Meeting

Regulatory Compliance Requirements

with VERITAS Enterprise Vault and Microsoft Windows Server Technologies

Creating an electronic messaging system to meet regulatory compliance requirements can be a complex process. This article provides guidance for organizations that need to implement such a system, outlining a strategy that is designed to enable centralized search and retrieval across archived data as well as workflow processes that can help provide quick response to requests for archived electronic data or correspondence. This approach allows fast, efficient data retrieval that can free administrators from the process of restoring messaging data from backup tapes.

BY SCOTT ROSEN

To meet regulatory compliance requirements, some organizations must preserve e-mail correspondence as a business record that can withstand scrutiny in a court of law or regulatory review. To help address this need, data archiving tools such as Enterprise Vault’s software and Discovery Accelerator from KVS, a business unit of VERITAS, can be combined with Microsoft® Exchange Server 2003 and Dell PowerVault network attached storage (NAS) servers powered by Microsoft Windows® Storage Server 2003. VERITAS Enterprise Vault software provides an enterprise-class platform for data archiving, and Discovery Accelerator enables centralized search and retrieval across archived data as well as workflow processes that help administrators respond quickly to requests for archived documents and messages. In addition, Enterprise Vault software and Discovery Accelerator can be integrated with Microsoft Windows Storage Server 2003, Microsoft Exchange Server 2003, and Microsoft SharePoint® Portal Server 2003 to create a prescriptive framework for message and document archiving.

The configuration described in this article includes Dell PowerVault NAS servers as well as Dell PowerEdge™ servers designed to provide a high level of performance, scalability, and reliability. Together, these products offer organizations key components of an overall information life-cycle management (ILM) strategy: the ability to capture, archive, and destroy data based on corporate policies; an audit trail that enables compliance; and dependable tools that leverage existing IT investments.

This article discusses the use of message archival systems and explores protection strategies that can help ensure that enterprise data is appropriately stored and maintained. Unless otherwise noted, the approach outlined in this article assumes that Microsoft Windows Server™ 2003,
the Microsoft Active Directory® directory service, and Exchange Server 2003 have been deployed in the data center.

**Understanding the current business environment and regulatory compliance**

Over the past decade, e-mail has become a mission-critical tool for many enterprises. However, e-mail archive and retrieval procedures are usually enacted in an ad hoc manner. Few organizations take the time to clearly define policies regarding the use of messaging, the types of data that will be transmitted, and the types of data protection to use. Many organizations are discovering the need for a system that can help ensure that data within their Exchange Server messaging environments is safely stored in a searchable, retrievable format.

Although many regulations affecting businesses do not necessarily require message archiving, today’s regulatory environment is changing and businesses need to be aware of the influence this change may have on the long-term operations of their messaging systems. Businesses in the financial and health-care industries have long been aware of the need to archive and track their communications because of regulations such as the Securities and Exchange Commission (SEC) Rule 17A-4 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Now, organizations in industries that have not previously felt the need to retain e-mail data may face that necessity. Regulations such as the Sarbanes-Oxley Act of 2002 have highlighted the need for organizations in all industries to maintain, store, and secure data, including electronic (instant) messages, for periods ranging from 90 days to 30 years or more.

**Identifying the components of a message archiving system**

The approach outlined in this article incorporates Microsoft Exchange Server 2003, Microsoft SharePoint Portal Server 2003, and Microsoft Windows Server 2003 running on Dell PowerEdge servers to provide messaging services. VERITAS Enterprise Vault software and Discovery Accelerator also run on Dell PowerEdge servers, and these applications archive information to Microsoft Windows Storage Server 2003, which runs on Dell PowerVault NAS servers. Figure 1 shows the overall architecture of this message archiving system.

**Microsoft Exchange Server 2003**

Message journaling within Exchange Server enables organizations to archive messages sent between end users and external Internet addresses. With minor configuration changes, all internal messages can also be archived. Service Pack 1 for Exchange Server 2003 introduces enhanced journaling capabilities that enable VERITAS Enterprise Vault software to provide a rich archiving tool set to organizations.

**VERITAS Enterprise Vault and Business Accelerators**

Delivering enterprise-class document and e-mail archiving services for Microsoft Exchange and SharePoint Portal Server implementations, Enterprise Vault 5 with Cumulative Patches 3 offers a single interface for archived e-mail messages, SharePoint file system documents, and instant messages. Enterprise Vault software enables administrators to consolidate Exchange server, eliminate Personal Folders (.pst) files from the environment, archive data within file servers, migrate data within Exchange public folders, archive current data within mailboxes, and meet regulatory compliance goals.

The content archiving approach provided by Enterprise Vault, along with the Discovery Accelerator add-on, can help reduce the ongoing cost of e-mail storage, bring control to mailbox management, optimize the backup and recovery cycle, and ensure that valuable information can be retrieved quickly and efficiently to facilitate compliance and knowledge management. Also, Compliance Accelerator for Enterprise Vault can be implemented to provide additional capabilities that help meet ILM requirements and alleviate business risk.

**Microsoft Windows Storage Server 2003**

In the approach described in this article, Windows Storage Server 2003 is configured to host the Enterprise Vault archives. Windows Storage Server 2003 is designed to provide dependability and seamless integration while enabling organizations to derive optimal value from their networked storage. For example, Windows Storage Server 2003 is well suited for consolidating organizational data such as Enterprise Vault archives into a single system that can help achieve cost reduction and policy-based management of storage resources.

Windows Storage Server 2003 includes advanced availability features such as point-in-time data copies, replication, and multi-node clustering. Because Windows Storage Server 2003 implementations...
are typically preconfigured to the purchaser’s specifications, they can be rapidly deployed out-of-the-box and require minimal expertise to set up. The Web-based user interface makes management easy. The Dell PowerVault 700 series storage servers can be preconfigured with Windows Storage Server 2003.

Defining data retention policies
Date retention is both an IT and a business concern that is defined by multiple groups within an organization, including the legal, IT, finance, and operations departments. A sufficient electronic messaging policy defines acceptable use of the system, such as permitting end users to send and receive personal e-mail, allowing e-mail solicitations, disallowing the use of e-mail for harassing or threatening messages, and prohibiting the transmission of potentially offensive images. The policy should define what company materials are confidential, and when and under what circumstances company-confidential materials can be shared with third parties. It is preferable to clearly state that users cannot send company-confidential data to a third party unless that third party is receiving the data for a legitimate business reason, and that illegal use of the system will not be tolerated. Retention periods for communications should be clearly defined; organizations that are subject to specific regulations defining retention periods should ensure that these requirements are clearly stated in their policies.

When creating an electronic messaging policy, organizations should ensure that the correct stakeholders are involved and that the policy is not created in a vacuum. The legal department, financial advisors, and systems managers must coordinate their efforts to create a policy that not only is legally correct, but also adequately protects the interests of the organization and can be properly implemented and enforced. The risks and realities of the organization’s structure must be considered, and the policy should be clearly defined and implemented.

The SANS (SysAdmin, Audit, Network, Security) Institute, a cooperative research and educational organization for information security professionals, provides a sample policy for e-mail retention, available at www.sans.org/resources/policies/e-mail_retention.pdf. This can help organizations begin the process of creating a data retention policy.

Examining the current regulatory environment
In the United States, numerous federal regulations affect various organizations.1 While the financial industry has long been subject to oversight by the SEC and the National Association of Securities Dealers (NASD), and the health-care industry has rushed to meet the requirements put in place by HIPAA, other types of organizations are now becoming actively involved in the regulatory process. The enactment of broad-reaching regulations, such as the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act, has created the need for organizations in various industries to identify ways to safeguard, disseminate, store, and track financial information. Many states have enacted regulations that supersede these federal regulations, so organizations also must ensure that they are complying with the pertinent state laws in addition to applicable federal regulations.

Regulations affecting electronic messaging
Regulations can affect how, where, and how long organizations must maintain electronic records, including e-mail. Compliance with the relevant regulations is a complex process and should be overseen by appropriate legal counsel. While the following regulations are pertinent to many organizations and present a good overview of the overall regulatory environment today, organizations should rely on legal counsel to determine applicability and analysis:

- Sarbanes-Oxley Act
- SEC Rule 17A-4
- HIPAA
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)
- Department of Defense Rule 5015.2-STD
- National Archives and Records Administration
- CFR Title 47, Part 42 – Telecommunications
- CFR Title 21, Part 11 – Pharmaceuticals

A more detailed discussion of these regulations can be found at www.veritas.com/compliance/home.html.

Retaining and archiving messaging data
While many regulations require a specific retention period for business-specific data, every business is not required to meet this requirement. Financial services organizations typically have the most stringent data retention requirements. Nonetheless, enterprises that are not subject to specific data retention requirements should document their data retention policies and follow these policies. Otherwise, organizations that define but do not follow their data retention policies may be required to spend innumerable hours restoring and retrieving data from backup media during a legal discovery process.

A well-thought-out data management plan should ensure that data retention policies mesh with actual data management processes.

---

1 The regulations referenced in this article are specific to the United States, but many other countries have similar legislation in place. Organizations should be aware of the regulatory requirements for the geographic areas in which they conduct business.
For example, if the data management plan states that e-mail is kept for one year, backup tapes should not be retained for more than that length of time. Centralized data storage for e-mail and other types of documents—such as a SharePoint Portal Server document repository—can help administrators recover such data easily. The ability to preview this documentation, should it be necessary, can be extremely helpful when approaching a legal proceeding.

Numerous factors can create the need for a regulatory compliance system. Determining whether an organization needs to implement such a system requires cooperation between various divisions of the organization. Understanding the drivers for the implementation of document life-cycle management tools such as Enterprise Vault and Discovery Accelerator can help organizations ensure that the data management plan will have proper system support.

The three primary components of a regulatory compliance system are archiving, retention, and discovery. These components complement one another, and organizations that must meet regulatory compliance rules should consider the factors driving each component before implementing such a system.

Business-critical data should be maintained in a logical, retrievable manner. The challenge of message archiving is determining what data to keep, how long to keep it, who should have access to it (or to a subset of the data), and where to store it.

**What data should be archived?**

Data that pertains to legal, financial, and business decisions should be archived according to the organization’s data retention policy. E-mail messages relating to lunch dates, personal conversations, and the minutiae of running a business probably do not need to be maintained.

Accurate data archiving, with an audit trail, is required to help ensure that all business data is accurately captured and can be verified as original data, or an accurate reproduction thereof. The right data must be captured and stored, and it also must be retrievable.

For the purposes of the data management strategy enabled by the configuration described in this article, the archived data is primarily messaging data. When envelope message journaling is enabled, all messages from, to, and within an Exchange environment are sent to a central journaling mailbox. The data sent to the journaling mailbox is then queued for delivery to the Enterprise Vault server.

**How long should data be retained?**

Businesses that are bound by the SEC should retain data for no less than seven years; during the first two years of retention, the data must be easily accessible. Other types of industries may have specific regulations that pertain to record keeping, and administrators must understand these regulations and their system requirements. Even businesses that are not bound by industry-specific legislation or rulings are well advised to define a specific data retention period and enact technical measures to comply with that decision.

Of course, data retention policies must be in place before organizations initiate any compliance efforts. It is important that all stakeholders within an organization are involved in creating this policy; IT cannot create a policy without input from other departments.

**Who can access the data?**

To track communications and help ensure that end users are complying with pertinent regulations, administrators may need to give specific trusted individuals access to stored data. This access should be controlled and audited to prevent abuse. Enterprise Vault software with Discovery Accelerator enables administrators to assign roles to users, thereby helping control data access and retrieval. Authorized reviewers can quickly target and mark specific data as necessary to support legal discovery, compliance-related audits, or investigations. Discovery Accelerator provides a structure to control which users may access data and how data is reviewed.

**Who should manage the data?**

Few enterprises employ corporate librarians to manage their company’s data. Even when this role exists within an organization, it is often underfunded, under-recognized, and under-supported. Organizations that do not have a corporate librarian need tools that can support this function—Microsoft and KVS are teaming up to help fill this role. Organizations that do have corporate librarians can also benefit from implementing the Microsoft-KVS system described in this article, because Enterprise Vault is designed to provide a single point of reference for data that originates from several sources.

Because documents from numerous sources—such as Exchange databases, file servers, and SharePoint Portal Server sites—can be merged into a single Enterprise Vault system, this system is designed to become the authoritative source for information gathering. Knowledge management teams can use this data repository not only for discovery purposes, but also for the purpose of gaining an enhanced understanding of the business value of the data. Corporate librarians and knowledge management teams do more than just find information—they analyze and evaluate data to maximize the utility of the information. Data is an important business asset, and the knowledge management team consists of people who understand the vital nature of an organization’s data.

Discovery Accelerator provides roles for data management and retrieval (see Figure 2). These roles include the System Administrator, who creates new cases (discovery processes), configures the marking scheme so messages can be accurately labeled once discovered, and creates user roles; the Case Administrator, who manages the case itself, assigns items to reviewers, and configures new marking schemes; and the Reviewer, who examines the data and marks it for further action, if necessary.
Where should the data be stored?
A centralized data repository can make the discovery process more efficient and reliable than is possible in a widely disparate storage system. Centralized archiving also can be less expensive than distributed storage because it helps provide a better economy of scale for the storage hardware. Although organizations can use either centralized or distributed archiving, most opt to use a centralized architecture for Enterprise Vault software because its caching is designed to provide reliable access to data over long distances and variable electronic link speeds. All business-related data should be kept on servers, and messaging data should be retained on Microsoft Exchange Server or within an archiving system similar to the one described in this article. Local Exchange .pst files pose a risk because they are not centrally controlled and present an unreliable long-term archival system; these files reside on local workstations that all too often are not backed up on a regular basis.

The archiving system described in this article uses NAS servers running Windows Storage Server 2003 to host the Enterprise Vault data archive. Windows Storage Server 2003 is easy to deploy, uses familiar technology for IT administrators, and can be controlled using a Web interface—enabling organizations to quickly add storage to the enterprise network without the need for intense training. Windows Storage Server 2003 also can host several terabytes of data and is designed to provide dependable storage for organizational data.

Reaping the benefits of data retention
Many enterprises that implement a message archiving system similar to the one presented in this article do so to meet regulatory compliance needs. However, implementing such a system can provide additional advantages:

- Archived data creates a searchable corporate knowledge base. Data can be readily searched for and retrieved using tools such as Discovery Accelerator.
- Duplication of effort is reduced. For example, global marking of data within Discovery Accelerator helps ensure that data that has been through a discovery process once does not need to be re-discovered and re-reviewed. This can be particularly helpful when the scope of multiple discoveries overlaps.
- Records of communications and processes that were previously stored in individual mailboxes can be made available to individuals or groups that were not involved in the initial communication or document approval path. This capability allows new employees to understand the history behind past business decisions.
- Archived data helps provide improved business continuity, enabling documentation and communications essential to the long-term success of an organization to be accessed in a single repository that can easily be searched and from which data can be quickly retrieved.

- Archived data helps increase end-user productivity. Because of mailbox size limits, users often resort to storing e-mail messages in .pst files, leading to the need to search multiple sources for an important message or document. Enterprise Vault helps eliminate the need for these files, and it enables information workers to quickly retrieve data using simple searches when the client tools are installed on their workstations or the Web retrieval tool has been made available.
- The ability to verify communications helps mitigate risk to business data, and document life-cycle management enables organizations to oversee data intelligently.

Implementing the message archiving system
The electronic messaging system described in this article is designed for an organization with fewer than 3,000 users that seeks to quickly implement a solid platform to meet information life-cycle needs and regulatory compliance requirements. Enterprise Vault software from VERITAS, together with offerings from Microsoft and Dell, is designed to provide reliable data archiving and to enable organizations to implement a message archiving system with minimal planning.
During the fourth quarter of 2003, Microsoft and KVS engineers demonstrated this approach at Microsoft’s labs using the systems described in this article, including Dell PowerEdge servers and Enterprise Vault software. The engineers found that the system architecture and implementation described in this article can provide a good fit for small to medium enterprises and that Windows Storage Server 2003 is well suited to store the Enterprise Vault archives. Microsoft Exchange Server 2003 and SharePoint Portal Server 2003 can be integrated with Enterprise Vault, and the products comprising the integrated architecture described in this article are designed to coexist without requiring numerous custom configuration steps.

Satisfying the growing need for reliable data retention
Organizations that do not have a long-term message archiving system in place should be planning one. To begin this process, administrators must thoroughly understand their system’s messaging capabilities, the processes and technologies involved, and the requirements to ensure that clear data retention policies are in place and being followed.

Microsoft Exchange Server 2003, Microsoft SharePoint Portal Server 2003, and VERITAS Enterprise Vault software with Discovery Accelerator can provide a solid foundation to help organizations meet regulatory compliance requirements. In addition, the flexible Dell PowerVault NAS servers and Microsoft Windows Storage Server 2003 enable organizations to quickly and easily implement large disk arrays that can support the storage needs of Enterprise Vault.

Scott Rosen manages the Global Dell Relationship and Appliance Systems for KVS, a business unit of VERITAS Software. His focus is on channel development. He graduated from the University of Michigan with a degree in Organizational Psychology and Finance.