Microsoft Exchange Server

Microsoft Exchange 2000 ASP Deployment Guide

White Paper

Published: June 2000

Contents

Microsoft Exchange 2000 ASP Deployment Guide

White Paper

Published: June 2000

For the latest information, please see http://www.microsoft.com/exchange/

Introduction

Microsoft® Exchange 2000 Server gives Application Service Providers (ASPs) a solid foundation on which to develop rich messaging and collaboration applications and services that run on a Windows® 2000 Server network. Together, Windows 2000 Server and Exchange 2000 Server provide a robust and cost-effective infrastructure that you can use to develop, deliver, and manage messaging and collaboration services such as e-mail, news, chat, Instant Messaging, and real-time multimedia conferencing, in addition to workflow, line-of-business, and collaboration applications.

This guide is part of Microsoft's initiative to develop ASP-enabled products and architectures. Microsoft is dedicated to meeting your company's requirements for availability, scalability, and reliability.

This document provides you with background information about the Windows 2000 Active Directory™ service and Exchange 2000 Server, discusses key issues to consider when planning your Exchange deployment, walks you through the process of setting up Exchange 2000 Release Candidate 1 (RC1) in a shared hosting environment, and provides information on how to use Network Load Balancing Service (NLBS) and Microsoft Cluster Services to configure your network for scalability, high availability, and reliability.

Note This paper does not cover redundancy. It's crucial that you build in mechanisms for fault tolerance and develop strategies for backup and recovery before going into production.

This paper assumes you are familiar with fundamental Windows 2000 networking and hosting concepts. To get the most out of this paper, you should have a basic knowledge of the following:

- Installing and managing Windows 2000 Advanced Server components such as Domain Name Service (DNS), IP, Internet Information Services (IIS), Active Directory, and so on.
- Using Active Directory policy administration tools for users, groups, domains, and sites.
- Data center design concepts, including firewalls, routers, Internet naming conventions, and protocol such as HTTP, IP, Domain Name System (DNS), Simple Mail Transport Protocol (SMTP), Post Office Protocol version 3 (POP3), Network News Transfer Protocol (NNTP), Internet Message Access Protocol version 4 (IMAP4), MAPI.

To provide feedback on this document and other ASP hosting documentation, please send e-mail to Asptech@microsoft.com. New information, document

revisions, and updates will be posted on http://www.microsoft.com/isn/asphosting/. For the latest information on Exchange Server, including release candidates to download, see http://www.microsoft.com/exchange/.

Recommended Reading and Resources

Before you proceed to the installation section, we recommend that you review the Windows 2000 Server and Exchange 2000 Server documentation and that you have those documents handy when you set up your system.

In addition, you should familiarize yourself with the following:

- Windows 2000 Resource Kit components, utilities, and documentation
- Exchange 2000 Server release notes and documentation
- Active Directory and Exchange 2000 Server white papers and deployment guides, which are available at http://www.microsoft.com/exchange/prodinfo/2000/0WA2000.htm and http://www.microsoft.com/WINDOWS2000/library/planning/
- Exchange 2000 ASP Hosting white paper,available at http://www.microsoft.com/ISN/whitepapers/exchange_2K_hosting_paper.asp
- Network Load Balancing Service (NLBS) documentation
- Directory Services Operations Reference for network operators, available at ftp://ftp.microsoft.com/services/isn/svcs/ds
- Windows 2000 Server Deployment Planning Guide, available at http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp

Overview of Exchange 2000 Server and Windows 2000 Server

This section provides an overview of Exchange 2000 Server, Windows 2000 Server, and Active Directory features.

Exchange 2000 Server

Exchange 2000 Server is Microsoft's next-generation platform for messaging and collaboration services, providing tight integration with Active Directory, Internet Information Services (IIS), Cluster Services, and Network Load Balancing Service (NLBS). Exchange addresses legacy interoperability and management needs through integration with Active Directory and support for protocols that are compliant with Request for Comments (RFC). Exchange offers the following features:

- **Real-time multimedia conferencing**. Exchange 2000 Server provides H.323- and T.120-compliant multimedia conferencing capabilities, which combine data, voice, chat, and video. Users can schedule meetings and book resources from Outlook® and connect to Exchange with Microsoft NetMeeting® conferencing software for person-to-person videoconferencing. Exchange Conferencing Service uses the concept of virtual conference rooms that are created on the computer running Exchange.
- **Universal Inbox**. Exchange 2000 Server supports multimedia (MIME) content types for voice, text, and video integration. A universal Inbox provides a single point of access that can hold messages in multiple message formats.
- **Outlook Web Access**. Outlook Web Access provides the basic messaging functions of Exchange 2000 Server through a browser-based interface. IIS hosts virtual roots and processing to facilitate browser-based access to the computer running Exchange.

Messaging Client and Protocol Support

Microsoft provides best-of-breed client applications with Outlook 2000, Outlook Express and Internet Explorer 5.0 (for Outlook Web Access), all of which you can use with Exchange 2000 Server.

- Internet Explorer 5.0 provides integrated Web browsing and Outlook Web Access to Exchange 5.*x* Server and Exchange 2000 Server through HTTPMail and Web distributed authoring and versioning (WebDAV).
- Outlook Express is a standard SMTP, POP3, HTTP, and NNTP mail and news client included free with Internet Explorer 5.0.
- Microsoft Outlook 2000, part of the Microsoft Office productivity suite, provides rich scheduling, messaging, and collaboration services.

Exchange 2000 Server provides rich out-of-the-box support for Internet-standard protocols such as POP3, SMTP, IMAP4, MAPI, NNTP, HTTP, and HTTPMail/WebDAV, and includes a new and improved version of SMTP. You can configure custom settings for each company that you host, allowing you to run custom applications for specific customers.

Note Outlook 2000 connections require remote procedure call (RPC) and MAPI protocol connections unless Outlook is running in Internet Mail Only mode. For information on running Outlook in Internet Mail Only mode, see the documentation provided with Outlook 2000.

Windows 2000 Server

The Windows 2000 Server family builds on the strengths of Windows NT® technology, integrating standards-based directory, Web, application, communication, file, and print services with high reliability, efficient management, and support for the latest advances in networking hardware. Windows 2000 Server provides the best foundation for integrating your business with the Internet. When combined with Exchange, Windows 2000 provides the following system services and components:

- **Active Directory**—provides group policy and security management through the Active Directory Users and Computers management console. The following section provides an overview of how to configure Active Directory.
- **Cluster Services**—provides stateful back-end clustering technologies to improve redundancy, reliability, scalability, and availability. For more information see http://www.microsoft.com/windows2000/guide/server/features/clustering.asp
- **Network Load Balancing Service (NLBS)**—clusters a group of computers together that run server programs on TCP/IP. NLBS distributes traffic across stateless IP front-end servers and is ideal for TCP/IP-based protocols such as HTTP, FTP, and SMTP.
- **SMTP**—the default transport for mail traffic between servers. Exchange extends this service with basic commands for routing, queuing, ATRN, ETRN, and other enhancements. SMTP is installed during Windows 2000 setup or through Internet Information Services (IIS) 5.0 setup from Control Panel.
- **NNTP**—provides standards-based news server (push/pull) feeds for Exchange. NNTP is installed during Windows 2000 setup or from the Control Panel during IIS setup.

Active Directory and Exchange 2000 Server

This section provides an overview of how Exchange 2000 Server and Active Directory work together to allow you to manage your network and administer security from a single, centralized location.

Active Directory is the directory service for both Windows 2000 Server and Exchange 2000 Server. It stores information about resources, users, groups, and objects on the network and makes this information easy for administrators and users to find, provision, and manage. The directory presents a logical view of information on the network, organized hierarchically as trees. If you're deploying Exchange 2000, Active Directory is probably the most important underlying Windows service with which to familiarize yourself.

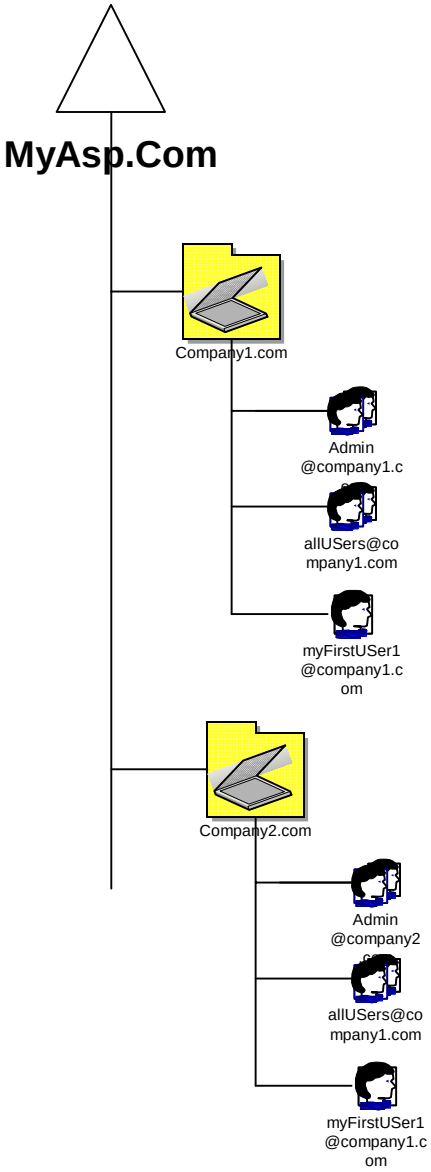
Exchange 2000 uses Active Directory for object browsing, security, and name resolution in addition to group policy, address book lookups, user authentication, and the mailbox stores and information in the directory. Active Directory also provides a centralized administration point from which you can provision security policies for Exchange. Because of this centralized design, you can delegate administration separately for each company that you host.

Exchange stores Global Address Lists, Access Control Lists, Offline Address Lists, Recipient Policies, and Exchange e-mail rules that map to Active Directory users and groups.

Organizational Units

Many ASPs want to host applications from a single point of operation, such as an existing data center. From there, you can deploy scalable offerings over time using your existing infrastructure. Such a design is based on a single, replicated root directory, called a *forest*. You can partition the root to host multiple customers. For redundancy, it is important to configure two servers as Windows domain controllers.

In a shared hosting scenario, you host each of your customers within an organizational unit. An organizational unit defines an area, or container, within the directory where you place users, groups, computers, and other organizational units. Within an organizational unit, you can nest other organizational units that represent groups, divisions, and teams within the company you are hosting. For example, in an organizational unit called *Customer1*, you might nest a secondary organizational unit called *marketing* and another called *sales*. The following illustration shows the topology for such a deployment.



By designing the directory around a single root domain (such as AspHosting.com) and creating organizational units for each customer (such as customer1), management and administration is simplified. You also benefit by maintaining only one namespace (a single Active Directory orest) and retaining ownership of all data center services, including Exchange. A section later in this paperdescribes setting up a sample organizational unit and assigning security properties to an administrator group for that organizational unit.

User Principal Names

The user principle name (UPN) feature of Active Directory provides logon names in a format similar to e-mail names. A UPN consists of two parts: a user identification portion and a domain portion, which are separated by the “at” symbol (@) to form <user>@<UPN suffix>. Every user is automatically assigned a default UPN, in which the <user> portion of the name is the same as the user’s logon name, and the <UPN suffix> portion of the name can be the organizational unit name in which the user account is located. When logging on using a UPN,

users no longer have to choose a domain from a list in the logon dialog box. Here is an example of a UPN:

Alison@aspDomain.com.

You can set UPNs to arbitrary values. For example, even if Alison's account is located in aspDomain.com, you can set her UPN to Alison@Customer1, an organizational unit within the domain *aspDomain.com*. When Allison logs on, her Windows user account is found by searching the global catalog for a user account with the same UPN value. By making UPN values independent from domain names, you can move user accounts between domains while leaving UPN values unchanged, making the move transparent to your users.

You can also define UPNs for users of Windows NT®. For these users, the logon name is the same as the UPN prefix. For additional information about UPNs, please see the Windows 2000 online documentation.

The "Configuring Organizational Units, Users, and Groups" section of this guide describes setting up a sample UPN in Active Directory.

Directory Security

You should consider security when you design your system and throughout its deployment. Security is integrated with Active Directory only as far as you apply it through logon authentication mechanisms, Access Control Lists, and Access Control Entries. Delegating administrative authority separately for each organizational unit eliminates the need for several administrators to have sweeping administrative authority because each organizational unit can have a different administrator.

Active Directory security permissions are hierarchical, inherited from highest container to lowest object. This gives domain-level administrators the ability to delegate authority to local security groups you can create for each organizational unit. Global-level administration defines authority for the domain, including organizational units.

Directory security is different from file-level security. Directory security restricts what a set of users can *see* in the directory, whereas file-level security blocks them from *accessing* certain information. If you secure your directory system correctly, one company cannot view the information of another company; for example, you can restrict addressbBook lookups to a specific organizational unit and, therefore, to a specific company. Using directory security, you can delegate security for each company, or organizational unit, separately.

Global Catalog

A global catalog is automatically created when you set up Active Directory on the *first* domain controller in the forest. In Exchange 2000, the global catalog contains the Global Address List, an address book of all the users in a hosted company.

The global catalog also stores a full replica of selected attributes for the Windows 2000 or Windows NT domain to which the global catalog belongs; the global catalog stores a *partial* replica of objects contained in other domain partitions. The global catalog performs two key directory roles:

- It enables network logon by providing universal group membership information to a domain controller when a user initiates a logon process.

- It enables users to find directory information regardless of which domain in the forest actually contains the data.

When a user logs on to the network, the global catalog provides universal group membership information for the account sending the logon request to the domain controller. If there is only one domain in the forest, each domain controller acts as a global catalog for all outbound queries. For example, if a user requests to be connected to a global catalog during an ldap_bind(…), the user will be connected only to a domain controller that you have specifically configured to be a global catalog server. If multiple domains exist in the forest, you must explicitly configure a domain controller to act as a global catalog server. If a global catalog server is not available when a user initiates a network logon process, the user can log on to only the local computer.

Note Members of the *Domain Admins* group can log on to the network even if no global catalog is available.

The global catalog is designed to respond to user and programmatic queries for objects anywhere in the forest with maximum speed and minimum network traffic. Because a global catalog contains information about objects in all domains in the forest, a query about an object can be resolved by a global catalog in the domain in which the query is initiated. Thus, finding information in the directory does not produce unnecessary query traffic across domain boundaries.

You can optionally configure any domain controller to host a global catalog, based on an organization's requirements for servicing logon requests and search queries. In the sample network we'll set up later in this guide, each customer site will be bound to connect to its partition in the namespace—its organizational unit—to receive group and user policies for e-mail and other Exchange-based collaboration programs.

Planning Your Exchange Deployment

This section describes the planning process and outlines key issues you need to consider when designing your Exchange deployment.

Once you've installed Windows and Exchange 2000 and familiarized yourself with the products and resource kit materials, take some time to think about the following project stages:

- **Envision**—Define the goals and limitations of the project, envision its scope, and create requirements based on the services you intend to offer your customers. Develop a conceptual design and assess high-level project risks.
- **Plan**—Write functional specifications and a project plan, gather information about current Web services, define and design your service offerings, and draft a project schedule.
- **Develop**—Develop, test, and build a prototype system; validate the physical design of the system by simulating a production environment. Perform unit, integration, and application testing. Build out systems, configure the production servers you will use in your data center. Conduct pilot testing and introduce your services to a narrow set of users. Train your administrators and key users.
- **Deploy**—Make your services available to end users. Evaluate performance and correct problems. Monitor your systems while you plan improvements and enhancements. Finish training administrators and users.

Configuring Hardware

Deciding how and where to deploy and partition Active Directory is a major design decision you'll need to make early in your design process. When planning a centralized model, it's important to understand how to partition and scale your data center *before* you deploy Exchange.

You should create a modular, scalable foundation that allows you to add physical resources as needed. There are some fundamental processes to take into account, covered in a set of design guidelines called the Microsoft Solutions Framework (http://www.microsoft.com/msf/).

It's important to provide fast drive access and a fault-tolerant hardware configuration. Providing multiple logical drives or drive arrays to partition the components improves performance. Depending on the level of reliability you need, you may want to use the different RAID technologies to find the most reliable configuration, for example, RAID 0+1.

You can partition Exchange and Windows on separate drives to avoid I/O resource conflicts and improve performance. Your drives must be large enough to accommodate the heavy paging processes that Information Store requires. And by archiving transaction logs on yet another logical drive partition, you increase reliability and recovery time in case a transaction or Exchange partition becomes corrupted or if the drive physically breaks.

Here is an example of how you can partition your drives:

- Logical Drive (1)—Windows 2000 Server
- Logical Drive (2)—Exchange 2000 Server
- Logical Drive (3)—transaction logs

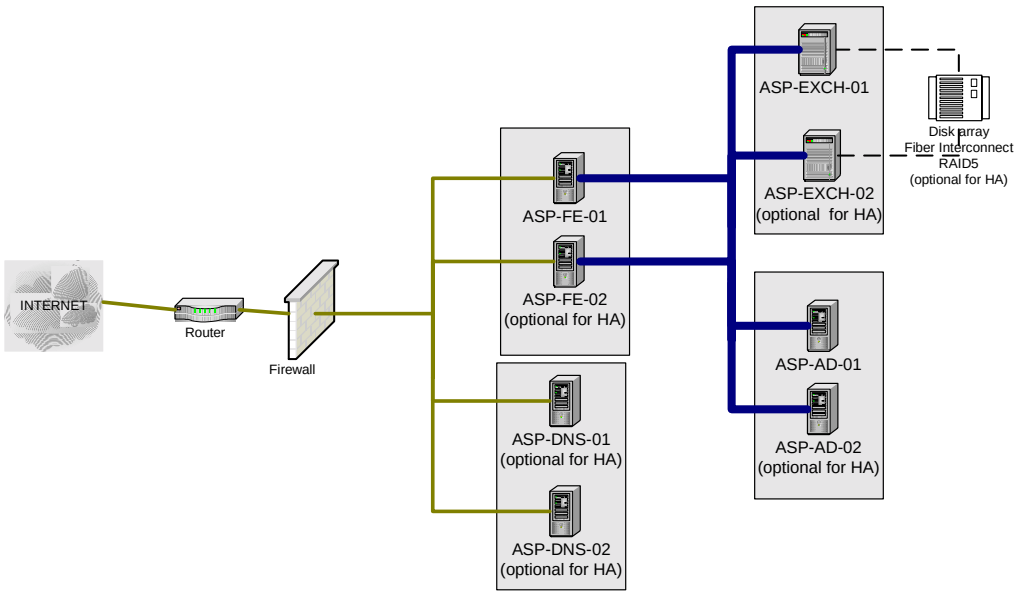
Planning a Front-End and Back-End Configuration

The front-end, outward-facing network provides communication with and connectivity to the Internet. All client requests are transferred to and from the front-end servers. In general, these are collections of stateless protocol servers used to route, or *proxy*, requests to the back-end servers. You can tier front-end servers with a load-balancing solution such as Network Load Balancing Service (NLBS), which is included with Windows 2000 Advanced Server. In a front-end and back-end configuration, the front-end servers must use remote procedure calls (RPCs) to communicate with the back-end server running Active Directory; the front-end servers must register for notifications from Active Directory and use RPCs to do so.

In general, back-end systems require:

- More capacity controls on faster computers.
- A private addressing scheme bound to a second network interface card (NIC).
- Microsoft Cluster Services. (For more information, see “Setting up Microsoft Cluster Services” later in this paper.)

The back-end server running Active Directory handles internal DNS name resolution, and the back-end server running Exchange holds user mailboxes, directory schemas, and file stores. With Outlook 2000 and some other mail clients, it’s important that you maintain these systems on high-performance computers and high-capacity networks.



Planning Capacity

When estimating the capacity your system will need, consider the following questions:

- What's the typical user mailbox size in megabytes, and how many transactions are recorded per minute?
- What's the typical user public folder size in megabytes, and how many transactions are recorded per minute?
- What Internet protocols are running and on what computers?
- What other applications are running on your Exchange store system and what resources are they consuming?
- What are the workflow profiles and applications of your user base?
- How long will the user be connected?
- How many times will users be authenticated?
- What client application will the user use?

Setting Up a Sample Network

This section walks you through setting up a sample configuration. By doing so, you will be able to test and deploy a preliminary shared hosting architecture. This scenario is based on a three-server configuration that includes a front-end server, Active Directory, and a back-end server; you can configure a fourth server for administration, but this is optional. After setting up your network, you will test three client access scenarios—Outlook Web Access (Internet Explorer 5.0), Outlook Express 5.0, and Outlook 2000. Finally, you will configure your system for high availability and reliability by installing NLBS and Windows Cluster Services and configuring storage.

For testing purposes only, you may want to start by setting up a single server running Windows 2000 Advanced Server, Active Directory, and Exchange 2000 Server. This is by far the fastest way to familiarize yourself with Exchange 2000 Server.

Network Configuration

The physical network is divided into public and private interfaces. Each computer on the public, front-end network runs NLBS. All front-end computers should have two NICs. The back-end server running Exchange and the server running Active Directory require only one NIC each. For each of the front-end computers, the NIC facing the Internet must contain a valid IP address (for example, 208.229.x/24) and a *virtual* IP address for NLBS. The aft-facing NIC will contain a non-routable IP address (that is, those in the 10.0.0.x/24 range). It is recommended that you place two NICS on the private, back-end computer.

System Requirements

This section lists the software and hardware you need to set up your sample network.

To set up the sample deployment this paper describes, you need the following software:

- Windows 2000 Advanced Server compact disc
- Microsoft Exchange 2000 Server RC1 compact disc

You also need the following hardware:

- Three Pentium III 400 Megahertz single-processor computers with 256 MB of RAM or more and 4 GB disk space
- Two NICs for each server

Naming Conventions

You'll set up your servers in a fictitious domain called *aspDomain.com*. The fully qualified *internal* domain name for each server is <yourcomputername>.AspHosting.com, in which *computername* is one of the following:

- ASP-FE-01—the front-end protocol server

- ASP-AD-01—Active Directory
- ASP-Exch-01—the back-end Exchange server

The following table shows the name and function of each server and provides sample IP addresses.

Internal Names	Services, Protocols	Private IP	Public IP	Virtual IP
ASP-FE-01	POP3, IMAP4, SMTP, HTTP	10.0.0.1	192.168.01.1	192.168.01.101
ASP-AD-01	Active Directory, Global Catalog	10.0.0.5		
ASP-Exch-01	Exchange 2000	10.0.0.6		10.0.0.10

During setup, you'll need to refer to this table, so you may want to print this page for easy reference.

After you set up your servers, you'll provision the directory for a fictitious company called *Customer1*. If you choose, you can add another company called *Customer2*.

To make administration easier, you'll create the following Active Directory groups:

- *allUsers@Customer1*. This group will contain all users that belong to Customer1.com.
- *admins@customer1*. This is an administrator group that you will use to delegate administration to hosted companies in the Customer1 organizational unit; set security policy for administrators of the domain Customer1; and create distribution lists for Customer1.

External DNS Names

When you configure DNS, you will need to create the following external DNS names for a second level domain such as www.Company1.com:

- A standard (primary) zone
- A Mail Exchange (MX) record for each virtual domain, such as Customer1.com
- An Alias (A) record for each physical computer, such as *www* and *mail*

Installation and Setup

This section walks you through the process of installing Exchange 2000 and Active Directory on the front-end and back-end servers in your network. In this section, you will perform the following procedures:

- Setting up Windows 2000 and installing Active Directory
- Installing Exchange 2000 on the back-end server
- Installing Exchange 2000 on the front-end server
- Promoting the front-end server
- Allowing anonymous connections
- Configuring smart host to route SMTP mail

Setting Up Windows 2000 and Installing Active Directory

The first steps in the process are to set up Windows 2000 Advanced Server and install Active Directory. When you perform the installation, you must specify the computer running Windows 2000 as a domain controller—or you can run the Dcpromo.exe utility manually after installation. Before you install Exchange, a domain controller must be set up and available on the network or subsequent Exchange installations will fail. For detailed step-by-step instructions on installing Windows 2000 Advanced Server, see the Windows 2000 documentation.

To set up Windows 2000 Advanced Server:

1. Install Windows with an NTFS file system, and then from Control Panel, install SMTP and NNTP services.
2. Run the Active Directory Wizard (Dcpromo.exe) to promote the server to a domain controller. Set DNS during this installation.
3. Install DNS during the Active Directory promotion.

To install Active Directory on ASP-AD-01 using the Dcpromo utility:

1. On the **Start** menu, click **Run**.
2. In **Run**, type **dcpromo**, and then click **OK**. The Active Directory Installation Wizard starts.
3. Click **Next**, click **Domain Controller for a New Domain**, and then click **Next**.
4. Click **Create a New Domain Tree**, and then click **Next**.
5. Click **Create new Forest of Domain Trees**, and then click **Next**.
6. Type the full DNS name for the new domain, and then click **Next**. In this example, the full DNS name is *ASPHosting.com*.
7. Accept the NetBIOS domain name, and then click **Next**. In this example, the NetBIOS domain name is *ASPHosting*.
8. Accept the default database and log locations, and then click **Next**. The recommended configuration is to have the database in a different hard disk drive than the log file.
9. Accept the shared system volume location, and then click **Next**.
10. Click **OK** when this message appears: **Wizard cannot locate the DNS server that handles the name ASPHosting.Com to determine if it supports dynamic update. Confirm your DNS configuration or install**

and configure a DNS server on this computer. The next steps will prompt you to set up a DNS server.

11. In **Configure DNS**, click **Yes, install and configure a DNS server on this computer**, and then click **Next**.
12. In **permission**, click **Permissions compatible with pre-Windows 2000 Server**, and then click **Next**.
13. In **Directory Services Restore Mode Administrator Password,** type a password such as *password*, and then click **Next**.
14. Accept the settings shown in the summary, and then click **Next**. This starts the creation of the Windows 2000 domain and installs the DNS server on Stage 1.
15. When setup is complete, click **Finish** to restart the server.

Installing Exchange 2000 on the Back-End Server

The back-end server running Exchange will hold user mailboxes and message stores. Place this server on the same network segment as your Windows 2000 Active Directory domain controller.

The computer on which you will install Exchange requires a clean installation of Windows 2000 Server on an NTFS drive. You should install Windows 2000 Server as a stand-alone server, but the computer must be a part of a domain. In addition, make sure that SMTP and NNTP services are installed on the computer.

To install Exchange 2000 on ASP-Exch-01:

1. Launch Exchange 2000 Server setup (<cd-rom>\launch), and from the setup screen, click **Setup**, and then click **Exchange Server Setup**. The Exchange Setup Wizard starts.
2. From the setup wizard, click **Next**, click **I Agree** to continue, and then click **next**.
3. Type your Product ID, and then click **Next**.
4. From the **Component Summary** screen, do the following:
   - Select **Microsoft Exchange 2000**, and under **Action**, select **Custom**.
   - Select **Microsoft Exchange Messaging and Collaboration Services**, and under **Action**, select **Install**.
   - Select **Microsoft Exchange System Management Tools**, and under **Action**, select **Install**, and then click **Next**.
5. On the **Installation Type** screen, select **Create a new Exchange Organization**, and then click **Next**.
6. Type **My ASP Organization**, read the agreement, and select **I agree** to continue. Then click **Next** to start the installation.
7. During installation, Exchange alters your Active Directory schema. The Microsoft Exchange 2000 Installation Wizard will display the following message: **Exchange Setup has determined that it must extend your Windows 2000 directory schema in order to continue installing into the Windows 2000 domain, This process may take a considerable amount of time to complete.** Select **OK** to continue or **Cancel** to exit Setup, click **OK**, and then click **Finish**.

Installing Exchange 2000 on the Front-End Server

This process is similar to setting up the back-end server ASP-Exch-01. After you install Exchange on this server, you will use the System Manager snap-in to promote this server to a front-end server. Again, start with a freshly formatted installation of Windows 2000 Advanced Server with SMTP and NNTP installed during Windows setup. Your computers must be part of the domain. In addition, a valid account with the valid security context must be logged on to the server before you launch Setup.

To install Exchange on ASP-FE-01:

1. Launch Exchange 2000 Server setup, and from the setup screen, click **Setup**, and then click **Exchange Server**. The Exchange Setup Wizard starts.
2. From the setup wizard, click **Next**, and then click **Agree** to continue.
3. Type your Product ID, and then click **Next**.
4. From the **Component Summary** screen, do the following:
   - Select **Microsoft Exchange 2000**, and under **Action**, select **Custom**.
   - Select **Microsoft Exchange Messaging and Collaboration Services**, and under **Action**, select **Install**.
   - Select **Microsoft Exchange System Management Tools**, and under **Action**, select **Install**.
   - Select **Microsoft Exchange Instant Messaging Services**, and under **Action**, select **Install**, and then click **Next**.
5. From the **Licensing Agreement** screen, select **"I agree"**, and then click **Next** to continue.
6. From the **Component Summary** screen, select **Microsoft Exchange 2000**. In the **Action** column, select **Custom**. Click **Next** to begin installing components.
7. From the **Component Progress** screen, wait for components to install, click **Next**, and then click **Finish**.

Promoting the Exchange Front-End Server

After you install Exchange on the front-end server, log on to the back-end server ASP-Exch-01 and promote ASP-FE-01 to a front-end server.

To promote an Exchange server to a front-end computer:

1. Start System Manager. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Open the **Servers** tree and right-click **ASP-FE-01**.
3. Click **Properties**, select the **This is a front-end server** check box, and then click **OK**.
4. When the message box appears, click **OK** again.
5. Log back on to the front-end server and reboot that computer.
6. Reboot the server you just promoted.

If this were a production scenario, you might have clusters of servers handling all protocols. In this scenario, we'll simply group all front-end protocols on ASP-FE-01. By default, when you install Exchange, all services are set to run. Using

System Manager, you can specify which services you want to run and which to turn off.

To turn off protocol services:

1. Log on to the front-end server.
2. Start System Manager. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
3. Expand **Servers**, select the server you want, and browse to **Protocols**.
4. Click the protocols you do not want to run, and then select **Stop**.

Allowing Anonymous SMTP Connections

Use the following procedure to allow anonymous SMTP connections to the front-end server ASP-FE-01.

To allow anonymous SMTP connections:

1. Log on to ASP-EXCH-01 and start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Double-click **Servers**.
3. Select the front-end server that will host SMTP (ASP-FE-01).
4. Expand the **Protocols** tree, and then expand **SMTP**.
5. Right-click **Default SMTP Protocol**, and then select **Properties**.
6. Click **Access**, and then click **Authentication**.
7. Select **Anonymous Access**.
   Note Make sure that **allow Basic** is still selected.
8. Click **OK**, and then click **OK** again.

Configuring Smart Host to Route SMTP Mail

Use the following procedure to configure smart host to route SMTP mail.

To configure smart host to route SMTP mail:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand **Servers**, browse to **Protocols**, and then expand **SMTP**.
3. Right-click **Default SMTP Protocol**, and then select **Properties**.
4. Click the **Delivery** tab, and then click **Advanced**.
5. In **Smart host:**, type the name of your *front-end* SMTP server (ASP-FE-01), and then click **OK**.
6. Click **OK** again to apply your changes.

Configuring Organizational Units, Users, and Groups

In this section, you'll use System Manager and Active Directory Users and Computers to create an organizational unit, users, and groups. These components make administering your network easier because you can use them to define security. This section contains the following procedures:

- Configuring an organizational unit
- Adding a UPN suffix
- Creating a security group
- Creating a user group

Configuring an Organizational Unit

Use this procedure to create an organizational unit for Customer1.com.

To create an organizational unit:

1. Log on to the back-end server running Active Directory, ASP-AD-01.
2. Start Active Directory Users and Computers: From the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
3. In the left pane, select the default company domain (aspHosting.com), and then select **Properties**.
4. Right-click **New**, and then select **Organizational Unit**.
5. Type **Customer1**, and then click **OK**.

Adding a UPN Suffix

User principle names (UPNs) provide logon names in a format similar to e-mail names. By making UPN values independent from domain names, you can move user accounts between domains while leaving UPN values unchanged, making the move transparent to users and easing administration.

Note Versions of Windows earlier than Windows 2000 limits user names to fewer than 20 characters.

To add a UPN suffix:

1. Launch Active Directory Domains and Trusts: On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. Right-click **Active Directory Domains and Trusts** (*not* yourDefaultDomain), and then select **Properties**.
3. On the **Alternative UPN Suffixes** tab, type **Customer1**, click **Add**, and then click **OK**.

Creating a Security Group

You'll use this security group to delegate administrative duties to the organizational unit Customer1. After you create this security group, you can view user permissions by selecting the group, right-clicking, and selecting **Properties**.

To create a security group:

1. Log on to the back-end server running Exchange, ASP-Exch-01.
2. Start Active Directory Users and Computers: From the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
3. Select the organizational unit **Customer1**.
4. Right-click **Customer1**, and then select **New/Group**.
5. Under **Group name**, type **Admins@customer1**.
6. Under **Group scope**, select **Global**, and under **Group** type, select **Security**, and then click **Next**.
7. Under **Alias**, select the suffix name **@Customer1** and delete the suffix name by pressing **Delete**, click **Next**, and then click **Finish**.

Creating a User Group

This user group will contain a sample set of user access privileges created for the organizational unit Customer1. Once you create this group, you can view user permissions by selecting the group, right-clicking, and selecting **Properties**.

To create a user group:

1. Log on to the Exchange back-end server ASP-Exch-01.
2. Select the organizational unit **Customer1**.
3. Right-click **Customer1**, and then select **New/Group**.
4. Under **Group name**, type **allUsers@Customer1**.
5. Under **Group scope**, select **Global**. Under **Group type**, select **Security**, and then click **Next**.
6. Under **Alias**, remove the suffix name *@Customer1*, click **Next**, and then click **Finish**.

Configuring Security and Creating Address Lists

In this section, you will set security on the organizational unit Customer1 by delegating administrative Write access privileges to the group Admins@customer1 and restricting access from users in other domains. You will create a policy to allow new resources (such as users, groups, and organizational units) to inherit permissions from Customer1.

This section contains the following procedures:

- Setting security policies on an organizational unit
- Creating a recipient policy for users in an organizational unit
- Creating a recipient policy for groups in an organizational unit
- Creating a global address list
- Setting security policies for a global address list
- Creating an offline address list for an organizational unit
- Setting security for an offline address list
- Setting security for Customer1 address lists

Setting Security Policies on an Organizational Unit

Use the following procedure to set security policies for the organizational unit Customer1.

To set security policies on an organizational unit:

1. Log on to the back-end Exchange server ASP-EXCH-01.
2. Start Active Directory Users and Computers: From the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
3. Navigate to Customer1, and then select it.
4. From the **View** menu, select **Advanced Features**.
5. Select **Customer1.com**, select **Properties**, and then click the **Security** tab.
6. Clear the **Allow inheritable permissions from parent to propagate to this object** check box.
7. When the dialog box appears, click **Copy**.
8. Select **Authenticated Users**, and then click **Remove**.
9. Click **Add**.
10. Browse to Admins@customer1, select it, and then click **Add**.
11. Browse to AllUsers@customer1, select it, click **Add**, and then click **OK**.
12. From the **Security properties** dialog box, select **Admins@customer1** and select the appropriate check boxes under **Allow** to enable the following permissions:
    - Read
    - Write
    - Create all child objects
    - Delete all child objects
13. Click **OK**.

Creating a Recipient Policy for Users

Using the following procedure, you will create a recipient policy called Customer1 – Users. This policy automatically generates an e-mail address for each user you add to the organizational unit Customer1.

To create a sample recipient policy for users:

1. Log on to the Exchange back-end server ASP-Exch-01.
2. Start System Manager On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
3. Expand the **Recipients** tree, and select **Recipient Policies**.
4. Right-click **Recipient Policies**, and then select **New/Recipient Policy**.
5. Type the name of the recipient policy, **Customer1 - User**, and then click **Modify**.
6. Change the **Find:** drop-down menu to point to **User, Contacts, and Groups** by selecting **User, Contacts, and Groups**.
7. Click the **Advanced** tab, click **Field**, and select **User/Logon Name**.
8. Under **Condition**, select **Ends with**, and under **Value**, type **@Customer1**.
9. Click **Add**, click **OK**, and then click **Apply**.
10. Click the **E-mail Addresses** tab, click **New**, and under **E-mail Address**, select **SMTP Address**, and then click **OK**.
11. In the **Address** section of the **SMTP Address Properties** dialog box, type **@Customer1.com**, and then click **OK**.
12. Select the SMTP check box you just created with @Customer1.com in the **Address** column, click **Set as Primary**, and then click **OK**.
13. From the System Manager warning box, click **Yes**, and then click **Yes** again.

Creating a Recipient Policy for Groups

Using the following procedure, you will create a recipient policy called Customer1 – Groups. This recipient policy automatically generates an e-mail address for each group you add to the organizational unit Customer1.com.

To create a recipient policy for a group:

1. Log on to the Exchange back-end server ASP-Exch-01.
2. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
3. Expand the **Recipients** tree, and then select **Recipient Policies**.
4. Right-click **Recipient Policies**, and then select **New/Recipient Policy**.
5. Type the name of the recipient policy, **Customer1 – Group**, and then click **Modify**.
6. From the **Find:** menu, select **User Contacts, and Groups**.
7. Click the **Advanced** tab, click the **Field** tab, and then select **Group/Display Name**.
8. Under **Condition**, select **ends with**. Under **Value**, type **Customer1**, click **Add**, and then click **OK**.
9. From the **Customer1 Properties** dialog box, click **Apply**, click the **E-mail Addresses** tab, and then click **New**.
10. Under **New E-mail Address**, select **SMTP Address**, and then click **OK**.
11. In the **Address** section of the **SMTP Address Properties** dialog box, type **@Customer1.com**, and then click **OK**.

12. Select the SMTP check box you just created with @Customer1.com in the **Address** column, click **Set as Primary**, and then click **OK**.
13. From the System Manager warning box, click **Yes**, and then click **Yes** again.

Note This creates SMTP rules for all users within the domain you assigned.

Creating a Global Address List

Using the following procedure, you will create a global address list for the organizational unit Customer1. Global address lists define a set of rules for looking up users in a global address book—for example, by alias name, long name, group name, and so on.

To create a global address list:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand the **Recipients** tree by selecting **Recipients**, and then **All Global Address Lists**.
3. Right-click **Default Global Address List**, select **Delete**, and then click **Yes** to confirm your selection.
4. Right-click **All Global Address Lists**, and select **New / Global Address List**.
5. In the **Address List Name** section of the **Exchange Address List** dialog box, type **Customer1**.
6. Click **Filter Rules**, and from the **Find:** drop-down menu, select **Exchange Recipients**.
7. Click the **Advanced** tab, click **Field**, select **Users,** and then select **E-mail Address**.
8. Under **Condition**, select **Ends with**, under **Value**, type **Customer1.com**, and then click **Add**.
9. Click **OK**, and then click **Finish**.

Setting Security Policies for a Global Address List

Using the following procedure, you will restrict global address list lookups to the AllUsers@Customer1 and Admins@customer1 groups of Customer1. After you set this policy, only users that belong to Customer1 will be able to perform lookups on the Customer1.com global address list.

To set security for a global address list:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Browse to Recipients, select **All Global Address Lists**, and then select **Customer1 - Users**.
3. Right-click **Customer1 – Users**, and then click **Properties**.
4. Click the **Security** tab, and at the bottom of the dialog box, clear the **Allow inheritable permissions from parent to propagate to this object** check box, and then click **Copy**.
5. Under **Name**, select **Authenticated Users**, and then click **Remove**.
6. Click **Add**, add AllUsers@Customer1 and Admins@customer1, and then click **OK**.
7. Select **AllUsers@Customer1**, and under **Permissions**, clear all options except the following:
   - Read

- Execute
- Read permissions
- List content
- Read properties
- Open address list
- List object

8. Click **OK**. A dialog box will display the following message: **Caution, deny entries take priority over allow entries, which can cause unintended effects due to group membership**. Click **Yes**.

Creating an Offline Address List for an Organizational Unit

Using the following procedure, you'll create an offline folder for Customer1. An offline address list is a replica of your global address list stored on your local computer that you use to synchronize your offline folders.

To create an offline address list:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Under **Recipient Policies**, select **Offline Address List**.
3. Right-click **Offline Address List**, and select **New / Offline Address List**.
4. In **Offline address list name**, type **Customer1**.
5. Click **Browse**, select the server on which you want to store the offline folder, and then click **Next**.
6. In **New Object Address List**, select **Customer1.com**, click **Next**, and then click **Finish**.
   Note Ensure that all other address lists are removed from this dialog box.
7. In the **Name** column in **System Manager**, right-click the default offline address book, and then press **Delete**. Click **Yes** to confirm the deletion.

Setting Security for an Offline Address List

Using the following procedure, you will set security for the Customer1 offline address list. After you perform this procedure, only users in the Customer1 organizational unit will be able to access the offline address list.

To set security for an Offline Address List:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Select the Offline Address List you just created, **Customer1**.
3. Right-click **Customer1**, and then select **Properties**.
4. Click the **Security** tab, clear the **All inheritable permissions** check box, and then click **Copy**.
5. Under **Name**, select **Authenticated Users**, and then click **Remove**.
6. Click **Add**, add AllUsers@Customer1 and Admins@customer1 and then click **OK**.
7. Select AllUsers@Customers1, and under **Permissions**, clear all options except the following:
   - Read
   - Execute

- Read permissions
- List content
- Read properties
- List object

8. Click **OK**. A dialog box will display the following message: **Caution, deny entries take priority over allow entries, which can cause unintended effects due to group membership.** Click **Yes**.
9. Right-click the Customer1.com offline address list, and then click **Rebuild**. This creates an offline file. Click **Yes**.

Setting Security for Customer1 Address Lists

To limit address list lookups to each organizational unit, you need to delete the default address list.

To delete the default address list:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Select each address list and click **Delete**.
3. Go to **All Address Lists**.

Creating Mail-Enabled Users and Configuring an External DNS Server

This section walks you through the process of creating mail-enabled users and configuring an external DNS server for name resolution.

Creating Mail-Enabled Users

Using the following procedure, you will create e-mail accounts and associate them with Active Directory user accounts and UPNs.

To create mail-enabled users:

1. Log on to the back-end server ASP-Exch-01.
2. Start Active Directory Users and Computers: From the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
3. In the left pane, select the organizational unit **Customer1**.
4. Right-click **Customer1**, select **New**, and then select **User**.
5. In **first name** type **Alice**, and in **last name**, type **Evergreen**.
6. In **user logon name** type **Alice**, and then select the default UPN suffix to associate with Alice @Customer1.
7. In **User logon name [pre-Windows 2000]**, type **alice@customer1**, and then click **Next**.
8. Type a password, and then click **Next**. In this example, the password is *password*.
9. Under **Alias**, remove the suffix *@Customer1*.
10. In **Server Name**, select your back-end Exchange server, **ASP-EXCH-01**, click **Next**, and then click **Finish**.
11. Right-click **allUsers@Customer1**, and then select **Properties**.
12. Click the **Members** tab and click **Add**.
13. Select **Alice Evergreen**, click **Add**, and then click **OK**.
14. Click **OK** again to confirm your selection.

Note It will take a few minutes for the new e-mail names and offline address lists to refresh and become available on your Exchange server.

Configuring an External DNS Server

This section walks you through the process of configuring your external DNS server and creating zone files, host records, and Mail Exchanger (MX) records. Ideally, you should let the Active Directory Installation Wizard (Dcpromo.exe) configure DNS for you. If performed manually on a stand-alone Windows 2000 Server or before you install Active Directory, you will need to perform the following steps on your external DNS server.

1. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **DNS**.
2. In **DNS/Your Server Name**, under **Forward Lookup Zones**, select **Create a New Zone**.
3. Right-click **Forward Lookup Zones**, select **New Zone**, and then click **Next**.
4. Leave **Standard primary** selected, and then click **Next**.

5. Type the name of the zone as **Customer1.com**, and then click **Next**.
6. Select **Create a new file with this name** and accept the default value, click **Next**, and then click **Finish**.

To create a reverse lookup zone file:

1. Right-click **Reverse Lookup Zones**, click **New Zone**, and then click **Next**.
2. Select **Standard Primary**, and then click **Next**.
3. In the **Network ID** tab, type your mail domain's host network ID, and then click **Next**.
4. Click **Next** again, and then click **Finish**.

To create a new host record:

1. From the DNS Administrative console, under **Forward Lookup Zones**, select **Customer1.com**.
2. Right-click **Customer1.com**, and then select **New Host**.
3. In **Name**, type **mail**. Add the virtual IP address of the Network Load Balancing server that will load balance POP3 and SMTP requests, and then click **Enable PTR record**.
4. Click **Add Host**, click **OK**, and then click **Done**.
5. Right-click **Customer1.com**, and then select **New Host**.
6. To create a new alias (A) record that will load balance HHTP requests for Outlook Web Access, in **name**, type **www** or the appropriate host name, and then add the virtual IP address of this Network Load Balancing server.
7. Click **Add Host**, select **Create an associated PTR (pointer) record**, and then click **OK**.
8. Click **OK** again, and then click **Done**.

To add a new MX record:

1. Right-click **Customer1.com**, and then select **New Mail Exchanger**.
2. In the **Mail server** text box, browse to your mail server under *Customer1.com* or type **MAIL.customer1.com**, and then click **OK**.

For a sample zone file, see "Appendix A: Sample Zone File for Customer1.com" later in this paper.

Testing Clients

The three-server network you set up earlier provides support for HTTP, SMTP, NNTP, POP3, and IMAP4. This section contains three sample client connection scenarios—Outlook 2000, Outlook Express, and Outlook Web Access. Use the procedures in this section to configure various clients; then you can send mail to test your three-server deployment. When you are ready to go into production, you can use only the protocols and clients that best fit your business needs.

This section contains the following procedures:

- Configuring TCP/IP
- Configuring Outlook 2000
- Configuring Outlook Express 5.0
- Configuring Outlook Web Access

Configuring TCP/IP

To configure TCP/IP:

1. From the **Start** menu, point to **Settings**, click **Control Panel**, and then double-click **Network and Dialup Connections**.
2. Right-click **Network Adapter**, select **Properties**, and then select **Internet Protocol/Properties**.
3. Type a valid IP address (for example, 10.0.0.100), click **OK**, and then click **OK** again.
4. From the **Start** menu, point to **Settings**, click **Control Panel**, and double-click **System**.
5. Click the **Network Identification** tab, click **Properties**, and in **Domain**, type the domain NetBIOS name.
6. Type the Administrator account name and password, and then click **OK**.
7. Click **OK** twice to close the dialog boxes, and then click **Yes** to reboot the computer.
8. Log on to the domain.

The user will type **user@Customer1** and the password. (Note that as soon as you enter @Customer1, the logon will not be available because Active Directory maps the UPN against the customer's organizational unit.)

Configuring Outlook 2000

You will configure Outlook 2000 in Corporate Workgroup mode, which uses MAPI to connect to an Exchange 2000 server. To use MAPI, the client must connect directly to a back-end server through a VPN or another firewall.

Note When using MAPI in a production environment, Microsoft strongly recommends that you use a VPN and secure tunnel architecture.
If you do not want to expose a MAPI client directly to your back-end server and instead want to route the connection through the front-end protocol servers, you can configure Outlook 2000 in Internet Mail Only mode. For information about how to do this, see the Outlook 2000 documentation.

To configure Outlook 2000 to send and receive mail:

1. From the **Start** menu, point to **Settings**, click **Control Panel**, and then double-click **Mail**.
2. Click **Show Profiles**, and then click **Add**.
3. Select the **Microsoft Exchange** check box, and then click **Next**.
4. Type a friendly name for the profile *Alice*, and then click **Next**.
5. In **Exchange Server Name**, type Asp-exch-1 and in **Mailbox**, type **alice@Customer1.com**.

Configuring Outlook Express 5.0

You can configure Outlook Express in the following ways, which are described in this section:

- Using standard POP3 and SMTP to send and receive mail
- Using IMAP4 to receive mail and SMTP to send mail
- Using HTTP to send and receive mail through Exchange, Hotmail®, or another HTTP mail server

Note POP3 and IMAP4 clients such as Outlook Express use Lightweight Directory Access Protocol (LDAP) for address book lookups.

To configure Outlook Express 5.0:

1. Start Outlook Express: On the **Start** menu, point to **Programs**, and then click **Outlook Express**.
2. If you are starting Outlook Express for the first time, use the wizard to set up Outlook Express.

   -or-

   From the **Tools** menu, select **accounts**.
3. Click **select Mail**, and in display name, type **select mail**.
4. In **Display Name**, type **Alice Evergreen**, and then click **Next**.
5. Click **"I already have an e-mail address ... "**
6. Type Alice@customer1.com.

Option 1

1. Type the POP3 and SMTP name, which in our case is **Mail.customer.com**, and then click **Next**.
2. Type the account name—Alice@Customer1.com.
3. Type the initial password, which is *password* in this example, click **Next**, and then click **Finish**.

Option 2

1. Select the incoming mail server as HTTP.
2. In the incoming mail server, type the name of the HTTP server as **http://www.Customer1.com**.
3. Click the Inbox folder, click the **Tools** menu, select **Send/Receive**, and then select **Send and Receive All**.

Configuring Outlook Web Access

Exchange 2000 Server provides support for HTTP access to e-mail through Outlook Web Access. This feature allows users to access mailbox, address book, and scheduling information using Internet Explorer. But in a hosting scenario,

you'll need to configure Outlook Web Access security to limit the scope of mail server queries. Outlook Web Access performs queries to address books through a programmatic query (*msExchQueryBaseDN*) to restrict the scope of the search within a given customer's global address list. Outlook Web Access uses MAPI-based RPC for address book lookups.

You can configure this using ADSIEdit.exe, which is available on the Windows 2000 compact disc.

Important note Using ADSIEdit.exe to alter the schema can potentially corrupt your directory. Use it only if you are an advanced Active Directory programmer or administrator.

To configure msExchQueryBaseDN:

1. Install support tools: Insert the Windows 2000 compact disc and run the following executable: \X86\SUPPORT\TOOLS\setup.exe.
2. Run ADSIEdit.exe: From the **Start** menu, point to **Programs**, point to **Windows 2000 Support Tools**, and then click **ADSI Edit**.
3. Click **Domain NC**.
4. In this example, use ASPHosting.com. Click **DC=ASPHosting, dc=COM**.
5. Navigate to the organizational unit Customer1.com.
6. In the right pane, right-click the user to which you want to restrict the research.
7. In **Select a property to view**, select **msExchQueryBaseDN**.
8. In **Edit attribute**, type **ou=customer1, DC=ASPhosting, dc=COM**.
9. Click **Set**, and then click **OK**.

To test Outlook Web Access, open Internet Explorer and type the following: http://<yourHttpServerName>/exchange/alice.

Creating a Virtual Outlook Web Access Server

To create a virtual Outlook Web Access server:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Navigate to your front-end server, ASP-FE-1.
3. Right-click **HTTP**, select **New Virtual Server**. Name = Customer1.com.
4. In the **IP Address** text box, click **Advanced**. In the host header, type **www.customer1.com.**
5. Click **OK**, and then click **OK** again.
6. In the Exchange path, click **Modify**, and then click **customer1.com**.
7. Click **OK**, and then click **OK** again.
8. Right-click the new virtual server and select **Start**.

Configuring Network Load Balancing, Cluster Services, and Storage

Once you have set up your network, you can install Network Load Balancing Service (NLBS) and Microsoft Cluster Services to make your system scalable, reliable, and highly available. Designing your data center for high availability requires that your systems perform required functions under stated conditions for specified periods. Although there is no industry-wide standard for calculating availability, the metrics most often used to calculate reliability are mean time to failure and mean time to recover.

Scalability is the capacity to grow your infrastructure, adding new domains, directory services, systems, and system components as your business grows. It's important that you're able to expand your data center *vertically*. Scalability also means that you can grow your data center *horizontally*. Windows 2000 Advanced Server supports clustering technologies to maintain existing services by increasing server numbers incrementally.

Reliability means that network operators can depend on services being up and available. If you need to take a computer offline for planned or unplanned service, the other systems should adapt gracefully and transparently to accommodate users. With the appropriate load balancing technologies in place, you can provide a guaranteed level of service to customers.

Setting up NLBS

This section walks you through the process of setting up and testing NLBS.

The NLBS driver, included with Windows 2000 Advanced Server, allows you to cluster a set of stateless, front-end computers, such as protocol servers, by virtual IP addresses. Once you connect these servers, users and other resources on the network view the cluster as a single system image, or single computer. NLBS supports up to 32 computers in a single cluster. If a server in the cluster goes down or is taken offline for repair, the NLBS cluster dynamically adjusts, distributing requests to the available servers. When you bring the server back online, the NLBS cluster automatically reincorporates that system.

NLBS enables you to set protocol-level security, which means you can block ports, set port rules, and customize load capacity levels.

Installing and Configuring NLBS

Setting up NLBS involves two main steps: installing and configuring NLBS components, and configuring TCP/IP settings on the server. You perform these steps on every server that you add to the cluster.

To install NLBS components, you will need the following:

- The full Internet name of the cluster. In this scenario, the name of the cluster is *aspHosting.com.*
- The IP address for the cluster. This IP address is sometimes referred to as the virtual IP of the cluster. The same cluster IP address is used on all

hosts in the cluster. It must be a valid IP address that is unique on the Internet. In this scenario, the IP address is 192.168.18.155.

- The IP address for the external-facing NIC in each cluster host. This NIC is sometimes referred to as the cluster adapter. The cluster adapter IP address is unique to each host, and must be unique on the Internet. It is used for communication with the individual host (not the cluster as a whole), such as during content deployment.

Note If you are using a router to connect a NLBS cluster to its clients, be sure that proxy Address Resolution Protocol (ARP) support is enabled for the router. This allows the router to map the primary IP address of the cluster and other multi-homed addresses to the corresponding media access control (MAC) address. If your router does not route to the cluster with proxy ARP support enabled, you can also create a static ARP entry in the router.

Additional information about NLBS is available at http://www.microsoft.com/ntserver/ntserverenterprise/exec/feature/WLBS/ and http://www.microsoft.com/ntserver/ntserverenterprise/techdetails/prodarch/Wlbs.asp.

To install and configure NLBS:

1. In Control Panel, double-click **Network and Dial-Up Connections**.
2. Right-click the local area connection that is configured for the external NIC, and then click **Properties**.
3. Select the **Network Load Balancing** check box, and then click **Properties**.
   The **Network Load Balancing Properties** dialog box appears.
4. Specify the cluster parameters. The example site uses the parameters in the following table.

Parameter	Value
Primary IP address	192.168.1.101
Subnet mask	255.255.255.0
Full Internet name	Mail.aspHosting.com
Multicast support	Disable
Remote password	Password
Remote control	Disable

Important Note If you enable remote control for your NLBS cluster, which is disabled by default, to maintain network security you must protect the NLB UDP control port (the port receiving remote control commands) with a firewall to shield it from outside intrusion. By default, this is port 2504 at the cluster IP address.

1. Click the **Host Parameters** tab, and specify the following values:
   - In Priority (ID), specify a unique sequential number. Specify 1 for the first server in the NLBS cluster, 2 for the second, and so forth up to 32 nodes. Specify the initial state as *active*.
   - Type values for the dedicated IP address and subnet mask. These values are the unique external IP addresses for each server in the NLBS cluster. They must be valid Internet addresses. In the example site, add an IP address of 192.168.18.158 with a subnet mask of 255.255.255.192.

- Create port rules to specify how you want NLBS to handle network traffic for specific ports. In this scenario, Web access is provided only to the front end, so only port 80 is enabled (for HTTP).
- Highlight the default port rule (0-65535).
- Change the port range to 80.
- Set **Affinity** to *none* (there will be no affinity settings for port 80 in this example).

2. Click **Modify**, and then click **OK**.
3. Click **Close** to close the **Local Area Connection Properties** dialog box.

Repeat this procedure for every server that you add to the cluster.

Note For information about configuration options for NLBS Hosts Connected to Layer 2 Switch ID:Q193602, go to http://support.microsoft.com/support/kb/articles/Q193/6/02.ASP.

Testing Network Load Balancing

When you have installed NLBS on all of the front-end servers, perform the following tests to verify that the cluster is performing correctly:

- Verify that you can send a message to the virtual IP address of the cluster. In this example, verify that you get a response when you send a message to 192.168.18.155.
- Verify that you can send a message to each host in the front-end cluster.
- Put a slightly different default page in the wwwroot directory for each host and repeatedly open the default Web page for the cluster. You should see the different pages in quasi-random order as the individual servers in the cluster respond to the HTTP requests to the cluster. Before you perform this test, make sure that caching is disabled on the client browser.
- Verify that you do not get a response when you send a message to the IP addresses on the internal (10.0.0.*x*) network from a computer on an external network.

To configure a server to be a Global Catalog Server:

1. From the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
2. Expand site\default-first-site-name\services\.
3. Select the server that you want to configure as a Global Catalog Server and expand the tree.
4. Right-click **NTD Setting**, and then select **Properties**.
5. Select **Global Catalog**, and then click **OK**.

Setting Up Cluster Services

Microsoft Cluster Services provide high availability for back-end servers. For example, Cluster Services can preserve client access to applications and resources during failures and planned outages. In the event that an application fails, the application will failover to another server in the cluster. When an offline server comes back online, the resource or application gracefully recovers.

There are two node states in a cluster: active and passive. Active nodes handle online application and resource activity; passive nodes are on standby to back up active nodes.

This section walks you through the process of installing and configuring Cluster Services, including the following procedures:

- Installing Cluster Services
- Configuring Cluster Services for Exchange
- Installing Exchange 2000 on the clustered computers
- Configuring Exchange 2000 cluster groups
- Assigning cluster resources
- Creating storage groups

For additional information about Microsoft Clustering Services, go to http://www.microsoft.com/windows2000/library/planning/server/clustersteps.asp.

Installing Cluster Services

Use the following procedures to install Microsoft Cluster Services on the first two servers in a cluster.

To install Windows 2000 Cluster Services on the first server in a cluster:

1. From the **Start** menu, point to **Settings**, point to **Control Panel**, and then double-click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select the Cluster Service check box to enable Cluster Service, and then click **Next**.
4. In the Welcome page, click **Next**.
5. In the Hardware Configuration page, click **I understand**, and then click **Next**.
6. Click the first node in the cluster, and click **Next**.
7. Type a name for the new cluster field (in this scenario, it is *Exchange*), and then click **Next**.
8. Type the user name, password, and domain for the account under which Cluster Services will run, and then click **Next**.
9. In the **Add Or Remove Managed Disk** dialog box, add or remove the disks on the RAID data store that you will use with your cluster, and then click **Next**.
10. In **Cluster File Storage**, click the name of the disk on the RAID data store on which you want to store the quorum resource, and then click **Next**. You can store the quorum resource on any shared physical disk array.
11. In **Configuration Cluster Network**, click **Next** to allow Setup to identify all network resources that are available on your server.
12. For each network adapter installed in the node, specify the following:
    - A name that describes the network, using a meaningful description so you can identify the networks when working in Cluster Administrator. In this scenario, name the 10.0.0.*x* network internal. Select **All Communication**.
    - Specify the name heartbeat for the 11.0.0.*x* network (used by the cluster for heartbeat communication, keeping the cluster

information updated). Select **Use only for internal cluster communication**, and then click **Next**.

- In **Cluster IP Address**, type the static IP address and subnet mask that you want to use to identify the cluster. In this scenario, the IP address is 10.0.0.10 and the subnet mask is 255.0.0.0.
- In **Network**, click **Internal**, and then click **Next**.

13. Click **Finish**, and then click **OK**.

To install Windows 2000 Cluster Services on the second server in a cluster:

1. From the **Start** menu, point to **Settings**, point to **Control Panel**, and then double-click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select the **Cluster Service** check box to enable Cluster Services, and then click **Next**.
4. In the **Welcome** page, click **Next**.
5. In the **Hardware Configuration** page, click **I understand**, and then click **Next**.
6. Click **Second or Next Node in the Cluster**, and then click **Next**.
7. In **Cluster Name**, type the name of the cluster that the server is joining, and then click **Next**. In this example, the name of the cluster is *EXCHANGE*.
8. Type the password for the domain user account you specified when installing the first server in the cluster, and then click **Next**.
9. Click **Finish**, and then click **OK**.

You can verify the installation of your cluster by starting Cluster Administrator and checking that both nodes in your cluster are detected.

On either node, from the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Cluster Administrator** to make sure that both nodes appear.

Installing Exchange on the Clustered Computers

Cluster Services requires that you install Exchange on one node completely before installing it on the second node. Do not install Exchange on both computers (nodes) at the same time.

Install Exchange on the same local drive and directory on both computers for binary files. You must install the same Exchange components on both nodes. At minimum, you must install **Microsoft Exchange Messaging and Collaboration** and **Microsoft Exchange System Management Tools** on both nodes.

Restart each computer after you install Exchange.

Creating a Resource Group (Exchange Virtual Server)

The following procedures describe how to create a virtual server. Creating a virtual server consists of the following steps:

- Creating a group for the cluster resources
- Creating the IP, network name, storage, and Exchange System Attendant resources

Complete these tasks using Cluster Administrator, which is installed automatically when you install Cluster Services.

To create an Exchange Cluster Group (Exchange Virtual Server):

1. On one of the clustered computer nodes, click **Start**, point to **Administrative Tools**, and then click **Cluster Administrator**.
2. Right-click the **Groups** node container, point to **New**, and then click **Group**. The New Group Wizard appears.
3. In **Name**, type **Exchange Virtual Server 1**. Optionally, in **Description**, you can type a description of this group. Click **Next**.

   Note You can give this group any name you choose. However, this section refers to the group that you name in this step as *Exchange Virtual Server Your Virtual Server*. To simplify administration, Microsoft recommends that you name this group according to its real network server name. For example, if the server name that clients use in their profiles is MailServ1, you might consider naming this group *MailServ1 VS*.

4. On the **Possible Owner** screen, verify that both cluster nodes are listed in the **Available nodes** box, and then click **Finish**. The Exchange Virtual Server *Your Virtual Server* appears under **Groups**.

Assigning Cluster Resources

Each virtual server in an Exchange cluster must be associated with a cluster group containing the following resources:

- IP address
- Network name
- Storage
- Exchange System Attendant

The following procedures describe how to assign these resources to your cluster group. If you have already associated a drive with the group, you can move the drive to the group using a drag-and-drop operation. If you do not have a storage resource or if you want to create an additional storage resource, see the Windows 2000 Advanced Server clustering documentation.

Note Except for protocol virtual servers, do not add more than one instance of an Exchange resource to a group.

To create an IP address resource:

1. Right-click **Exchange Virtual Server**, point to **New**, and then click **Resource**. The New Resource Wizard starts.
2. On the **New Resource** screen do the following:
   - In Name, type Exchange Virtual Server 1IP.
   - In Description, type a description of the resource. (This is optional.)
   - In Resource type, select IP Address. Group displays *Your Virtual Server* Exchange Virtual Server. Click next.

Note You can give this resource any name you choose. However, in this scenario, the IP address that you name in this step is called Exchange Virtual Server IP.

3. On the **Possible Owners** screen, verify that both nodes appear in **Possible owners**.
4. On the **Dependencies** screen, verify that no resources appear in **Resource dependencies**.
5. On the **TCP/IP Address Parameters** screen, type the unique static IP address and subnet mask for this virtual server. This is the IP address for the virtual server running Exchange Server on your network; it does not refer to the physical computer.
6. In **Network**, select the appropriate network card for this network connection, and then click **Finish**. This IP address is now associated with the ***Your Virtual Server*** **Exchange Virtual Server** resource group.

To create a network name resource:

1. Right-click ***Your Virtual Server*** **Exchange Virtual Server**, point to **New**, and then click **Resource**. The New Resource Wizard starts.
2. On the **New Resource** screen, do the following:
   - In **Name**, type **Exchange Network Name**. The name you type is the display name; it is not the actual unique network name that identifies this virtual server on the network.
   - In **Resource type**, click **Network Name**.
   - In **Group**, verify that **Exchange Virtual Server** appears.
3. On the **Possible Owners** screen, verify that both nodes appear in **Possible owners**, and then click **Next**.
4. On the **Dependencies** screen, in **Available resources**, click ***Your Virtual Server*** **Exchange Virtual Server IP**, and then click **Add**.
5. On the **Network Name Parameters** page screen, in **Name**, type a name for the Exchange server. This is the network name that uniquely identifies this Exchange virtual server on your network. Click **Finish**.

Moving an Existing Disk or Creating a Storage Resource

If you already have a disk with which to associate the Exchange group, you can move the drive to the group using a drag-and-drop operation.

You can also create an additional storage resource. For information on creating storage resources, see the Windows 2000 Advanced Server clustering documentation.

To move the disk to the cluster group node:

1. Open Cluster Administrator, and then click **Groups**.
2. In the Groups container, select the container that contains the disk drive that you want to move to the cluster group node. Drag the drive into the Exchange Virtual Server 1 container; this will be the drive that holds the data for the virtual server.
3. After you move a drive into the Exchange Virtual Server 1 container, clicking the **Exchange Virtual Server 1** container displays the drive in the result pane.
4. Right-click **Exchange Virtual Server 1** and then click **Bring Online**.

To create the Exchange System Attendant resource:

Important Note Before creating the Exchange System Attendant resource, the disk storage, IP address, and network name resources must be online.

1. Right-click **Exchange Virtual Server 1**, point to **New**, and then click **Resource**. The New Resource Wizard starts.
2. On the **New Resource** screen, do the following:
   - Type a name for the resource and a description of the resource.
   - In **Resource Type**, select **Microsoft Exchange System Attendant**.
   - In **Group**, select **Exchange Virtual Server 1**.
3. On the **Possible Owners** screen, verify that both of the servers on which you installed Exchange appear.
4. On the **Dependencies** screen, add **Exchange Network Name** and **Disk** to the **Resource dependencies** box by selecting each resource and clicking **Add**.
5. On the first **Exchange** screen, select the administrative group and routing group that you want to manage the virtual server.
6. On the **Data Directory** screen, verify the location of the data files, and then click **Finish**. Be sure that this directory is empty. The Exchange service instances appear in the result pane.
7. To bring the service online, right-click **Exchange Group**, and click **Bring Online**.

Important Note Do not use Service Control Manager, the command line, or System Manager to start or stop services or instances of protocols; use Cluster Administrator to perform these tasks.

Creating Additional Resource Groups (Exchange Virtual Servers)

Follow the procedures described earlier to create multiple resource groups on your cluster. You must have an external independent drive and an IP address for each Exchange virtual server resource group that you create. The number of virtual servers that you can create on a cluster is limited to the number of external independent hard disks that you have attached to the cluster and the number of storage groups that you have in each virtual server group. Each node can support up to four storage groups; however, it is recommended that you limit storage groups to three for each node for the non-failover state.

You cannot reuse any resource name in a cluster.

Important Note There can be only one public folder store in the cluster. After adding additional Exchange virtual servers, you must delete the public folder store for the new virtual server in new groups before you bring the Exchange virtual servers online.

You cannot give any single resource the same name as existing resources within the cluster.

Scaling the Exchange Store

Exchange 2000 Server introduces the concept of the Web Storage System and Information Store. The Web Storage System provides an integrated database and file-management system for storing mailboxes, public folders, e-mail, newsfeeds, and other semi-structured types of documents. With transaction-based logging technology, the Web Storage System improves reliability and reduces recovery time. The Exchange Information Store is a Windows 2000 service that manages mailbox and public folder databases, including documents, files, and applications.

Exchange 5.5 included only one central storage area. Exchange 2000 storage supports *multiple* storage units, which are called storage groups. A storage group is a collection of mailbox stores and public folder stores that use a common set of transaction log files. Each storage group has a set of one or more transaction log files for the databases it contains.

These groups can be stored locally or distributed across server clusters. Each server can hold up to four storage groups, and each storage group can hold up to five mailbox stores and public folder stores. Here are some tips for planning your storage groups:

- Create mailboxes based on resource capacity and availability.
- Do not create storage groups for each domain or for each resource. Spread storage groups and databases across multiple servers.
- Assign Active Directory resources (organizational units, users, groups, and so on) to the most available storage group within the server cluster.
- Keep storage groups small to reduce recovery time.
- Create load balancing *within* storage groups and storage databases.

For additional information about scaling and storage groups, see Appendix B, "Processor Guidelines and Scaling Scenarios."

Creating a Storage Group

Use the following procedure to create a sample storage group.
To create a sample storage group:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Open the **Servers container** in the console tree.
3. Right-click the server to which you want to add a storage group, point to **New**, and then click **Storage Group**.
4. On the **General** tab, set the name of the storage group.
5. To add additional information, on the **Details** tab, use **Administrative note**.

To create a sample mailbox store:

1. Start System Manager: On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. In the console tree, open the **Servers** container. Click the server to which you want to add the mailbox store.
3. Right-click the storage group container to which you want to add the mailbox store, point to **New**, and then click **Mailbox Store**.
4. On the **General** tab, set the following properties:
   - In **Name**, type a name for the mailbox store.
   - To change the name and location of the default public store, use **Default public store**.
5. When a message appears stating that the mailbox storage was created successfully, click **OK**.

Appendix A: Sample Zone File for Customer1.com

```
;      Zone version:  8
;

@                       IN  SOA martaduro.martaduro.com.
administrator.martaduro.com. (
                        8            ; serial number
                        900          ; refresh
                        600          ; retry
                        86400        ; expire
                        3600       ) ; minimum TTL

;
;  Zone NS records
;

@                       NS  martaduro.martaduro.com.

;
;  Zone records
;

@                       MX  10   mail.Customer1.com.
MAIL                    A   208.217.184.2
www                     A   208.217.184.3
```

Appendix B: Processor Guidelines and Scaling Scenarios

The following table contains guidelines for processors running Windows 2000 Server.

Version	Processors	RAM
Windows 2000 Server	4-way SMP	4 GB
Windows 2000 Advanced Server	8-way SMP	8 GB
Windows 2000 Data Center Server	32-way SMP	64 GB

The following table outlines the capabilities of NLBS and Microsoft Cluster Services.

Version	Network Load Balancing	Cluster Services
Windows 2000 Server	N/A	N/A
Windows 2000 Advanced Server	Yes, up to 32 servers	2-node
Windows 2000 Data Center Server	Yes, up to 32 servers	4-node

Scaling Scenarios

When choosing a server configuration, it's important to have a capacity and scalability plan based on your hosted companies' user base and transaction records. Use the following scenarios to help you determine server size, capacity, and scale.

Scenario 1: Single Server (test purposes only)

This is not a fault-tolerant configuration. In this scenario, the maximum number of storage groups is four. Because the maximum number of databases for each storage group is five, a single server can support 20 databases.

Scenario 2: Two-Server Cluster

In this scenario, the maximum number of storage groups is also four, because each active node is a mirror of the other. As in the single-server configuration, the maximum number of databases this configuration can support is 20, because the maximum number of databases for each storage group is five.
This scenario works well if you are hosting small companies with two-node server configurations.

Scenario 3: Three-Server Cluster

In this scenario, the maximum number of storage groups is six. The maximum number of databases for each storage group is five, making the maximum number of databases 30. This scenario works well if you host companies with a large number of mailboxes and public folders.
<<CREATE GRAPHIC OR SCREEN SHOT>>

Scenario 4: Four-Server Cluster

In this configuration, the maximum number of available storage groups for all three active servers is 12. Optimally, each active node runs three storage groups or a maximum of four, bringing the maximum number of databases to 60. This configuration works well for ASPs and ISPs that host companies that have a large number of mailboxes and public folders. Although this configuration is the most fault tolerant, it may also be cost-prohibitive.

Appendix C: Scripts

This section contains scripts that you can use to automate common administrative tasks. The scripts use Windows Management Instrumentation (WMI), ADSI, CDOEXM, and CDO.

Filtering Eventlog Entries

The following script subscribes to the WMI Eventlog provider and queries for messages generated when a user's mailbox goes over its size limit (error code = 8528).

```
Dim events

'basic SQL query to subscribe to the mailbox limits message

set events =
GetObject("winmgmts:{impersonationLevel=impersonate}").ExecNotificationQuer
y ("select * from __instancecreationevent where targetinstance isa
'Win32_NTLogEvent' and TargetInstance.LogFile='Application' and
TargetInstance.EventCode=8528")

'if something goes wrong give an error message

if err <> 0 then

  WScript.Echo Err.Description, Err.Number, Err.Source

End if

WScript.Echo "Waiting for Events..."

do
  set NTEvent = events.nextevent

  if error <> 0 then

    WScript.Echo Err.Description, Err.Number, Err.Source

    exit do

  else

    WScript.Echo NTEvent.TargetInstance.Message

  end if

loop

'just to let you know....

WScript.Echo "Finished!"
```

Creating a Mail-Enabled User

The following script uses ADSI to create the user and CDOEXM to create the mailbox and settings, set the virtual organization (organizational unit) that will contain the user, and set the storage group that will contain the mailbox. In this script:

- The virtual organization is called CompanyA.com.
- Data is stored in a storage group called SG A.
- The mailbox store is called CompanyA.com.

```
org="CompanyA.com"

SG="CompanyA.com,CN=SG A"

' bind to container, create user and set some (basic) settings

Set ou = GetObject("LDAP://OU=" + org + ", DC=MYNET, DC=COM")

Set usr  = ou.Create("user", "cn=JSmith")

usr.Put "samAccountName", "jsmith"

usr.givenName = "John"

usr.sn = "Smith"

usr.displayName = "John Smith"

usr.userPrincipalName = jsmith@CompanyA.com

usr.mail = JSmith@CompanyA.com

usr.SetInfo

' use CDOEXM to create mailbox, this is not possible with ADSI

' when using this script take care of the correct names !

Set objMailbox = usr

objMailbox.CreateMailbox ("LDAP://MyNet-BE/CN=" + SG +
",CN=InformationStore,CN=MyNet-BE,CN=Servers,CN=First Administrative
Group,CN=Administrative Groups,CN=MyNet ASP,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=MyNet,DC=com")

'use IMailboxStore interface from CDOEXM to set Store Limits

objMailbox.EnableStoreDefaults = FALSE

objMailbox.StoreQuota = 10000
```

```
objMailbox.OverQuotaLimit = 12000

objMailbox.HardLimit = 15000

' set password and enable account

usr.setPassword "password"

usr.AccountDisabled = False

usr.SetInfo

wscript.echo "Finished!"
```

Sending Mail

The following script uses CDO to send e-mail. You can use this script to create load on your server running Exchange.

```
for i = 1 to 1000

  set objSendMail = CreateObject("CDONTS.NewMail")

    objSendMail.From = administrator@MyNet.com

    objSendMail.To = JSmith@CompanyA.com

    objSendMail.Subject = "Sent from Script!"

    objSendMail.Body = "I sent this message from a VB Script using CDO...."

    objSendMail.Send

  set objSendMail = Nothing

Next

WScript.Echo "Sent!"
```

Querying Active Directory

The following script uses ADSI to query Active Directory for the properties of a user.

```
Dim usr

Dim MyData

Dim str


' bind to the user object
```

```
set
usr=GetObject("LDAP://CN=JSmith,OU=CompanyA.com,DC=MyNet,DC=COM")

usr.GetInfo

'count the number of properties and display the number

Number=usr.PropertyCount

WScript.Echo "There are ", Number, " properties"

' Enumerate the properties and put them in a string

str = ""

For i=1 to Number

  Set MyVar = usr.Next

  str = str + Myvar.Name + vbCrLf

Next

' Display the properties string

WScript.Echo str
```

For more information: http://www.microsoft.com/exchange/

◆ ◆ ◆ ◆