



***Microsoft***<sup>®</sup>  
**Exchange 2000 Operations Guide**

Version 1.0



ISBN: 1-4005-2762-7

*Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2001 Microsoft Corporation. All rights reserved.*

*Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Outlook, and Visual Basic are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Contents

## Chapter 1

<b>Introduction</b>	<b>1</b>
Microsoft Operations Framework (MOF) . . . . .	1
How to Use This Guide . . . . .	3
Efficiency, Continuity, and Security . . . . .	3
Chapter Outlines . . . . .	5
Planning and Deployment . . . . .	6
Service Level Agreements . . . . .	7
Features . . . . .	7
Performance . . . . .	8
Recovery . . . . .	8
Support . . . . .	8
Summary . . . . .	9
Related Topics . . . . .	9

## Chapter 2

<b>Capacity and Availability Management</b>	<b>11</b>
Introduction . . . . .	11
Chapter Sections . . . . .	12
Capacity Management . . . . .	12
Availability Management . . . . .	15
Service Hours . . . . .	15
Service Availability . . . . .	16
Minimizing System Failures . . . . .	16
Minimizing System Recovery Time . . . . .	19
Performance Tuning . . . . .	19
Making Changes to the Registry . . . . .	20
No Performance Optimizer . . . . .	20
Optimizable Features . . . . .	21
Tuning Considerations . . . . .	21
Upgrading from Exchange 5.5 to Exchange 2000 . . . . .	22
Tuning the Message Transfer Agent (MTA) . . . . .	22
Tuning SMTP Transport . . . . .	22
Store and ESE Tuning . . . . .	26

Tuning Active Directory Integration . . . . .	30
Tuning Outlook Web Access (OWA) . . . . .	33
Hardware Upgrades . . . . .	34
Summary . . . . .	35

### Chapter 3

## **Change and Configuration Management 37**

Introduction . . . . .	37
Prerequisites . . . . .	38
Chapter Sections . . . . .	38
Change Management . . . . .	38
Defining Change Type . . . . .	38
Security . . . . .	43
Software Control and Distribution . . . . .	43
Documentation . . . . .	43
Configuration Management . . . . .	44
Tools for Configuration Management . . . . .	45
Configuration Management and Change Management . . . . .	45
Configuration Items . . . . .	45
Maintaining the Configuration Management Database . . . . .	49
Exchange System Policies . . . . .	51
Summary . . . . .	52

### Chapter 4

## **Enterprise Monitoring 53**

Introduction . . . . .	53
Prerequisites . . . . .	53
Chapter Sections . . . . .	53
Performance Monitoring . . . . .	54
System Monitor . . . . .	54
Exchange 2000 Objects and Counters to Monitor . . . . .	55
Windows 2000 Objects and Counters to Monitor . . . . .	59
Centralized Monitoring . . . . .	61
Event Monitoring . . . . .	62
Event Viewer . . . . .	63
Log Files . . . . .	64
Centralized Event Monitoring . . . . .	64
Availability Monitoring . . . . .	65
Monitoring and Status Tool . . . . .	65
Centralized Availability Monitoring . . . . .	67
Client Monitoring . . . . .	68
Summary . . . . .	69

**Chapter 5**

<b>Protection</b>	<b>71</b>
Introduction . . . . .	71
Chapter Start Point . . . . .	71
Chapter End Point . . . . .	71
Chapter Sections . . . . .	71
Protection Against Hacking . . . . .	72
Firewall Operations . . . . .	73
Anti-Virus Measures . . . . .	75
Staying Current . . . . .	76
Dealing With Virus Infection . . . . .	77
Blocking Attachments at the Client . . . . .	77
Disaster Recovery Procedures . . . . .	79
Backing Up . . . . .	80
Restoring . . . . .	82
Recovery Testing . . . . .	86
Summary . . . . .	87

**Chapter 6**

<b>Support</b>	<b>89</b>
Introduction . . . . .	89
Chapter Sections . . . . .	89
Providing Support for End Users . . . . .	90
Reducing End User Support Costs . . . . .	90
Exchange Problem Management . . . . .	94
Summary . . . . .	96
<b>Glossary</b>	<b>97</b>



## Content Lead

Andrew Mason – Microsoft Prescriptive Architecture Group

## Key Authors

Paul Slater – ContentMaster  
Kent Sarff – Microsoft Consulting Services  
Sasha Frljanic – Microsoft Consulting Services

## Reviewers

Jon LeCroy – Microsoft ITG  
Thomas Applegate – Microsoft ITG  
Erik Ashby – Microsoft Exchange 2000 Product Group  
Chase Carpenter – Microsoft Consulting Services







# 1

## Introduction

### Introduction

Welcome to the Microsoft® Exchange 2000 Server Operations Guide. This guide is designed to give you the best information available on managing operations within an Exchange 2000 environment.

To manage Exchange in a day-to-day environment, an operations team needs to perform a wide variety of procedures, including server monitoring, backup, verification of scheduled events, protection against attack, and user support. This guide includes instructions for the procedures along with steps for dealing with unresolved issues in a timely manner.

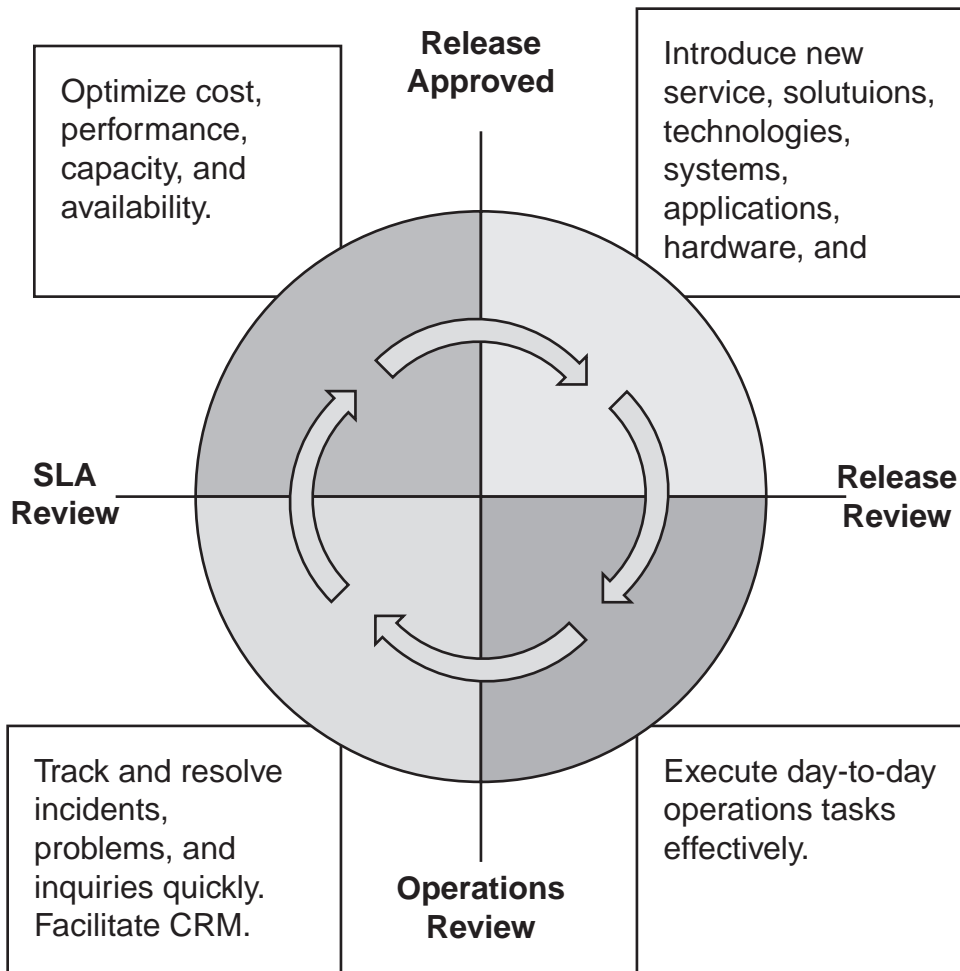
### Microsoft Operations Framework (MOF)

For operations to be as efficient as possible in your environment, you must manage them effectively. To assist you, Microsoft has developed the Microsoft Operations Framework (MOF). This is essentially a collection of best practices, principles, and models providing you with technical guidance. Following MOF guidelines should help you to achieve mission-critical production system reliability, availability, supportability, and manageability on Microsoft products.

The MOF process model is split into four integrated quadrants. These are as follows:

- ◆ Changing
- ◆ Operating
- ◆ Supporting
- ◆ Optimizing

Together, the phases form a spiral life cycle (see Figure 1.1) that can apply to the operations of anything from a specific application to an entire operations environment with



**Figure 1.1**  
*MOF Process Model*

multiple data centers. In this case, you will be using MOF in the context of Exchange 2000 operations.

The process model is supported by 20 service management functions (SMFs) and an integrated team model and risk model. Each quadrant is supported with a corresponding operations management review (also known as review milestone), during which the effectiveness of that quadrant's SMFs are assessed.

It is not essential to be a MOF expert to understand and use this guide, but a good understanding of MOF principles will assist you in managing and maintaining a reliable, available, and stable operations environment.

If you wish to learn more about MOF and how it can assist you to achieve maximum reliability, availability, and stability in your enterprise, visit [www.microsoft.com/mof](http://www.microsoft.com/mof) for more detailed information. For prescriptive MOF information on all 20 service management functions, complementing the Exchange-specific information found in this guide, examine the detailed operations guides at:

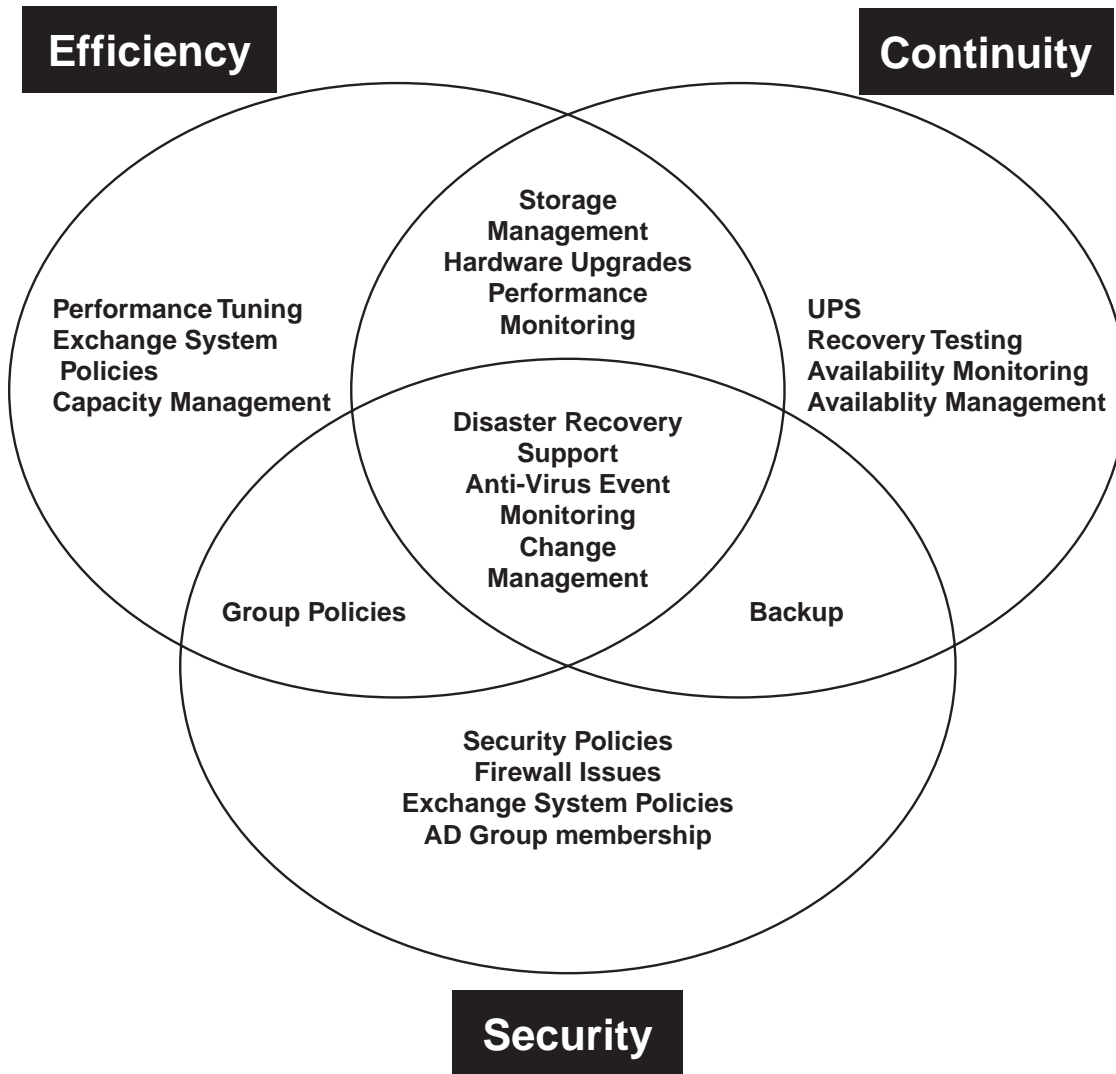
<http://www.microsoft.com/technet/win2000/win2ksrv/default.asp>

## How to Use This Guide

While this guide is designed to be read from start to finish, you may wish to “dip in” to the guide to assist you in particular problem areas. To assist you in doing so, the guide contains a number of symbols that you will not find elsewhere. It is very important that you read the following section if you are going to get the most out of your piecemeal approach.

## Efficiency, Continuity, and Security

Not every Exchange Operations manager thinks in terms of the MOF. Another way of considering operations is in terms of the categories in which they fit. The wide variety of tasks that constitute Exchange 2000 operations can be divided into three broadly overlapping groups. Figure 1.2 on the next page shows these groups and how the operations fit within them.



**Figure 1.2**  
*Exchange 2000 Operations divided into groups*

This guide covers all three areas described above. Although the chapters are structured according to Microsoft operations principles, you will find information about all of these areas in the guide.

## Chapter Outlines

This guide consists of the following chapters, each of which takes you through a part of the operations process. Each chapter is designed to be read in whole or in part, according to your needs.

### **Chapter 2 – Capacity and Availability Management**

To continue to function as it should, Exchange must be managed over time as the load on the system increases. The chapter looks at the different tasks that you may need to perform as the Exchange environment is used more.

This chapter deals with these topics:

- ◆ Capacity management
- ◆ Availability management
- ◆ Performance tuning
- ◆ Hardware upgrades

### **Chapter 3 – Change and Configuration Management**

This chapter presents many of the processes used to manage an Exchange 2000 environment. These processes will help you to evaluate, control, and document change and configuration within your organization.

This chapter deals with the following:

- ◆ Change management
- ◆ Configuration management (including use of Exchange system policies)

### **Chapter 4 – Enterprise Monitoring**

To track any problems and to ensure that your Exchange 2000 Server is running efficiently, you need to monitor it effectively. Monitoring is not something that should occur only when there are problems, but should be a continuous part of your maintenance program. The chapter shows how you can monitor your Exchange 2000 to deal with any problems as (or preferably before) they arise.

This chapter deals with these topics:

- ◆ Creating an enterprise monitoring framework
- ◆ Performance monitoring
- ◆ Event monitoring

- ◆ Availability monitoring
- ◆ Proactive monitoring
- ◆ Availability prediction

### **Chapter 5 – Protection**

To protect your Exchange environment from failure, you need good protection from intrusion and attack, along with a documented and tested disaster-recovery procedure to cope with system failure. The chapter shows how to ensure that your server running Exchange is protected against these eventualities.

This chapter deals with the following:

- ◆ Firewall issues
- ◆ Anti-virus protection
- ◆ Disaster-recovery procedures
- ◆ Recovery testing
- ◆ Backup
- ◆ Restore

### **Chapter 6 – Support**

An effective support environment allows you to deal more efficiently with unforeseen issues, increasing the reliability of your Exchange environment. This chapter shows how to manage your support in an Exchange 2000 environment.

This chapter deals with these topics:

- ◆ Helpdesk support
- ◆ Problem management

## **Planning and Deployment**

To make the most out of your Exchange 2000 environment, you should make sure that your operations are carefully planned and structured. The best way of ensuring that your operations are efficient is to have operations intrinsically involved in the planning and deployment phases of Exchange 2000, providing valuable input into those processes.

Many times deployment teams do not involve the operations team in the project until it is near completion. If you are going to perform successful operations from the outset, you should make sure that you plan effectively for the operations team to take over the infrastructure and processes. Making sure that at least one member of operations attends all planning and deployment meetings will help to ensure that your design and implementation takes operations needs into account.

Operations procedures need to be defined during the planning and deployment process. Service level agreements, disaster-recovery documents, and monitoring procedures all need

to be created at this stage, because waiting until the system is live could be too late. The operations team should be using the planning phase (and in some cases the deployment phase) to test procedures that are defined, such as those for disaster recovery.

Planning and deployment are covered in more detail as part of the Exchange 2000 Upgrade Series. You will find this at the following Web site:

<http://www.microsoft.com/technet/exchange/guide/default.asp>

## Service Level Agreements

Your goal for successful operations is to produce a high quality of service at a reasonable cost. The definition of a high quality of service will vary according to the needs of your organization. The level of service you offer will generally be a compromise between quality-of-service requirements and the costs necessary to provide it.

Central to the idea of successful operations is the service level agreement (SLA) process. Success or failure of an operations environment is measured against the requirements of the SLA. It is therefore very important that you define the SLA realistically according to the resources you can devote to your operations environment.

---

**Note:** When it is internal to IT, an SLA is often referred to as an operating level agreement (OLA). For the sake of clarity, this guide refers to SLAs only. However, the recommendations in the guide apply to OLAs as well as SLAs.

---

Your SLAs should be a commitment to providing service in four different areas:

- ◆ Features
- ◆ Performance
- ◆ Recovery
- ◆ Support

### Features

Here you state which Exchange services you will be offering to the client base. These would include some or all of the following:

- ◆ E-mail (via some or all of MAPI, POP3, IMAP4, and OWA)
- ◆ Defined mailbox size for different categories of user
- ◆ Public folder access
- ◆ Ability to schedule meetings
- ◆ Instant messaging
- ◆ Chat
- ◆ Video conferencing

## Performance

Here you show the performance you would expect from each of the previously mentioned features. This would include some or all of the following:

- ◆ Service availability (this may be given across all services or on a service-by-service basis)
- ◆ Service hours
- ◆ Mail delivery times (note that you are not able to guarantee mail delivery times, either to the Internet or within your organization, if you use the Internet as part of your intra-organization mail topology)
- ◆ Mailbox replication times (dependent on Active Directory™ service)

## Recovery

Here is where you will specify what you expect in terms of disaster recovery. Although you naturally hope that disaster never strikes, it is important to assume that it will and have recovery times that will meet in a number of disaster-recovery scenarios. These include the following:

- ◆ Recovery from failed Exchange Store
- ◆ Recovery from total server failure

## Support

Here you specify how you will offer support to the user community, and also how you would deal with problems with your Exchange Server environment. You would include commitments on the following:

- ◆ Helpdesk response time
- ◆ When and how problems will be escalated

Of course it is one thing to determine what your SLAs should measure, and quite another to come up with the right figures for them. You should always define them realistically according to the needs of the business. Realistically is the key word here. For example, while your business might *want* Exchange to have guaranteed uptime of 100 percent, it is unrealistic to require this in an SLA because a single incident anywhere within your organization will cause you to fail to meet the SLA.

Your operations environment should be built around meeting the requirements of your SLAs.



## Summary

This chapter has introduced you to this guide and summarized the other chapters in it. It has also provided brief descriptions of both service level agreements and planning and deployment. Now that you understand the organization of the guide, you can decide whether to read it from beginning to end, or whether you want to read selected portions. Remember that effective, successful operations require effort in all areas, not just improvements in one area, so that if you decide to read the Supporting chapter first, you should go back and read the other chapters as well.

## Related Topics

The Microsoft Operations Framework provides technical guidance and industry best practices that encompasses the complete IT Service Management environment, including capacity management, availability management, configuration management, service monitoring and control, service level management, and their inter-relationships. For more information on the Microsoft Operations Framework, go to:

<http://www.microsoft.com/mof>

For prescriptive MOF information on capacity management, availability management, configuration management, service monitoring and control, and service level management, please review the detailed operations guides that can be found at:

<http://www.microsoft.com/technet/win2000/win2ksrv>





# 2

## Capacity and Availability Management

### Introduction

In the vast majority of cases, the load on your Exchange 2000 Server computers will increase over time. Companies increase in size, and as they do, the number of Exchange users increases. Existing users tend to use the messaging environment more over time, not only for traditional e-mail, but also for other collaborative purposes (for example, voicemail, fax, instant messaging, video conferencing). The load on the messaging environment will also vary over the course of the day (for example, there may be a morning peak) and could vary seasonally in response to increased business activity.

The aim of your operations team should be to minimize the effect of the increased load on your users, at all times keeping within the requirements set by your service level agreement (SLA). You will need to ensure that existing servers running Exchange are able to cope with the load placed upon them (and upgrade hardware if appropriate).

Another important requirement of the operations team is to minimize system downtime at all times. The level of downtime your organization is prepared to tolerate needs to be clearly set out in the SLA, separated into scheduled and unscheduled downtime. Many organizations can cope perfectly well with scheduled downtime, but unscheduled downtime almost always needs to be kept to a minimum.

Exchange 2000 is predominantly self-tuning, but there are areas where tuning your servers running Exchange will result in an improvement in performance. It is important to identify these areas and tune where appropriate.

Inevitably there will come a point where the load on your servers running Exchange is such that hardware upgrades are required. If you manage this process effectively, you can significantly reduce the costs associated with upgrading.

## Chapter Sections

This chapter covers the following procedures:

- ◆ Capacity management
- ◆ Availability management
- ◆ Performance tuning
- ◆ Hardware upgrades

After reading this chapter, you will be familiar with the requirements for capacity and availability management in an Exchange 2000 environment and the steps necessary to ensure that the requirements of your SLA are met.

## Capacity Management

Capacity management is the planning, sizing, and controlling of service capacity to ensure that the minimum performance levels specified in your SLA are exceeded. Good capacity management will ensure that you can provide IT services at a reasonable cost and still meet the levels of performance you have agreed with the client.

This section will help you meet your capacity management targets for an Exchange 2000 environment.

Of course, whether an individual server reaches its SLA targets will depend greatly upon the functions of that server. In Exchange 2000, servers can have a number of different functions, so you will need to ensure that you categorize servers according to the functions they perform and treat each category of server as an individual case. In particular, do not consider servers purely in terms of the number of mailboxes they hold.

When you are looking at the capacity of a server running Exchange, consider the following:

- ◆ How many mailboxes are on the server?
- ◆ What is the profile of the users? (Light, medium, or heavy use of e-mail; do they use other services, such as video-conferencing?)
- ◆ How much space do users require for mailboxes?
- ◆ How many public folders are on the server?
- ◆ How many connectors on the server are on the server?
- ◆ How many distribution lists are configured to be expanded by the server?
- ◆ Is the server a front-end server?
- ◆ Is the server a domain controller/Global Catalog server? (generally not recommended)

Generally, the more functions a server has, the fewer users that server will be able to support on the same hardware. To gain the maximum capacity from your servers, consider having servers dedicated to a specialized function. In many cases your planning will have

resulted in specialized hardware for specialized functions, for example, in the case of front-end servers.

To ensure that you manage capacity appropriately for your Exchange 2000 server, you need a great deal of information about current and projected usage of your server running Exchange. Much of this information will come from monitoring. You will need information about patterns of usage and peak load characteristics. This information will need to be collected on a server-by-server basis, because a problem with a single server in an Exchange 2000 environment can result in a loss of performance for thousands of users. The performance of your network is also critical in ensuring delivery times and timely updating of Exchange directory information.

The main areas you should monitor to ensure that your servers running Exchange exceed your SLAs' capacity requirements include the following:

- ◆ CPU utilization
- ◆ Memory utilization
- ◆ Hard-disk space used
- ◆ Paging levels
- ◆ Network utilization
- ◆ Delivery time within and between routing groups
- ◆ Delivery time to and from foreign e-mail systems within your organization
- ◆ Delivery time to and from the Internet (although this depends greatly on minute-by-minute performance of your connection to the Internet and the availability of bandwidth to other messaging environments)
- ◆ Time for directory updates to complete

You will find more information on monitoring in Chapter 4.

It is fairly common to choose the size the disks of a server running Exchange based on how many mailboxes you plan to have on the server multiplied by the maximum allowable size of each mailbox. Using this approach, however, will generally not help you to meet your SLAs. You should strongly consider approaching this problem from a different perspective. When determining the capacity of your server running Exchange, consider basing it on the time it takes to recover a server from your backup media. Recovery time is generally very important in organizations because downtime can be extremely costly. If you are using a single store on your server running Exchange, use the following procedure to help you size it.

1. Divide the recovery time of a database (defined in your SLA) by half. Around half the recovery time will generally be spent on data recovery, the rest on running diagnostic tools on the recovered files, database startup (which includes replaying all later message logs) and making configuration changes. Of course, this is only a general figure—the longer you leave for recovery time, the smaller the proportion of that time is required for configuration changes.
2. Determine in a test environment how much data can be restored in this time.

3. Divide this figure by the maximum mailbox size you have determined for the server (again listed in your SLA). This will give you the number of mailboxes you can put on the database.

As an example, assume that your SLA defines a recovery time of four hours for a database. In testing, your recovery solution can restore 2 gigabytes (GB) of Exchange data per hour and your maximum mailbox size is 75Mb.

Using the preceding procedure, the following calculations can be done.

1. The recovery time divided by 2 is 2 hours.
2. 4 GB of Exchange data can be restored in this time.
3. 4 GB divided by 75 MB is 54 Mailboxes.

In this example, if you wanted to provide more mailboxes per server, you would either have to a) alter your SLA to increase recovery time or b) find a faster restore solution.

Each server running Exchange can support up to 20 stores, spread across 4 storage groups (in Enterprise edition). If your server running Exchange is configured with multiple stores, recovery times can be more difficult to calculate. Stores in the same storage group are always recovered in series, whereas ones in separate storage groups can be recovered in parallel. You may also have created multiple stores to allow you to offer different SLAs to different categories of user (for example, you might isolate managers on one store so that you can offer them faster recovery times than the rest of the organization.) If you do have multiple stores, you will need to consider the SLA on each store and the order in which stores will be recovered to accurately determine recovery time.

As a result of the first two steps in the preceding calculations, you will have a figure for the maximum amount of data located in your information stores. Generally, you should at least double this to determine the appropriate disk capacity for the disks containing your stores. This will allow you to perform offline maintenance much more quickly as files can be quickly copied to a location on the same logical disk.

By using a key SLA to define your capacity, you are creating an environment in which you are far more likely to meet the targets you set.

Sizing servers to meet SLAs is crucial, but servers must also meet user performance expectations. Using Microsoft and third-party tools, ensure that your predicted user usage will be accommodated on the servers.

If you have sized your database according to the techniques mentioned here, you should be able to ensure that your database is kept to a manageable size. However, keeping an eye on the size of your Exchange 2000 databases is still important. In a large enterprise, it is typical for users to be moved from one server to another quite often, and for users to be deleted. This can result in significant fragmentation of databases, which results in large database sizes, even if you do keep the number of mailboxes below the levels you have determined.

To deal with this problem, you should continually monitor available disk space on your servers running Exchange. If the RAID array containing the stores gets close to half full, an alert should be sent indicating the problem, and that the Exchange Database might need to be defragmented offline. To do this, perform an alternate server restore (see Chapter 5 for details) and then defragment the database on this alternate server. If this is successful and results in a significant reduction in database size, you can perform the defragmentation at the next scheduled maintenance time.

Performing the alternate server restore also has the advantage of ensuring that your backup and restore procedures are working effectively. You should check this regularly in any case. This is also covered in more detail in Chapter 5.

Probably the most important thing to remember when performing capacity planning is to size conservatively. Doing so will minimize availability problems, and the cost reduction will generally more than compensate for any excess capacity costs.

As well as looking at technical issues, you will need to examine staffing levels when you are capacity planning. As your Exchange 2000 environment grows, you might need more people to support the increased load. In particular, if there are more users requiring increased services, there is likely to be a greater need for help desk support.

## Availability Management

Availability management is the process of ensuring that any given IT service consistently and cost-effectively delivers the level of availability required by the customer. It is not just concerned with minimizing loss of service, but also with ensuring that appropriate action is taken if service is lost.

One of the main aims of Exchange 2000 operations is to ensure that Exchange is available as much as possible and that both planned and unplanned interruptions to service are minimized. Availability in an organization is typically defined by your SLAs in two ways—service hours and service availability.

### Service Hours

These are the hours when the Exchange services should be available. Typically, for a large organization this will be all but a very few hours a month. Defining your service hours allows you to create defined windows when offline maintenance of your servers running Exchange can be performed without breaching the terms of your SLA.

You might choose to define in the SLA the exact times when Exchange services might be unavailable. For example, you might state that Exchange services might be unavailable for four hours every first Saturday of the month. However, in large organizations it is often more practical to commit to, for example, no more than four hours of scheduled downtime per month, with a week's notice of any scheduled change. This allows changes to be made much more easily across the organization, at times when the right staff can be devoted to the tasks.

Of course, just because you have allowed for a certain amount of downtime per server per month, this does not mean that you have to use it, and in most cases you will not. On the other hand, just because you haven't performed offline maintenance one month does not mean that the hours can be carried over to the following month. Your user community will be very unhappy if you take a system down for 2 days, even if it has been up solidly for 2 years!

You might wish to define different service hours for the different services available in Exchange (mail, public folders, etc). This would depend on the amount of offline maintenance that is typically required for each service. For example, you might determine that your SMTP bridgehead servers and firewall servers never require offline maintenance and so might set the level of service hours for mail delivery significantly higher than for mailbox access. If you are prepared to spend the appropriate money on resources, it is very possible to achieve extremely low levels of scheduled downtime, and this can be reflected in your SLA.

## Service Availability

Service availability is a measure of how available your Exchange services are during the service hours you have defined. In other words, it defines the levels of unscheduled downtime you can tolerate within your organization. Typically levels of availability in an SLA of an enterprise are between 99.9 and 99.999 percent. This corresponds to a downtime of as much as 525 and as few as 5 minutes per service per year.

Of course, ANY unscheduled downtime is inconvenient at best, and very costly at worst, so you need to do your best to minimize it.

To ensure high levels of availability, you need to consider two key questions:

- ◆ How often, on average, is there downtime for a service?
- ◆ How long does it take to recover the service if there is downtime?

Once you have considered these questions, you can set about minimizing the number of times a service fails and the time taken to recover that service.

Availability management is intrinsically linked with capacity management. If capacity is not managed properly, then overloaded servers running Exchange might fail, causing availability problems. A classic example of this would be running out of disk space on a server running Exchange, which would result in the databases shutting down and in users losing a number of services.

## Minimizing System Failures

To minimize the frequency of failure in Exchange 2000, you need do the following:

- ◆ Decrease single points of failure
- ◆ Increase the reliability of Exchange 2000 itself.



## Decreasing Single Points of Failure

You can maintain availability in Exchange 2000, even in the event of a failure, provided you ensure that it is not a single point of failure. In some areas, such as database corruption, it is not possible to eliminate single points of failure, but in many cases you can guard against individual failures and still maintain reliability. An obvious example is the directory. By having multiple domain controllers and Global Catalog servers available in any part of your network, you maintain availability of Exchange even in the event of failure of a particular domain controller or Global Catalog server. Having local domain controllers or Global Catalog servers keeps Exchange available in the event of a non-local network failure.

Using front-end servers is another way to avoid single points of failure. The failure of a single front-end server will have no effect on the availability of Exchange to non-MAPI clients. The clients will simply be rerouted to another front-end server, with no loss of service.

Exchange 2000 routing can be modified to minimize single points of failure. In particular, you can modify Routing Group connectors to ensure that there are multiple bridgeheads available, and thus maintain delivery from one part of the organization to another. You can also set up Routing Group meshes, which consist of a series of fully interconnected Routing Groups with multiple possible routes between them.

Multiple messaging routes between servers are useless if they all rely on the same network connections and the network goes down. You should therefore ensure that there are multiple network paths (using differing technologies) that Exchange and Windows 2000 can use.

One of the most significant single points of failure is a mailbox server. This can affect very large numbers of users, depending on the server. Mailbox servers can be clustered to ensure their continued high availability. If you are running Exchange 2000 on Windows 2000 Advanced Server, you can cluster over two nodes and you have two possible ways to cluster the servers—active/passive and active/active. Active/passive clustering is the current recommended clustering implementation for Exchange. If you choose to implement active/active clustering, you should realize that it requires careful planning to ensure that Exchange can fail over correctly to the other node. With Service Pack 1 of Exchange 2000 and Windows 2000 Datacenter server, you can have four nodes in your cluster. In this implementation consider active/active/active/passive clustering.

In a standard clustered environment, however, the disk array is still the single point of failure, so you should think seriously about using a storage area network (SAN) to maximize the availability of all your servers running Exchange.

If you are creating truly redundant Exchange 2000 servers, you shouldn't stop at the disk subsystem. Your servers should be equipped with redundant RAID controllers, network interface cards (NICs), and power supplies. In fact, you should aim to have redundancy everywhere.

Single points of failure can also be created by improper maintenance of systems. For example, if you are using a RAID 5 array on a server running Exchange with a hot spare,

the disk subsystem becomes a single point of failure once that hot spare is invoked. If you have robust systems in place, you must ensure that any failures are resolved promptly. Make sure that you have notification and monitoring procedures in place and a system for resolving problems.

Remember that Exchange relies on Active Directory and Global Catalog servers to function. If no domain controllers are available to a server running Exchange, stores will dismount. If Global Catalog servers are unavailable, Exchange clients will not function (as they require a Global Catalog server to access the Global Address List). You should minimize single points of failure on these servers as much as possible, or at least ensure that you have redundant servers in every location.

Finally, do not forget non-computing issues. You can have the most robust e-mail system in the world and then find that it falls apart due to a fire in a building, a power failure, or theft of server hardware or data. You should take precautions against all these possibilities. This would include ensuring that you have taken the following into account:

- ◆ Good physical security
- ◆ Protection from fire
- ◆ Protection from flooding
- ◆ Concealed power switches
- ◆ Air conditioning
- ◆ UPS systems
- ◆ Alternate power generation

You will need to make sure that all of these services are in place and that you have defined a drill to deal with their failure. For example, you should ensure that there are personnel on call for all emergency systems.

You might also wish to house your servers running Exchange in separate locations from one another to help reduce the impact of such events.

Good availability management is intrinsically linked with good change and configuration management. If you manage change and configuration well, you are well positioned to have good availability of your servers running Exchange. You will learn more about change and configuration management with Exchange 2000 in Chapter 3.

### **Increasing the Reliability of Exchange 2000**

While Exchange 2000 is a very robust messaging system, like any product, there are configurations that in particular cases could result in a loss of reliability. In an Enterprise environment, it is important to guard against these difficulties by continually monitoring Exchange. For more detail on monitoring, see Chapter 4.

One area where you can guard against problems is database errors. Database errors can be caused by a number of factors, but they are typically hardware related. You will be able to minimize these by doing the following:

- ◆ Ensure that your hardware is on the Hardware Compatibility List
- ◆ Checking Event Viewer for database-related errors
- ◆ Periodically running the Information Store Integrity Checker (isinteg.exe) on the database to check for errors

Part of your maintenance program should also include routinely searching the Microsoft Web site ([www.microsoft.com/exchange](http://www.microsoft.com/exchange)) for any issues that need to be resolved by patches and/or service packs. The patches and service packs will be tested and recorded as part of your change-management program, which is covered in more detail in Chapter 3.

### Minimizing System Recovery Time

To recover from failure in an Exchange 2000 environment as quickly as possible, you need to be thoroughly prepared. You will need the following:

- ◆ Available hardware
- ◆ Complete configuration information
- ◆ A recent, working backup
- ◆ An effective disaster-recovery procedure
- ◆ Fast access to support resources
- ◆ Staff availability to perform the restore

System recovery is covered in more detail in Chapter 5.

## Performance Tuning

When you tune for performance, you are aiming to reduce your system's transaction response time. Performance tuning can take a number of forms, including the following:

- ◆ Balancing workloads between servers
- ◆ Balancing disk traffic on individual servers
- ◆ Using memory efficiently on servers
- ◆ Upgrading hardware

The most effective factor in improving performance comes from upgrading the hardware on your servers that are running Exchange. However, regardless of the hardware, there are a number of software changes that you can make to maximize the efficiency of Exchange 2000.

While obtaining the best performance from your Exchange 2000 computers is always an important goal, it is crucial to be cautious in your tuning changes. You should track all alterations in case you make a change that inadvertently reduces performance. Making one change at a time makes it easy to identify which change needs to be reversed.

Customer variation is probably the greatest variable in tuning Exchange for optimum performance. Even customers with similar needs often choose solutions that differ significantly. Hardware varies in the number and speed of the processors, the available RAM, the number of disks, and the disk configuration chosen (RAID level).

Exchange 2000 can be configured with different numbers of storage groups and databases, and can be clustered with other servers accessing a central storage subsystem. The server load will vary based on the total number of users with mailboxes on the server, the number of users logged on at a given time, the actions they are performing, and any additional load imposed by the routing of outside messages through the server.

Whenever you are doing performance tuning, you should consider the cost of extensive analysis versus the benefits you expect to get from the tuning. Put simply, if you need to analyze an individual server extensively to gain a 5 percent performance gain, it is probably not worth it, since you could easily spend a fraction of the money on buying better hardware. Not only that, but in some cases performance tuning might become ineffective as the load on the server increases, meaning further analysis might be required after a change has been made. For this reason, this guide does not cover extensive performance analysis; instead it concentrates on the performance tuning changes that are easy to identify. This usually involves modifying settings in the registry.

## Making Changes to the Registry

Before you edit the registry, make sure that you understand how to restore it if a problem occurs. For information on how to do this, view the “Restoring the Registry” Help topic in Registry Editor (Regedit.exe) or the “Restoring a Registry Key” Help topic in Regedt32.exe.

---

**Warning:** Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

---

If you are unfamiliar with the registry and how to change it, consult an expert. Even if you are very familiar with the registry, you should always carefully document the changes that you make, and monitor your system after each change.

For information about how to edit the registry, view the “Change Keys and Values” Help topic in Registry Editor (Regedit.exe) or the “Add and Delete Information in the Registry”

and “Edit Registry Information” Help topics in Regedt32.exe. Note that you should back up the registry before you edit it. If you are running the Microsoft Windows NT® or Microsoft Windows® 2000 operating system, you should also update your emergency repair disk (ERD).

## No Performance Optimizer

The Performance Optimizer (also known as PerfWiz) is an Exchange 5.5 tool that enables you to specify how an Exchange 5.5 computer is to be configured—for example as a private store or a public store server. In addition, you can limit an Exchange 5.5 server’s memory usage and specify how many users it would be expected to handle. Based on your choices, files written by the various Exchange components (information store, message transfer agent [MTA], and so forth) can be assigned to specific fixed disks, depending upon available storage.

Exchange 2000 does not use a tool like Performance Optimizer. One reason for this is that the new release of Exchange is better capable of performing certain tasks as they are required, such as dynamically changing certain parameters, spinning up more threads, and so on. To go beyond these dynamic changes, the administrator must manually optimize disk utilization and manually modify registry keys, but fewer such registry changes are necessary.

## Optimizable Features

Features in Exchange 2000 that can be optimized include:

- ◆ Disks
- ◆ Message transfer agent (MTA)
- ◆ Simple Mail Transfer Protocol (SMTP)
- ◆ Information-store database
- ◆ Extensible storage engine (ESE) cache and log buffers
- ◆ Active Directory connector
- ◆ Active Directory integration
- ◆ Installable file system (IFS) handle cache, credentials cache, and mailbox cache, DSAccess cache and DSProxy
- ◆ Post Office Protocol v3 (POP3) and Internet Mail Access Protocol (IMAP) settings
- ◆ Outlook Web Access (OWA)

## Tuning Considerations

The efficiency and capacity of Microsoft Exchange 2000 depends on the administrator's choices of server and storage hardware, and on the installation's topology. These should be chosen based on expected types and levels of usage. Exchange can be made more efficient through changes to various registry settings on the Exchange computer.

There are three main types of tuning parameters:

- ◆ Those with fixed optimal values (or values that can be treated as such)
- ◆ Those that can be dynamically tuned by the software
- ◆ Those that must be manually tuned (using setup, the exchange system manager, the registry, and the Active Directory Services Interface Edit tool ADSIEdit)

Some parameters may need to be manually tuned for the following reasons:

- ◆ Hardware or Exchange configuration information may be needed and this information cannot or will not be obtained dynamically.
- ◆ Server load information may also be required; this cannot be obtained dynamically either.

## Upgrading from Exchange 5.5 to Exchange 2000

When Exchange 5.5 is upgraded to Exchange 2000, some registry keys altered by PerfWiz retain their PerfWiz values, some do not, and some keys no longer appear in the registry or they appear in a different location. This means that there might be significant differences between an Exchange 2000 Server that has been upgraded from Exchange 5.5 and one that is a new installation, installed on new hardware. Because there are significant performance improvements with Exchange 2000, and because optimizations do not necessarily transfer from Exchange 5.5, it is best to start from scratch in evaluating the optimization of Exchange 2000. It is useful in this process to know your Exchange 5.5 settings before upgrading to Exchange 2000. The text file `WINNT\System32\perfopt.log` provides a record of those registry keys and disk assignments changed by PerfWiz.

## Tuning the Message Transfer Agent (MTA)

As mentioned earlier, Exchange 2000 does not include a Performance Optimization wizard, mainly because the majority of Exchange 2000 components are self-tuning. However, when the MTA is installed, its tuning state reflects that of an Exchange 5.5 computer that has never been performance optimized.

In scenarios where an organization only has servers running Exchange 2000, the MTA does not perform any processing, and so does not need to be performance tuned. However, when your servers co-exist with X.400-based messaging systems and other foreign systems (such as Lotus cc:Mail, Lotus Notes, Novell GroupWise, and Microsoft Mail) the MTA might be used heavily and you should consider tuning the MTA registry parameters. You will also need to tune the MTA if there is substantial co-existence with Exchange 5.5

servers. These areas are beyond the scope of the Exchange 2000 Operations Guide. If you need to tune your Exchange 2000 MTA, consult the deployment section of the Exchange 2000 Server Upgrade Series, available on the following Web site:

<http://www.microsoft.com/technet/exchange/guide/default.asp>

## Tuning SMTP Transport

When messages arrive into Exchange 2000 through the SMTP protocol, the data is written to disk in the form of an NTFS file (.EML). By default, these files are written to a directory (*drive:\Program Files\Exchsrvr\mailroot*) on the same disk partition as the Exchange 2000 binaries.

### Mailroot Directory Location

Under certain scenarios, such as configuring a bridgehead server, a positive performance effect can result if the SMTP mailroot directory is located on the fastest disk partition on the computer. If you determine that the mailroot directory is not on the most optimal disk partition, you can relocate the folder by following these steps:

---

**Note:** If you are performing this procedure on an Exchange 2000 Server active/passive cluster, perform the following steps on the node that has the Exchange 2000 group online.

---

1. From your computer, log on to the domain using an account with enterprise admin permissions.
2. Install the support tools from the \Support\Tools folder on the Windows 2000 CD-ROM onto your computer (this does not need to be installed on the computer running Exchange 2000).
3. Shut down the Microsoft Exchange System Attendant and World Wide Web publishing service on the Exchange 2000 computer that you want to change.
4. **Important:** Explore the installation drive for the data store and make a backup copy of the **Exchsrvr\mailroot** directory (the default location for this directory is \Program Files\Exchsrvr\mailroot)

---

**Note:** If you perform the following step on a clustered Exchange 2000 server, you will need to first start Cluster Administrator and set the Exchange group to offline.

---

5. Move the **VSI 1** directory (and all subfolders and content) under **Exchsrvr\mailroot** to the desired location.

---

**Note:** Do not move the actual mailroot directory itself.

---

6. Click **Start**, point to **Programs**, point to **Windows 2000 Support Tools**, point to **Tools**, and then select **ADSI Edit**.
7. Expand the **Configuration Container** Naming Context of Active Directory.



8. Navigate to the following path: Configuration Container\ CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=<organization>, CN=Administrative Groups, CN=<admin group>, CN=Servers, CN=<server>, CN=Protocols, CN=SMTP, CN=1.
9. Right-click the **CN=1** object, and then choose **Properties**.
10. Select **Both** from the **Select which properties to view** drop-down list.
11. Adjust the paths of the following attributes to the appropriate subdirectories under the VSI 1 directory:
  - msExchSmtplibBadMailDirectory
  - msExchSmtplibPickupDirectory
  - msExchSmtplibQueueDirectory
12. After editing each attribute, click **Set**.
13. Click **OK**.
14. Wait for Active Directory replication to replicate these changes to the rest of your forest (or at least the domain controller or Global Catalog servers that your Exchange 2000 computer is referencing).
15. Start the **Microsoft Exchange System Attendant** service. This will copy changed paths from the Active Directory into the metabase. In less than one minute after initialization, you should notice three 1005 application events (Source: MExchangeMU, Category: General) indicating that the paths in the metabase were updated successfully.
16. Restart the Exchange 2000 computer.

### SMTP File Handles

When the Exchange 2000 SMTP stack receives a new message, it writes the contents to a file on an NTFS partition. While the message is being processed (that is, waiting for the next hop or delivery point) a file handle is held open by the operating system. By default, SMTP is constrained to a maximum of 1,000 open file handles. This restriction is put in place to prevent out-of-memory problems in kernel memory and to ensure that the SMTP service shuts down in a relatively short period of time (upon shutdown, all buffers have to be flushed and all file handles released).

On servers with large amounts of memory (over 1 GB), you can raise the SMTP handle threshold. Each message that is open (being processed) holds a handle and uses 5 kilobytes (KB) of kernel memory and 10 KB of memory inside the INETINFO process. When you raise the threshold, more messages can be open, which enables SMTP to process a large queue at a faster rate. However, if the total number of messages in the SMTP queues is less than 1,000, this adjustment will not improve performance. Therefore, raise the value only if your server is heavily loaded and you consistently see large queues.

If you increase this value, you should decrease the maximum installable file system (IFS) handles value to avoid running out of kernel memory when there is a large queue. When



your server becomes low on kernel memory, your system becomes unresponsive. To regain control of your server, you must restart it to free up the kernel memory.

Table 2.1 shows the registry parameters you might need to alter if you are to make performance gains on servers with more than 1 GB RAM.

**Table 2.1 Registry Parameters to Alter for Large Servers**

Location	Parameter	Default Setting	When to Change	Recommended Setting
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SMTPSVC\Queuing	MsgHandle Threshold (REG_DWORD)	Not present, but defaults to 0x3e8	To gain additional performance when message queues are consistently greater than 1,000	Enough to accommodate the total number of messages in the queues at any one time. You should not raise the value to greater than 15,000 decimal
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SMTPSVC\Queuing	MsgHandle AsyncThreshold (REG_DWORD)	Not present, but defaults to 0x3e8	To gain additional performance when message queues are consistently greater than 1,000	Set to the same value as "MsgHandle Threshold"
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Inetinfo\Parameters	FileCache MaxHandles (REG_DWORD)	Not present, but defaults to 0x320	If the "MsgHandle Threshold" registry parameter value is increased from defaults	0x258 (600)

MaxMessageObjects is a registry parameter that correlates to the number of messages that can be queued up at a given time by SMTP. Each e-mail message resident in the SMTP queue uses at least 4 KB of memory; therefore, it is possible to run into a low memory situation with a very large queue. Setting MaxMessageObjects lower reduces the maximum number of messages that can reside in the queue, thus decreasing the maximum memory footprint for SMTP. After this limit is reached, each SMTP connection made to the server will return with an out-of-memory error. For example, if MaxMessageObjects is

reduced to 10,000, SMTP will refuse any inbound mail after the queue reaches 10,000 messages.

You may need to alter the following registry entry if the Exchange 2000 computer is running out of memory because the number of incoming messages is too great for the server to process:

- ◆ **Location.** HKEY\_LOCAL\_MACHINE\Software\Microsoft\Exchange\Mailmsg
- ◆ **Parameter.** MaxMessageObjects (REG\_DWORD)
- ◆ **Default setting.** Not present but defaults to 0x186a0

## Store and ESE Tuning

Due to advances in the store process, the Exchange information store requires very little manual tuning. However, better performance can be achieved with good implementation and configuration.

### Online Store Maintenance

The store requires periodic online maintenance to be run against each database. By default, each database is set to run online maintenance between the times of 1:00 A.M. and 5:00 A.M. Online maintenance performs a variety of tasks necessary to keep the store in good health. These include, but are not limited to, the following:

- ◆ Checking Active Directory to determine if there are any deleted mailboxes.
- ◆ Removing any messages and mailboxes that are older than the configured retention policy.
- ◆ Performing online defragmentation of the data within the database.

All of the operations performed by online maintenance have specific performance costs and should be understood in detail before implementing an online maintenance strategy.

### Active Directory Checking

This consists of a Windows 2000 Active Directory service lookup for each user in the database. The more users you have in each database, the more Active Directory searches (using Lightweight Directory Access Protocol [LDAP]) will be made. These searches are used to keep the store in sync with any Active Directory changes (specifically to check for deleted mailboxes). The performance cost of this task is negligible on the server running Exchange but can be significant for domain controllers, depending on the number of users, number of databases, and the online maintenance times of each database. In a corporate

scenario, the online maintenance occurs during the night (by default) when very few users are logged on, so the load on the Active Directory servers should be very low. The extra domain controller load created by online maintenance should not be a problem in this scenario.

If Exchange 2000 is installed in a global data center, serving customers from multiple time zones, the default online maintenance time could become an issue. The effect that online maintenance has on Active Directory is proportional to the number of users in each of the server's databases. A check for a deleted mailbox is performed against each user in a database. Thus, if you have 10,000 users in a database, it will perform 10,000 LDAP searches against Active Directory at the beginning of that database's online maintenance. If Active Directory servers are under moderate load at all times, it is necessary to stagger the online maintenance (set each database to start maintenance at a different time on the server-configuration object). This is especially critical if you have hundreds of thousands of users spread across dozens of servers and hundreds of databases.

#### **Message Deletion and Online Defragmentation**

These are very disk-intensive tasks and only affect the server on which the maintenance is being run. During this portion of online maintenance, the server might be perceived by users as sluggish if many databases are set to perform online maintenance at the same time. Again, in corporate scenarios this would occur at night where the server can easily handle the extra load. In a global data center, it might be a good idea to stagger the databases (in respect to each other on a single server) to spread the disk-intensive tasks over a greater amount of time.

Defragmenting the database consists of 18 separate tasks. After a task has started, it must complete fully before the process exits. Therefore, online maintenance can run over the time window. The next task will execute during the next online maintenance window. Depending upon the run window and the backup schedule, it might take a number of days before a full defragmentation completes.

#### **Online Backups**

Online backups complicate online maintenance even further. Backing up an Exchange 2000 database halts the maintenance of any database within that storage group, although it will restart if the backup is finished before the maintenance interval has been passed. If you have two databases in a single storage group and one is running online maintenance, the online defragmentation on the database that is running online maintenance will stop when a backup is started against either database.

It is critical that the backup time for any database within a storage group does not conflict with the maintenance times of any database within the same storage group. If it does, backup will terminate the online defragmentation portion of the store online maintenance and the database might never finish defragmenting.

### Choosing the Correct Maintenance Strategy

The correct online maintenance strategy can be devised by examining the typical behavior of the user community; by knowing how many users, databases, and servers are in the site; and by coordinating this information with the online backup strategy.

On the next page is an example of an online store maintenance schedule for a corporate Exchange 2000 mailbox server that hosts users who are in a single time zone.

#### First Storage Group

- ◆ Database One  
Online maintenance runs between 9:00 P.M. and 1:00 A.M.
- ◆ Database Two  
Online maintenance runs between 9:30 P.M. and 1:30 A.M.
- ◆ Database Three  
Online maintenance runs between 10:00 P.M. and 2:00 A.M.

Online Backup begins at 2:00 A.M.—it backs up all databases in the first storage group when all of them have finished online maintenance.

#### Second Storage Group

- ◆ Database Four  
Online maintenance runs between 10:30 P.M. and 2:30 A.M.
- ◆ Database Five  
Online maintenance runs between 11:00 P.M. and 3:00 A.M.
- ◆ Database Six  
Online maintenance runs between 11:30 P.M. and 3:30 A.M.

Online Backup begins at 3:30 A.M and backs up all databases in the second storage group when all databases have finished online maintenance. This configuration staggers the Active Directory LDAP queries generated by online maintenance, which are performed in the first minutes of the procedure, and ensures that online backup does not interfere with online defragmentation.

## Extensible Storage Engine (ESE) Heaps

When Exchange 2000 is installed on servers with more than four processors, you might notice high virtual memory usage by the Extensible Storage Engine (ESE) multi-heap. This can lead to performance problems, especially when the server has more than one GB of memory, and many databases and storage groups have been configured. It is recommended that you add the following registry parameter to all servers with more than four processors:

Location:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ESE98\Global\OS\Memory
Parameter:	MPHeap parallelism (REG_SZ)
Default setting:	(Doesn't exist) = Parallelism set to four times the number of processors installed.
Recommended setting:	For up to four processors, take no action. If the server has four or more processors and has the maximum number of storage groups and MDBs, set the value to "0." When set to zero, the parallelism is set to three plus the number of processors on the computer. For example, on eight-processor computers, it is recommended that this registry key be set to "11."

**Note:** You must restart the Exchange information store process after the preceding registry parameter has been changed.

## Store-Database Cache Size

Exchange 2000 is configured with a hard-coded maximum store-database cache size. This default value is 900 MB. On servers with more than 2 GB of memory, it can be beneficial to increase the size of this cache. Due to virtual address space limitations, this value should never be set higher than 1200 MB.

**Note:** The 900-MB limit is in place to ensure that the store process always has ample virtual address (memory) from which to allocate. Increasing this value too much can lead to system instability. For more information regarding virtual address space, see Knowledge Base article Q266096 available at:

[http://support.microsoft.com/support/kb/articles/Q266/0/96.ASP?LN=EN-US&SD=gn&FR=0&qry=Q266096&rnk=1&src=DHCS\\_MSPSS\\_gn\\_SRCH&SPR=MSALL](http://support.microsoft.com/support/kb/articles/Q266/0/96.ASP?LN=EN-US&SD=gn&FR=0&qry=Q266096&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=MSALL)

Factors which affect the virtual address-space size in the Store.exe process include the following:

- ◆ Initial allocation on start-up
- ◆ Number of storage groups and databases on the server
- ◆ Number of threads running
- ◆ Size of the store-database cache

Prior to increasing the maximum cache size, it is recommended that you use the Windows 2000 performance monitor to monitor the memory of the server under normal load. You should monitor the following:

Performance Object: Process  
Counter: Virtual Bytes  
Instance: STORE

This will give you an accurate value for the virtual address space that the store has allocated. On a server with the /3GB setting in the boot.ini, this should be below 2.8 GB. On a server without the /3GB setting in the boot.ini, this should be below 1.8 GB (it is recommended that servers with 1 GB or more of memory have the /3GB switch added to boot.ini).

If you see values that are higher than this for either configuration, do not increase the size of your max cache size. If you see values that are lower than this for either configuration, you can safely increase the size of your database max cache size. That is, if you have a /3 GB configured server and the performance monitor shows the virtual bytes count at 2.5 GB under heavy load, then you know you are safe to increase your max cache size by 300 MB from the default 900 MB or to 1,200 MB total.

- ▶ **To modify the store-database cache size, you will need to use the ADSI Edit tool, which is included with Windows 2000 Support Tools.**
  1. To start ADSI Edit, click **Start**, point to **Programs**, point to **Windows 2000 Support Tools**, point to **Tools**, and then select **ADSI Edit**.
  2. Expand the **Configuration Container** Naming Context of your Active Directory.
  3. Navigate to the following path:  
Configuration Container | CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=<organization>, CN=Administrative Groups, CN=<Admin Group>, CN=Servers, CN=<server>, CN=InformationStore
  4. Right-click the **Information Store** object and then select **Properties**.
  5. Select **Both** from the **Select which properties to view** drop-down list.
  6. Select the **msExchESEParamCacheSizeMax** attribute and adjust the value. Although no value will be present, the default is 230400 (which is 900 MB). The recommended maximum for this value is 307200 (which is 1,200 MB).

---

**Note:** Be careful when setting this value, because it is very easy to make a mistake and set the *msExchESEParamCacheSizeMin* attribute instead.

---

7. Click **Set** after changing the **Edit Attribute** field for the attribute and then click **OK**.
8. Close the ADSI Edit tool by closing the MMC console application.
9. Wait for Active Directory replication to replicate this new value throughout the forest (this might take some time—using ADSIEdit elsewhere in the organization will show you how replication is proceeding).
10. Restart the Microsoft Exchange information store service on the Exchange 2000 computer.

### Log Buffers

ESE uses a set of log buffers to hold information in memory before writing to the transaction logs. For back-end servers, the default value is too low. This can cause excessive disk I/Os to the transaction log drive. A significant performance improvement will be seen when the server is under load or when users are sending large messages. The default value is 84; this should be increased to 9,000 on all back-end servers.

The process for setting log buffers is very similar to increasing the store-database cache size (as detailed earlier). You will need to use ADSI Edit to navigate to the storage group object and then find the **msExchESEParamLogBuffers** attribute. The value is an integer and it should be set manually to 9,000.

### Tuning Active Directory Integration

When there are numerous computers running Exchange 2000 in a Windows 2000 site, a very large LDAP load can be put on the Active Directory servers. An Active Directory server, by default, is configured to support a maximum of 20 active LDAP queries. If this limit is reached, Active Directory will return the error **LDAP\_ADMIN\_LIMIT\_EXCEEDED** and will refuse to process further LDAP queries until the active number drops below 20. Twenty is generally sufficient for most Active Directory servers, but it is necessary to increase this value when you are running Exchange 2000 on six- or eight-processor servers, or if the preceding error message is logged.

The maximum LDAP queries can be configured through the **MaxActiveQueries** attribute. This can be adjusted using the **NTDSUTIL.EXE** tool. Increasing this setting will use a little more memory in the **LSASS.EXE** process on the Active Directory server, so do not increase this value any more than is necessary. The following steps show how you would increase **MaxActiveQueries** to 40:

1. After opening the command prompt window, type **NTDSUTIL**.
2. Type **LDAP POLICIES** and press Enter.
3. Type **CONNECTIONS** and press Enter.
4. Type **CONNECT TO SERVER** <domain controller/Global Catalog server name> and press Enter.
5. Type **Q** and press Enter.

6. Type **SHOW VALUES** and press Enter.
7. Type **SET MAXACTIVEQUERIES TO 40** and press Enter.
8. Type **COMMIT CHANGES** and press Enter.
9. Type **SHOW VALUES** and press Enter.
10. Verify that the new setting is shown.
11. Type **Q** and press Enter.
12. Type **Q** and press Enter.

---

**Note:** This setting will be replicated to all Active Directory servers within the forest. You do not have to restart domain controllers or Global Catalog servers for this to take effect.

---

Under normal circumstances, Exchange 2000 will access Global Catalog servers and the user partition of domain controllers by consulting a dynamically created list of available servers. While this is fine in the majority of circumstances, in some environments you might want to change the behavior to maintain performance. For example, you might have some underspecified domain controllers on your network, and you might wish to prevent these from being used. Or you might have very slow links in your environment and you might want to prevent servers running Exchange elsewhere in the domain from using these Global Catalog servers or domain controllers.

To ensure that particular domain controllers or Global Catalog servers are used to service requests, you can statically configure DSAccess to channel directory service loads to a specified set of directory-service servers.

You should think carefully before deciding to statically define these entries, as you generally run a greater risk of losing directory access entirely. DSAccess does not check to see if the names you specify are valid, so if you spell server names wrong in the registry, you can end up with a loss of service. Also, if static entries have been defined, then Exchange will not check dynamic entries, even if the static ones are invalid.

The following entries can be added to statically define domain controllers and Global Catalog servers:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess
\Profiles\Default\UserDC1 (UserDC2, and so on)
```

```
IsGC = REG_DWORD 0x0
```

```
HostName = REG_SZ DC_DomainName.CompanyName.com
```

```
PortNumber = REG_DWORD (0x185 by default or 0x27C for SSL)
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess
\Profiles\Default\UserGC1 (UserGC2 and so on)
```



```
IsGC = REG_DWORD 0x1
HostName = REG_SZ GC_DomainName.CompanyName.com
PortNumber = REG_DWORD (0xCC4 by default or 0xCC5 for SSL)
```

---

**Note:** Domain controller entries are defined independently of Global Catalog server entries, so it is conceivable that a static list would be used to locate Global Catalog servers, whereas a dynamic list would be used to find domain controllers.

---

Exchange 2000 stores and reads some information in the configuration partition of Active Directory. You might want to define which domain controllers Exchange 2000 should use when accessing the configuration partition. This is not a particularly dangerous setting, because it is a preference, not a requirement. If your favored domain controller is not available, it will switch to another on the list of available domain controllers (chosen by the method indicated previously).

To set your preferred configuration partition domain controller in the registry, alter the following:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess
\Instance0
ConfigDCHostName = REG_SZ configDC_DomainName.CompanyName.com
ConfigDCPortNumber = REG_DWORD (0x185 by default or 0x27C for SSL)
```

For more information on how Exchange 2000 selects domain controllers and Global Catalog servers, see the Knowledge Base article Q250570 available at:

[http://support.microsoft.com/support/kb/articles/Q250/5/70.ASP?LN=EN-US&SD=gn&FR=0&qry=Q250570&rnk=1&src=DHCS\\_MSPSS\\_gn\\_SRCH&SPR=MSALL](http://support.microsoft.com/support/kb/articles/Q250/5/70.ASP?LN=EN-US&SD=gn&FR=0&qry=Q250570&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=MSALL)

## Tuning Outlook Web Access (OWA)

In environments where many users will use Outlook Web Access as their client, traffic and resources on the Exchange 2000 server—as well as latencies apparent to the user—can all be reduced by increasing the time until expiration of static files from the \Program Files\Exchsrvr\Exchweb\Controls and \Img directories. These static files include all the .gif icons, navigation or tool bars, and windows for display of messages, calendar items, and so forth.

By default, these files are marked as expiring in one day when they are received from the server by the browser; thus, once each day, each user will request and receive these files from the server. Except in cases where static content is modified to include system messages or advertisements, these files will not change except possibly in the event of a future Exchange Service Pack installation. Increasing the time before expiration to a month or a year (or setting the content to not expire) might make more sense. In such a case, these objects might only be expired out of the client's browser cache if the cache became full and older items were

deleted. In addition, each time the user accesses Outlook Web Access, the browser will send an “is modified” request for each static file cached; therefore, even if a future Service Pack does modify \Exchweb content, the browser will immediately pick up the changes.

Changing this setting does not involve the registry. Instead, you will need to perform the following steps:

1. Start the Internet Services Manager. Click **Start**, point to **Programs**, point to **Administrative Tools**, and select **Internet Services Manager**.
2. Expand the server icon.

---

**Note:** If you are performing this procedure on an Exchange 2000 Server cluster, expand the Exchange Virtual Server instead of the Default Web Site in the following step.

---

3. Expand the Default Web Site.
4. Expand Exchweb, and view **Properties** on the \Controls and \img directories.
5. Under the **HTTP Headers** tab, you can either clear the **Enable Content Expiration** checkbox or select the **Expire after** property to a value greater than the one day default.



**Figure 2.1**  
*Setting OWA Properties*

---

**Note:** If you ever need to force Internet Explorer to refresh the entire content of a page, thus ignoring data in the cache, open the URL, then hold down CTRL and press F5. In Netscape Navigator, hold down SHIFT and click Reload.

---

## Hardware Upgrades

Exactly when hardware upgrades are required depends on the results of your capacity planning. If you plan your capacity well, you will be able to predict when hardware upgrades are required, which is particularly important when there are long lead times on hardware. Failing to predict when new hardware will be required can lead to severe availability management problems, for example if a server running Exchange were to fail because you ran out of disk space.

It can be very beneficial to perform hardware upgrades on a regular basis, standardizing on new hardware each time. This allows you to keep your hardware consistent across each Exchange 2000 role and therefore reduce support costs for the new environment. Always ensure that you test Exchange and Windows 2000 thoroughly on the new hardware to ensure that there are no unforeseen anomalies.

In many cases hardware upgrades coincide with software changes or with consolidation of servers. If this is the case, you must ensure that the new hardware is able to cope adequately with the new environment and with any intermediary changes you need to make to get to your final environment. As with all areas, ensure that you plan and document thoroughly any changes that you make to the hardware environment. If you are rolling out hardware changes across the entire organization over a short period, this can be a very labor intensive period for your operations department, so ensure that you plan carefully for the appropriate skills to be assigned.

Having a clustered environment is the best way to perform an upgrade while simultaneously minimizing downtime. Under these circumstances, you can perform a rolling upgrade—manually failing over the system to node A, performing an upgrade on Node B, failing it back over again to Node B, performing an upgrade on Node A, and then returning the system to normal.

You will also need to ensure that there is provision in your SLAs for hardware upgrades. Hardware upgrades often involve periods of scheduled downtime, especially if you do not have clusters everywhere, and you need to allow for this when you define your SLAs. With proper planning, both scheduled and unscheduled downtime can be kept to a bare minimum.

## Summary

This chapter has shown you how to manage capacity and availability in your Exchange 2000 environment. You have seen performance-tuning changes that are easy to identify and implement to obtain better performance and you have learned how to examine what areas to consider when implementing hardware changes in your organization.







# 3

## Change and Configuration Management

### Introduction



Exchange 2000 Server is highly configurable and has the potential for huge variation in hardware and software configuration. It is also likely to be one of the most important elements of your IT environment. For Exchange to run as smoothly as you hope, providing the best possible service to users, you need to make sure that your environment is carefully managed. In particular, you need to ensure that any changes to the environment are considered in detail before implementation and that good records are kept of all elements of the IT environment.



The goal of the change management process is to introduce change into the IT environment quickly, with minimal disruption. All businesses are subject to change, and IT is a business area which is subject to more change than most. A fundamental part of good IT operations is to accept change and control it appropriately. A good change management process also includes a method for quickly implementing urgent changes required to quickly restore IT services. Change management should be a core and constant part of your IT operations, not just something you visit when there is a major upgrade.

Change management is closely related to configuration management, which is the process responsible for identifying, controlling, and tracking all of the elements of the IT environment. Good configuration management ensures that only authorized components are used in the IT environment and that all changes are recorded in a configuration management database.

This chapter discusses both change and configuration management, with particular reference to Exchange 2000 Server.



## Prerequisites

By now you have defined a set of acceptable service level agreements for your Exchange environment and you understand the concepts of availability management that were discussed in Chapter 2, “Capacity and Availability Management.”

## Chapter Sections

This chapter covers the following procedures:

- ◆ Change management
- ◆ Configuration management

## Change Management

Effective change management allows you to introduce change into your IT environment quickly and with minimal service disruption. Change management is responsible for changes in technology, systems, applications, hardware, tools, documentation, and processes, as well as changes in roles and responsibilities.

A key goal of the change management process is to ensure that all parties affected by a particular change understand the impact of the impending change. Because most systems are heavily interrelated, any change made in one part of a system can have major impacts on others. Change management attempts to identify all affected systems and processes before the change is implemented so that adverse effects can be minimized.

As with many areas of management, you can measure how effective your change management is by how boring it is. Providing a smooth running change management process is one of the most challenging aspects of IT management because of the very nature of what you are managing—change. With the proper processes in place however, your environment should run very smoothly.

### Defining Change Type

To most effectively manage change within your organization, you need to categorize the types of changes that could occur. In Exchange, these changes could include the following:

- ◆ Applying Service Packs
- ◆ Adding new servers
- ◆ Adding new users
- ◆ Adding new administrative groups
- ◆ Changing routing group topology
- ◆ Changing backup and restore procedures
- ◆ Modifying and applying policies
- ◆ Changing other existing settings
- ◆ Changing a process or script used to administer servers

Change can be broadly categorized into four groups, each requiring its own style of management. The groups are:

- ◆ **Major change.** Significantly impacts the IT environment, and requires major resources to plan, build, and implement (for example, upgrading all Exchange 2000 Server hardware).
- ◆ **Significant change.** Requires substantial resources to plan, build and implement (for example, upgrading to a new Service Pack).
- ◆ **Minor change.** Requires no significant resources and doesn't significantly impact the IT environment (for example, modifying certain Exchange system policy settings).
- ◆ **Standard change.** Follows a standard documented procedure, which should not affect the IT environment at all (for example creating new mailboxes).

Of course, the more changes that you can successfully fit into the latter two categories, the less likely there will be a significant disruptive impact upon your organization. This does not mean that you should avoid significant or major change. Indeed, major or significant change can often prevent problems with availability management later on. For example, deploying a new Service Pack throughout your organization may enable you to avoid encountering problems with your environment.

By thoroughly documenting as much of the Exchange environment as possible, including how changes should be made, you can maximize the number of changes that are categorized as minor or standard, thereby significantly decreasing the costs associated with change.

Change management involves the following five activities:

- ◆ A change is requested.
- ◆ The impacts (technical and business) of making the change are assessed (this includes testing in a lab environment).
- ◆ The change is authorized.
- ◆ The change is handed to Release Management for implementation.
- ◆ The change is verified.

Numerous parties should be involved in Exchange change management. To see how these parties would typically interact, examine the following major change, upgrading *all* servers running Exchange to new hardware.

### Step 1 – Request for Change Is Submitted to Change Manager

Everybody in your organization should be authorized to submit a request for change (RFC). In this scenario, the likelihood is that the RFC has come from a member of your IT staff.

Other change sources include IT staff responsible for problem management (for example, root cause analysis), service level managers who are planning to sell new kinds of service or upgraded levels of existing service, and so on.

## Step 2 – Change Manager Assesses the RFC

The change manager receives the RFC and records it in the change management log. The manager examines the RFC, checking to see if it is a complete and practical proposal. If in any way the proposal is deemed unsatisfactory, it is handed back to the person who submitted the RFC (known as the change initiator) with appropriate red marks, or even if it is approved, the change manager may pass it back to the change initiator for further analysis.

After the change is determined to be satisfactory, and appropriate information is gathered, the change manager prioritizes the change. Change is prioritized as urgent, high, medium, or low, which determines how soon the change will be made:

- ◆ **Urgent.** Changes that must be performed immediately and are quickly transferred to the urgent change process.
- ◆ **High priority.** Changes that must be performed quickly to maintain Exchange availability to a significant number of users.
- ◆ **Medium priority.** Changes that are necessary to resolve problems, but are not of immediate importance, or only affect a small number of users.
- ◆ **Low priority.** Changes that can typically wait till the next major release of Exchange to resolve the problem.

In this case, upgrading server hardware is usually categorized as medium priority.

Now the change needs to be categorized. In this case, as already mentioned, it would be judged as major change. The change manager will make a note of this prioritization and categorization in the change management log.

At this stage, if the RFC is assessed as a minor or standard change, the change manager would probably pass the RFC directly to the change owner responsible for implementing the change. If the RFC is considered to be a significant or major change, it will be passed to a delegated team that will prepare implementation options for consideration in the next stage.

## Step 3 – Change Is Passed to IT Executive Committee for Approval

The IT executive committee has the responsibility of approving major change in the organization. It will typically consist of senior members of the IT staff in your organization. It will judge if the hardware upgrade should proceed or not.

## Step 4 – Change Is Passed to the Change Advisory Board for Scheduling

The change advisory board consists of a core group of individuals, people who are familiar with business requirements, the user community, IT system technology, and the organization's application development, testing, and support staffs. Typically the change advisory board includes the release, capacity, configuration, network, security, and systems administration managers. In addition, the change manager appoints others who have expertise relevant to the particular RFC and representatives from the group affected by the



change. In this case, expertise with Exchange and hardware is very important. In fact, the change manager may decide to appoint an OEM vendor representative to the change advisory board.

The change advisory board determines the hardware upgrade schedule, according to IT executive committee recommendations. The change advisory board is also responsible for monitoring the change and it ensures that all authorized changes are coordinated and scheduled to eliminate the possibility of one change negatively affecting another change.

### Step 5 – Change Is Passed to the Change Owner

The change owner is responsible for planning and implementing the hardware upgrade once it has been approved and scheduled by the change management process. The change owner will provide feedback to the change advisory board, the change manager and perhaps the change initiator during the implementation. However, the change manager remains involved at this stage, monitoring what the change owner is doing.

After the upgrade is complete, the change owner will help the change manager and change initiator assess the impact of the change.

All of this may seem to be a deeply complicated process, but remember this describes a major change to the environment. Minor changes would pass through a significantly simpler path, involving the change owner.

### Step 6 – Change Process Evaluation

After the change is implemented, the entire change management process from receipt of RFCs through implementation must be evaluated. This is done by conducting personnel interviews and reviewing documentation. The main objective is to assess the effectiveness of the change process. Unsuccessfully implemented changes should also be evaluated so that problems can be identified and corrected before further changes are initiated.

Figure 3.1 illustrates the change management process, with the parties responsible for each stage. (For the sake of clarity, this diagram largely ignores inter-related areas of management such as configuration and availability management.)



**Figure 3.1**  
*The Change Management Process*

## Minor and Standard Changes

The advantage of minor and standard changes is that individuals with less authority can be pre-assigned the permissions to perform them. This is perfectly fine, because the changes themselves are not likely to cause significant problems when implemented. Of course, the change manager, and perhaps the change advisory board will, at some point, have determined whether a particular change is minor or standard. However, once this is done and the nature of the change is documented, the change owner can be pre-authorized to either perform the change in person or to delegate that authority to another person.

A classic example of a standard change is the addition of a user. This type of change should have been anticipated, so the change manager will have already pre-authorized the change owner to be responsible for this change. The change should be thoroughly documented with standard settings for items such as mailbox size limits and deleted item retention time.

## Scripting Minor and Standard Changes

Although minor and standard changes do not take very long, they are among the most repetitive of tasks and therefore the ones most likely to benefit from automation.

To further reduce the amount of time spent on these tasks, you may want to consider using automated tools. Using the example of mailbox creation, the change advisory board may have previously categorized users according to job role. There would be a series of pre-defined settings for each type of user. Administrators could then use a Web-based tool to create the users, specifying the job role. Scripts would run against Active Directory to place

the user in the appropriate Windows 2000 groups and create the Exchange 2000 mailbox with the appropriate settings for that user.

Over time, your team will build a set of custom tools that are used frequently to administer standard changes. Those tools and others will likely be used for implementing larger changes. Treating these tools and procedures as configuration items and managing their evolution over time is another example of the close relationship of change management and configuration management.

## Security

A very important part of effective change management is your security infrastructure. If you do not carefully control who is capable of making which change, you can end up with undocumented and unauthorized change occurring in your organization. You should always ensure that your administrators only have rights to perform tasks that they have been specifically pre-authorized to perform. In Exchange 2000 Server, administrators require View Only Administrator rights over the Exchange 2000 organization if they are to create and modify user accounts.

## Software Control and Distribution

Updating software represents significant change. It can have a major impact on users, and as such it should be planned very carefully to ensure that the update has minimal impact on users. (Occasionally such a change may be urgent, and under those circumstances you will not have time for thorough planning, but you should still plan as much as possible).

In a multi-national company with distributed administration, one of the challenges can be to ensure that software updates are distributed as smoothly as possible. One solution to this is Microsoft Systems Management Server, while another is to use the software assigning and publishing functionality of Windows 2000.

## Documentation

Linking all of the change management process together is the very strong need for up-to-date, complete, and accurate documentation. Without thorough documentation, many of the benefits of change management will be lost for your organization.

Thorough documentation is invaluable when implementing recurring changes. One of the main benefits of thorough documentation is that it can turn major or significant change into minor or standard change. Many changes are major or significant simply because you have never made them before. But if you have, and you have documented standard procedures that allow you to avoid downtime and periods of poor performance for users, it may allow your IT executive committee or change advisory board to pre-authorize that change for the future, significantly reducing the number of steps required to make the change the next time.

You should ensure that entire process of change is properly documented in the change management log. The log contains information about the change, including RFC status,

schedule information, and work orders. It is the responsibility of the change initiator, change manager, and change owner to ensure that you have appropriate documentation about the change. Change management should also work closely with configuration management to ensure that all changes to IT components are properly documented in the configuration management database, which is a repository used to track the status of all components of the IT environment. (For more information, see the “Configuration Management” section later in this chapter.)

Of course it is not enough just having the data available, it needs to be easily accessible by those who need it, easily searchable, and of a standard form. This allows others to get to and understand the data when they see it. If you have a good knowledge management system in your organization, you are able to ensure that the documentation is available to the appropriate people where and when they need it. By implementing Exchange 2000, you will already have many of the tools to create a good knowledge management system! RFCs can be easily submitted via Microsoft Outlook® messaging and collaboration client forms and the change management log stored in public folders, indexed using full text indexing.

## Configuration Management

You cannot accurately know where you want to go today, or indeed how to get there, unless you know where you already are. Configuration management is a process which determines and records exactly that.

Configuration management is responsible for identifying, controlling, and tracking all versions of hardware, software, documentation, processes, procedures, and all other components of the IT environment under the control of change management. These items are referred to as configuration items and all changes to them are recorded and tracked throughout the component lifecycle.

Central to configuration management is the configuration management database. The configuration item data controlled by configuration management is stored in the configuration management database, which is a relational database used to track configuration items in the IT environment.

What makes configuration management so useful to your organization is that the relationships and dependencies between configuration items are recorded. As a simple example, imagine that an RFC is submitted to the change manager, requesting a memory upgrade on all of your domain controllers. Assuming that the request is approved, the configuration management database can be checked to see which users and which applications will be affected when that server is taken offline. In this case, because Exchange depends upon domain controllers for its functionality, the configuration management database would indicate how Exchange 2000 Server functionality would be affected and the resultant impact on the users. The users can then be forewarned of the impending problems so that they can plan their activities around it.

Another example is hardware tracking. Imagine that your hardware vendor releases a new firmware version for the standard network adapter that you use in some or all of your servers. If you track firmware versions of each network adapter, and the relationship of each network adapter to a system, and the relationship of a system to a rack location, it is straightforward to identify the physical location of each network adapter requiring the firmware upgrade.

## Tools for Configuration Management

There are numerous good tools for performing configuration management. It is not necessary to write your own tools in most cases, especially because the existing tools are very configurable. Before you spend much time on defining the exact form of your configuration management, examine the capabilities and limitations of each tool. This allows you to determine how your configuration management process may need to be modified to accommodate the vagaries of your chosen tool.

## Configuration Management and Change Management

Configuration management is intrinsically linked to change management. In fact, only items that come under the control of change management are entered into the configuration management database. Configuration items are initially entered into the configuration management database when RFCs are approved for implementation by the change advisory board or the IT advisory committee. From this point on, changes to and status of the configuration items are recorded in the configuration management database.

Therefore, the configuration management database acts as a historical record of changes to the environment and maintains a “picture” of the existing IT environment. After they are logged into the configuration management database no changes to configuration items in the IT environment should be made without authorization from change management by following the RFC process as discussed in the change management process. Change and configuration management work closely together to ensure that a clear and complete “picture” of the environment is always available.

## Configuration Items

Configuration items are objects that fall under the category of change management, and are therefore subject to change. In Exchange 2000, configuration items include the following:

- ◆ Exchange Server hardware
- ◆ Domain controller hardware
- ◆ Hardware vendor
- ◆ Server role (that is, a server running Exchange or domain controller)
- ◆ Windows 2000 software
- ◆ Exchange 2000 Server software

- ◆ Service Packs
- ◆ Hot fixes
- ◆ Anti-virus software
- ◆ Fax/voice mail Gateways
- ◆ Monitoring software
- ◆ Backup software
- ◆ Network equipment connecting the servers
- ◆ Processes and procedures
- ◆ Documentation
- ◆ Exchange users
- ◆ RFCs

Each configuration item will have attributes associated with it. Take as an example the Exchange software. It will have the following attributes associated with it:

- ◆ A software identifier
- ◆ The RFC identifier that led to the current software version
- ◆ The name of the application (for example, Exchange 2000 or Exchange 2000 Server Enterprise Edition)
- ◆ The version number of the software
- ◆ The date the current version was installed
- ◆ The latest Service Pack installed
- ◆ The latest hot fix installed
- ◆ The vendor who supplied the current software (for example, Microsoft Corporation)
- ◆ The documentation required to support the current version of the software

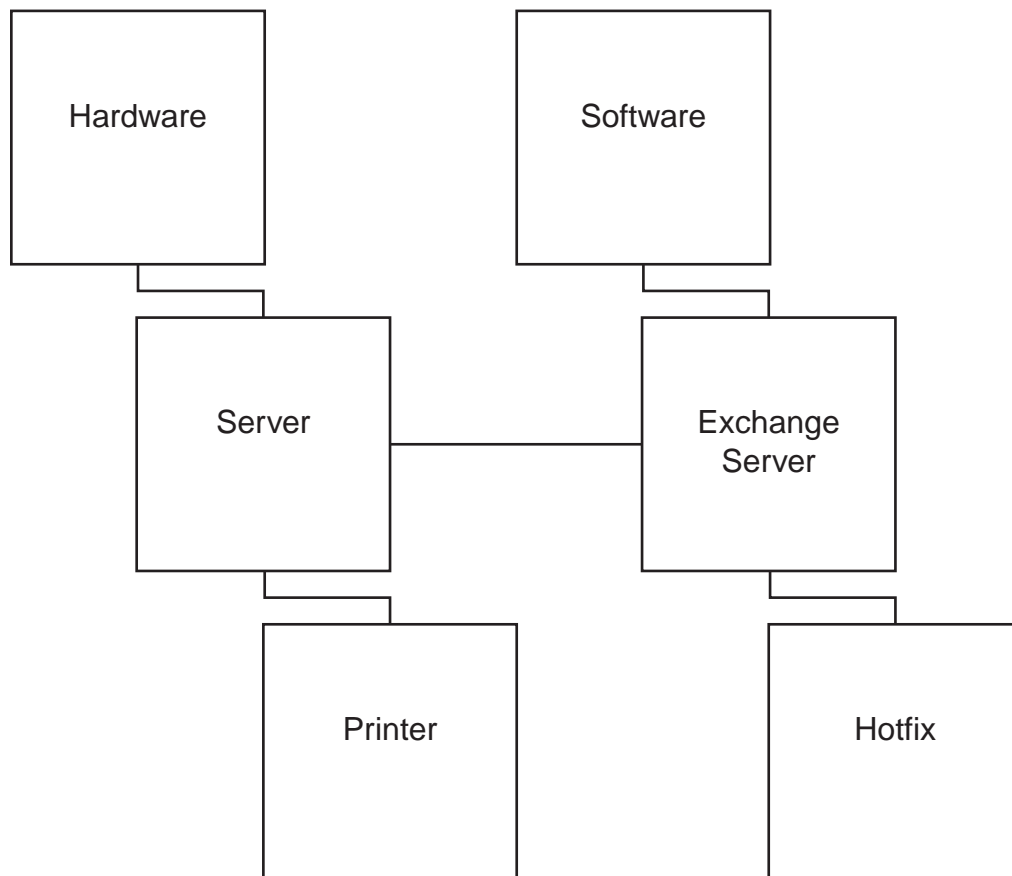
The number of configuration items depends on the level of granularity you choose when defining them. It is, of course pointless to store configuration items that you will never use. A simple configuration management database will give you much less data to store and so will be much less work to store. However, if you do not have data at a sufficiently granular level, you will limit the effectiveness of the configuration management database.

You can always add more detailed information at a later date, if you want. However, despite the initial pain, you will generally find it better to set your granularity of configuration items at the level of the lowest replaceable unit. In terms of servers running Exchange, this would be, for example at the RAID Controller, or network adapter level. For example, this allows you to change every network adapter in every server running Exchange in your organization, and effectively monitor and manage that change.

### Configuration Management Relationships

Many of the main benefits of configuration management come from the relationships between the configuration items that are defined in the structure of the configuration management database. Getting these relationships correct is vital for successful configuration management.

The relationships grow more complex the more configuration items you have. To see the principle, take a very simple example, with only six configuration items, showing a simple relationship between Exchange hardware and software, as illustrated in Figure 3.2.

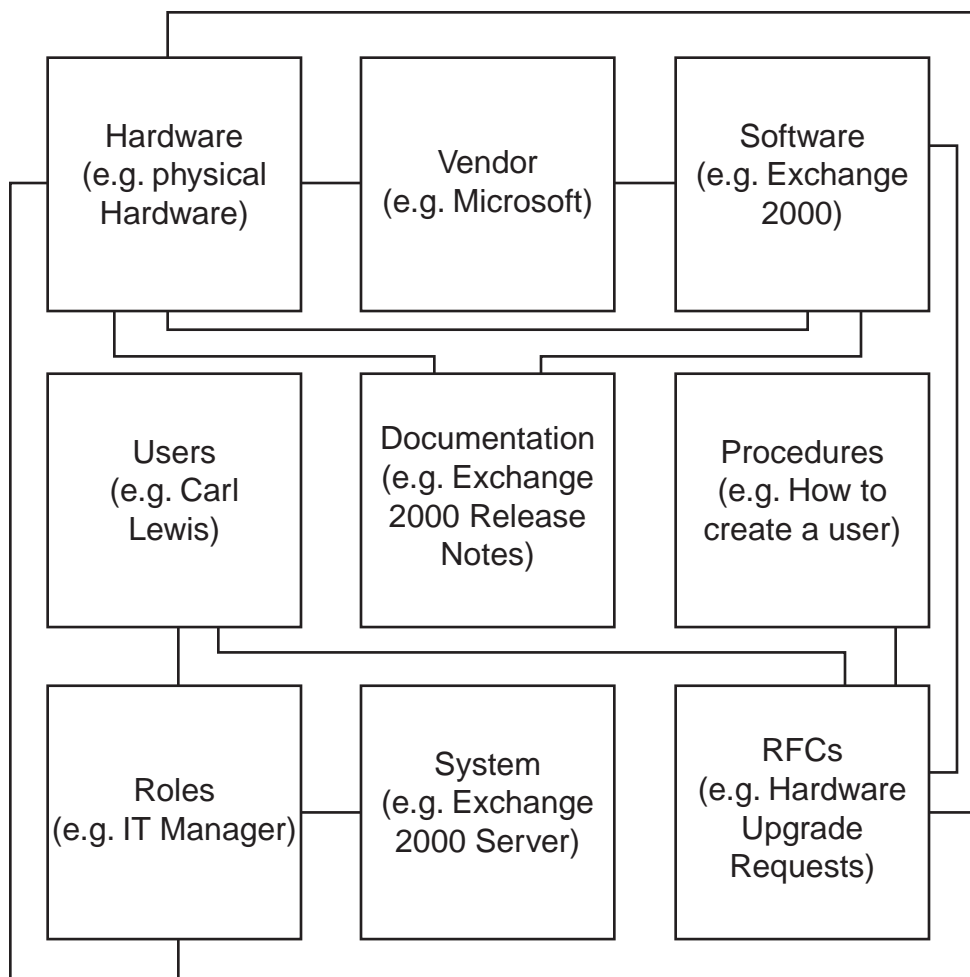


**Figure 3.2**  
*Six Configuration Items and Relationships Between Them*

Here the server itself is obviously hardware, but it also represents the software that is to be installed on it. These elements depend on each other. If there was no hardware, Exchange would have nothing to be installed on, and if there is no Exchange 2000 software, there is little point in having the hardware.

Here, the printer is related to the server because it is connected to it. Exchange 2000 Server is licensed to the server hardware. The hot fix is another configuration item, but one that clearly has a relationship to the server running Exchange on which it is installed.

Of course with more configuration items, this process is significantly more complicated. To see this, take a look at a slightly more complex example. Figure 3.3 illustrates nine types of configuration items, with suggested relationships between them.



**Figure 3.3**  
*Nine Configuration Items with Relationships Between Them*

As you can see, there is still a fairly small number of configuration item types at this stage, although the configuration items themselves will differ in a substantial way (for example, anti-virus software will have significant differences from Exchange 2000 hot fixes).



## Defining Configuration Items

When defining configuration items you need to decide how deeply you want to go in recording the them. Too many configuration items makes the relationships too difficult to manage and costs start to increase. There are strong benefits to making the configuration management database as simple as possible to actively reflect the environment in which it is working, then adding in additional configuration items as and when they are required.

## Configuration Management and Exchange

One of the main barriers to implementing configuration management in an organization is the perception that it must be implemented throughout the organization or not at all. This is by no means true. Configuration management can effectively apply to one part of the organization without touching other parts of it. It is true, of course, that the more wide-spread configuration management is in a company, the more cost-effective it becomes, but this does not preclude you from implementing configuration management cost-effectively in your company, even if it affects only Exchange.

In many cases, setting up configuration management for Exchange proves to be a precursor to setting it up elsewhere. You should not be afraid of starting with Exchange for the configuration management process if it has not been implemented before in your company.

In the example of upgrading the servers running Exchange shown previously, you can see from the simple set of relationships, that upgrading the hardware affects a series of related areas:

At the very least, new hardware may affect the following elements of the configuration management database:

- ◆ **User roles.** All users who have their mailboxes located on the server may have service interrupted and after the upgrade should expect better service. Consulting the configuration management database should reveal the identity of these users.
- ◆ **The RFC.** An RFC will have been submitted to initiate this change. The RFC status will be altered as the change is implemented
- ◆ **Vendor.** If the new hardware is from a different vendor, new configuration items may be required.
- ◆ **Documentation.** New documentation will be needed to support the new hardware in place.

## Maintaining the Configuration Management Database

For configuration management to work properly, it is vital that all the information in the configuration management database is up to date and accurate. Your IT staff will very rapidly lose confidence in the system if, for example, they consult the database to find

which connectors will be affected by taking a server running Exchange offline for maintenance, only to find when they actually examine the servers that different connectors are present.

The configuration management database is initially populated by an inventory of your existing hardware, software, tools, and processes. The configuration management database contents change over time as the result of implemented changes of all kinds. You will want to periodically (perhaps annually) audit the configuration management database against reality to ensure that the configuration management database and your IT environment are in synchronization.

To ensure that the database is maintained with accurate information, the following areas must be tightly controlled:

- ◆ Change management
- ◆ Ownership of the configuration management database
- ◆ Security of the configuration management database
- ◆ Backup of the configuration management database

To be effective, the configuration management database must be operated as though it is a central component of your IT environment.

### Change Management

As already mentioned, change management and configuration management are intrinsically linked. If the configuration management database is to be accurate and up to date, then no aspect of change to configuration items may be carried out without that change also being recorded in the configuration management database. For this reason, RFCs are recorded in the configuration management database and are the driving force behind change in the configuration management database. By adding and modifying entries in the RFC part of the configuration management database you will also modify the components that act as dependencies.

### Ownership

If your configuration management database is going to remain fully accurate, you must ensure that there is ownership of each part of the configuration management process. The configuration manager should ensure that the configuration management database is always kept fully up to date and that only authorized personnel can modify it. Exactly who modifies the configuration management database depends on nature of the relationship between change and configuration management, but in many cases different configuration items have different owners (often the corresponding change owner).

## Security

Security is a vital component of configuration management. The only way in which you can maintain control over your configuration and ensure that the configuration management database is accurate is by ensuring that only authorized personnel change configuration items and that only authorized personnel can make the corresponding changes to the configuration management database.

## Backup

With good configuration, the configuration management database is an essential part of your organization. It is therefore essential that you back it up regularly and can ensure that you are able to recover to the point of failure. Examine carefully the configuration management tools that you use, to ensure that you have an effective back up and restore strategy.

## Exchange System Policies

Microsoft Exchange 2000 Server is equipped with policies to control recipient e-mail addresses, server configuration, mailbox store configuration, and public folder store configuration. Using Exchange 2000 system policies you can centrally manage as many or as few servers running Exchange as you desire, and you can dramatically reduce your costs in maintaining a consistent configuration across your enterprise. You can create as many system policies as you like; however, each server can have only one server policy, mailbox store policy, and one public folder store policy associated with it.

## Administering System Policies

One of the main advantages of Exchange 2000 system policies is that it allows you to centralize administrative control easily. The administrative model you follow determines how you should implement system policies. It can often make sense to create one or more management administrative groups. You would give your policy administrators rights over these groups, plus any other administrative groups where you want the policies to be applied. Local administrators would have rights to their own administrative groups but not over the management groups, therefore preventing them from removing the policies or changing anything set in the policies.

When you are creating your policies, you have a choice over which settings to determine. Typically you will look to use policies to define almost every aspect of servers, mailbox stores, and public folder stores. However, think carefully before deploying the Associated Public Store parameter, because this is likely to be different for a large number of servers and would therefore in many cases require the creation and maintenance of a large number of policies.

## Summary

Whatever the size of your organization, you should consider the processes described here and how they can benefit your organization. Remember that the change initiator, the change manager, the change advisory board, and the IT executive board are just descriptions of roles in your organization and can easily overlap.

Many organizations have some difficulty justifying the cost of implementing configuration management. However, for most companies, the benefits of implementing and correctly administering a configuration management process far outweighs the costs of establishing and maintaining the process. Deciding upon a level of granularity of configuration items that is appropriate for you allows you to decide upon a cost structure that will benefit your organization.

If you do not have change and configuration management in your organization currently, you can still implement it for your Exchange 2000 Server environment. It is very likely that doing so will considerably improve the efficiency and the reliability of your operations.



# 4

## Enterprise Monitoring

### Introduction

Monitoring is an essential part of successful Exchange 2000 Server operations. Through effective monitoring, you are able to determine if you are meeting service level agreements, and if you are not, which areas are causing problems (known as reactive monitoring). You can even use a trend analysis of the data you have collected to predict future problems for your organization and to obtain a global picture of your Exchange 2000 Server environment (known as proactive monitoring). Good reactive and proactive monitoring will help you to maintain high availability for your servers running Exchange.

In this chapter, you will learn how to monitor at the server level and the client level, the key areas to monitor, and what benefits you will gain from thorough monitoring.

### Prerequisites


Before beginning this chapter, you should be familiar with service level agreements and basic operations procedures (covered in Chapter 1, “Introduction”).

### Chapter Sections

This chapter covers the following procedures:

- ◆ Performance monitoring
- ◆ Event monitoring
- ◆ Availability monitoring
- ◆ Client monitoring
- ◆ Operation personnel notification

At the end of this chapter, you will be able to monitor your Exchange 2000 Server environment effectively.



## Performance Monitoring

Performance Monitoring is the monitoring of existing system(s) to ensure that optimum use is made of the hardware resources, and that agreed performance levels can be maintained.

Performance Monitoring allows you to determine if your server running Exchange 2000 is meeting the performance standards you have defined in your service level agreements (SLAs). Over time, you can use Performance Monitoring to generate data that can be used in trend analysis. This alerts you to possible performance and availability issues in the future, and allows you to solve problems before they arise).

One of the first tasks involved in performance monitoring is to generate a baseline. This baseline is a measure of what figures you expect to see when measuring a healthy system. This can then be compared to the figures you gather in day-to-day monitoring, allowing you to track problems easily.

In this section, you will look at the objects and counters that you may want to monitor using System Monitor. These parameters will form the basis of your baseline. You will also examine centralized monitoring techniques for remote servers.

### System Monitor

If your e-mail system was Exchange Server 5.5, you are probably accustomed to using Microsoft Windows NT 4.0 Performance Monitor to analyze the performance of your Exchange 5.5 server. Exchange Server 5.5 includes a series of Performance Monitor Workspaces to allow you to quickly see in graph form a series of key counters.

The Windows 2000 operating system includes System Monitor (which consists of Performance Monitor and Network Monitor) for analyzing the performance of your system. When you install Exchange 2000 Server, a large number of objects are installed and counters are associated with those objects.

It is worth noting that while real-time graphs created in System Monitor often look very pretty, they are only of limited use, particularly if no one is looking at them. If you continually monitor 500 different counters on your server running Exchange, the self-monitoring uses CPU cycles. You have now undermined the performance of that server just by monitoring it. So only monitor what you need to, and consider using Performance Logging and Alerts, which can produce much more useful information with less of a load on the server. Reducing the frequency of monitoring produces much less of a load on the server and in many cases produces a more accurate picture, depending on the counters in question.

---

**Note:** Remote monitoring is almost always better than self-monitoring, because performance is not tainted by the load caused by monitoring. For more information about remote monitoring, see articles Q243283, Creating a Log File to Send to Customers for Remote Monitoring and Q240389, Error Message: Event ID: 2028 "The Service was Unable to Add the Counter \\Server\_Name\Counter\_Name" in the Microsoft Knowledge Base.

---

## Exchange 2000 Objects and Counters to Monitor

Every Exchange 2000 performance object has at least one counter associated with it. For information on particular counters, in Performance Monitor, click **Select Counters from List**, select a counter, and then click **Explain**.

Table 4.1 shows the various Exchange services and resources and the associated performance objects that you can monitor.

**Table 4.1 Services, Resources, and Associated Performance Objects**

Service or Resource	Performance Object
Active Directory DXA Connector	MSExchangeADDXA
Address List	MSExchangeAL
Chat Communities	MSExchange Chat Communities
Chat Service	MSExchange Chat Service
Directory Service Access Caches	MSExchangeDSAccess Caches
Directory Service Access Contexts	MSExchangeDSAccess Contexts
Directory Service Access Processes	MSExchangeDSAccess Processes
Document Conferences	MSExchangeCONF
Document Conferencing Manager	MSExchangeDcsMgr
Document Conferencing Protocol (Multipoint Control Unit)	MSExchangeT.120
Epoxy Queues and Activity	EXIPC
Event Store	MSExchangeES
File Replication Connector	FileReplicaConn
File Replication Settings	FileRepSet
HTTP Extension	Exchange Server HTTP Extension
Internet Information Server Store Driver	Exchange Store Driver (IIS)
IMAP4	MSExchangeIMAP4
Web Storage System	MSExchangeIS
Mailbox Store	MSExchangeIS Mailbox
Public Folder Store	MSExchangeIS Public
System Information Store	MSExchangeIS

(continued)

Service or Resource	Performance Object
Lotus CC Mail	MSEExchangeCCMC
Lotus Notes Message Center	MSEExchangeNMC
Service or Resource	Performance Object
Message Transfer Agent	MSEExchangeMTA
Message Transfer Agent Connections	MSEExchangeMTA Connections
MS Mail Connector Interchange	MSEExchangeMSMI
Exchange Referral Service	MSEExchangeSA-RFR
MS Mail Connector Message Transfer Agent	MSEExchangePCMTA
Name Service Provider Interface (AD Integration)	MSEExchangeSA-NSPI Proxy
Network News Transfer Protocol Commands	NNTP Commands
Network News Transfer Protocol Server	NNTP Server
Novell Groupwise Connector	MSEExchangeGWC
Object Linking and Embedding database events	MSEExchangeOledb Events
Object Linking and Embedding database resources	MSEExchangeOledb Resources
Post Office Protocol Version 3	MSEExchangePOP3
Service Account	MSEExchangeSA
Site Replication Service	MSEExchangeSRS
Simple Mail Transfer Protocol	SMTP
Store Driver	Exchange Store Driver (Store)
Video Conferencing	MSEExchangeIPConf
Web Mail	MSEExchangeWebMail

The following sections describe the counters that are the most important to monitor, categorized by object.

**Note:** In the following sections, a number of queues are mentioned. Large queue buildup on any server usually indicates a problem, generally in routing. If you see unusually large queues for your environment, check your connector.



## Information Store Counters

### MSExchangeIS

For this object, monitor the following counters:

- ◆ User Count – This displays the number of people currently using the Information Store (not the number of connections). It is impossible to properly judge the performance of a server running Exchange unless you know how many people are using it.
- ◆ RPC Requests – This shows the number of client requests currently being processed by the store. You should expect this figure to be fairly small, typically below 25. If it is consistently higher than this, your server is overloaded.

### MSExchangeIS Mailbox and MSExchangeIS Public

For these objects, monitor the following counters:

- ◆ Send Queue Size – This shows the queue of messages outbound from the Information Store. In situations where the SMTP service is down or there is a reduction in performance, you will see a nonzero value for this queue. On large busy systems (2000 users or more) you may never see this value at zero, but on smaller ones (500 or so medium users) you would not expect to see nonzero values for any significant period of time.
- ◆ Messages Sent/Min – This shows the rate at which messages are sent to the transport. This figure being low is not a problem in itself, but if the Send Queue Size is nonzero and the value is still low compared to your baseline, then there are performance issues that need to be resolved (you will only be able to tell what these are by monitoring other Exchange 2000 Server and Windows 2000 counters)
- ◆ Received Queue Size – This shows the queue of messages inbound to the Information Store. Unlike the Send Queue size, this is often nonzero, except on a bridgehead server with no local mailboxes. However, if the value is consistently high compared to your baseline, it could indicate a problem.
- ◆ Messages Received/Min – Again a low value here could simply indicate a quiet server; however if the Receive Queue Size value is high and this value is low, it indicates that you are receiving messages that are stacking up and are not being processed.

## SMTP Server

SMTP traffic can be from SMTP Servers, such as other servers running Exchange, or it can be from POP3 or IMAP4 Clients such as Microsoft Outlook Express. When monitoring SMTP parameters, remember that your client base will affect these figures:

- ◆ Local Queue Length – This shows the number of messages in the local queue (this queue contains messages that are queued for local delivery on the server running Exchange to an Exchange mailbox). Under normal operating conditions, this number is

rarely greater than zero. A reading of greater than zero shows that the server is receiving more messages than it can process. If this number increases steadily over time, there is probably a problem with the Exchange Store you are trying to deliver to.

- ◆ **Categorizer Queue Length** – This shows the number of messages waiting for advanced address resolution. After this, the messages either go to the local queue or are sent to the routing engine to be delivered elsewhere. A high figure here compared to your baseline can indicate message flow problems.
- ◆ **Inbound Connections Current** – Shows the number of current inbound connections. If this reading remains zero over time, then there may be network problems.
- ◆ **Message Bytes Sent/Second** – Examine this figure in conjunction with other counters and your baseline to determine if your SMTP Server is passing messages as quickly as it should. If, for example, this figure is low, but queues leading to this transport are high, then there is a problem with the SMTP transport.
- ◆ **Message Bytes Received/Second** – Again, use this in conjunction with other counters and your baseline to determine overall health. For example, there may be a problem with the SMTP transport if a queue going into this transport is high while the Message Bytes Received/Second is low.
- ◆ **Avg. retries/Msg delivered** – When Exchange fails to deliver messages, those messages enter a retry queue. The SMTP server is configured with a retry interval showing how long the server will wait before a first retry, second retry, and so forth. This counter shows how many messages are going into retry as a fraction of the overall messages delivered. You should expect the figure to be close to zero. If large number of messages are being retried, the figure will approach 1. This counter is therefore a good indicator of general message delivery problems on your network.
- ◆ **Avg. retries/message sent** – This counter is the same as the previous counter, except it applies to outgoing messages as opposed to incoming ones.

### **MSExchangeMTA and MSExchangeMTAConnections**

In a pure Exchange 2000 Server environment running in native mode, the MSExchangeMTA and MSExchangeMTAConnections objects are not particularly important. However, in cases of coexistence with Exchange Server 5.5, or where messages are being relayed to and from X.400 recipients, you may want to measure the Messages/Sec and Work Queue Length of the MSExchangeMTA object and the Queue Length of the MSExchangeMTAConnections object.

In Exchange 2000 Server, you may find the Message Transfer Agent (MTA) shutting down fairly frequently, especially if it cannot find a domain controller temporarily. To resolve this problem, you may want to use the recovery actions option in services to restart the service in the event of it being stopped.

## MSExchangeIM Virtual Servers

If you are running Instant Messaging in your organization, you may find that the organization quickly becomes as reliant on Instant Messaging as it is on e-mail. It is therefore important that you monitor Instant Messaging Counters. You should examine the following:

- ◆ **Current Online Users** – This shows the number of users logged on to the server. Examining this parameter over time helps to determine the actual take up of Instant Messaging in your organization and therefore help you to scale it properly across multiple servers.
- ◆ **Current Subscriptions** – This shows the number of subscription notifications sent to the server by the Instant Messaging client. A subscription notification occurs when a user is added to the contact list. This gives an indication of how heavily clients are using Instant Messaging.
- ◆ **Inbound Subscribes/sec** – This shows the average number of subscribes/second. If this figure is low but the usage of Instant Messaging is high, it could indicate an over-worked Instant Messaging server.

## MSExchangeAL

The Recipient Update Service (RUS) plays a crucial role in the day-to-day operations of Exchange 2000 because it is responsible for keeping e-mail addresses and membership of address lists up to date. You should measure the Address List Queue Length when examining the RUS:

The Address List Queue Length shows the load the Recipient Update Service is under. If this value is consistently high compared to your baseline, you should seriously consider upgrading the server that has this role, or transferring the role from a weak or overloaded server to a more powerful one.

## Windows 2000 Objects and Counters to Monitor

A heavily used Exchange 2000 server may have a number of bottlenecks. Simply monitoring Exchange 2000 Server performance objects and counters in isolation will not give you information about the condition of the server itself. You will need to monitor for bottlenecks in the Disk Subsystem, Memory, Processor, and the Network Subsystem. For example, in many cases there will be multiple instances of disks and processors, so make sure that you monitor all instances (that is, each disk or each processor). Table 4.2 shows which objects and counters it would be most useful to monitor, along with any specific notes regarding Exchange.

---

**Note:** When monitoring disk counters, you need to enable them to start at boot, using the `diskperf -y` command.

---

**Table 4.2 Subjects and Associated Objects and Counters**

Subsystem	Object	Counter	Exchange Comments
Disk	Logical Disk	% Free Disk Space	
	Physical Disk	% Disk Time	Usually unreliable for RAID systems, so rarely applicable
	Physical Disk	Disk Reads/sec	
	Physical Disk	Disk Writes/sec	
	Physical Disk	Current Disk Queue Length	Should occasionally dip to zero
	Physical Disk	Avg secs per read	Should be analogous to published disk speed
	Physical Disk	Avg secs per write	Should be analogous to published disk speed or 1-2ms if you have write back caching enabled on your RAID controller
Memory	Memory	Committed Bytes	
	Memory	Pages/sec	Exchange 2000 makes heavy use of a pagefile. A large amount of paging is not in itself an indication of a problem.
	Memory	Page Reads/sec	Value should generally be below 100. If the value is consistently high, you may need to increase system memory.
	Memory	Page Writes/sec	Value should generally be below 100. If the value is consistently high, you may need to increase system memory.
	Paging File	% Usage	You may need to increase the size of your pagefile for Exchange. Try to keep this counter below 70%.
	Process	Page Faults/sec	

Subsystem	Object	Counter	Exchange Comments
Processor	Processor	Interrupts/sec	
	Processor	%Processor Time	The creation of indexes by Full Text Indexing generally uses a great deal of processor time. However, a low priority thread is used, so it does not necessarily cause performance issues.
	Process	%Process Time	Measure the following instances: store (Information Store), inetinfo (IIS), Isass (security system including AD), and mad (System Attendant)
Process	System	Processor Queue Length	
	System	Context Switches/sec	
Network	Network Segment	% Net Utilization	
	Redirector	Bytes Total/sec	
	Redirector	Network Errors/sec	
	Server	Bytes Total/sec	
	Server	Work Item Shortages	
	Server	Pool Paged Peak	
	Server Work Queues	Queue Length	

For more information about monitoring Windows 2000 objects, see the Windows 2000 Server Resource Kit.

## Centralized Monitoring

In an enterprise environment, you can reduce operations costs dramatically if you can capture performance data in a central location. Doing so moves the load of monitoring from the monitored server to the centralized server and also allows you to compare the performance of similarly configured servers and ensure a consistent response in the event of a problem with a server running Exchange.

An example of a centralized monitoring tool for Exchange 2000 Server is AppManager from NetIQ.

AppManager consists of four components:

- ◆ Console – A collection of programs for examining and managing your AppManager environment. It communicates with the Repository through Open Database Connectivity (ODBC).
- ◆ Repository – A SQL Server database that is the data store for AppManager. It stores configuration information for AppManager and information gleaned from the Agents
- ◆ Agent – This runs on each computer that you monitor. It sends data to and receives commands from the Management Server. It gathers information from the computer on which it runs, returning it to the Management Server. The agent communicates with the Management Server through RPC.
- ◆ Management Server – This component communicates with the Repository through ODBC, issuing commands and receiving responses from the Agents.

AppManager detects the Exchange 2000 servers in your enterprise (through registry entries), giving you the option to install an agent on each server you want to monitor. After the agents are installed, they communicate with the Management Server, sending it data about the performance of the computer on which the agent is running.

AppManager collects information about Exchange 2000 Server performance objects and counters, storing them in the repository where they can be used for long-term analysis. However, it also monitors other aspects of performance. For example, AppManager examines the amount of time taken to send and receive messages between servers running Exchange, and from servers running Exchange to the Internet. It reports on e-mail traffic flow (from message tracking logs, which it also collates). It can identify the servers (and users) that send and receive most e-mail, and monitor the amount of space used by e-mail on servers. AppManager issues notifications or alerts where necessary.

In a feature that is very useful for operations managers, AppManager tracks performance of Exchange against defined service level agreements, reporting when and how these have not been met.

Using a tool such as AppManager is not the only way to gather centralized performance monitoring information. Exchange is a Windows Management Instrumentation (WMI) provider, so it is possible to create your own Web interface for gathering information from other servers on the network.

## Event Monitoring

When Exchange 2000 Server is running smoothly, event monitoring does not seem especially important. However, when performance is poor, you will quickly see the benefits of event monitoring. Event Viewer is a useful source of information about Exchange 2000 Server, along with log files that you may choose to generate. Large organizations may require an application such as Microsoft Operations Manager for reporting on Exchange 2000 Server events.

### Event Viewer

Exchange reports to the Application event log. By default, it logs all critical events to the Application log. By increasing the logging on particular Exchange services, you can ensure that more data is available.

To enable logging for a particular Exchange service, right click the server in Exchange System Manager, select **Properties**, and then select the **Diagnostics Logging** tab.

The logging levels are:

- ◆ None – Only error messages are logged (the default setting on all the services)
- ◆ Minimum – Warning messages and error messages are logged
- ◆ Medium – Informational, warning, and error messages are logged
- ◆ Maximum – Troubleshooting (extra detail), informational, warning, and error messages are logged

You can log the following services in Exchange 2000 Server:

- ◆ IMAP4Svc (IMAP4 Protocol)
- ◆ MS-ExchangeAL (Address List)
- ◆ MSEExchangeIS\System (Information Store System)
- ◆ MSEExchangeIS\Mailbox (Information Store Mailbox)
- ◆ MSEExchangeIS\Public Folder (Information Store Public Folders)
- ◆ MSEExchangeSRS (Site Replication Service)
- ◆ MSEExchangeTransport (SMTP Routing Engine and Transport)
- ◆ MSEExchangeMTA (MTA Service)
- ◆ MSEExchangeSA (System Attendant Service)
- ◆ POP3SVC (POP3 Protocol)

Under normal operating conditions, it is not necessary to set logging levels any higher than minimum, because increasing logging rapidly fills your event log with a great deal of unnecessary information. When issues arise, you can increase the level of logging to allow you to diagnose the problem, reducing it again after the issue has been resolved.

The Windows 2000 Resource Kit includes `elogdmp.exe`, a utility which allows you to dump the information in any Event Viewer log to a file for analysis elsewhere.

One of the difficulties of viewing event logs is knowing which events are more worrisome than others. In some cases, Exchange 2000 Server issues Stop events, which record temporary issues that resolve themselves in the course of time. In other cases it records warning events, which are indicative of more substantial problems.

In general terms, the errors and warnings that are likely to cause the most problems are Store errors, because they can affect the ability to access e-mail. 1018 and 1019 errors can indicate major problems for Exchange, typically caused by faulty hardware. You should watch for these two explicitly, and for Store errors and warnings in general.

You should also be careful to watch for errors indicating that domain controllers/global catalog (GC) servers cannot be found. If a GC cannot be found, the store will automatically dismount. Similarly, if the MTA service is temporarily unable to contact a domain controller, it will shut down. Watching for these errors allows you to diagnose quickly why services are being lost in the event of a problem.

One of the main problems with event viewing in Exchange 2000 Server is the sheer volume of information Exchange produces when you increase the logging level. It is often beneficial to use filters in the Event Log to produce only warning and critical events, or to use utilities that only display the more significant events.

## Log Files

As well as logging events to Event Viewer directly, Exchange 2000 Server also produces a series of log files that can prove useful in troubleshooting problems. The Protocol Logging tool generates specific information about the commands being sent and received by SMTP and NNTP.

To enable logging for SMTP or NNTP, select the properties of the appropriate virtual server and enable logging. You can then alter the logging frequency and the name and location of the log file.

To enable logging for HTTP on the default Web site, use IIS administrative tools.

## Centralized Event Monitoring

As with performance monitoring, monitoring events centrally provides distinct benefits to many organizations. A number of tools help you to do this efficiently, including Microsoft Operations Manager, or MOM (formerly NetIQ Operations Manager) and NetIQ AppManager.

Operations Manager pulls information from a variety of locations, including event logs, WMI events, SNMP traps, and transaction logs. It consolidates these events from multiple sources to give you an overall picture of the Exchange 2000 Server environment. You can script responses to particular events, issuing notifications or taking predefined actions in response to particular events. One particularly useful feature is the ability to integrate events with a knowledge base, ensuring that useful explanations and recommended actions are issued to operators when particular events occur.



NetIQ AppManager contains useful features to help with Event monitoring. It detects whether any servers have written critical error messages to the Event Log and automates responses to actions, including issuing SNMP traps.

## Availability Monitoring

To meet your availability SLAs, you need to ensure that, as much as possible, you protect against downtime. Because it is impossible to guarantee that there will be no unexpected downtime in your organization, you need to ensure that you are notified quickly in the event of unexpected downtime.

Whenever you are monitoring and measuring Exchange 2000 Server availability, it is important to consider domain controllers as well as servers running Exchange. You may do all you can to ensure high reliability of servers running Exchange, but they will not have high availability if there are no domain controllers available for Exchange or the clients to use. Therefore you should also monitor domain controller/global catalog server availability as well as network availability.

### Monitoring and Status Tool

The monitoring and status tool is available in Exchange System Manager. This tool is used to monitor Exchange services and perform actions if the services fail. For Exchange to run as it should, a set of default services should be running. These services are:

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

If any of these services are not running, Exchange 2000 logs a critical state warning in Event Viewer.

---

**Note:** The Monitoring and Status tool does not notify you if a store has become dismantled. To ensure that you are notified of a dismantled store, you will need to use other monitoring tools such as Prospector. Prospector is available at no charge if you engage Microsoft Consulting Services (MCS). For more information about this tool, contact MCS.

---

### Adding Services to the Default Configuration

You can add additional services to the default Microsoft Exchange services that are monitored by the Monitoring and Status tool. If any of these additional services fail, they log a critical state warning, just as the default services do. This is particularly useful if you

have other Exchange services that are vital to the user experience in your environment (for example, if Instant Messaging is used heavily in your organization).

## Monitoring Resources

You can monitor other resources using the Monitoring and Status tool. To do so, click **Add** on the **Monitoring** tab and select the resources you want to monitor. These resources are monitored to see if they pass two thresholds. Resources that pass the first threshold enter a “warning” state; those that pass the second threshold enter a “critical” state. The following resources can be monitored:

- ◆ Available Virtual Memory – You can set minimum availability thresholds for memory and a minimum period of time for which available virtual memory must be above a particular threshold.
- ◆ CPU Utilization – You can set maximum CPU utilization thresholds for the CPU(s) in your server running Exchange.
- ◆ Free disk space – You can set minimum drivespace thresholds for the disk drives in your server running Exchange.
- ◆ SMTP queue growth – SMTP queues should not continue to grow. You can issue notifications if they continue to grow for longer than a specified period of time.
- ◆ X.400 queue growth – X.400 queues should not continue to grow. You can issue notifications if they continue to grow for longer than a specified period of time.
- ◆ Windows 2000 service – You can add additional Windows 2000 services to monitor. These services can be added to the default configuration just as you can add other services.

Although passing these thresholds does not necessarily affect availability directly, you will often find that your server is close to being unavailable in these circumstances, so it is very important to monitor them. A good example is free disk space. If you run out of disk space on the disk containing the transaction logs, the latest transactions will be written to res1.log and res2.log and the Exchange services will be shut down, resulting in a loss of availability.

## Notifications

When services or resources enter a warning state or a critical state, it is important that operations staff is notified, so they can react accordingly. The configuration objects in the Notification Container allow you to determine which server does the monitoring, which servers, services and resources are being monitored, at what point a notification is being sent out (at the warning state or the critical state), and what to do in the event of entering a warning state or a critical state. You can either launch a script, or send an e-mail notification.

---

**Note:** Be very careful about how you configure e-mail notifications. If you are notifying users of a failure in the e-mail service, there is a possibility that the notification may never be received.

---

## Status

The details pane of the Status container allows you to view the status of servers and connectors in your organization.

The Status container shows the following server states:

- ◆ Available – This shows that the server is online and all the main services are running normally.
- ◆ Unreachable – This shows that one of the main services on the server is down.
- ◆ In Maintenance Mode – This shows that monitoring is disabled on this server for maintenance.
- ◆ Unknown – This shows that the system attendant on the monitoring server cannot communicate with the monitored server.

When looking at connectors in the Status container, you will see the following possible states:

- ◆ Available – This shows that the connector is functioning normally.
- ◆ Unavailable – This shows that something is not functioning properly on the connector and that someone will need to investigate further.

## Disabling Server Monitoring

In some circumstances it is necessary to take a server down for scheduled maintenance, or to rebuild a server that has failed. In cases where you are already aware of the problem, you can prevent a series of alerts from being issued by choosing the properties of the server in the Status details pane and selecting **Disable all monitoring on this server**. When your maintenance is complete, you can return to this dialog box and clear the option.

## Centralized Availability Monitoring

In many environments, it is particularly important to have some sort of centralized availability monitoring if you are to meet your SLAs. Trend analysis is also very important, so you can avoid losing availability. In particular, if you monitor and find a degradation in performance over time, it may be an indicator of impending availability problems.

AppManager from NetIQ has a number of features that assist in availability monitoring. A lengthy response time in sending and receiving mail to another server running Exchange may indicate a loss of availability somewhere in the path the message would normally follow. AppManager also tells you when services are down, when queue lengths are abnormally high, or when public folders are inactive (perhaps because of a problem with replication to that folder).

Regardless of whether or not you choose to use AppManager or similar third-party tools in your organization, you should carefully consider finding a way of gathering information centrally about your Exchange environment. It is very important that information on existing or impending availability problems quickly reaches a person who can do something about it.

## Client Monitoring

While it is very important to monitor the availability and performance of servers running Exchange, domain controllers, and the network, none of these directly cover one critical area – the experience of the Exchange end user. This area can be very challenging because your clients can differ greatly. They may be HTTP, POP3, or IMAP4 clients running over an intranet or the Internet. They could be MAPI clients connecting over an internal network, or using a VPN to tunnel in. While this makes client monitoring more difficult, it also makes it more important. After all, the main reason you monitor at the server level is to ensure better performance and availability for the end users of Exchange. Without monitoring at the client level, you cannot prove that your improved server performance is reaching the client. Furthermore, in many cases, you will be required to deliver particular levels of performance at the client level. You will need to be in a position to prove that you are meeting the client expectations. Client monitoring tools give you the ability to prove that you are meeting your target levels of performance and availability.

Monitoring at the client level differs dramatically from monitoring at the server level in that you will almost certainly not want to monitor all clients. Monitoring affects the performance of the client, but more significantly, if you monitor all workstations, you will generate a significant amount of network traffic, which could affect the overall performance of Exchange. Furthermore, if a server running Exchange is unavailable, you do not need to be told this by 5000 clients. Being told by one is usually sufficient.

There are a number of third-party tools on the market for monitoring clients. These tools generally work by having an agent installed on the client, simulating typical Exchange client activities (starting up Outlook, performing an address book lookup, accessing public folders, sending e-mail, and so forth). Agents report to a central management server, which collates their information and issues reports, notifications, and alerts in the event of problems.

For more information about how to handle problems when they arise, see Chapter 6, “Support.”

Think of client monitoring not as something that examines the performance levels of each client, but rather as something that you use to verify that your server performance and availability levels are being reflected in appropriate client performance and availability. It is generally a good idea to ensure that you have at least one agent running per subnet because this will help you to identify problems at the client due to lack of network connectivity to a server running Exchange or to the domain controller/global catalog server. You should also have at least one agent running for each type of client. If, for example, the clients differ in operating system or in the Exchange client software they use, they could be affected differently, and so should be monitored separately. If you give users some freedom over the configuration of their computers, it is usually a good idea to run the agent on computers that users do not directly interact with. (It is important not to confuse a loss of service on the client due to Exchange 2000 Server issues with loss of service on the client due to user error.)

## Summary

It is impossible to operate servers running Exchange efficiently if you do not know what they are doing. It is very important to ensure that you always have enough information about your Exchange environment to predict problems and to verify that you are meeting your service level agreements. However, there is such a thing as too much information. Servers running Exchange can produce a huge amount of information, much of which is unnecessary in a healthy Exchange environment. If your monitoring is to be useful and efficient, you need to ensure that you collate useful data, have an understanding of what it means, and are prepared to increase or decrease logging levels according to what is required at that time.

When monitoring Exchange, do not restrict yourself to real-time monitoring. Use recorded data to perform trend analysis. Doing so allows you to prove that you are meeting your SLAs and alerts you to potential problems in the future.

In larger scale environments, seriously consider a centralized approach to monitoring. This helps to ensure that information about problems is available in the data centers where more expertise is available. It also allows you to compare similar servers running Exchange for performance and to get a consolidated picture of your Exchange environment.





# 5

## Protection

### Introduction

By its very nature, Exchange 2000 Server has a public face. You will be offering e-mail and other functionality to a large number of users. In many cases those users will not only be able to collaborate with other users in their own company, but also with others across the Internet. This high visibility makes it potentially more subject to attack than other services. You need to make sure that Exchange is well protected against potential attacks, including hacking attempts and viruses.


This chapter also examines disaster recovery scenarios. If you are to meet your service level agreements (SLAs) on availability, you must first ensure that your system is down as infrequently as possible. This is covered in Chapter 2, “Capacity and Availability Management,” but you must also make sure that if you do suffer downtime, it is kept to the bare minimum required to restore service. Disaster recovery procedures for Exchange 2000 are detailed in this chapter.

### Chapter Start Point

At the start of this chapter, you should be familiar with basic security concepts and different types of backup and restore hardware.

### Chapter End Point

By the end of this chapter, you should be aware of appropriate measures to take when guarding against hacker attacks and e-mail bound viruses. You will also be aware of disaster recovery procedures in the event of a failure.



## Chapter Sections

This chapter covers the following procedures:

- ◆ Protection against hacking
- ◆ Anti-virus measures
- ◆ Disaster recovery procedures
- ◆ Recovery testing
- ◆ Backup
- ◆ Restore

## Protection Against Hacking

Whenever you consider protecting your organization against malicious attack, it is worth recalling one of the golden (and most disillusioning) rules of security: the majority of attacks on a network security come from inside. The reasons for this are obvious. Security is typically more relaxed on the inside of an organization than on the outside, and employees generally have far more knowledge of the workings of a company than outsiders.

Security of an e-mail system is extremely important, because of the power associated with it. Envisage a scenario where an unhappy employee (it is possible that even your company contains some of these people) manages to gain access to their managers e-mail account. The unhappy employee then sends various e-mails posing as their manager, authorizing various decisions that adversely affect the company (and thus their managers position).

To gain access to another person's e-mail account you need to either log in as that person, or gain administrative access to Active Directory, allowing you to grant *send as* and *receive as* permissions on the mailbox. (Specifically, you require Account Operator or greater access on the user object and Exchange administrative permissions on the mailbox itself to make the changes.)

The problem with the former method of attack is that it is almost impossible for operations to spot, as the user is successfully logging in as the other party. However, there are steps you can take. In particular, you should have a method for users to report any unusual activity with their e-mail accounts, and you should teach the users how to report any such activity. Typically this would be to notify the help desk. Any reported unusual activity on e-mail should be treated as a security violation and investigated immediately.

Mailboxes that are being accessed by someone other than the primary mailbox owner are reported in the Event Log. Wherever possible, you should ensure that you are notified whenever a security descriptor on a mailbox is changed. If you are able to also maintain a list of users who should be able to access each mailbox, then you will be able to compare any changes against this list. At the very least, you should try and collect Event Log information that you can consult in the event of a security problem.



To keep your Exchange Server computers secure, look carefully at group memberships. One of the most critical groups you should monitor is the Exchange Domain Servers Group. Any user or computer account that is a member of the Exchange Domain Servers account has full control of the Exchange Organization, so it is extremely important to secure membership of this group. You should also ensure that the membership of the Built-in/Administrators group on the Exchange Server computers is also tightly locked down. Members of this group automatically have Send As permissions on all mailboxes for that server. The most efficient way to control membership of these groups is through Group Policy.

You would also be advised to audit for configuration changes to Exchange. A good change and configuration management system ensures that no changes are made to the system which have not been pre-authorized. So, regular checks of your Event Logs (or any other monitoring system you have chosen) allow you to see if unauthorized changes have been made.

Your Exchange operations department should ensure that it receives security bulletins from Microsoft. To receive these bulletins, visit the following Web site:

<http://www.microsoft.com/technet/security/notify.asp>

In cases where a security breach has been exposed and a new hot fix needs to be applied, the change should generally be considered urgent and should travel through the change configuration process accordingly.

One of the best ways of protecting against malicious use of e-mail is to use Key Management Server. This allows you to digitally sign and seal messages so that you can determine if a mail has actually come from the person who claims to send it and that the mail has not been altered in transit. Of course for this to work, the security of Key Management Server itself is paramount. Your operations practice should ensure very high security for this server, controlling very tightly who is in the local groups on the server. A password is used to start the Key Management Server and this should be kept on a floppy disk, physically separate from the server after the service has been started.

Of course, you still need to protect your Exchange Server computer against external attack. The rest of this section examines what you need to consider when you are operating one or more firewalls in your environment.

## Firewall Operations

Exchange can exist in a variety of different firewall configurations. As part of your planning and deployment you will have chosen how to deploy your firewall solutions around Exchange. Possible deployments could include a single firewall in front of servers running Exchange, to multiple firewalls in front of and behind front-end servers.

Firewall configuration is typically rather complex, so it is very important that operations personnel have a good idea as to exactly how firewalls are configured within their organization, what they should keep out and what they should let in, when they are correctly

operating. In a multi-firewall environment, the firewalls are generally manufactured by a number of different vendors, which can make management issues even more complex.

The responsibilities of the operations department in these circumstances will include the following:

- ◆ Ensuring that the firewalls continue to operate properly, implementing authorized changes, and ensuring that there no unintended effects of authorized changes
- ◆ Ensuring that firewalls only admit the traffic they are supposed to
- ◆ Monitoring to detect hacker intrusion
- ◆ Managing security breaches

### Maintaining Firewall Availability

Unless your firewall(s) are up and running properly you will be unable to exchange e-mail messages with the outside world. You should therefore place high importance on maintaining the availability of your firewalls. Monitor your firewall availability just as you would monitor the servers running Exchange and ensure that in the event of a failure, notifications are sent to the appropriate parties.

Typically when an Exchange Server computer sends messages via Simple Mail Transfer Protocol (SMTP), it actually drops the e-mail message at the firewall, which in turn forwards it to an external SMTP server. This means that, as far as Exchange is concerned, the message is delivered the moment it is sent to the firewall. So, if the firewall fails, Exchange does not detect this as a problem and reroutes messages accordingly. If a firewall is down for any period of time, you must manually alter the configuration of your environment to make sure that messages route to other firewalls (this typically involves altering the configuration of the SMTP Gateway on the affected route). Make sure that you plan for firewall failure through training, exercises, and drills so you can recover your environment quickly.

### Ensuring That Only the Correct Traffic Passes Through the Firewall

Your firewall is only secure if it remains configured as it should be over time. A typical configuration of Exchange is to use front-end servers and have them sitting on a screened subnet with one firewall in front and one behind them, protecting the back-end servers. For example, envisage a situation where you use a front-end server for Outlook Web Access, which you perform over a Secure Sockets Layer (SSL) connection. Table 5.1 shows which ports need to be let through each firewall. (This scenario does not deal with outgoing SMTP mail):

**Table 5.1 Port-to-Firewall Configuration Example**

Source	Destination	Service	Protocol and port
Internet/External	Screened Subnet	HTTPS	TCP 443
Screened Subnet	Internal/Private Network	DNS	TCP, UDP 53

Source	Destination	Service	Protocol and port
Screened Subnet	Internal/Private Network	HTTP	TCP 80
Screened Subnet	Internal/Private Network	RPC EP Mapper	TCP 135
Screened Subnet	Internal/Private Network	KERBEROS	TCP UDP 88
Screened Subnet	Internal/Private Network	LDAP	TCP 389
Screened Subnet	Internal/Private Network	NETLOGON	TCP 445
Screened Subnet	Internal/Private Network	DSAccess (GC)	TCP 3268
Screened Subnet	Internal/Private Network	TCP High Ports	TCP 1024+

You should regularly check your firewalls to ensure that the settings have not been altered to allow traffic that should not pass. The outside firewall should only be allowing traffic on port 443 specifically to the front-end servers, and only these front-end servers should be allowed to communicate with the back-end servers on the ports you have defined. You may also want to perform network monitoring to monitor the nature of the traffic that goes through the firewall.

### Monitoring Against Hacker Intrusion

No matter how good your firewall setup is, there is still a risk that a hacker may manage to infiltrate it. You should ensure that you have a good intrusion detection system in place to notify you of any firewall breach, and you should make sure that you always have the ability to shut down services if necessary.

### Dealing With Security Breaches

In the event of security breach, your priority should be to protect the system. In the majority of corporate e-mail systems, the stores will contain extremely sensitive information and should be protected. This means that, in the case of a security risk, the initial response may be to prevent access to the internal network from the outside world. Provided you manage to catch the intrusion early enough, you will still in most cases be able to allow internal mail to flow.

Once you have contained the breach, you should inform firewall vendors and/or Microsoft about the nature of the breach, so that they can come up with a fix. At this point you can revert the system to its state prior to the breach and apply the fixes supplied.

## Anti-Virus Measures

As part of your planning and deployment of Exchange 2000, you will have put in place appropriate measures against virus attack. However, regardless of how much protection you put in place, it is quite possible that viruses may affect Exchange. It is therefore very important that you have measures to deal with this possibility.

You are likely to be protecting against viruses at several levels. These may include at the firewall level, outside or at the SMTP Gateway, at each Exchange Server and at the client level. You should of course bear in mind that non e-mail bound viruses can affect Exchange, so all your servers running Exchange should be protected against viruses in the same way that clients are.

Virus scanning at the gateway means scanning each inbound message (and perhaps all outbound messages as well) to detect and clean any infected content. Several vendors provide such software. The neatest technical solution is to use an anti-virus product that integrates as an SMTP event sink. Some vendors do not integrate with the SMTP engine and require the use of the vendor's proprietary SMTP engine. These solutions can work very well, but troubleshooting an additional type of SMTP engine adds complexity to your troubleshooting procedures.

Like gateway virus scanning, a number of vendors provide Exchange Server scanning software. These products scan and disinfect content at the Exchange server and come in one of two varieties:

Scanning software based on the Anti Virus API (AVAPI V2.0). This kind of anti-virus software scans and disinfects virus-laden content before it is added to the Exchange information store.

Scanning software that uses undocumented Exchange store interfaces. These products generally work well, but there is additional support risk in using these products because they use an unsupported interface. If there is a store-related incident on a server with this product, Microsoft Product Support Services (PSS) will recommend that the anti-virus software be disabled early in troubleshooting.

Both gateway-based and information store-based scanning products should provide an automated mechanism for updating the virus scanning patterns. Having timely updates is the best way to ensure that your Exchange implementation remains free of new nasty viruses. Additionally, some scanning products offer the optional use of more than one scanning engine, further increasing the likelihood of catching a virus before it infects your systems.

As part of your operations you must ensure the following:

- ◆ The virus protection is completely up to date at all levels.
- ◆ You have defined procedures in the event of a virus infection.
- ◆ You have a mechanism for handling attachments that pose a virus risk.

## Staying Current

New viruses are constantly emerging, and they have the potential to spread worldwide within a period of hours. If you are not fully up to date in your protection, then you run a real risk of viruses infecting your organization. Your operations procedure should ensure that all areas where you scan for viruses are fully up to date. You must make sure that you receive regular security updates from your anti-virus vendors.

In some cases you will receive a warning about a new virus before an update to your anti-virus software is proposed. The first thing to do here is to verify that the virus is genuine. Many problems are in fact caused by hoax virus notifications. Ensure that the virus is a genuine problem by checking with your anti-virus vendors. After you have verified that the virus is indeed a genuine threat, you should notify users so they know what to do if they receive e-mail messages that may contain the virus. You should have a pre-defined mechanism that the user base is fully aware of as to how they should report any suspected viruses. As a short term measure for dealing with this eventuality, most anti-virus software will allow you to block messages with particular subject lines or from particular sources. This can act as a blocking mechanism until you receive an update for your anti-virus software.

### Dealing With Virus Infection

Assuming the worst does happen, and you are infected with a virus, the steps you take next are extremely important. You should of course issue an advisory to the user community, so that they know what to do if they receive the virus. You should also notify any partners that you regularly associate with, along with the anti-virus vendors themselves.

Your biggest threat in spreading viruses is the user community, who are, incidentally, your best weapon in defending against the viruses after they have attacked. It is vital that you find a way of communicating with all users, in such a way that all are likely to listen and take notice. If there is a new virus threat, you should e-mail a high-priority message to the users detailing the threat and the recommended action. Make sure that the subject line of the message prominently displays the nature of the threat. You should also advertise the problem prominently on your intranet and use any real-time notification system you have to notify the users, such as voicemail or public address systems. You should even consider having a mechanism in place for putting posters at public parts of your building, for example receptions and elevators. If the users know what to do when they receive a particular message, you can severely restrict the flow of the messages within and outside your organization.

After you have notified the relevant parties, you must do all you can to ensure that the virus does not spread. If a fix is not yet available, in a worse case scenario, this could involve restricting the flow of e-mail within your organization and outside of it (i.e. disabling connectors and possibly network connections).

As soon as a fix is available, you must have a mechanism for deploying updates from each of the virus vendors. In some cases, you may use the e-mail system as a means of distributing hot fixes to local administrators, but in this case, you must have an alternative mechanism, because it is possible that you have had to shut down e-mail communication between servers to prevent the virus from spreading.

## Blocking Attachments at the Client

One of the best ways of protecting against virus infection is to block particular attachments from running. Attachments may be blocked at the server level, but they may also be blocked at the client. You can install a security patch on Microsoft Outlook 98 and Outlook 2000. This patch is built into Outlook 2000 Service Release 2 and Outlook 2002 (a component of Microsoft Office XP). The effect of this is to prevent certain attachments from running directly from the client (instead they must be saved first) and to prevent other attachments (those considered more dangerous) from being downloaded at all.

Table 5.2 shows the attachments that are prevented from running.

**Table 5.2 File Extensions and File Types**

File Extension	File Type
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML help file
.cmd	Microsoft Windows NT command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.exe	Executable
.hlp	Help file
.hta	HTML program
.inf	Setup information
.ins	Internet naming service
.isp	Internet communication settings
.js	Javascript file
.jse	Javascript encoded script file
.lnk	Shortcut
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package

File Extension	File Type
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD image, Microsoft Visual compiled script
.pif	Shortcut to MS-DOS programs
.reg	Registration entries
.scr	Screen saver
.sct	Windows script component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBscript file
.vbe	VBscript encoded script file
.vbs	VBscript file

**Note:** Not all attachments considered to be dangerous are blocked by this patch. For example, the Microsoft Access file types .mda and .mdz are not blocked, nor are zipped versions of any of the above files.

It is good practice to quarantine all suspect content, where it can be examined individually before deciding whether it can be safely passed on or not.

While this security patch can be useful in preventing the use of unauthorized attachments, it is important to remember that for it to work across the user community, it depends on everyone using a client with the patch. Therefore, to be fully protected you would need to ensure not only that MAPI clients each contained the patch, but also prevent access via POP3, IMAP4, or HTTP.

For more information about the Outlook Security Patch, see the knowledge base article Q262631.

Many organizations prohibit the receipt of scripts written in Microsoft Visual Basic® Scripting Edition (VBScripts) through e-mail. If you choose to do this, it will not prohibit those who want to receive and run VBScripts from doing so, for they can simply ask the sender to use a different file extension and then change it back to .vbs on arrival. It will, however, prevent the running of VBScripts that have not been pre-arranged. If you wish to go further in preventing the effects of VBScripts, you will need to prevent them from running at the client at all.

Again, the best way of dealing with the threat of attachments is to educate the user community.

## Disaster Recovery Procedures

Chapter 2, “Capacity and Availability Management,” examined ways of minimizing system failures. As mentioned there, to reduce overall downtime you need to look at how frequently a system is down, alongside how long it takes to bring a system back up again. For more information on Availability Management, refer to Chapter 2.

It makes no sense to have a sound, well-exercised backup strategy unless it's matched with a similarly mature recovery strategy. Backups are meaningless if you can't restore service using them.

Exactly how you perform disaster recovery will depend on how much money you are willing to spend alongside which backup products you want to use. Third parties offer a variety of solutions, including mailbox level backup, and even message level backup in some cases. Another alternative is real-time byte level replication. You will find a list of third party vendors offering backup solutions for Exchange 2000 at the following Web site:

<http://www.microsoft.com/exchange/thirdparty/E2Ksolutions.htm#backup>

Whichever tools you use, the Operations Manager will need to ensure that the disaster recovery procedures meet the following criteria:

- ◆ Backup is performed regularly and reliably.
- ◆ Your data is protected against fire/theft/natural disaster.
- ◆ Recovery can be performed reliably and quickly.
- ◆ You regularly do test restorations on an offline server to ensure that backups are being correctly created.
- ◆ You regularly run disaster recovery drills to keep skill levels high and ensure that your recovery procedures are up to date.

### Backing Up

The rest of this section assumes that you are using Windows NT Backup as your backup and restore software. However, much of the information contained here is relevant whichever backup solution you choose to adopt.

One of the major considerations when performing a backup is how long it will take. When performing an online backup of stores on your servers running Exchange, you suspend other online maintenance activities. Therefore, to allow appropriate time for the other online maintenance activities to occur each night, you need to minimize the length of time backup takes. Also, if it takes a long time to back up these servers, it will almost certainly take a long time to restore them, and to meet your SLAs you will want to keep your recovery times to a minimum.



Your servers running Exchange will potentially consist of multiple stores and storage groups. When backing up stores online, your backup utility will ensure that the appropriate .stm, .edb and .log files are backed up. Although you can back up stores individually, you should back up storage group by storage group. Each store within a storage group is backed up in series, one immediately after the other. You therefore need to size your stores to ensure that you can back up all of the stores in a storage group within the backup window you have defined. By contrast, you can back up your storage groups in parallel, so if you do this, you will not necessarily add to the length of time your backup takes.

One of the best ways of minimizing your backup time is to back up to disk rather than to tape. You should then perform a file backup of the resulting files to an offsite location. Typically these files would be backed up to disk, and multiple copies of the disks made in separate locations. Backing up to disk also has the benefit of ensuring that your restore times are quicker if your disk backup is available at restore time.

Another way of reducing backup times is to perform incremental and/or differential backups. However, wherever possible you should not perform these, because they are likely to increase restore time, and keeping restore times to a minimum is critical in meeting SLAs.

The Operations Manager must ensure that the backups are safely stored in locations that are well protected from natural disaster, fire, and theft.

---

**Note:** Think carefully about the offsite storage location you choose. In particular, you may encounter legal difficulties if you choose to store data in another country. Some Exchange data (such as Outlook contacts) are considered private data and may be covered under data protection acts of certain countries.

---

To make sure you have full recovery of your server running Exchange, it is not enough to simply back up the stores and log files. Exchange is unusable without Active Directory, so you must ensure that Active Directory is being backed up properly, even if the backup itself is not part of your remit.

In Exchange System Manager, when you make configuration changes for a server in the Protocols container, most of those changes are written to the Microsoft Internet Information Services (IIS) metabase (some of the same information is also kept in Active Directory.) So as well as backing up Active Directory, you should also back up the IIS metabase successfully.

Back up the metabase by using the Internet Service Manager Microsoft Management Console (MMC) snap-in will simply back up the metabase.bin files. However, you will also need metabase and installation-specific security keys to allow you to start the metabase upon restore. These are backed up when you back up the system state of the server.

The metabase changes frequently during routine Exchange operations, so you should back up your metabase as often as you back up your server running Exchange. Successful backup of the metabase will prevent you from having to reconfigure settings when restoring the server.

If you are making use of the Key Management Service (KMS) functionality in Exchange to give you secure e-mail, it is absolutely vital that you successfully back up the right components. If you do not, you could end up losing mail across your entire enterprise. You will need to ensure that the following components are backed up:

- ◆ Certification Authority (CA) certificates for each of your CA servers
- ◆ The passwords protecting the CA certificates
- ◆ The KMS database itself

You will also need to ensure that the KMS database startup password is kept in a secure location.

If Exchange 2000 is co-existing with Microsoft Exchange Server 5.5, you may also want to back up the Site Replication Service (SRS). However, this is not essential, and is beyond the scope of this guide.

Finally, you must ensure that you have a complete record of the setup of each of your servers running Exchange. This will allow you to configure similar hardware specifications for similar servers. All of this information would normally be present in the Configuration Management Database. For more information about change and configuration management, see Chapter 3.

### Offline Backup

As well as an online backup of Exchange, it may be appropriate under some circumstances to take an offline backup. An offline backup is not always possible in many production environments, because taking databases offline affects whether you can meet your service level agreements. However, where they can be performed, offline backups provide a useful alternative method for restoring an Exchange server if an online backup does not work as it should.

Each Exchange 2000 store consists of an .edb file and an .stm file. With up to 20 stores, public and private, on a server, you need to back up, up to 40 files per server. When you shut down the information store correctly, all the log file information is written to the corresponding .edb and .stm databases, so you do not need to back up the log files when backing up offline.

### Disk Imaging

You may want to consider taking a disk image of the server immediately prior to installing Exchange on it. This will allow a recovery server to be built very quickly with all the appropriate settings in the event of a complete server failure.

## Restoring

To ensure a swift restore of Exchange 2000, you will need the following items:

- ◆ Available Hardware.
- ◆ Microsoft Windows 2000 Server and Exchange 2000 Server software, plus any appropriate service packs and hot fixes.
- ◆ Any other required Microsoft or third-party software.
- ◆ Full drive backups of the system drives and other logical drives where critical applications or data are installed.
- ◆ System state backups.
- ◆ Exchange database backups. Along with backups of the information store database, you may also need backups of ancillary databases such as the SRS databases and KMS databases.

There are obviously different levels of restore which you may have to perform, varying from recovering single messages to recovering the Exchange Configuration Database (in other words recovering Active Directory).

### Recovering Individual Messages

Exchange 2000 has a setting to allow deleted item retention time. By default, this is set to zero. The easiest way of allowing the recovery of individual messages is to increase this value. While there is backup software available offering individual message recovery, you may be advised to set a uniform value for mail item retention time and offer that value as your SLA on message-level retention.

### Recovering Lost Mailboxes

Exchange 2000 also has a setting to allow deleted mailbox retention time. The default for this is set at 30 days (although the policy default is set to zero). When you delete an Exchange 2000 mailbox, the mailbox contents are no longer immediately deleted from the information store database. Instead they are preserved for the time you have defined. During the time that the deleted mailbox is on the disconnected list, you can connect that mailbox to another user.

► **To connect an Exchange 2000 mailbox to another user:**

1. Start **Exchange System Manager**.
2. Locate the database that contains the disconnected mailbox, and then click the **Mailboxes** object for the database.
3. If the mailbox is not already marked as disconnected, right-click the **Mailboxes** object, and then force the Mailbox Cleanup Agent to run by clicking **Run Cleanup Agent**.
4. Right-click the disconnected mailbox, and then click **Reconnect**. A dialog box is displayed in which you can choose the new mailbox owner.

Once again, you would be advised to define your SLAs so that mailbox recovery is not possible outside the period of time you specified in the Administrator program. While mailbox recovery is possible outside of this time span, dependent upon your backup software, you may have to restore an entire Exchange database to a server in a different Windows 2000 forest to get the appropriate missing mailbox.

### Recovering Exchange Stores and Storage Groups

In this scenario, there has been a problem with the database, for example a corruption in one of the databases and you need to restore them from backup. The rest of your environment has not been affected.

Before doing anything else here, if you are recovering from tape, you should ensure that you have made copies of your existing database files. It may be that when you have recovered from tape, you discover that the tape is bad. You may be able to recover the files that you archived by using troubleshooting techniques, even though the database has a problem. If you always make sure that you never let your database drive become more than half full, then you can quickly save a copy of a database that “crashes” on the same logical drive, dramatically decreasing the time it takes to copy the files, and therefore your recovery time.

When you come to do the restore, you will need to ensure that the information store service is started, and the databases you want to restore are dismounted. You will need to select a temporary folder for the restore. This will contain restored log and patch files, alongside `restore.env`, a binary file which ensures that the log and patch files are replayed properly at the end of the restore.

Assuming you are recovering a full backup (as opposed to incremental or differential) you should ensure that you select the Last Restore Set in the backup set. This ensures that the log files and patch files are replayed after the restore, taking you more or less to the point of failure. You will not be able to mount the databases unless the last restore set option is checked, so if you forget to do this, you will either have to run the restore again, or use `Eseutil` to specify that it is the last restore set.

If you are restoring multiple storage groups simultaneously, you must specify a different temporary folder for each one. This ensures that the different `restore.envs` do not overwrite one another.

Restoring an offline backup is not generally recommended because it does not allow you to roll forward to the current status. However, it can be useful in a situation where a restore from an online backup has failed. The important thing to realize here is that the `.edb` and `.stm` files should be regarded as one and restored together in the same directory. Also, when performing the restore, you should delete all log and database files on the recovery server before copying over the new ones. The recovery server will create its own new log files when you start the services up again.

## Full Exchange Server Recovery

In any area where a server running Exchange is liable to fail, you will need hardware to perform the restore. Lack of redundant hardware can often be the most significant factor in downtime resulting from a full server failure. If you standardize your hardware for each Exchange 2000 server role, you can significantly reduce the number of standby Exchange 2000 computers required, and make recovery more of a standard procedure. In most cases the standby servers will need to be physically located at the data centers, so reducing the number of data centers can also reduce the amount of redundant hardware required to ensure fast recovery time.

Even if your Exchange Server computer suffers a catastrophic hardware failure, you should not lose the majority of its configuration information because this is stored in Active Directory and Active Directory will be available on many other servers.

You will need to ensure that you can quickly build the server to a point where you can put Exchange on to it. This means that the server will need to be running the version of Windows 2000 that Exchange was previously running on, have the same name and be a member of the same domain that the previous server was. One of the fastest ways of achieving this is to use disk imaging (as mentioned in a previous section).

After you have done this, it is not enough to simply re-install Exchange. This would fail, because the Exchange configuration information is already in Active Directory and a reinstall would try (and fail) to overwrite it. So instead, you should run setup with the /disasterrecovery switch. This switch assumes that the configuration information for Exchange is already in place and just installs the program files and registry settings. It searches Active Directory for information about the Exchange Server Object and reconfigures local settings according to what it finds.

When running the /disasterrecovery switch, it is important to ensure that you are aware of which components are installed on the system, because you need to explicitly state these when performing the recovery. This information should be in your Configuration Management database, but it will also be visible, of course, under the server object in Active Directory.

After you have recovered the Exchange Server, it will then be a matter of recovering stores (as described earlier), recovering the IIS metabase and potentially recovering the SRS, KMS, and CA databases.

## Recovering Exchange After Active Directory Failure

One of your main concerns in operations should be to ensure that this never happens. As you will have already noticed, Exchange 2000 is completely dependent on Active Directory. If you are to fully protect your Exchange environment, you should do all you can to ensure that Active Directory is as resilient as possible.

However, this does not mean that an Active Directory failure makes Exchange 2000 completely unusable. You should be able to recover an Exchange Organization, provided you have access to information about the Exchange configuration, including the Exchange storage group and store names for each server, plus a key item, known as the legacyExchangeDN attribute for each administrative group. Although this attribute is designed to allow servers running Exchange 5.5 and Exchange 2000 to communicate with one another, the attribute is used by all servers running Exchange, and the legacyExchangeDN of the server must match that of its administrative group. It is worth noting however that this procedure across an enterprise will cost a huge amount of time, pain and money and should be avoided if at all possible.

### Alternate Server Recovery

You may wish to perform alternate server recovery for a number of reasons. One of the most common is that you need to perform some sort of database maintenance and you want to check that the maintenance will not cause any problems with the database (you should note however, that unless the hardware of the alternate server is identical, you cannot guarantee that the same results will occur in the live environment). Another reason for alternate server recovery is to recover a mailbox that has expired from the Exchange Server.

Alternate server recovery is like rebuilding Exchange when you have lost Active Directory except on a much smaller scale. If you are recovering Exchange stores onto another server while the original server exists, the second server must be in a separate Windows 2000 forest. You will need to know the storage group and database names on the original server and the legacyExchangeDN of the administrative group the server belongs to.

You may end up performing alternate server recovery quite regularly. For example, you may undergo this process and then perform offline defragmentation of the database. If the offline defragmentation produces significant reduction in the database size, you could then take the production server offline to defragment it (depending on the terms of your SLA).

If alternate server recovery is a regular part of your operations routine (and it probably should be, as discussed in the next section), you should have a separate Windows 2000 forest set up permanently. This forest would contain administrative groups with all the correct legacyExchangeDNs already set up, preventing you from having to recreate it each time you did the alternate server restore.

### Recovery Testing

The key to reducing downtime during a restore procedure is to assume that system failure will happen and that you are fully prepared for it when it does. This involves having hardware, software, and backup sets available. It also involves having staff trained in restore procedures available at all times.

In training your staff, you should note that restoring to another online server while the first is online is a very difficult procedure to the majority of disaster recovery procedures, because you have to recover to a different forest under those circumstances. The best way to simulate the type of restore you may have to perform in an emergency is using a test network that is completely separate from the main network. This allows you to simulate anything from failures of stores, to total hardware failures of servers and learn what to do under those circumstances.

However, this does not mean you should not perform alternate server restores. These restores tell us other information, such as the fact that the backup software/tapes/storage procedures are working properly, and that a particular live database can be backed up and restored with no hitches. After all, there is no point in having highly trained staff to do a restore if the restores themselves will fail because of faulty tapes. You should ensure that every one of your databases has been restored to an alternate server at least once every six months.

The Operations Manager should be responsible for ensuring that the organization is fully prepared for disaster recovery. This involves regular restores being performed for each Exchange server and each backup device, by the staff who would be involved in restores when they are actively required.

## Summary

In an ideal world, Exchange would never suffer problems. However, we live in a world of very diverse hardware and software, viruses and hackers, so it is inevitable that sometimes you are going to run into difficulties with your Exchange configuration.

As you have seen here, to help you meet your SLAs it is vital to minimize the recovery time in the event of a failure. However, in some cases it is very important that you shut down services to protect the system, even though this will affect the availability measurement defined in your SLA.

To protect operations against the unforeseen it is important to factor in unusual circumstances in your service level agreements. For example you may have established that you have such resilient hardware and such efficient restore technology that you are able to achieve 99.998 percent uptime in your organization (around 10 minutes downtime across your organization per year). However, if a new virus hits your company because the anti-virus vendor hasn't informed you about it, then you may end up having to shut down Exchange services just to prevent more damage. You can deal with this eventuality in two ways. Either you can take a risk assessment on the effect of such unforeseen circumstances and reduce the SLA accordingly, or you can simply modify the SLA so it states that if the corporation is victim to an unforeseen hacker attack or virus attack and you are able to show that you used your best efforts to combat the problem, then this downtime will not count against the service level agreement.







# 6

## Support

### Introduction

The more you can do with a product, the more you can do wrong. Exchange 2000 Server is an extremely diverse and complex product. If you use Exchange to its full potential, you will be exposing more functionality to your users than ever before, thus creating more and tougher challenges for the support environment than ever before.

To offer effective support to an Exchange 2000 Server environment, you first need to define what is being supported. There are two broad categories of support:

- ◆ End user support
- ◆ Server support

In this chapter, you will learn how to create an effective support environment for dealing with both end-user issues and server problems.

### Chapter Sections

This chapter covers the following procedures:

- ◆ Service desk support
- ◆ Problem management
- ◆ Troubleshooting

At the end of this chapter you will be able to ensure that your environment provides appropriate support for users and administrators of Exchange 2000 Server.



## Providing Support for End Users

It is likely that almost everyone in your organization will be an e-mail user. All of those users may require support at some point in time. In most environments, it is critical to maintain service as much as possible to all users. A single user without e-mail may cost the organization large amounts of money and present the organization in a bad light to any outsiders who want to e-mail that user.

Your Exchange 2000 Server environment may be one of the most complicated and diverse of your IT infrastructure. You may have a wide range of different clients, including the following:

- ◆ MAPI clients (Exchange Client, Outlook 97 , Outlook 98, Outlook 2000, and Outlook 2002)
- ◆ POP3/IMAP4 clients (Outlook, Outlook Express, Netscape Communicator, Eudora, and so on)
- ◆ HTTP clients (Microsoft Internet Explorer, Netscape Communicator, and so on) for Outlook Web Access (OWA)
- ◆ Instant messaging client
- ◆ Conferencing server clients (Net Meeting and others)

End users may have a number of different uses for a client. Internet Explorer can be used for OWA or alongside Net Meeting for video conferencing. Outlook XP can be used as a MAPI client, but also as a POP3, IMAP4, or HTTP client. In many cases it will be used with custom forms, or have extra third-party functionality built into it (for example, the ability to read faxes or listen to voicemail). Not only that, but your client base may be inside or outside a firewall, on the road on laptops, accessing Exchange via dial-up lines or via the Internet. The number of combinations is enormous.

Ironically, the very complexity of the client base is actually of benefit when trying to maintain service to users. For example, users having problems with their Outlook client should still be able to send and receive mail from their computer using Internet Explorer and OWA as their client. This allows you to maintain service to the users while investigating their problem.

### Reducing End User Support Costs

The following are some reasons users could require support:

- ◆ User error
- ◆ Client software problems
- ◆ Client hardware problems
- ◆ Client connectivity problems (for example, to a server running Exchange or domain controller)
- ◆ Server software problems (servers running Exchange or domain controllers)

- ◆ Server hardware problems (servers running Exchange or domain controllers)
- ◆ Server connectivity problems (to domain controllers, other servers running Exchange or the Internet)

Educating your users is one of the key ways to reduce support costs. If users know how to use their clients efficiently and effectively, they will need to contact the Service Desk much less frequently. This results in fewer Service Desk incidents and reduced costs.

In the other areas, the main way of reducing costs is to ensure that the problems occur less frequently in the first place, and that they are resolved quickly when they do occur. This is covered in detail in the other chapters of this guide.

A best practice for reducing the cost of user support is to provide a Web site containing help information that is accessible to all messaging users. There are significant cost savings any time users can obtain the information they need without assistance from the Service Desk. The following are some examples of the type of information that might be included in the Web site:

- ◆ Assistance for creating and managing mailboxes
- ◆ How-to guides for client configuration (according to your standards) and for resolving common connectivity problems
- ◆ Answers to frequently asked questions
- ◆ Workarounds for known problems (related to the problem-management process discussed later in this chapter)
- ◆ Links to other online help information (internal or external)
- ◆ Server status and instructions for determining a user's mailbox server
- ◆ Information about current incidents that affect more than one user. This will reduce the number of calls that tend to flood Service Desks when there is a major incident. A good example is when you've disabled parts of the system to scan for and remove virus-infected messages and/or attachments.

Even in the best of environments, you will still need to resolve end-user problems on occasion. If you are going to deal with client-support issues effectively, you will need to make sure that you clearly define which clients are supported and in what configuration they are supported. Your change and configuration management strategy should include a complete record of your client base. You can use Windows 2000 Group Policy and/or Systems Management Server to ensure that workstation configuration is controlled and that the Change Management Database (CMDB) remains accurate.

---

**Note:** It is important to periodically audit the CMDB to ensure that it reflects your inventory.

---

If you are dealing with clients outside the company firewall, it is much more difficult to have tight control over the configuration. You can, however, minimize support costs by insisting that only certain clients are supported. For example, you may choose to support Outlook Express as a POP3 client, but not Eudora. You can also choose to minimize the

number of protocols supported. For example, you may choose to only support OWA as the means of access outside the firewall.

Not all of these problems are necessarily client issues. End users will be directly affected by problems at the server level. The main difference is that client issues generally affect small numbers of users, whereas server issues normally affect larger numbers of users.

Whatever the end-user support issue is, an effective support team will ensure the following:

- ◆ Problems can be reported easily
- ◆ End users are notified quickly that their problem is being investigated and are kept informed of the status of their problem
- ◆ Problems are resolved as quickly and efficiently as possible

The result of all this should be to ensure that service is restored as soon as possible in accordance with the SLA.

### Problem Reporting

Problems will typically be reported in one of two ways: as a result of your extensive monitoring (see Chapter 5), you may receive alerts that warn you of a problem; or a user may report a problem.

The sooner you can receive an accurate report of a problem from a user, the earlier you can begin to solve that problem before it becomes an issue for the organization at large.

You may want to consider using Exchange itself as the basis for your Service Desk application. You could create a custom form for Service Desk requests, which would be routed to a public folder. The Service Desk staff would examine these requests as they came in and either reroute them or deal with them. As the requests are being dealt with, further information could be added to the form. Then, when the request is resolved, this information could be routed to a second public folder and could form the basis of your internal knowledge base.

---

**Note:** There is risk to using Exchange Server as the basis for your helpdesk application, as a widespread Exchange outage will affect your ability to resolve problems.

---

Of course, you must not use the e-mail system as your only means of receiving user notification of e-mail problems! Ensure that there is a telephone support line which can be used as an alternative method of reporting problems. If you have a support-related web site, consider adding a problem reporting page.

## Dealing with User Problems

You must have a mechanism for dealing with user problems once they are reported. The first step in this process is to determine the scope of the problem. In doing so, you should consider the following:

- ◆ How many users are affected by the problem? (Does it affect a single user, all users on a server, all users in a region, and so on?)
- ◆ How critical is the problem? (Does it prevent users from using all e-mail? Can they use another client to send e-mail? Is just calendar functionality affected?)

This information will help you to prioritize the problem. For example, as a general rule, if one user cannot use Outlook e-mail (but can use other forms of e-mail clients), this would be a lower priority than if an entire region were unable to access their mailboxes. Other factors also affect the prioritizing of the problem. For example, if the CEO of a corporation is unable to access e-mail, that may be more important than the entire Milwaukee office not being able to do so.

Once the problem has been prioritized, you will need to gather more information about the nature of the problem to determine how it is dealt with. If you have an up-to-date Change and Configuration Management Database and tight control over the client base, you should be fully aware of the client configuration when a problem is reported. This is often critical in resolving Exchange issues swiftly. The Service Desk may be able to resolve the problem themselves, or they may need to escalate the problem further.

## Notifying Users

Once you are aware of a problem, it is important to make sure that the end users are informed of the continuing status of the problem.

Exactly how you do this depends on the nature of the problem. For example, if there is a problem with a server running Exchange being unavailable, using e-mail to notify users is pointless. You would generally post this kind of information on the corporate intranet. If, however, the problem is with public folders being unavailable to users on a particular server, it may be more appropriate to send an e-mail to all users affected, and then send another e-mail when the problem has been resolved.

---

**Note:** Generally you should be cautious about notifying users of problems via e-mail. E-mail notification can lead to floods of phone calls from users that would otherwise be unaffected by the issue.

---

If individual users have problems, it is generally inappropriate to post update information to the intranet. In those circumstances, you should contact the user directly. If the user's e-mail client is unavailable, call or send an instant message. However, if only one e-mail client is unavailable, you could remind your users that they can use other clients to access mail. You will then be able to use e-mail to notify them of progress with their problem.

Regardless of the scope of the problem, you will need to ensure that the initial response to the user community is quick. This ensures that they are aware that their problem is being dealt with and when they can expect a solution (even if at this stage, the time to a solution is unknown). You should define in your SLA an initial response time to Service Desk queries.

## Exchange Problem Management

While the Service Desk should resolve all reported incidents associated with known problems, the role of problem management is to determine the root cause of unresolved incidents. As problem management identifies and corrects the underlying causes of problems, it should ensure that the same problems do not occur repeatedly.

One of the most complicated things about Exchange problem management is that messaging as an IT service is dependent on a large number of non-messaging technologies. The following are some of the issues that would affect a user's ability to access e-mail.

- ◆ Slow client-to-server connectivity (causing RPC timeout problems for MAPI clients)
- ◆ No DNS server listed in client (causing problems finding servers running Exchange, Domain Controllers and Global Catalog servers)
- ◆ Global Catalog server failure (meaning no Global Address Lists are available to clients)
- ◆ Name-resolution problems on a server running Exchange (causing services to stop and databases to dismount)
- ◆ Moving of client from one location to another (resulting in the client accessing Exchange and the Global Catalog [for address book lookups] across the WAN)
- ◆ Network connectivity problems to Routing Group Master (causing the static routing table to be used instead and resulting in unpredictable routing)

In just the few examples listed above, network-connectivity problems, name-resolution issues, and failure of Global Catalog servers could all cause problems for Exchange. In many cases, the apparent Exchange problem is not an Exchange problem at all, but is caused by the failure of a related technology. The key to good problem management for Exchange 2000 Server is a good understanding of the interdependencies Exchange has, and good knowledge management in your support environment.

To help you with Exchange problem management, you should create dependency charts for a number of scenarios. Examples include the following:

- ◆ A chart for MAPI client connectivity that lists all dependencies, for example, DNS, WINS, Exchange, Active Directory, and so on
- ◆ A chart for POP and IMAP client connectivity that lists all dependencies, for example, DNS, WINS, Exchange, Active Directory, SMTP relay, and so on
- ◆ A chart for OWA client connectivity that lists all dependencies, for example, DNS, WINS, Exchange, Active Directory, FE servers, and so on
- ◆ A chart for message-delivery issues, for example, DNS, SMTP relays, Internet connection, and so on

These charts can be modular and interrelated. For example, each of the client-connectivity charts can all reference the same Active Directory chart.

Part of the problem management process is ensuring that you have good communication within and across different support departments. The closest link in terms of support should be between the Active Directory support team and the Exchange support team. Exchange configuration information is stored in Active Directory, and Exchange clients and servers both make heavy use of it. In some organizations you may choose to merge these two departments, but even if you do not, you must ensure that the Exchange team is aware of problems with access to Active Directory.

The first level of support in an organization is usually the Service Desk. Depending on your environment, the Service Desk dealing with server problems may be the same one that deals with end user problems. However, the more information the Service Desk has, the less frequently it has to refer problems to outside sources and the lower the cost of resolving the problems.

As already mentioned, you may want to use Exchange as your means of dealing with Service Desk requests. Whichever method you use, you must make sure that Service Desk issues are reported fully and that the solutions are stored in a knowledge base that is easily searchable and available to all support staff. Many problems that are reported are well-known issues. If you can ensure quick resolution of these problems, not only will those users be helped, but you will also be able to deal more quickly with other problems. This can also lower the number of problems that have to go beyond the Service Desk in the future.

If you can ensure that the knowledge base is updated in real time to reflect current incidents, problem management will be able to use it to determine the impact of a widespread problem. You may also wish to make the application available to end users online, because this can reduce the amount of direct service desk intervention.

Do not simply rely upon your own knowledge base. The Microsoft Knowledge Base (available with TechNet or on <http://support.microsoft.com>) is a very useful record of support issues that have been encountered by Microsoft. If your support staff finds problems that have already been resolved in the Microsoft knowledge base, they should ensure that a reference to the corresponding article in the Microsoft knowledge base is present in their own knowledge base.

You will also find useful information in the various newsgroups and list servers available for Exchange. While the information delivered from these sources cannot be guaranteed to be accurate, it is often provides useful tips on how to deal with issues.

Event monitoring can be a very useful source of information to Service Desk staff trying to resolve a problem. If you do encounter problems with an area of Exchange, the Service Desk staff may wish to increase the monitoring level for that area of Exchange. Individual events now have hyperlinks associated with them, to allow your Service Desk staff to find out more information about the particular event. Event monitoring is covered in more detail in Chapter 4.

Education of the Service Desk staff is very important too. If they are aware only of Exchange issues, it can be difficult for them to deal with many problems themselves, and also difficult to route problems accordingly. You should ensure that your support staff has a complete picture of Exchange and its interdependencies.

For most organizations, it is not economically sound to have all Exchange 2000 Server expertise directly employed within the company. Normally the higher levels of support are contracted out. This could be to Microsoft or a third-party solution provider. However, it is important to have these relationships already in place to ensure swift response times when required.

## Summary

Exchange 2000 Server, with its large number of interdependencies, large user base in organizations, and sheer importance to most of those organizations is a great challenge to support effectively. However, if you do provide effective support, the many improvements in the product's reliability can allow your users and support staff to gain the real benefits offered by the product.





# Glossary

## **Access Control Entry – ACE**

An object such as a user or group that is present on an Access Control List.

## **Access Control List – ACL**

A description of security permissions applied to an object, property, or resource. An ACL normally includes membership (ACEs) and the associated actions or manipulations that each member can perform on the item.

## **Active Directory**

The Windows 2000 directory service. This replaces the Security Accounts Manager (SAM) in Microsoft Windows NT version 4.0. Active Directory consists of a forest, domain(s), organization units, containers, and objects. Different classes of objects can be represented within Active Directory including users, groups, computers, printers, and applications. The use of Active Directory is governed by its schema.

## **Active Directory Connector – ADC**

The service that replicates information between the Exchange Server 5.5 directory and Active Directory. Replicated objects include mailboxes, custom recipients, distribution lists, and site configuration information. ADC uses Connection Agreements (CAs) to define individual configurations for replication. The Exchange 2000 ADC is also used to allow Exchange 5.x and Exchange 2000 servers to coexist within the same Exchange site.

Note that two versions of the ADC exist; one for Windows 2000 and one for Exchange 2000.

## **Active Directory Migration Tool – ADMT**

The Active Directory Migration Tool provides an easy, secure, and fast way to migrate from Windows NT to the Windows 2000 Server Active Directory service. You can also use ADMT to restructure your Windows 2000 Active Directory domains. This tool can help a system administrator diagnose any possible problems before starting migration operations. The task-based wizards will then allow you to migrate users, groups, and computers; set correct file permissions; and migrate Microsoft Exchange Server mailboxes. The tool's reporting feature allows you to assess the impact of the migration, both before and after move operations.

## **Active Directory Services Interfaces – ADSI**

A directory service abstraction interface that allows programming languages that are compatible with the Component Object Model (COM), such as Visual Basic, VBScript, JavaScript, C, and C++ to make common directory calls to an underlying directory service. ADSI providers include Lightweight Directory Access Protocol (LDAP), NDS, Bindery, and Windows NT (SAM). Programmers and system administrators normally use ADSI to automate or script the bulk manipulation of directory entries.

**ActiveX Data Objects – ADO**

A programming layer built on top of OLE DB that allows high-level programming languages such as Visual Basic and VBScript to access an underlying data store through a common query language. In this instance, a data store can be Active Directory, the Exchange 2000 store, or a SQL database.

**Administration group**

A collection of servers running Exchange 2000 that can be administered as a single unit. An administration group can include zero or more policies, routing groups, public folder trees, monitors, servers, conferencing services, and chat networks. When security settings (permissions) are applied to an administration group, all child objects in the DS tree inherit the same Access Control Lists (ACLs) as the administration group node. Note that an administration group does not define the routing topology for messages; this is handled by routing groups.

**ADSI Edit**

A Microsoft Management Console (MMC) snap-in used to view all objects in the directory (including schema and configuration information), modify objects, and set access control lists on objects.

**Asymmetric Cipher**

The asymmetric cipher, or public-key cipher, is a means of solving the key management problem of symmetric key encryption. This system involves using two keys, one for encryption, and the other for decryption. One of the keys is called the public key, and the other is called the private key. You can use either the public or private key for encryption, and you use the opposite key for decryption. The public key is placed in a directory, or a location available to other users, but the private key is kept in a secure location, and is available only to the owner of the key pair. By using an asymmetric cipher, the sender and recipient do not need to agree on a key before sending data.

**Block Cipher**

A block cipher uses shared-key encryption. It takes a message and breaks it into fixed length blocks, and applies the shared-key to each block. In most cases, this block size is 64 bits. The decryption operation takes the encrypted blocks, decrypts each with the same shared-key, and rebuilds the original message.

**Bridgehead**

A nominated server that acts as a message transfer point between Exchange 2000 routing groups. This term can also refer to the computer hosting a directory replication connector.

**CAST**

A variable key length encryption algorithm developed by Carlisle Adams and Stafford Tavares of Northern Telecom Research. This algorithm supports keys 40 to 128 bits long.

**Ciphers**

A cipher is a mathematical function for encrypting and decrypting data. It is performed on readable clear text data to convert it to an unreadable version called cipher text. There are four types of ciphers: symmetric, asymmetric, block, and stream

**Clear item**

A message that is not encrypted and is thus readable.

**Collaboration Data Objects 1.21 – CDO 1.21****(Also known as Active Messaging and OLE Messaging)**

An application programming interface (API) that allows users and applications to access data objects within a server running Exchange. CDO defines the concept of different object classes including messages (**IPM.Note**), posts (**IPM.Post**), and appointments (**IPM.Appointment**). Message stores and folder hierarchies can also be manipulated through CDO 1.21.

CDO 1.21 is included with Exchange Server 5.5 and its services are supplied from the CDO.DLL file

**Collaboration Data Objects (CDO) for Windows 2000**

CDO for Windows 2000 is defined in the Windows 2000 section earlier in this document.

**Collaboration Data Objects**

An Application Programming Interface that is a superset of CDO for Windows 2000. In addition to gaining programmatic access to the Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP) stacks, CDO for Exchange 2000 provides support for the creation and manipulation of message items, appointments, and contact cards.

**(CDO) for Exchange 2000**

CDO for Exchange 2000 is included with Exchange 2000 and its services are supplied from the CDOEX.DLL file.

**CDO for System Management (formerly known as Exchange Management Objects – EMO)**

An API that allows administrators to programmatically access management information on an Exchange 2000 server, including databases and mailboxes. Services are supplied out of EMO.DLL file.

**Collaboration Data Objects (CDO) for Windows 2000**

A high-level application programming interface (API) that allows applications to programmatically access Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP) protocol stacks on a computer running Windows 2000; for example, an automated mailer routine can send Web pages by e-mail which contain reports to employees. CDO for Windows 2000 is included with the Windows 2000 operating system and its services are supplied from the CDOSYS.DLL file.

#### **Conferencing Management Service – CMS**

The network service that coordinates the booking of virtual resources for online meetings in the Exchange Conference Service. Each site (not domain) normally has an active Conferencing Management Service to allow fast connection for data conferencing users.

#### **Conference Technology Provider – CTP**

A provider of data conferencing services such as real-time video, audio, and telephony integration.

#### **Configuration Connection Agreement – ConfigCA**

A special Connection Agreement implemented as part of the Active Directory Connector that replicates configuration naming context data from downlevel Exchange 5.x sites to administration groups in Active Directory and vice versa. ConfigCAs work in conjunction with the Site Replication Service.

#### **Connection Agreement – CA**

The configuration of information to be replicated using the Active Directory Connector. This configuration information includes the servers that participate in the replication, which object classes (mailbox, custom recipient, distribution list user, contact, and group) to replicate, containers and organizational units to use for object placement, and the activity time schedule.

#### **Contact**

A non-security principal that represents a user outside of the organization. A contact will generally have an e-mail address, facilitating messaging between the local organization and the remote object. A contact is similar to a custom recipient in Exchange Server 5.5.

#### **Data Encipherment Standard – (DES/Triple DES)**

An IBM symmetric encryption block cipher that uses a fixed 56-bit key. It was defined and endorsed by the U.S. government in 1977 as an official standard and is regarded as the most widely used cryptosystem in the world. A process of enciphering plain text three times with DES and three different potential series of actions. DES-EEE3 (Three DES encrypts with three different keys), DES-EDE3 (three DES operations in the sequence encipher-decipher-encipher with three different keys), or DES-EEE2 and DES-EDE2 (same as the previous formats except that the first and third operations use the same key).

#### **Distributed Authoring and Versioning – DAV (also known as HTTP-DAV and Web-DAV)**

An extension to the Hypertext Transfer Protocol 1.1 (HTTP/1.1) that allows for the manipulation (reading and writing) of objects and attributes on a Web server. Exchange 2000 natively supports WebDAV. Although not specifically designed for the purpose, DAV allows for the control of data using a filing system-like protocol. DAV commands include **Lock**, **Unlock**, **Proppind** and **Proppatch**.

**Domain controller**

A server that can authenticate users for a domain. There must be at least one domain controller in each domain within the forest. Each domain controller holds a complete replica of the domain naming context that the server is in and a complete replica of the configuration and schema naming contexts for the forest. A domain controller can be promoted and demoted through the Dcpromo utility.

**Domain mode**

An Active Directory domain can be in either *mixed mode* or *native mode*. In mixed mode, the domain is restricted to limitations (such as 40,000 objects) imposed by the Windows NT 4.0 domain model. However, Windows 2000 domain controllers and Windows NT 4.0 backup domain controllers can seamlessly co-exist within the domain without problems. Switching to native mode, which is irreversible, allows the directory to scale up to millions of objects and overcome the constraints of the earlier SAM, but requires that all domain controllers be upgraded to Windows 2000. A domain in native mode allows for rich group creation and nesting, which is advantageous to Exchange 2000.

Note that Windows NT 4.0 member servers can still exist within a native-mode domain. Additionally, clients do not have to be upgraded before the domain mode is switched.

**Domain Name Services – DNS**

A major standards-based protocol that allows clients and servers to resolve names into Internet Protocol (IP) addresses and vice versa. Windows 2000 extends this concept even further by supplying a Dynamic Domain Name System (DDNS) service that enables clients and servers to automatically register themselves in the database without needing administrators to manually define records.

**Domain tree**

A collection of domains that have a contiguous namespace, such as *microsoft.com*, *dog.microsoft.com* and *cat.microsoft.com*. Domains within the forest that do not have the same hierarchical domain name are located in a different domain tree. A *disjoint namespace* is the term used to describe the relationship between different domain trees in the forest.

**DSAccess**

The Exchange 2000 component that provides directory lookup services for components such as Simple Mail Transfer Protocol (SMTP), Message Transfer Agent (MTA), and the store. Client requests use the DSProxy service for directory access.

**DSProxy**

The Exchange 2000 component that can proxy (and refer) Messaging Application Programming Interface (MAPI) directory service requests from Outlook clients to Active Directory for Address Book lookup and name resolution.

### **Enterprise**

See *Forest*.

### **Encryption**

Encryption is the mathematical transformation of data from a readable, clear text form, into an unreadable, cipher text form. The transformation generally requires additional secret information available only to the sender and intended recipient. This information is called a key. The key allows the message to be encrypted by the sender, and decrypted only by the intended recipient using the recipient's private key. Decryption is the opposite of encryption — it transforms unreadable, cipher text data back into readable, clear text form. Using cryptography provides not only privacy, but it provides an identity every time a user logs on to a network, accesses voice mail, or uses a user name and password to access anything. This identification is called authentication. Authentication is a crucial part of network data security.

As electronic transaction use increases over networks, it is important to sign documents electronically. Cryptography provides the ability to create digital signatures, which in many cases are as legally binding as written ones.

### **Epoxy**

See *EXIPC*

### **Event sink**

A piece of code that is activated by a defined trigger, such as the reception of a new message. The code is normally written in any COM-compatible programming language such as Visual Basic, VBScript, JavaScript, C, or C++. Exchange 2000 supports the following event sinks:

- ◆ Transport
- ◆ Protocol
- ◆ Store

Event sinks on the store can be synchronous (code executes as the event is triggered) or asynchronous (code executes sometime after the event).

### **Exchange Conferencing Services – ECS**

A service that allows users to meet in virtual rooms on a server running Exchange. Exchange Conferencing Services defines the use of a Conferencing Management Service to coordinate the room bookings and a T.120 Multipoint Control Unit (MCU) for the actual connection of clients to a conferencing session.

### **Exchange Virtual Server – EVS**

When clustering, you allocate different resources (such as storage groups) to an EVS. Upon node failure, an EVS can be moved from the failed node to one of the remaining nodes.

**EXIPC (formerly known as Epoxy)**

A queuing layer that allows the Internet Information Server (IIS) and store processes (Inetinfo.exe and Store.exe) to shuttle data back and forth very quickly. This is required to achieve the best possible performance between the protocols and database services on a server running Exchange 2000. Conventional applications require the processor to switch contexts when transferring data between two processes.

Exchange Server 5.5 incorporated protocols such as Network News Transfer Protocol (NNTP), Post Office Protocol 3 (POP3), and Internet Messaging Access Protocol (IMAP) directly into the Store.exe process, so data transfer was very efficient. The Exchange 2000 architecture separates the protocols from the database for ease of management and to support future architectures.

**Extensible Storage Engine – ESE (also known as JET)**

Formerly known as Joint Engine Technologies (JET), the ESE is a method that defines a very low-level Application Programming Interface (API) to the underlying database structures in Exchange Server. Other databases, such as the Active Directory database (Ntds.dit), also use ESE. Exchange 2000 uses ESE98, whereas Exchange 5.5 and Active Directory use the older ESE97 interface.

**Event Service**

A Windows NT service that is installed by Exchange Server 5.5. This service allows programmers to write programs that use Exchange's Event Handler to process events that occur in a Public Folder or Mailbox.

**Forest (also known as enterprise)**

A collection of domains and domain trees. The implicit name of the forest is the name of the first domain installed. All domain controllers within a forest share the same configuration and schema naming contexts. To join an existing forest, the Dcpromo utility is used. The first domain within the forest cannot be removed.

**Front-end/back-end**

An Exchange 2000 configuration in which clients access a bank of protocol servers (the front-end) for collaboration information, and these in turn, communicate with the data stores on separate servers (the back-end) to retrieve the physical data. A front-end/back-end configuration allows for a scalable, single point of contact for all Exchange-related data.

**Global Catalog**

A server that holds a complete replica of the configuration and schema naming contexts for the forest, a complete replica of the domain naming context in which the server is installed, and a partial replica of all other domains in the forest. The global catalog knows about every object in the forest and has representations for them in its directory, however, it may not know about all attributes (such as job title and physical address) for objects in other domains. The attributes that are tagged for replication to the global catalog are assigned through the Active Directory Schema Manager Microsoft Management Console



(MMC) snap-in. There is only one *policy* for global catalog attribute replication in the forest. A global catalog will listen on port 3268 for LDAP queries (that are global to the forest), and port 389, which standard domain controllers use (for local domain queries). A domain controller can be made into a global catalog (and vice versa) by selecting or deselecting a check box in the Active Directory Sites and Services MMC snap-in.

#### **Group**

An object defined in Active Directory that contains members of other objects such as users, contacts, and possibly other groups. A group may be one of two types, either *distribution* or *security* depending on the requirement, and have a scope of either local, domain, or universal. This is similar to a distribution list in Exchange Server 5.5.

#### **Hash Functions**

A hash function provides a means of computing an electronic fingerprint, or checksum of a message. This electronic fingerprint is called the *hash* of a message.

Hashing secures messages and private key data by using them as elements in a mathematical function that creates a checksum of the package. The algorithm is then used on the receiving end to decrypt the message. Hashes typically compute quickly, and are designed so that every imaginable message can have a unique hash. Hash algorithms include MD-4, MD-5, and SHA-1

#### **Hosted organization (also known as virtual server, virtual machine, virtual organization)**

A collection of Exchange services including, but not limited to virtual servers (that is, instances of IMAP4, SMTP, POP3, NNTP, HTTP, RVP), storage space, and real-time collaboration facilities that exist to serve the needs of a single company. A hosted organization is normally used by Internet Service Providers to host multiple companies on the same physical computer. However, a hosted organization is not limited to a single server running Exchange 2000.

#### **HTTP-DAV**

See *Distributed Authoring and Versioning*.

#### **Installable File System – IFS**

See *Web Storage System*

#### **Instant Messaging – IM**

The Exchange 2000 service that allows for real-time messaging and collaboration between users. Clients generally use the MSN Messenger client to log on to Instant Messaging and subscribe to other users.

#### **Instant Messaging Presence Protocol – IMPP**

The standards-based protocol clients use to interact with an Instant Messaging server. IMPP is being developed by leading vendors, including Microsoft and Lotus. The Instant



Messaging service in Exchange 2000 uses a Microsoft published protocol called Rendezvous Protocol (RVP) while IMPP is being ratified

#### **Internet Messaging Access Protocol version 4 – IMAP4**

A standard-based protocol for accessing mailbox information. IMAP4 is considered to be more advanced than POP3 because it supports basic online capabilities and access to folders other than the Inbox. Exchange Server 5.x and Exchange 2000 both support IMAP4.

#### **Joint Engine Technology – JET**

Defines the low-level access to underlying database structures in Exchange Server 4.0 and 5.0. JET was superseded with the Extensible Storage Engine (ESE) in Exchange Server 5.5 and Exchange 2000.

#### **Lightweight Directory Access Protocol – LDAP**

A standards-based protocol that can be used to interact with conformant directory services. LDAP version 2.0 allows for reading the contents of a directory database, whereas LDAP version 3.0 (defined under RFC2251) allows users and applications to both read and write to a directory database. LDAP was developed by Tim Howes and the University of Michigan.

#### **Link State Algorithm – LSA**

The algorithm used to propagate routing status information between servers running Exchange 2000. Based on 'Dijkstra's algorithm', link state information is transferred between routing groups using the X-LINK2STATE command verb over Simple Mail Transfer Protocol (SMTP)SMTP and within a routing group using a Transmission Control Protocol (TCP) connection to port 691.

#### **Mail-based replication – MBR**

A mechanism to replicate directory information through a messaging transport. This term applies to Exchange 5.x inter-site directory replication, and additionally, Active Directory replication through SMTP.

#### **MD (Message Digest Algorithm, MD4, MD5)**

Developed by Rivest, this takes a message of arbitrary length and produces a 128-bit message digest. The algorithm is optimized for 32-bit machines. Description and source code for MD4 and MD5 can be found as Internet RFCs 1319 – 1321.

#### **MDB**

An instance of a database implemented in Exchange server. A single MDB is normally identified as being public or private depending on the type of data that it stores. A single server running Exchange 2000 can accommodate up to 20 active MDBs.

#### **Message Transfer Agent – MTA**

The component in all versions of Exchange Server that transfers messages between servers using the X.400 protocol.

### **Messaging Application Programming Interface – MAPI**

The API that is used by Microsoft messaging applications such as Outlook to access collaboration data. MAPI, or more specifically, MAPI Remote Procedure Calls (RPC), is also used as the transport protocol between Outlook clients and servers running Exchange.

### **Metabase**

A store that contains metadata such as that used by Internet Information Server IIS to obtain its configuration data. The metabase can be viewed through utilities such as Metaedit.

### **Metabase update service**

A component in Exchange 2000 that reads data from Active Directory and transposes it into the local IIS metabase. The metabase update service allows the administrator to make remote configuration changes to virtual servers without a permanent connection to each system.

### **Metadata**

Data about data. In relation to Exchange, this term can be used in the context of Active Directory, but can also be used to describe the structure within the store or the MTA.

### **Mixed-vintage site (also known as “PtOz”)**

An Exchange 5.x site that also contains servers running Exchange 2000.

### **Multipoint Control Unit – MCU**

A reference to the T.120 protocol that allows clients to connect to data conferencing sessions. MCUs can communicate with each other to transfer conferencing information.

### **Name Service Provider Interface – NSPI**

Part of the DSProxy process that can accept Outlook client directory requests and pass them to an address book provider.

### **Namespace**

A logical collection of resources that can be managed as a single unit. Within Active Directory, a domain defines a namespace.

### **Naming context**

A self-contained section of a directory hierarchy that has its own properties, such as replication configuration and permissions structure. Active Directory includes the domain, configuration, and schema naming contexts. Exchange Server 5.5 also uses naming contexts; Organization, Address Book Views, Site, Configuration, and Schema.

### **Network News Transfer Protocol – NNTP**

A standards-based protocol that includes simple command verbs to transfer USENET messages between clients and servers, and between servers. NNTP uses Transmission Control Protocol/Internet Protocol (TCP/IP) port 119.

**OLE DB**

An Application Programming Interface (API) that allows low-level programming languages such as C and C++ to access dissimilar data stores through a common query language. OLE DB is seen as the replacement for Open Database Connectivity (ODBC). Data stores such as those in Exchange 2000 and SQL Server allow for OLE DB access, which makes application development easier and faster.

High-level programming languages such as Visual Basic can use ActiveX Data Objects (ADO) to issue queries through OLE DB.

**Opaque item**

Message text that cannot be read without being deciphered, also known as an enciphered item.

**Outlook Web Access**

The Web browser interface to Exchange Server mailbox and public folder data. The Outlook Web Access client in Exchange Server 5.x uses Active Server Pages to render collaboration data into HTML, whereas the Outlook Web Access Client in Exchange 2000 uses native access to the store.

**Policy**

A collection of configuration settings that can be applied to objects of the same class in Active Directory. In relation to Exchange 2000, this may include mailbox thresholds and deleted item retention.

**Post Office Protocol version 3 – POP3**

A standards-based protocol for simple access to Inbox data. All versions of Exchange server except version 4.0 support POP3. POP3 uses TCP/IP port 110 for client to server access.

**Protocol farm**

A collection of virtual servers that are used as the primary connection point for users in an organization. The farm abstracts the connection protocols from the location of the back-end data, which allows users to access information without having to know its physical location.

**Public folder connection agreement – PFCA**

A connection agreement in the Active Directory Connector (ADC) that is responsible for replicating Public Folder proxy objects between the Exchange 5.5 directory and Active Directory. These objects are necessary for sending e-mails directly to the folder. Each PFCA is hard-coded to be two-way, and will replicate between the site naming context in Exchange 5.5 and the 'Microsoft Exchange System Objects' container in the Active Directory domain. It is normal to create one PFCA for each Exchange 5.5 site in the organization.

**Public folder tree (also known as public folder root and top level hierarchy – TLH)**

A collection of public folders created under the same hierarchical namespace. Previous releases of Exchange server used only a single tree (called: All Public Folders), whereas multiple trees can be defined in Exchange 2000. Each tree is a unit of hierarchy replication and can be replicated to one or more Public MDBs. A Public MDB can host only one tree. Messaging Application Programming Interface (MAPI) clients such as Outlook can only access a single tree called *All Public Folders*, whereas other clients such as a Web browser or a networking client using the Microsoft Web Storage System can access any tree that is defined.

**RC2**

a variable key-size block cipher designed by Rivest for RSA Data Security. “RC” stands for “Ron’s Code” or “Rivest’s Cipher.” It is faster than Data Encypherment Standard (DES) and is designed as a “drop-in” replacement for DES.

Because of the variable key size it can be made more secure or less secure than DES against exhaustive key search. The algorithm is confidential and proprietary to RSA Data Security.

**RC4**

A variable key-size stream cipher with byte-oriented operations designed by Rivest for RSA Data Security.

**Recipient Update Service – RUS**

This is part of the Exchange System Attendant and is responsible for keeping Address Lists up-to-date and creating proxy addresses for users.

**Remote Procedure Calls – RPC**

A reliable synchronous protocol that transfers data between clients and servers, and between servers. Outlook clients use Messaging Application Programming Interface (MAPI) RPC for accessing mailboxes and public folders, and servers running Exchange 2000 communicate with the Exchange Server 5.x Message Transfer Agent (MTA) using RPC (in a mixed-vintage organization).

**Resource**

In real-time collaboration, a user object in Active Directory that represents a facility. A resource is used by Outlook users for booking meetings and data conferences. Resources are stored in the “System \ Exchange” Organization Unit in the Active Directory.

**Resource mailbox**

A mailbox that is associated with a resource instead of a user (such as a conference room for reservation purposes). In Exchange 5.5 one user (Windows security principal) may have had several mailbox accounts associated with it – such as a receptionist with a personal mailbox and a conference room mailbox associated. In Exchange 2000, there must be a one-to-one correspondence between a Windows 2000 security principal and a mailbox. Consequently, Exchange 5.5 resource mailboxes must have a Windows 2000 security

principal (usually with no logon rights) associated with it, and a resource mailbox owner (with their own personal mailbox) is given delegated access to the resource mailbox.

### Routing group

A collection of Servers running Exchange 2000 that can transfer messaging data to one another in a single-hop without going through a bridgehead. In general, Exchange computers within a single routing group have high-bandwidth, resilient network links between each other.

Additionally, a routing group defines the boundary for public folder access.

### Routing Group Connector – RGC

A connector in Exchange 2000 that connects routing groups to one another. An RGC is uni-directional and can have separate configuration properties (such as allowable message types over the connection). Routing Group Connectors use the concept of local and remote bridgeheads to dictate which servers in the routing groups can communicate over the link. The underlying message transport for an RGC is either Simple Mail Transfer Protocol (SMTP) or Remote Procedure Calls (RPC) and it uses link state information to route messages efficiently.

### Routing Engine

This COM component runs on the Event Service on Microsoft Exchange Server version 5.5. It acts as a simple state engine that executes and tracks multiple process instances within a Microsoft Exchange folder. The state is advanced when events fire within the folder. The routing engine supports the execution of flow-control activities (workflow) directly, and it can call VBScript functions for other activities. Microsoft Exchange Server Routing also works with the Microsoft Transaction Server (MTS)

### Routing service

A component in Exchange 2000 that builds link state information.

### Routing Objects

Component Object Model (COM) objects that are used to program Exchange's routing engine behavior. These objects allow the creation and manipulation of *process maps*, which define the series of states to be tracked by the routing engine and the activities to be performed at each step. Routing objects are used primarily in workflow applications.

### Rendezvous Protocol (RVP)

**(Note that this name is preliminary).** The Microsoft published protocol that is used between the MSN Messenger service and the Instant Messaging server that is implemented on Exchange 2000. RVP uses an extended subset of HTTP-DAV with an Extensible Markup Language (XML) payload to send subscriptions and notifications between Instant Messaging clients and servers.

### **SASL**

Simple Authentication and Security Layer. Defined in RFC2222.

### **Schema**

The metadata (data about data) that describes the use of objects within a given structure. In Active Directory, the schema governs the type of objects that can exist and the mandatory and optional attributes of each object. Windows 2000 Active Directory has an extensible schema that allows third parties to create their own object classes.

Schemas also exist for other components such as the message transfer agent (MTA) and information store in Exchange Server.

### **Secure Hash Algorithm version 1**

Published in 1994 as a federal information-processing standard (FIPS PUB 180), this was developed by the National Institute of Standards and Technology (NIST). Similar to the MD4 family of hash functions, this takes a message of less than 264 bits and produces a 160-bit message digest. It is slightly slower than MD5 but is more secure against brute-force collision and inversion attacks.

### **Security principal**

A user who can log on to a domain and have access to network resources. In Active Directory, a user object is a security principal.

A non-security principal is an object represented in Active Directory that cannot access resources within the enterprise.

### **Simple Message Transfer Protocol – SMTP**

A major standards-based protocol that allows for the transfer of messages between different messaging servers. SMTP is defined under RFC821 and uses simple command verbs to facilitate message transport over TCP/IP port 25.

### **Site**

A collection of IP subnets. All computers that are in the same site have high-speed connectivity—local area network (LAN) speeds—with one another. Unlike an Exchange site, an Active Directory site does not include a unit of namespace; for example, multiple sites may exist within a single domain, and conversely, a single site may span multiple domains.

### **Scripting Agent**

Exchange Server Scripting Agent lets you use server-side scripts that run as a result of events occurring in Exchange folders. There are four events that can trigger the scripting agent, timer events and actions: posting, editing, receiving or deleting a message.

### **Sink**

See *Event Sink*.

**Site Consistency Checker – SCC (also known as the SKCC)**

The updated version of the Exchange Server 5.5 Knowledge Consistency Checker (KCC) that works in conjunction with (and is part of) the Exchange Site Replication Service to ensure that knowledge consistency of sites, administration groups and Active Directory domains is maintained when interoperating between Exchange 2000 and Exchange 5.5. When changes are detected in either environment, the SCC may adjust existing configuration connection agreements.

**Site Replication Service – SRS**

A directory service (similar to the directory used in Exchange Server 5.5) implemented in Exchange 2000 to allow the integration with downstream Exchange 5.x sites using both Remote Procedure Calls (RPC) and mail-based replication. The SRS works in conjunction with the Active Directory Connector to provide replication services from Active Directory to the Exchange 5.x Directory Service.

**Storage group**

A collection of Exchange databases on a server running Exchange 2000 that share the same Extensible Storage Engine (ESE) instance and transaction log. Individual databases within a storage group can be mounted and dismounted. Each server running Exchange 2000 can architecturally host up to 16 storage groups, although only four can be defined through the Exchange System Manager.

**SSL**

Secure Sockets Layer version 3.0 is defined in the Internet draft [<draft-ietf-tls-ssl-version3-00.txt>](#).

**Store**

The generic name given to the storage subsystem on a server running Exchange. This term is used interchangeably to describe the Store.exe process and Exchange databases.

**Stream Cipher**

A stream cipher is another use of symmetric encryption. Stream ciphers process small units of plaintext, usually bits. Stream ciphers are much faster than block ciphers, and can be applied to data as it is sent or received. You do not need to know the size of the message, or receive the entire message before beginning to decrypt the message. This is useful for encrypted conversations over a network such as SSL rather than individually-encrypted messages.

**Symmetric Cipher**

Symmetric, or shared-key, ciphers are a form of data encryption in which a single key, known by the sender and the recipient, is used to encrypt and decrypt a message. While this form of encryption is efficient and effective, it is often difficult to share the key between both parties in a secure manner. It requires that the sender communicate the key to the recipient in a secure way.

### **System attendant**

One of the core Exchange 2000 services that performs miscellaneous functions (usually related to directory information) such as generation of address lists, offline Address Books, and directory lookup facilities.

### **T.120**

A standards-based protocol used with Exchange Data Conferencing. Clients such as Microsoft NetMeeting are T.120 compatible.

### **User**

In Active Directory, this is a security principal (a user who can log on to the domain). A user may have an e-mail address and/or an Exchange mailbox, making the object mail-enabled and/or mailbox-enabled, respectively.

### **User Principal Name – UPN**

A multi-valued attribute of each user object that the system administrator can set. A UPN allows the underlying domain structure and complexity to be hidden from users; for example, although 50 domains may exist within a forest, users would seamlessly log on as if they were in the same domain. For consistency purposes, system administrators can make the UPN and users' SMTP address the same.

A user can log on to Active Directory through a number of different methods:

- ◆ By specifying the user name and domain name
- ◆ By using the convention of *username@domain-name* in the user box
- ◆ By using his or her UPN, such as *e-mailalias@microsoft.com*

### **Virtual root**

A shortcut pointer to a physical storage location. Virtual roots are normally defined to allow users and applications to connect with a short "friendly" path instead of navigating a complex hierarchy.

Internet Information Server (IIS) uses the concept of virtual roots to expose resources provided by a web server.

### **Virtual server**

An instance of any service type normally implemented in Internet Information Server (IIS). For example, a virtual server can be an instance of:

- ◆ FTP
- ◆ IMAP
- ◆ Instant Messaging (RVP)
- ◆ HTTP
- ◆ NNTP
- ◆ POP
- ◆ SMTP



**Web-DAV**

See *Distributed Authoring and Versioning*.

**Web Storage System**

The database architecture in Exchange 2000. Previous releases of Exchange only exposed data such as public folders through MAPI, whereas Exchange 2000 exposes all of its data through MAPI, HTTP, OLE DB and Win32 layers.

This means that an object stored in a public folder can be retrieved and manipulated through a Web browser or a standard client with a network redirector. The Exchange 2000 store exposes itself to the operating system as an installable filing system, which means that the underlying data can be accessed through a drive letter, and in turn, this drive and its folders can be shared via a universal naming convention (UNC) path to allow other clients to connect to the data.

**X.509**

A standard released by the International Telecommunications Union that specifies the formatting of a mechanism to verify public keys issued to security principals in an organization.

