Dell Software

Protecting Exchange: Best Practices and Practical Tips

Abstract

Protecting email data is mission-critical for today's organizations. While disaster recovery (DR) and business continuity (BC) plans are necessary, they do not constitute a comprehensive and effective email data protection strategy. This white paper offers the best practices and practical tips you need to protect the mission-critical email data in your Microsoft® Exchange environment.

Introduction

Today, email is mission-critical.

Data protection, including protection of email, is now both more important and more difficult. The increased importance derives from the growing dependency on data. According to Gartner, most organizations now categorize over half of their data as "mission critical" to their operations, and email is included in this classification. Once considered a convenient and additional means of communication, email is now the primary form of online communication in most organizations.

The increased difficulty derives from the growing volume and velocity of data. According to Gartner's June 2011 report "Technology Trends You Can't Afford to Ignore," most organizations are experiencing a minimum of 20-30 percent growth in the amount of data they store every year, and most analysts predict average annual data growth rates will be around 50 percent in the foreseeable future.

A good data protection strategy enables quick recovery of email without data loss.

A good data protection strategy must prevent the loss or corruption of the growing volumes of mission-critical data, and most data protection solutions do that well. But the best practice today in data protection is really about minimizing downtime. And for good reason: According to a 2011 Forrester survey reported in **Disaster Recovery Journal**, the cost of business downtime averaged approximately $145,000 per hour.

Storage-level resiliency, such as that provided by RAID, affords little or no protection against data losses caused at the application level.

The key to minimizing downtime is rapid recovery to normal operations with minimal or zero data loss. For email, the return to normalcy requires fully restoring the organization’s Exchange or other mailbox servers and all its individual mailboxes—without the loss of a single message.

E-discovery requirements are important to a data protection strategy.
Today, recovery for email has another important role to play due to the occasional need for e-discovery of messages pertaining to a specific topic, timeframe or individual. The requirement could be internal, such as a need to investigate suspicious activity, or it might come from outside the organization as part of a customer complaint, an open record or regulatory compliance request or even a lawsuit. The ability to quickly and easily discover and recover all pertinent active and archived emails should, therefore, be considered an important aspect of a data protection strategy for Exchange.

About this document.
This white paper provides an overview of today’s best practices and offers some practical tips for protecting mission-critical email data in Microsoft Exchange environments. The material is organized into three sections. The first section outlines the key considerations involved in an email protection strategy. The second section explores some of the options for protecting Exchange with an emphasis on minimizing both downtime and the loss or corruption of email data. The third section provides a brief introduction to Dell’s data protection solutions for Exchange.

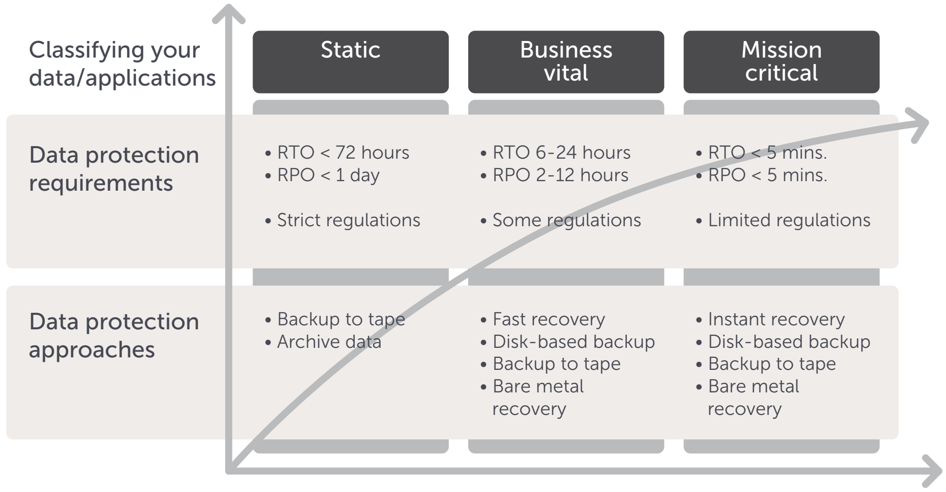
Considerations for an email protection strategy

Disaster recovery strategies should span everything from the data center to the inbox.
A best practice in data protection has always been to anticipate and plan for the worst: Imagine the worst possible event or circumstance, and make sure the data protection strategy includes the means to remedy the situation or mitigate the consequences. For email, the scope of the effort must span everything from an entire data center to an individual email message. The organization’s disaster recovery (DR) or business continuity (BC) strategy likely already addresses the rare but catastrophic natural disaster, as well as the occasional power or network outage that affects the data center. The DR or BC strategy probably also encompasses most server-level failures, whether caused by software or hardware.

While the typical DR/BC strategy addresses failures at the system and data center levels, it might not address failures at a more granular level, such as an individual mailbox or email message. And storage-level resiliency, such as that provided by a redundant array of independent disks (RAID), also affords little or no protection against data losses caused at the application level. Should the Exchange application ever crash, for example, the database could become corrupted. And if the corruption goes unnoticed for a while, every mirrored, replicated or backup copy only perpetuates the problem.

Email problems can also occur at an even smaller scale, of course, including in a single mailbox or even a single email. Any administrator who thinks the loss of a single email could not possibly constitute a catastrophe should imagine getting a call from a CEO who has just accidentally deleted a business-critical email that must be recovered prior to an important meeting starting in just 10 minutes.

Understand the requirements for your email protection strategy.
Creating a robust email protection strategy begins with understanding the organization’s needs, and interviewing key stakeholders is a good way to gain insight into the value the organization places on email communications. Be certain to ask about acceptable levels of both service downtime and data loss, which should also include corruption



Classifying your data/applications	Static	Business vital	Mission critical
Data protection requirements	• RTO < 72 hours • RPO < 1 day • Strict regulations	• RTO 6-24 hours • RPO 2-12 hours • Some regulations	• RTO < 5 mins. • RPO < 5 mins. • Limited regulations
Data protection approaches	• Backup to tape • Archive data	• Fast recovery • Disk-based backup • Backup to tape • Bare metal recovery	• Instant recovery • Disk-based backup • Backup to tape • Bare metal recovery

Figure 1. A robust data protection strategy has the granularity to accommodate different requirements for different applications with different approaches.

It is desirable to establish different RTOs and RPOs for different data sets.

as a form of loss. In most organizations, where email is likely to be mission critical to daily operations, the answer to both questions is likely to be, "None!"

Other key stakeholders to interview include the legal department or corporate counsel to gain an understanding of how regulatory compliance requirements apply to email, especially concerning privacy and retention. This is also a good time to understand the IT infrastructure requirements involving your data centers, networks, physical and virtual server configurations, and so on.

Set RTO and RPO standards.
The hallmark of a carrier-class data protection strategy is the ability to recover from any problem quickly and completely. For this reason, recovery time and recovery point objectives are of paramount importance.

- **Recovery time objective (RTO)** is the acceptable amount of time it takes to recover fully from a loss or outage, thereby restoring business operations to normal. While some applications can tolerate hours or even days of downtime, the RTO for mission-critical applications like email is usually mere minutes.
- **Recovery point objective (RPO)** is the last acceptable point in time that data can be recovered (i.e. most recent backup). For mission-critical applications, the RPO is most likely to be the most recent transaction, which, in the case of email, is the most recent email sent or received.

Understand the granularity of recovery.
An often overlooked aspect of recovery objectives involves granularity. As shown in Figure 1, it is desirable to establish different RTOs and RPOs for different data sets. For data that is rather static or less critical to the business, a delayed recovery to a daily backup might be adequate. A good example is archived data that changes rarely (if ever) and might, therefore, be stored more economically on tape. Mission-critical applications, by contrast, cannot tolerate much (if any) downtime or data loss/corruption. In the case of email, granularity should also take into account the smallest increment of data, which is an individual email message.

Best practices for Exchange data protection

The rise of email's importance to mission-critical status has been accompanied by an increase in the options available for protecting email applications and data. A particularly powerful way to evaluate the many different options available involves viewing email protection "backwards" from the perspective of a recovery from potential worst-case scenarios.

In other words: The faster and more complete the recovery, the better the data protection strategy. Here are some of the best practices for Exchange data protection to keep in mind:

Understand the two types of backups.
Recovery from the loss or corruption of an email database typically utilizes the most recent backup, but it may utilize an older or archived backup for valid reasons, such as to recover from corruption or for e-discovery. At the risk of oversimplification, there are two types of backups: traditional and continuous data protection.

- **Traditional backups**—Traditional backups can be either full or incremental. As the name implies, a full backup creates a complete copy of the full database. With incremental backups, only the data that has changed (often on a daily basis) since the previous full or incremental backup is included. The target medium can be either disk or tape, with the former providing faster recovery speeds and the latter being less expensive.
- **Continuous data protection backups**—When email is considered mission-critical and RTO and RPOs are stringent, continuous data protection is preferable. As the name implies, the backup occurs in near real time as changes are made to the source data. Because this also makes the backup continuous, near-real-time backups are also called "continuous data protection" (CDP). CDP requires an initial synch or seed of the source data being protected (analogous to the traditional full backup), which is then updated in near real time with each and every change made. For this reason, CDP is capable of making the recovery point the most recent transaction or, in this case, the most recent email sent or received.

High availability (HA) should not be considered a substitute for a robust data protection strategy.

CDP is sometimes confused with high-availability (HA) provisions because both copy or replicate data in near real time. But HA is intended to fulfill an entirely different need and, therefore, should not be considered a substitute for a robust data protection strategy. For Exchange, HA is provided by Database Availability Groups (DAG), a redundancy framework that made its debut with the 2010 version. A DAG contains up to 16 mailbox servers that each replicate Exchange databases to one another, providing rapid recovery from server and application or database failures. DAGs employ Exchange Continuous Replication (log shipping and replay) and a subset of Windows failover clustering technologies to provide HA within and across data centers. So while a DAG can protect against data loss (depending on the lag period specified), it does not protect against corruption.

Establish offsite protection using replication.
Perhaps the most challenging need to restore data occurs in the event of a major disaster. Because some disasters, such as major earthquakes, tornados or fires, are big enough to affect entire data centers, data protection strategies should always include routine replication of data stored on local backup servers to backup servers at another site (and vice versa) or in the cloud. To accelerate the recovery process, the replicated copies are typically stored on disk (rather than tape), and may use deduplication or compression to conserve network bandwidth and space, as well as encryption to secure data replicated to a public cloud.

Document and test the data protection plan.
While establishing a robust data protection strategy and choosing the best available backup and replication options are necessary, these two steps are far from being sufficient. Indeed, the most important aspect of data protection may well be documenting and testing the plan to ensure it actually works as intended. Even the best plan (on paper, at least) could be worthless if the recovery fails owing to mistakes or errors that could have been prevented.

Have a communications plan.
Recoveries are inevitably stressful, so anything that can be done beforehand to instill a calm confidence in the staff is well worth the effort. This is why a comprehensive communications plan is the foundation for good execution. The communications plan should identify and document all of the personnel who might need to be involved in different disaster recovery scenarios, along with their specific responsibilities and the chain of command that might be required for substitution and/or escalation.

Establish the order in which items are to be restored.
Because resources are finite and recovery procedures take time, the plan should establish clear priorities for what should be restored and in what order. This is particularly true for Exchange, where it may be necessary to restore Active Directory before restoring any mailbox servers or databases. The order for restoring mailbox servers might also be important, with the mailbox servers of the IT staff responsible for the recovery likely to be the top priority.

Keep email operational during outages.
Another high priority is something that is often overlooked as a best practice: establishing a "dial-tone" email system that enables all users to send and receive new emails during a power outage. The term "dial-tone" is used because even during power outages, phones often continue to work, and users really should be able to expect a similar level of dial-tone service for communications as mission-critical as email. It may take a while to restore all of the email history for all of the users, but that is largely irrelevant to the pressing need to communicate in real time following a major outage or disaster. The dial-tone email service can also help relieve some of the pressure on the IT staff to get "everything" up and running as soon as possible.

Dell's recovery solutions for Exchange

Dell™ recognizes that the best data protection solutions take into account an organization's RTOs, RPOs, granular recovery objectives, retention requirements and budget. Therefore, Dell offers a suite of recovery solutions for Microsoft Exchange.

Dell NetVault Backup.
NetVault™ Backup is a cross-platform backup and recovery solution designed to simplify data protection across a wide range of operating systems, applications and storage technologies in both physical and virtual environments. Features of specific interest for mission-critical Exchange environments include:

- Backup, replication and long-term retention/archiving to disk, tape, SAN and/or NAS, including third-party disk storage arrays, virtual and physical tape libraries, autoloaders and tape drives.
- Online backups via the Extensible Storage Engine (ESE) API or the Volume Shadow Copy Service (VSS).
- Exchange Server high-availability support for Single Copy Clusters (SCC), Cluster Continuous Replication (CCR), Local Continuous Replication (LCR) and Database Availability Groups (DAG).
- NetVault Backup is a scalable solution that can protect large organizations with massive numbers of servers and petabytes of data. Moreover, its broad heterogeneous support, modular architecture and intuitive user interface makes it easy for administrators to monitor and manage their backup operations, reducing operating costs. NetVault Backup also offers data deduplication to reduce backup storage footprints by up to 90 percent, replication for offsite protection against site disasters and bare metal recovery for fast and easy system restores.

AppAssure features near-continuous data protection for Exchange Servers, deep integration with Exchange for message-level search and recovery and built-in snapshot replication for easy offsite disaster recovery and cloud backup of Exchange servers.

Dell AppAssure.
Dell AppAssure™ is backup, replication and recovery software that features near-continuous data protection for Exchange Servers, deep integration with Exchange for message-level search and recovery, and built-in snapshot replication for

With Dell Recovery Manager for Exchange, administrators can search and retrieve message-level data from multiple sources in minutes.

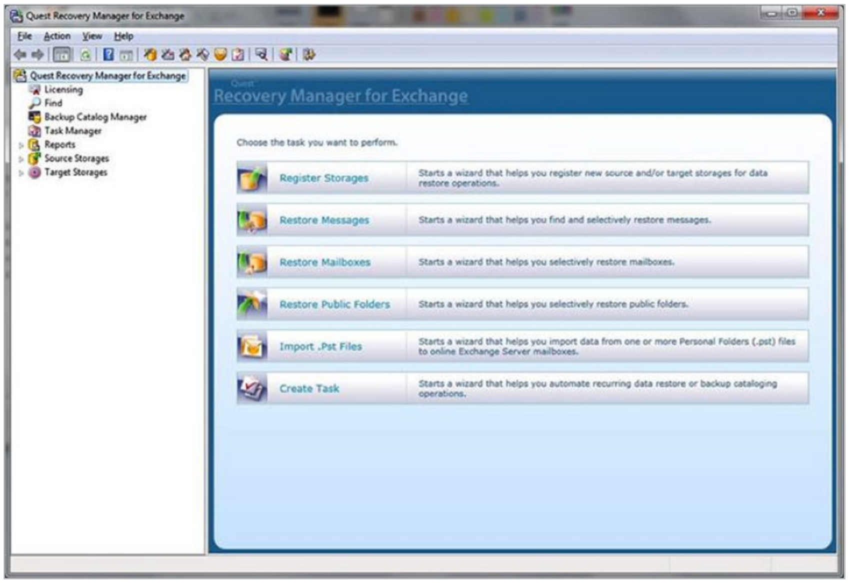
easy offsite disaster recovery and cloud backup of Exchange servers. AppAssure for Exchange delivers mission-critical protection for Exchange with these four industry-leading capabilities:

- **No-impact, "hot" backups** that require no downtime, providing continuous protection with no adverse impact on performance.
- **Near-zero RPOs** with snapshots taken every five minutes, resulting in up to 288 recovery points in a 24-hour period.
- **Near-zero RTOs** with a Live Recovery™ capability that enables users to begin using Exchange in 15 minutes or less after a failure..
- **Recovery Assure™** lets you perform automated recovery testing and verification of Exchange backups. By identifying data corruption early and preventing corrupted data blocks from being maintained or transferred during the backup process, you can be certain that Exchange is recoverable.

In addition, the solution's data deduplication and compression capabilities allow backup snapshots to be stored using 80 percent less disk space. AppAssure also offers built-in support for remote office servers and snapshot replication, offsite disaster recovery and cloud-based backup strategies.

Dell Recovery Manager for Exchange. Dell delivers the granularity of recovery that you need. Dell™ Recovery Manager for Exchange makes discovering and exporting mission-critical email data fast and easy. From a single console, administrators can search and retrieve message-level data from multiple sources in minutes. Searches can be based on sender, recipient(s), subject, date, message or attachment keyword(s), attachment type and content, conversation threads and deleted items. The results can be exported in a variety of formats to facilitate virtually any e-discovery request. Searches can also compare the contents of online and backup mailboxes to restore any emails that have been inadvertently deleted.

Dell Recovery Manager for Exchange has been designed to work in the most popular data protection environments, offering support for NetVault Backup as well as most major third-party backup software. The federated search also supports a broad range of file types, including Office 365®, production and archived mailboxes, public folders, personal folders (.pst), offline Exchange database files (.edb), Dell™ Archive Manager and most backup and snapshot formats.



Choose the task you want to perform.

Register Storages — Starts a wizard that helps you register new source and/or target storages for data restore operations.

Restore Messages — Starts a wizard that helps you find and selectively restore messages.

Restore Mailboxes — Starts a wizard that helps you selectively restore mailboxes.

Restore Public Folders — Starts a wizard that helps you selectively restore public folders.

Import .Pst Files — Starts a wizard that helps you import data from one or more Personal Folders (.pst) files to online Exchange Server mailboxes.

Create Task — Starts a wizard that helps you automate recurring data restore or backup cataloging operations.

Figure 2. Dell Recovery Manager for Exchange offers a wide range of capabilities, plus intuitive navigation.

Conclusion

Protecting Microsoft Exchange Server requires a backup and recovery solution that is capable of supporting a range of recovery requirements. The solution should be affordable and easy to use, so you can minimize your capital and operating costs. It should support your recovery point and recovery time objectives, enabling rapid and full recoveries under all possible circumstances. It should be able to restore data at any granularity—from the entire application to a single email. And the solution should be dependable to minimize problems during stressful recovery efforts.

To learn more about how Dell data protection solutions can help you protect your mission-critical email, and to download free trials, visit the Dell Software website at www.software.dell.com.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.