Integrated solutions for regulatory compliance with Microsoft® Windows Server technologies

Abstract

Creating a solution to meet regulatory compliance is a complex process. This solution blueprint provides guidance for organizations that must implement a data life cycle solution for 3,000 or fewer information workers, using KVS Discovery Accelerator, KVS Enterprise Vault, Microsoft® Exchange Server 2003, Microsoft Office SharePoint Portal Server 2003, and an HP ProLiant Storage Server. KVS Enterprise Vault provides a powerful platform for data archiving, and KVS Discovery Accelerator enables searching and retrieval of the data within the Enterprise Vault. With this solution, there is no need to restore backup tapes for discovery purposes; all data is readily available to be quickly and efficiently retrieved. The instructions in this solution blueprint enable the reader to integrate KVS Discovery Accelerator and KVS Enterprise Vault into an existing Exchange Server 2003 organization.

Introduction

Microsoft Exchange Server 2003, the best selling messaging and collaboration server, combined with storage provided by an award-winning HP ProLiant Storage Server and intelligent archiving solutions from KVS, Inc. (KVS, a business unit of VERITAS), provides organizations with the ability to preserve e-mail correspondence as a business record that can withstand scrutiny in a court of law or regulatory review. Together, these products offer organizations document life cycle management—the ability to capture, archive, and destroy data based on corporate policies with an audit trail that helps create the infrastructure for compliance. For organizations that must implement an efficient, cost-effective approach for meeting document life cycle management, Microsoft and KVS deliver a robust set of familiar, adaptable, and dependable tools that leverage existing IT investments to meet immediate and evolving requirements.

HP, Microsoft, and KVS are partnering to present this solution blueprint to help organizations become compliant with regulatory requirements. HP ProLiant Storage Server, Exchange Server 2003, Microsoft Office SharePoint Portal Server 2003, KVS Enterprise Vault, and KVS Discovery Accelerator integrate to create this prescriptive framework for message and document archiving. The deployment guidance provided within this document is:

- Proven—Based on practical experience
- Authoritative—Providing the best advice available
- Accurate—Technically validated and tested
- Actionable—Directly usable in projects
- Relevant—Addressing real-world scenarios

Current business environment

Over the past decade, e-mail has become a mission-critical tool for many businesses. However, e-mail archive and retrieval procedures are enacted in a largely ad hoc fashion in today's environment. Few companies have taken the time to clearly define policies regarding the use of messaging, what sorts of data will be transmitted, and what types of protection messaging data must have. Many organizations are discovering the need to have a system in place to ensure that data within their Exchange Server messaging systems is safely stored in a searchable, retrievable format.

While many regulations impacting businesses do not necessarily call out a requirement for message archiving, today's regulatory environment is undergoing a period of change, and all businesses should be aware of the influence this will have regarding 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 SEC Rule 17A-4 and the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA). Now, industries that have

not previously felt the need to retain data sent using e-mail might face that necessity. Regulations such as the Sarbanes-Oxley Act of 2002 (SOX) have highlighted the need for all industries to maintain, store, and secure data, including electronic messages, for periods of up to several years.

Enterprise Vault, in conjunction with Exchange Server 2003, provides the ability to archive, or journal, messaging data sent within an organization and to and from external systems and enables organizations to quickly search and retrieve archived data. This capability is vital in ensuring an organization's communications are captured and can be verified if necessary.

Solution components

Microsoft Exchange Server 2003

Message journaling within Exchange Server provides organizations the ability to archive messages sent between their 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 KVS to provide a richer archiving toolset to organizations.

HP ProLiant servers

Microsoft and HP have been business partners for over 20 years and have a relationship that has its roots in a key factor for both companies: Microsoft runs its business on HP servers, and HP runs its business on Microsoft software.

Since the very beginnings of Microsoft Exchange Server as a product, HP has been a key Microsoft partner and has made huge investments in the technology. These investments have positioned HP as the premiere provider of platforms, services, and solutions for Exchange.

HP ProLiant servers are the computer platform of choice by Exchange customers with more than 40% market share.

HP has a unique marketing and engineering relationship with Microsoft. A group of HP software engineers are colocated with Microsoft engineers at the Microsoft Redmond facility, where, under non-disclosure, they work closely with the Microsoft engineers in the testing and debugging of new versions of Exchange and other Microsoft products. This relationship helps benefit customers in that:

- Good engineering-level communications provides HP updates on product development and certification.
- HP products get qualified on Microsoft right from deployment.
- When specific problems are identified, HP engineers can talk directly with Microsoft engineers.

In addition, HP provides solutions engineering expertise in benchmarking, characterization, solution development, deployment guidelines, planning and sizing tools, and so on—all available freely from HP ActiveAnswers.

Key proof points for HP/Exchange expertise

- HP is the only vendor designated by Microsoft as "Prime Integrator" for Exchange Server 2003.
- HP has over 13 million Microsoft Exchange Server 2000/2003 seats under contract through HP Services, plus over 6 million seats through HP authorized business partners.
- HP has over 550 global enterprise customers.
- HP employs over 5,000 Microsoft Certified Engineers.
- Over 850 dedicated Exchange Solution Integration experts are available worldwide from HP.

- HP ProLiant servers are the platforms of choice for Exchange with more market share than the three largest HP competitors combined 24x7 leadership through highly available, reliable systems based on clustering and SAN technologies
- HP solutions architects have published several new books and many white papers on Exchange 2000 and 2003.
- An HP road map can help move you from your present version of Exchange to Exchange 2000/2003
- HP has enlisted best-of-breed partners to ensure a secure and powerful Exchange environment.
- Continuing investment in engineering resources enables HP to expand the existing messaging framework by adding voice, collaboration, and wireless applications
- Microsoft Information Technology Group (ITG) has deployed Exchange 2000/2003, servicing over 60,000 mailboxes on HP ProLiant servers and HP StorageWorks storage within Microsoft infrastructure.

KVS Enterprise Vault and Discovery Accelerator

KVS delivers document and e-mail archiving solutions for Microsoft Exchange and SharePoint Portal Server implementations using Enterprise Vault 5 with Cumulative Patches (CP) 1, an enterprise-class archiving system. Enterprise Vault 5 CP1 offers a single interface for archived e-mail, SharePoint file system documents, and instant messages. The content archiving solution of Enterprise Vault, along with the Discovery Accelerator add-on, reduces the on-going cost of e-mail storage, brings control to mailbox management, optimizes the backup and recovery cycle, and ensures that valuable information can be retrieved quickly and efficiently for compliance and knowledge management use. Also, KVS Compliance Accelerator for Enterprise Vault can be implemented to provide additional capabilities as needed to meet requirements for life cycle management and alleviate business risk.

Enterprise Vault enables you to consolidate Exchange servers, eliminate .PST files from your environment, archive the data within file servers, migrate data within Public Folders, archive current data within mailboxes, and meet regulatory compliance goals for your organization. All messages within the Enterprise Vault archive are stored in both their original message (.MSG) format and either in plain text or HTML format. The message archive also supports envelope journaling, which retains all pertinent message-related data.

Users can browse the archive and view messages using Microsoft Internet Explorer from any workstation, provided the user has the correct permissions to access the archive. Enterprise Vault also provides client access though Microsoft Office Outlook and Outlook Web Access for users both online and offline. All of these capabilities do not impede the way the information worker utilizes Microsoft technologies.

The integration of Enterprise Vault with your SharePoint Portal Server implementation also enables documents to be archived for future reference and recovery. The aggregation of enterprise content enables information workers to better communicate and collaborate, as well as ensures that content will be deleted at the end of its legal and information-valued life.

KVS Discovery Accelerator provides a fully managed review process that enables roles to be assigned to users within the organization. It offers a flexible marking scheme to reviewers so that data can quickly be marked as pertinent when applicable. The powerful searching capability of Discovery Accelerator makes finding content simple, and items can be produced quickly for disclosure to external reviewers.

HP ProLiant Storage Server

An HP ProLiant Storage Server (running Microsoft Windows® Storage Server 2003) is used to host KVS Enterprise Vault archives in the solution presented within this paper. HP ProLiant Storage Server solutions are based on the industry's number one business platform—HP ProLiant servers. The same

industry-leading server technology used in HP ProLiant application servers (Integrated Lights-Out management, HP Insight Manager management, and HP ProLiant Essentials software) is available on equivalent HP ProLiant Storage Server products.

As a member of the HP StorageWorks family of products, HP ProLiant Storage Servers benefit from the reliability, scalability, performance, cost of ownership, investment protection, and peace of mind benefits inherent to HP storage. Available storage technologies include low-cost Serial ATA (SATA) disks, which are ideal for many archiving scenarios.

Because HP ProLiant Storage Servers are built on Windows Storage Server 2003, customers benefit from the dependability, seamless integration, and the best value in networked storage. Windows Storage Server 2003 includes advanced availability features such as point-in-time data copies, replication, and server clustering. This HP/Microsoft storage solution is ideal for organizations wanting to consolidate data such as Enterprise Vault archives into a single solution that enables cost reduction and policy-based management of storage resources.

Because HP ProLiant Storage Servers are preconfigured, they can be deployed out-of-the-box in minutes and require little expertise to set up. In addition, the Web-based user interface makes management easy. Preconfigured HP ProLiant Storage Servers are available in both tower and rack mount form factors. Available storage capacities range in size from a few hundred gigabytes to multiple terabytes.

This solution blueprint is designed to provide information regarding messaging data retention, clarify how HP, Microsoft, and KVS can enable businesses to move in the right direction today, and enable you to implement a solution that meets your organization's needs for data retention. You do not have to build a solution from the ground up—HP provides network attached storage in its HP ProLiant Storage Servers, Microsoft provides basic journaling and archiving capabilities within Exchange, and KVS provides out-of-the-box solutions that can enhance the message journaling and retrieval capabilities of Exchange.

This paper discusses the use of message archival systems to provide a greater understanding of which protection strategies and solutions are reasonable and appropriate to ensure that data is appropriately stored and maintained. Unless otherwise noted, this solution blueprint assumes that Microsoft Windows Server 2003 with the Microsoft Active Directory directory service and Exchange Server 2003 have been deployed in your organization.

The importance of data

Today's information workers utilize their Exchange servers all day, every day—Outlook 2003 is the first application users open upon arriving in the office, and it is the last thing they check before going home at night—and more often, users check and respond to e-mail off-business hours using Outlook Web Access, Remote Procedure Call (RPC) over HTTP(S), or a virtual private network (VPN) connection. Exchange Server has become a critical application in the quest for productive, efficient businesses. Today, contracts are negotiated using e-mail, and documents are attached to messages for review; paper memos are becoming obsolete as the use of electronic communications gains popularity. Business no longer relies on filing cabinets or index cards to locate information; computers are used to produce and store vast amounts of information. To properly utilize this data, efficient ways to search for documents and data must exist.

Exchange Server 2003, the latest version of the Exchange messaging and e-mail-based collaboration server, is specifically designed to help address business requirements for heightened security in today's computing environments. In accordance with the Microsoft Trustworthy Computing Initiative, Exchange 2003 running on Windows Server 2003 provides many new features and enhancements to improve reliability, manageability, and security.

SharePoint Portal Server 2003 provides an enterprise portal and document management system by enabling users to store, access, and search for information. Properly managing this data is imperative—corporate knowledge is an invaluable asset and must be adequately protected and retained, not only for compliance purposes, but also to retain the business value of past efforts.

The ability of SharePoint Portal Server to manage the entire document chain—authoring, versioning, and publishing—enables businesses to easily implement an out-of-the-box solution for workflow processes. The integration of KVS Enterprise Vault with SharePoint Portal Server enables organizations to manage the life cycle of documents based on the retention policy and regulatory requirements of the business.

The inherent flexibility of SharePoint Portal Server enables businesses to create separate sites for compliance-related documents and official communications such as memoranda. The data within these sites can then be archived through the use of KVS Enterprise Vault and searched and retrieved using KVS Discovery Accelerator.

HP ProLiant servers and HP StorageWorks storage provide the hardware infrastructure to build a complete solution. These industry-leading systems are the components of choice for Microsoft Exchange deployments. Their reliability, scalability, performance, and manageability combine to provide the ideal deployment platform for this solution.

All of these hardware, communication, and messaging options, combined with the heightened emphasis on tracking and auditing business records and correspondence, means that it is vital for businesses to be able to track and find data relating to their internal operations and their internal and external interactions and communications. The challenge is finding and implementing a system that efficiently manages this data, stores the data in its original format, and allows the data to be discovered.

Data retention policies

HP recommends that each business create a team from various divisions of the company (including representatives from your legal, financial, and information technology departments) to make recommendations about how the business will meet compliance-related regulations. This team should be tasked with creating policies for data retention within the organization, determining what data should be considered official business communications and records, developing a written policy for related data retention, and providing education to the information worker community on how to follow these policies.

A good electronic messaging policy defines acceptable use of the system, including whether it is permissible for users of the system to send and receive personal e-mail, whether solicitations using e-mail are allowed, disallowing the use of e-mail for harassing or threatening messages, and prohibiting the transmission of potentially offensive images using the messaging system. The policy should state that users cannot send company-confidential data to third parties except in cases in which the third party is receiving this data for a legitimate reason, and that illegal use of the system will not be tolerated. Retention periods for communications should be clearly defined; businesses that are subject to the specific regulations defining retention periods should ensure that these requirements are clearly stated in their policies.

When creating an electronic messaging policy, ensure that the correct stakeholders from your organization are involved and that the policy is not created in a vacuum. Your legal department, financial advisors, and system managers must coordinate their efforts to create a policy that is legally correct, adequately protects the interests of your organization, and can be implemented and enforced. The risks and realities of your organization's structure must be considered, and the implementation of the policy should be clearly structured.

The SANS Institute, a cooperative research and education organization, provides a sample policy for e-mail retention that is available for viewing at http://www.sans.org/resources/policies/e-mail_retention.pdf and can help you begin the process of creating a policy for your organization.

Current regulatory environment

Understanding regulatory requirements

Numerous federal regulations impact diverse organizations. While the financial industry has long been subject to oversight by the Securities and Exchange Commission (SEC) and 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 must now become actively involved in this process. The enactment of more broad-reaching regulations, such as Gramm-Leach-Bliley Act (GLBA) and SOX, has created the need for businesses in other industries to focus on how they safeguard, disseminate, store, and track financial information. Many states have enacted regulations that supersede these federal regulations; ensure that you are complying with the pertinent laws for your state, in addition to applicable federal regulations.

Note
The regulations named within this document are specific to the United States of America. Many other countries have similar legislation in place; ensure that you understand the requirements of regulations in areas where your business operates.

Regulations impacting electronic messaging

Many regulations impact 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. The following regulations are pertinent to many organizations and present a good overview of the overall regulatory environment today. However, you should rely on your legal counsel for applicability and analysis:

Sarbanes-Oxley Act

- Requires that executives of publicly traded companies certify the validity of company financial statements
- Requires that financial control and risk mitigation processes be documented and verified by independent auditors
- Requires companies to implement extensive policies, procedures, and tools to prevent fraudulent activities

SEC Rule 17A-4

- Requires that original copies of all communications, such as inter-office memoranda and communications, be preserved for a period of no less than three years, the first two in an easily accessible location
- Requires that records that must be maintained and preserved be available to be produced or reproduced using either "micrographic media" (such as microfilm or microfiche) or "electronic storage media" (any digital storage medium or system)

Gramm-Leach-Bliley Act (Financial Institution Privacy Protection Act of 2001, Financial Institution Privacy Protection Act of 2003)

- Amended in 2003 to enhance the protection of nonpublic personal information
- Requires that financial records be properly secured and safeguarded, and eventually disposed of, in a manner that will destroy the information completely so it cannot be further accessed

Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA)

- Requires the adoption of security standards that control who may access health information, provide audit trails for computerized record systems, and meet the needs and capabilities of small and rural health care providers
- Requires that health data be isolated and inaccessible to unauthorized access
- Requires that the transmission of health information is physically, electronically, and administratively safeguarded to ensure the confidentiality of data

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)

- Requires that financial institutions implement reasonable procedures to maintain records of information used to verify the identity of a person opening an account
- Provides law enforcement organizations broad investigatory rights

Department of Defense Rule 5015.2-STD

- Requires systematic management of records, including how records are classified, created, deleted, maintained, reproduced, and used

National Archives and Records Administration

- Oversees official government recordkeeping
- Requires adequate and proper documentation with regard to how the business of the U.S. government is conducted, including the policies and procedures of government agencies
- Defines records as "…machine-readable materials…made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business…"
- Requires that electronic records that relate to a particular subject or function be organized within a record series that facilitates the management of these records

CFR Title 47, Part 42—Telecommunications

- Requires that telecommunications carriers keep original records or reproductions of original records, including memoranda, documents, papers, and correspondence that was prepared either by the carrier itself or on behalf of the carrier

CFR Title 21, Part 11—Pharmaceuticals

- Requires that controls be in place to protect content stored on both open and closed systems to ensure the authenticity and integrity of electronic records
- Requires the ability to "generate accurate and complete copies of records…in electronic form" so that the Food and Drug Administration can inspect such records

Retaining messaging data

While many regulations require a specific retention period for business-specific data, not all businesses fall under these requirements. Financial services organizations typically have the most stringent data retention requirements. Businesses that are not subject to specific data retention requirements should document their data retention policies and follow these policies. There have been

several cases in which organizations with clearly defined data retention policies had not followed their policies and were therefore required to spend innumerable hours restoring and retrieving data from backup media.

As discussed previously in this solution blueprint, a well thought out data management plan is essential. Your data retention plans should mesh well with your actual data management processes. If your plan states that e-mail is kept for a year, your 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 Server document repository) will ensure that you can easily recover such data in the event you are required to do so in legal discovery processes. The ability to preview such documentation, should it be necessary, is helpful when approaching any legal proceeding.

Numerous components meld to create the need for a regulatory compliance solution. Determining whether an organization must implement such a solution requires cooperation between many divisions of the organization. Understanding the drivers for the implementation of document life cycle management tools such as KVS Enterprise Vault and Discovery Accelerator ensures that the solution will have the proper support within your organization.

The three primary components of a regulatory compliance solution are data archiving, data retention, and discovery of data. These components complement one another, and all organizations that must meet regulatory compliance rules should consider each of these points before implementing a solution.

Message archiving and retention

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

What data?

Data that pertains to legal, financial, and business decisions should be archived according to the data retention policy of your organization. E-mail messages relating to lunch dates, personal conversations, and the minutiae of running a business (such as an e-mail message to an administrative assistant regarding the purchase of office supplies) probably does not need to be maintained.

Accurate data archiving, with an audit trail, is necessary to 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 must also be retrievable.

For the purposes of this solution blueprint, data archived will primarily be messaging data. When envelope message journaling is enabled, all messages from, to, and within your Exchange organization will be sent to a central journaling mailbox. The data sent to the journaling mailbox will then be queued for delivery to the Enterprise Vault server.

How long?

Businesses that are bound by the SEC should retain data for a period of no less than seven years. During the first two years of retention, the data must be easily accessible. Other types of industries can have specific regulations that pertain to their recordkeeping; ensure that you understand these regulations and their requirements. Companies whose industries are not bound by specific legislation or rulings should define a specific data retention period and enact technical measures to comply with this decision.

As discussed earlier, data retention policies must be in place before beginning any compliance efforts. It is important that all stakeholders within your organization are involved in creating this policy; IT cannot create a policy without input from other departments.

Who can access the data?

It might be necessary to allow specific trusted individuals access to stored data to track communications and ensure that users are complying with pertinent regulations. Access to data should be controlled and audited to ensure that this function is not abused.

KVS Discovery Accelerator enables roles to be assigned to users to 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 structure to control which users may access data and how data is reviewed.

Who should manage the data?

Few businesses employ corporate librarians to manage their company data. Even when this role exists within a company, it is often under-funded, under-recognized, and under-supported. Organizations that do not have a corporate librarian need tools that can support this function. HP, Microsoft, and KVS are teaming to help you fill this role. Businesses that do have corporate librarians can also benefit by implementing this solution because Enterprise Vault provides a single point of reference for data that originated from many sources.

When documents from numerous sources (such as Exchange databases, file servers, and SharePoint Portal Server sites) are merged into a single Enterprise Vault system, the Enterprise Vault becomes the authoritative source for information gathering. Knowledge management teams can utilize this data repository not only for discovery purposes, but also to gain a better 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. Ensure that your data is respected for the important business asset it is and that your knowledge management team consists of people who understand the vital nature of your company data.

Discovery Accelerator provides roles for data management and retrieval. These roles include the:

- System Administrator, who creates new cases (a case is a discovery process), configures the marking scheme so messages can be accurately labeled once discovered, and creates user roles
- Case Administrator, who manages a case itself and assigns items to reviewers and can configure new marking schemes
- Reviewer, who delves into the data and marks it as appropriate for further action

Where should the data be stored?

A centralized data repository makes any discovery processes more efficient and reliable than widely disparate storage systems, and centralized archiving is the least expensive way to house an archive because it provides the best 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 because its caching provides reliable access to the data over long distances and variable electronic link speeds. All business-related data should be kept on servers, and messaging data should be retained either on the Exchange Server or within an archiving system, as detailed later in this solution blueprint. Your users should never store messaging data in Personal Folders (PSTs), because .PST files are not centrally controlled and present an unreliable long-term archival system.

Note

The use of .PST files on network shares is not supported. Refer to Microsoft Knowledge Base Article 297019 (http://support.microsoft.com/default.aspx?scid=kb;en-us;297019) for further information.

This solution makes use of an HP ProLiant Storage Server using on Windows Storage Server 2003 to host the Enterprise Vault data archive. The HP ProLiant Storage Server was chosen because of the

industry-leading HP ProLiant technology it is based on, which is reliable, scalable, simple to deploy, controllable using a Web interface and enables organizations to quickly add storage to their network without the need for intense training. A single HP ProLiant Storage Server can host tens of terabytes of data and provide dependable storage for your organization's data.

Data retention benefits

Many organizations that will implement the solution presented in this paper are doing so to address their regulatory compliance needs; however, there are other advantages of implementing this solution:

- Archived data provides a searchable corporate knowledge base. Data can be readily searched for and retrieved through the use of KVS Discovery Accelerator.
- Global marking of data within Discovery Accelerator ensures that data that has been through a discovery process once does not need to be re-discovered and re-reviewed and marked. This reduction in the duplication of effort is 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 availability enables new workers to understand the history behind the business decisions that were made in the past.
- Archived data provides improved business continuity. The documentation and communications that are essential to the long-term success of your business are available in a single repository that can easily be searched and from which data can be quickly retrieved.
- Archived data provides increased productivity for users. Because of mailbox size limits, users must often resort to storing e-mail messages in PSTs, leading to the need to search multiple sources for an important message or document. Enterprise Vault eliminates the need for PSTs and enables users to quickly retrieve data using simple searches when the client tools are installed on each workstation or the Web retrieval tool has been made available.
- The ability to verify communications mitigates risk; document life cycle management enables businesses to oversee data intelligently.

Message journaling considerations

Standard message journaling

Message journaling creates and saves a copy of all e-mail messages sent and received within an Exchange information store. Journaling can be enabled either globally within an information store or only for specific mailboxes within the information store. Details on configuration steps to enable message journaling are provided later within this solution blueprint.

When message journaling is enabled, all messages sent within that information store, and to and from mailboxes residing on that information store (or for the mailboxes specified), are retained in a specified mailbox. Large organizations, or organizations that send and receive large amounts of e-mail traffic, should dedicate significant resources to support the server hosting mailbox that will receive this data.

Access to the repository that is chosen for the message journaling should be carefully controlled. The mailbox is used for the repository; it should also be hidden from the Global Address Book, and permissions to the mailbox should be carefully controlled.

Exchange envelope journaling capabilities

Service Pack 1 for Microsoft Exchange Server 2003 introduces the envelope journaling tool (exejcfg.exe). Standard message-only journaling delivers a copy of a message flagged for archiving

to a designated journal mailbox. Envelope journaling instead delivers archival messages using an envelope message containing a journal report with the original message as an attachment.

E-mail messages are composed of numerous attributes. The actual message envelope, known commonly as P1 data, includes the actual recipient information that was used to route and deliver the message. This information includes the message headers, including the message originator's e-mail address, one or more recipient e-mail addresses, and, optionally, the protocol extension material. The message contents, known as the P2 data, include the body of the message and any other contents to be delivered to the recipient, such as the subject line of the message.

Note
The recipient data that is visible within e-mail clients is defined in the P2 portion of the message. Blind carbon copy (BCC) data is contained within the P2 data of a message and is not visible to the message recipient. Refer to RFC 2821 (http://www.ietf.org/rfc/rfc2821.txt) for more information on P1 data, and RFC 2922 (http://www.ietf.org/rfc/rfc2822.txt) for more information on P2 data.

The body of the journal report provides the presentation for the relevant transport envelope data associated with the attached archived message. Envelope journaling ensures that all message data is recorded by enabling the contents of the message itself to be journaled and capturing all recipient information, including:

- All recipients of the message from the RCPT TO portion of the Simple Mail Transfer Protocol (SMTP) transaction
- The sender identification from the MAIL FROM portion of the SMTP transaction
- Expanded distribution list membership
- Recipients from transport forwarding rules
- The date and time the message was sent and received
- Protocol extension material

Envelope journaling ensures that all recipients of a message that were on the BCC line of the message, recipients from transport forwarding rules, and recipients that are a part of a distribution list are not reliably documented when standard message journaling is used.

Note
Microsoft Knowledge Base article 810999 (http://support.microsoft.com/default.aspx?kbid=810999) explains how to obtain the hot fix to enable Envelope Journaling in Exchange 2000.

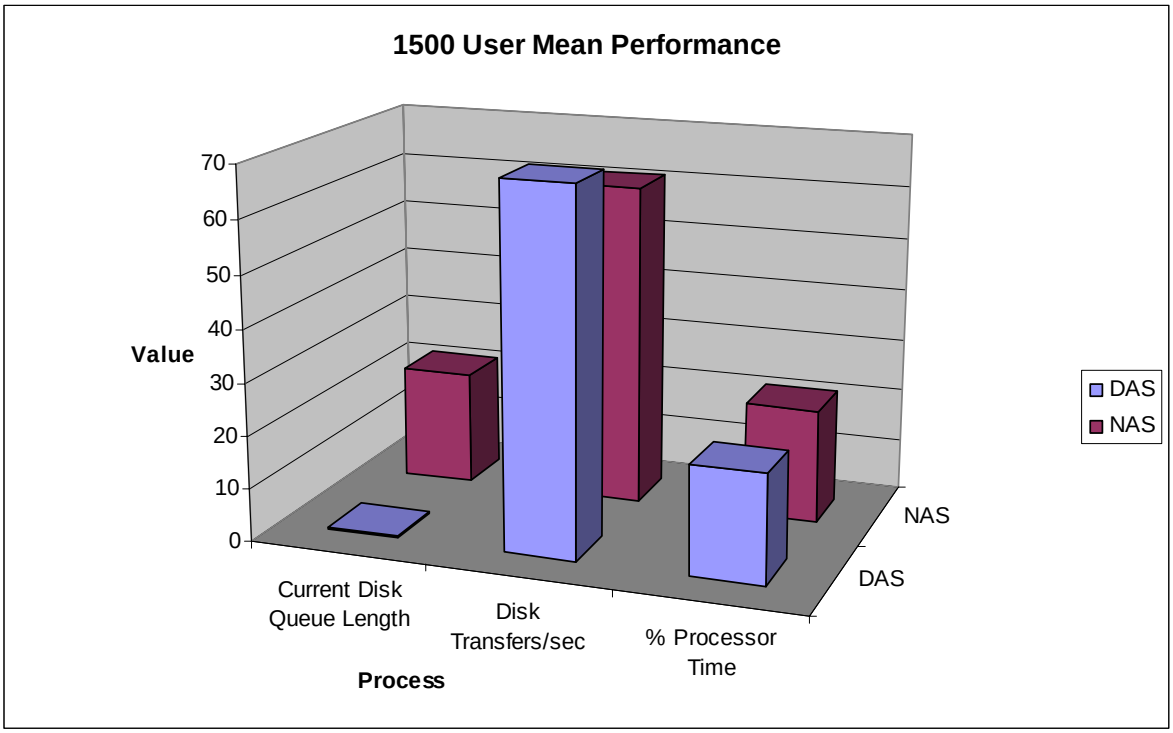
Envelope journaling is enabled on a per-information store basis. When this functionality is enabled, all messages sent within that information store, and to and from mailboxes residing on that information store, are retained in either a mailbox or Public Folder of your specification. Large organizations, or organizations that send and receive large amounts of e-mail traffic, should dedicate significant resources to support the server hosting the mailbox that will receive this data. Access to the mailbox that is chosen to host the message journaling archive should be carefully controlled, and the mailbox should also be hidden from view in the Global Address Book.

Message journaling and performance

Before enabling message journaling on an Exchange server, consider the performance impact of this operation. Message journaling increases the load on an Exchange server, and careful planning will enable you to continue to meet current service levels after enabling message journaling. A simplified estimate for large organizations is that you will need approximately three times your original resources to maintain your Exchange servers at their current level of use. Smaller organizations will see less impact within their environments but also must plan to make additional resources available to ensure service levels are not adversely impacted by enabling message journaling on their Exchange servers.

The solution presented within this document is aimed at small to medium enterprises (SME) with typically fewer than 3,000 users. An HP ProLiant Storage Server built on Windows Storage Server 2003 is used to host the KVS Enterprise Vault archive. The HP ProLiant Storage Server solution provides a flexible, solid foundation for file sharing and storage and is proven to be a stable, highly responsive platform for the Enterprise Vault archive. Response times within close range were recorded between HP ProLiant Storage Server and direct attached storage (DAS) when performance testing simulated 1,500 Exchange mailboxes being journaled to Enterprise Vault. The sole difference between the storage solutions was the placement of the drives, which were swapped between a DAS array and the HP ProLiant Storage Server disk array (HP SmartArray technology made this direct DAS to network attached storage [NAS] migration possible). The Exchange 2003 MAPI Messaging Benchmark (MMB3) (http://www.microsoft.com/exchange/evaluation/performance/mmb3.asp) was used with LoadSim to gather the performance data. Performance results for the 1,500-user testing are shown in Figure 1.

Figure 1. 1,500-user mean performance



Exchange Server 2003 message journaling planning

Organizations with heavy messaging loads intending to implement message journaling should plan to install an additional Exchange server that will host the journaling mailbox to support:

- A storage group with a single information store that hosts the target mailbox for message journaling.
- Almost two times the normal hardware-related resources, such as disk I/O, RAM, and CPU cycles.
- One journal mailbox server for every two to three mailbox servers (this server is not intended to support Messaging Application Programming Interface (MAPI) traffic, such as that generated by Outlook clients).
- Sufficient disk space for the information store dedicated to message journaling. The journaling mailbox on the information store will be receiving duplicate copies of all e-mail messages sent and received on all journaling-enabled information stores within your organization (the data within the journaling mailbox is transitory because it is deleted from the journaling mailbox when it is moved into the Enterprise Vault). Each message is saved in both its original format (.MSG) and either in HTML or text so it can be viewed using the Web browser.
- A dedicated RAID 1+0 (mirroring and striping) volume to host the information store for the best performance.
- Sufficient disk space for the transaction logs. When messages are journaled, transaction logs are created and can quickly accrue in high-volume situations like message journaling. Expect high levels of transaction logs because each message that transits the journaling mailbox will also be deleted from the mailbox when it is moved into the Enterprise Vault. The transaction logs will roughly double what would be expected if all data was to be retained in the mailbox.
- A dedicated RAID 1 (mirroring) volume configured to host the transaction logs for optimal performance.

Because you must ensure that sufficient resources are available, testing within your organization will be necessary to determine the exact amount of resources that will be needed to smoothly add message journaling into your environment. The following statistics should be included when gathering baseline performance data within your environment to determine your needs:

- The average number of recipients per message. If most messages are sent to large distribution lists within your environment, your resource needs might be reduced.
- The level of MAPI access to information stores. The performance counters available under the MSExchangeIS Mailbox and MSExchangeIS Public objects can be logged and analyzed.
- The number of messages handled (sent, received, and submitted) per minute on your current Exchange mailbox server.
- The resources in use on your current Exchange server, including the processor (% Processor Time), logical disk (Disk Transfers/sec, Current Disk Queue Length), and memory (Available Mbytes).

Enabling envelope journaling requires additional resources on Global Catalog servers because envelope journaling records the expanded membership of distribution groups. The benefits of enabling envelope journaling outweigh any perceived performance concerns; without enabling envelope journaling, all necessary data might not be captured and regulatory compliance might be questionable. If large universal distribution groups are heavily used within your organization, you might determine you must add an additional Global Catalog server to your network or dedicate a single Global Catalog server to handle distribution list expansion. (You designate an expansion server by using the Exchange Advanced tab within the properties page of each distribution group.)

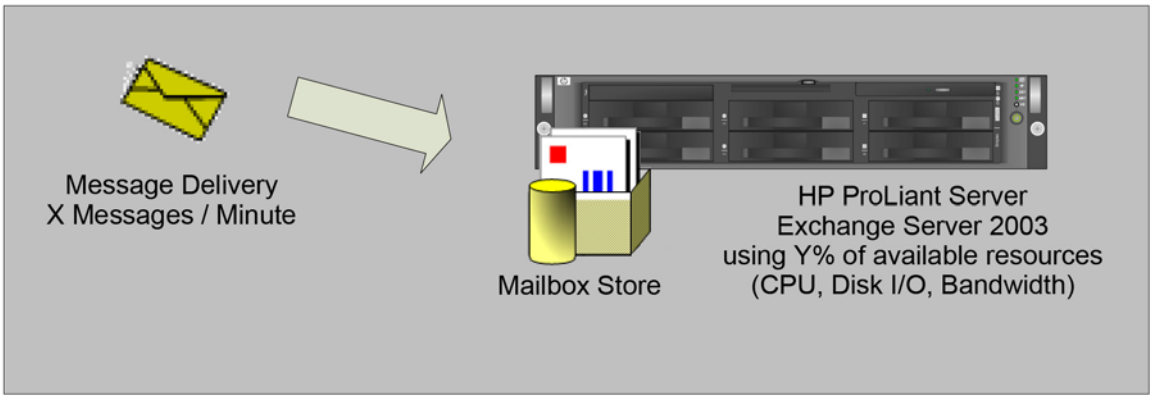
Note
Exchange Server 2003 relies on the DSAccess process to determine which domain controller and which Global Catalog server will be used when directory information must be retrieved. If you want to statically assign a Global Catalog server to provide directory services to Exchange, follow the instructions in Microsoft Knowledge Base article 250570 (http://support.microsoft.com/default.aspx?scid=kb;en-us;250570&sd=tech).

Analyzing data

After you have gathered performance data from your Exchange 2003 server, analyze the data to ensure that adequate resources will be available when you enable envelope journaling. This example assumes that without envelope journaling, your mailbox server deal with X messages per minute with Y% of the resources (CPU, disk I/O bandwidth) used. The goal is to enable envelope journaling and have the same use of resources on each server.

Before enabling journaling, each mailbox is dealing with X inbound messages per minute, with load Y%, graphically represented in Figure 2.

Figure 2. Standard Exchange 2003 message traffic

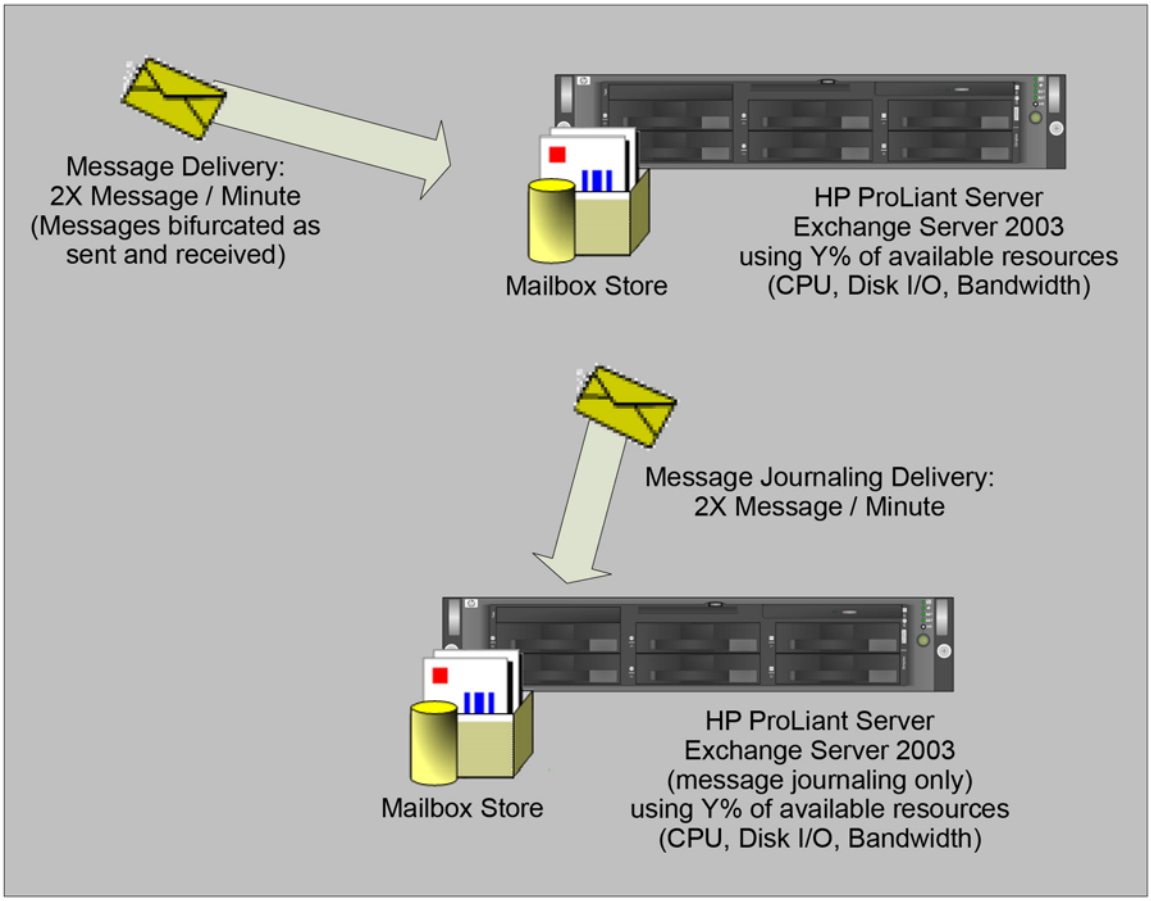


After enabling envelope journaling:

- Each mailbox server deals with twice as many messages per minute because the messages are bifurcated.
- You will generally need between one and a half and two mailbox servers for each original mailbox server because of the additional load of envelope journaling. This requirement might necessitate deploying an additional Exchange server within your environment if your current server is low on available system resources. (If the total load on all mailbox servers is low, such as with 10 to 30% of resources in use, adding a single journaling mailbox server might be sufficient.)
- A dedicated journaling mailbox server will need to be deployed to support each two to three mailbox servers.

The impact of enabling envelope journaling on Exchange Server 2003 and the additional actions performed within the information stores when envelope journaling is enabled is shown in Figure 3.

Figure 3. Exchange Server 2003 message traffic with envelope journaling



KVS Enterprise Vault integration and features

When KVS Enterprise Vault is deployed, messages will be sent from the journaling mailbox to the Enterprise Vault for long-term archival. The journaling mailbox will be used for data in transit between Exchange mailbox servers and the Enterprise Vault. Messages within the journal mailbox are deleted as they are moved into the Enterprise Vault. Because Enterprise Vault will serve as the long-term repository for all archives, the hardware used to host the vault data should be sufficiently robust to support this use. An HP ProLiant Storage Server using Windows Storage Server 2003 provides a solid platform to store the Enterprise Vault archive and has proven capable of handling high levels of usage through performance testing. It is included in this solution blueprint as the recommended platform to host the archive.

Enterprise Vault stores archive messages as individual compressed files. All items are indexed, compressed, and de-duplicated as they are stored, and the structure and location of this archive can change as the archive ages. This functionality enables Enterprise Vault to integrate with information life cycle management scenarios. De-duplication of messages occurs when the Share Archived Copies option is selected on the Enterprise Vault partition. An Enterprise Vault partition is created to host the archived messages, and Microsoft SQL Server 2000 is used to host the associated configuration and metadata, which enables retrieval of items within the vault. The Enterprise Vault Open Storage Layer allows archived information to be stored, using the technology most appropriate for the age of the item. Single items can be concatenated into more efficient collections, and these collections can be

automatically migrated to other storage systems—all invisibly to the end user. The Open Storage Layer also gives organizations the flexibility to adopt new storage technologies as they are introduced, thereby protecting the archive over time.

The Enterprise Vault server uses Microsoft published application programming interfaces (APIs) (mostly MAPI) to integrate with Exchange. The Outlook client can be extended to include an add-in that communicates directly to the Enterprise Vault sever (or its own offline cache if the Outlook client is in cached mode). Extensions are added to the servers hosting Outlook Web Access (OWA) to ensure seamless access to the messages in the vault.

Note
The solution presented within this document does not require the implementation of Enterprise Vault client extensions because the messages must be managed with the KVS Discovery or Compliance Accelerator add-ons to meet regulatory requirements.

The configuration and metadata of Enterprise Vault are stored on SQL Server 2000, which provides a solid foundation for retrieval of data within the Enterprise Vault archive. Indexing of the contents of Enterprise Vault is managed by AltaVista Search. The storage location and optimal size of the index are configurable—to control the size of the index files, Enterprise Vault allows for brief, medium, or full indexing. Brief indexing allows for simple key word searches, and full indexing allows for more complex searches (approximately 12% of the archive size). Archives can be re-indexed at any time to change the index level search, but HP recommends that brief indexing be initially configured.

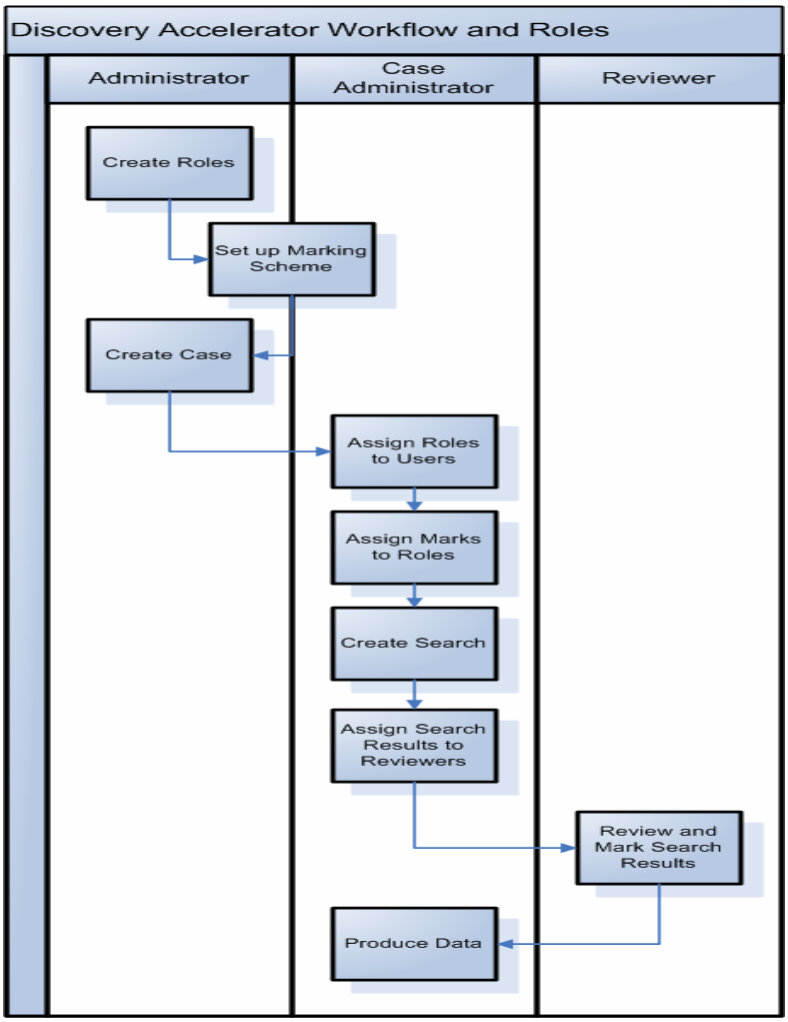
KVS Enterprise Vault Discovery Accelerator integration and features

KVS Enterprise Vault Discovery Accelerator is a flexible, customizable Web-based tool that enables organizations to automate the search and discovery of data within Enterprise Vault in an optimal manner. The content archived within Enterprise Vault can be effectively managed using Discovery Accelerator to ensure cost-effective, accurate findings when you must locate data within Enterprise Vault. Access to the data within Enterprise Vault is customizable and should be limited to designated reviewers. With Enterprise Vault and Discovery Accelerator, there is no need for support from your company's IT team—the days of restoring numerous backup tapes to disk are gone. The data archive within Enterprise Vault is easily accessible to authorized users without IT interaction.

Discovery Accelerator enables the tracking, marking, and review of data within the Enterprise Vault for litigation support, legal discovery, and investigation. Content within the Enterprise Vault is easily tracked and reviewed and can be marked for further action by authorized reviewers within your organization. Global marking schemes within Discovery Accelerator help organizations avoid duplicating review efforts and make discovery processes more efficient.

When the need to perform discovery processes presents itself, you must be able to quickly find the data, review and organize it, and present it to the appropriate party. Discovery Accelerator enables this process to flow smoothly and provides controls so that the data is used appropriately. Figure 4 displays the interaction of roles within Discovery Accelerator and shows the process flow of discovery, along with the attendant roles and responsibilities.

Figure 4. Discovery Accelerator workflow and roles



Implementing the solution

This solution has been created to enable organizations with 3,000 or fewer users to quickly implement a solid platform for their document life cycle needs and support their compliance requirements. HP, Microsoft, and KVS together provide solid solutions for data archiving and share the common goal of enabling businesses to implement this solution with minimal planning on the businesses' part.

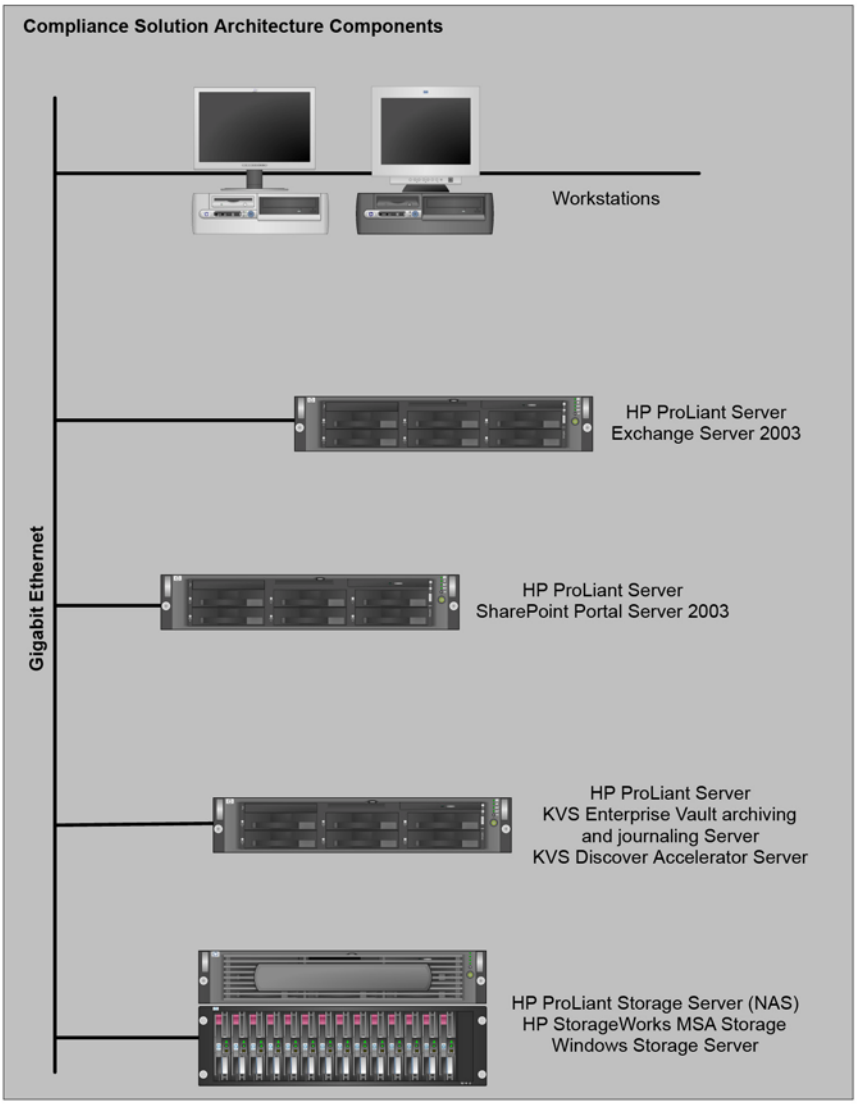
Testing in a Microsoft lab proved that the solution architecture and implementation provided herein provides a good fit for the SME environment and that HP ProLiant Storage Server will serve well as the end-point for the Enterprise Vault archives. Microsoft Exchange Server 2003 and SharePoint Portal Server 2003 are well-integrated with KVS Enterprise Vault, and the architecture coexists well without numerous custom configuration steps.

Solution architecture components

HP ProLiant servers, Exchange Server 2003, SharePoint Portal Server 2003, HP ProLiant Storage Server built on Windows Storage Server 2003, KVS Enterprise Vault, and KVS Discovery Accelerator combine to provide a solution for your document life cycle needs. This document assumes that both Exchange Server 2003 and SharePoint Portal Server 2003 are deployed in the production environment and that SQL Server 2000 is implemented and can support Enterprise Vault. During the installation process, if you have any questions, contact KVS at sales@kvsinc.com for advice or visit their website at http://www.kvsinc.com.

The solution architecture, when fully implemented, is shown in Figure 5.

Figure 5. Solution architecture components



HP ProLiant server and HP StorageWorks components

The results reported from this white paper were achieved using the following HP components.

- HP ProLiant DL380—Exchange server
- HP ProLiant DL380—KVS server
- HP ProLiant DL380 Storage Server (NAS)—KVS Enterprise Vault Storage
- HP StorageWorks MSA 30 (10 x 146GB/10K HDDs)

No matter the size of your business, HP has a solution that will meet your needs now and grow with you into the future as your business grows. Your HP reseller and the HP website have many tools to help you choose the exact combination of HP servers and storage to meet your particular needs. For more information, visit http://h71019.www7.hp.com/enterprise/cache/3844-0-0-0-121.aspx.

Discovery Accelerator

Discovery Accelerator will be installed on Windows Server 2003, the same server that will run Enterprise Vault. You may install Discovery Accelerator on a separate server—if you opt to do so, you must first install Enterprise Vault on the server, following the instructions for Enterprise Vault provided herein. You need not perform the configuration steps for Enterprise Vault on a dedicated Discovery Accelerator server.

Discovery Accelerator is comprised of three components:

- EVDiscovery database, which hosts data such as configuration details, cases that have been created, users and their associated roles, marking scheme templates, searches, and search results
- Discovery Service, which provides control and management for Discovery Accelerator
- EVDiscovery Web Application, which provides a management interface to control roles and process flow within Discovery Accelerator

Enterprise Vault

Enterprise Vault 5 CP1 must be installed on Windows Server 2003 to support the archive for Exchange and SharePoint data. The Enterprise Vault data will be stored on an HP ProLiant Storage Server. Every message being sent to, from, or within your organization's Exchange environment will be journaled into the Enterprise Vault. Generally, Enterprise Vault can compress all items down to 50% of their original size (some file formats, such as .ZIP, .JPG, and .GIF, are already compressed and cannot be further compressed). Additional overhead is necessary for storage because each item also contains control information that averages 5 KB per item.

Exchange Server 2003

Exchange Server 2003 will be configured to support mailbox journaling. If the current mailbox server is running Exchange Server 2003, Enterprise Edition and has sufficient memory, disk volumes, and processing power to support an additional mailbox store for hosting the journaling mailbox, you can create an additional storage group to host a single database that will support the journaling mailbox.

For every 12,500 items journaled per hour within Exchange Server 2003, the load on the Exchange server itself will increase approximately 10%. If your current Exchange server is heavily used or is running Exchange Server 2003, Standard Edition, deploy an additional server to host the journaling mailbox.

SharePoint Portal Server 2003

The data in SharePoint Portal Server 2003 can easily be archived into Enterprise Vault—there is no need to change your current SharePoint Portal Server configuration. Your current storage point for SharePoint Portal Server will not alter as a result of this solution; however, any data archived into Enterprise Vault will be stored on an HP ProLiant Storage Server.

SQL Server 2000

SQL Server 2000 supports configuration data and metadata for Enterprise Vault and enables Discovery Accelerator to quickly find and retrieve data. One SQL server is necessary to support four Enterprise Vault servers of equivalent size. The SQL server supporting Enterprise Vault will require a minimum of 1 GB of memory—if additional Enterprise Vault servers are added, additional memory might be necessary. If you will be using a currently deployed SQL server to support Enterprise Vault, ensure adequate system resources are available to support Enterprise Vault. SQL Server is designed to claim all available memory so that the memory is available should the services need it.

SQL Server needs approximately 250 bytes of disk space per journaled item. An additional 3 GB of space should be available for static and temporary tables. Regular online maintenance of the SQL database will reduce the size of the entries associated with the journaled items to 169 bytes.

HP ProLiant Storage Server

An HP ProLiant Storage Server using Windows Storage Server 2003 will be used to host the data being managed by Enterprise Vault. Data storage needs for Enterprise Vault can be determined by using the following formula:

((Number of items) * (Average item size) * 0.5) / (Average single instance storage ratio) + ((Number of items) / (Average single instance storage ratio)) * 7 + (Number of items) * 2

For example: suppose you have 500 items, with an average item size of 10 Kb and an average single instance storage ratio of 2.2. The data storage needs would be:

((500) * (10 Kb) * 0.5) / (2.2) + ((500) / (2.2)) * 7 + (500) * 2 = 3727.28 Kb

Single instance storage on Exchange servers is similar to the de-duplication of messages within Enterprise Vault, and your current single instance storage ratio is a good indicator as to how messages will be shared within Enterprise Vault. The single instance storage ratio can be determined by using performance monitor, selecting an information store as the performance object, and selecting single instance storage ratio from the counter list.

Determining the average number of items that are sent and received by your organization and the average size of these items is trickier. One way to determine these figures is by careful analysis of message tracking logs; another is to enable message journaling for a few days to gather a baseline as to how much data is being collected.

Creating your own solution

Introduction

This implementation, using an HP ProLiant Storage Server, is configured to easily support the integration of KVS Enterprise Vault and Discovery Accelerator into an existing network architecture containing Windows Server 2003, Exchange Server 2003, SharePoint Portal Server 2003 (optional), and SQL Server 2000.

Before beginning the installation process, ensure that you have the KVS 5.0 software, KVS CP1, and have a license key from KVS.

Installation summary

This solution blueprint will guide you through the installation process to help meet regulatory requirements. The installation process should follow the steps listed in this section. If the process is not followed in the correct order, the solution might not perform correctly. The configuration process includes:

1. Windows Server 2003 configuration
2. Windows Server 2003 domain controller configuration (creating a service account in Active Directory to support Enterprise Vault services and access)

Note
It is assumed that the Domain Naming Service (DNS) is Active Directory integrated and that servers are automatically updating their records in DNS correctly.

3. Exchange Server 2003 configuration
4. HP ProLiant Storage Server configuration
5. SQL Server 2000 configuration

Note
The SQL client tools should be installed on the Enterprise Vault servers and on any server or workstation that will run the Enterprise Vault Administration Console.

6. Enterprise Vault application installation and configuration
7. Discovery Accelerator installation and configuration

Windows Server 2003 configuration for Enterprise Vault, part 1

Enterprise Vault must run on a Windows Server 2003 installation. Configure Windows Server 2003 to use the NT file system (NTFS) format for the file system during the installation. Internet Explorer 6.0 is installed on Windows Server 2003 computers by default; ensure that Internet Explorer is working correctly before installing the Enterprise Vault application.

The Windows Server 2003 Message Queuing Service, the ASP.NET Service, and the NNTP component of Microsoft Internet Information Services (IIS) must be installed. Have the Windows Server 2003 installation disk available during these configuration steps. When installing these components, ensure you are logged onto the domain with administrator rights.

Installing the Message Queuing Service and the ASP.NET Service

1. Click **Start** and select **Control Panel.**
2. Double-click **Add or Remove Programs.**
3. Click **Add/Remove Windows Components.**
4. Select **Application Server,** and click **Details.**
5. Select the **Message Queuing** and the **ASP.NET** checkboxes.
6. Click **OK.**
7. Click **Next.**
8. Click **Finish.**

Installing the IIS components

1. Click **Start** and select **Control Panel.**
2. Double-click **Add or Remove Programs.**
3. Click **Add/Remove Windows Components.**
4. Select **Application Server,** and click **Details.**
5. Select **Internet Information Services (IIS),** and click **Details.**
6. Select the **NNTP Service** checkbox (you might need the original Windows Server 2003 installation CD to install the NNTP service).
7. Select **World Wide Web Service,** and click **Details.**
8. Select the **Active Server Pages subcomponent** checkbox.
9. Click **OK>OK>OK.**
10. Click **Next.**
11. Click **Finish.**

Installing Outlook 2003 on the Enterprise Vault server

Outlook 2003 must be installed on the Enterprise Vault server and connect with a mailbox on the Exchange Server 2003 computer before Enterprise Vault itself is installed. To install Outlook 2003 on the Enterprise Vault server:

1. Insert a CD-ROM with the Outlook 2003 installation code into the Windows Server 2003 computer. Outlook 2003 is available on the Office 2003 and the Exchange Server 2003 installation disks.
2. Browse to setup.exe on the installation media (this location will vary depending on which media you are using). Double-click **setup.exe** to begin the installation.
3. Enter the appropriate product key for the media.
4. Click **Next.**
5. Enter the appropriate information in the User name, Initials, and Organization areas.
6. Click **Next.**
7. If you agree with the terms of the licensing agreement, select the **I accept the terms in the License Agreement** checkbox.
8. Click **Next.**
9. Click **Custom Install.**
10. Click **Next.**
11. Choose to install Outlook 2003 and to have it run from your computer.
12. Expand the Microsoft Office Outlook object, and click **Collaboration Data Objects.** Select the **Run from My Computer** option.
13. Click **Install.**
14. After the setup files have been installed, select the **Check the Web for updates and additional downloads** checkbox. You may leave the Delete installation files check box cleared.
15. Click **Finish.** Internet Explorer will start.
16. Install any critical or recommended updates.

Windows Server 2003 domain controller configuration

Creating an Enterprise Vault Service Account in Active Directory

1. On a domain controller or a server with the Windows Server 2003 Administrative tools installed, click **Start,** and select **All Programs>Administrative Tools>Active Directory Users and Computers.**
2. In the left pane of Active Directory Users and Computers, double-click the icon displaying your domain name to expand the container.
3. Right-click the **Users** container, and select **New>User.**
4. Enter the details for the service account with appropriate information (suggested: First name: Enterprise; Last name: Vault; User logon name: enterprisevault).
5. Click **Next.**
6. Enter a password that conforms to your security policies, and confirm it. The Vault Service Account password cannot be blank.
7. Select the **Password never expires** checkbox.
8. Click **Next.**
9. Ensure the **Create an Exchange mailbox** checkbox is selected.
10. Click **Next.**
11. Click **Finish.**

Note

The mailbox created in step 7 will serve as the service mailbox for Enterprise Vault. This mailbox will be used by the archiving, journaling, public folder, and retrieval services, and should not be used for any other purpose.

12. Double-click the **Users** container in the left pane of Active Directory Users and Computers to expand the container.
13. In the right pane of Active Directory Users and Computers, right-click the Enterprise Vault user object you created, and click **Properties.**
14. In the Properties dialog box, click the **Member Of** tab.
15. Click Add. Enter `Administrators` in the Enter the object name to select box, and click **Check Names.**
16. Click **OK** after the name resolves.
17. Click **OK** to close the Properties dialog box.

Creating an alias in DNS for Enterprise Vault

1. Click **Start,** and select **All Programs>Administrative Tools>DNS.**
2. Expand your forward lookup zones. Right-click the domain hosting your Enterprise Vault server, and click **New Alias (CNAME).**
3. In the Alias name box, enter an alias for the Enterprise Vault directory (such as entvaultdir).
4. In the Fully qualified domain name (FQDN) for target host box, enter the fully qualified name of the Enterprise Vault server.
5. Leave all checkboxes in the configuration cleared.
6. Click **OK.**

Exchange Server 2003 configuration, part 1

Existing Exchange 2003 servers will need minor configuration changes to enable message journaling. If the server is running Exchange Server 2003, Enterprise Edition and has sufficient resource availability, an additional storage group can be enabled to host the journaling mailbox. If the Standard Edition of Exchange Server 2003 is deployed or the current server is using most available hardware resources, deploy an additional server to host the journaling mailbox. You will need to use an account with proper permissions (Exchange Administrator or Exchange Full Administrator) on the Exchange server to complete these steps.

Note
It is assumed that Exchange Server 2003 has been updated with Service Pack 1. If Service Pack 1 (or higher) has not been applied to the server, install the Service Pack before proceeding.

Assigning the Enterprise Vault Service Account permissions within Exchange Server 2003

1. Click **Start,** and select **All Programs>Microsoft Exchange>System Manager.**
2. In the left pane, right-click the Exchange organization name, and select **Properties.**
3. In the Administrative Views area of the General tab, select the **Display Administrative Groups** checkbox if it is not already enabled. Click **OK.**
4. Expand **Administrative Groups** and then **First Administrative Group** (or the appropriate administrative group, if you have renamed administrative groups within your organization).
5. Right-click **First Administrative Group,** and select **Delegate Control.** Click **Next.**

Note
If you will use the one Enterprise Vault Service Account for multiple Exchange servers within your organization, you can delegate control at the organization level by right-clicking the organization icon instead of the Administrative Group.

6. Click **Add,** and then click the **Browse** button to add the Enterprise Vault Service Account that was created in Active Directory. Click **OK.**
7. Select **Exchange Full Administrator** in the drop-down Role list.
8. Click **OK>Next>Finish.**
9. Click **OK** if prompted. If necessary, add the Enterprise Vault Service Account as a local administrator on all Exchange Server 2003 computers.

Assigning the Enterprise Vault Service Account permissions to access mailboxes

Note
These steps must be performed on each Exchange server that will be used in conjunction with Enterprise Vault.

1. Click **Start,** and select **All Programs>Microsoft Exchange>System Manager.**
2. In the left pane, double-click **Administrative Groups,** and then double-click **First Administrative Group.** Double-click **Servers** to expand the object. Select the Exchange server from the list.
3. Right-click the Exchange server name, and click **Properties.**
4. In the Properties dialog box, click the **Security** tab.
5. In the Group or user names area, select the Enterprise Vault Service Account.
6. Click **Advanced** to open the Advanced Security Settings for Exchange Server dialog box.
7. On the Permissions tab, click **Add,** and select the Enterprise Vault Service Account from the domain user list. Click **OK>OK.** The Permission Entry dialog box appears.
8. In the Allow column, select the **Receive As** and **Send As** checkboxes. Click **OK.**
9. Click **Apply,** and then click **OK>OK.**

HP ProLiant Storage Server configuration

The Enterprise Vault configuration will need space available on the HP ProLiant Storage Server to support journaling of all messages sent to, from, and within the Exchange organization. Because data will only be deleted from the Enterprise Vault according to the rules you configure, plan your disk space needs in accordance with the volume of messaging data within your organization.

The storage configuration on your HP ProLiant Storage Server differs slightly based on which model Storage Server you are using. Some models come with all of the storage preconfigured, so there is nothing that must be done to create storage areas. The hardware used to build the solution detailed in this paper is not preconfigured. On other Storage Servers with configurable storage (the Storage Server hardware detailed in this paper is of this type and must be configured using the **Array Configuration Utility** referred to in the following procedure), create a storage area to hold the Enterprise Vault data by following these steps:

1. Open a Web browser, and enter the following URL: http://StorageServerName:3202.
2. Select the **DISKS** tab.
3. Select the **Adaptec Storage Manager** or **Array Configuration Utility** item. Only one will be present, which depends on the model of Storage Server being used. It will be located in the upper left part of the screen, also visible as a nested tab. If neither item is present, you likely have a system without hardware RAID. In this situation, your storage should already be configured.
4. Using the tool from step 3, create a RAID 5 storage area of the required size, using the formula in the "HP ProLiant Storage Server" section on page 23. Exit the tool when this step is completed.
5. Back in the Web GUI, on the DISKS tab, select the **DISKS** item (also available as a nested tab).
6. Select the disk in the list that you just created (it will not have a label but will be recognizable by matching the size of the storage created in step 4). Select the **New Volume** button, which will launch the Microsoft Disk Management tool.
7. In Disk Manager, find the "Disk" that was just created. It will not be in the list at the top of the screen. It will be found on the scrollable pane at the bottom of the screen.

8. Right-click the "Disk," and select **New Partition.** Follow the wizard, such that all the available space is consumed, a drive letter is assigned, and an NTFS file system is created. You can give this volume a meaningful name. Selecting the **Perform a quick format** checkbox will speed the time it takes before the storage is ready to use.

After the storage has been configured, continue the configuration using the following steps. The following steps outlined use the standard Windows management tools. Some of the steps could alternatively be done from within the available Web-based GUI.

Adding the HP ProLiant Storage Server to the domain

1. Click **Start,** right-click **My Computer,** and select **Properties.**
2. Click the **Computer Name** tab, and rename the computer to meet your organization's naming conventions. On the same tab, add the computer to your Windows 2003 domain by clicking **Change** near the bottom of the page. Confirm this change, and close the **Properties** dialog box (you must have permissions within the domain to perform this operation).

Configuring disks to host Enterprise Vault

1. Click **Start,** and select **All Programs>Administrative Tools>Computer Management.**
2. Double-click the **Storage** object in the left pane to expand the object. Click the **Disk Management** object.
3. Ensure that the disks you want to use for the Enterprise Vault storage are formatted with the NTFS file system. If software RAID is being used (used on some older HP StorageWorks NAS devices), ensure it is an appropriate RAID configuration for the data (RAID 5 is the recommended configuration and should be the default for any NAS system using software RAID). Finally, assign a drive letter to the disks.
4. Click **Start** and select **Windows Explorer.**
5. Right-click the disk volume you formatted, and click **Sharing and Security.**
6. Select **Share this folder.**
7. Name the shared folder appropriately, and note the name for future use (the use of a hidden shared folder is suggested).
8. Click **Permissions.**
9. Click **Add.**
10. Enter the name of the Enterprise Vault Service Account in the Enter the names to select box, and click **Check Names.** If necessary, select the name from the list provided.
11. Click **OK** (twice, if necessary).
12. Highlight the service account name, and select the **Full Control** checkbox.
13. Click **Apply>OK>OK.**

Creating a folder in the disk volume for Enterprise Vault

You must create a folder on the disk volume that the Vault Store Partition will reside on, or the Vault Store Partition will not be created.

1. Click **Start** and select **Windows Explorer.**
2. Expand the disk volume you created for Enterprise Vault.
3. Right-click in the empty right pane, and select **New>Folder.**
4. Name the new folder Message Journal.

Windows Server 2003 configuration for Enterprise Vault, part 2

Adding the Enterprise Vault Service Account to local administrators

1. Click S**tart,** right-click **My Computer,** and select **Manage.**
2. In the left pane, double-click the **Local Users and Groups** object to expand it. Click the **Groups** object to expand it.

3. In the right pane, double-click the **Administrators** object to open its Properties dialog box. Click **Add.**
4. In the Enter the object names to select dialog box, enter the Enterprise Vault Service Account name that you created earlier. Click **Check Names,** and select the account you created.
5. Click **OK>OK.**
6. Close the Computer Management console.

After the service account for the Enterprise Vault has been configured, create a profile in Outlook 2003 for the Enterprise Vault mailbox.

Creating a profile for the Enterprise Vault mailbox in Outlook 2003

1. Click **Start,** and select **All Programs>Microsoft Office>Microsoft Office Outlook 2003.** The Outlook 2003 setup wizard starts.
2. Click **Next.** The Account Configuration page appears, asking whether you would like to configure an e-mail account.
3. Click **Yes>Next.**
4. On the E-mail Accounts page, click **Microsoft Exchange Server,** and click **Next.**
5. In the Microsoft Exchange Server area, enter the name of an Exchange server within your organization. In the User Name area, enter the name of the Enterprise Vault Service Account. Click **Check Name.**
6. Click **Next.**
7. Click **Finish.**

Installing the SQL client tools

The SQL client tools must be installed on the Enterprise Vault server (and any other computer that will be used to administer Enterprise Vault). To install them, use the following procedure:

1. Insert the SQL Server 2000 CD-ROM into the CD-ROM drive of the server.
2. Click **Start,** select **Run,** browse to \X86\setup\setupsql.exe, and click **OK** to begin the SQL Server 2000 installation program.
3. Click **Next** on the Welcome page.
4. Ensure that **Local Computer** is selected in the Computer Name page.
5. Click **Create a new instance of SQL Server** or **install Client Tools** in the Installation Section page.
6. Click **Next.**
7. Enter your name and company information.
8. Click **Next.**
9. Read the software licensing information, and, if you agree with the licensing, click **I Agree.**
10. Click **Next.**
11. Click **Client Tools Only** on the Installation Definition page.
12. Click **Next.**
13. Select the **Management Tools** and **Client Connectivity** checkboxes on the Select Components page. Deselect the **Books Online** and **Development Tools** checkboxes.
14. Click **Next** after confirming the settings. Click **Next** again if prompted regarding Microsoft Data Access Components (MDAC) setup.
15. Click **Finish** (if prompted by the MDAC setup).
16. When setup of the SQL tools completes, select the **Yes, I want to restart my computer now** checkbox.
17. Click **Finish.**
18. Obtain and install the latest Service Pack for SQL Server 2000. The latest service pack should be linked for download from http://www.microsoft.com/sql. SQL Service Pack 2 or later is required for SQL client tools to work properly on Windows Server 2003. You will need the database components.

Installing the Exchange System Management Tools

1. Insert the Exchange Server 2003 CD-ROM into the CD-ROM drive.
2. Browse to the **setup\i386** directory.
3. Double-click **setup.exe** to start the installation program.
4. Close all other programs, and click **Next.**
5. Read the licensing agreement, and click **I agree** if you agree.
6. Click **Next.**
7. In the Action column, select **Custom** next to Microsoft Exchange.
8. In the Action column, select **Install** next to Microsoft Exchange System Management Tools.
9. Click **Next.**
10. Ensure that the data in the System Summary page is accurate.
11. Click **Next.**
12. Click **Finish** after installation completes.

Creating a persistent drive mapping to the HP ProLiant Storage Server drive

1. Click **Start,** and select **Windows Explorer.**
2. Select **Tools>Map Network Drive**.
3. Specify a drive letter that is not in use, and enter the path to the HP ProLiant Storage Server drive that you shared earlier.
4. Ensure the **Reconnect at logon** checkbox is not selected.
5. Click **Finish.**

Installing the Enterprise Vault software

1. Click **Start,** and select **All Programs>Administrative Tools>Services.**
2. Right-click the **IIS Admin Service,** and select **Stop.** You will be prompted that stopping the IIS Admin Service will also stop several other services. Click **Yes** to stop all of these services.
3. Place the Enterprise Vault CD-ROM into the CD-ROM drive.
4. Browse to the **Enterprise Vault <version>\Enterprise Vault\Server** directory. Double-click **setup.exe.**
5. Click **Next.**
6. Read the licensing agreement, and if you accept the agreement, click **Yes.**
7. Verify that the installation will be performed in the correct directory (c:\Program Files\ Enterprise Vault is the default setting and should be left intact).
8. Click **Next.**
9. Ensure the **Enterprise Vault** and **Administration Console** checkboxes are selected.
10. Click **Next.**
11. Confirm that the program folders to be used are appropriate for your environment.
12. Click **Next.**
13. Click **Next** on the installation page to confirm your installation settings.
14. On the Installation Complete page, ensure that the **Run the Configuration** checkbox is selected.
15. Click **Finish.**
16. In the Enterprise Vault Configuration Wizard, ensure **Yes** is selected so a new Vault Directory will be installed on this server.
17. Click **Next.**
18. Enter the name of the Enterprise Vault Service Account you created earlier, and enter the service account password twice to confirm it.
19. Click **Next.** You will be notified that the service account you designated has been granted permissions to log on as a service, act as part of the operating system, and to debug programs.
20. Click **OK** to confirm.
21. Enter the name of your computer running SQL Server 2000 in the SQL Server location box (if you want to create the database in a named instance of SQL Server 2000, instead enter the instance in the format of <server name\instance name>).
22. Click **Next.**

23. Enter the locations where you would like to store the database and the transaction log files on the computer running SQL Server 2000.
24. Click **Next.** The Enterprise Vault directory is created.
25. Enter a name and description for the Vault Site.
26. Enter an alias that DNS will use for the Vault Site. This alias can be the name of the Enterprise Vault server and should be fully qualified.
27. Click **Next.**
28. Confirm that the next DNS alias will correctly identify the Enterprise Vault computer.
29. Click **Next.**
30. Enter the password for the Enterprise Vault Service Account.
31. Click **Next.**
32. Read the information regarding the services, and click **Next.**
33. Click **Add.**
34. Select **Enterprise Vault Retrieval Service,** and add the name of the Exchange server that will host the journaling mailbox in the Exchange Server area.
35. Click **Next.**
36. Confirm the locations of the services, and ensure the **Run archiving service in report mode** checkbox is selected.
37. Click **Next.**
38. Click **Use this mailbox,** and click **Browse.**
39. Select the Enterprise Vault Service Account mailbox from the list, and click **OK.**
40. Click **OK.**
41. Click **Next** to start the Enterprise Vault services.
42. Click **Next** again to confirm that you want to start the services.
43. Click **Finish** to close the configuration program.
44. Ensure that your Enterprise Vault license key is named keys_computername.txt and in place in the Program Files\Enterprise Vault directory.

Creating an Enterprise Vault Store

1. Click **Start,** and select **All Programs>Enterprise Vault>Administration Console.**
2. Enter the name of the Enterprise Vault server in the Directory Service Computer box.
3. Click **OK.** The Enterprise Vault Administration Console opens.
4. Double-click **Enterprise Vault,** click **Directory on <server name>,** then select the name you chose for your Enterprise Vault store alias.
5. Right-click **<Vault Store alias>,** and select **New>Vault Store.**
6. Click **Next>Next.**
7. Enter a name and description for the new Vault Store.
8. Click **Next.**
9. Enter the name of the computer running SQL Server 2000 (or named instance) on which you want to store the Vault Store database.
10. Enter appropriate locations for the Vault Store database and log files on your computer running SQL Server 2000.
11. Click **Next.**
12. Leave the default settings in place for safety copies and automatic creation of Vaults.
13. Click **Next.**
14. Click **Finish.**
15. Click **Next** to add a Vault Store Partition to the new Vault Store.
16. Click **Next** to begin creating the partition.
17. Name the partition, and enter a description for it (or accept the suggested name and description). Ensure **Open** is selected.
18. Click **Next.**
19. Click **Network Share.**
20. Click **Next.**

21. Enter the name of the network share and folder you created on your HP ProLiant Storage Server in the correct format (\\StorageServerName\sharename$\Message Journal). Be sure to use the $ if you created a hidden share.
22. Click **Next.**
23. Select the **Share archived items** and **Create Vault Store Partition with security ACLs** checkboxes.
24. Click **Next.**
25. Click **None.**
26. Click **Next.**
27. Click **Finish.**

Creating a Vault

1. Click **Start,** and select **All Programs>Enterprise Vault>Administration Console.**
2. Enter the name of the Enterprise Vault server to identify the Directory Server.
3. Double-click **Enterprise Vault,** double-click **Directory on Enterprise Vault,** and then double-click the name you chose for the server's Directory alias.
4. Right-click **Archives,** and select **New>Vault.**
5. Click **Next.**
6. Select the Vault Store you created in step 4.
7. Click **Next.**
8. Enter a name and description for the new Vault.
9. Click **Next.**
10. Click **Add,** and add the Enterprise Vault Service Account to the Add Names area. Click **Control** in the Type of Access list.
11. Click **OK** (if you want others to have access to this Vault, you can either select those names now or add them later).
12. Review your choices.
13. Click **Next.**
14. Leave the indexing service options at their defaults.
15. Click **Next.**
16. Leave the **Use site setting** checkbox selected.
17. Add a billing account by clicking the **Browse** button and selecting an appropriate user account from your domain.
18. Click **OK.**
19. Click **Next.**
20. Click **Finish.**
21. Click **Close.**

Adding the Enterprise Vault Journaling Service

1. Click **Start,** and select **All Programs>Enterprise Vault>Administration Console.**
2. Enter the name of the Enterprise Vault server.
3. Double-click **Enterprise Vault,** double-click **Directory on Enterprise Vault,** and then double-click the name you chose for the server's Directory alias.
4. Double-click the **Computers** object.
5. Right-click the **Enterprise Vault server** icon, and select **New>Service.**
6. Select the **Enterprise Vault Journaling Service,** and add the name of the Exchange server that will host the journaling mailbox in the Exchange Server area.
7. Click **Add.** You will be prompted to configure the Journaling Service.
8. Click **Yes.**
9. Select the mailbox you want to use as your journaling destination by clicking **Browse** and clicking the mailbox in the list.
10. Click **OK.**
11. Select the Vault you want to use for the journaling by clicking **Browse.**

12. Click **Apply.**
13. Click **OK.**
14. Enter the password for the Enterprise Vault Service Account.
15. Click **OK.**

Starting Enterprise Vault Services

1. Click **Start,** and select **Administrative Tools>Services.**
2. Scroll to the Enterprise Vault services listings in the Services MMC.
3. If any Enterprise Vault service is set to Disabled or Manual, change the setting to Automatic by right-clicking the service, clicking **Properties,** and changing the Startup Type to Automatic. Click **OK.**
4. If any Enterprise Vault Service status is Stopped, right-click the service and click **Start.**

Exchange Server 2003 configuration, part 2

Enabling message journaling

1. Click **Start,** and select **All Programs>Microsoft Exchange>System Manager.**
2. Double-click **Administrative Groups,** and browse to the Administrative Group hosting your Exchange server.
3. Double-click **First Administrative Group** (or the appropriate Administrative Group that hosts your Exchange server).
4. Double-click **Servers,** and select the Exchange server on which you want to enable journaling.
5. Expand the appropriately named Storage Group (usually First Storage Group).
6. Right-click **Mailbox Store,** and select **Properties.**
7. On the General tab of the Mailbox Store Properties dialog box, select the **Archive all messages sent or received by mailboxes on this store** checkbox.
8. Click **Browse.** Either enter the journaling mailbox name in the Enter the object name to select box, or use the **Advanced** option to find the name in the address list.
9. Click **OK.**
10. Click **Apply>OK.**

SQL Server 2000 configuration

Creating an SQL logon for the Enterprise Vault Service Account using SQL Enterprise Manager

1. Click **Start,** and select **All Programs>Microsoft SQL Server>Enterprise Manager.**
2. In the left pane, double-click to expand the **SQL Server Group** container, and then double-click to expand the local object.
3. In the right pane, double-click the **Security** folder to expand it.
4. Right-click **Logins,** and click **New Login** on the shortcut menu.
5. In the Name box, enter the name of the Enterprise Vault Service Account in the format of domain name\service account.
6. Ensure that **Windows Authentication** and the correct domain name for the account are selected.
7. Under Security Access, ensure that **Grant access** is selected.
8. On the Server Roles tab, select the **Database Creators** checkbox.
9. Click **OK.**

Windows 2003 Server configuration for Discovery Accelerator

Discovery Accelerator will be installed on the same Windows 2003 server that is running Enterprise Vault.

Installing the Internet Explorer WebControls

The Internet Explorer WebControls are necessary for Discovery Accelerator to install and run correctly. WebControls are available in the Redistributables folder on the Discovery Accelerator CD-ROM. To install:

1. Insert the Discovery Accelerator CD-ROM into the CD-ROM drive of the Enterprise Vault server.
2. Browse to the **Redistributables** folder.
3. Double-click **IEWebControls.exe.** If prompted, click **Open.**
4. Read the terms of the licensing agreement. If you agree with the terms, select **I accept the terms in the license agreement.**
5. Click **Next.**
6. Leave the installation path in its default configuration. Click **Next.**
7. Click **Finish.**

Setting temp folder access for the IIS Worker Process User

1. Right-click **Start** and select **Explore.**
2. Click **My Computer** and open **c:\.**
3. Right-click **temp** (if there is no temp directory, create one) and select **Properties.**
4. Select the **Security** tab.
5. Click **Add.**
6. Enter Network Service in the Enter the object names to select box.
7. Click **Check Names.** The name should resolve.
8. Click **OK**.
9. Ensure **Network Service** is highlighted, and, in the Allow column, select **Full Control.**
10. Click **Apply,** and then click **OK.**
11. Close the **Properties** page.

Installing the Discovery Accelerator software

1. Log on to the Enterprise Vault server using the Enterprise Vault Service Account you created earlier.
2. Insert the Enterprise Vault installation CD-ROM into the CD-ROM drive of the server.
3. Right-click **Start** and select **Explore.**
4. In Windows Explorer, browse to the server CD-ROM drive, and double-click it to open the CD-ROM.
5. Double-click the **Enterprise Vault 5.0 CP1 directory\Discovery Accelerator\Kit** directory to open it, and double-click **setup.exe.**
6. Click **Next** on the Welcome screen.
7. Read the licensing agreement. If you agree with it, click **Yes.**
8. Enter an appropriate User Name and Company Name in the area provided.
9. Ensure **Anyone who uses this computer** is selected.
10. Click **Next.**
11. Select **Typical.**
12. Click **Next.**
13. Review the settings presented. Click **Next** if they are correct.
14. Click **OK** to acknowledge the Information dialog box that informs you that the next screen will request a login name and password that Discovery Accelerator will use.
15. Enter the Enterprise Vault Service Account name in the format of domain\username.
16. Enter and confirm the password in the correct fields.
17. Click **OK.**
18. Click **Finish.**

Installing the license key for Discovery Accelerator

1. Send the file c:\Program Files\KVS\Discovery Accelerator\ EVSystemInfo_Computername.txt (computername should be the NETBIOS name of the Enterprise Vault server) to KVS. In return, you will receive a license key.
2. Copy the **keys_computername.txt** file that KVS returned to you into the c:\Program Files\KVS\Discovery Accelerator directory.
3. Click **Start,** and select **Administrative Tools>Services.**

4. Right-click **Enterprise Vault Discovery Accelerator Service,** and select **Start.**
5. Close the Services applet.

Configuring Discovery Accelerator

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery` in the address bar, substituting the name of the Enterprise Vault server for `servername`.
4. On the Discovery Accelerator home page, click **Configure.**
5. In the SQL Server box, enter the name of the SQL Server 2000 computer (or instance) that will be supporting Discovery Accelerator.
6. In the Database name box, leave EVAccelerator in place.
7. In the Data file folder box, enter the drive location that will host the database file. This location should be a valid, existing path on the SQL Server computer and can be a local or mapped drive.
8. In the Log file folder box, enter the drive location that will host the database file. This location should be a valid, existing path on the SQL Server computer and can be a local or mapped drive.
9. In the Directory DNS Alias box, enter the DNS alias or server name of the Enterprise Vault Directory Service computer.
10. Click **OK.**
11. Click **Start,** and select **Administrative Programs>Services.**
12. In the Services applet, right-click **Enterprise Vault Discovery Accelerator Service,** and select **Restart.**
13. Close the Services applet.
14. Refocus on the Discovery Accelerator home page, and click **OK.**
15. Close Internet Explorer.

Discovery Accelerator in action

The EVDiscovery Web Application is the main interface for Discovery Accelerator and is used to find data within Enterprise Vault. The main uses of the EVDiscovery Web Application are:

- Creating cases
- Assigning a case administrator to a case
- Creating users
- Creating and assigning roles for users
- Setting up marking schemes such as ”personal,” ”spam,” or ”relevant”
- Creating searches (After a case is created, a search is created where search parameters are defined.)
- Assigning reviewers for data returned in a search
- Enabling reviewers to use defined marking schemes to annotate items returned in a search
- Exporting reviewed items so they can be presented as necessary

When a request for information is received from a governing body, first create a knowledge management team to process the data requested. Generally, a knowledge management team consists of representatives from the legal department and corporate librarians; the Information Technology department does not need to be highly involved in this process. Roles, as shown earlier in Figure 4, should be assigned to members of this team to designate the responsibilities of each team member. You can customize permissions when assigning roles; however, you should assign as few permissions as necessary. The permissions you choose to assign can vary depending on the size of your organization and the size of the team assigned to the discovery process.

Note
The EVDiscovery Web Application interface only reveals the tasks that the currently logged on user has permissions to complete.

To familiarize you with Discovery Accelerator, the following instructions walk through the EVDiscovery Web Application, creating a case, searching for data, marking the data, and producing the data. This process follows the workflow shown in Figure 4. For the purposes of this example discovery exercise, imagine the following team exists within your organization and is responsible for discovery:

1. Senior legal department representative—The Administrator of the system who oversees all cases
2. Legal department representative—The Case Administrator who manages the case on a day-to-day basis
3. Corporate librarians—Three Reviewers who mark the search results

While the IT department does not have an active role in managing cases, IT interaction is initially required to set up the first case and perform system administration.

Creating roles in Discovery Accelerator

The IT representative will initially create roles to be assigned to the other team members, using the following procedure:

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
4. Click **Roles** in the Application Administration column.
5. Click **New Role.**
6. In the Name box, enter `Case Administrator`.
7. In the Description box, enter a description such as Team Leader.
8. Select either **Application** or **Case** as the Scope for the role. For the example in this document, Case is selected.
9. In the Permissions area, select the **Case Administration, Search, Assign, Production,** and **Review** checkboxes.
10. Click **OK.**
11. Click **New Role.**
12. In the Name box, enter `Reviewer`.
13. In the Description box, enter a description such as Corporate Librarian.
14. In the Permissions area, select the **Review** checkbox.
15. Click **OK.**
16. Click **Close.**

Reviewing scheme templates

Scheme templates exist on a global level within Discovery Accelerator and serve as templates for marking schemes created in cases. Do not initially change any scheme templates, but ensure the default Review Marks scheme template, which serves as the base scheme for all marking, exists. If you ever intend to create a new scheme template, this is the interface you will use to do so.

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
4. Click **Scheme Templates** in the Application Administration column.

5. Ensure the Review Marks template, with a description of Review Marks, exists.
6. Click **Close.**

Creating marks in Discovery Accelerator

Marks are used when reviewing search results. The default marks and their definitions are:

- No mark—The item has yet to be reviewed.
- Relevant—The item is relevant to the discovery in process.
- Not relevant—The item is irrelevant to the discovery in process.
- Query—The item has yet to be queried for the search.

Every mark that is created is assigned a status (for example, the status of a relevant item would be included, while the status of a mark of not relevant would be excluded). Create a new mark named "UCE" so you can classify unsolicited commercial e-mail (UCE) messages. When this mark is applied to an item returned in queries, the item will retain the marking and the messages can be excluded from examination during other case reviews.

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
4. Click **Marks** in the Application Administration column.
5. Click **New Mark.**
6. Enter `UCE` in the Name box.
7. Enter `Unsolicited Commercial E-mail` in the Description box.
8. Select **Reviewed from the Status applied** listing.
9. Select the **Items retain this mark for use in other cases** checkbox.
10. Click **OK.**
11. Click **Close.**

Adding a mark to a scheme template

After a new mark is created, it must be added to the scheme template so it can be used when marking items searched in a case. To add the UCE mark to the existing scheme template:

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
4. Click **Scheme Templates** in the Application Administration column.
5. Click **Review Marks.**
6. Click **Next** on the Edit Template page.
7. Select **UCE** and click the carat icon (>).
8. Click **Finish.**
9. Click **Close.**

Creating a case in Discovery Accelerator

Discovery Accelerator cases are used to oversee the data discovery process. When discovering data, a case must be created to manage the process and isolate the results of the search for review, marking, and production, if necessary. The Discovery Accelerator Web interface is used to perform this operation. The following procedure creates a case regarding widget trading and assigns case ownership to the legal representative from the team.

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Internet Explorer.**
3. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
4. Click **Cases** in the Application Administration column.
5. Click **New Case.**
6. In the Name box, enter a name for the case, such as Widget Trading.
7. Click **Add User** next to the Case Owner box. In the Add User dialog, enter the user name for the Case Administrator in the format of domain\user name. The Case Owner is also referred to as the Administrator.
8. Click **Close.**
9. In the Vault Stores box, select the Vault Store (or multiple Vault Stores) to be included in the case.
10. Leave the Next export number and Size of the export ID boxes set to their default values.
11. In the Prefix box, enter a relevant prefix for the search results. This prefix should clearly relate to the case name. Widget was used in this testing environment.
12. In the Output folder box, enter the path where the results should be written, such as c:\caseoutput\case name.
13. Click **OK.**
14. Click **Close.**

Assigning roles to users

The Administrator, as assigned in the previous section, assigns roles to other users as necessary. After the Case Administrator role is assigned, the Case Administrator may also assign roles to other users.

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Case Administrator's user name in the format of domain\username and password, if prompted.
4. Click **Widget Training** (the case name) in the Case Administration column.
5. Click **User Roles** under Options.
6. Click **Add User.**
7. In the Login name box, enter the name to add team member in the format of domain\username.
8. Click **Add.**
9. Repeat steps 7 and 8 to add all team members.
10. Click **Close.**
11. In the Roles column, click the **Admin** role.
12. In the Users column, select the checkbox for each user that must have Administrator rights for the case.
13. In the Roles column, select the **Case Administrator** role.
14. In the Users column, select the checkbox for each user that must have Case Administrator rights for the case.
15. In the Roles column, select the **Reviewer** role.
16. In the Users column, select the checkbox for each user that needs Reviewer rights for the case.
17. Click **OK.**

Assigning marks to roles

Marks, as discussed earlier, are used during the review of items returned from a search. You can allow only specific users to apply certain marks to items returned in a search. In this example, all reviewers are allowed to use all marks; you might want to allow reviewers to use fewer marks. Administrator rights are necessary to perform this operation.

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Administrator's user name in the format of domain\username and password.
4. Click **Widget Training** (the case name) in the Case Administration column.
5. Click **Schemes** under Options.
6. Click **Review marks.**
7. Click **Next** on the Edit Scheme page.
8. Click **Next** on the Scheme Marks In Review Marks page.
9. Click **Reviewer,** and select the checkboxes for all marks listed.
10. If you want to assign marks to other roles, select the role and select the checkbox for each mark the role should be able to assign to an item.
11. Click **Finish.**
12. Click **Close.**

Creating targets

Targets are specific users that can be searched for in cases. Target groups are groups of specific users that can be searched for in cases. If you want to include all data within a search, there is no need to create targets. Administrator or Case Administrators rights are required to create target groups. To create a target for one user and add that user to a target group:

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Case Administrator's user name in the format of domain\username and password if prompted.
4. In the Case Administration column, click **Widget Trading** or the appropriate case name.
5. Under Options, click **Address Manager.**
6. Click **New Target.**
7. In the First Name box, enter the user's first name.
8. In the Last Name box, enter the user's last name.
9. In the Email Addresses box, enter `address@domain.com`.
10. Click **OK.**
11. Click **Close.**
12. Click **New Group.**
13. In the Name box, enter a name for the group, such as Test Group.
14. In the Description box, enter a description, such as Testing.
15. Click **Edit Targets.**
16. Select the checkbox for the target added earlier.
17. Click **OK.**
18. Click **Close.**

Searching Enterprise Vault

Discovery Accelerator enables searching for specific information within vaults. Case Administrators and other roles that have the search permission may create searches. It is best to carefully control the ability to create searches and to clearly document what keywords have been used in searches. The fields in the search options are optional and do not need to be completed if you want to do a wide-ranging search. Multiple searches, using different key words, can be performed in a single case. To search Enterprise Vault:

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.

3. Enter the Case Administrator's user name in the format of domain\username and password if prompted.
4. In the Case Administration column, click **Widget Trading** or the appropriate case name.
5. Under Options, click **Searches.**
6. Click **New Search.**
7. In the Search name box, enter a name for the search, such as Widget.
8. Click the calendar icon next to the Date from box, and select the starting date for the search.
9. Click the calendar icon next to the To box, and select the last date that should be included in the search.
10. To isolate the message's originator or select multiple originators, select the address book icon to view targets or groups. Select the appropriate checkbox for the target users or groups, and click **OK.**
11. To isolate the message's recipient or select multiple recipients, select the address book icon to view targets or groups. Select the appropriate checkbox for the target users or groups, and click **OK.**
12. To search for a specific word or phrase in the subject line of the messages returned from your search, enter the word or phrase (such as widget) in the Subject box.
13. To isolate a word or phrase in the message body or within an attachment to a message, enter the word or phrase (such as widget trades) in the Content box.
14. Click **OK.** The search process begins, and results are shown. You can click an individual result to view the message.
15. Click **Accept.**
16. Click **Close.**
17. On the Search Accepted page, click **Close.**

Assigning search results to reviewers

When your search has produced results, the items returned should be assigned to designated reviewers for marking. To do so, use the following procedure:

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Case Administrator's user name in the format of domain\username and password if prompted.
4. In the Case Administration column, click **Widget Trading** or the appropriate case name.
5. Under Options, click **Review Assignment.**
6. In the Role listing, select **Reviewer** (or the role assigned to your reviewers).
7. In the Name listing, assign each reviewer a number of items returned from your search to review by entering a number in the Assign column.
8. Click **Apply.**
9. Click **Close.**

Reviewing and marking search results

Reviewers mark their search items as appropriate for their pertinence to the matter at hand. If items are not necessary for production, they should be marked as excluded from the case. Items that must be produced should be marked as included. Each designated Reviewer should follow the steps presented within this section. When reviewing search results, Reviewers can filter messages within the case, or begin at the first message within their case. To review and mark search results:

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Reviewer's user name in the format of domain\username and password if prompted.

4. In the Reviewer column, click **Widget Trading** (or the appropriate case name). The items assigned to the current users are listed under Your Items in the Case Status row. The number of total items returned from the search is listed under All Items.
5. To filter the messages assigned to the reviewer, select any of the following options:
   - The Items option enables Reviewers to view only the items assigned to them (My Items or All Items).
   - The Mark option enables Reviewers to filter the items they view by their current marking (such as Relevant, Not Relevant, or No Mark).
   - The Status option enables Reviewers to filter the items they view by their current status (such as Included, Excluded, or Pending).
   - The Search option enables Reviewers to filter the items they view by each search that was performed or view items assigned to the reviewer from all searches.
   - The Go to option enables Reviewers to select which item they will view.
6. Leave all options under Options in their default state, and click **OK.** The first item to be reviewed appears.
7. Review the text of the message by using the scroll bar in the message frame.
8. If there is a comment, enter it in the Comment box. Comments can be seen and used for further review by others.
9. Select the appropriate mark for the item by using the Mark option and selecting a mark, such as Relevant.
10. Click **Next** to proceed to the next item for review.
11. Repeat steps 10 and 11 for each item to be reviewed.
12. After all items have been reviewed, End of review set appears on the screen.
13. Either close the browser, or click **Home** to go to the Discovery Accelerator home page.

Producing items

When the items returned from a case have all been reviewed and marked, they might need to be produced to external governing bodies, such as the SEC, for examination. To produce all items from the case that are assigned the included status:

1. From any computer, click **Start,** and select **All Programs>Internet Explorer.**
2. Open the Discovery Accelerator home page by entering `http://servername/evdiscovery`, substituting the name of the Enterprise Vault server for `servername`.
3. Enter the Case Administrator's user name in the format of domain\username and password if prompted.
4. In the Case Administration column, click **Widget Trading** or the appropriate case name.
5. Under Options, click **Production.**
6. Click **Select Items.**
7. Select the **Included in the Status** box.
8. In the Number of items box, enter the number of items to produce. If the number of items available, shown as the Maximum number, is large, you might want to initially produce only a portion of the items.
9. Click **OK.**
10. Click **Close.**
11. Click **New Run.**
12. Enter a name for the production run in the Name box.
13. Enter the number of items you want to produce in the Number of items box.
14. Click **OK.**
15. Click **Close.**
16. After the run is completed, click **Start,** select **Run,** and enter `c:\caseoutput\case name`, as designated during the initial creation of the case.
17. Click **OK.**
18. Double-click the name used for the production run in step 12.

The items that were produced should be within this folder. You can now copy the items to other media that can be provided to external governing bodies.

Optional solution component installation and configuration

When KVS Enterprise Vault and Discovery Accelerator are installed and operational, you may decide which additional components may be installed.

Enabling SharePoint Portal Server 2003 archiving

Data from SharePoint Portal Server 2003 sites can be archived into a separate Vault Store to provide a repository of project-related documents, which enables organizations to easily retrieve data that is no longer active and allows SharePoint to continue to be used for projects that are in process. The Vault Store used for SharePoint data should be separate from the Vault Store hosting journaled data from Microsoft Exchange Server.

Note
The Enterprise Vault SPS Service will not install unless SharePoint Portal Server 2003 client components are installed on the Enterprise Vault server to allow backward compatibility. SharePoint Portal Server 2003 client components are on the SharePoint Portal Server 2003 CD-ROM and are also available for download at http://www.microsoft.com/downloads/details.aspx?FamilyID=DF39E250-F7AE-445A-AC9D-A80C9035ED6B&displaylang=en.

Configuring Enterprise Vault to support SharePoint Portal Server data

1. Log on to the Enterprise Vault server using the Enterprise Vault Service Account.
2. Click **Start,** and select **All Programs>Enterprise Vault>Administration Console.**
3. In the Directory Service Computer box, enter the name of the computer running the Enterprise Vault Directory Service that you want to use.
4. Click **OK.**
5. Double-click **Enterprise Vault.**
6. Double-click **Directory on <server name>.**
7. Double-click the directory server alias.
8. Double-click **Computers.**
9. Right-click the Enterprise Vault computer you want to support SharePoint Portal Server 2003, and select **New>Service.**
10. Select **Enterprise Vault SPS Service.**
11. Enter the name of the SharePoint Portal Server to use in the SharePoint Portal Server box.
12. Click **Add.**

Supplemental installation for end-user archive access

Adding an archiving service for users

A separate Vault Store can be created to enable users to archive data within their mailboxes. This capability can help keep data that is not accessed on a regular basis accessible, but not within the Exchange Server information store. The Vault Store used for message journaling should never be used for mailbox archiving because the data within that store might be needed for legal purposes and should not be mixed with other data.

Use the Enterprise Vault Configuration program to create a new Vault Store and install the Enterprise Vault Archiving Service on the Enterprise Vault server to support users' data archiving needs.

Requirements for users' computers

User extensions must be installed on users' workstations for users to be able to archive items from their mailboxes. When user extensions are installed, users can search, view, and restore archived messages from all Outlook client versions. The workstation must be running one of the following operating systems to use user extensions:

- Windows Server 2003
- Windows 2000
- Microsoft Windows NT® Server Version 4.0 with Service Pack 6a or later
- Windows XP Professional
- Windows 2000 Professional
- Windows NT Workstation Version 4.0 with Service Pack 6a or later.
- Windows Millennium Edition
- Windows 98 with DCOM 98 1.3 or later
- Windows 95 OSR2 or later with DCOM for Windows 95

When a message is archived from a user's mailbox, the message is moved from the Microsoft Exchange information store into the appropriate Vault Store for the Enterprise Vault Archiving Service, and a shortcut is created on the Exchange server that links the archived message to the original message data. The shortcut displays the from and subject lines of the message. You can customize what users see when they click a shortcut to a message. The options are:

- Show contents—Double-clicking the shortcut displays the item's contents in their original format.
- Show properties—Double-clicking the shortcut displays the properties of the shortcut.

Alternatively, OWA extensions can be installed on the Exchange servers, enabling access to the Enterprise Vault archive using OWA. Internet Explorer 5.01 or later is required.

Mailbox archiving can be set up globally and rules can be created to enable automatic archiving of data in mailboxes, or users can be given discretion over the archiving of data within their mailboxes. Default retention categories can be used to enable smart data retention, and customized retention categories can be created to provide more flexible data archiving.

When a user's mailbox is enabled for message archiving, a welcome message is automatically sent to the mailbox. This message tells users how to take advantage of Enterprise Vault features and should be edited to include information on installing the Enterprise Vault user extensions.

Conclusion

Meeting the regulatory requirements pertinent to your organization is an on-going process and should be well understood before implementing a long-term message archiving system. To begin this process, you must thoroughly understand your organization's messaging capabilities, the processes and technology involved, and your organization's needs to ensure that clear policies are in place and are followed. The processes within this solution blueprint enable you to immediately realize the benefits of a message archiving and retrieval solution that enhances and extends the native message journaling capabilities of Microsoft Exchange Server 2003. Implementing KVS Enterprise Vault and Discovery Accelerator can help your organization craft an Exchange-based solution that will help meet regulatory requirements. Using HP ProLiant Storage Servers as the storage solution provides you with the peace of mind that your data is safe.

This solution blueprint guides you through the process of installing and configuring numerous Windows Server technologies to help support your organization's regulatory compliance goals. Microsoft Exchange Server 2003, SharePoint Portal Server 2003, and KVS Enterprise Vault and Discovery Accelerator provide a solid foundation to help companies address regulatory compliance

requirements. The flexible storage solutions of HP ProLiant Storage Servers built on Windows Storage Server 2003 enable organizations to quickly and easily implement large disk arrays to support the storage needs of Enterprise Vault. Enterprise Vault, in turn, provides an unparalleled collection of tools to help both users and the organization exploit the message archive. Users can view the hierarchy of all archived information in the feature-rich Archive Explorer client that does not require deployment. Organizations can retain their e-mail and documents, model the retention against corporate guidelines, and quickly and easily discover content as needed.

For more information

- For more information on e-mail archiving solutions, contact HPKVS@hp.com.
- HP ProLiant Storage Servers (NAS)
  http://www.hp.com/go/StorageServers
- HP StorageWorks
  http://www.hp.com/go/StorageWorks
- HP ProLiant servers
  http://www.hp.com/go/ProLiant
- HP Microsoft Exchange Resources
  http://h71019.www7.hp.com/enterprise/cache/3844-0-0-0-121.aspx
- "Introduction to Windows Storage Server 2003 Architecture and Deployment"
  http://www.microsoft.com/windowsserversystem/wss2003/techinfo/plandeploy/wss2k3archdeploy.mspx
- "A hotfix is available to enable the Envelope Journaling feature in Exchange 2000 Server"
  http://support.microsoft.com/?kbid=834634
- "Server Consolidation Using Exchange Server 2003"
  http://www.microsoft.com/downloads/details.aspx?FamilyId=BC3A8D76-FC58-4E3C-9152-1CE35E9466EA&displaylang=en
- Microsoft Windows Storage
  http://www.microsoft.com/storage
- Microsoft Windows Server 2003
  http://www.microsoft.com/windowsserver2003
- Microsoft Exchange Server 2003
  http://www.microsoft.com/exchange
- KVS Enterprise Vault and Discovery Accelerator
  http://www.kvsinc.com

5982-8988EN, Rev. 1 12/2004

invent