Installing, Configuring and Administering

Microsoft Exchange 2000 Server

Version 3.0.0

Installing, Configuring, and Administering

Microsoft Exchange 2000 Server

Version 3.0.0

Abstract:

This study guide will help you prepare for the Microsoft Exam 70-224, Installing, Configuring, and Administering Microsoft Exchange 2000 Server. Exam topics include installation, administration, and troubleshooting information systems that incorporate Microsoft Exchange 2000 Server.

Find even more help here:

Contents:

Introduction to Exchange 2000 Server

Client/Server Messaging Systems

Exchange 2000 is a client/server messaging system (i.e., client sends a request to the server, and the server processes that request).
Advantages of a Client/Server environment

- More secure environment
- Reduced network traffic
- Increased stability

Disadvantages of a client/server messaging system

- Requires more powerful hardware because of the increased processing

Versions of Exchange Server

Exchange 2000 Server

- Single 16-gigabyte (GB) database per server
- Does not support Chat, Windows Clustering, or distributed configuration

Exchange 2000 Enterprise Server

- Allows multiple servers, with unlimited message store
- Allows multiple stores on each server

Exchange 2000 Conferencing Server

Allows data conferencing through a T.120 client (i.e., Microsoft NetMeeting)

Limitations of Exchange 2000 Server over Exchange 2000 Enterprise Server:

- Information Store limitation to 16GB
- One database per server
- Clustering is not available
- Front-end/back-end is not available
- Chat is not available

Core Components

Core components in Exchange 2000 messaging infrastructure

- Information Store Service
- System Attendant

- Simple Mail Transport Protocol
- Active Directory
- Web Storage System
- Extensible Storage Engine

Web Storage System

Provides the following functionality:

- EXIFS - allows streaming data, and office applications to read and write to mailboxes as if it was a file system
- Native Content Store – stores non-MAPI client data in native MIME format
- URL Addressing – access to mailboxes and data via a URL
- Web Distributed Authoring and Versioning (WebDAV) – allows enhanced web development capabilities
- Extensible Markup Language (XML) – defines HTML data

It also offers the following development capabilities:

- Event Programming Support
- Web Forms
- Workflow Designer for Exchange
- CDO for Exchange 2000
- CDO for Exchange Management

Extensible Storage Engine (ESE)

The main function of ESE is to handle database transactions.
ESE supports full *ACID* transactions:

- *Atomic* – transactions are always either complete or not complete.
- *Consistent* – each transaction takes the database from one consistent state to another.
- *Isolated* – Changes are not visible until the entire transaction is committed.
- *Durable* – Committed transactions are not lost during a system crash.

ESE uses physical memory to store changes while they are being made. All operations are recorded sequentially, in transaction logs, on the hard disk.
ESE generates the following file types:

File Type	Function
Current Streaming Database (.stm)	Stores MIME content, voice, video, etc.
Current Rich Text Database (.edb)	Contains MAPI content (i.e., Outlook 2000).
Current Transaction Log file (E*xx*.log)	Secures transactions before they are written to the ESE database. There is one transaction log file per storage group.
Previous Transaction log files	Are the previous log files to the current

(E*xxnnnnn*.log)	transaction log file.
Checkpoint file (E*xx*.chk)	Contains a pointer which specifies which transaction log contains the last committed transaction.
Reserved transaction log files (Res1.log and res2.log)	Holds reserved space in case of an out-of-disk-space situation arises.
Temp files (tmp.edb)	Contains transient storage of information for re-indexing, store maintenance, etc.
Patch Files	Are temporary log files that store special transactions during an inline backup.

Administration Tools

Exchange System Manager

Opening the Exchange System Manager will connect you to any domain controller on the same subnet, where AD is queried to populate the console with the relevant data for the Exchange 2000 Organization.
The Exchange System Manager:

- Must be installed to manage Exchange 2000 recipients
- Can be installed on any computer running Windows 2000

Available MMC Snap-ins:

- Exchange Advanced Security
- Exchange Message Tracking Center
- Exchange System
  - MS Exchange GroupWise Connector
  - MS Exchange Notes Connector
  - Protocols
  - Exchange SMTP
  - Exchange Servers
  - Exchange System
  - Exchange X.400
  - Exchange cc:Mail

ADSI Edit

Adsiedit.exe is a low-level utility that uses Active Directory Services Interface (ADSI) to view and modify objects within Active Directory.

Active Directory Administration Tool (ldp.exe)

An LDAP tool used to connect to an LDAP compatible directory (i.e., Active Directory) to view and modify objects.

Active Directory Schema

AD Schema MMC snap-in allows you to view attribute and class configuration.
N.B. Before loading Active Directory Schema, you must register its DLL by typing this at the command prompt: **regsvr32 schmmgmt.dll**

Exchange Task Wizard

Many tasks can be completed using the Exchange Task Wizard, including the ability to:

- Add or remove mailboxes for user objects.
- Establish or delete e-mail addresses for users, contacts, and groups.
- Move a user's mailbox to another server running Exchange 2000 in the organization
- Enable or disable Instant Messaging for a user.
- Hide or expose group memberships.

Dependencies on Windows 2000 Components

Active Directory

Only one Exchange 2000 organization can exist per forest.
When adding an Exchange 2000 Server to an existing Exchange 5.5 site, you must install the Exchange 2000 version of the ADC (Active Directory Connector) first.
There are two versions of the ADC:

- Windows 2000 version: for connecting Exchange 5.5 to Active Directory
- Exchange 2000 version: does not support Exchange 5.5 co-existence

Internet Information Services (IIS)

The protocols supported by IIS are:

- HTTP – for Outlook Web Access clients
- SMTP – for SMTP clients
- NNTP – for access to news groups

The protocols supported by IIS with Exchange 2000 are:

- POP3 – for SMTP clients to retrieve messages
- IMAP4 – for SMTP clients to retrieve messages

N.B. *MAPI clients do not connect to Exchange 2000, they connect directly to the IS*.

NNTP

NNTP is required to be installed on Win2000 machines before you install Exchange 2000.
NNTP is used to access public folders on NNTP hosts.

LDAP

Exchange 2000 uses LDAP v3 as a message-based protocol to access directory services.
LDAP uses TCP port 389 by default, but queries the global catalog using TCP port 3268.
The following components use LDAP to communicate:

- DSAccess (Directory Service Access) uses LDAP to access Active Directory
- RUS (Recipient Update Service) uses LDAP to build address lists
- Exchange System Manager uses LDAP to view AD objects

Installing and Upgrading Exchange 2000 Server

Install Exchange 2000 Server On A Server Computer

Hardware and Software Requirements

Minimum	Recommended
Pentium-compatible 133MHz	300MHz
128MB RAM	256 MB
500MB of free disk space on installation partition	
200MB of free disk space on system partition	
CD-ROM drive	
VGA Monitor	

Page file should be increased to twice the size of the installed RAM.
NTFS is the recommended file system.

Extending Active Directory Schema and Configuration

The first installation of Exchange 2000 in the forest modifies the schema and configuration partitions of AD through the use of the /forestprep and /domainprep commands.

Added Groups and Permissions

There are two groups added by the Exchange 2000 installation:

- Exchange Domain Servers – contains all Exchange 2000 computers (Domain Global)
- Exchange Enterprise Servers – contains all *Exchange Domain Servers* groups (Domain Local)

The User account that is used to install Exchange 2000 is granted permissions to run the Exchange System Manager, and delegate permissions.

Security can be established at install for one of two options:

- Permissions compatible only with Windows 2000 Server – does not allow anonymous access to view group and user information
- Permissions compatible with pre-Windows 2000 servers – allows anonymous access to view group and user information.

It is extremely important that the following commands are run on the server before you install Exchange 2000 Server.

/forestprep

X:\setup\i386\setup.exe /forestprep
Function of /forestprep:

- Schema and configuration changes are made to AD.
- Allows AD preparation without actually installing Exchange 2000.
- Establishes Exchange Organization name.

Considerations:

- It's recommended that you install Exchange 2000 on the Schema Master so that AD changes can be made locally.
- The user account that runs /forestprep must be a member of the Schema Admins and Enterprise Admins groups.
- Organization name cannot be changed after running /forestprep.

Information required when running /forestprep

- Product Identification.
- Component Selection.
- Installation Type.
- Organization Name.
- Exchange 2000 Administrator Account.

/domainprep

X:\setup\i386\setup.exe /domainprep
Prepares the AD domain for Exchange 2000.
Function of using /domainprep:

- Creates *Exchange Domain Servers* domain global group.
- Creates *Exchange Enterprise Servers* domain local group.
- Grants permissions on the domain for these groups.
- Creates user account *EUSER_EXSTOREEVENTS* for use with script event host.

Considerations:

- User account that runs /domainprep must be a member of the Domain Admins group.

Information required when running /domainprep:

- Product Identification.
- Component Selection.

Recommended Order of Installation

1. Run /forestprep.
2. Run /domainprep.
3. Install the Exchange 2000 System Manager tools.
4. Create the Administrative Groups using System Manager.
5. Install Exchange 2000 on computers in the administrative groups.

Setup allows the installation or removal of the following components:

- MS Exchange Messaging and Collaboration Services
  - MS Exchange MSMail Connector
  - MS Exchange Connector for Lotus cc:Mail
  - MS Exchange Connector for Lotus Notes
  - MS Exchange Connector for Novell GroupWise
  - MS Key Management Service
- MS Exchange System Management Tools
  - MS Exchange Server 5.5 Administrator
- MS Exchange Chat Service
- MS Exchange Instant Messaging Service

Considerations:
The user account being used to install Exchange 2000 must be a member of the Exchange Administrator group, and a member of the local computer Administrator group.

Unattended Installation

Considerations:

- /forestprep and /domainprep are not supported in the unattended installation and must be run beforehand.
- .ini file can be encrypted for extra security.

Setup switches

Switch	Description
/createunattend *file_name*.ini	Creates .ini file
/unattendfile *file_name*.ini	Installs using .ini file
/encryptedmode	Used with /createunattend to encrypt .ini file
/showUI	Displays User Interface during unattended install.

Installing Exchange in a Clustered Environment

Requirements:

- Exchange 2000 must be installed on the same drive letter, folder, and shared storage device in the cluster.
- EXIFS drive letter must be the same on all nodes in the cluster (default is **M**:)
- The same components must be installed on all nodes in the cluster.
- A virtual server must be established before the cluster can be put into service.

The Cluster Administrator MMC can be used to create a Virtual Server by:

- Creating Exchange resources groups.
- Adding IP addresses, network names, and shared disk and by creating the Exchange System Attendant resources.

Mixed vs. Native Modes

- Mixed mode means there are Exchange 5.5 and 2000 servers in the organization.
- Native Mode means that there are only Exchange 2000 servers in the organization.
- Routing groups cannot span administrative groups in Mixed mode.
- Exchange 5.5 servers in the Administrative group will communicate with all other servers as if they were in a single Exchange Server 5.5 site.
- Exchange 5.5 servers will not recognize any other routing groups other than the one they are in.

Multilanguage Support

Additional language support can be installed by performing the following on all global catalogue servers in the domain:

1. Opening Control Panel | Regional Options.
2. Under **Languages setting for the** system, select the languages you require.
3. Restart the global catalogue server.

Organization Object Properties

The organization object is the top-level of your Exchange 2000 system objects. The following table describes the function of each of the tabs in the Property dialogue box of the Organization object:

Tab	Option	Function
General	Display routing groups	Displays routing groups
	Display administrative groups	Displays admin groups (disabled by default)
	Operation Mode	Mixed or Native Mode
	Change Operation Mode	Converts to native Mode
Details	Creation Date	Date the Organization object was created

	Last Modification	Date of last modification.
	Administrative note	Optional additional notes.
Security	Name	Users and Groups with permissions on Organization object. Click **Add** or **remove** to modify the list.
	Permissions	Permissions for the selected object. Click **Allow** or **Deny** to modify.
	Advanced	Configures specific permissions, auditing, and object owner properties
	Allow inheritable permissions to propagate to this object.	Allows or prevents inheritable permissions.

N.B. The Security tab is not available by default. To enable it, you must add the following registry value:
HKEY_CURRENT_USER\Software\Microsoft\Exchange\EXAdmin\ShowSecurityPage=dword:00000001 (enable) or 0 (disable)

Top Level Containers

The Organization object holds the following objects and their properties:

Container	Child Containers
Global Settings	Organization-Wide system settings, formats, etc.
Recipients	Recipient Policies, address lists, etc.
Administrative Groups	Administrative Groups defined for the Organization
Servers	Servers defined for the Organization
Connectors	SMTP, IMS, cc:Mail, Lotus Notes, etc, Connectors defined for the Organization.
Tools	Site Replication Services, track messages, monitor servers and connectors.

Making Bulk Changes to Active Directory

You can use either of the following to import and export data from AD:

- LDAP Data Interchange Format Directory Exchange (LDIFDE)
  - Can be used to add, delete, and modify objects
- Comma Separated Value Directory Exchange (CSVDE)
  - Can be used to only add objects

Considerations:

- New users are created with blank passwords.
- New users are disabled by default.

- The import file must contain the Distinguished Name (DN) of the object being added, modified or deleted, and the ChangeType (add, modify, or delete) for the operation being carried out.
- Attribute names are not case sensitive.

LDIFDE and CSVDE Command Line Parameters

Use the LDIFDE and CSVDE commands with the following parameters:

Ldifde –i –k –v –f *filename.ldf*
Csvde –i –k –v –f *filename.ldf*

The parameters used are categorized into four areas: General, Export Specific, Import Specific, and Credential.

General Parameters

Parameter	Purpose
-f filename	To specify the input or output filename
-s servername	To specify the server to bind to
-c FromDNToDN	To replace occurrences of FromDN to ToDN
-v	To enable verbose mode
-j	To specify the location of the log file
-t	To specify the port number. The default port number is 389
-?	To access online help

Export Specific Parameters

Parameter	Purpose
-d RootDN	To specify the root of the LDAP search
-r Filter	To specify the LDAP search filter
-p Search Scope	To specify the search scope
-l list	To specify the list of attributes to look for in an LDAP search
-o list	To specify the list of attributes to omit in an LDAP search
-g	To disable paged search
-n	To ensure that binary values are not exported

Import Specific Parameters

Parameter	Purpose
-I	To enable Import mode
-k	To ensure the import continues regardless of errors

Credentials Parameters

Parameter	Purpose
-a DN password	To use a different user ID and password when running the

	command, in distinguished name format
-b username domain password	To run the command as *username* and *domain password*, instead of the user currently logged on

Establishing Administrative Groups and Routing Groups

Administrative Groups

Administrative Groups define the areas of administrative control. It is possible to delegate control of an entire administrative group to one or more administrators.
Considerations:
You cannot move computers running Exchange 2000 between administrative groups.

Routing Groups

Routing groups are groups of Exchange 2000 servers that are connected by permanent network links. Messages travel between the routing groups by traveling over Routing Connectors. Routing Groups cannot span multiple Administrative Groups.
Considerations:
You can move computers running Exchange 2000 between routing groups as long as they are both within the same administrative group.
Exchange 2000 servers that are in the *same routing group* communicate directly with each other. Therefore, if messages being sent from one server to the other are sent directly, using SMTP, and are not scheduled, they are sent immediately.
Exchange 2000 servers can be in the same routing group if:

- They have a permanent, reliable, and direct connectivity between them.
- They belong to the same AD forest.
- They have permanent, direct SMTP connectivity to each other.
- They can connect to a routing group master (which maintains link data about all the servers in the routing group)

Exchange Servers that are *not in the same routing group* route messages using Bridgehead servers and connectors.

- Bridgehead Server - a server that has a connector to another routing group.
- Connector – routing groups can be connected using one of the following connectors,
    - Routing Group Connector
        - All bridgehead servers will use RPC to deliver messages between routing groups.
    - SMTP Connector
        - If all target bridgehead servers are running Exchange 2000, then SMTP will be used to deliver messages between routing groups.

- If *any* bridgehead servers are running Exchange 5.5, RPC is used to deliver messages between routing groups.

- X.400 Connector

The **Routing Group Connector**:

- Allows restrictions on the types of messages the connector transports.
- A delivery schedule can be configured for all messages, or messages over a particular size.
- The routing group connector does not allow for security as Exchange 2000 servers authenticate when they connect, but do not apply encryption.
- Encryption can be applied by using TLS on the SMTP virtual server.
- AD can be configured to require all communications to be secured using IPSec.

N.B. Messages transferred between Exchange 2000 servers are not sent in plain text, but are encapsulated in TNEF (Transport-Neutral Encapsulation Format).

Diagnosing And Resolving Failed Installations

There are many reasons why an installation would fail. Causes range from insufficient permissions for the account that is being used to install Exchange 2000 Server, to insufficient hardware, to media errors. To properly troubleshoot installation, you must first adhere to installation guidelines. A good whitepaper on installing Exchange 2000 Server can be found at the following link: http://www.microsoft.com/exchange/techinfo/administration/2000/Ex2000SETUP.doc

Upgrade Or Migrate To Exchange 2000 Server From Exchange Server 5.5.

A good whitepaper on upgrading from Exchange 5.5 to Exchange 2000 can be found at:
http://www.microsoft.com/exchange/techinfo/deployment/2000/InPlac55to2K.doc
and also at:
http://support.microsoft.com/support/exchange/content/whitepapers/upgradev27a.doc

Diagnosing And Resolving Problems Involving The Upgrade Process

A good whitepaper on troubleshooting and backing out of an upgrade from Exchange 5.5 to Exchange 2000 can be found at:

http://www.microsoft.com/exchange/techinfo/deployment/2000/UpgradeRecover.asp

Managing Coexistence With Exchange Server 5.5.

Coexistence between Exchange 5.5 and Exchange 2000 is done using the Active Directory Connector (ADC). The ADC allows the mailboxes in the Exchange 5.5 organization to be synchronised with the user accounts in the Windows 2000 forest. Information on understanding and deploying the ADC can be found here: http://www.microsoft.com/TechNet/prodtechnol/exchange/proddocs/ex2kupgr/deploy/d_03_tt1.asp
The ADC also allows the *Maintaining Common User Lists* between Exchange 5.5 and Exchange 2000 servers.

Maintaining Existing Connectors

The number of intra-organizational connectors has been reduced to include:

- Routing group connector
- SMTP connector
- X.400 connector

More information on migrating transports, connectors and hubs can be found here: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/exchange/proddocs/ex2kupgr/deploy/d_07_tt1.asp

Moving Users From Exchange Server 5.5 To Exchange 2000 Server

Follow these steps to move a mailbox from an Exchange 5.5 server to an Exchange 2000 server:

1. Start the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.
2. Right-click the user being moved, and then click **Exchange Tasks**.
3. In **Select a Task to Perform**, click **Move Mailbox**.
4. In the Move Mailbox pane, verify that **Current Mailbox Store** is the Exchange Server 5.5 computer and that **SERVER** name is the Windows 2000 server name. Choose the storage group and mailbox store where you want to move the user to.

More information on moving mailboxes between servers can be found at:

http://support.microsoft.com/support/kb/articles/Q259/7/12.ASP

Configuring The Exchange 2000 Active Directory Connector To Replicate Directory Information.

It is very important to ensure the correct deployment of Active Directory and directory replication. This functionality is one of the most troublesome areas when dealing with multiple-site organizations. The following paper provides in-depth information on Active Directory Integration and Replication.
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/exchange/reskit/ex00res/deploygd/part2/c05adint.asp

Diagnose And Resolve Exchange 2000 Active Directory Connector Problems.

When troubleshooting ADC problems, you should collect the following information to help diagnose the problem:

- Collect popup messages.
- Collect application logs.
- Get an overview of the forest and Microsoft Exchange Server 5.5 structure (topology).
- Note how many Connection Agreements and ADC servers there are.
- Note what problems the customers think they are having and why.
- Find out if there has been an access violation; collect Drwtsn32.log and User.dmp files.
- Where necessary, collect an LDP dump of the object that is having problems and the Connection Agreement that is responsible for replicating the object.

Performing Client Deployments

Clients include Microsoft Outlook 2000, Outlook Web Access, POP3, IMAP4, and IRC. You should be familiar with the installation of Outlook 2000, both as a Corporate and Workgroup installation, and as an Internet e-mail client. Further information on setting up Outlook 2000, and creating Outlook profiles can be found here:
http://support.microsoft.com/support/search/canned.asp?FR=1&R=d&H=Outlook%202000%20'How%20to'%20Guide&LL=ol20+or+exchange+or+ol20codekb&Sz=ol20setcfght

Configuring Client Access Protocols

Exchange 2000 supports several different clients:

- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transport Protocol)

- POP3 (Post Office Protocol, version 3)
- IMAP4 (Internet Message Access Protocol, version 4)
- LDAP (Lightweight Directory Access Protocol)
- NNTP (Network News Transfer Protocol)
- MAPI (Messaging Application Programming Interface)
- EXIFS (Exchange Installable File System)

N.B. MAPI and EXIFS are Microsoft proprietary standards. All others are Internet standards.

User Authentication Modes

Both POP3 and IMAP4 use the following authentication methods:

- Basic Authentication – using clear text, challenge/response
- Integrated Windows Authentication – using NTLM for non-Windows 2000 clients, and Kerberos v5 for Windows 2000 clients.

SSL encryption can also be configured to provide an encrypted channel through which client and server can communicate.

POP3 Capabilities

With POP3 you can list, download and delete messages only. Any other function must be performed on the client after the messages have been downloaded.
POP3 uses TCP port 110 to retrieve messages, and uses simple text commands when communicating with the server. POP3-SSL uses TCP port 995.

IMAP4 Capabilities

IMAP4 allows you to list, preview, download, flag, move messages between folders, and organize your messages on the server. IMAP4 supports the downloading of an entire message or a portion of it (e.g., an attachment), as well as commands to create, delete, and rename folders on the server.
IMAP4 uses TCP port 143 to retrieve messages, and uses more advanced commands when communicating with the server. IMAP4-SSL uses TCP port 993.

Configuring Outlook Web Access (OWA)

Outlook Web Access provides an HTTP-based interface through which Exchange clients can access their mailboxes using a web browser.
OWA provides the following benefits:

- Supports messages that contain embedded items and Microsoft ActiveX objects
- Supports public folders that contain contact and calendar items
- Supports multimedia messages

- Uses named URLs to reference items
- Supports front-end/back-end configurations
- Supports IE 3.x and higher, Netscape 3.x and higher.
- OWA and IE5 supports:
    - DHMTL and XML
    - Drag and drop functionality
    - Rich text formatting

OWA has the following limitations:

- No offline access
- No advanced security
- No advanced e-mail functionality
- No calendaring and group scheduling
- No task management

The following components are used by OWA:

- Active Directory
- Exchange 2000 Components:
    - Information Store
    - DSAccess
    - OLE DB provider for Exchange (ExOLEDB)
    - Directory Service to the IIS metabase (DS2MB)
- EXIPC
- IIS Components:
    - Metabase – to store configuration data.
    - W3srv – World Wide Web publishing service.
    - DAVEx – to render data to send to the client.
    - ExProx – acts as a protocol gateway when using Front-end servers.
    - Forms Registry – to store the OWA forms.

HTTP-DAV

HTTP-DAV is an extension of HTTP, and is used by OWA to access Exchange 2000 mailbox data.
HTTP-DAV provides the following functionality:

- Overwrite file protection
- Namespace management
- Property (metadata) access

HTTP Virtual Server

HTTP virtual servers, like all other virtual servers, require a unique IP address or TCP port to communicate, and they can provide the illusion of several different OWA servers to provide different configuration options.
HTTP Virtual servers are created by using the Exchange System Manager.

Security using OWA

Security measures can be put in place by using SSL encryption, or by placing a firewall between the OWA server (Front-end server) and the back-end server. Authentication can be achieved by:

- Anonymous Authentication – Supported by all clients, but not secure.
- Basic Authentication - Clear text, simple challenge/response authentication. It is more secure to implement with SSL to encrypt username and password.
- Integrated Windows Authentication – Non-Windows 2000 clients can be authenticated using NTLM; Windows 2000 clients can be authenticated using Kerberos v5 authentication.

Configuring Exchange 2000 Server

An Exchange 2000 server can be configured to perform several services for the organization, or it can be configured to provide one of many services. Types of servers include mailbox, public folder, gateway, virtual, Chat, and Instant Messaging. All of the above services can be simply installed as the only functioning service on the computer. One of the more advanced configuration options is *Front-end/Back-end Server* configuration.

Front-end/Back-end Server Configuration

Front-end/Back-end Exchange 2000 server configuration provides several benefits:

- Front-end servers can perform the encryption processing, leaving the back-end servers to process the client request.
- User profiles can all point to the one front-end server regardless of which back-end server hosts their mailbox.
- Using a Front-end on the network perimeter increases security, as it contains no mailbox or public folder data.
- It allows greater flexibility in scalability as front-end and back-end servers can be added, transparently to clients.
- When back-end servers are used with Windows 2000 Advanced Server's clustering capabilities, load balancing can be achieved.

Considerations:
HTTP, POP3, and IMAP4 clients are able to take advantage of Front-end/Back-end server configurations, but MAPI clients (i.e., Outlook) cannot, because they access the IS directly.

Front-End Servers

A front-end server is an Exchange 2000 server that does not host mailboxes or public folders in its Information Store. The Front-end server passes client requests to the back-end server for processing.
Front-end servers use the following ports to communicate:

Front-end service	TCP Port
POP3	110
POP3-SSL	995
IMAP4	143
IMAP4-SSL	993
SMTP (and SMTP-SSL)	25
NNTP	119
NNTP-SSL	563
HTTP	80
HTTPS	443
LDAP to Domain Controller	389
LDAP to Global Catalogue Server	3268
Kerberos	TCP port 88, UDP port 88
DNS Lookup	TCP port 53, UDP port 53
RCP port endpoint mapper	135
RPC service points	1024+
Netlogon	445

N.B. It is not necessary to open the AD domain controller ports if users are accessing their mailbox using Outlook Web Access.
The **alternatives to opening ports** are:

- Use a hosts file on the Front-end server to remove the requirement for DNS lookups.
- Edit the registry to specify the name of a domain controller and a global catalog server.

Back-end Servers

A Back-end server is an Exchange 2000 server that hosts at least one mailbox or public folder on its Information Store.
Detailed information on configuring Front-end/Back-end servers can be found at: http://www.microsoft.com/TechNet/prodtechnol/exchange/maintain/optimize/e2kfront.asp

Configuring information store objects.

The Information Store is made up of *Storage Groups*. Each Storage Group can contain multiple *Stores*.
There are two types of stores in Exchange 2000: mailbox stores and public folder stores. Each store consists of the following database files:

- Streaming Database file (.stm) – Contains MIME content.
- Rich Text Database file (.edb) – Contains data placed there by MAPI clients, as well as messages, folders and attachments.

Benefits of Multiple Message Databases

A single Exchange 2000 Server can contain multiple stores. Each store can contain a subset of the total mailboxes for the following reasons:

- Increased System Reliability.
- Faster and more flexible backups.
- Decreased recovery time.

N.B. Exchange 2000 Enterprise Server supports multiple mailbox stores per server, but Exchange 2000 Server supports only one mailbox store and multiple public stores.

Benefits of Storage Groups

Storage groups enable you to:

- Support more users per server through smaller storage groups.
- Backup and restore functions can effect a smaller number of users.
- Each company/department can have its own storage group.
- Provide individual support to critical mailboxes by creating its own store.
- Use circular logging for non-critical stores.

Storage Group Limits

Exchange 2000 Server allows up to four storage groups per server.
Each storage group can support up to five stores, which have no size limit.

Creating Stores

You have several options when configuring new Storage Groups and Stores, the most important of which are:

- Zero out deleted database pages – automatically writes zeros (0) to deleted database pages during online backup.
- Enable circular logging – reduces hard disk requirements, but also reduces redundancy and recovery options.

To create a new store, right click on the storage group and select **New | Public Store** or **Mailbox Store**.
When you create a new store, you are able to enter various information into the properties page of the object, through the following tabs:

- **General** – Store name, associated public store (if applicable), offline address book, text type, and support for MIME clients.
- **Database** - Database file locations and online maintenance schedule.
- **Replication** (public store only) – Frequency of replication to other servers.
- **Limits –** Maximum store, mailbox, message age, message sizes and triggers for warning messages.
- **Full-Text Indexing**
- **Details** – Administrative notices, notes, etc.
- **Policies** – Associated policies.
- **Security** – Accounts and permissions associated to the store.

Moving Storage Groups and Stores

Any database can be moved by opening the properties page of the object, selecting the **database** tab, clicking the **Browse** button, and selecting a new location for the database. The database will be dismounted, moved, and mounted again automatically.

Deleting Stores

Stores can be deleted by right clicking on the object and selecting **delete**.
Considerations for deleting Pubic Stores:

- You cannot delete the only remaining public store.
- The store cannot be the default public store for any mailboxes.
- Any public folders containing system folders must have their contents relocated prior to deleting them.
- If the public store contains the only replica of a particular public folder, deleting that store will also remove the only copy of the public folder.

Transaction Log Files

Server activity is recorded in Transaction Log Files, which are always 5MB (5,242,880 bytes) in size, and can be used to restore data. Logs that are not this size are most likely damaged.
Each log files series is stamped with a unique signature by the ESE, so that it can distinguish it from another series of log files.
By maintaining older log files, it is possible to apply the transactions within to bring an out-of-date database up-to-date.

Database Considerations

Plan stores so that they are a manageable size for backup and recovery purposes. Place all users that communicate with each other frequently in the same store so that you can take advantage of single-message delivery and storage.
Stores are best managed when part of a Storage Group, so that configuration options are applied only once to the entire group. Consider separate Storage Groups when you require different configuration options.

Configuring the Information Store

The following article describes the advantages and considerations for multiple storage groups for data partitioning, and configuring multiple databases within a single storage group.
http://www.microsoft.com/TechNet/prodtechnol/exchange/proddocs/ex2kplan/c07info.asp

Configuring Virtual Servers To Support Internet Protocols

Exchange 2000 supports Virtual Servers:

- Each virtual server has a unique name and IP address
- Allows for different client connection configuration options
- Allows for different Authentication methods.

Virtual servers can be used to send and receive Internet mail on one network adapter configured as one virtual server, and a second network adapter can be configured to send and receive mail on the local network. This is not as secure as using a firewall though, as the Exchange Server is connected directly to the Internet.
Filters can be applied to Virtual Servers to filter specific types of messages as they pass through the interface. This can be used to filter out messages that have no reply address, messages from specific domains or users, etc. Filters can be applied to the IP address assignments though the **Filters** tab of the **Message** Delivery object property page, under **Global Settings**.
You can limit the number of incoming SMTP **Connections** any virtual server can have. The default limit is 1000 outbound, and unlimited incoming connections.
It is very important to note with virtual servers that it is good practice to always use the Exchange System Manager to make any configuration changes, rather than using the IIS MMC. When you use the Exchange System Manager, configuration changes are written directly to the Active Directory, and then synchronized periodically with the IIS metabase by the DS2MB service. If you make configuration changes using the IIS MMC, those configuration options may be over-written by the synchronization process.

SMTP Virtual Servers

SMTP Virtual Servers use four default system queues:

- Local Delivery – messages awaiting delivery to a mailbox
- Messages awaiting directory lookup – messages waiting to have their address resolved, or distribution list to be expanded
- Messages waiting to be routed – Messages waiting for their route to be determined
- Final Destination unreachable – messages that have exceeded the delivery period

Global SMTP Parameters

You can configure the following Global SMTP parameters:

- Internet Message Format – encoding, format, and types of messages to be sent to the Internet.
- Message Delivery options – filters that are applied to the SMTP virtual server.

Be aware that you can configure the following components of an SMTP Virtual Server:

- **Message Limits** – message size, SMTP session size, Number of messages per connection, and Number of recipients per message.
- **Message Delivery** – number of retries to deliver a message, time-out periods, and non-delivery periods.
- **Inbound Relay Restrictions** – authentication required before relaying is allowed, if you want to allow relaying at all.
- **Filters** – to specify specific types of messages, i.e., no reply address, etc.
- **Connection Settings** – number of inbound and outbound connections that can be made.
- **Message logging** – logging can be done in a variety of formats.

Exchange 2000 Server's relationship with the Windows 2000 Active Directory.

All Exchange 2000 Server information is stored in Active Directory.
An Exchange organization cannot span multiple forests.
A forest cannot contain more than one Exchange Organization.

Benefits of Integrating with Active Directory

- Centralized Object Management
- Simplified Security Management
- Creation of one distribution list (Security groups can be used as distribution lists)
- Active Directory Connector (ADC)

- Active directory is able to replicate updated attributes instead of the entire object.

Storage of Exchange 2000 Data in Active Directory

Active Directory information is partitioned into three areas.

- Domain Partition (recipient objects, users, groups, and computers).
- Configuration Partition (connectors, protocols, service settings and routing topology.
- Schema Partition (object types and attributes)

Instant Messaging (IM)

You should be familiar with the following functions:

- Configuring a user object for instant messaging
- Configuring a user object for Chat

Further information on deploying Instant Messaging and Chat can be found at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/reskit/ex00res/deploygd/part5/c19chat.asp
Instant messaging provides a real-time method of communication through user chat windows.
Users require an Instant Messaging client such as MSN Messenger, for both communication purposes and to establish the online status contact.
The status of a contact, referred to as *Presence Notification*, can be viewed as any of the following:

- Invisible – equivalent of appearing offline.
- Busy
- Be right back
- Away from the Computer
- On the phone
- Out to Lunch
- Online

Instant Messaging Components

Instant Messaging Home Server – Home servers of the user accounts.
Instant Messaging Router – Determines the route messages will take to reach the appropriate Instant Messaging Home Server
Instant Messaging Domain – The group of IM users and virtual servers.
Instant Messaging Transport and Message Format – Messaging takes place over HTTP using XML format for messages.
Rendezvous Protocol – Communication between clients is handled by the Rendezvous Protocol (RVP).

IM Dependencies on Windows 2000

Active Directory – Used to enable user accounts for IM.
Internet Information Services – IM clients connect to IIS to use the IM service.
DNS – The IM router uses DNS to lookup the "A" record to find the IM Server.
Be aware that you can configure a separate or unified namespace for the IM users; i.e., the user's contact address could be "Daniel@brainbuzz.com" (unified), or "Daniel@im.brainbuzz.com" (separate). This helps in establishing a separate contact address from the user's normal e-mail address.

Client Operations

Logon Process – requires a unique IM ID in the form of *user@domain*, and an AD username and password for authentication.
TCP Ports used – clients use TCP port 80 to establish a connection to the Home Server, then negotiate a >1024 port to listen for messages.
Contact Subscriptions – adding a contact to the IM client is referred to as a subscription.
Status Notification – all client status information is updated in the Node Database of their home server.

Server Operations

It is possible to create multiple IM routers to provide for the following:

- Scalability – one IM router can handle up to 50,000 clients.
- Fault Tolerance – to preserve IM routing if one router goes down.
- Multiple Instant Messaging Domains – there needs to be one IM router per Domain.
- Geographically Dispersed Instant Messaging Deployment – you should disperse IM Routers on each end of a slow link, and near Home Servers.
- Multiple Active Directory Forests – each AD forest contains a distinct IM Domain.

Scalability

Each Instant Messaging home server can handle up to 10,000 simultaneous users, and a single IM Router can handle up to 50,000 simultaneous users.
Further reading on Instant Messaging and presence monitoring can be found at:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/exchange/proddocs/ex2kplan/c11inst.asp

Configuring Chat objects.

Server Components

You can create an IM virtual server through the Exchange System Manager as either a Router or a Home Server.
IM supports both Integrated Windows and Digest Authentication.
The following describes the server components that make up an Instant Messaging domain:
Server Application Layer – performs AD lookups, performs presence notification, and communication with other IM components.
Node Database – an extension of the Extensible Storage Engine
Firewall Topology – when IM is used to communicate with clients outside the organization, or local network, security in the form of a firewall should be in place. Firewall topology can be configured using the *Global Settings* object within the Exchange System Manager.
Locator – works with the IM Router to determine the correct destination of IM messages.
Exchange System Manager – used to configure IM, home servers, and IM routers.

Client Components

Messenger Client User Interface (UI) – used to write, send, and receive messages.
Accounts – each IM user requires an account to use IM. Normally this is an AD account that has IM enabled through *Active Directory Users and Computers*. An account can also be a Hotmail or an MSN account.
Enabling a user automatically creates two URLs for the user:

- IM Home server URL
- IM Domain URL

The requirements for computers running IM are:

- Win9x (with Winsock 2.0), NT4 Server or Workstation, or Windows 2000
- Internet Explorer 5 (for proxy settings)
- MS Proxy Client 2.0 (to communicate outside of organization)
- MSN Messenger Service

Be aware that you can configure several registry entries on the local computer to change the look and feel of the IM client (i.e. banner space, default warning message, and default NTLM domain).

Configuring Virtual Servers To Limit Access Through Firewalls.

Smart Hosts

Smart Hosts are Exchange 2000 servers that are configured to perform the DNS lookups and to deliver messages on behalf of other Exchange 2000 Servers. Some reasons for using a Smart Host would be:

- Single entry and exit point for all messages for the organization.
- Can be used as a dial-up point for clients the periodically connect to collect their mail from the permanently connected Smart Host.

Relay Hosts

Exchange 2000 server can be configured as in incoming relay host for the following scenarios:

- Preventing Spam – by configuring specific computers, domains, or users that are allowed to use the server to relay.
- Relaying to other Domains – if you have multiple domain names within the organization, a relay host can accept messages for all domains, and relay to the specific destination host.

Creating And Managing Administrative Groups.

Administrative Groups are collections of Exchange 2000 objects grouped together for ease of management. They can include:

- Routing groups
- Public folder trees
- Policies
- Monitors
- Servers
- Conferencing services
- Chat networks

Single Administrative Groups

The installation of Exchange 2000 creates an administrative group called "First Administrative Group".
Administrative groups are hidden by default.

Multiple Administrative Groups

The main idea behind multiple administrative groups is to separate servers for administrative control.

Securing Administrative Groups

Permissions can be set either through the Exchange System Manager, or by using ADSIEdit.exe
Permissions applied to an object will automatically propagate to any new objects created below that object.
Permissions applied at the Administrative Group level can be applied to propagate to all objects within the group.

Configuring Separate Exchange 2000 Server Resources For High-Volume Access

Resources can include stores, logs, and separate RAID arrays.

Windows Clustering in Exchange 2000

Def. Two physically connected computers and a shared storage device.
Exchange 2000 supports *active/active clustering*. (i.e., all members of the cluster are online and able to accept client requests)
Further details about Windows Clustering can be found here:
http://www.microsoft.com/windows2000/library/howitworks/cluster/introcluster.asp

Diagnosing And Resolving Exchange 2000 Server Availability, Performance, and Growth

A whitepaper on Exchange 2000 server availability can be found here:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/exchange/reskit/ex00res/deploygd/part4/c14avail.asp

Using Monitoring And Status To Monitor Exchange 2000

To ensure that your Exchange 2000 servers and network is running properly, you can configure monitoring and status alerts for all the major components of Exchange. The Monitoring and Status tool consists of Notifications (e-mail and script) and Status (viewing of the state of connectors and services). Monitoring the status of connectors and services, and configuring notifications, can reduce the total downtime if there is a problem.

Monitoring Services

From the Exchange System Manager, expand **Tools | Monitoring and Status | Status**, and then double click on the server you want to monitor.
By default Exchange 2000 monitors and logs the status of the following services:

- Microsoft Exchange Information Store Service
- Microsoft Exchange MTA Stacks
- Microsoft Exchange Routing Engine
- Microsoft Exchange System Attendant
- Simple Mail Transport Protocol (SMTP)
- World Wide Web Publishing Service

You can add other services to the monitoring configuration, thereby generating a critical error if any of the monitored services stops running.
You can monitor the following resources:

- Available Virtual Memory
- CPU Utilization
- Free disk space
- SMTP Queue growth
- Windows 2000 service
- X.4000 queue growth

The various *Server Status* states are:

- Available – server is on-line
- Unreachable – one of the main server services is down.
- In Maintenance Mode – monitoring is disabled for maintenance.
- Unknown – cannot communicate with the server.

The various *Connector Status* states are:

- Available – connector is running
- Unavailable – connector is not running

Configuring Notifications

Configure notifications to produce e-mail or script alerts that trigger when the status of a monitored object changes. View and configure notifications in Exchange System Manager, expanding **Tools | Monitoring and Status | Notifications**.
You can configure the following notification parameters:

- Monitoring Server
- Servers and connectors to monitor
- State
- E-mail notifications
- Script notifications

Diagnosing and Resolving Server Performance and Growth

The following outlines the performance counters and objects that you can use to monitor the *various components of Exchange 2000*:

Object	Counter
MSExchangeIS	User Count
MSExchangeIS Mailbox MSExchangeIS Public	Send Queue Size Receive Queue Size Messages send/min Messages Delivered/min
SMTP Server	Local Queue Length Categorizer Queue Length Inbound connections current Messages Bytes Received/sec Message Bytes Send/sec
MSExchangeMTA	Messages/Sec Work queue length
MSExchangeMTA Connections	Queue Length
MSExchangeSRS (5.x replication)	Replication Updates/sec Remaining Replication Updates
MSExchangeIM Virtual Servers	Current Online Users Current Subscriptions Inbound SUBSCRIBE/sec
MSExchangeAL (recipient update service)	Address Lists Queue Length

Diagnosing And Resolving Server Resource Constraints

Resources include processor, memory, and hard disks. Using the performance monitor and notification, you can perform benchmark analysis of the Exchange 2000 server, and be alerted to potential problems before they escalate into availability problems.

The following outlines the performance counters and objects that you can use to monitor for *Disk Subsystem Bottlenecks*:

Counter	Object
LogicalDisk	% Free Space
PhysicalDisk	% Disk Time Disk Reads/sec Disk Writes/sec Current Disk Queue Length Avg. Disk Read Queue Length Avg. Disk Write Queue Length

The following outlines the performance counters and objects that you can use to monitor for *Memory Bottlenecks*:

Counter	Object
Memory	Committed Bytes Pages/sec Page Faults/sec
Page File	% Usage
Process	Page Faults/sec

The following outlines the performance counters and objects that you can use to monitor for *Processor Bottlenecks*:

Counter	Object
Processor	Interrupts/sec % Processor Time
Process	% Process Time/store % Process Time/inetinfo % Process Time/Isass % Process Time/mad
System	Processor Queue Length Context Switches/sec

The following outlines the performance counters and objects that you can use to monitor for *Network Subsystem Bottlenecks*:

Counter	Object
Network Segment	% Net Utilization
Redirector	Bytes Total/sec Network Errors/sec
Server	Bytes Total/sec Work Items Shortages Pool Paged Peak
Server Work Queues	Queue Length

The following article provides useful information on monitoring and maintaining and Exchange 2000 Server:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/reskit/ex00res/resguide/c29monit.asp

Configuring Exchange 2000 Server For High Security

Authentication

Clients are authenticated by Windows 2000 security (i.e., Kerberos Authentication, NTLM, or basic Authentication).

Kerberos Authentication

Exchange 2000 uses Kerberos v5 to authenticate Windows 2000 clients in the following scenarios:

- The Authentication of two Exchange 2000 SMTP servers in the same organization.
- Used by the global catalogue server to authenticate an Exchange 2000 server during an LDAP query.
- Used by OWA to authenticate users running IE5 or higher.
- Used by the Routing Group Master when authenticating to relay link-state information.

A Kerberos authentication session consists of the following messages:

1. **Kerberos Authentication Service Request** – The client requests a Ticket-Granting Ticket (TGT) from the Key Distribution Center (KDC).
2. **Kerberos Authentication Service Response** – The authentication service queries AD for the user object, then passes the Ticket-Granting Ticket (TGT) to the client.
3. **Kerberos Ticket Granting Server Request** – To access a resource, the client sends a request (with the TGT) to the Ticket-Granting Service (TGS) for a ticket to authenticate with the computer on which the resource resides.
4. **Kerberos Ticket Granting Server Response** – The TGS examines the TGT and the authenticator. Once validated, the TGS generates a service ticket to allow the client to authenticate with the computer on which the resource resides, and passes it to the client.
5. **Kerberos Application Server Request** – The client then passes the service ticket and the TGT to the computer on which the resource resides. The hosting computer decrypts both tickets, and generates an access token to the client for access to the resource.
6. **Kerberos Application Server Response (optional)** – The client has the option to request validation of the target server's identity. This is called *Mutual Authentication*.

Further details about Windows 2000 Authentication can be found here:
http://www.microsoft.com/windows2000/library/howitworks/security/kerberos.asp

Virtual Server Authentication

There are three levels of Authentication that you can configure for an *SMTP Virtual Server*:

- **Anonymous Authentication** – does not provide any security; anonymously authenticated users can access any resources the *IUSER_Computername* account can access.
- **Basic Authentication** – uses clear text to perform simple challenge and response authentication.
- **Integrated Windows Authentication** – for clients that use Windows 2000 and Internet Explorer 5 or higher. Uses Kerberos and offers the best security. Non-Windows 2000 clients use LAN Manager (NTLM) for authentication.

Exchange 2000 servers use Kerberos version 5 to authenticate when communicating between them.
You can configure both **Incoming** and **Outgoing** authentication options.
Reverse DNS can be configured to verify the sending host's IP address from its domain name, though this adds extra burden on the server.

Permissions

Permissions can be granted in two categories

- Exchange Administrator permissions
- Client permissions

Exchange 2000 uses the security model of Windows 20000 and AD to manage access to objects. Objects are secured by applying DACL (Discretionary Access Control List) and ACEs (Access Control Entries) to them on the **Security** tab of the objects property page.

The **standard** permissions used in Exchange 2000 are:

Permission	Description
Full Control	Full permissions on object
Read	View the object
Write	Make changes to the object
Delete	Delete the object
Read Permissions	View the security settings for the object
Change Permissions	Modify the permissions on the object
Take ownership	Take ownership of the object
Create children	Create child objects
Delete children	Delete child objects
List Contents	View the contents of the container

Read properties	View the properties of the object
Write properties	Modify the properties of the object
List object	View the object in a container

The **Extended** permissions used in Exchange 2000 are:

Permission	Description
Add PF to Group	Allows Public Folders to be added to a group.
Create Public Folder	Allows the creation of a PF
Open Mail send queue	Allows the viewing of the send queue
Read metabase properties	Allows the viewing of the metabase properties
Administer information store	Allows changes to the IS
View information store status	Allows viewing of the IS status
Receive as	Allows a recipient to receive messages as if they were another recipient
Send as	Allows a recipient to send messages as if they were another recipient

Permission Inheritance

Permission inheritance is enabled by default. Permissions applied to a parent object are applied consistently to all child objects.
Permission inheritance can be overridden by modifying the permissions on the child object, or clearing the **Allow inheritable permissions from parent object to propagate to this object** check box on the Security tab of the object's property page.

Delegating Permissions to Administrators

The Exchange Administration Delegation Wizard provides the ability to delegate Administrative permissions to a user or group. By right-clicking on a particular container, and choosing *Delegate*, you can delegation administrative permissions broken up into three roles:

- *Exchange Full Administrator* – Full administrative permissions on the container object, and its child objects.
- *Exchange Administrator* – Full administrative permissions, but not *Modify* permissions, for the container object and its child objects.
- *Exchange View Only Administrator* – View configuration information only.

N.B. In order to run the Delegation Wizard, you must have Full Administrator permissions at the Organization level.
You can also configure Exchange 2000 permissions using the **ADSIedit.exe** utility.

Delegating Permissions Manually

Permissions can be delegated manually to objects by making changes to the Security tab on the Properties page of the object.
Considerations:

- You must grant *at least* read permissions on any parent objects so that the child objects can be viewed.
- Send As and Receive As permissions are granted by default. To prevent this, you must add an explicit deny on the object's property page.

N.B. When using the Delegation Wizard, Send As and Receive As permissions are *not* granted by default.

Permissions Required for Administrative Tasks

In order to perform certain tasks in Exchange 2000, the administrator must have specific permissions depending on the task:

Tasks	Exchange 2000 Permissions	Windows 2000 group memberships
Create and delete mailboxes	View Only Administrator	"Allow" permissions to create objects in AD
Move mailboxes from 5.5 to 2000 server (same organization)	In Exch 5.5, Exchange Administrator In Exch 2000, Exchange Administrator	Domain Admins or Account Operators group
Create administrative groups	Exchange Administrator	
Configure routing groups and connectors	Exchange Administrator at the target site	
Configure global message formats or thresholds	Exchange Administrator	Administrator group membership on the local machine for SMTP operations
View message queues	View Only Administrator	Local Administrator group membership
Remove messages from queues	Exchange Administrator	Local Administrator group membership
Create System Policies	Exchange Administrator, and Write permissions on the object the policy will apply	

Encryption

Exchange 2000 supports Internet Protocol Security (IPSec) or Transport Layer Security (TLS) for point to point encryption.
Digital Signatures and Encryption can be implemented using Key Management Server.
Information on the following topics can be found at the link below:

- Configuring Exchange 2000 Server to issue v.3 certificates
- Enable Digest authentication for Instant Messaging.
- Configure Certificate Trust Lists.
- Configure Key Management Service (KMS) to issue digital signatures

http://www.microsoft.com/technet/prodtechnol/exchange/reskit/ex00res/resguide/c30scrty.asp?frame=true#c

Creating, Configuring, And Managing A Public Folder Solution

Public Folder Features

Exchange 2000 public folders provide the following features:

- E-mail enabled
- Multiple public folder trees
- Secure items in public folders
- Accessibility from the Web
- Accessibility from the file system
- Full-text indexing capabilities
- Referrals enabled by default

Creating Public Folders

By using Exchange System Manager: expand the **Organization | Administrative Groups | Administrative Group | Folders**, right-click **Public Folders**, select **new**, **Public Folder**.
By using the Outlook client: Expand **Public Folders**, expand **All Public Folders**. From the file menu, select **Folder | New Folder**.

Client Support for Top-Level Hierarchies

There are two types of top-level public folders. The *default* Public Folder, which is created when Exchange 2000 is installed, can be viewed by all MAPI, IMAP4, HTTP, and NNTP clients.
Any additional hierarchies that are created are considered *General-purpose* top-level hierarchies and are only accessible from standard MS applications like Word and

Excel, but must be mapped to as a network drive using IFS (Installable File System), WebDAV (Web Distributed Authoring and Versioning). These General-purpose hierarchies are not available to MAPI clients unless viewed as a web page.
Considerations:

- The default public folder is always replicated. General-purpose folders must be specifically configured to replicate.
- The default public folder tree is controlled using MAPI permissions (Owner, Editor, etc.), whereas general-purpose trees are controlled using Windows 2000 permissions.
- There can only be one MAPI top-level hierarchy, but there can be multiple general-purpose folder trees.
- The default public folder does not support searches down the entire tree, whereas general-purpose trees do.
- Default public folder tree folders are mail-enabled by default. General-purpose folders are not.

Configuring The Active Directory Object Attributes Of A Public Folder

Several configuration options are available from the following tabs on the property page of the Public Folder object:

Tab	Description
General	Folder Name and Description. Enable/disable read/unread information
Replication	Specifies Replica Servers, schedule, and replication priority
Limits	Age/store limits and deleted item retention period
Details	Administrative Notes
Permissions	Security permissions to the folder

Public Folder Security in Exchange 2000

Exchange 2000 uses the following principles to implement security:

- Access control can be applied to any resource or folder.
- Permissions to objects or folders can be assigned to users or groups.
- The ACL (Access Control List) uses the SID (Security Identifiers) of Windows 2000 users and groups.
- Deny permissions over-rule any other permission to the object.

Permissions applied to a folder will be inherited by the folders below it, just as they do in Windows 2000.
Folders will propagate the following properties to subfolders: Permissions, Replication, Limits, General, and Directory properties.
Exchange 2000 permissions are separated into four categories: Folder Rights, Message rights, Directory Rights, and Administrators Rights.

Unless you specifically configure a property for an object or folder, it will automatically inherit the properties and permissions of its parent folder.

Assigning Permissions through Outlook

Permissions can be applied, as **Roles**, to public folders using a MAPI client, such as Outlook 2000. The roles that can be assigned are:

Role	Grants Permission to
Owner	All rights to the folder.
Publishing Editor	Create, Read, Modify, Delete all items and files, and Create Subfolders.
Editor	Create, Read, Modify, and Delete all items and files
Publishing Author	Create and Read items and files, Modify and /delete items and files you create.
Nonediting Author	Create and Read items and files, and Delete items and files you create.
Reviewer	Read items and files only. The contents of the folder do not appear.
None	No permissions to the folder.

Configuring the Store Attributes Of A Public Folder

The public store contains sub containers with information on the following:

- Logons
- Public Folder Instances
- Public Folders (details on the number and location of folders and their contents)
- Replication Status
- Full-text Indexing

Public folders behave differently in Mixed and Native modes. The following outlines the differences:

Top-level hierarchy	Mixed Mode	Native mode
MAPI top-level hierarchy	Mail enabled by default. Cannot be disabled. Hidden from the Global Address list by default.	Mail that is disabled by default can be mail-enabled. If mail-enabled, defaults to visible in global address list.
General Purpose top-level hierarchy	Mail disabled by default. Can be mail enabled. If mail enabled, defaults to visible in GAL (Global Address	Mail disabled by default. Can be mail enabled. If mail enabled, defaults to visible in GAL.

	List)	

Configure multiple public folder trees.

Configuring additional public folders requires the configuration of additional public stores; i.e., one public folder per public store. You cannot span a public folder across multiple stores.

NNTP Services

NNTP is a Windows 2000 service designed to allow access to news groups, as well as hosting news groups for group discussions.
There are three main types of newsfeeds:

- Newsfeeds from outside the organization (i.e., from Usenet)
- Sharing news data with other NNTP servers in your organization
- Load balancing with other NNTP servers in your organization

NNTP Virtual Servers

Like all other Virtual servers, the NNTP virtual server requires a unique IP address or TCP port to communicate. The NNTP virtual server allows NNTP clients to access virtual directories, which can be made up of public folders, remote directories or file systems.
NNTP virtual servers use TCP port 119 for basic authentication, and TCP port 563 for SSL authentication.
You can configure the following security parameters on an NNTP virtual server:

- Authentication method
- Number of connections allowed
- SSL requirements
- Connectivity restrictions by computer, groups of computers, or domains
- Allowing Client and newsfeed posts
- Posting size

Creating Newsgroups

Newsgroups can be created by:

- MAPI clients creating a directory in a public folder.
- Using the Exchange System Manager.

Storing Newsgroups

Newsgroups can be stored on a local or remote location, in a public folder tree, or in multiple locations. It is advisable to:

- Store newsgroups on a high-performance disk volume or array.

- Store newsgroups in another public folder than the default public folder tree.

Troubleshooting NNTP Connectivity

You can troubleshoot NNTP connectivity by using the telnet command in the following syntax:

telnet *servername* 110

More information on configuring Public Folders as NNTP folders can be found at: http://support.microsoft.com/support/kb/articles/Q169/9/15.ASP

Configuring And Monitoring Public Folder Replication

Public folder replication is handled by different services:

- Public Folder directory objects are replicated by AD
- Public Folder hierarchies are replicated by the Exchange 2000 store
- The Administrator controls replication of the content of the public folder

A replica of a public folder is considered a separate instance of the contained objects. There is no master replica in Exchange 2000.

You can create a replica of a public folder by:

- Specifying the replica server on the **Replication** tab on the folder's property page.
- By clicking **All Tasks | Add Replica** from the Public Folder instances object.

Replication priorities are broken down to : **Not Urgent**, **Normal**, and **Urgent.**

The status of public folder replication can be viewed by:

- Opening the **Last Replication Message Received** tab on the **Replication** tab of the public folder's property page.
- Selecting the store in which the public folder resides, and clicking on the **Replication Status** container to display the status on the right-hand pane.

Exchange 2000 Public folder replication is a mail-based process. SMTP is the replication transport mechanism. It allows replicated instances of public folders to reside on Information Stores located on different physical LANs where e-mail may be the only connecting medium.

There are three main concepts relating to Exchange 2000 replication that are important to understand:

- Multiple Master Replication Model – is when changes can be made to one or more master replicas, and the changes will be replicated to all other instances.
- Public Folder Replication Transport Mechanism – is SMTP.
- Public Folder Replication Agent (PFRA) – is responsible for monitors for changes, additions and deletions.

Diagnosing And Resolving Public Folder Replication Problems

To keep track of the changes, the PFRA uses **Change Numbers** and **Time Stamps** to determine which copy of a message needs to be replicated.

- Change numbers are made up of a globally unique Information store identifier, and a server-specific *change counter*. Numbers are changed sequentially across the messages on that Information Store.
- Time stamps are used as a primary method of deciding which message is the most recent.

The **Backfill Process** is the process in which out-of-sync public folders resynchronize. This is done by the replica server comparing the change numbers on an update notification and comparing them to its own replica. When a discrepancy is found, a backfill request is sent.
Public folder policies can also be configured to define settings for the following:

- General – support of S/MIME signatures, display of text message format
- Database – defines the maintenance intervals
- Replication – defines replication intervals and message size limits
- Limits – sets storage and age limits, and deleted item retention
- Full-text Indexing – scheduled times for the index to be updated or rebuilt

More information on Public Folder replication can be found on the following whitepaper:
http://www.exinternals.com/Whitepapers/PFRepl.pdf

Configure And Manage System Folders

Share-Points and Permissions

Folder	Shared as	Permissions
C:\Program Files\Exchsrvr\Address	Address	Administrators and computer account – Full Control Everyone – Read
C:\Program Files\Exchsrvr*servername*.log	*Servername*.log	Administrators and computer account – Full Control Everyone – Read

Managing Recipient Objects

Recipient objects are users, contacts, groups, or public folders that have been mail-enabled.
There are three main types of recipients:

- User – can be either of the following:

  - Mailbox-Enabled User – is a user that has an Exchange 2000 mailbox and e-mail address
  - Mail-Enabled User – is a user that has a Windows 2000 authentication account, and an external e-mail address associated with it
- Contact – is a user that has neither a Windows 2000 authentication account, nor an Exchange Mailbox in that organization
- Group – can be a mail-enabled Windows 2000 security or distribution group

Mailbox Configuration

The following outlines the configurable options on the property page of a recipient object:

Tab	Relevant Properties	Usage
General	E-mail	Incoming e-mail address
Organization	Title	
	Department	
	Company	
	Manager	
	Direct Reports	
E-mail addresses	E-mail addresses	View, add, delete, and modify e-mail addresses for the recipient
Exchange Features	Instant Messaging	Enable or Disable
Exchange General	Mailbox store	Location of home store
	Alias	Alias for mailbox
	Delivery Restrictions	Size and schedule limitations
	Delivery Options	"Send on behalf of" options
	Storage Limits	Mailbox size limits and warning limits
Exchange Advanced	Simple display name	
	Hide from Address lists	
	Downgrade high priority mail to X.400	
	Custom Attributes	Custom administrator notes
	Protocol Settings	Enable or disable HTTP, IMAP4, or POP3 access to the mailbox
	ILS Settings	Location of user's ILS home server for NetMeeting
	Mailbox Rights	Access rights to the mailbox

N.B. Rich-text is disabled by default. Some mail systems cannot process Outlook Rich text and will package the entire e-mail and attachments into a Winmail.dat file.

Exchange Mailbox Permissions

By opening the mailbox Property page, choosing the *Exchange Advanced* page, and clicking *Mailbox Options*, you can add the following permissions:

Permission	Allows a user or group to
Delete Mailbox Storage	Delete the mailbox from the Store
Read Permissions	View the permissions for the mailbox
Change permissions	Modify the permissions for the mailbox
Take ownership	Take ownership of the object
Full Mailbox access	Open the mailbox
Associated external account	Used to specify an external account for a user that is external to the AD forest

N.B. On the property page of the *User* object, you can specify *Send As* permissions, although Exchange 2000 does not use the *Receive As* permissions located on the Security tab.

Moving Mailboxes

You can move mailboxes to any server running Exchange 2000 within the Active Directory forest. However, when you move the mailbox, the user object remains where it was created.
When moving mailboxes, single instance store is maintained as much as possible. If a copy of a message in the mailbox already exists on the target server, another will not be created. If no copy exists, one will be created.

Configuring A User Object For E-Mail

The following e-mail addresses can be configured:

- Custom Address
- X.400 Address
- Microsoft Mail address
- Simple Mail Transfer Protocol (SMTP)
- CC:Mail address
- Lotus Notes Address
- Novell GroupWise Address

N.B. The *Primary* mailbox will be the address that will appear in the recipient's "From:" field, and will be the address that any Replies are sent to.

Creating And Managing Address Lists

There are three types of address lists used in Exchange 2000: default, custom, and offline.

Default Address lists

Address Lists	Description
All Contacts	All mail-enabled contacts in the Organization.
All Groups	All mail-enabled groups in the Organization.
All Users	All mail-enabled users in the Organization.
Public Folders	All mail-enabled public folders in the Organization.
Default Global Address List	All recipients in the organization; i.e., all of the above.

Custom Address Lists

Custom address lists can be created based on field properties of recipient objects.
Any mail-enabled recipient object can be added to an address list.
Filter rules can be applied to decide which objects should be allowed membership, based on the following parameters:

Condition	Description
Starts with	Value must start with characters specified
Ends with	Value must end with characters specified
Is (exactly)	Value must be match value specified.
Is not	Value must not match value specified
Present	Selected field must contain value specified.
Not Present	Selected field must not contain value specified

LDAP searches can also be used to define recipients to be included in the Custom Address List.
N.B. The LDAP query must conform to RFC 2254.

Offline Address Lists

By default all lists can be downloaded and used offline as a local copy. Offline address books have an .oab extension.
Right clicking on the Offline Address List container and choosing New | Offline Address List can create new Offline Address Books.
Offline address lists are show in the following order:

- GAL to which the user has access
- GAL of which the user is a member
- GAL that is the largest

Modifying Full-Name Auto-Generation Of Display Names

By default, display names are shown as:
First, Last
Editing the **createDialog** property of the **user-display** or **contact-display** object in AD can change this.

Diagnosing And Resolving Recipient Update Service Problems

RUS is responsible for building and maintaining address lists, and runs as part of the System Attendant service.
The RUS regularly polls AD (every one minute by default) and checks for changes that it uses to update the address lists.
The address lists can be manually updated by right clicking the address list and choosing **Update Now** (updates changes only) or **Rebuild** (rebuilds the entire list).
Further reading on working with Groups, Lists, and Templates can be found at:
http://www.microsoft.com/TechNet/prodtechnol/exchange/maintain/monitor/c05x2kad.asp?frame=true

Monitoring and Managing Messaging Connectivity

Monitoring Tools

The following tools are used to monitor the performance and status of Exchange 2000:

- *Performance MMC* – Comprises the System Monitor and Performance Logs and Alerts.
- *Monitoring and Status* – Use notification to set up scripts and e-mail notifications, and use Status to configure warnings and critical states.
- *Event Viewer* – provides event information about applications, directory services, file replication service, security, and system components.
- *Diagnostic logging* – used to monitor connectors, and other system components, then viewed through Event Viewer.
- *Protocol logging* – IIS allows detailed logging of messages sent and received by the SMTP protocol.

Additional tools for more specific monitoring are:

- *Queue Viewer* – allows viewing of transport protocol queues installed.
- *Message Tracking Center* – monitors the path a message takes.
- *Network Monitor* – Windows 2000 tool to capture, display, and analyze network traffic.
- *Network Diagnostic Tool (netdiag)* – Windows 2000 tool to diagnose network and connectivity problems through the command line.

- *Task Manager* – allows the viewing of running services and processes on the local machine.
- *HTTPMon* – Windows 2000 Resource Kit tool that provides real-time monitoring of Web site availability.
- *Windows Management Instrumentation (WMI)* – the MS implementation of Web-based Enterprise Management (WBEM), which provides uniform access to management information.

Using Performance Monitor

Performance Monitor is made up Performance Logs and Alerts and System Manager, and can be used to monitor a system over a period of time to produce data on the running of a specific component, or the entire system.
You can use Performance Logs and Alerts to:

- Configure real-time alerts on object counters.
- Configure and view real-time analysis of a server.
- Plan for the future capacity requirements or perform trend analysis.

The System Monitor can be used to:

- View server activity during times of performance degradation.
- Perform analysis of processor activity and queues.

Exchange 2000 Performance Objects and Counters

Exchange 2000 installs its own set of performance objects and counters to provide information about the services and processes that are running on the system. It is important to have an understanding of what objects and counters can be monitored to gather appropriate data about the system.

Managing And Troubleshooting Messaging Connectivity

Message Flow Architecture

Each component of Exchange 2000 has a function in the message flow architecture.

- Information Store – is the end point for messages, and the start point for messages sent from connected MAPI clients
- EXIPC – the Exchange InterProcess Communication provides the queuing layer and allows IIS and the store process to move data between each other.
- IIS – provides the protocol engine, and allows for such functions as Virtual Servers.
- Advanced Queuing Engine – defines and manages the queues. The Advanced Queuing Engine gets destination information from the Message Categoriser and routing information from the Routing Engine.
    - Message Categoriser – performs advanced address resolution, and *bifurcation* for RTF and MIME clients.

    - Routing Engine – creates and maintains link state information.
- SMTP – Processes incoming traffic from SMTP clients.

Intraserver Message Flow

Messages to users on the same server are received by the Information Store, passed to IIS for processing, and then passed back to the Information Store for delivery.

Outbound Message Flow

Messages bound to users on another server are received by the Information Store, and passed to IIS, which routes it through SMTP.

Outbound Messages to X.400 Recipients

Messages bound for external X.400 recipients are placed in the MTS-OUT folder, where they are processed by the MTA and delivered to their next hop.
The **X.400 Connector** can be used:

- When there is a slow or unreliable connection between the routing groups.
- When using X.25 as the connection medium.

Inbound Message Flow

Inbound messages are received by SMTP and processed by IIS before being passed to the Information Store for delivery.

Inbound Messages for X.400 Recipients

Messages are received by the MTA and placed in the MTS-In folder before being picked up by the Information Store for delivery.

SMTP

SMTP is the standard protocol for transmitting messages between TCP/IP hosts. It uses port 25 to send and receive messages.
SMTP message transfer is reliant on DNS to resolve the destination FQDN (Fully Qualified Domain Name) to an IP address.
The DNS server entry that represents a mail-exchange is an MX record. You must have at least one MX record on your DNS server to resolve each SMTP address used in your Organization. For example:

Record	Preference	SMTP host
MX	10	smtp.brainbuzz.com

SMTP Connector

The **SMTP Connector** can be used in the following scenarios:

- The other side of the connector is an IMS on a Exchange Server 5.5 (or earlier) site
- You require a *pull* relationship between the servers
- You want to define SSL or other security parameters at the connector level
- You require TLS security on the connector

Exchange 2000 Servers that are within the same routing group use SMTP to communicate.
Bridgehead servers use SMTP connectors to:

- Define the route, over other bridgehead servers using SMTP connectors that a message must take to reach the destination address space.
- Relay messages to other domains.
- Configure security for specific domains.

At a minimum, you must specify a name for the SMTP Connector, its address space, the connecting bridgehead server, DNS, local Bridgehead, or Smart Host.
Exchange 2000 SMTP uses three folders as queues to store messages during transfer. These folders can be found in *C:\Program Files\Exchsrvr\Mailroot.*
The three folders are:

- Pickup – used by IIS SMTP for mail delivery. Not used by Exchange 2000.
- Queue – used for inbound mail.
- Bad mail – used to store undeliverable mail.

To change the location of these folders, you must use ADSI Edit to modify the configuration partition of AD.

Delivery Options

You can configure the SMTP connector to deliver SMTP messages based on the following parameters:

- Message Delivery Schedule
- Queuing messages for later delivery
- Message Restrictions
- Outbound Security
- Relaying to other domains
- Limiting the domains that the connector can be used to deliver to

Using SMTP Connectors for Load Balancing and Fault Tolerance

Using multiple connectors can provide load balancing and fault tolerance by specifying the cost associated with each connector, and the DNS MX record preference for delivery.

Fault Tolerance and Load Balancing using Multiple Bridgehead Servers

Configuring multiple bridgehead servers between routing groups provides the following:

- Using two bridgehead servers to a routing group, if one goes down the other can be used.
- Exchange 2000 randomly chooses the connector to use if they both have the same cost. This provides load balancing.

Diagnosing And Resolving Routing Problems

Route Selection

When deciding on a message route, Exchange 2000 first determines which of the connectors meet the following criteria:

- The message does not exceed any restrictions on the connector (size, schedule, priority, etc)
- All the connectors in the route have a status of UP
- Which destination connector has the closest match to the destination address space (i.e., brainbuzz.com or *, brainbuzz.com would be chosen)

Of the remaining connectors on the message route, Exchange 2000 will then choose the route with the least cost.
If multiple routes exist between routing groups in an organization, the link-state table is used to determine the best route based on connection cost and link status.
When sending a message outside of the organization, Exchange 2000 may route the message across multiple routing groups to reach an external routing connector.

Routing Group Master

The *Routing Group Master* maintains a master copy of the link state information for the routing group. All changes are propagated over TCP port 691
The Routing Group Master is, by default, the first server added to a routing group, although you can change this through the Exchange System Manager console.
If the Routing Group Master fails, the administrator must designate a new one.

Link Status

Each Exchange 2000 server maintains a *Link-State* table, which contains information about all the other connectors in the organization, and their status.
Each link has one of two states: UP or DOWN.
Each link has a cost associated to it, which is used when calculating the best route to the destination.
N.B. You can use the *WinRoute* utility (included in Exchange 2000) to view the link-state table.

The *Link State Algorithm* is used to maintain the status of all connectors and propagate this information to other Exchange 2000 Servers.
Link-state information is propagated between routing groups over TCP port 25.

Troubleshooting SMTP Connectivity

Message non-delivery can be the result of bad connectivity to the destination host. You can use the following tools to test connectivity:

- Telnet – can be used to physically connect to the destination host, e.g. Telnet *fully_qualified_domainname_of_the_host* 25
- NSLookup – to verify the MX records to the host exist and are correct, e.g. Nslookup –querytype=mx *domainname*

Further reading on Message Routing can be found at:
http://www.microsoft.com/TechNet/prodtechnol/exchange/reskit/ex00res/deploygd/part4/c16route.asp
You must be familiar with interpreting the information provided in Non-Delivery Reports (NDRs). Several documents can be found on the Microsoft Knowledgebase related to many NDRs.

Managing Messaging Queues For Multiple Protocols

Exchange 2000 message queues can be viewed and monitored by:
Clicking **Start**, **Programs**, **Microsoft Exchange**, and then click **System Manager**.

To locate SMTP queues, use the following path:

> Servers/*Server*/Protocols/SMTP/SMTP virtual servers/*SMTP virtual server*/Queues/*Queue*

To locate X.400 queues, use the following path:

> Servers/*Server*/ Protocols/X.400/Queues/*Queue*

To locate Messaging Application Programming Interface (MAPI) system queues that are associated with connectors such as Microsoft Exchange Connector for GroupWise, Microsoft Exchange Connector for Lotus Notes, Microsoft Exchange Connector for Lotus cc:Mail, use the following path:

> Connectors/*Connector*/Queues/*Queue*

If you can view the routing groups or Administrator groups in the Exchange System Manager, you must browse through these objects to reach Queue Viewer.

Monitoring Link Status

Working With Failed Links

Once Exchange discovers that a link is failed, it must reroute all messages via a different link, and attempt recovery of the failed link. You should have a good understanding of the process involved in each of these scenarios.
Q263249 - XCON: Link State Routing in Exchange 2000 Server
If all routes to a routing group are unavailable, the messages are held in that routing group in the local message queue, until the timeout period has expired.
While a connection between two routing groups is down, the local bridgehead server will continue to test the connection at retry intervals configured on the Virtual Server.

Monitoring Messages Between Exchange 2000 Systems And Foreign Systems

Message Tracking

Message tracking can be enabled on the General tab of the Exchange Server's property page, or by using a system policy.
Message tracking can record information about the sender, the message, the recipient, and the subject line of the message.
The message tracking log is stored in a shared directory and is named *servername*.log. The location of this file can be edited in the registry.
N.B. If a message passes through a server that does not have message tracking enabled, the audit trail will end there. No more information about the message route will be recorded.

Configure And Monitor Client Connectivity

Clients include Outlook 2000, Outlook Web Access, POP3, IMAP4, and IRC.

Diagnosing And Resolving Client Connectivity Problems

Problems include DNS structure, server publishing structure, DS Proxy/DS Access, address resolution, Instant Messaging clients, various connection protocols, and non-Windows 2000 environments.
You should be familiar with various techniques for determining connectivity problems. Some of these techniques are outlined in the following KB article:
http://support.microsoft.com/support/kb/articles/Q174/7/01.ASP

Logging and Viewing Diagnostic Data

Diagnostic logging levels are configured within the Exchange System Manager, and results are viewed via the Event Manager.

Logging Diagnostic Data

Exchange 2000 allows various levels of diagnostic logging for services to provide trend analysis and troubleshooting data for those services.
The following components can be selected for diagnostic logging:

Service	Description
IMAP4Srv	Enables users to access mailboxes and public folders by using IMAP4.
MSExchangeAL	Enables users to address e-mails messages using address lists.
MSExchangeIS	Enables access to IS
MSExchangeMTA	Provides services to X.400 connectors
MSExchangeSA	Record an entry when Exchange 2000 uses Active Directory to store and share directory information.
MSExchangeSRS	Records an entry whenever Site Replication Service is being used to replicate data from Exchange 2000 to 5.5
MSExchangeTransport	Records an entry when a SMTP is used to route messages.
POP3Svc	Records and entry when a POP3 client accesses e-mail.

You can set the Diagnostic Logging to the following levels:

Level	Description
None	Logs only error messages
Minimum	Logs warning messages and error messages
Medium	Logs informational messages, error messages, and warning messages
Maximum	Logs troubleshooting messages (more detailed information), error messages, warning messages, and information messages.

All diagnostic logging messages are entered into the Windows 2000 Event Logs. The various messages are broken down in to three categories:

- Information – Signify normal system operations
- Warning – Signify minor problems or inconsistencies that may cause problems in the future
- Error – Indicates a possible service failure or impending shutdown of a service.

Protocol Logging

You can log protocol information by selecting the appropriate Virtual Server from the **Protocols** container, opening the Property Page, then select **Enable Logging** on the General tab.
You can monitor NNTP and SMTP protocols.

Monitoring Services Use

Services include messaging, Chat, public folder access, Instant Messaging, and calendaring.
Further reading on all the services that can be monitored in Exchange 2000 server can be found at:
http://www.microsoft.com/technet/prodtechnol/exchange/reskit/ex00res/resguide/c29monit.asp?

Manage Recipient And Server Policies

A Policy is a collection of configuration settings, which can be applied to one or more objects of collection of objects.
A *System Policy* is a collection of configuration settings that you can apply to a mailbox store, a public store or a server.

Managing Policies

You can perform the following tasks on existing policies:

- **Delete** – to remove a policy from the server and any objects to which it has been applied. Settings applied by the policy remain.
- **Copy** – to create a new policy identical to the original.
- **Rename** – to rename the policy

Applying Policies

To apply a policy, right click on the policy object and add the required objects. Policy settings take effect immediately; users do not need to refresh or log off.
Default e-mail addresses are configured when Exchange 2000 is installed. To add additional e-mail addresses, such as a CC:Mail address, a recipient policy can be applied to the group of mailboxes that require them.
It is possible to create multiple recipient policies with their own e-mail addresses. Applying a policy to a group of recipients is a quick method of applying an e-mail address format.
When you create a Recipient Policy, you must define a search criteria that defines which mailboxes the policy will apply to. Some of the parameters you can define are:

- Primary and Secondary addresses
- By creating a custom LDAP query

Recipient policies are ordered according to their priority, so when two policies conflict, the one with the higher priority takes precedence.

Mailbox Store Policies

You can configure a mailbox store policy to over-ride some of the configuration options defined on the mailbox itself.
On the Mailbox **General** tab:

- Default Public Store
- Office Address List
- Archive all messages sent or received by mailboxes on this store
- Clients support S/MIME signatures
- Display plain text messages in a fixed font size.

On the Mailbox **Database** tab:

- Maintenance Interval

On the Mailbox **Limits** tab:

- Issues warning at *kilobytes*
- Prohibits at *kilobytes*
- Prohibit send and receive at *kilobytes*
- Warning message interval
- Keep deleted items for (days)
- Keep deleted mailboxes for (days)
- Do not permanently delete mailboxes and items until the store has been backed up.

On the mailbox **Full-text Indexing** tab:

- Update interval
- Rebuild interval

Diagnose and resolve problems that involve recipient and server policies.

An object can only have one policy applied to it at any one time. If two policies contain conflicting settings for an object, you are asked to decide which policy applies.
Further information on configuring recipient policies can be found at:
Q249299 - XADM: *How to Configure Recipient Policies in Exchange 2000 Server*

http://support.microsoft.com/support/kb/articles/Q249/2/99.ASP
Further information on configuring system policies can be found at:
Q256141 - XADM: *How to Create System Policies in Exchange 2000*

http://support.microsoft.com/support/kb/articles/Q256/1/41.ASP

Optimize Public Folder And Mailbox Searching

Configure the public folder store or mailbox store for full-text indexing.

Exchange 2000 supports full-test indexing (or context indexing) to provide linear search and performance capabilities.
Benefits of Full-Text Indexing:

- Faster Searching
- Searching of Attachments
  - Word (*.doc)
  - Excel (*.xls)
  - PowerPoint (*.ppt)
  - HTML (*.html, *.htm, *.asp)
  - Text Files (*.txt)
  - Embedded MIME Messages (*.eml)
- Normalized Searching.
- Individual Store Configuration.

Considerations for Full-Text indexing:

- There is considerable time and CPU resources required to index.
- Indexing can take up to 20% of the database being indexed. (i.e. a 1GB database will require 200MB free space to index)
- Searches on an index that has not completed can provide unpredictable results.
- Full-text indexing does not index all properties of each document; it only indexes the address fields, subject and body.

Creating an Index

Indexes can be created by right clicking on the store to be indexed and selecting **All Tasks | Create Full-Text Index**.
Options provided on the *property* page of the index include:

- Update interval
- Rebuild interval
- This index is currently available for searching by clients

Right clicking the index and selecting **All Tasks** provides the following options:

- Start Incremental Population – finds only new or modified information
- Start Full Population – completely rebuilds the index
- Pause Population
- Stop Population
- Delete Full-Text Index

Troubleshooting Full-Text Indexing

Use the following tools to troubleshoot Full-Text indexing:
Gather Files record errors found during indexing. These files exist in the :\Program Files\Exchsrvr\ExchangeServer\Gatherlogs folder, with a .gthr extension. The error numbers recorded can be decoded using the **Gthrlog.vbs** utility found in the :\Program Files\Common Files\System\MSSearch\Bin folder.
The **Application Log** records all errors and information messages according to the logging level specified on the store.
The **System Monitor** can be used to determine the resource usage indexing takes on your systems, and to identify performance bottlenecks.

Restoring System Functionality and User Data

Apply a backup and restore plan

For complete recoverability, you should ensure to backup the following databases:

- Information Store Database
- Site Replication Service Database
- The Key Management Server (KMS) database

It is also advisable to make a System State backup for Windows 2000, which captures the following information:

- Active Directory configuration
- Local system registry
- IIS metabase

Comprehensive information regarding Exchange 2000 Server backup and recovery techniques can be found at:
http://support.microsoft.com/support/exch2000/whitepapers/e2kdbrecovery.doc

Recovering Deleted Mailboxes

Comprehensive information regarding mailbox recovery techniques can be found at:
http://www.microsoft.com/exchange/techinfo/deployment/2000/MailboxRecovery.doc

Configure A Server For Disaster Recovery

File Location Considerations

You should keep the transaction logs and database files on separate physical hard disks for the following reasons:

- Increased performance as the disk heads can read and write to both sources at the same time.

- Increased redundancy. If the disk the databases are being stored on fails, you can recover from the transaction logs.

The best performance is normally obtained with a hardware mirror array (RAID0)
Storage group databases should be stored on:

- Drives formatted with NTFS.
- Drives configured in a RAID configuration.
- Distribute the drives across multiple SCSI channels (if possible) but configured them as a single logical drive.

Circular Logging

Circular logging is disabled by default in Exchange 2000.
Circular logging can be used to overwrite older transaction logs after a period of time.
N.B. You should use circular logging if recovery is not important; e.g., on a front-end server which contains no mailbox or public folder data.

Special thanks to
Daniel Johns
for contributing this
Cramsession.