Bullet proofing Microsoft Exchange with HP OpenView Storage Mirroring white paper

Executive overview of options to protect Microsoft Exchange

The preceding quote may sound dramatic, but chances are it also rings true. E-mail has gone from being "nice to have" to being the one application that is shared and demanded from the warehouse to the executive boardroom. Not CRM, not even file services, but e-mail.

Whether or not your responsibilities include the IT department, you have an interest and dependence on e-mail—for many companies that means Microsoft® Exchange. So then, the question becomes: "How do I ensure that my Exchange environment is always protected?"

This white paper is an executive overview of the options available for protecting Exchange. A more technical discussion and details can be found in the *HP OpenView Storage Mirroring Exchange Failover utility* white paper (May, 2005) at:
http://h18006.www1.hp.com/storage/softwhitepapers.html

This white paper covers:

- How to protect Exchange data
- How to achieve disaster preparedness
- How to ensure Exchange availability
- How to quantify Exchange outage vulnerability
- Other considerations for Exchange
- Why use HP OpenView Storage Mirroring

How to protect Exchange data

Regardless of availability goals or disaster preparedness, all efforts start with ensuring the resilience of the Exchange data.

As of the writing of this white paper, there are three major versions of Exchange in use—5.5, 2000, and 2003—running on a combination of Windows NT®4, 2000, and 2003. For each of the preceding permutations, consider the addition of service packs and hardware platforms, and you have a wide variety of systems to protect. In addition, consider that many different tape backup programs offer widely varying Exchange backup capabilities. The only common denominator in all of these configurations is that the various Exchange files are stored on Microsoft Windows® file systems.

One of the strengths of the HP OpenView Storage Mirroring replication technology is that it protects files at the byte-level, regardless of the application. In this case, when the mail application (or any other application) changes any file, the actual byte-strings are sent to another Windows server. After the data is protected to another server, multiple solutions are available for achieving availability goals. But it all starts with the data and that means it starts with Storage Mirroring.

Storage Mirroring protects data on any Windows server to any other Windows server across TCP/IP. If two different Windows platforms (including servers, NAS, and clusters) have IP connectivity, Storage Mirroring can protect your data.

How to achieve disaster preparedness

"Disaster recovery" means different things to different people. In a broad sense, it includes changes to corporate culture, additional processes and documentation, identifying key personnel and their emergency roles, and equipping an alternate infrastructure. To the more focused IT executive, it all starts with the protection of the data.

One of the presumptions of disaster recovery is that there are only two technologies: tape and synchronous hardware.

- With tape, one might routinely ship cartridges to a storage facility or vaulting service. This can be expensive to the bottom line and still leaves large windows of data exposure.
- With synchronous hardware, the data is protected but at a solution cost that often exceeds many annual IT budgets. And due to the nature of those solutions, both copies of data are typically in the same power grid, weather zone, and municipality. In fact, some industries have started mandating that synchronous hardware does not provide enough distance and must be supplemented.

This brings up asynchronous software replication for discussion. Storage Mirroring can replicate your Exchange data to any location across the city or country. By taking advantage of the built-in bandwidth control and extended queuing features of Storage Mirroring, you can use your current infrastructure to protect your existing Exchange servers to any other location.

If you maintain multiple data centers, one can deploy redundant servers at key locations. This allows the local IT teams to maintain the platforms and conduct disaster preparedness exercises (see Figure 1).

Figure 1. Exchange servers, bow-tied bidirectional between company sites
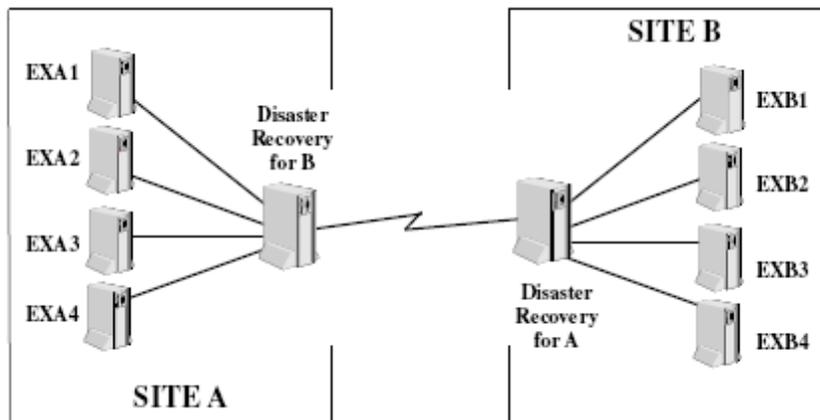
If you already have a relationship with a disaster recovery vendor (for example, SunGuard) or a storage service provider, then they probably have a relationship with HP and can serve as the "target" for your data (see Figure 2).

Figure 2. Exchange disaster recovery to an SSP/hotsite
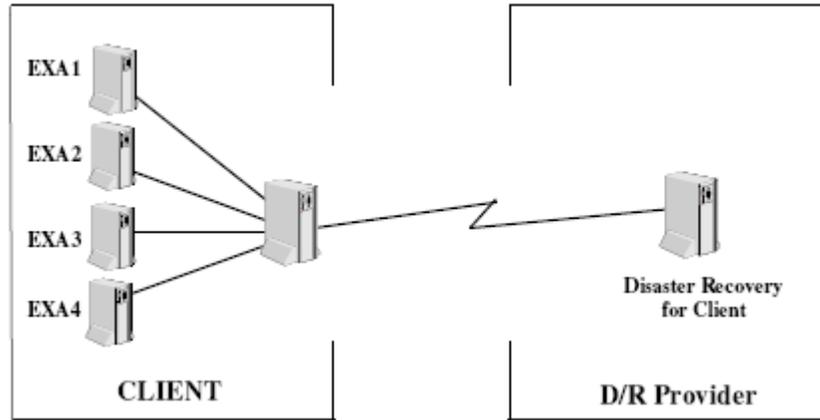
How to ensure Exchange availability

Ensuring Exchange availability is the most important issue. How does one ensure that in all scenarios, the Exchange system continues to be available to users?

With the release of Exchange 2000, it is clear that the best way to "fail over" or provide a redundantly available instance of Exchange is through Microsoft clustering. Because of Exchange 2000's reliance on Active Directory and other technical concerns, Exchange behaves best when the name, IP, mailboxes, and so on are abstracted into a "virtual server" within Microsoft Cluster Service (MSCS). Then, MSCS handles moving the virtual server between physical machines—for availability.

Unfortunately, MSCS has some inherent architectural limitations, such as shared single storage solution and node/distance limitations.

- All MSCS nodes must share the same physical storage. If the storage technology were to fail, none of the nodes would be able to function. This means that the shared data solution becomes a single point of failure.
- Because the nodes are assumed to share the solution, the existing MSCS technology does not provide for the nodes to be geographically separated. This means that if a single building (or even just the computer room) were to be impacted, the entire solution would be affected.

To address these limitations, technologies of Storage Mirroring can be used to significantly increase the availability of Microsoft Exchange.

If you already have clusters, then you already have a local availability solution, although with shared storage. But what happens if the computer room or building that contains both Exchange nodes and the shared storage were to suffer an outage?

When considering regional-type outages (for example, September 11, the August 2003 blackouts, or even annual hurricanes and tornados), city-wide measures may not be adequate.

4

To eliminate a city-wide or larger impact, Storage Mirroring can replicate the data from the cluster to another platform, anywhere in the world. In fact, Storage Mirroring can protect traditional MSCS clusters (see Figure 3).

Figure 3. Disaster recovery of any cluster
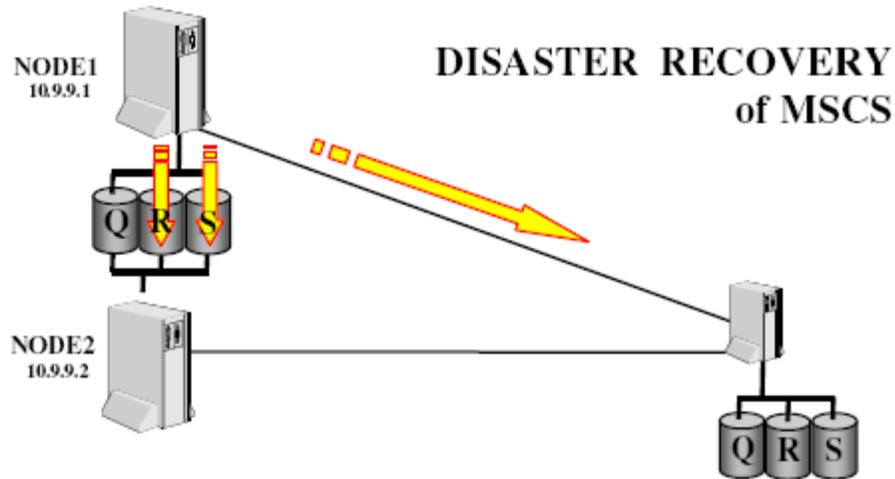
The target platform can be located anywhere in the world and brought back online to stand in for a failed production Exchange instance.

How to quantify Exchange outage vulnerability

After recognizing that higher levels of resilience are possible for Exchange environments, you must determine the business impact of an Exchange outage so that you can decide what level of protection is adequate.

There are commonly two processes for quantifying outages and business impact, and really, the two build on each other.

The first is to calculate the cost in man-hours due to Exchange downtime. Determine the average annual "unavailable" time for your Exchange servers. "Unavailable" encompasses scheduled outages and unplanned interruptions. After assessing how often each server is down, identify the users who are supported by each Exchange server. Calculate the hourly cost for these groups of users. This information can be obtained from Human Resources/Payroll or by using industry averages. When you have the hourly costs, multiply that by the unavailable time to determine your average cost of downtime as it applies to lost user productivity. There are other cost factors not accounted for that you might want to consider, such as the lost business opportunities and transactions during these downtimes. And after doing this exercise, you now understand financially what your Exchange server is worth. And the uptime or downtime becomes a business decision, instead of a technology decision.

The second idea is to extrapolate the business impact over the estimated lifespan of technology in your environment. For example, you might assume that server hardware has a 24–36 month value.

If so, any technology added to those servers would have the same lifespan. Therefore, one can objectively consider fault-tolerant technologies in an ROI analysis to the cost of the problem.

What most people find when they have assessed the business/financial implications of downtime, and compared it with more traditional technology alternatives, is:

- Tape backup does not provide enough protection since it only runs nightly. All Exchange messages on the day of the failure are lost. And often, users are less or non-productive for most of the next business day. From the "lost manpower" perspective, most companies cannot afford to simply use tape.
- Synchronous mirrored hardware is the other end of the spectrum. When considering the proprietary hardware, software, and additional components, most hardware solutions provide zero data loss but at a solution cost that often rivals or exceeds entire IT budgets, much less than the cost of being down. Very few Exchange environments can justify this solution.

It is for this reason that Gartner predicted that, by the end of 2003, companies would be mixing tape backup (for weekly/monthly archives) and replication technology "for more rapid application recovery."[1]

Other considerations for Exchange

It is likely that Microsoft Exchange will continue to grow in dominance in the Windows networking space. It is even more likely that new versions, service packs, hot fixes, and third-party add-ons will make protecting Exchange even more difficult.

When considering enterprise technologies, it can be difficult to select vendors that support large areas of the organizations. When considering applications (such as Exchange, SQL, Oracle®, and file services) into their various versions, the task is even more daunting. However, because Storage Mirroring replication technologies focus on files and not applications, the same level of data protection for Exchange is equally viable for other Windows-based applications. More simply stated, you can standardize on one Windows availability solution, regardless of the myriad applications in your environment.

Why use HP OpenView Storage Mirroring

HP OpenView Storage Mirroring goes beyond periodic backup to provide continuous data protection and ensure minimal data loss and immediate recovery from any disaster or system outage. Storage Mirroring utilizes patented replication and failover technology that continuously captures byte-level changes as they happen and replicates those changes to one or more target servers at any location— locally or at a site miles away. By replicating only the bytes that change, Storage Mirroring uses the absolute minimum bandwidth required to back up your data. Powerful advanced features let you control bandwidth usage and queue data changes for replication during off-peak usage times. Storage Mirroring provides the ability to recover from your target server in minutes, if not seconds, in the event of a disaster.

Host-based, Storage Mirroring delivers better protection than many hardware-based solutions and costs thousands of dollars less. Start with as few servers as you like, scale organically as your data requirements grow, and receive a fast, continuous return on your investment. Additional savings results from server, storage, and network independence so it will work with the applications you have today and will work with whatever best-of-breed hardware and software your purchase tomorrow.

The Exchange Failover utility, which is a free download from HP, automates the failover process for MS-Exchange and MS-SQL environments.

---

[1] Gartner, IT Trends for 2002

For more details, go to: http://h18006.www1.hp.com/storage/softwhitepapers.html and download *HP OpenView Storage Mirroring Exchange Failover utility*. Available in August, 2005 is a wizard-based utility that will automate the configuration of Exchange server and Active Directory as well as provide self-check and fix capabilities to ensure your replication/failover of Exchange environments will work the first time.

Features and benefits of Storage Mirroring include:

- One-to-one failover solution for MS-Exchange, MS-SQL, and Oracle—Provides automatic failover and near instantaneous access to replicated data or uses replicated data to recover or rebuild your local server.
- Server groups—Enables the "grouping" of servers on the management console (GUI) allowing focus on only those servers under your span of control.
- Continuous, asynchronous byte-level replication with intelligent data compression—Captures changes as they occur, ensures sequence of data mirrored on target, and provides user-configurable compression levels to ensure efficient usage of network resources.
- One-to-many and many-to-one host configurations—Allows multiple production servers to use the same target server.
- Standard network protocol—Replicates over any existing IP network (LAN/WAN) to protect your investment in your existing network infrastructure.
- Elimination of geographic limitations—Replicates to a disaster recovery site as far away from your production server as you would like to ensure maximum protection against data loss from failure or other disaster.

Storage Mirroring is an OEM solution from NSI Software, the leader in protecting applications running on Windows file systems and Exchange protection technology.

For more information

http://h18006.www1.hp.com/products/storage/software/sm/index.html

Call to action

To download a technical white paper on MS-Exchange Failover:

http://h18006.www1.hp.com/storage/softwhitepapers.html

To download a 60-day no-risk trial of HP OpenView Storage Mirroring:

http://www.openview.hp.com/products/mirror/tc_mirror_0001.html