FalconStor® Software

A White Paper

Simplifying Disaster Recovery (DR):

One-Button Replication for Combined Physical/Virtual Data Centers

Abstract: Having a disaster recovery (DR) plan is mandatory. Most organizations recognize this— particularly those that have learned this 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 (SRM) to streamline virtual server DR, but physical infrastructure DR procedures have remained difficult and time-consuming.

The FalconStor® Network Storage Server (NSS) solution can be deployed in conjunction with VMware vCenter SRM to empower VMware vCenter SRM to automate and manage the DR process for the entire physical and virtual infrastructure. This unique implementation dramatically speeds failover 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

There are other steps as well. 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.

Not only are the tasks difficult and time-consuming; 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 in terms of hardware acquisition.

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

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 a "hybrid" data center that uses both physical and virtual servers. Some servers cannot be virtualized due to support and warranty requirements, while others cannot be virtualized because of process, management, or performance impacts. 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 also 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 VMs to physical, 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 SRM to the rescue

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

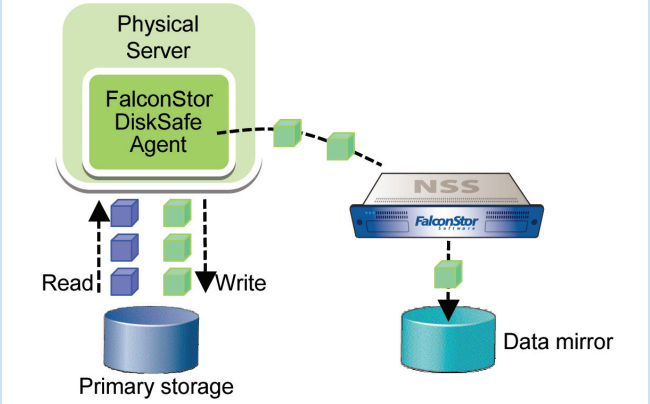
However, the physical servers must also have a DR plan and an effective set of recovery procedures. Unfortunately, the only option has been the old-fashioned, resource-intensive, complicated, and error-prone set of manual steps. This means that Tier 2 virtualized applications are back in operation in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

FalconStor NSS with VMware vCenter SRM

There had to be a better way to recover data, and FalconStor developed it. By using the FalconStor® Network Storage Server (NSS) solution with VMware vCenter SRM, organizations can manage the entire physical and virtual failover process. This is a tremendous advantage that saves time and money, makes RTOs achievable, and delivers proof of compliance.

FalconStor NSS combines local snapshots and remote replication for fast, reliable recovery of both physical and virtual servers. In this joint deployment, FalconStor NSS software takes a snapshot of the storage LUNs in physical servers to create corresponding VMs based 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 SRM. For example, an IT staff can run a complete VMware vCenter SRM recovery plan at the touch of a button for testing or complete failover, and include all physical and virtual servers at the primary site. Unlike other solutions, the FalconStor NSS solution lets users complete DR testing functions without interrupting storage replication and protection activities.

By combining these two applications, companies can execute both V2V and physical-to-virtual (P2V) failover, all automated and managed by VMware vCenter SRM. In addition, FalconStor NSS can



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

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 SRM can then automatically power on the physical machine, enabling P2P failover as well.

Cost and Management Benefits

The most obvious benefit of this combined solution is that users now have a unified tool with which to automatically fail over their entire physical and virtual infrastructure to a DR site. Failover is now a single process, not two separate processes, providing simpler management and lower costs.

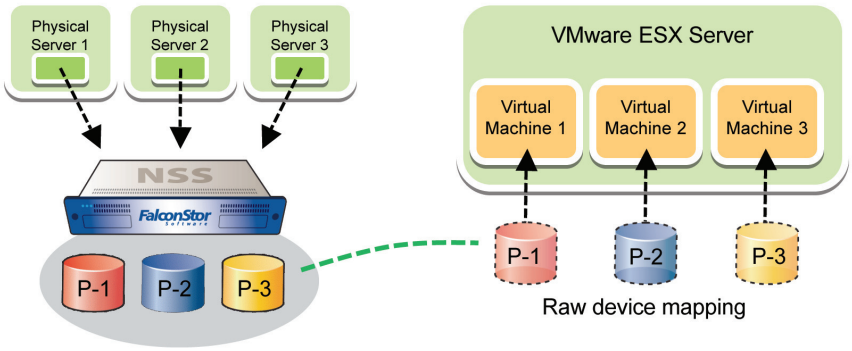
Application-specific agents enable FalconStor NSS to replicate data with 100% transactional integrity so that data is ready for immediate use once the failover is complete. The agents quiesce each application prior to capturing a data point; as a result, data replicated by FalconStor NSS isn't subject to lengthy data integrity checks. Other solutions have no method of securing data integrity, so the data is copied in a crash-consistent state during replication. The lack of post-processing required for recovery makes returning to business operations much quicker.

In addition, FalconStor NSS uses very limited server resources for data protection since protection and replication operations take place on the FalconStor NSS appliances. FalconStor NSS replication can run continuously or periodically without interrupting production operations, offering a dramatic improvement in recovery point objectives (RPOs). Because replication can occur more frequently, a greater number of transactionally-consistent recovery points are available.

By linking VMware vCenter SRM with FalconStor NSS, users gain the benefits of both technology offerings. These include:

> **WAN-optimized replication.** Patented FalconStor disk-scanning technology and built-in data compression reduce replication bandwidth utilization by 70%-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 SRM and FalconStor NSS, 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) By failing over to a virtual infrastructure, you eliminate the need for one-to-one mapping of physical equipment between the primary and remote sites; therefore, less hardware is needed.



The FalconStor NSS 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 SRM, you gain one-button failover, one-button recovery, one-button testing, etc. This simplification of management dramatically lowers the cost of your DR implementation.

> **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 of RTOs.** The synergy of VMware vCenter SRM automation for both physical and virtual servers, FalconStor NSS application agents that enable data consistency, and the replication speed of FalconStor NSS make it much easier to achieve your 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.** The FalconStor NSS / VMware vCenter SRM solution reduces costly downtime, minimizes the risk of losing business or customers due to a failure, and enables a fast return to operations.

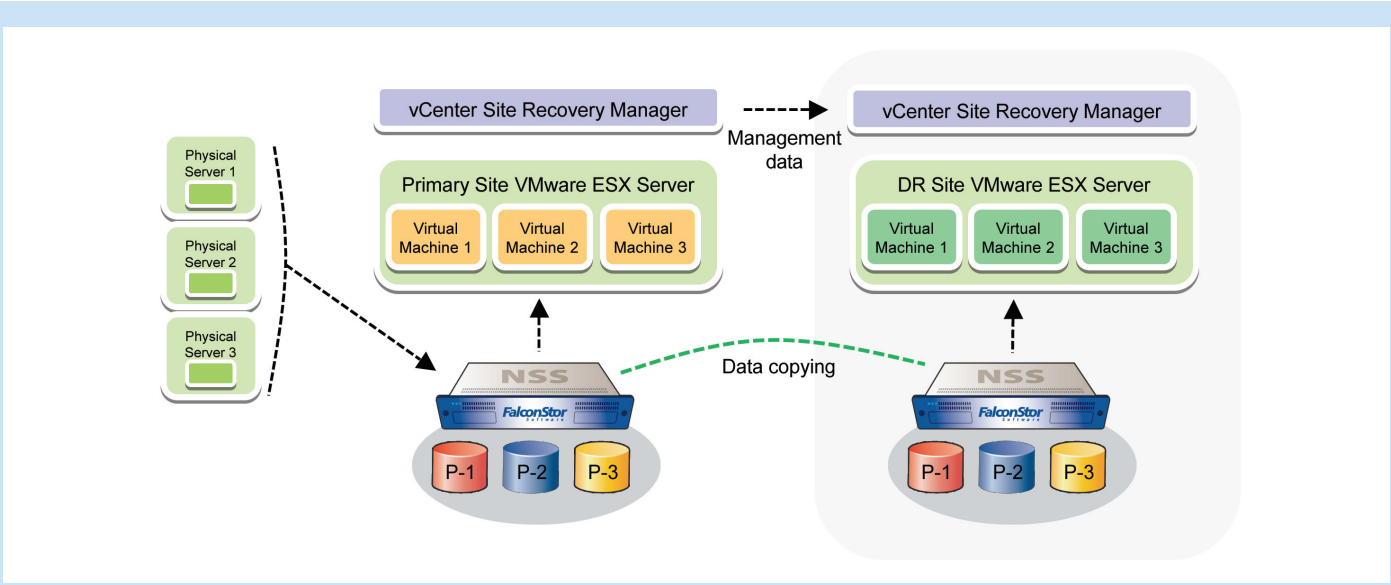
> **Flexibility.** With this solution, users can implement iSCSI or Fibre Channel (FC) protocols, leverage thick-to-thin disk replication if desired, and select any storage array that meets their unique requirements.

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 SRM to automate and streamline the DR process for virtualized servers.

While VMware vCenter SRM 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 NSS can be deployed in combination with VMware vCenter SRM in order to automate and manage the DR process for the entire physical and virtual infrastructure.

With FalconStor NSS and VMware SRM, disaster failover processes can be streamlined and automated, applications replicated in transactionally consistent format, and RTOs much more easily met. This unique deployment offers cost savings, management ease, and fast recovery — making disaster failover simple and fast for your entire infrastructure, and making heroes out of an IT department.



Mirrored data from physical servers is replicated by FalconStor NSS and is used to create corresponding VMs that serve as management points for VMware vCenter SRM. At the DR site, these VMs can be started using raw device mapping, allowing the physical machine identities to be restarted quickly and easily using VMware vCenter SRM recovery plans.

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

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

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

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

FalconStor® Software