if desired, and select any storage array that meets their unique requirements.

Summary

DR is necessary, but DR procedures have always been complicated for the physical server infrastructure. With the advent of server virtualization, with multiple virtual machines hosted on fewer physical machines, the complications have increased. Recognizing that problem, VMware developed vCenter Site Recovery Manager to automate and streamline the DR process for virtualized servers.

While VMware vCenter Site Recovery Manager automates the virtual servers, the physical servers still require a long and complex DR process. Most data centers consist of a combination of physical and virtual infrastructures, resulting in separate management silos. FalconStor CDP can be deployed in combination with VMware vCenter Site Recovery Manager in order to automate and manage the DR process for the entire physical and virtual infrastructure.

With FalconStor CDP and VMware vCenter Site Recovery Manager, disaster failover and failback processes can be streamlined and automated, applications can be replicated in transactionally consistent formats, and RTOs can be much more easily met. This unique deployment offers cost savings, management ease, and fast recovery — making disaster failover simple and fast for the entire infrastructure, and making heroes out of the IT department.



For more information, visit www.falconstor.com or contact your local FalconStor representative.

Corporate Headquarters
USA
+1 631 777 5188
salesinfo@falconstor.com

European Headquarters
France
+33 1 39 23 95 50
salesemea@falconstor.com

Asia-Pacific Headquarters
Taiwan
+866 4 2259 1868
salesasia@falconstor.com

FalconStor
Software