Is IP Storage DR leaving you Exposed?

by George Crump, Lead Analyst

As the world of applications explode, an increasing amount of critical business information is being passed between data center sites using IP storage. Most IP storage systems have excellent replication software built into them, but the infrastructure that IP storage counts on for the transfer between data centers should be of grave concern to IT professionals responsible for supporting it. That infrastructure may be exposing the organization to unintended downtime and may send the IT professional looking for a new job.

These applications are not necessarily mission critical, but many are business critical. If these “apps” suffer a brief outage, the organization doesn't shut down, but it can lead to angst from the intended users of those applications. The exception is when a disaster strikes, causing operations to move to another facility. Then these apps need to be restored quickly to a working state. At that point, they have the same requirements as mission-critical applications running on a Fibre Channel SAN.

Both IP storage and Fibre Channel (FC) storage can leverage the same WAN connectivity to facilitate data communications to remote or disaster recovery (DR) sites. But in practice today they are treated differently. The SAN storage teams managing mission-critical applications run storage extension products that connect the FC storage system to the WAN. These extension products are uniquely designed to ensure optimal performance, quality of service (QoS) and security in addition to basic connectivity.

But what about the less critical applications? Email for example or a specific application for mobile users. Both applications commonly use IP storage and are well protected by replication and backup applications, and that data is inside the data center. But how about when that data leaves the data center? Is the system natively connected to the WAN that connects to the remote data center? Is that data always encrypted? Has recovery from the remote location been tested? Rapidly returning a business critical application to production requires crisp answers to these questions.

The "app" Explosion

The time it takes to create a basic application to solve a specific problem has reduced significantly. Again, this has led to an application explosion where small, purpose-built apps proliferate throughout the enterprise. Many organizations create these applications to solve specific problems that their employees, suppliers, customers or potential customers face. They also use these apps to enable a specific platform, like mobile, that these users are demanding. A brief outage typically does not mean the loss of revenue or user abandonment, but a prolonged outage will. Since a disaster has the potential to cause the longest period of outage, planning for business critical applications after a site failure is more important than recovery from an internal failure.

IP Storage for the App Driven World

IP based storage (iSCSI or NAS) systems often support these business-critical applications. As such they often choose the seemingly less expensive native IP connection for WAN connectivity. In

addition to native connectivity, another perceived advantage of IP storage systems is that most include replication software to move data off-site. The combination of native connectivity and included replication software give the appearance of getting "DR for Free".

In many cases however, the value of these applications becomes increasingly important to the organization. IT professionals eventually find that the business critical applications, from a DR perspective, must adhere to the same standards of their mission-critical, often FC based, counterparts. Meeting these standards means improved redundancy, reliability, and QoS.

No Free Lunch in DR

Again, the typical IP storage system is connected directly to the WAN via a dedicated port on the storage system itself. While this native access seems simple enough, it leaves the organization exposed to some problems. First, and potentially most concerning is a lack of security. The IP storage systems direct connection to the WAN data is rarely encrypted, meaning that data is transferred between data centers essentially in the clear and open for attacks.

Second there is little, if any, performance optimization. While many IP storage vendors will claim to be WAN optimized, they are not. The use of changed block replication, compression, and deduplication allow these vendors to claim that they are WAN optimized. While these technologies can reduce the amount of data that is transferred, the actual data being transferred in not optimized at all. They don't have the ability to aggregate WAN bandwidth or to provide automatic failover between segments.

As the distance between the primary data center and the disaster recovery site increases, more latency is introduced. Since these arrays have no true WAN optimization built into them, replication performance degrades by as much as 500% as distances increase.

Third, most enterprises will have a mix of IP storage and FC storage. FC storage will often replicate through a storage extension appliance. Because each IP storage device replicates via a native connection to the WAN, the process is silo'ed per storage system. Having a replication connectivity silo for IP storage and another for FC storage means that managing and monitoring each replication process is done separately.

This attempt to achieve "free DR" with IP storage started when it was a point solution for less critical data sets. As the data sets placed on it have become more business-critical it is important that IT planners upgrade the infrastructure that connects one storage system with another to eliminate the possible exposure they might be leaving their organization open to.

Designing Enterprise Grade DR for IP Storage

WAN bandwidth is constantly increasing, and the price for that bandwidth is decreasing. Data centers of all sizes are investing in faster connections. But WANs have some intrinsic weaknesses that can't be overcome by buying more bandwidth alone. IT planners need to look for solutions for their IP Storage systems that can securely transfer data in an optimal and highly available way.

The first design concern is the WAN connection itself. This connection is potentially the least reliable component in the enterprise. Most data centers try to overcome WAN link reliability concerns by purchasing multiple WAN connections from different vendors. When IP storage is natively connected, the use of the connections is manually allocated. IP storage will benefit from a device that can consolidate these into a single connection. Multi-line aggregation provided by a single device can deliver both load balancing and automatic failover.

A centralized device would eliminate the second design concern, silo'ed WAN traffic management. Silos of traffic management make it almost impossible to efficiently use available WAN bandwidth. QoS policies could be applied to all storage replication traffic from a single interface if the single device could also integrate FC storage.

The final design concern is encryption. All data being transferred across a WAN should be encrypted, and this device should be able to encrypt data universally. Not only would this increase data security it should also simplify the management of encryption keys by reducing it to one. It would also off-load the encryption function from the storage system itself, allowing it to focus its CPUs on providing better on-site performance.

The Solution: Consolidated Extension

FC storage has provided devices that have had some of these capabilities for years in the form of SAN Extensions. Last year an upgrade for extension products made them more enterprise-class by adding the ability to support load balancing and multiline aggregation, which maximized performance and availability. More improvements are coming as data centers take advantage of higher speed fiber optics coming online across most industries.

There are devices now available which manage the business-critical IP storage traffic merged right into the mission critical FC traffic. This consolidated extension technology still provides the same high performance, deterministic, resilient and secure traffic as before, but unifies the DR replication process for both IP and FC. With them all together in one solution there are no trade-offs like there are today. The expertise and technologies used for the “mission critical” data is now available to “business critical data” with no additional training or administration time.

Most importantly there is no trade-off in security. With a consolidated extension technology all data being transferred, IP and FC are encrypted by the same device with the same high level of security. Not only does this increase data security it also, once again, reduces administration time.

IP Storage may be IP based, but it is often a dedicated network just for storage traffic. It makes sense then that the IP storage network and the FC storage network are consolidated into the same extension device for DR. The Enterprise Class Storage Extension is evolving by adding support for business-class IP storage.

Conclusion

IP Storage is increasingly used as the storage infrastructure for the app-driven world. Most applications are not necessarily mission critical, but many are business critical and when disaster strikes they need to be returned to operation as quickly as possible. While most IP storage systems have excellent replication software built into them, the infrastructure they count on for the transfer between locations is seldom up to the job when it comes to speed, resiliency, and security. IT planners need to act now to eliminate the potential devastating impact of a prolonged outage of these applications caused by a weak infrastructure.

Sponsored by Brocade