Crafting a Storage Strategy
Storage that allows for effective retrieval of apps and data is a cornerstone to an effective continuity of operations plan.

Today's governmental and educational organizations recognize the value of their data. The maintenance and protection of that information is a key operations consideration. Having a firm strategy in place for storage before a disaster or systems failure strikes is of the utmost importance.

Storage is the repository from where all of an organization's information is stored and gathered. Given this important role, choosing the right storage options plays a vital role in the future development and maintenance of the data center.

In addition, any consultant will tell you that having good continuity of operations plan (COOP) and disaster recovery (DR) plans in place is essential. Organizations must proactively face the challenge of keeping their vital services functioning during times of emergency.

In the event of a failure or disaster, having these plans in place will help organizations re-establish operations with a sense of direction and relative ease. Having the right storage and backups in place can minimize the IT manager’s headaches.

“What you end up seeing, from the storage administrator’s perspective, is that they are challenged to make sure that the data is always available and accessible by [the organization],” says Bob Laliberte, an analyst with Enterprise Strategy Group (ESG). He adds, “Making sure that the data for particular applications is, not only protected, but also recoverable and available on a continuous basis is critical.” Fortunately, there are many storage hardware and software products and technologies available that can help organizations with their data-availability requirements.

**Analyze Operations Needs**

One of the first things organizations need to do when planning the storage aspects of their continuity strategy is analyze operations needs, such as the role information plays in day-to-day operations.

“Typically this is accomplished through an impact analysis,” says Laliberte. “All applications are assessed based on their impact to the [organization] if they were not available.”

Applications are typically categorized as: mission critical, operations critical and less than critical.

**Mission-critical applications:** These include applications where the organization would be at a complete standstill if the systems were not online.

**Operations-critical applications:** These applications would disrupt an organization, but not shut it down.

**Less-than-critical applications:** These don’t require 24x7 availability and can be preserved by physical backup to tape, followed by transporting the backup tapes to an offsite location.

**Synchronous vs. Asynchronous Replication**

Replication is an important part of any storage system. It is achieved in one of two ways: synchronously or asynchronously.

Synchronous replication: This is characterized by the acknowledgment from both the local and remote storage that the write has occurred. Here, the write either completes on both sites, or not at all.

Most applications will not proceed with further work until this has happened. This double write and dual confirmation introduces latency, affecting the application’s response time.

With synchronous replication, distance plays a key role. Performance is proportional to distance. The farther away the remote site, the greater the impact on application response time.
“Typically somewhere around 100 to 150 kms is the limit,” says Laliberte. However, synchronous replication does allow for a recovery point objective of zero, meaning there is zero data loss.

Asynchronous replication: This is characterized by the immediate acknowledgement of the write once the local storage receives it. This allows applications to proceed with the next batch of transactions. At a later time, the remote storage is updated but with some lag.

Performance is greatly increased with asynchronous replication, and distance is not a factor. However, if there is a loss at the local storage, the remote storage may not have been updated, resulting in the loss of data.

**RPO and RTO**

“The name of the game for IT managers is to match technology with their [organizations’] demands for recovery point objectives and recovery time objectives,” says Rob Emsley, the senior director of product marketing at EMC.

The concepts of recovery point objective (RPO) and recovery time objective (RTO) are key factors that must be addressed in an organization’s COOP. And the choice the organization makes regarding storage and replication can have a profound effect on these factors.

RPO: This is the maximum amount of data loss, measured in time, acceptable in the event of a disruption. Depending on the organization, RPOs can be measured in seconds, minutes, hours or days. For instance, financial organizations generally aim for an RPO of zero.

RTO: This is a maximum amount of time it takes to recover from an interruption in operations. That is to say, the allowable amount of time it takes to get an application up and running again.

“We just did a survey and for most [organizations, operations-critical apps] need to be up and running within 10 hours,” says Dan Lamorena, senior product manager for Symantec. “For tier-one, mission-critical apps, that requirement is less than four hours usually.”

Of great importance here is that not all applications have the same RPOs and RTOs, nor must a single application have matching RPOs and RTOs. As part of its COOP, more specifically as part of its operations impact analysis, an organization should determine what these numbers are.

According to EMC’s Emsley, “By understanding the different types of systems that you have inside of the data center, you can have different types of disaster recovery and [COOP] solutions to match the criticality of the information that exists.”

Another crucial thing to note about RTOs and RPOs is the cost-to-benefit ratio. Here, parallels can be drawn to the concept behind insurance. The goal with insurance is to determine the right amount of coverage that you need; as the level of protection increases, so too do your out-of-pocket costs.

Lamorena adds, “To get higher availability, there is a cost curve. No data loss and no downtime can get very expensive.

“Our goal is to help you reduce the management, operational and deployment costs so while you’re putting in some of these solutions, you’re also solving some other problems that are expensive,” he adds.

**Clustering and Mirroring**

Other storage strategies to look at include clustering and mirroring. Clustering servers and applications and mirroring data are technologies used for rapid application recovery and data availability.

Much like data replication and failover, clustering and mirroring provide for higher levels of operational availability and can ensure continuity of services in the event of failures.

“Clustering and mirroring are key technologies for implementing disaster-tolerant solutions,” says John Bennett, worldwide director, Data Center Transformation Solutions, at HP.
“These are appropriate where the costs of downtime and the costs of site outages outweigh the costs of investing in additional resources and sites.”

Mirroring: The concept of mirroring is synonymous with the notion of redundancy. Your remote location “mirrors” your local data center. It makes it feasible for an organization to maintain up-to-date copies of data at offsite backup locations.

This allows for uninterrupted access to the data if there is an outage at the local storage. And though it can be asynchronous, mirroring is typically only synchronous. However, mirroring does have the drawback of requiring double the storage capacity.

Clustering: This refers to the use of multiple, interconnected servers working together to handle variable workloads or to provide continued operation in the event one fails. Most commonly, clustering is used for load-balancing, the division of work among multiple servers allowing for an increase in work performed, as well as users getting served faster.

“I think the simplest way to look at it is that clustering is a way of improving performance and mirroring is a way of improving availability,” notes Ravi Pendekanti, vice president of worldwide sales and marketing at Overland Storage.

**Failover and Failback**

Failover and failback are functions that organizations need to take a close look at when weighing storage options. Failover is when a secondary storage system automatically takes over for a primary system in the event of a failure. Then, following the crisis, failback occurs when the storage is shifted back to the primary system.

Failover makes systems more fault-tolerant. It is especially important for critical applications that organizations can’t afford to be without — even for a brief period of time.

“The ability to failover to a secondary site is critical if the [organization] wants to resume operations in a timely manner in the event of a catastrophic event to the primary data center,” says ESG’s Laliberte.

“This is more than just replicating data; it also involves clustering servers and applications,” he adds. “The technology involved for this has dramatically improved, as it is now possible to failover a data center in just minutes."

Failover “plays a key role in situations where the business impact of an outage is significant enough that disaster tolerance, rather than disaster recovery, is required,” says HP’s Bennett.

“Failover makes riding through a system failure both possible and effective,” he says. “Where the [operations] impact of downtime or a site outage is not as significant, failover solutions are not required.”

As the cost of fault tolerant systems continues to drop, Bennett says, organizations would be wise to look for storage systems that provide a high degree of tolerance for component failure, and thus a high system availability time.

An example of a product that provides failover is EMC’s PowerPath. The product automatically tunes a storage area network (SAN) and selects alternate paths for data if necessary. PowerPath integrates multiple path I/O capabilities, automatic load-balancing and path failover functions.

**Offsite Backup**

As most of us know by now, backing up your data is essential. It is not only a key component to any COOP or DR plan, it just makes sense. The question then becomes what to do with that data once you have saved and replicated it.

The best practice would consist of sending replicated data to a remotely located device or service. The important thing to note, however, is that replicating the data is no good unless it is actually sent to the offsite location.

If you back up every night, but only send the tapes off at the end of the week, you risk losing a week’s worth of data. In today’s climate, many organizations have a redundant, secondary data center that can receive this replicated data.
For many organizations, it makes more economic sense to use a secondary storage center hosted by a vendor than to own one, says Don D’Errico, vice president and general manager of the infrastructure software group at EMC.

Ownership of a site means incurring significant real estate and other operational costs, not to mention the labor costs of staffing the site. Using a hosted site leverages shared resources.

In addition to the lower costs of the shared storage model, some vendor sites include space for staff, computers and communications equipment.

Another option is to use floor space in existing offices for the secondary storage site. “This is not just a second site but a second site that is completely active,” D’Errico says. Secondary storage sites should be located some geographic distance from the primary site in case of disruption.

Yet another option is to rent space at a collocation facility. Like disaster recovery sites, they have raised floors and provide power and cabling for setting up a dedicated infrastructure. Usually these locations lack “people space,” so the organization must have a plan in place to accommodate these other important aspects of recovery.

When the Lights Go Out

Disaster recovery plans should address situations where power is interrupted, providing for alternate electric power supplies during a loss or alteration of utility power.

Common power problems include: power failure, short-term voltage sags and spikes, long-term over and under voltage, frequency variation and harmonic distortion.

Generally, uninterruptible power supplies (UPSs) combined with diesel generators are used to combat power issues, with a UPS providing backup power for a short period of time until the generators kick in.

UPSs come in three forms:

• Offline, or standby, which kicks in only in times of power failure;

• Line interactive, which uses an inverter/converter to charge the battery and convert its energy to AC for the output as required;

• Online, which differs from the other two in that the battery is the primary power supply while the utility power is the secondary source. Here, the utility power is used to charge the battery only.

Choosing a UPS comes down to engineering quality and cost generally, after determining the specific features required for its application.

Sometimes there can be generator and UPS compatibility issues, so organizations should do their due diligence in researching their specific needs.

Though often overlooked, having an adequate amount of fuel on hand for the generators is of great importance.

CALL 800.808.4239 TO TALK TO A SPECIALIST TODAY.

031809