Chapter 1

Getting to Know Exchange Server 2007

If you are reading this book, then chances are good that you are getting ready for a migration from an earlier version of Exchange Server to Exchange Server 2007. Let’s face it, Exchange 2007 is pretty intimidating at first glance. When I got my first glance at it in December 2005, many of the features — such as the Exchange Management Shell, messaging records management, transport rules, continuous replication, and the requirement for 64-bit Windows — kind of stressed me out.

Now when people ask me about Exchange Server 2007, I tell them, ‘‘It’s different, but in a good way.’’ There are quite a few changes and differences that we need to get used to. There are certainly some changes that I didn’t like initially, but now I’m used to them and understand why they were made.

In this book, I am assuming that you are an Exchange 2000 or Exchange 2003 administrator and looking for the differences and changes that you need to know about to get you up and running on Exchange 2007. I am going to avoid a lot of the fluff, such as ‘‘how to configure DNS,’’ ‘‘what a public folder is,’’ or ‘‘how SMTP works,’’ and just focus on relevant changes and how you can take some of the new features of Exchange 2007 and apply them quickly to your organization.

In the first chapter, I want to introduce you to the changes that have been introduced by Exchange Server 2007 as well as Service Pack 1 for Exchange 2007. Specifically, I will focus on the changes that will help you transition your knowledge of Exchange 2000 or 2003 to Exchange 2007. The following topics are included:

- Completely new features
- Improvements to existing features
- Things you need to know before upgrading
- Exchange Server 2007 administration
- Hardware and software requirements

New Exchange Server 2007 Features

When people ask me to name the single most important or compelling feature of Exchange 2007 that would make them want to upgrade, I generally don’t have a single feature answer. However, Exchange Server 2007 is a compelling upgrade when you take a look at the product as a whole. There are many valuable new features that can help you make your users more productive, improve availability and reliability, reduce spam, improve security, and give you more flexibility in managing Exchange.

Many people wait until the first service pack before they deploy a new version of anything. The release to manufacturing (RTM) build of Exchange Server 2007 was a fairly stable release, but Service Pack 1 introduced improvements to the management interface, made usability improvements, and added new features.

Improvements to the Administrative Interface

The administrative interface for Exchange Server 2007 has been so completely reworked that it really does deserve to be called a new feature. The underlying architecture of the Exchange Management Console is based on extensions to the Windows PowerShell; these extensions can be accessed either directly from the Windows PowerShell or, if you are a developer, using the .NET Framework.

The management of servers, recipients, and global settings is now handled differently than it was in Exchange 2000/2003. The concept of an administrative group is going away, and there are new ways to delegate server administrative permissions as well as management of organization settings.

The improvements to the administrative interface are so extensive, in fact, that I am going to devote an entire chapter (Chapter 2, ''Exchange Server 2007 Administration'') to the new interface and an entire chapter to getting to know the Exchange Management Shell (Chapter 7, ''Exchange Management Shell Primer'').

Continuous Replication

If I had to pick the most compelling collection of features in Exchange Server 2007, it would be continuous replication. This new technology supports three flavors of replication from the ''active'' data source to a passive data source.

Continuous replication comes in three flavors. For stand-alone Mailbox servers, there is local continuous replication, which allows you to keep a replicated copy of one or more mailbox databases on the local server. If you want high-availability replication, there is cluster continuous replication, which keeps a replicated copy of the active databases on the passive node of the cluster. Exchange 2007 Service Pack 1 introduced standby continuous replication, which allows you to keep copies of one or more databases from one or more mailbox servers.

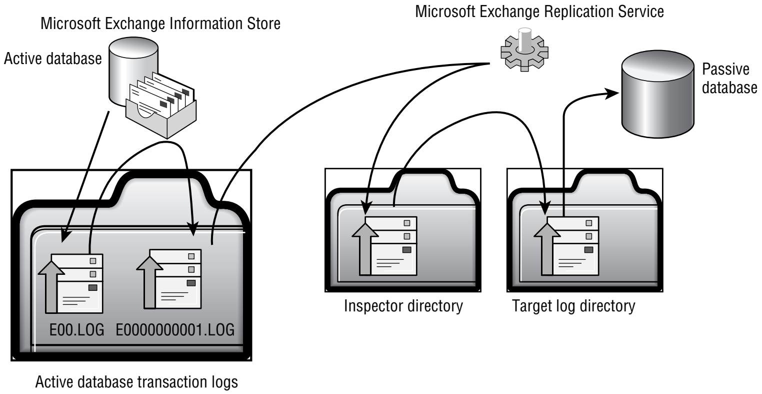
How Continuous Replication Works

Unlike many tools from third-party vendors that replicate data either at the disk block level or by taking snapshots of the disk and replication changes, Exchange continuous replication is more similar to the SQL Server *log shipping* technology. This is considered a *pull* model. The active Exchange database, logs, and database engine do not even realize they are being copied. The Microsoft Exchange Replication Service (`Microsoft.Exchange.Cluster.ReplayService.exe`) handles copying the logs and managing the passive databases.

Initially (as when continuous replication is set up or reconfigured), the current copy of the database is copied to the passive location; this is called *seeding*. As an Exchange transaction log is filled up and renamed, (i.e., when the `E00.LOG` file is filled and then renamed `E000000001.log`), the renamed log file is copied to the passive location. The replication service then verifies the log file and commits it to the passive copy of the database. So the actual database file is not replicated at all, but it is kept in sync because the the log files are copied and replayed.

You will probably understand this concept better with an illustration. Figure 1.1 shows an example of how this process works. The Exchange database engine is run by the Microsoft Exchange Information Store; transactions fill up the current transaction log (`E00.log`). The transaction log file (`E00.log`) is renamed with the next available transaction log filename (in this case, `E0000000001.log`). All of this is handled by the Information Store service.

FIGURE 1.1 Example of how continuous replication works


Microsoft Exchange Information Store
Active database
Microsoft Exchange Replication Service
Passive database
E00.LOG
E0000000001.LOG
Inspector directory
Target log directory
Active database transaction logs

If continuous replication is enabled, the Microsoft Exchange Replication Service copies the `E0000000001.log` file to the inspector directory. This folder may be on the local machine (in the case of local continuous replication), a passive cluster node (in the case of cluster continuous replication), or a remote mail server (in the case of standby continuous replication).

The service verifies the checksum and signature of the log files in the inspector directory to ensure that they are not corrupted and that they are in the correct sequence. Once this is verified, the replication service copies the log file (`E0000000001.log`) to the target log file directory. The transactions found in log file `E0000000001.log` are then committed to the passive copy of the database.

At any given time, the most out of sync the passive copy of the database will be is approximately 15 minutes. This lag would be in the dead of night when there is absolutely no activity on the mailbox database. During a normal workday when users are actually using the database, the passive copy of the database will be no more than a few minutes behind.

If a database is dismounted or the information store service is stopped, the data is committed to the active database and then passed over passive copy. If the administrator has to manually switch over to the passive copy of the database, the passive copy should be completely synchronized with the active copy of the database.

Local Continuous Replication

For even a small organization, local continuous replication (LCR) is one of the most interesting new features of Exchange 2007; LCR helps to ensure that an alternate copy of a mailbox database is maintained on the local server. This feature was at one time called *continuous backup*. The concept of LCR is illustrated in Figure 1.2. A backup copy of the production mailbox database is maintained on the local server. As the transaction logs of the production database are completely filled, they are copied to the backup location (step 1) and committed to the backup copy of the database (step 2).

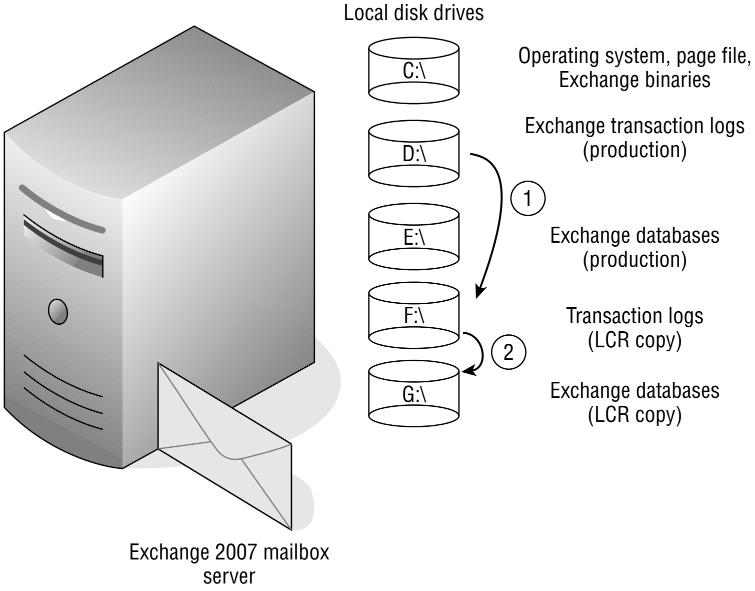

Local disk drives
C:\
Operating system, page file, Exchange binaries
D:\
Exchange transaction logs (production)
1
E:\
Exchange databases (production)
F:\
Transaction logs (LCR copy)
2
G:\
Exchange databases (LCR copy)
Exchange 2007 mailbox server

Figure 1.2
Local continuous replication

In the event that the production database becomes corrupted, the administrator can switch from the production database to the backup copy of the database. Here are some important points and tips to remember with respect to local continuous replication:

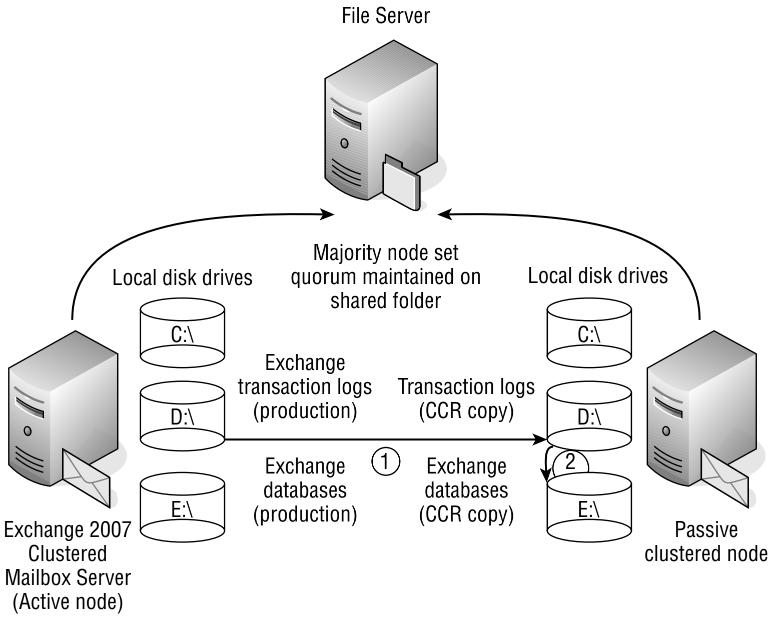
- LCR is designed to reduce restore time by keeping on the local server a copy of the database that can be brought into service in a very short period of time (a few minutes).
- Activation of a passive copy of the database is performed manually by the administrator.
- The LCR database must be stored on the local server.
- Each database that will be replicated must be in its own storage group.
- Plan to use separate logical units (LUNs) or physical disks for the LCR databases and transaction logs.
- Disk storage capacity will be double the requirements of a mailbox server without LCR if you replicate all mailbox databases.
- Replication will increase disk I/O capacity requirements by 125 to 150 percent.
- Add an additional 1GB to 2GB of physical memory for servers that will use LCR.
- Factor in an additional 20 percent CPU capacity on top of a standard mailbox server.
- If you use snapshot backups, you can configure your disk snapshots to be done on the passive copies of the database. This can significantly improve performance for the active copies of the database during the snapshot period.

Cluster Continuous Replication

Cluster continuous replication (CCR) is another interesting new feature of Exchange 2007. CCR introduces a whole new level of high availability and clustering. Unlike traditional single copy clustering (SCC), in which there is only a single copy of the database, CCR has not only redundant hardware but also a backup copy of the database. This backup copy is kept current using replication technology similar to LCR. As transactions are committed to the production copy of a database, the log file is copied to the backup location and committed to the backup copy of the database.

CCR is implemented in the form of two-node, active-passive clustering. Quorum is maintained using a majority node set cluster; a third server acts as a witness by providing a file share on which the shared quorum database is located. The active node has one or more mailbox databases; the concept of CCR is illustrated in Figure 1.3. As transactions are committed to the active node's databases and transaction logs, the transaction logs are shipped (copied) to the passive node (shown in step 1).

FIGURE 1.3
Clustered continuous replication


File Server
Majority node set quorum maintained on shared folder
Local disk drives
Local disk drives
C:\
D:\
E:\
C:\
D:\
E:\
Exchange transaction logs (production)
Transaction logs (CCR copy)
1
2
Exchange databases (production)
Exchange databases (CCR copy)
Exchange 2007 Clustered Mailbox Server (Active node)
Passive clustered node

When the transaction log has been successfully copied to the passive node, the transactions in that log are committed to the corresponding database on the passive node (step 2). In the event of any type of failure on the active node, the passive node will automatically fail over and assume responsibility for the clustered mailbox server (formerly called an Exchange virtual server).

When you are running Windows 2003, the active and passive nodes must be on the same IP subnet; however, if you are using Windows Server 2008, you can have clustered nodes on different subnets. If an organization has VLAN capability, it can conceivably place two nodes of a Windows 2003 CCR cluster in separate locations.

Cluster continuous replication will help to reduce the ''cost of entry'' for organizations wishing to move to Exchange clustering since it eliminates the need for costly shared storage such as storage area networks (SANs). Keep in mind the following important points and tips when implementing CCR:

- Failover of the active clustered node is automatic, such as in the event of the failure of the server hardware.
- A single database failure will not induce an automatic failover.

- Data storage for CCR clusters can be located on direct attached storage (DAS) or you can continue to use SAN storage. However, unlike with traditional Exchange 2000/2003 clusters, the disks are not shared on the SAN. Each node of the cluster uses its own disks.
- Each database must be in its own storage group. If you need 10 mailbox databases, you must have 10 storage groups.
- The only Exchange server role that can live on a CCR cluster is the Mailbox server role. Hub Transport, Client Access, and Unified Messaging cannot be installed on a clustered server. This is by design and is intended to reduce the complexity of clusters and thus improve availability.
- If you want to put a public folder store in a CCR cluster, it can be the only instance of the public folder store in your organization. High availability of public folder data should be implemented using multiple public folder servers and multiple replicas of public folder data.
- If an unplanned failover of the active clustered node occurs, the new active node will need to contact each of the Exchange 2007 Hub Transport servers in the site to make sure it has not missed any recently delivered e-mail messages.

Standby Continuous Replication

Short of maybe some fixes to the management interface, standby continuous replication (SCR) is the most valuable addition to Exchange 2007 Service Pack 1. This is one of the most commonly requested capabilities from Exchange customers. I frequently hear questions such as, ''How do I provide remote recoverability for mailbox data?'' and ''How do I provide a standby solution short of implementing clustering?'' Many third-party products have been introduced to the market that address these types of requests.

Before I jump into a description of standby continuous replication, I want to make something very clear. SCR is a resiliency or contingency solution; it does not provide *high availability* in the same way that CCR clustering provides high availability. Clustering-type high availability solutions provide near immediate failover to a backup server (and data in the case of CCR); the failover is usually automatic and takes between 2 and 10 minutes, depending on the configuration. Clustering also implies little to no data loss.

In addition to providing high availability and automatic failover solutions, clustering is useful in other ways. If you need to perform maintenance on an active node of the cluster, you simply move the Exchange services to a passive node of the cluster. Within a few minutes, all of the clients are right back at work and you can perform necessary maintenance.

The failover involved in switching over to an SCR copy of a database is less trivial than it is for clustering and it is not automatic. You do not deploy this sort of solution for high-availability requirements or the *we need to do maintenance on this node* requirements. You deploy it for situations in which a server has failed permanently or where an entire site will become unavailable, such as in the case of a natural disaster. For this reason, I call it a resiliency or contingency solution, not a high-availability solution. Setting expectations for features and functions will help you to do your job more easily.

That said, let's look at standby continuous replication for Exchange Server 2007 Service Pack 1. SCR is implemented on an Exchange Server 2007 mailbox server and is configured to pull transaction logs from one or more Exchange Server 2007 mailbox servers. SCR can actually pull transaction logs from many Exchange Server 2007 mailbox servers in many different locations; the limiting factor will be whether or not you have enough bandwidth to pull transaction logs across the network to the SCR server. One other configuration point to keep in mind is that you are limited to a single database per storage group if you want to take advantage of the new replication technologies; however, that is okay because Exchange Server 2007 Enterprise Edition allows for up to 50 storage groups.

In the wild, I have seen a few different implementations of SCR so far. They fall into a few categories; the first, in Figure 1.4, shows how an organization would implement SCR if it is simply looking for resiliency of its mailbox data to a standby data center. The Exchange servers in Sydney and San Francisco are *combined function* servers, meaning that they implement multiple Exchange Server 2007 server roles. In this example, these servers each have the Mailbox, Hub Transport, and Client Access server roles.

The third location is the contingency location in New York. This could be another of the company's offices or it could be a contingency site provider that provides the company rack space for a few servers. SCR is configured on a server in New York; initially the databases from Sydney and San Francisco are seeded onto a server in New York. Then SCR is configured to pull the committed transaction logs from the Sydney and San Francisco servers. SCR can be configured to immediately replay these logs to the passive copies of the database or wait a configured amount of time so that the passive copy is always a certain interval behind the active copy.

Figure 1.4 can be scaled so that Exchange servers at additional offices are replicated to New York. The limiting factor on the contingency server in New York will be the disk storage and I/O capacity as well as the maximum number of storage groups or storage databases that can be active on that server.

The server in New York is configured as a combined function server. If there is a failure of the San Francisco site, the administrator makes the decision to bring one or all of the San Francisco databases live on the New York server. The URL for Outlook Web Access would have to be pointed to the alternate server. Outlook 2007 clients would automatically connect to the New York server after Active Directory has replicated the fact that the users' mailboxes in San Francisco are now on the New York server. The administrator would have to manually update Outlook 2003 and earlier clients.

For organizations that are concerned about both high availability and site resiliency, SCR can be combined with CCR. The source databases do not have to be on a stand-alone mailbox server but can be on a clustered mailbox server. Figure 1.5 shows how an organization can combine a CCR cluster in its main office (for high availability) with an SCR system in a remote office that provides site resiliency.

In this organization, the CCR cluster provides high availability in the event of hardware failure or in the event that the company needs to perform maintenance on one of the two nodes of the CCR cluster. The SCR system always pulls transaction logs from the active node of the cluster; it does not pull the logs from the passive node.

If there is ever a complete failure of the San Francisco site, the administrator must make the decision to perform the failover to the New York contingency site.

Room and Equipment Resource Management

Allowing users to use Outlook to schedule conference rooms and equipment such as televisions is a pretty popular feature. You would think it would be a built-in feature in all versions of Exchange. Have you ever tried to create *resource* mailboxes in Exchange 2000/2003? It was pretty easy to do, wasn't it? You simply created a user account/mailbox whose display name was Conference Room 1 and you were in business. You might give another user permission to accept appointments for the Conference Room 1 resource, set Outlook up to run continually and accept appointments automatically, or write a script that accepts the appointments automatically. But, woefully and unfortunately, to Exchange and to Outlook, Conference Room 1 is just another mailbox. There is nothing special that identifies that particular mailbox as a conference room.

FIGURE 1.4
Basic standby continuous replication implementation

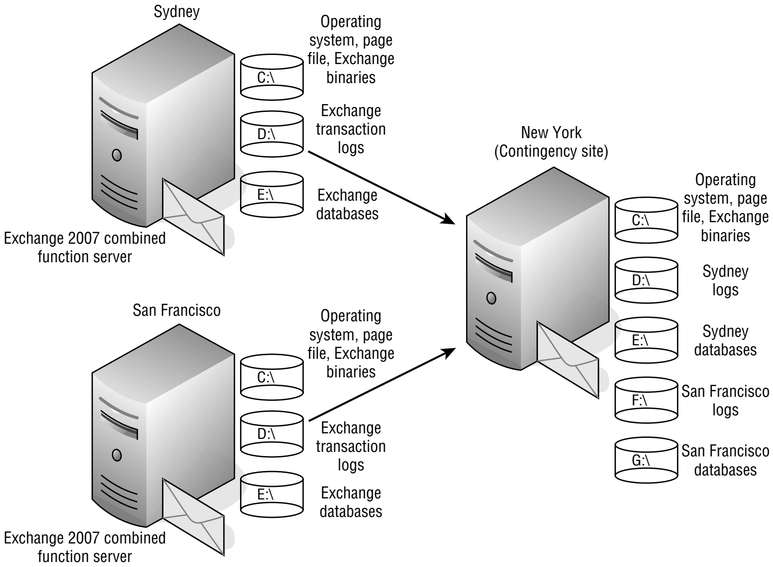
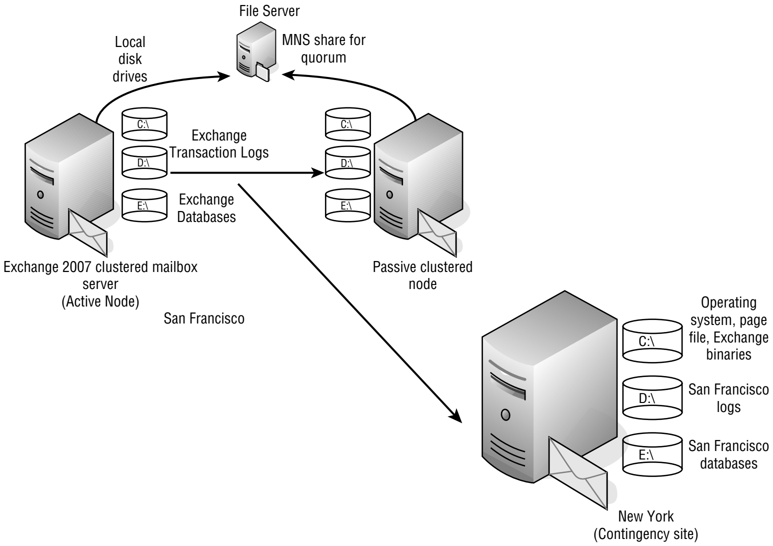

Sydney
Operating system, page file, Exchange binaries
C:\
Exchange transaction logs
D:\
Exchange databases
E:\
Exchange 2007 combined function server
San Francisco
Operating system, page file, Exchange binaries
C:\
D:\
Exchange transaction logs
E:\
Exchange databases
Exchange 2007 combined function server
New York (Contingency site)
C:\
Operating system, page file, Exchange binaries
D:\
Sydney logs
E:\
Sydney databases
F:\
San Francisco logs
G:\
San Francisco databases

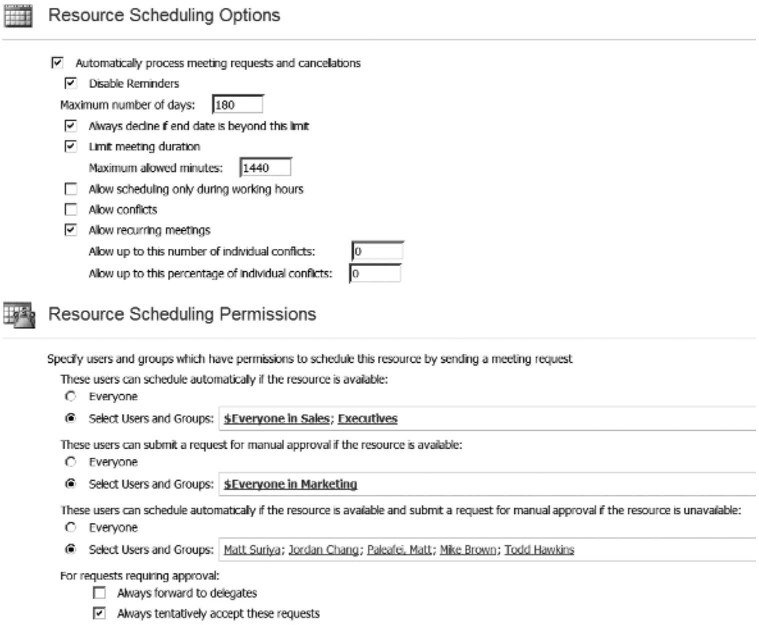
FIGURE 1.5
Basic standby continuous replication implementation



The good news is that the weakness in Exchange Server has finally been addressed with Exchange Server 2007. First, during account creation, you can flag a mailbox as a room or equipment resource; this sets flags in Active Directory that uniquely identifies that mailbox as a resource mailbox rather than a user mailbox.

Second, when a resource mailbox is created, the administrator can log in to the mailbox through Outlook Web Access and set resource management settings that are available only to a resource mailbox. Some of these options are shown in Figure 1.6. They include the ability to specify who can schedule a meeting automatically and who can request a meeting that has to be approved by one of the resource owners.

FIGURE 1.6
Viewing resource management settings for a resource mailbox



Resource Scheduling Options

☑ Automatically process meeting requests and cancellations
☑ Disable Reminders
Maximum number of days: 180
☑ Always decline if end date is beyond this limit
☑ Limit meeting duration
Maximum allowed minutes: 1440
□ Allow scheduling only during working hours
□ Allow conflicts
☑ Allow recurring meetings
Allow up to this number of individual conflicts: 0
Allow up to this percentage of individual conflicts: 0

Resource Scheduling Permissions

Specify users and groups which have permissions to schedule this resource by sending a meeting request
These users can schedule automatically if the resource is available:
○ Everyone
● Select Users and Groups: $Everyone in Sales; Executives
These users can submit a request for manual approval if the resource is available:
○ Everyone
● Select Users and Groups: $Everyone in Marketing
These users can schedule automatically if the resource is available and submit a request for manual approval if the resource is unavailable:
○ Everyone
● Select Users and Groups: Matt Suriya; Jordan Chang; Paleafei, Matt; Mike Brown; Todd Hawkins
For requests requiring approval:
□ Always forward to delegates
☑ Always tentatively accept these requests

When the meeting request is sent to the resource mailbox, the *calendar concierge* feature in Exchange Server examines the request and approves it based on the rule the administrator defines. No special scripts or third-party applications are required! If this feature piques your interest, don’t worry, I will get back to it in Chapter 10, ‘‘Managing Resource Mailboxes.’’

64-bit Architecture

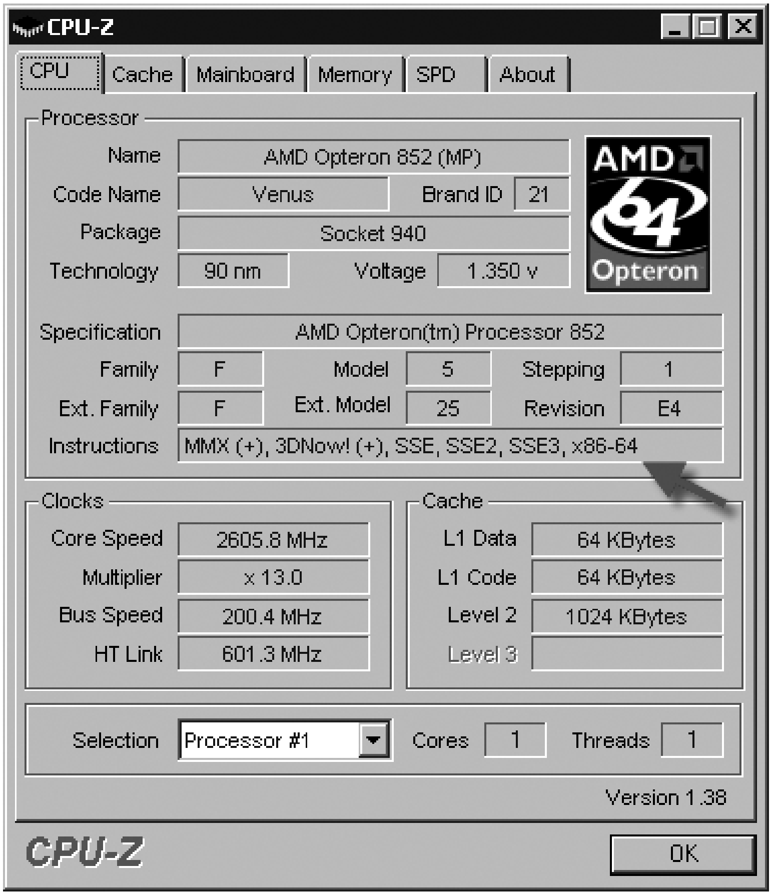
In some people’s minds, the move to the AMD x64 or Intel EM64T architecture was a pretty bold and controversial one. At this point in the book, you are probably not looking for a narrative on the merits of using the 64-bit memory architecture, so I am not going to give you one. Instead, in a very small amount of space, I will answer why this move makes sense.

First, on most Exchange 2000/2003 servers with more than about 1,000 mailboxes (depending on how heavily they use the Exchange server), the server’s main bottleneck becomes disk I/O. This is because, at best, Exchange 2003 allows for 1.2GB of cache memory. For 1,000 simultaneous users, that is about 1.2 MB of cache per user. As you scale upward to more users, that is even less cache. With less cache, Exchange has to *go to the disk* more frequently for both reads and writes.

To truly reduce the burden on the disk and make the disk reads and writes more efficient, you need more cache per simultaneous user. Exchange Server 2007 uses the x64 memory extensions for Intel and AMD processors. Microsoft has tested Exchange Server 2007 with up to 32GB of physical memory; the RAM recommendation for a mailbox server is at least 2GB of base memory plus 5 MB of RAM for each mailbox.

The reason this decision is controversial in some circles is that companies want to reuse their older hardware. If you have purchased new server hardware anytime since 2005, the hardware probably has these extensions. If you are not sure if your existing hardware supports the x64 extensions, there are a number of ways that you can check, including confirming it with the hardware vendor. It the computer is already running Windows, you can get a handy little program called CPU-Z from `www.cpuid.com`. Figure 1.7 shows the CPU-Z program.

FIGURE 1.7
Using CPU-Z to identify the CPU type



Processor

Name: AMD Opteron 852 (MP)
Code Name: Venus
Brand ID: 21
Package: Socket 940
Technology: 90 nm
Voltage: 1.350 v

Specification: AMD Opteron(tm) Processor 852
Family: F
Model: 5
Stepping: 1
Ext. Family: F
Ext. Model: 25
Revision: E4
Instructions: MMX (+), 3DNow! (+), SSE, SSE2, SSE3, x86-64

Clocks

Core Speed: 2605.8 MHz
Multiplier: x 13.0
Bus Speed: 200.4 MHz
HT Link: 601.3 MHz

Cache

L1 Data: 64 KBytes
L1 Code: 64 KBytes
Level 2: 1024 KBytes
Level 3:

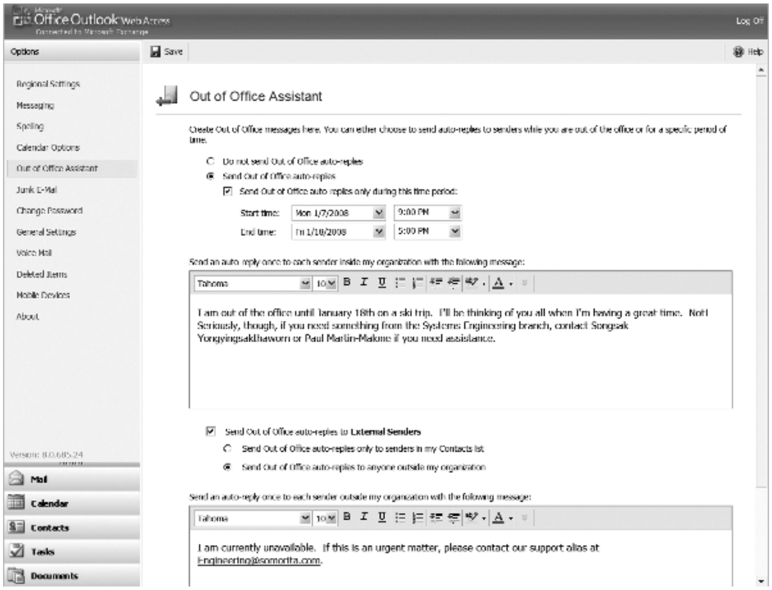
Selection: Processor #1
Cores: 1
Threads: 1

Version 1.38

Notice in the Instructions line of CPU-Z that this particular chip supports x86–64. This means that this particular chip will support the x64 instruction sets. Intel chips will report that they support the EM64T instruction set.

Schedulable and Internal/External Out-of-Office Messages

A very nice improvement from the user's perspective is the ability to schedule when out-of-office messages start and finish and the ability to specify a separate message for internal users than you have for external users. This feature requires either Outlook Web Access 2007 or Outlook 2007 in order to manage this feature. Figure 1.8 shows an example of the Out Of Office Assistant in Outlook Web Access.



Out of Office Assistant

Create Out of Office messages here. You can either choose to send auto-replies to senders while you are out of the office or for a specific period of time.

○ Do not send Out of Office auto-replies
● Send Out of Office auto-replies
☑ Send Out of Office auto-replies only during this time period:

Start time: Mon 1/7/2008 9:00 PM
End time: Fri 1/18/2008 5:00 PM

Send an auto-reply once to each sender inside my organization with the following message:

Tahoma 10

I am out of the office until January 18th on a ski trip. I'll be thinking of you all when I'm having a great time. Not! Seriously, though, if you need something from the Systems Engineering branch, contact Songsak Yongyingsakthaworn or Paul Martin-Malone if you need assistance.

☑ Send Out of Office auto-replies to **External Senders**
○ Send Out of Office auto-replies only to senders in my Contacts list
● Send Out of Office auto-replies to anyone outside my organization

Send an auto-reply once to each sender outside my organization with the following message:

Tahoma 10

I am currently unavailable. If this is an urgent matter, please contact our support alias at Engineering@somorita.com.

FIGURE 1.8
Scheduling out-of-office messages for internal and external recipients

When setting up an out-of-office message for external recipients, the user can specify that the response goes only to senders whose address is in their Contacts folder or to any sender.

Transport Rules

A pretty common question in Exchange 2000/2003 is, Can I do X, or Y, or Z? when a message is sent or received by a user. The answer is almost always, Yes, if you write some custom code or buy a third-party software package.

Exchange Server 2007 introduces the concept of transport rules. Transport rules are executed by the Hub Transport server role, and because all messages must pass through a Hub Transport server (even local ones), all messages will be subject to the rules.

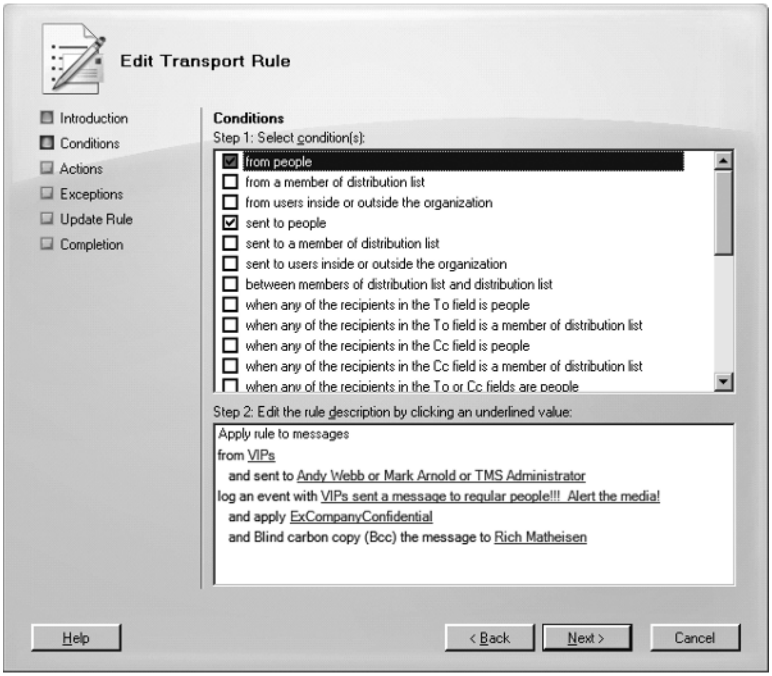
Transport rules are created using a wizard that looks very similar to the Outlook Rules Wizard, but these rules are executed by the Hub Transport server; a sample rule is shown in Figure 1.9.

A transport rule consists of three parts: the conditions on which the rule will apply, the action the rule will perform, and the exceptions to the rule. Here are some examples of actions you can take with transport rules.

- Append a disclaimer to all outbound messages or even different disclaimers for different departments.
- Prevent messages with sensitive or private classifications from leaving the organization.

- Log events or forward copies of messages sent by specific users.
- Examine a message's content (including message body and subject) and take action on the message.

FIGURE 1.9
Managing a transport rule



Conditions

Step 1: Select condition(s):

☑ from people
☐ from a member of distribution list
☐ from users inside or outside the organization
☑ sent to people
☐ sent to a member of distribution list
☐ sent to users inside or outside the organization
☐ between members of distribution list and distribution list
☐ when any of the recipients in the To field is people
☐ when any of the recipients in the To field is a member of distribution list
☐ when any of the recipients in the Cc field is people
☐ when any of the recipients in the Cc field is a member of distribution list
☐ when any of the recipients in the To or Cc fields are people

Step 2: Edit the rule description by clicking an underlined value:

Apply rule to messages
from VIPs
and sent to Andy Webb or Mark Arnold or TMS Administrator
log an event with VIPs sent a message to regular people!!! Alert the media!
and apply ExCompanyConfidential
and Blind carbon copy (Bcc) the message to Rich Matheisen

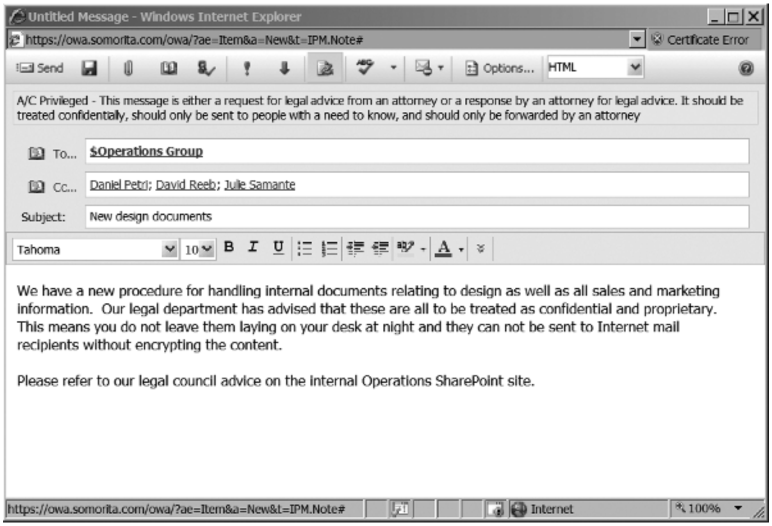
Not only can transport rules be created and managed on Hub Transport servers and applied to internal messages, but similar transport rules can be applied on Edge Transport servers. I expect as Exchange 2007 matures and becomes more common, third-party vendors will further extend the capabilities of transport rules.

Message Classifications

If you work in an organization that sends sensitive content via e-mail, then a new feature called message classifications may be just the feature for you. There are third parties that sell classification tools for Outlook that will prepend or append text to a message body, but the text is found only in the message body. Exchange 2007 message classifications include not only text describing the message classification but an additional message property that can be examined (or applied) by transport rules.

The message classification label shows up on the top of the message directly above the addressing information; an example is shown in Figure 1.10. Both the classification and the label can be customized by the Exchange server administrator.

Depending on how you want to use classifications and control the distribution of classified messages, you can incorporate classifications with transport rules.



https://owa.somorita.com/owa/?ae=Item&a=New&t=IPM.Note#

A/C Privileged - This message is either a request for legal advice from an attorney or a response by an attorney for legal advice. It should be treated confidentially, should only be sent to people with a need to know, and should only be forwarded by an attorney

To... $Operations Group

Cc... Daniel Petri; David Reeb; Julie Samante

Subject: New design documents

We have a new procedure for handling internal documents relating to design as well as all sales and marketing information. Our legal department has advised that these are all to be treated as confidential and proprietary. This means you do not leave them laying on your desk at night and they can not be sent to Internet mail recipients without encrypting the content.

Please refer to our legal council advice on the internal Operations SharePoint site.

FIGURE 1.10
Applying a message classification

Messaging Records Management

I had a tough time deciding if messaging records management was a new feature or just vast improvements over an existing feature. By an existing feature, I mean the Exchange 2000/2003 Mailbox Management feature that allows the administrator to define retention policies for folders in a mailbox.

However, messaging records management takes that concept and carries it quite a bit further. Let's take a quick look at some of things that you can do with messaging records management.

- Control the length of time and the content types in users' folders.
- Define additional folders that should be created in a user's folder and that the user can use for message retention. Differing retention policies can be defined for the custom folders that you create for your users.
- Automatically send copies of messages that users place in a managed folder to another e-mail address.
- Move messages from a specified folder based on content type (e-mail, contact, calendar, fax, voicemail, etc.) to another managed folder.

The first time you look at messaging records management, it is a bit confusing until you realize that it must be configured in a few different steps. The following list contains some of the steps:

- Create managed folder mailbox policies to define which managed default and managed custom folders will be managed.
- Assign the managed folder mailbox policy to one or more users. A user does not need a managed folder mailbox policy. Only a single managed folder mailbox policy can be assigned to a user at one time.
- Create managed content settings for default folders (Inbox, Sent Items, etc.) to control the length of time that messages should remain in these folders and types of content that are allowed. This step is optional.

- Create managed custom folders that will appear in the user's Managed Folders folder in their mailbox. This step is optional.
- Create managed content settings for managed custom folders to control how content is managed or retained in the folders that will be created in the user's mailbox. This step is optional.

Tip

Messaging records management is a premium feature of Exchange 2007 and requires an Enterprise client access license for each user who will have their mailbox managed by it.

Per-User Journaling

Journaling is a feature that arrived in Exchange 5.5 with the need to keep a copy of everything that a user sends or receives. This feature is usually required when the specified user works within a department that may be audited, such as an accounting or finance department; a historical archive of all user communication (including e-mail) may be required by law.

In Exchange 5.5/2000/2003, you designated what was archived by putting everyone on a single mailbox database. This was not the most elegant solution, though. For example, a law in the United States called Sarbanes-Oxley requires that companies have the ability to audit all communications sent by people that deal with company finance. Many organizations implement journaling for all members of the organization's accounting department. However, these users may span many servers and physical locations, and thus it will be difficult to put them all on a single mailbox database.

Exchange 2007 lets you specify a single recipient or group of recipients for whom you want to journal mail. Figure 1.11 shows a journal rule that will send copies of all mail sent and received (internally or externally) to the compliance officer.

Journaling rules are processed by the Hub Transport server role; therefore, a message will be journaled regardless of the original server, the recipient mailbox, or which mailbox database holds the mailbox.

Tip

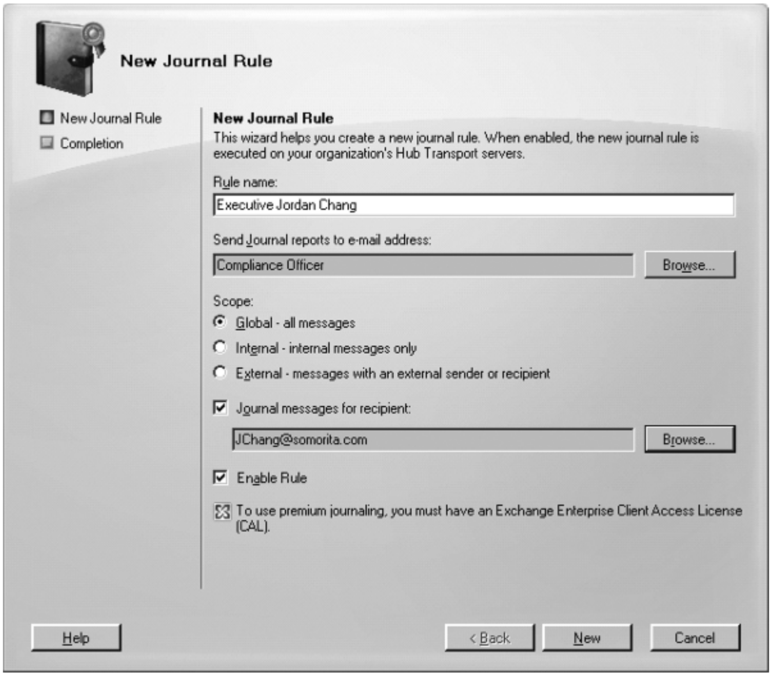
Journaling rules are a premium feature and require Exchange Enterprise client access licenses for each mailbox on which journaling will be used.

Unified Messaging

Unified Messaging allows for integration of inbound faxing and voicemail with an Exchange server; a voicemail or a fax is recorded by the Unified Messaging server and then delivered to the user's mailbox (via the Hub Transport server). This can make users more efficient by providing a single location for inbound information; voicemails and faxes can be read via Outlook Web Access or Outlook. In addition, missed call information (someone calls but does not leave a voicemail message) is sent to the user's mailbox.

An example of a voicemail that has been delivered to a user is shown in Figure 1.12. The form you see in the figure is in Outlook Web Access 2007 and includes a player control for playing the message via the PC speakers.

FIGURE 1.11
Creating a journaling rule



New Journal Rule

This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.

Rule name: Executive Jordan Chang

Send Journal reports to e-mail address: Compliance Officer

Scope:

● Global - all messages

○ Internal - internal messages only

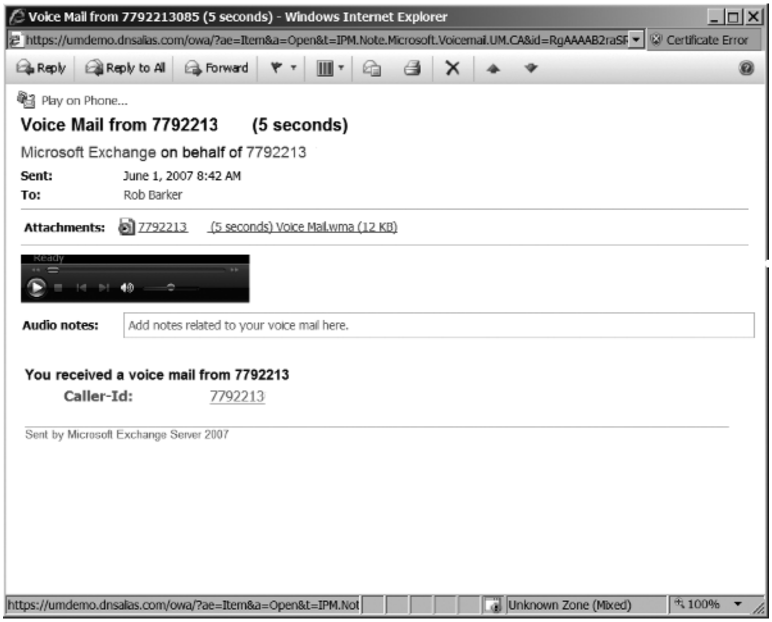
○ External - messages with an external sender or recipient

☑ Journal messages for recipient: JChang@somorita.com

☑ Enable Rule

To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).

FIGURE 1.12
Viewing a voicemail message sent via Unified Messaging



Voice Mail from 7792213085 (5 seconds) - Windows Internet Explorer

https://umdemo.dnsalias.com/owa/?ae=Item&a=Open&t=IPM.Note.Microsoft.Voicemail.UM.CA&id=RgAAAAB2raSF

Voice Mail from 7792213 (5 seconds)

Microsoft Exchange on behalf of 7792213

Sent: June 1, 2007 8:42 AM

To: Rob Barker

Attachments: 7792213 (5 seconds) Voice Mail.wma (12 KB)

Audio notes: Add notes related to your voice mail here.

You received a voice mail from 7792213

Caller-Id: 7792213

Sent by Microsoft Exchange Server 2007

https://umdemo.dnsalias.com/owa/?ae=Item&a=Open&t=IPM.Not

You can also play the voice message on your desk phone. The Play on Phone option allows you to instruct the Unified Messaging server to call you at a specified extension (or optionally an external phone if the Unified Messaging dial plan allows you to call outside of your organization).

Further, the user can call the Unified Messaging server via the telephone and listen to their voicemail, have their e-mail read to them, listen to their calendar, rearrange appointments, or look up someone in the global address book. Unified Messaging also allows the administrator to build a customized auto attendant for call routing. In my experience, a typical voicemail (using the default Windows Mobile codec) takes between 2 KB and 3 KB per second of message time, but this amount can be changed. However, with higher-quality recordings come higher message sizes.

One barrier to entry for some organizations is that Exchange 2007 Unified Messaging integrates only with specific Voice over Internet Protocol (VoIP) telephone systems. The session initiator protocol (SIP, and specifically SIP over TCP) is used for call setup/teardown and the real-time protocol (RTP) is used for call management. If you include inbound faxing, Exchange Server Unified Messaging uses the T.38 protocol for faxing.

Not all voice and faxing systems are going to support this feature ''right out of the box.'' More and more vendors are tweaking their VoIP systems to talk directly to Exchange Server 2007 Unified Messaging (such as Cisco and Mitel), but you may still require a VoIP gateway of some type. Many traditional ''hard wired'' PBXs will require a PBX-to-VoIP gateway, but even some VoIP systems will require a VoIP-to-VoIP gateway.

If you are like me, then you are more of a specialized network administrator. I have never managed a phone system in the past and am only slightly familiar with some of the phone terminology. I just assumed that VoIP was VoIP and that was that. Working with the folks that manage your telephone system will be a new and exciting experience. I was quite surprised to learn that there are over 100 implementations of SIP out on the market.

As of 2007, Unified Messaging solutions have only about a 10 to 15 percent market penetration. That is, of course, depending on whose survey you read and how you define Unified Messaging. Some vendors define it as delivering a voicemail to a user's computer and allowing them to play the voicemail over the PC speakers; this voicemail might have been delivered to the user's mailbox (on the server) or it might have been *pulled* by Outlook or another client application and stored in the user's PST file. Some vendors consider solely inbound faxing to be a Unified Messaging solution, though in my opinion that is not terribly unified.

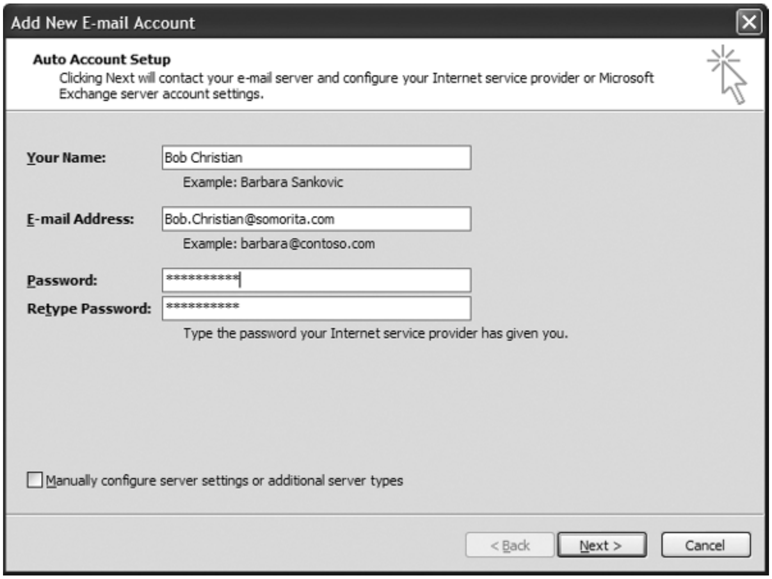
Microsoft has decided to get into the Unified Messaging market for a number of different reasons, including the fact that Unified Messaging has a fairly low market penetration thus far. Customers are often reluctant to deploy Unified Messaging solutions due to the complexity, administrative overhead, schema changes, client-side deployment requirements, and cost. Microsoft is determined to make its Unified Messaging implementation less expensive than competing products and much better integrated with Active Directory.

Automatic Configuration of Outlook 2007

One of the biggest headaches for a desktop or network administrator is configuring Outlook profiles. If you are not using Windows roaming profiles on your network, each time a user moves to a new computer, they must re-create their Outlook profile. Even worse, if the user's mailbox gets moved off of one server and that server is shut down before the user can load Outlook and get redirected, then the user gets an error and has to reconfigure the server name in the Outlook profile.

Exchange Server 2007 and Outlook 2007 together introduce a new feature called Autodiscover. Autodiscover allows Outlook to automatically locate the mailbox server for the specified user. When a user launches Outlook for the first time, they are presented with the Add New E-mail Account Wizard, shown in Figure 1.13. The user provides their name, e-mail address, and password.

FIGURE 1.13
Launching Outlook 2007 for the first time



Add New E-mail Account

Auto Account Setup
Clicking Next will contact your e-mail server and configure your Internet service provider or Microsoft Exchange server account settings.

Your Name: Bob Christian
Example: Barbara Sankovic

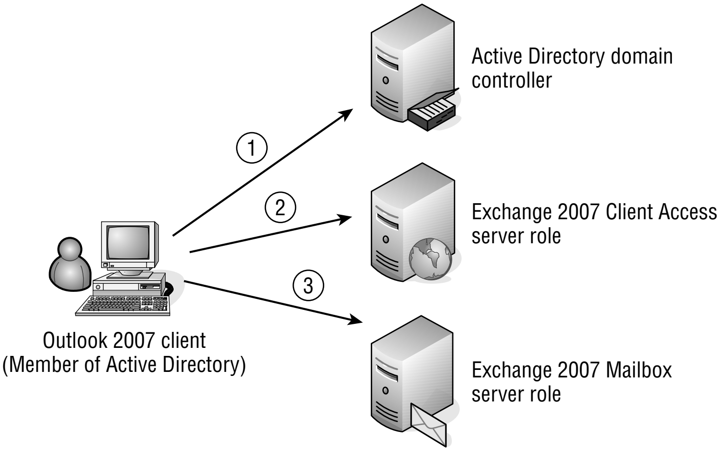
E-mail Address: Bob.Christian@somorita.com
Example: barbara@contoso.com

Password: ***********
Retype Password: ***********
Type the password your Internet service provider has given you.

□ Manually configure server settings or additional server types

Outlook then works in the background to locate the mailbox server and create the profile. This process is shown in Figure 1.14. The first thing the client does is contact the Active Directory to look up the name of the nearest Exchange 2007 Client Access servers. In this case, we are assuming that the computer is a member of the Active Directory; if the computer is not a member of the Active Directory, Outlook queries DNS to find the Autodiscover resource (`https://autodiscover.somorita.com/autodiscover/autodiscover.xml` or `https://somorita.com/autodiscover/Autodiscover.xml`). These URLs should point to the location of the Client Access server.

FIGURE 1.14
Outlook 2007's Autodiscover process



Active Directory domain controller
1
2
Exchange 2007 Client Access server role
3
Outlook 2007 client
(Member of Active Directory)
Exchange 2007 Mailbox server role

Once the Outlook client finds the Client Access server, it queries the Client Access server to determine the correct Exchange server location of the user's mailbox. If the user's mailbox is moved, the Autodiscover process is used once again.

The bottom line is that this process can reduce your administrative overhead when you create new users, or if users move from one computer to another frequently, this can help reduce the amount of assistance you have to render.

Outlook 2007 and Exchange Server 2007

The Autodiscover feature is one of a number of features and enhancements that are available only if you are both using the Outlook 2007 client and have your mailbox located on an Exchange Server 2007 server. While this might not seem very fair, you have to keep in mind that sometimes not only a client-side interface but also a server-side component is required to implement the feature.

Note

When comparing client and server features, it's important to note that a mailbox must be on Exchange Server 2007 in order to use either the premium or light Outlook Web Access interfaces.

I am including some tables to help you figure out which of the new features are available to you, which depends on the clients you are using and the location of the user's mailbox. Table 1.1 shows the mail features that are available with the different Outlook and Exchange server combinations.

Table 1.1: Mail Features Available with Outlook Client and Exchange Server Combinations

	O2K7/	OWA 2007	OWA 2007	Outlook	O2K7/	O2K3/
Feature	**E2K7**	**Premium**	**Light**	**Mobile**	**E2K3**	**E2K7**
Attachment preview in reading pane.	✓				✓	
View attachments as web page without client application.		✓	✓			
Instant search across all Outlook items.	✓	✓	✓	✓		
Better rules; 32 KB rule limit removed.	✓					
Native support for RSS feeds.	✓				✓	
RFC 2822 support for in-reply-to SMTP header for conversations.	✓	✓	✓	✓	✓	✓
Message classifications.	✓	✓				
Improved accessibility features for low-vision and blind users.	✓		✓			
Color categories freely defined and assigned to any type of item.	✓	✓			✓	

Note that some features, such as RSS feeds, will show up via Outlook Web Access if they were pulled into the user's mailbox, but the user will not have an interface to see them properly.

The different calendaring features that are available depend on the version of Exchange server and Outlook you are using. Table 1.2 shows the calendaring features and the server/client.

TABLE 1.2: Calendaring Features available with Outlook Client and Exchange Server Combinations

FEATURE	**O2K7/ E2K7**	**OWA 2007 PREMIUM**	**OWA 2007 LIGHT**	**OUTLOOK MOBILE**	**O2K7/ E2K3**	**O2K3/ E2K7**
Improved interface for booking meetings (Scheduling Assistant).	✓	✓	✓		✓	
Scheduling Assistant looks directly into a user's calendar instead of free/busy public folder.	✓	✓	✓			
Improved resource picker interface with attributes such as room capacity.	✓	✓	✓			
Add room as resource when you place the display name in to the To field.	✓	✓	✓			
Conference room resource settings configuration.		✓	✓			
Multiple meeting updates collapsed, only latest one shown.	✓	✓	✓	✓		✓
Meeting updates highlight updated fields.	✓	✓	✓			
Updates with no time change apply automatically, no reply required.	✓	✓	✓			
Dual time zone when scheduling a new meeting.	✓				✓	
Notification of time change when dragging/dropping a meeting.	✓				✓	
Calendar snapshots to share calendars with outside users.	✓				✓	
Caching of other users' calendar data.	✓				✓	
Two-way sync with team calendars in SharePoint.	✓				✓	
Overlaying of multiple calendars in the same view.	✓				✓	

As you can see in Table 1.2, many of the new features of the calendaring interface require Outlook 2007 exclusively, but a few nice improvements are available in that area via Outlook Web Access.

Next let's look at some of the new tasking features that are available. Table 1.3 shows the tasking features and which clients let you take advantage of them.

TABLE 1.3: Tasking Features Available with Outlook Client and Exchange Server Combinations

FEATURE	O2K7/ E2K7	OWA 2007 PREMIUM	OWA 2007 LIGHT	OUTLOOK MOBILE	O2K7/ E2K3	O2K3/ E2K7
To-Do Bar with improved task information.	✓	✓			✓	
Task information at the bottom of the calendar view.	✓	✓			✓	
Assign a task by dragging into calendar.	✓	✓			✓	
Flag message and assign task due date.	✓	✓			✓	

As you can see from Table 1.3, all of the tasking features require either Outlook 2007 or Outlook Web Access 2007 Premium; tasking features are not dependent on the mailbox server version. Next, let's look at the new out-of-office (OOF) features that are available. In my opinion, the new OOF features are some of the best in the new client interface. Table 1.4 shows the new out-of-office features and the circumstances under which they can be used.

TABLE 1.4: Out-of-Office Features Available with Outlook Client and Exchange Server Combinations

FEATURE	O2K7/ E2K7	OWA 2007 PREMIUM	OWA 2007 LIGHT	OUTLOOK MOBILE	O2K7/ E2K3	O2K3/ E2K7
Schedule OOF messages for future date/time.	✓	✓	✓	✓		
Internal and external OOF messages.	✓	✓	✓			
Send external OOF message only to contacts.	✓	✓	✓			
OOF messages can include HTML formatting.	✓	✓	✓	✓		

Tip

In case you were wondering, while we use OOF to mean *out-of-office*, it originally stood for *out-of-facility*; this acronym originated at Microsoft in the pre-Exchange days when it used a Xenix-based mail system.

Finally, there are some additional client/server features that your users may find useful. These are mostly security-related features. Table 1.5 shows these features and the circumstances under which they may be used.

Table 1.5: Additional Features Available with Outlook Client and Exchange Server Combinations

Feature	O2K7/ E2K7	OWA 2007 Premium	OWA 2007 Light	Outlook Mobile	O2K7/ E2K3	O2K3/ E2K7
Content policies for folders such as item retention, archive, and expiration.	✓	✓	✓			
Outlook generates postmark for use with antispam systems.	✓				✓	
Warning for e-mail messages that appear to be phishing messages.	✓	✓	✓		✓	
End user has the ability to remotely wipe out mobile device.		✓	✓			

Windows Mobile and Improved Security

Windows Mobile and ActiveSync device support are certainly not new to Exchange Server 2007. Exchange Server 2003 had good support for Windows Mobile devices, and you could even support mobile devices using Microsoft Mobile Information Server and Exchange 2000. Microsoft continues to improve the support and the manageability of mobile devices with newer versions of Windows Mobile, Exchange Server 2007 SP1, and updated versions of ActiveSync.

If you have supported Windows Mobile devices or other types of mobile devices, then you realize how important centralized policies and security can be for your organization and your users. The latest versions of the Exchange ActiveSync (EAS) have been improved greatly over the years. The newest features can be assigned to users based on the ActiveSync policy that is assigned to the user. Figure 1.15 shows two of the advanced property pages.

Of course, you must have the corresponding version of Windows Mobile to take advantage of all of the newest features. Windows Mobile 5 with the Microsoft Security and Feature Pack (MSFP) uses EAS v2.5, Windows Mobile 6 uses EAS v12, and Windows Mobile 6.1 uses EAS v12.1. Table 1.6 shows a comparison of some features of various versions of EAS and the versions of Exchange Server.

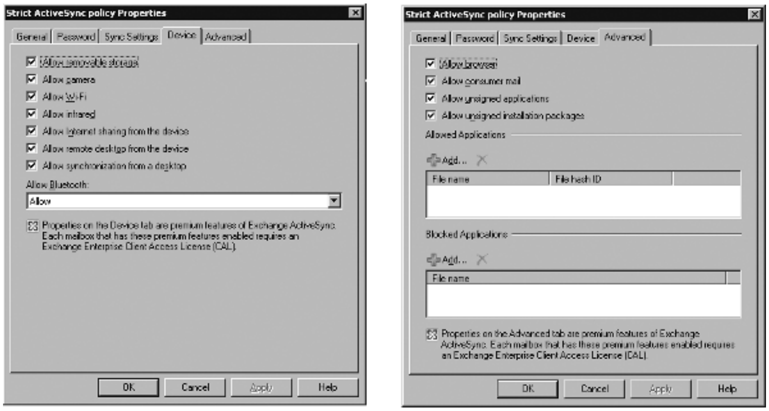


FIGURE 1.15
Examples of ActiveSync policies

Strict ActiveSync policy Properties

General | Password | Sync Settings | Device | Advanced

☑ Allow removable storage
☑ Allow camera
☑ Allow Wi-Fi
☑ Allow infrared
☑ Allow Internet sharing from the device
☑ Allow remote desktop from the device
☑ Allow synchronization from a desktop

Allow Bluetooth: Allow

Properties on the Device tab are premium features of Exchange ActiveSync. Each mailbox that has these premium features enabled requires an Exchange Enterprise Client Access License (CAL).

Strict ActiveSync policy Properties

General | Password | Sync Settings | Device | Advanced

☑ Allow browser
☑ Allow consumer mail
☑ Allow unsigned applications
☑ Allow unsigned installation packages

Allowed Applications

File name	File hash ID

Blocked Applications

File name

Properties on the Advanced tab are premium features of Exchange ActiveSync. Each mailbox that has these premium features enabled requires an Exchange Enterprise Client Access License (CAL).

TABLE 1.6: Exchange ActiveSync Features

SETTING/RESTRICTION	E2K3 SP2/ EAS v2.5	E2K7/ EAS 12	E2K SP1/ STANDARD CAL/ EAS v12.1	E2K7 SP1 ENTERPRISE CAL/ EAS v12.1
Password Required	✓	✓	✓	✓
Min Password Length	✓	✓	✓	✓
Alphanumeric Password	✓	✓	✓	✓
Inactivity Timeout	✓	✓	✓	✓
Max Failed Password Attempts	✓	✓	✓	✓
Policy Refresh Interval	✓	✓	✓	✓
Allow Non-provisionable Devices	✓	✓	✓	✓
Attachments Enabled		✓	✓	✓
Storage Card Encryption		✓	✓	✓
Password Recovery Enabled		✓	✓	✓
Allow Simple Device Password		✓	✓	✓
Max Attachment Size		✓	✓	✓
WSS Access Enabled		✓	✓	✓
UNC Access Enabled		✓	✓	✓

(CONTINUED)

Table 1.6: Exchange ActiveSync Features *(CONTINUED)*

			E2K SP1/	E2K7 SP1
	E2K3 SP2/	E2K7/	Standard CAL/	Enterprise CAL/
Setting/Restriction	EAS v2.5	EAS 12	EAS v12.1	EAS v12.1
Password History		✓	✓	✓
Require Manual Sync When Roaming			✓	✓
Min Device Pwd Complex Characters			✓	✓
Max Calendar Age Filter			✓	✓
Allow HTML Email			✓	✓
Max Email Age Filter			✓	✓
Max Email Body Truncation Size			✓	✓
Max Email HTML Body Truncation Size			✓	✓
Require Signed SMIME Messages			✓	✓
Require Encrypted SMIME Messages			✓	✓
Require Signed SMIME Algorithm			✓	✓
Require Encryption SMIME Algorithm			✓	✓
Allow SMIME Encryption Algorithm Negotiation			✓	✓
Allow SMIME Soft Certs			✓	✓
Require Device Encryption			✓	✓
Allow Storage Card				✓
Allow Camera				✓
Allow Unsigned Applications				✓
Allow Unsigned Installation Packages				✓

Table 1.6: Exchange ActiveSync Features *(CONTINUED)*

Setting/Restriction	E2K3 SP2/ EAS v2.5	E2K7/ EAS 12	E2K SP1/ Standard CAL/ EAS v12.1	E2K7 SP1 Enterprise CAL/ EAS v12.1
Allow Wi-Fi				✓
Allow Text Messaging				✓
Allow POP/IMAP Email				✓
Allow Bluetooth				✓
Allow IrDA				✓
Allow Desktop Sync				✓
Allow Browser				✓
Allow Consumer Email				✓
Allow Remote Desktop				✓
Allow Internet Sharing				✓
Unapproved InROM Application List				✓
Approved Application List				✓

Note that some of the advanced device configuration features require the use of a Exchange Server 2007 Enterprise client access license (CAL) for the device. This does not mean that the Exchange 2007 server requires Enterprise Edition of Exchange Server though.

Changes and Improvements to Existing Features

In the following sections, I want to discuss some improvements that have been made to existing features. Sometimes it was difficult to differentiate between a new feature and a feature that has been so completely reworked that it appears to be new.

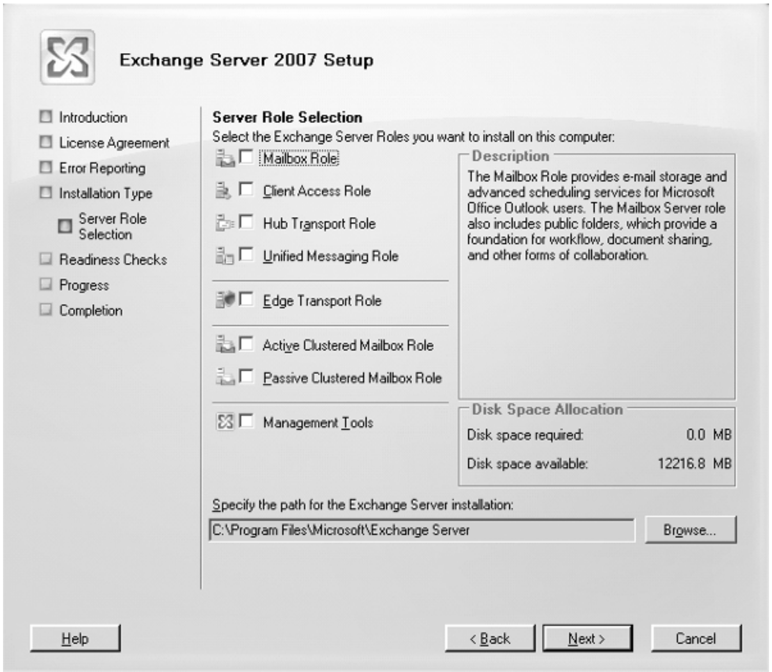
Server Roles

Server roles are useful for organizations with more than one Exchange 2007 server; server roles allow you to install only the features and software necessary to support a specific set of functions. This, of course, is only useful in multiserver organizations. In small and medium-sized businesses, you will probably just run a single server that has multiple roles installed on it.

I have put server roles in the improvements section because in my experience we already had server roles, we just didn't call them that. For example, to create a front-end server for Exchange 2003 Outlook Web Access, we first installed Exchange 2003, then deleted the public folder store, disabled the SMTP server, set the information store service startup type to disabled, and then set the check box to designate that particular Exchange server as a front-end server. There might have been additional hardening that we then performed.

The point is that in a multiserver environment, even in Exchange 2000/2003, we had multiple server roles but the role configuration tasks were performed after the Exchange server software was installed. With Exchange 2007, the roles that a specific piece of hardware will support are chosen at installation. The Exchange Server 2007 Setup program prompts the installer to choose the roles (see Figure 1.16).

FIGURE 1.16
Selecting server roles



Exchange Server 2007 Setup

Server Role Selection

Select the Exchange Server Roles you want to install on this computer:

□ Mailbox Role
□ Client Access Role
□ Hub Transport Role
□ Unified Messaging Role
□ Edge Transport Role
□ Active Clustered Mailbox Role
□ Passive Clustered Mailbox Role
□ Management Tools

Description

The Mailbox Role provides e-mail storage and advanced scheduling services for Microsoft Office Outlook users. The Mailbox Server role also includes public folders, which provide a foundation for workflow, document sharing, and other forms of collaboration.

Disk Space Allocation

Disk space required:	0.0 MB
Disk space available:	12216.8 MB

Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server

For people that are new to Exchange 2007, there is still a common misconception that each server role must be on a separate physical server. This is not true; all of the server roles (except Edge Transport) can reside on a single physical Windows 2003 or Windows 2008 server. I have worked on a number of installations where a customer had all four server roles on a single Exchange 2007 server that was servicing up to 500 mailboxes. There is nothing magical about the number 500; it was just the largest single function server I have seen.

NOTE

Server roles can be reconfigured (installed or removed) without reinstalling the entire server. This is useful when a server's responsibilities grow or shrink.

The following is a brief discussion of the Exchange Server 2007 server roles and their functions and requirements.

Mailbox server The Mailbox server role directly supports MAPI clients such as Outlook 2003 and 2007 as well as public folders. In most organizations, the Mailbox server role will consume the most resources (CPU, disk, memory). It requires at least one instance of the Hub Transport role to send and deliver mail both inside and outside the Exchange organization. The Mailbox role can be co-located on the same server with the following other roles:

- Hub Transport
- Client Access
- Unified Messaging

However, there are some caveats you should be aware of before deciding to install any other roles on an Exchange server that hosts the Mailbox server role:

- Clustering is not supported with any other role. If you intend to cluster (CCR or SCR) your Mailbox servers, you cannot install any other roles on those servers.
- If the Hub Transport role is installed on the same server as the Mailbox role, the Mailbox components will always use the local Hub Transport in favor of remote Hub Transports.
- Exchange servers that host the Mailbox server role typically have the most RAM and processing power and are connected to the largest and fastest storage in a data center. One way you can maximize the Mailbox role's efficiency is by offloading other roles to servers with fewer resources.
- The Mailbox server role should be installed within your organization's intranet, preferably as close as possible to the users it will serve. The Mailbox role uses Messaging Application Programming Interface (MAPI) Remote Procedure Calls (RPCs) to communicate with servers running the Hub Transport, Client Access, and Unified Messaging roles as well as the Outlook client and should have at least Fast Ethernet (100 Mb/sec) connectivity to other Exchange servers in the same Active Directory site that hosts those roles.
- The Mailbox role must also provide a file share for the Client Access role, so you cannot disable the file and print services if you're trying to harden your Exchange server.
- The Mailbox role is responsible for generating the offline address book, which your users will need when their Outlook client is not directly connected to the Exchange server (for instance, laptop users). Bear in mind that Exchange 2007 no longer relies upon public folders to distribute the offline address book to Outlook 2007 clients; instead it uses the Background Intelligent Transfer Service (BITS) via HTTP(S). If you still have older clients like Outlook 2000 or 2003, you will need public folders just as with Exchange 2000/2003.

Hub Transport server The Hub Transport server role is required; it is responsible for *all* message delivery. Even a message you send to someone on the *same* mailbox database as you will go through a Hub Transport server. The Hub Transport server that will be used is a Hub Transport server in your own Active Directory site. Each Active Directory site that has a Mailbox server must also have at least one Hub Transport server role running in the same site.

The Hub Transport server can deliver e-mail outside of the organization (to the Internet, your antispam system, or an Edge Transport server) as well as to other Hub Transport servers in other Active Directory sites. Optionally, the Hub Transport server can receive messages directly from the Internet, and the antispam agents found on the Edge Transport server can be installed on the Hub Transport server.

The Hub Transport server is also responsible for handling transport rules and per-mailbox journaling. It communicates with other Hub Transport servers in your organization using SMTP (authenticated via Kerberos and protected via TLS encryption). The Hub Transport communicates with the Mailbox server role using MAPI over RPC.

The Hub Transport role is similar to the concept of an Exchange 2000 or 2003 bridgehead server. The Hub Transport role handles the following responsibilities:

- SMTP communication — This function delivers all inbound and outbound messages to and from other organizations. If all the servers hosting the Hub Transport role fail within a site or domain, no mail will enter or leave your Exchange organization.
- Recipient name resolution — This function resolves the addressees for every message that is sent through an Exchange organization. This function also converts the contents of messages for transmission outside an Exchange organization.
- Executing transport rules and journaling — A new feature in Exchange 2007, transport rules allow administrators to define system-wide rules based on message sender, recipients, or contents. These rules can redirect, return, delete, or copy messages, allowing your organization to meet legal, regulatory, and internal compliance policy.
- Delivery and routing of messages — This is the most critical and complex function of the Hub Transport role. When messages are originated within your Exchange organization, they are collected by the store driver, which is a function of the Mailbox role. There they sit in a submission queue until the Hub Transport role collects them and processes them for delivery. If you have many Mailbox roles within your site and many sites within your organization, the Hub Transport role will find the most efficient route for your messages and ensure that they adhere to your organization's transport rules and journaling policies. If there are no functioning Hub Transport roles within your site, all mail will cease to be delivered.

The Hub Transport role is intended for your organization's intranet. Do not try to install the Hub Transport role in a DMZ or perimeter network; instead use an Edge Transport role. If you want an SMTP system in your perimeter network to send and receive mail outside your organization, you will have to allow inbound and outbound traffic on port 25 (TCP) between Exchange servers hosting the Hub Transport role and one of the following:

- An Exchange server hosting the Edge Transport role in a DMZ network
- A third-party mail relay host in a DMZ network
- The Internet

The Hub Transport role uses both MAPI RPCs and SMTP to communicate with servers running the Mailbox and Unified Messaging roles and should have at least Fast Ethernet (100 Mb/sec) connectivity to other Exchange 2007 servers in the same site that hosts those roles.

The Hub Transport role can be collocated on the same server with the Client Access, Unified Messaging, and Mailbox roles. However, unless you have a small organization, you may want to consider installing the Hub Transport role and the Mailbox role on separate servers so you can take advantage of its native load-balancing and failover features.

If the Hub Transport role is collocated on the same Exchange server as the Mailbox role, it will always use the locally installed Hub Transport service and only look for additional Hub Transport roles if the local Hub Transport service is not functioning. While this configuration generates the least amount of network traffic between the Mailbox role and the Hub Transport role, the best solution for organizations wishing to maximize their redundancy or those with high message volume is to use multiple Hub Transport roles installed on separate Exchange servers.

Note

Because the Mailbox role uses LDAP to directly communicate with Active Directory, it automatically discovers all Hub Transport roles installed in its native site and attempts to load-balance between the Hub Transport roles as long as they are not installed on the same server as the Mailbox role.

Client Access Server The Client Access server handles web services such as Outlook Web Access, Exchange ActiveSync for mobile devices, Outlook Anywhere (formerly RPC over HTTP), Autodiscover, the Availability service, and others. Each Active Directory site that has a mailbox server and requires these services must also have a Client Access server. While these services are not technically required for organizations that use Outlook 2003 and earlier exclusively, you may find that certain other features of Exchange 2007 will not work if you do not have a Client Access server in the Active Directory site. Unlike an Exchange 2003 front-end server, the Client Access server uses MAPI over RPC to communicate with mailbox servers; it does not use HTTP.

The Client Access role was designed to handle all of the protocols used by clients except SMTP and direct MAPI connections between Outlook and the Mailbox role. The Client Access role is responsible for the following services:

- Outlook Web Access (OWA) via HTTP(S) — OWA allows users to access their mail via a web browser.
- ActiveSync for mobile devices via HTTP(S) — ActiveSync allows mobile devices to securely synchronize mail, appointments, contacts, and in some cases tasks with Exchange. Popular clients include PocketPC 2002–2003, Windows Mobile 5–6, and PalmOne's VersaMail. Users running Windows Mobile 5 or later with the Messaging and Security Feature Pack or the latest version of PalmOne's VersaMail can also take advantage of Exchange 2007's Remote Wipe feature if their PDA is lost or stolen.
- Outlook Anywhere — This feature was formerly known as RPC over HTTPS. Outlook Anywhere allows remote users to *tunnel* MAPI RPC through SSL so they can securely use the full-featured version of Outlook as though they were inside your intranet.
- POP3 — Post Office Protocol 3 allows users to have basic access to their Inbox via almost every e-mail client on the planet. Some of the most popular POP3 e-mail clients are Outlook Express, Apple Mail, Mozilla Thunderbird, and Eudora. POP3 is limited in that it depends on the client to act as the authoritative message store, not the server. This can lead to problems when you are trying to synchronize more than one POP3 client to a server.

- IMAP4 — Exchange 2007 supports Internet Message Access Protocol version 4 revision 1. Like POP3, IMAP4 is supported by almost every e-mail client; however, IMAP4 depends on the server to act as the authoritative message store. Using IMAP4, clients can create subfolders on the server and can delete messages only when connected to the server. This allows users with multiple IMAP4 clients to access the same server without difficulty.
- Free/Busy data — Outlook 2007 clients leverage the Client Access role via the Availability service; this helps offload some of the Mailbox role's burden.
- Automatic Outlook 2007 client configuration — This eliminates the need for administrators to manually define connection parameters for Outlook 2007 clients by taking advantage of the Autodiscover service running on the Client Access role.
- WebDAV — Web-based Distributed Authoring and Versioning refers to a set of HTTP(S) extensions that allow users to remotely edit and manage files on a web server. WebDAV is required by both the Mac OS X Exchange client, Entourage, which is part of Microsoft Office for the Mac, and the Linux Exchange client, Evolution, developed by Novell.

Unlike with past versions of Exchange and IIS, a *default* install of the Client Access role on IIS 6.0 forces you to connect via at least a 128-bit encrypted SSL connection using a self-signed certificate. We strongly urge you to purchase a signed SSL certificate from a trusted certificate authority as all your users' login credentials are passed over this connection.

You must have at least one Client Access role per site and domain that has a Mailbox role, even if you don't intend to allow access to remote users via POP3, IMAP4, or Outlook Web Access. Certain features within Outlook 2007 depend on the Client Access role.

The Client Access Role is intended for your organization's intranet. Do not try to install the Client Access role in a DMZ or perimeter network; trying to do so will make your firewall administrator angry, and it is not supported by Microsoft. The Client Access role should have at least 100 Mb/sec connectivity to the Mailbox role and Unified Messaging role.

Note that the one remote user protocol not supported by the Client Access role is SMTP. If you plan to allow your users to send mail remotely via SMTP, you will require a Hub Transport server role configured to allow relay only from authenticated users.

Unified Messaging server The Unified Messaging server role is optional. It is only required if you are implementing Voice over IP voicemail integration, inbound faxing, Automated Attendant, or inbound Outlook Voice Access. All of these features require a compatible Voice over IP system.

Edge Transport server The Edge Transport server role is another optional server role, though Microsoft's marketing material might make it seem as if it's required. The Edge Transport server is designed to be an inbound/outbound mail hub that lives in your organization's perimeter or DMZ network. It is intended for a stand-alone server, not a domain member server. It receives its configuration regarding accepted domains, valid recipients, and per-recipient safe senders lists via a process called EdgeSync; data is pushed out to the Edge Transport server via LDAP and is stored in the Edge Transport server's Active Directory Application Mode (ADAM) database. The Edge Transport server includes antispam features such as sender filtering, recipient filtering, Sender ID, attachment filtering, block lists, and the content filter (formerly known as the Intelligent Message Filter). Additionally, you can install antivirus software on the Edge Transport server. If you already have a perimeter message hygiene system you are happy with, you can continue to use it instead of the Edge Transport system.

The advantage of using an Exchange server to host the Edge Transport role is that you can effectively quarantine and intelligently filter messages in a DMZ or perimeter network before they enter or exit your Exchange organization. The Edge Transport is designed to accept inbound SMTP messages from the Internet, isolate them while providing message hygiene (such as antivirus, antispam, and content filtering), and deliver them to the Hub Transport role. It is worth noting that the Edge Transport role is completely optional; however, it has some distinct advantages over similar third-party smart relay hosts and can greatly improve your Exchange servers' performance and security.

When defining your Exchange 2007 topology, you have three choices for how you would like to accept incoming messages from the Internet:

- You can route all inbound messages directly to an Exchange server running the Hub Transport role. This method bypasses all filtering and message isolation features, effectively allowing all inbound mail universal access. I do not recommend this configuration because it forces the Hub Transport role to filter all spam- and virus-laden e-mail in addition to its normal duties.
- You can route all inbound messages to a third-party smart relay host (either hosted in a DMZ or outsourced), which then forwards messages onto your Hub Transport. This method is a best practice of Exchange 2000 and 2003, but it offers no way to synchronize individual users' Blocked Senders list from Outlook with the smart relay host. I generally would not recommend this configuration unless you have a compelling reason to use an existing third-party solution because it usually requires your firewall administrator to open ports between the third-party solution and your Active Directory or Exchange servers in order to validate recipients.
- You can route all inbound messages to an Exchange server hosting the Edge Transport role residing in a DMZ or perimeter network. This solution allows you to take advantage of the Edge Subscription service, a new feature in Exchange 2007 that allows the Hub Transport role to perform a scheduled one-way synchronization of the Exchange configuration and recipient information via ADAM and the EdgeSync driver to the Edge Transport role. You don't have to open any firewall ports other than SMTP (port 25, TCP) from the DMZ to the intranet and two nonstandard LDAP ports (50389 and 50636, TCP) from the intranet to the DMZ.

Microsoft strongly recommends that you don't connect the Edge Transport role to your internal Active Directory forest, though you can connect the Edge Transport role to a domain in your DMZ or leave it as a stand-alone server if it makes your life easier. The Edge Subscription service also allows you to leverage all of Microsoft's built-in antispam features while the Hub Transport role allows only a subset of those features.

Note

One of the coolest features in the Edge Transport role is the ability to receive updates of an individual user's Allowed Senders list preferences from the Outlook client, thanks to the Edge Subscription service. This feature allows the Edge Transport role to accept e-mail from a user's safe senders without administrator intervention.

The Edge Transport role must be installed on its own server and cannot be colocated with any other roles. It should be placed in a DMZ and allowed inbound SMTP (port 25, TCP) connections both from the Internet and to the Hub Transport role inside your intranet. While activating the Edge Subscription feature is not included in the installation process, you should enable this feature to leverage the Hub Transport's ability to push filtering policies and recipient lists to the Edge Transport.

Tip

The Edge Transport role, when configured to use the Edge Subscription service, is managed by the Exchange Management Shell and Exchange Management Console. If you don't utilize the Edge Subscription service, you can manage the Edge Transport role only from the Exchange server on which it is installed.

Databases and Transaction Logs

There have been a number of changes made to the Exchange 2007 database to make it more robust and scalable, but the underlying architecture is still the Extensible Storage Engine (ESE). The database architecture has *not* been moved to a SQL Server database. Rather than writing a lengthy, wordy paragraph on each of the changes to the Exchange database system, I think a bulleted list is easier to digest.

- The STM file (the streaming database or native content store) is gone. Each Exchange database consists of a single EDB file (just as in Exchange 5.5).
- We now refer to the databases as databases again instead of *stores*.
- The transaction log file size is now 1 MB instead of the 5 MB in Exchange 2000/2003. This facilitates more efficient replication technologies. In a period of absolutely no activity, the current log (`E00.LOG` for example) is closed after 15 minutes.
- The database page size is now 8 KB instead of 4 KB.
- Just as in Exchange 2000/2003, each database page has a checksum that is verified to ensure page integrity.
- Just as in Exchange 2003, each transaction log has a checksum that is verified to ensure log file integrity.
- Databases can be moved to any Exchange 2007 mailbox server.
- Dial-tone restore to an alternate server or moving databases to an alternate server is now easier since the Exchange Management Shell `Move-Mailbox` cmdlet includes an option to move the user's configuration in Active Directory without actually trying to move their mail data.
- The maximum *recommended* database size is 100GB if continuous replication technology is not used and 200GB if continuous replication technology is used.
- The maximum *theoretical* database size of an Exchange Server 2007 database is 16TB.
- Exchange Server 2007 storage groups can have up to five databases. The recommendation is that you should scale upward (more storage groups) rather than adding more databases to a single storage group. However, if using clustered continuous replication, local continuous replication, or standby continuous replication, you must have only one database per storage group.
- Exchange Server 2007 Standard Edition allows up to five storage groups/databases of 50GB in size, but this can be increased up to 16TB via Registry keys.

- Exchange Server 2007 Enterprise Edition allows up to 50 storage groups/mailbox databases per server. The default database size is unlimited (16TB).
- The recommended disk allocation unit size is 64 KB when formatting disks for use with Exchange 2007 databases.

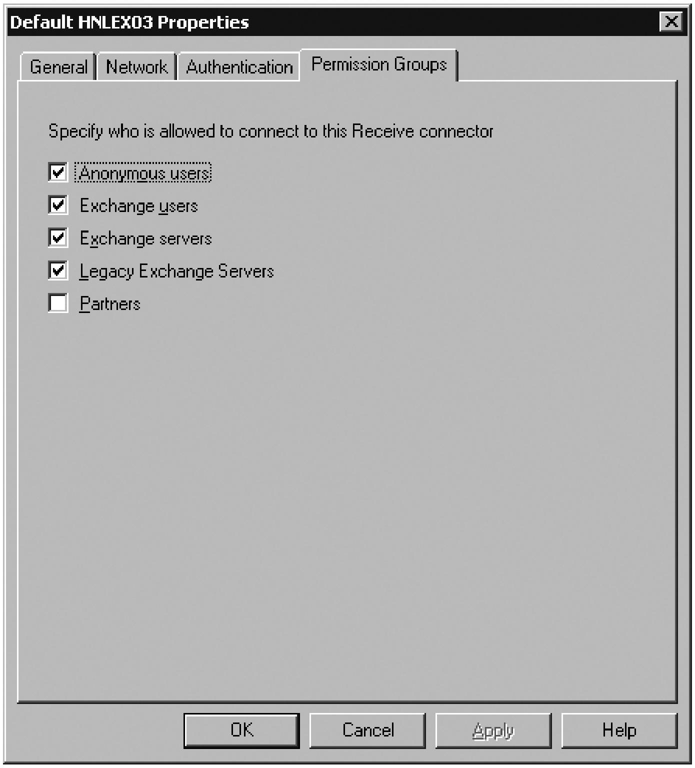
Send and Receive Connectors

In Exchange 2000/2003, e-mail was received over SMTP virtual servers and was sent over either an SMTP virtual server or an SMTP connector. Each server had at least one SMTP virtual server; SMTP connectors or routing group connectors could be configured to use that SMTP virtual server for inbound or outbound e-mail.

In Exchange Server 2007, only Hub Transport servers have Receive connectors. Each Hub Transport has (by default) two Receive connectors that will accept inbound SMTP mail. The client *ServerName* Receive connector is configured to use TCP port 587 and is designed for internal mail clients such as Outlook Express or other POP/IMAP clients.

The default *ServerName* Receive connector is configured to use TCP port 25 to accept mail. This Receive connector accepts mail from other Exchange 2007 Hub Transport servers within the organization. You might think that since this Receive connector listens on port 25, it would automatically accept mail from the Internet (or anonymous users). However, the default Receive connector accepts mail from only authenticated connections unless you configure on its Permissions page (shown in Figure 1.17) that it should accept mail from anonymous connections.

FIGURE 1.17
Setting permissions on the default Receive connector


Default HNLEX03 Properties

Specify who is allowed to connect to this Receive connector

☑ Anonymous users
☑ Exchange users
☑ Exchange servers
☑ Legacy Exchange Servers
☐ Partners

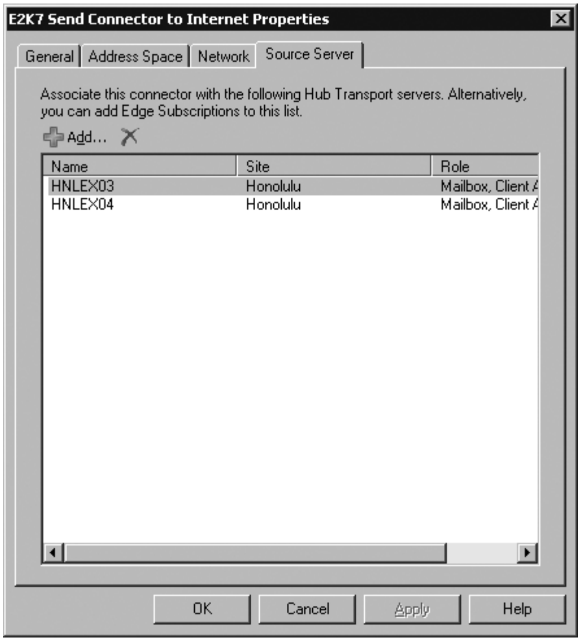
TIP

The SMTP protocol in Exchange 2007 is run by the Microsoft Exchange Transport service. The Transport service will stop processing messages if the free disk space on the transport database disk (usually the C: drive) drops below 4GB.

Outbound messages are handled by Send connectors. These are not a *per-server* resource but rather an organizational resource. You will not find any Exchange 2007 Send connectors (by default); if you are migrating from Exchange 2003, you will see your SMTP connectors, though. Exchange 2007 does have a hidden *internal* Send connector that is used for delivery of messages between Hub Transport servers in different Active Directory sites. You do not need to worry about this internal Send connector since there is nothing that the administrator can configure on it.

For e-mail that will be leaving your organization, you must configure a Send connector and define source servers; this is much like configuring bridgehead servers for the Exchange 2000/2003 SMTP connectors. The Send connector interface allows you to specify which Hub Transport servers will be responsible for delivering outbound SMTP mail; this is shown in Figure 1.18. The mail can be delivered directly to the Internet, sent to a smart host, or sent to an Edge Transport server.

FIGURE 1.18
Defining source servers for a Send connector



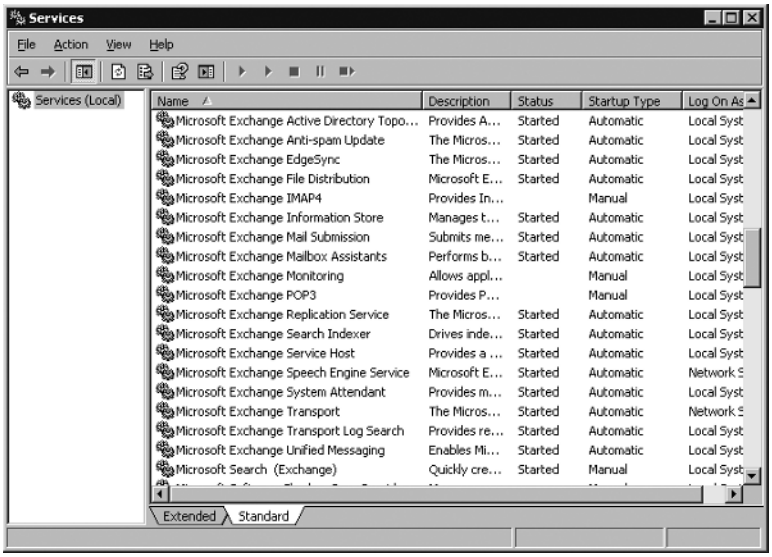
Associate this connector with the following Hub Transport servers. Alternatively, you can add Edge Subscriptions to this list.

Name	Site	Role
HNLEX03	Honolulu	Mailbox, Client A
HNLEX04	Honolulu	Mailbox, Client A

Service Names

The services and components that you find on an Exchange 2007 server will vary depending on which roles are installed for that server. Figure 1.19 shows some of the Exchange 2007 services that are found in the services console.

FIGURE 1.19
Common Exchange Server 2007 services



Name	Description	Status	Startup Type	Log On As
Microsoft Exchange Active Directory Topo…	Provides A…	Started	Automatic	Local Syst
Microsoft Exchange Anti-spam Update	The Micros…	Started	Automatic	Local Syst
Microsoft Exchange EdgeSync	The Micros…	Started	Automatic	Local Syst
Microsoft Exchange File Distribution	Microsoft E…	Started	Automatic	Local Syst
Microsoft Exchange IMAP4	Provides In…		Manual	Local Syst
Microsoft Exchange Information Store	Manages t…	Started	Automatic	Local Syst
Microsoft Exchange Mail Submission	Submits me…	Started	Automatic	Local Syst
Microsoft Exchange Mailbox Assistants	Performs b…	Started	Automatic	Local Syst
Microsoft Exchange Monitoring	Allows appl…		Manual	Local Syst
Microsoft Exchange POP3	Provides P…		Manual	Local Syst
Microsoft Exchange Replication Service	The Micros…	Started	Automatic	Local Syst
Microsoft Exchange Search Indexer	Drives inde…	Started	Automatic	Local Syst
Microsoft Exchange Service Host	Provides a …	Started	Automatic	Local Syst
Microsoft Exchange Speech Engine Service	Microsoft E…	Started	Automatic	Network S
Microsoft Exchange System Attendant	Provides m…	Started	Automatic	Local Syst
Microsoft Exchange Transport	The Micros…	Started	Automatic	Network S
Microsoft Exchange Transport Log Search	Provides re…	Started	Automatic	Local Syst
Microsoft Exchange Unified Messaging	Enables Mi…	Started	Automatic	Local Syst
Microsoft Search (Exchange)	Quickly cre…	Started	Manual	Local Syst

If you are an experienced Exchange 2000/2003 administrator, you will also find that many of the services and executables are not recognizable; at least I did. Exchange 2000/2003 has fewer core components and all core components were installed on any Exchange server that you built. The Exchange Server 2007 components are shown in Table 1.7.

TABLE 1.7: Exchange Server 2007 Components

SERVICE NAME/ SHORT SERVICE NAME	EXECUTABLE NAME	FUNCTION
Microsoft Exchange Active Directory Topology / MSExchangeADTopology	`MSExchangeADTopologyService.exe`	Provides Exchange Server 2007 with Active Directory site, domain controller, and global catalog server information. This component is found on all Exchange 2007 server roles except the Edge Transport.
Microsoft Exchange ADAM / ADAM_MSExchange	`Dsamain.exe`	This is the ADAM instance that holds the Edge Transport server role's configuration, recipient information, safe senders lists, and blocked senders lists. This service is only found on the Edge Transport role.
Microsoft Exchange Anti-spam Update / MSExchangeAntispamUpdate	`Microsoft.Exchange.AntispamUpdateSvc.exe`	This service provides updates for the content filter service. This service is found on the Edge Transport and Hub Transport server roles.

Table 1.7: Exchange Server 2007 Components *(CONTINUED)*

Service Name/ Short Service Name	**Executable Name**	**Function**
Microsoft Exchange Credential Service / EdgeCredentialSvc	`EdgeCredentialSvc.exe`	This service monitors credential changes for the ADAM database and updates the Edge Transport server. This service is found only on the Edge Transport server role.
Microsoft Exchange EdgeSync / MSExchangeEdgeSync	`Microsoft.Exchange.EdgeSyncSvc.exe`	Handles synchronization of recipient and Hub Transport information to Edge Transport servers in the perimeter network. The EdgeSync process synchronizes to the Edge Transport server's ADAM database; the synchronization is a push synchronization from the Hub Transport role out to the Edge Transport server. This component is found on Exchange 2007 Hub Transport server roles.
Microsoft Exchange File Distribution / MSExchangeFDS	`MSExchangeFDS.exe`	The File Distribution service handles distribution of offline address books on Client Access servers and custom Unified Messaging prompts on UM servers. It is found on Exchange 2007 Client Access and Unified Messaging server roles.
Microsoft Exchange IMAP4 / MSExchangeIMAP4	`Microsoft.Exchange.Imap4Service.exe`	Provides IMAP4 client connectivity and is found on Exchange 2007 Client Access server roles. This service is set to manual by default and must be enabled to support IMAP4 clients.
Microsoft Exchange Information Store / MSExchangeIS	`Store.exe`	The information store service runs the database engine and provides client access for MAPI clients as well as access to mailboxes for connections from Client Access and Hub Transport servers. This service is only found on Exchange 2007 servers with the Mailbox server role. It also consumes the most RAM of any of the Exchange 2007 services.
Microsoft Exchange Mail Submission Service / MSExchangeMailSubmission	`MSExchangeMailSubmission.exe`	Handles notifying Hub Transport servers that a message is waiting to be retrieved from a local database. This service attempts to distribute the message delivery load if multiple Hub Transport servers are found. This role is found on the Exchange 2007 Mailbox server role.

(CONTINUED)

Table 1.7: Exchange Server 2007 Components *(CONTINUED)*

Service Name/ Short Service Name	Executable Name	Function
Microsoft Exchange Mailbox Assistants / MSExchangeMailboxAs-sistants	`Microsoft.Exchange .InfoWorker .Assistants.exe`	The Mailbox Assistants service handles calendaring functionality such as Calendar Assistant, Resource Booking Assistant, Out-of-Office Assistant, and the Managed Folder Mailbox Assistant. This service is found only on Exchange 2007 mailbox servers.
Microsoft Exchange Monitoring / MSExchangeMonitoring	`Microsoft.Exchange .Monitoring.exe`	Provides an interface for applications to use Exchange 2007 monitoring tasks. This service is found on all Exchange 2007 server roles.
Microsoft Exchange POP3 / MSExchangePOP3	`Microsoft.Exchange .Pop3Service.exe`	Provides POP3 client connectivity and is found on Exchange 2007 Client Access server roles. This service is set to manual by default and must be enabled to support POP3 clients.
Microsoft Exchange Replication Service / MSExchangeRepl	`Microsoft.Exchange .Cluster .ReplayService.exe`	This service handles copying log files from their original location to the backup log location on Exchange 2007 Mailbox servers that have the local continuous replication or clustered continuous replication functions enabled. This service is found only on Exchange 2007 Mailbox server roles.
Microsoft Exchange Search Indexer / MSExchangeSearch	`Microsoft.Exchange .Search.ExSearch.exe`	The Exchange Content Search Indexer provides content to the Microsoft Search (Exchange Server) service for full-text indexing. This service is found only on Mailbox server roles.
Microsoft Exchange Service Host / MSExchangeServiceHost	`Microsoft.Exchange .ServiceHost.exe`	This service handles the RPC virtual directories and Registry information necessary to support Outlook Anywhere (RPC over HTTP). This service is found on Exchange Mailbox and Client Access server roles.
Microsoft Exchange Speech Engine / MSS	`MSSService .SpeechService.exe`	The Speech Engine service provides the speech processing capabilities that are used by Unified Messaging services. This service is found only on Unified Messaging server roles.
Microsoft Exchange System Attendant / MSExchangeSA	`Mad.exe`	This service provides monitoring and directory lookup services for Exchange Server. This service is found only on Mailbox server roles.

Table 1.7: Exchange Server 2007 Components *(CONTINUED)*

Service Name/ Short Service Name	Executable Name	Function
Microsoft Exchange Transport / MSExchangeTransport	`MSExchange-Transport.exe`	This service provides the SMTP transport functions. Mail will not flow at all if this service is halted. This service is found on all Exchange 2007 Hub Transport and Edge Transport server roles.
Microsoft Exchange Transport Log Search / MSExchangeTransport-LogSearch	`MSExchange-TransportLogSearch.exe`	Provides the ability to search the Exchange message transport logs. This service is found on all Exchange 2007 Mailbox, Hub Transport, and Edge Transport server roles.
Microsoft Exchange Unified Messaging / MSExchangeUM	`Umservice.exe`	The Unified Messaging service handles access to a user's mailbox via Outlook Voice Access, the creation of voicemail messages, and the creation of fax messages. This service is found only on the Unified Messaging server role.
Microsoft Search (Exchange) / MSFTESQL-Exchange	`Msftesql.exe`	This Search service creates full-text indexes on mailbox content. This service is only found on the Exchange 2007 Mailbox server role.
World Wide Web Publishing Service	`svchost.exe` / `inetinfo`	A component of Internet Information Services that is required on all Exchange 2007 Client Access server roles in order to provide access to web services. This service is required on Exchange 2007 Mailbox servers if you will be managing public folders using Exchange System Manager or PFDAVAdmin.

Depending on the server's role(s), you will see many of these executables in the Windows Task Manager (shown in Figure 1.20). One frequently misunderstood service is the Microsoft Exchange Information Store service, or `store.exe`; by design this service will attempt to allocate as much physical memory as possible. On a server with 32GB of physical memory, it may not be unusual to see this service using 80 to 90 percent of that RAM. This is a feature, not a bug.

Notice also in Figure 1.20 that there are some service names that start with FSC; these services are part of Microsoft's Forefront Security for Exchange Server. This product can be used if you have enterprise client access licenses for all of your users.

Message Security Features

In my first meeting with my organization's IT team leads, where I was briefing them on our plans to deploy Exchange Server 2007, everyone was asked for comments. When it came time for our information security lead to speak, he said, ''I have no objections; everything I have read indicates

Exchange Server 2007 is more secure.'' I was pleased since that meant I could avoid a lengthy process of proving it was more secure, but it also indicates that people perceive that Exchange 2007 provides better security. This does not mean that you can avoid good security practices, but hopefully it will mean that you are providing better security out of the box.

In the following sections, I'll review some of the improvements that have been made to Exchange Server 2007 so that it provides better, more secure messaging services to end users.

FIGURE 1.20 Viewing the top consumers of RAM on an Exchange 2007 server

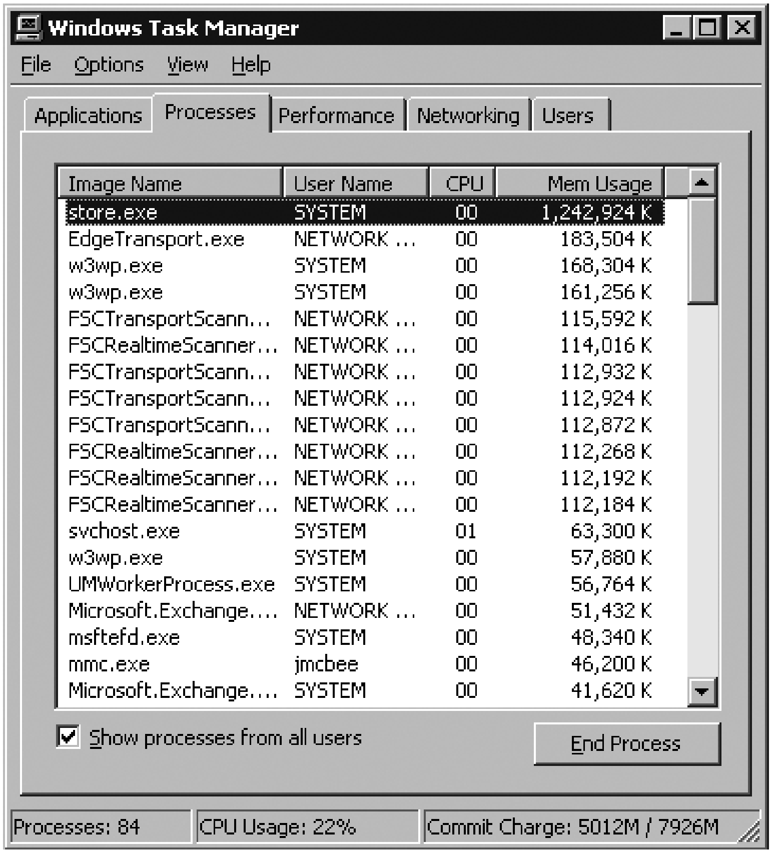


Image Name	User Name	CPU	Mem Usage
store.exe	SYSTEM	00	1,242,924 K
EdgeTransport.exe	NETWORK ...	00	183,504 K
w3wp.exe	SYSTEM	00	168,304 K
w3wp.exe	SYSTEM	00	161,256 K
FSCTransportScann...	NETWORK ...	00	115,592 K
FSCRealtimeScanner...	NETWORK ...	00	114,016 K
FSCTransportScann...	NETWORK ...	00	112,932 K
FSCTransportScann...	NETWORK ...	00	112,924 K
FSCTransportScann...	NETWORK ...	00	112,872 K
FSCRealtimeScanner...	NETWORK ...	00	112,268 K
FSCRealtimeScanner...	NETWORK ...	00	112,192 K
FSCRealtimeScanner...	NETWORK ...	00	112,184 K
svchost.exe	SYSTEM	01	63,300 K
w3wp.exe	SYSTEM	00	57,880 K
UMWorkerProcess.exe	SYSTEM	00	56,764 K
Microsoft.Exchange....	NETWORK ...	00	51,432 K
msftefd.exe	SYSTEM	00	48,340 K
mmc.exe	jmcbee	00	46,200 K
Microsoft.Exchange....	SYSTEM	00	41,620 K

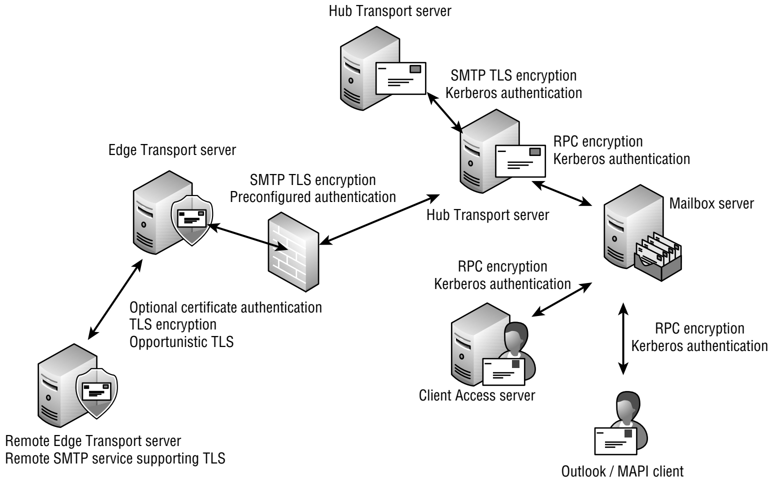
☑ Show processes from all users

Processes: 84 | CPU Usage: 22% | Commit Charge: 5012M / 7926M

Network Data Protection

When we talk about network data protection, it can mean many different things. In this particular case, I am referring to protecting the data in transit. Figure 1.21 shows a number of different improvements and components that allow for better protection of message content while a message is in transit. First, all Exchange 2007 servers in the same organization use Kerberos for authentication; this has not actually changed since Exchange 2000/2003. Figure 1.21 also shows the Outlook MAPI client using RPC encryption between Outlook and the Mailbox server; this feature has been available with Outlook and Exchange Server for a long time, but now the Exchange Server administrator can require MAPI client encryption through a server configuration option.

FIGURE 1.21
Network encryption between clients and servers



All communication between the Hub Transport or Client Access server roles and the Mailbox server is also encrypted with RPC encryption. As Hub Transport servers deliver messages to one another or as messages to and from the Edge Transport servers, TLS encryption is used to protect the messages in transit. Hub Transport servers use Kerberos to authenticate with one another, while Hub Transport and Edge Transport servers use credentials that are established when the EdgeSync process is configured.

Opportunistic TLS

As most mail administrators know, most SMTP traffic over the Internet is sent via clear text. A message may be *encoded* using multipurpose Internet mail extensions (MIME), but ultimately if someone intercepts this message, it can be decoded very easily. If you are interested in protecting SMTP data over the Internet, a new feature of the Edge Transport and Hub Transport servers you will like is called opportunistic TLS, or opportunistic SSL/TLS

Many SMTP mail transport engines support opportunistic TLS today, so it is nice that Exchange 2007 is finally on the bandwagon. If you have configured an SSL certificate to work with SMTP, then it will automatically negotiate a TLS session if the remote SMTP system also supports TLS. This means that any mail you send over the Internet to a TLS-compatible SMTP server will automatically be encrypted while it is being transmitted.

Domain Security

Domain Security is probably one of the most poorly named features in Exchange 2007, mostly because it does not really give you much of an idea of what it does. I personally would have gone for something like Trusted Messaging, although that's not much better. Domain Security takes advantage of opportunistic TLS, certificates issued by a trusted certificate authority, Exchange 2007, and Outlook 2007/Outlook Web Access so that messages that have been sent to your users by a previously configured trusted source are delivered with the label *Domain Secured*. This gives the user an indication that the message really did originate from a trusted source.

Domain Security provides some assurances about the trustworthiness of a message, but it is not an end-to-end solution like S/MIME, nor is it a content control system like Windows Rights

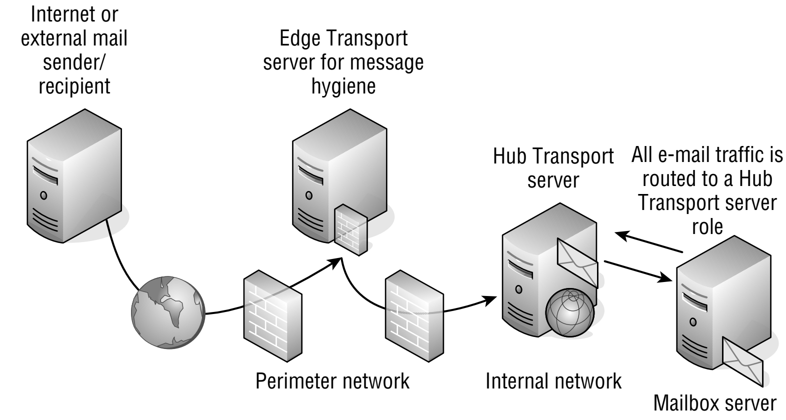
Management. There are a few requirements for Domain Security to work properly, including both software and administrative tasks:

- The remote Exchange organization must use Exchange 2007 and use a certificate that was issued by a trusted certificate authority.
- The administrator in the remote organization must configure your SMTP domain as a trusted domain.
- You must configure the remote organization's SMTP domain as a trusted domain.
- You must use a certificate that was issued by a trusted certificate authority.
- The clients must be using Outlook Web Access 2007 or Outlook 2007 in order to see the *Domain Secured* information.

Antispam Features

Microsoft has made a concerted effort to ensure that Exchange 2007 offers a better platform for spam control. I briefly mentioned the Edge Transport server earlier in this chapter, but let's take a look at some of the basics. Figure 1.22 shows what it would look like if you deployed an Edge Transport server in your organization. Inbound SMTP mail is delivered to the Edge Transport server for antispam inspection (and possibly antivirus inspection). Outbound mail is delivered through the internal Hub Transport to the Edge Transport server. Figure 1.22 shows this arrangement.

FIGURE 1.22
Deploying the Edge Transport server


Internet or external mail sender/ recipient
Edge Transport server for message hygiene
Hub Transport server
All e-mail traffic is routed to a Hub Transport server role
Perimeter network
Internal network
Mailbox server

The Edge Transport server has specifically been designed so that it is easier to ''harden'' and to place in the organization's perimeter/ DMZ network. The Edge Transport server role should be a stand-alone server (not part of the internal Active Directory). However, since it must be a 64-bit version of Windows, it cannot coexist with ISA Server 2006 (unless Microsoft releases a 64-bit version of ISA Server, which will probably happen someday).

The Edge Transport has a number of antispam agents preinstalled (and some configured with defaults already enabled). Here are the antispam agents that are installed on the Edge Transport server:

- The *content filter* is the agent formerly known as the Intelligent Message Filter. This agent technology is based on Microsoft's SmartScreen technology; the filter definitions can be updated hourly if you have Enterprise client access licenses or every two weeks otherwise. The content filter can be configured to reject, delete, quarantine, and put suspected spam into the user's Junk E-mail folders. It includes the ability to specify safe words and blocked words.

- *Block lists* and *allow lists* allow you to specify lists of IP addresses from which you will always accept mail or always reject mail. You can also use a real-time block list such as Spamhaus or SORBS and reject mail based on known sources of spam.
- *Per-user safe senders lists* allow you to push to the Edge Transport server each user's safe senders list that they create in Outlook. This reduces the possibility that valid mail will be rejected or quarantined by another filter such as the content filter. Per-user block lists are not pushed to the Edge Transport server.
- The *attachment filter* allows you to specify filenames, extensions, and MIME types that will be stripped before the message is allowed to pass through the transport system. The attachment transport filter is only available on the Edge Transport server role.
- The *recipient filter* allows you to specify a list of recipients that will be rejected when they are sent to your Edge Transport server or to specify that messages will be rejected for all invalid recipients.
- The *sender filter* allows you to specify a list of senders from which you should not accept mail.
- The *sender reputation filter* enables the Edge Transport server to analyze connections from external mail servers for protocol errors or for an open proxy. If consistent errors are found, the sender's IP address is placed on a quarantine list for some period of time (the default is 36 hours).
- Sender ID is an antispoofing technology that allows your server to inspect the sender's server information and verify that the message was indeed sent from an authorized server for the sender's domain. If the message is not from an authorized server, Sender ID can pass along information to the content filter that increases the spam confidence level.

All of these filters (except the attachment filter) can be installed on an Exchange Server 2007 Hub Transport server role. Installing all of the anti-spam agents on the Hub Transport server role will be useful for small organizations that have only a single server and don't want to put an additional Edge Transport server in the perimeter/DMZ network.

Since the release of Exchange 2007, there have been a lot of misconceptions about the Edge Transport server. I want to run through a list of facts (and my opinions) that you will probably want to know as you deploy Exchange 2007 and hopefully clear up those misconceptions:

- Edge Transport server is an optional server role; it is not required for Exchange 2007.
- You can continue to use your existing third-party message hygiene system if you do not want to use the Edge Transport role.
- You will not realize the complete benefits of an Edge Transport server until you have deployed Exchange 2007 Hub Transport servers, moved your users' mailboxes to Exchange 2007 Mailbox servers, and created EdgeSync to synchronize your configuration to the Edge Transport server.

- An antivirus solution is not included with the Edge Transport; you must separately install a solution such as Microsoft's Forefront Security for Exchange.

Outlook Web Access

Outlook Web Access was one of the components of Exchange 2007 that was almost completely rewritten from scratch. The major reason that OWA was rewritten was so that it would use the new web services APIs instead of using WebDAV (Exchange 2000/2003) and so that it better used the client/server architecture of the Client Access server. In Exchange 2000/2003, an Outlook Web Access front-end server communicated with the Mailbox server using HTTP, but with Exchange 2007, the Client Access server uses an optimized version of MAPI to communicate with the Mailbox server. The result is a smoother and more functional interface than we had in Exchange 2000/2003. The main page is shown in Figure 1.23.

For those of you who reviewed Exchange 2007 when it was initially released, let's catch you up. Exchange 2007 Service Pack 1 and later includes not only an interface for accessing public folders but also the S/MIME web control (for viewing and sending S/MIME messages), a rules editor, and the calendar month view. Users can now also manage their personal distribution groups. These were features that were missing from the original release of Exchange Server 2007.

Some of the new features are certainly very noteworthy though. For users that need access to SharePoint document libraries or shared folders on the network, the remote file access feature is useful. If the user clicks on the Documents shortcut link, they can open up document libraries and documents on the internal network; an example of this is shown in Figure 1.24. The user can only open the documents or copy them though; they cannot update them or delete them.

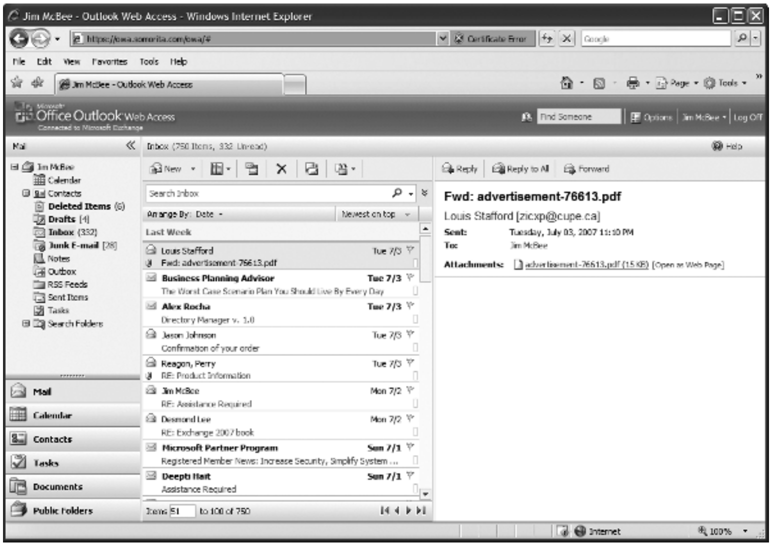


FIGURE 1.23
Introducing Outlook Web Access 2007

Louis Stafford Tue 7/3
Fwd: advertisement-76613.pdf

Business Planning Advisor **Tue 7/3**
The Worst Case Scenario Plan You Should Live By Every Day

Alex Rocha **Tue 7/3**
Directory Manager v. 1.0

Jason Johnson Tue 7/3
Confirmation of your order

Reagon, Perry Tue 7/3
RE: Product Information

Jim McBee Mon 7/2
RE: Assistance Required

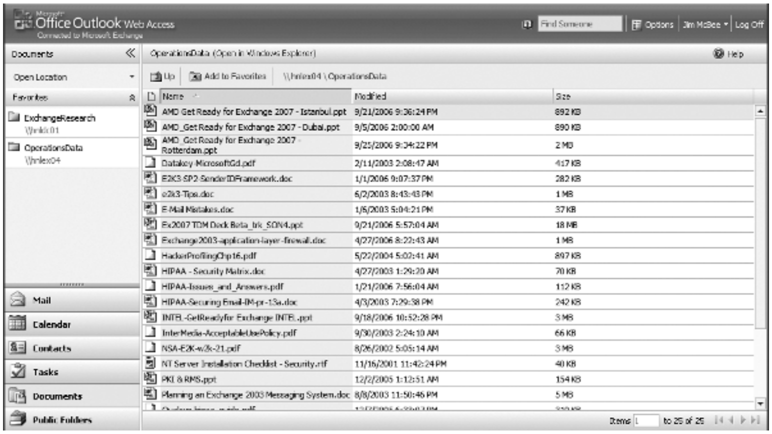
Desmond Lee Mon 7/2
RE: Exchange 2007 book

Microsoft Partner Program **Sun 7/1**
Registered Member News: Increase Security, Simplify System ...

Deepti Hait **Sun 7/1**
Assistance Required

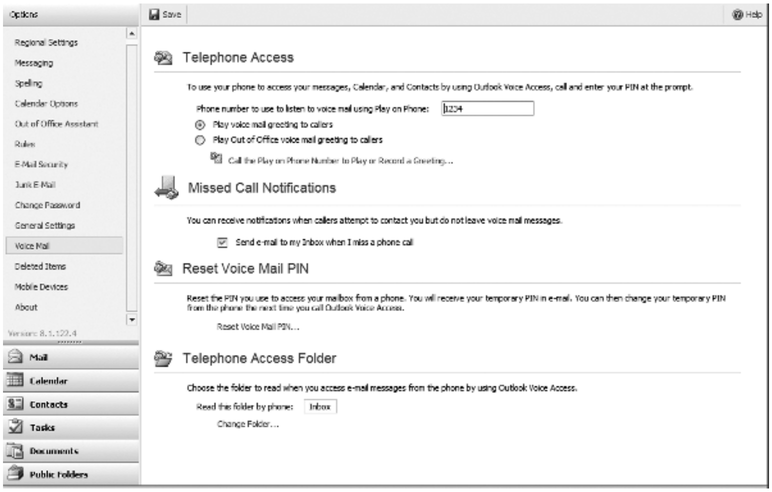
Fwd: advertisement-76613.pdf
Louis Stafford [zicxp@cupe.ca]
Sent: Tuesday, July 03, 2007 11:10 PM
To: Jim McBee
Attachments: advertisement-76613.pdf (15 KB) [Open as Web Page]

If your organization is using Unified Messaging, users can now control some of their own Unified Messaging features, such as the extension number where they can redirect voicemails for playback, missed call notification, and which folder to use to read e-mail messages via Outlook Voice Access. Users can also reset their Unified Messaging personal identification number (PIN) via OWA. These actions can all be performed via the Voice Mail configuration options in OWA (shown in Figure 1.25).



Name	Modified	Size
AMD Get Ready for Exchange 2007 - Istanbul.ppt	9/21/2006 9:36:24 PM	892 KB
AMD_Get Ready for Exchange 2007 - Dubai.ppt	9/5/2006 2:00:00 AM	890 KB
AMD_Get Ready for Exchange 2007 - Rotterdam.ppt	9/25/2006 9:34:22 PM	2 MB
Datakey-MicrosoftGd.pdf	2/11/2003 2:08:47 AM	417 KB
E2K3-SP2-SenderIDFramework.doc	1/1/2006 9:07:37 PM	282 KB
e2k3-Tips.doc	6/2/2003 8:43:43 PM	1 MB
E-Mail Mistakes.doc	1/6/2003 5:04:21 PM	37 KB
Ex2007 TDM Deck Beta_trk_SON4.ppt	9/21/2006 5:57:04 AM	18 MB
Exchange2003-application-layer-firewall.doc	4/27/2006 8:22:43 AM	1 MB
HackerProfilingChp16.pdf	5/22/2004 5:02:41 AM	897 KB
HIPAA - Security Matrix.doc	4/27/2003 1:29:20 AM	70 KB
HIPAA-Issues_and_Answers.pdf	1/21/2006 7:56:04 AM	112 KB
HIPAA-Securing Email-IM-pr-13a.doc	4/3/2003 7:29:38 PM	242 KB
INTEL-GetReadyfor Exchange INTEL.ppt	9/18/2006 10:52:28 PM	3 MB
InterMedia-AcceptableUsePolicy.pdf	9/30/2003 2:24:10 AM	66 KB
NSA-E2K-w2k-21.pdf	8/26/2002 5:05:14 AM	3 MB
NT Server Installation Checklist - Security.rtf	11/16/2001 11:42:24 PM	40 KB
PKI & RMS.ppt	12/2/2005 1:12:51 AM	154 KB
Planning an Exchange 2003 Messaging System.doc	8/8/2003 11:50:46 PM	5 MB

FIGURE 1.24
Document access via Outlook Web Access



Telephone Access

To use your phone to access your messages, Calendar, and Contacts by using Outlook Voice Access, call and enter your PIN at the prompt.

Phone number to use to listen to voice mail using Play on Phone: 1234

● Play voice mail greeting to callers

○ Play Out of Office voice mail greeting to callers

Call the Play on Phone Number to Play or Record a Greeting...

Missed Call Notifications

You can receive notifications when callers attempt to contact you but do not leave voice mail messages.

☑ Send e-mail to my Inbox when I miss a phone call

Reset Voice Mail PIN

Reset the PIN you use to access your mailbox from a phone. You will receive your temporary PIN in e-mail. You can then change your temporary PIN from the phone the next time you call Outlook Voice Access.

Reset Voice Mail PIN...

Telephone Access Folder

Choose the folder to read when you access e-mail messages from the phone by using Outlook Voice Access.

Read this folder by phone: Inbox

Change Folder...

FIGURE 1.25
End-user management of Unified Messaging features through Outlook Web Access.

Finally, another of the most promising new features of Outlook Web Access is the ability to let the users manage properties of their Windows Mobile devices. This is something that had to be done by the administrator in Exchange 2003. End-user management features include removing the device partnership with the mailbox, remotely wiping out the device, and viewing the device password.

Exchange Editions and Licensing

When you plan to purchase Exchange 2007, you need to make sure that you purchase the correct edition of Exchange server and purchase the client access licenses to license the features that you will require. Table 1.8 lists some of the features that are included with Exchange 2007 Standard Edition versus Enterprise Edition.

TABLE 1.8: Exchange 2007 Standard Edition versus Enterprise Edition

FEATURE	STANDARD	ENTERPRISE
Maximum database size	16TB (unlimited)	16TB (unlimited)
Maximum number of storage groups	5	50
Supports Recovery Storage Group	✓	✓
Number of databases	5	50
Supports Client Access Server role	✓	✓
Supports single copy clustered mailbox servers		✓
Supports clustered continuous replication mailbox servers		✓
Supports Edge Transport role	✓	✓
Supports Hub Transport role	✓	✓
Supports local continuous replication	✓	✓
Supports Mailbox role	✓	✓
Supports Unified Messaging role	✓	✓

In the past, you only had a single option when purchasing Exchange server client access licenses (CALs). Exchange 2007 introduces the Exchange Enterprise CAL and Exchange Standard CAL. Either of these CALs can be used against either Exchange Server Enterprise Edition or Exchange Server Standard Edition. The choice for which CAL you require will depend on which premium features of Exchange Server 2007 you will need.

The Exchange Enterprise CAL adds additional features above and beyond the Exchange Standard CAL. The Exchange Standard CAL provides your users with the ability to use Exchange features such as accessing their mailbox from a MAPI client, Outlook Web Access, ActiveSync devices, and Outlook Anywhere (RPC over HTTP). The Exchange Enterprise CAL includes the following additional functions:

- Unified Messaging services
- Microsoft Forefront Security for Exchange Server
- Advanced compliance capabilities such as per-user and per-distribution-group journaling
- Messaging records management features
- Antispam and antivirus protection using Microsoft Exchange Hosted Filtering Services as an external service provider.

Standard client access licenses must be purchased for each mailbox that is accessed on your system. If you have users that use multiple devices (Outlook, Outlook Web Access, ActiveSync, Outlook Anywhere) to access their mailbox and the total percentage of time they spend accessing their mailbox from their primary device is less than 80 percent, then you must purchase an additional CAL for that user.

If you use Exchange Enterprise CALs for all of your users, then you get to use all of the features available for Enterprise CALs. However, if you purchase Enterprise CALs for only a subset of your users that require a feature such as Unified Messaging and journaling and also choose to use Forefront Security for Exchange, then the remainder of the users must be licensed separately for Forefront Security for Exchange.

Shortly after Exchange 2007 was released, Microsoft changed the licensing for the messaging records management features. Originally you had to have an enterprise client access license for each mailbox on which you were going to run messaging records management. However, the license agreement was changed so that messaging records management could be used against the default folders (Inbox, Sent Items, Deleted Items, and so on) even if you only have standard client access licenses for your users.

Hardware and Software Requirements

One of the most important decisions you make when you are installing Exchange Server is to make sure you are using the right hardware. Incorrectly sized hardware may cause you to spend too much money for the functionality you need, or if you don't have enough hardware capacity, you may be continually low on disk space, have backups that take too long, or worst of all, have users complaining about performance and message delivery.

When you are sizing your hardware, even if you will initially be using Windows Server 2003 SP2, you should make sure you can support Windows Server 2008.

Hardware Requirements

In the past, Microsoft has made recommendations for hardware based on the absolute minimum resources required to run Exchange Server. Now, however, the recommendations are much more practical for real-world deployment and take into consideration the goal of optimal performance and supporting applications that often run in concert with Exchange Server, such as antivirus, antispam, archiving, management, monitoring, and reporting software.

Since the launch of Exchange 2007, Microsoft has made several revisions to the official best practices guide for sizing your Exchange server hardware. These revisions are based on feedback from customers running Exchange in production as well as the developers who are writing code to take advantage of the latest hardware. In the following sections, I will summarize Microsoft's best practices and add my recommendations where applicable.

With previous versions of Exchange, Microsoft's minimum hardware recommendations were laughable even for a test environment. While Windows 2000 can theoretically run on a Pentium 133 MHz processor with 32 MB of RAM, no IT professional would punish their most despised user with such a meager configuration. Lately, Microsoft has opted instead to provide customers with the following three tiers of configurations:

- Minimum: The bare minimum hardware configuration necessary to run the product. The minimum configuration must be met in order to receive technical support from Microsoft.
- Recommended: The ideal hardware configuration for a server that is running at 75 to 80 percent of its capacity during peak hours. The recommended configuration is one that Microsoft feels is the best balance between price and performance.

- Maximum: The maximum hardware configuration that the product is designed to utilize. The maximum recommendation is based on the product only; if you have additional services or applications running on the server, you may opt to exceed the maximum recommendation.

Processors

The requirement for 64-bit processors is the first big change for Exchange 2007. The processor should be at least an 800 MHz processor, though you will certainly benefit from processors faster than 2GHz or dual-core processors. The processor must be either an Intel Xeon or Intel Pentium x64 processor that supports the Intel Extended Memory 64 Technology (EM64 T) or an AMD Opteron or Athlon 64-bit processor that supports the AMD64 platform. The Intel Itanium IA64 processor family is not supported. Table 1.9 shows the processor recommendations from Microsoft for different Exchange Server 2007 roles.

You may have noticed in Table 1.9 that the maximum number of processors or processor cores for some server roles is less than the maximum that Windows can actually support. Most multithreaded applications will reach a point of diminishing returns when you add more processors, so it may not be worth it to add the maximum number of processors that Windows supports.

In environments that scale past a few hundred mailboxes, certainly dual- or quad-processor systems will be put to good use. For organizations that deploy a combination of roles to different physical machines, you will almost always benefit from a dual-processor or dual-core-processor system.

Table 1.9: Processor Recommendations Based on Server Role

Exchange 2007 Server Role	Minimum	Recommended	Recommended Maximum
Edge Transport	1 x processor core	2 x processor cores	4 x processor cores
Hub Transport	1 x processor core	4 x processor cores	4 x processor cores
Client Access	1 x processor core	4 x processor cores	4 x processor cores
Unified Messaging	1 x processor core	4 x processor cores	4 x processor cores
Mailbox	1 x processor core	4 x processor cores	8 x processor cores
Multiple server roles (combinations of Hub Transport, Client Access, Unified Messaging, and Mailbox server roles)	1 x processor core	4 x processor cores	4 x processor cores

The single most debated and significant change between Exchange 2003 and Exchange 2007 is the move to 64-bit architecture. For those of you who missed the memo, Exchange 2007 will not run in production on 32-bit hardware or in a 32-bit operating system.

Note the subtle use of the word *production*. There is a 32-bit version of Exchange, but it is only meant to be deployed in a lab or training environment. For those of you thinking of blurring the line between your lab and production network, forget it. There's no way to activate the 32-bit version of Exchange (I've tried). The good news is that you can still run the 32-bit version of Exchange after the trial period has expired (for now) so you don't have to rebuild your lab environment every 120 days. However, you will be faced with a *nag dialog* every time you open the Exchange Management Console.

Tip

Microsoft's recommendations are for processor cores, not processors. If you have a dual-processor, quad-core server, you effectively have eight cores.

Physical Memory

As we have mentioned previously, the advantage that Exchange 2007 really gets out of the 64-bit architecture is the ability to access more physical memory. Additional physical memory improves caching, reduces the disk I/O profile, and allows for the addition of more features.

Microsoft recommends a minimum of 1GB of RAM in each Exchange 2007 server or 2GB for each server supporting the Mailbox server role. This will, of course, depend on the roles that the server is supporting. Table 1.10 shows the minimum recommended memory for each of the server roles.

Tip

There can be a profound difference between different manufacturers and even models of servers depending on the motherboard. Years ago, I purchased a server that could recognize a maximum of 16GB of RAM. A year or so later, I hoped to upgrade the RAM but found in the small print that the server could only recognize 16GB of single-ranked DIMMs, which are twice as expensive as dual-ranked DIMMs. After researching the issue, I realized that the dual-ranked DIMMs offer considerably better performance than single-ranked DIMMs but are limited to a maximum of 8GB because all the available ranks are in use. It made a nice coffee table in the end.

Table 1.10: Minimum and Recommended RAM for Exchange Server 2007 Roles

Server role	Minimum	Recommendation	Maximum
Mailbox	2GB	2GB base memory plus per-mailbox calculation	32GB
Hub Transport	1GB	1GB per CPU core	16GB
Client Access	1GB	1GB per CPU core	4GB
Unified Messaging	1GB	1GB minimum, plus 512 MB for each additional CPU core	4GB
Edge Transport	1GB	1GB per CPU core	16GB
Multiple roles	2GB	4 GB for combination Hub Transport, Client Access, and Unified Messaging, plus add the per-mailbox calculation.	8GB

Note

Based on my own experiences with Exchange Server 2007, I recommend a minimum of 4GB of RAM for any server that has the Mailbox server role installed on it. Even if the server will only support a few dozen mailboxes, it will run much better with 4GB of RAM.

After you have calculated the minimum amount of RAM that you require for the server, if you are configuring a mailbox server, you will need to add some RAM for each mailbox. The amount will depend on your user community's estimated load profile. Table 1.11 shows the additional memory required based on the number of mailboxes supported.

Table 1.11: Additional Memory Factor for Mailbox Servers

User profile	Mailbox Memory Recommendation
Light	Add 2 MB per mailbox
Average	Add 3.5 MB per mailbox
Heavy	Add 5 MB per mailbox

So, for example, a server handling a Mailbox server role should have 2GB of memory plus the additional RAM shown in Table 1.11 (for heavy users). For a mailbox server that is supporting 1,000 mailboxes, where 500 of the users are average (3.5 MB × 500 for 1.75GB of RAM) and 500 are heavy users (5 MB × 500 for 2.5GB of RAM), the server should have about 6.3GB of RAM. For good measure, I recommend going with 8GB of RAM so you have additional RAM in case you need it. Seasoned administrators of previous versions of Exchange will immediately notice that restrictions on usable physical memory no longer apply to Exchange 2007.

Remember that these RAM estimates are just that, estimates. Additional factors may require more or less RAM (usually more) than the calculations and recommendations here. For example, antivirus and antispam software on Mailbox servers can place a significant burden on RAM. The `store.exe` (information store) process will always allocate a significant amount of RAM. In the following screen shot of the Windows Task Manager, notice that the `store.exe` is using 1.4GB of physical memory. This server is running Exchange Server 2007 on a Windows 2003 SP2 server with 2.5GB of RAM and supports 15 mailboxes. You should expect this kind of memory growth from the `store.exe`.

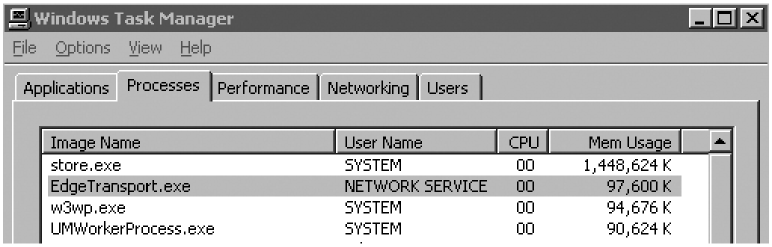


Image Name	User Name	CPU	Mem Usage
store.exe	SYSTEM	00	1,448,624 K
EdgeTransport.exe	NETWORK SERVICE	00	97,600 K
w3wp.exe	SYSTEM	00	94,676 K
UMWorkerProcess.exe	SYSTEM	00	90,624 K

An alternate way to size memory for Mailbox servers is to estimate the amount of RAM required based on the number of storage groups. This method is calculated to ensure that each storage group (and mailbox database) that is in use is allocated sufficient memory for database caching. Table 1.12 shows the minimum memory recommendations based on storage groups.

If you calculate two different minimum recommendations for RAM, you should use the larger of the two calculations. Up to 32GB, Exchange 2007 Mailbox servers will always benefit from additional performance. Of course, 32GB of RAM may not be required on a Mailbox server that is supporting only 200 mailboxes, so approach RAM sizing with a certain cautious exuberance.

Optical Media

Exchange Server 2007 ships only on DVD media. Although installing from a network share does work, it is generally a good idea to ensure that your servers have DVD drives available rather than CD-ROM drives. If your servers do not have DVD drives, you can still copy the Exchange software across the network or install from a network share folder.

File System

All disks must be formatted using the NTFS file system.

Table 1.12: Minimum RAM Recommendations Based on Storage Groups

Number of Storage Groups	Minimum RAM Required
1–4	2GB
5–8	4GB
9–12	6GB
13–16	8GB
17–20	10GB
21–24	12GB
25–28	14GB
29–32	16GB
33–36	18GB
37–40	20GB
41–44	22GB
45–38	24GB
49–50	26GB

Disk Space

Exchange Server 2007 is certainly not the first edition of Exchange for which administrators or designers have improperly sized the amount of available disk space. More than a few times, I have seen administrators scrambling for more disk space, adding additional hard drives, moving databases and transaction logs around, or begging the storage area network (SAN) administrator for more disk space.

I recommend that the operating system disk and the disk on which you will install the Exchange binaries have at least 10GB of free disk space prior to the installation of Exchange 2007. The actual recommendation from Microsoft is 1.2GB disk space free and 200 MB of free space on the system disk, but that is a bare minimum. If the Exchange server is supporting the Unified Messaging server role, plan for an additional 500 MB of disk space for each Unified Messaging language pack that will be installed.

Disk Space for Exchange Data

The amount of disk space that each of the servers will actually require will depend on the server role, the number of users you support, mailbox limits, and how much room you want for growth. I will present a more thorough discussion of disk space requirements and database sizing in Chapter 12, ''Sizing Storage Groups and Databases.''

Page File Size

You may place your page file on the operating system disk or you may place it on a dedicated volume or spindle. The actual size of the page file has been widely debated over the years and the debate continues. After all, if you have just configured a server with 16GB of RAM, you would hope that it will not page all that much! The recommendation from Microsoft for a large page remains the same, though.

You should set the initial size of your page file to RAM plus 100 MB. Yes, I know, ''Ouch!'' That means on a server with 16GB of RAM, your page file will be just over 16GB. I had wondered myself if this would change with 64-bit Windows and Exchange 2007, but I continue to see this guidance from Microsoft.

One important thing to note about the page file is that I like to ensure that I can accommodate the entire page file on the operating system disk even if I move it to a different disk. If you ever get the blue screen of death, the page file can be dumped to a file on the hard disk, but in order for Windows to do this, the page file on the operating system disk must be large enough to accommodate the contents of the RAM. I have rarely needed a crash dump of the entire memory, but it is a nice option to have if you need it.

Operating System Requirements

There are a few requirements for the Windows Server operating system. For the release to manufacturing (RTM) version of Exchange 2007, the only version of Windows Server that can be used is the Windows Server 2003 x64 SP1 (or later) or Windows Server 2003 x64 R2 family. Windows 2003 with the Multilingual User Interface (MUI) Pack can also be used. Exchange 2007 can be installed on either the Standard Edition or Enterprise Edition of Windows Server 2003. Windows 2003 Enterprise Edition is required if you will be installing clustered mailbox servers.

Exchange Server 2007 Service Pack 1 requires either Windows 2003 Service Pack 2 or Windows Server 2008.

The following list includes other requirements for preparing the Windows Server to run Exchange 2007:

- Install the Microsoft .NET Framework v2.0.
- Install the Windows PowerShell. The released version can be downloaded from `www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx`.
- Install Microsoft Management Console 3.0. You can find more information and download links in Microsoft Knowledge Base article 907265, ''MMC 3.0 update is available for Windows Server 2003 and for Windows XP.''

Note

Unlike with previous versions of Exchange, the Internet Information Server components Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) should not be installed.

All additional applications that you run on an Exchange 2007 server should be 64-bit applications. Although Windows x64 supports 32-bit applications in WOW64 emulation provided the application's kernel mode components are 64-bit, it remains to be seen whether mixing and matching 32-bit and 64-bit applications on an Exchange 2007 server is a good idea. Many of us still remember poorly performing and unstable 16-bit Windows applications that adversely affected Windows NT 4.0, so this may potentially be true with 32-bit Windows applications on Windows 64-bit.

32-bit applications running on 64-bit Windows are supported in WOW64. The only requirement is that kernel mode components of those applications have to work, so those have to be x64. The main application can be 32-bit running in WOW64. In my opinion, any third-party tools and utilities that run on an Exchange 2007 server should be 64-bit versions.

Conclusion

In this chapter, I reviewed some of the features that I feel are significant in Exchange Server 2007 as well as improvements found in Exchange Server 2007 Service Pack 1. Most organizations will find at least a few compelling features in Exchange Server 2007 that will make the upgrade worthwhile.

In the next chapter, I will cover the new Exchange management interface for Exchange Server 2007 and then later (in Chapter 7) provide you with a primer on the Exchange Management Shell.