CIO VIEWPOINTS: EXCHANGE 2007 RISKS & MITIGATION STRATEGIES

WHITE PAPER
Dell | Modular Services

www.dell.com/modularservices

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

OVERVIEW

Understanding the strengths and limitations of the Microsoft® Exchange Server 2007®'s new offerings, and the associated costs, is key to mitigating the risks inherent in Exchange 2007 and designing an Exchange architecture that economically meets the total messaging goals for your organization.

While Exchange 2007 includes many new features and provides a solid foundation for corporate email, it has minimal support for many of the security, high availability, e-Discovery search, archiving, and compliance features that many organizations now require. Taking full advantage of Exchange 2007's new features can require a substantial investment. Add to this, augmenting Exchange with third-party solutions required to fill any feature gaps anticipated for your organization can yield an expensive and difficult to manage messaging solution.

As a result, many CIOs are leveraging their Exchange 2007 upgrades to re-architect their broader messaging environment to incorporate solutions that address these important issues with an eye toward optimizing the total cost of ownership. This white paper:

- Outlines areas of functionality where many companies may want to consider augmenting Exchange 2007's built-in capabilities with third-party offerings in order to fully address a wider range of High Availability (HA) design issues and to more completely meet their organization's messaging needs.
- Outlines the some of the major costs and risks of deploying Exchange 2007.
- Suggests five rules to consider when planning an Exchange 2007 investment.
- Concludes with a description of Dell's Email Management Services™ (EMS™) and how they can augment an Exchange Server 2007 deployment to provide increased availability and resiliency and help lower total operating costs.

1 MICROSOFT EXCHANGE AND YOUR BROADER MESSAGING GOALS

While Microsoft Exchange Server 2007 provides a basic level of service and support for a number of today's common business scenarios, there are gaps in functionality and features. When evaluating an Exchange 2007 installation or upgrade, CIOs are considering not just native Exchange functionality, but also the additional capabilities currently in place or that need to be deployed that will interact with Exchange.

For instance, organizations have differing requirements for email uptime and while Exchange 2007 has been improved to offer new high-availability options, these options have limitations and may need augmentation with third-party solutions. In addition, the increasing reliance on email for everyday business processes continues to fuel rapid growth in email data stores and warrant a focus on storage scalability during deployment planning. Rapid, cross mailbox e-Discovery search, legal hold functionality, and robust retention policy management are other areas where many organizations will want to supplement Exchange 2007. While third party solutions exist to minimize storage growth and augment functionality, these solutions can result in complex, expensive solutions that can be difficult to manage when implemented piece-meal.

Carefully consider what government regulations may require, what your users will ask of you, and what your budget can support, and look for solutions that can solve your needs as simply as possible to help ensure a low cost, manageable Exchange environment.

DETERMINE IF EXCHANGE 2007 MEETS YOUR HIGH-AVAILABILITY NEEDS

Microsoft Exchange is a messaging and collaboration tool that is now expected to be available from anywhere at any time with similar utility level reliability that is expected from the phone and power services. In addition to delivering highly reliable messaging, Exchange is now being tasked to deliver capabilities that it has historically not included, such as site resiliency, business continuance, compliance support, remote access, anti-virus and anti-spam, and legal discovery support.

Yet during an outage or failure, Exchange 2007 provides minimal continuity functionality. Failover technologies can be used to shift load between systems to shorten the duration of an outage, but this process is not invisible to users. If the outage lasts for more than a few seconds, user access to email may be interrupted. Microsoft has included four models for built-in high availability:

- Single Copy Clusters (SCC) – Enables a cluster with shared storage.
- Clustered Continuous Replication (CCR) – Replication of email to a clustered server (typically in the same datacenter) to reduce outages from local infrastructure failures.
- Local Continuous Replication (LCR) – Replication of local email storage, but not the server, to protect against drives failure.
- Standby Continuous Replication (SCR) – Allows email data to be replicated to one or more remote servers that are not clustered to reduce outages from local infrastructure failures.

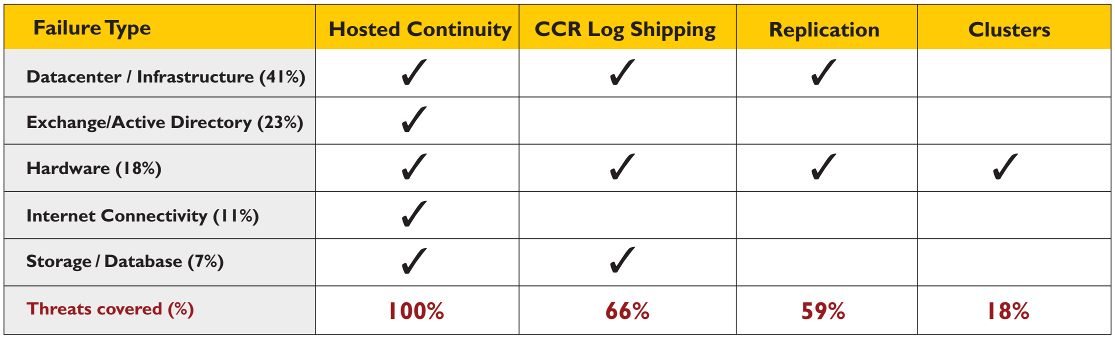
Organizations that want to help ensure email outages never last more than 24 hours will likely consider deploying Exchange 2007 with CCR or SCR across multiple sites. While protecting against many common outage types, expenses for these architectures can add up rapidly for larger organizations with multiple sites.

When servers with the Mailbox role are clustered using either the SCC or CCR configurations, no other roles can be located on these servers. If your organization requires redundancy in a site that uses mailbox clustering, you will need a minimum of four servers: two servers with the clustered Mailbox roles and two servers with the combined Hub Transport and Client Access Server roles.

Exchange 2007 provides some very useful HA capabilities that greatly extend the range of design options compared to Exchange 2003. However, there are still some limitations that may affect your ability to meet your messaging needs using only Exchange 2007. Unfortunately, the Exchange 2007 high availability (HA) deployments that protect against mailbox server outages require expensive enterprise Exchange server licenses along with redundant hardware and storage. Despite the high level of investment, none of these HA options fully protect against Active Directory® outages, Exchange configuration errors, corrupt logs and other problems that affect the global messaging environment. These limitations include:

- Limited or no support for continuity operations during an outage or a server recovery.
- Limited or no support for essential services that aren't provided directly by Exchange (e.g., BlackBerry® Enterprise Server access).
- A lack of protection from some failure types, including Active Directory problems and large-scale events that affect multiple servers or multiple sites.
- The requirement that some functionality (like Unified Messaging and client access servers) must be protected by adding servers instead of using clustering or other technology.

Figure 1: **Types of Failure**[1]



Failure Type	Hosted Continuity	CCR Log Shipping	Replication	Clusters
Datacenter / Infrastructure (41%)	✓	✓	✓	
Exchange/Active Directory (23%)	✓			
Hardware (18%)	✓	✓	✓	✓
Internet Connectivity (11%)	✓			
Storage / Database (7%)	✓	✓		
Threats covered (%)	100%	66%	59%	18%

[1] Dell EMS Activation Data, 2008

For these reasons, some organizations will bypass the native Exchange 2007 clustering options for an Exchange 2007-ready email continuity service. Continuity services like Dell EMS Email Continuity^{TM} can provide comprehensive protection against outages by seamlessly switching users to a back-up email service in minutes. These services can often be added at a fraction of the fully burdened cost of CCR or SCR.

TIP

Make sure that your Exchange 2007 architecture provides adequate protection against outages and data loss to meet your needs. Avoid settling for less than full email protection and closely examine the total cost of ownership of your high availability architecture.

MULTIPLE DATA COPIES CAN CAUSE COMPLIANCE PROBLEMS AND INCREASE COSTS

With the growth of email, data stores continue to get much larger. Many companies are compounding this trend by storing as many as five copies of data in disparate systems; copies for tape back-up, copies as replicates for recovery/availability, and copies for e-discovery and archiving. Exchange 2007 addresses this growth by increasing the number of servers that can be reliably included in the email system, however more can be done.

Attachments often make up the bulk of most data stores. An archiving system with storage management features to stub off attachments and keep only a single copy can reduce data stores by as much as 80%. Multiple copies can also make compliance with retention and deletion policies difficult to manage, can make e-discovery for litigation expensive and unreliable, and can add complexity to daily maintenance procedures.

While storage management features can be added with third-party software, the concept of a single storage instance can be extended to the architecture as a whole with integrated messaging services that store only a single document copy for use by archiving, storage management, recovery, and continuity systems. Integrated storage management capabilities as part of a comprehensive email management solution can reduce data store sizes, improve backup times, and reduce recovery and maintenance window times while additionally providing increased uptime potential and filling other feature gaps.

FUNCTIONALITY RISKS ASSOCIATED WITH EXCHANGE 2007

Many organizations have messaging and archiving needs that are not fully met with Exchange 2007's standard features. Exchange Server 2007 either lacks or has limited capabilities for the following:

- The ability to set, secure, or easily manage granular message retention and deletion rules.
- The ability to easily place legal holds on selected mailboxes to prevent the destruction of messages.
- The ability to execute rapid and finely tuned searches for messages, and/or attachments across multiple mailboxes.
- End user search and recovery of deleted or lost messages and attachments.
- Continuity service that helps protect against site outages, infrastructure problems, data loss, Active Directory problems, and configuration errors.
- Email recovery services that help protect against message loss in the event of database corruption.
- Wireless device continuity services that help protect against BlackBerry downtime during Exchange, Active Directory, and infrastructure outages.

Many organizations — such as U.S. companies regulated under Sarbanes-Oxley or with active litigation subject to the Federal Rules of Civil Procedure — consider these archive, compliance, and disaster recovery capabilities to be essential email requirements. As a result, many companies will deploy Exchange 2007 with a complementary email archiving, storage management, and continuity service.

Exchange 2007 is an important step in the evolution of email management but does not include archiving capabilities adequate for most organizations. It also does not provide email continuity or protection during many types of local infrastructure outages. If it cannot help ensure that messages are not lost during a crisis or outage, the archive will not be complete and accurate.

2 COSTS AND RISKS

The upgrade to Exchange 2007 can have substantial up-front costs, some obvious but others require careful planning to avoid hidden costs while meeting your messaging needs. Below are listed some of these costs:

- The cost to upgrade the servers to 64-bit hardware.
- The cost to upgrade the operating system to a 64-bit version of Microsoft Windows® Server.
- The impact of deploying Windows Server 2008.
- The presence of third-party software and integration with other applications.
- The increased reliance on Active Directory for the routing topology.
- The new server roles provided by Exchange 2007.
- The new HA options for the Mailbox server role.
- The impact to your backup and disaster recovery processes.

HARDWARE COST

One of the main concerns many administrators voice about Exchange 2007 is the cost of replacing their existing Exchange server hardware with new 64-bit hardware. While Dell and other major hardware vendors have been selling 64-bit hardware for several years, there are many organizations still using 32-bit machines that are more than adequate for their pre-Exchange 2007 needs. These companies will have to purchase new 64-bit capable hardware in order to upgrade to Exchange 2007. Even if an existing system is 64-bit capable, it may require significant upgrades (such as additional processors, more RAM, RAID controllers, or hard drives), or even complete replacement, to satisfy increased requirements for redundancy and future scalability.

OPERATING SYSTEM COST

An issue that hides costs associated with an Exchange 2007 upgrade is that the Windows Server 2003 operating system does not permit in-place upgrades from the 32-bit to 64-bit architectures. For many companies, this has the immediate consequence of requiring them to purchase additional Windows Server 2003 x64 licenses for the servers they will use for Exchange 2007.[2]

Even when an organization enjoys a licensing contract that neutralizes the cost of converting existing 32-bit Windows Server licenses to a 64-bit version of Windows Server, they may still need to buy licenses for a number of new machines. While Microsoft recommends that Exchange be run on dedicated servers, many small- to medium-sized organizations feel that they must place Exchange and other applications together on otherwise underutilized server hardware in order to gain the most value for their dollar. Many of these applications are not compatible with x64 versions of Windows; they must be separated and placed on different systems or on virtual servers as part of the upgrade process.

WINDOWS SERVER 2008 IMPACT

Factor in your company’s plans to deploy Windows Server 2008. This permits the new servers to be cleanly installed in a near-greenfield configuration, and may be especially desirable if there is a desire to deploy and migrate to a new Active Directory forest to clean up existing problems.

[2] Chris Scharff, Microsoft MVP, MCSE, October 2008.

THIRD-PARTY SOFTWARE COSTS

Third-party software can be an additional source of unexpected costs and challenges. Many companies use products such as message hygiene suites, fax gateways, and others to provide additional functionality not provided by Exchange Server 2003. Most examples in this category of software are designed to be collocated with Exchange and will often require their own upgrades to help ensure 64-bit Windows compatibility and the other pre-requisite technologies used by Exchange 2007.

Even when third-party software runs on hardware separate from the Exchange servers, it may rely on Application Protocol Interfaces (APIs) and technologies, that are no longer supported in Exchange 2007, such as Collaboration Data Objects (CDO) for Exchange Management (CDOEXM), the Exchange Windows Management Instrumentation (WMI) classes, or Internet Information Services (IIS) protocol event sinks. Any add-ons that use on these technologies for Exchange integration must also be updated. For a complete list of the technologies that have been removed from Exchange 2007, see the following post on the Exchange team blog: http://msexchangeteam.com/archive/2005/09/15/410941.aspx.

INCREASED ACTIVE DIRECTORY INTEGRATION IMPACT

Microsoft Exchange has always relied heavily on a functional directory service and Exchange 2007 further increases this integration by removing the concept of the Exchange routing group. Instead, Exchange 2007 relies on the underlying Active Directory site topology to provide any necessary routing infrastructure.

With previous versions of Exchange, the connections between routing groups were completely divorced from the site links used for Active Directory replication. As a result, it is critical that enterprises upgrading to Exchange 2007 first perform a comprehensive review of their Active Directory topology, sites and subnets, and site links to ensure that the forest and domains are in good health. If your Active Directory deployment is suffering from any under-the-radar problems, the chances are very good that they will be exposed by Exchange 2007 – and impair the health of your Exchange organization until they are corrected.

NEW SERVER ROLE IMPACT

The new Exchange 2007 server roles provide a great deal of flexibility and control over the organization, but they can also introduce new levels of overhead into your organization and increase the number of servers you require. For more information on these new roles and what they do, please see the Exchange Server 2007 documentation.

When the role dependencies are taken into account in the upgrade design, additional Exchange 2007 servers may be required to meet the placement and redundancy needs as the following examples help demonstrate:

- When you place a server with the Mailbox role in a site, it must have the Client Access Server role and the Hub Transport role in the same site as well. These roles may be placed on the same server as the Mailbox role except under specific conditions such as specific HA configurations (see page 3).
- The Edge Transport role cannot be placed on the same server as any other role. If you require redundancy for the Edge Transport role, you will need a separate server for each additional Edge Transport instance.
- Unified Messaging (UM) is a major driver for Exchange 2007 upgrades in many companies. While the Unified Messaging role can be placed on the same server as the Mailbox, Hub Transport, and Client Access Server roles, in many cases the UM role will need to be placed on its own server to provide adequate voice quality for more than a few dozen concurrent calls.

HIGH AVAILABILITY IMPACT

The built-in HA options that help protect against mailbox server outages require expensive enterprise Exchange server licenses along with redundant hardware and storage yet none of these HA options fully protect against Active Directory outages, Exchange configuration errors, corrupt logs and other problems that affect the global messaging environment.

Calculating the acquisition cost of HA system hardware is fairly straightforward. However, the long-term maintenance and operating costs of these solutions is harder to calculate and a more significant calculation.

Consider an example of a medium-size organization that currently deploys Exchange 2003 clustered mailbox servers: in addition to the purchase cost of the clustered servers and shared storage, the company must also spend money on cluster-aware versions of the operating system, applications, and third-party products like backup utilities and spam filters. In addition, the organization must also attract, train, and retain administrators with the skills necessary to maintain the cluster environment. Despite these complexities, it is very important to compute the cost of a given HA technology so that you can compare it with the benefit (in the form of reduced downtime) that it is expected to deliver.

BACKUP AND DISASTER RECOVERY

Every organization should have a clear, comprehensive, and (most importantly) tested strategy for performing backups, restores, and disaster recovery of their critical data. Unfortunately, while most companies pay attention to backup and recovery, many administrators do not have adequate processes in place for these activities.

Upgrades can be especially chaotic for data protection processes. For example, if you lose the datacenter that houses a new Exchange 2007 mailbox server just after moving mailboxes to it, what steps do you take to recover the mailbox data and where do you recover to? Will your administrators be able to provide continuation of critical services while they are recovering the older mailbox data, ensuring that your employees can at least send and receive current email, or will everything be offline until they complete the restore process?

CONTROL MIGRATION RISKS

No IT upgrade is without risk. This is as true for upgrades performed to increase availability as it is for every other type of upgrade. For instance, Exchange 2007 does not allow in-place upgrades from previous versions of Exchange. Since it requires the 64-bit version of Windows Server 2003, you can neither install it on your existing Exchange servers running 32-bit Windows Server 2003, nor can you install Exchange 2003 on 64-bit Windows. This limitation reduces the degree of risk you face in upgrading, because the primary supported means of upgrade is moving mailboxes from the old servers to the new ones.

The Exchange mailbox mover is robust and well-tested. However, there are a significant number of other risks that can occur during migrations and upgrades, including problems with mail flow, schema updates, Active Directory replication, and ancillary services. Careful planning of recovery and continuity capabilities can mitigate these migration risks to help ensure that no messaging data is lost and users do not experience unplanned outages.

CAREFULLY CONSIDER THE TOTAL COST OF OWNERSHIP

While none of these factors are overwhelming by themselves – and many of them offer genuine benefits to your organization beyond the mere financial – in the end, they can combine to become a significant addition to the total cost of ownership (TCO) for Exchange 2007. It is important to ensure that you have adequately identified these issues now so that your plans for the upgrade will reflect the real costs, limitations, and goals for your organization. By collecting this data, you can more objectively assess the benefits and drawbacks of all of your deployment options and find the choices that will provide you the best overall value for your messaging system and allow it to meet all of its design goals over its lifetime.

Upgrading to Exchange 2007 offers the potential to correct any existing flaws in your messaging system and introduce new capabilities and features. At the same time, though, it defines a period of increased risk. These risks, their overall impact to your organization, and your ability to mitigate or even remove them, must be a part of process you use to evaluate the choices made in designing your migration strategy. By employing Dell's Email Management Services (EMS) as part of your upgrade, you not only can begin to see immediate benefits for your existing Exchange deployment, but also help reduce the cost and complexity of your upgrade to Exchange 2007 by providing a fallback for your mission-critical messaging operations even if your upgrade runs into unexpected problems or delays.

3 FIVE CONSIDERATIONS FOR EVALUATING EXCHANGE 2007 RISKS AND INVESTMENTS

Deciding how to invest in your messaging systems can be difficult. These five considerations will help you identify whether your planned investments will provide the benefits looking for in Exchange 2007.

1. **Look at the broader picture.** Will your proposed investments solve multiple problems at once? Will updating your Exchange installation address all of your messaging needs, or will you still need capabilities that Exchange doesn't provide? Can you effectively use Exchange 2007's site redundancy features to protect your data?

2. **Don't let complexity spiral out of control.** It's better to start small and expand your deployment scope as you gain knowledge. Will a migration to, and the support of Exchange 207 be possible with your current staff, or will it require additional training, more employees, support contracts, and consulting services?

3. **Avoid esoteric configurations.** You can easily get into a reliability spiral: you deploy new technologies to raise availability, but they add complexity, which increases downtime, so you look for more new technologies…

4. **Pay close attention to how many copies of messages are being stored across the enterprise.** More copies means more cost, difficult policy management and expensive e-Discovery

5. **Strategically use managed services to reduce risk, cost, and complexity.** Does it make business sense to consider the use of managed services to provide in-house high availability, business continuance, compliance applications, email retention, and anti-spam and anti-virus filtering?

4 DELL EMS AUGMENTS EXCHANGE 2007 ARCHITECTURE

For CIOs and email administrators, email may appear to be a no-win proposition fraught with risk. Exchange 2007's new capabilities will help reduce these risks, but still fall short of providing a complete solution for organizations that desire the following capabilities:

- Granular message retention policies with near-effortless management.
- Easily executed, rapid search capabilities to find required messages for legal, HR, or compliance purposes.
- Protection against the loss of BlackBerry[3] connectivity.
- Effectively eliminate email data loss windows between nightly backups.
- Control and minimization of the growing size of email data stores.
- The ability to easily block new types of spam and viruses.

[3] BlackBerry continuity is dependent on the availability of the customer's BES server.

Although piecemeal solutions exist to solve many of these problems individually, the typical results are overly complicated, expensive, and difficult to manage and maintain. Adding Dell's Email Management Service to Exchange 2007 is a low cost and easily managed solution capable of addressing all of these needs.

For organizations that just require high availability email services, Dell EMS and Exchange 2007 together can provide an elegant solution enabling low-cost, direct-attached primary storage to be coupled with back up email data and services provided from a top-tier, datacenter. Users get reliable, increased-capacity mailboxes. Administrators get the worry-free maintenance and known cost structure of a managed service that helps eliminate data loss.

Dell EMS Email Continuity captures email before a failure occurs, storing it in a secure datacenter, and providing off-premise activation of the continuity system through a Web interface or a toll-free number. This allows you to activate the EMS Email Continuity service within minutes to resume business operations with an existing database of recent mail, plus the ability to send, receive, and search mail using either Microsoft Outlook®, a browser-based interface or optionally BlackBerry wireless devices. These capabilities greatly reduce your window of vulnerability during outages by allowing your business to keep operating normally while you restore your Exchange infrastructure and operations.

If email archiving is required, adding EMS Enterprise Archive to Exchange 2007 enables worry-free retention policy management and rapid enterprise-wide search and discovery for email and attachments. The service helps ensure that the archive is always available to users regardless of what may happen to local infrastructure.

Dell EMS Enterprise Archive's comprehensive archival integration with Exchange allows you to set granular attachment stubbing policies. Stubbed attachments are removed from the Exchange data store but can still be accessed out of the archive directly from the original Microsoft Outlook message. With Dell EMS, companies can provide virtually infinitely expandable mailboxes while simultaneously decreasing Exchange data stores by as much as 80%.

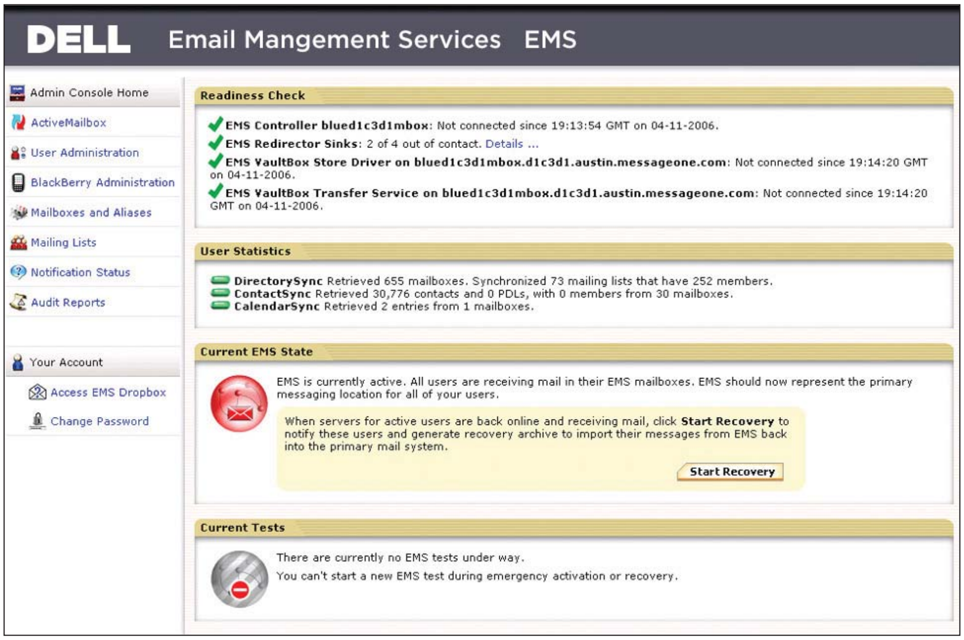
Dell EMS's granular retention policies provide the ability to perform legal holds; they also allow the creation of centrally managed retention policies at the individual, topological, geographical and departmental levels. While end-users can be granted search capabilities for their individual mailboxes, retention policies are set by IT and cannot be modified by end users.

Dell EMS's enterprise-wide search capabilities make it easy for legal counsel to search selected mailboxes or the entire environment using any search criteria, limited only by the scope of the investigation. EMS provides full text search and retrieval of all email and 400 types of attachments in seconds. Search results can easily be exported to a legal discovery system or to a dedicated Microsoft Exchange mailbox for legal review.

Adding EMS to your Exchange 2007 deployment helps provide:

- Effective email downtime protection for users.
- Effectively eliminate data loss.
- Rapid search and discovery of email and attachments.
- Granular retention policy management.
- Reduced storage costs coupled with increased user mailbox sizes.
- Increased protection during the Exchange 2007 migration.
- World-class spam and anti-virus filtering.
- A very efficient architecture to achieve your messaging needs.

Dell EMS provides functionality that Exchange 2007 is missing including, effectively eliminating email downtime and data loss in your primary environment while delivering the benefits of email archiving. As an on-demand service closely coupled with in-house software, Dell EMS fully integrates with Active Directory and Microsoft Outlook providing a seamless experience for end-users. EMS and Exchange 2007 together yield a new email architecture that helps eliminate downtime, eliminate the risk of data loss, reduces costs, and shrinks maintenance, backup, and recovery times. EMS has been the choice of over a thousand companies and can be deployed as quickly as in a single day.



Readiness Check

✓ **EMS Controller blued1c3d1mbox:** Not connected since 19:13:54 GMT on 04-11-2006.
✓ **EMS Redirector Sinks:** 2 of 4 out of contact. Details ...
✓ **EMS VaultBox Store Driver on blued1c3d1mbox.d1c3d1.austin.messageone.com:** Not connected since 19:14:20 GMT on 04-11-2006.
✓ **EMS VaultBox Transfer Service on blued1c3d1mbox.d1c3d1.austin.messageone.com:** Not connected since 19:14:20 GMT on 04-11-2006.

User Statistics

DirectorySync Retrieved 655 mailboxes. Synchronized 73 mailing lists that have 252 members.
ContactSync Retrieved 30,776 contacts and 0 PDLs, with 0 members from 30 mailboxes.
CalendarSync Retrieved 2 entries from 1 mailboxes.

Current EMS State

EMS is currently active. All users are receiving mail in their EMS mailboxes. EMS should now represent the primary messaging location for all of your users.

When servers for active users are back online and receiving mail, click **Start Recovery** to notify these users and generate recovery archive to import their messages from EMS back into the primary mail system.

Current Tests

There are currently no EMS tests under way.

You can't start a new EMS test during emergency activation or recovery.

ABOUT DELL

Millions of people around the world depend on Dell Modular Services' on-demand solutions for business continuity, archiving and disaster recovery. More than one thousand CIOs at global companies including Allianz Global Investors, Siemens and the American Red Cross Lee County Florida, trust Dell to prevent downtime, protect communications and data, and streamline compliance and discovery.

CONTACT DELL TODAY

For additional information including pricing and a free demo, please visit **www.dell.com/modularservices**