Installing Exchange Server 2010

Installing an Exchange Server is like taking a hike through the woods. If you have a map and can accurately follow the directions, you can quickly and safely arrive at your destination. If you get lost in the process (or try to "wing it") you may or may NOT reach your destination, but even if you do, it is likely that you will take a lot longer and travel over more challenging roads.

To those who have worked with Exchange Server 2007 in the past, the Exchange Server 2010 Installation Wizard will seem very familiar. The Wizard walks the administrator through the installation of several of the prerequisites and allows for the selection of specific server roles for deployment. However, the installation wizard does *not* cover all twists and turns. There are steps that must be taken to prepare the Active Directory environment and steps that must be taken to prepare the underlying operating system on the server you are installing on.

This chapter will focus on the installation process for a new Microsoft Exchange Server 2010 server in a typical configuration. In addition, this chapter assumes that the supporting infrastructure and server operating system do not exist and includes step-by-step instructions on how to install Windows Server 2008, Active Directory, supporting configuration settings, and the Exchange Server 2010 prerequisites from scratch.

Understanding the Exchange Server 2010 Server Roles

As with Exchange Server 2007, Exchange Server 2010 has various roles that can be installed on the server to perform specific functions. There are five major server roles, most of which are modular and can reside on a single server (for small environments) or be distributed to multiple servers throughout an organization.

The roles are as follows:

- ▶ Edge Transport server role
- ▶ Client Access server role
- ▶ Hub Transport server role
- ▶ Mailbox server role
- ▶ Unified Messaging server role

Edge Transport Server Role—Establishing Perimeter Security

The Edge Transport server role provides antivirus and antispam message protection for the Exchange Server infrastructure. Edge Transport servers act as message hygiene gateways and are designed to reside in a perimeter network or demilitarized zone (DMZ). This allows them to block harmful traffic *before* it reaches the corporate network.

Edge Transport servers are often utilized as the SMTP gateway for sending and receiving mail to and from the Internet.

For more information on the Edge Transport server role and details on how to install and configure the role, review Chapter 8, "Implementing Edge Services for an Exchange Server 2010 Environment."

Client Access Server Role—Providing User Connectivity

As its name suggests, a client access server is responsible for providing connectivity between the user community and their data. Like the front-end servers found in Exchange Server 2003, client access servers manage connectivity via Outlook Web Access and ActiveSync, and like the client access servers in Exchange Server 2007, they also manage connectivity from POP and IMAP users.

In Exchange Server 2010, however, the client access servers also manage MAPI (such as Outlook) client connectivity. In a pure Exchange Server 2010 environment, clients never have to connect directly to their mailbox servers—all connectivity is to the client access server.

By taking responsibility for managing these additional connections, client access servers allow Mailbox servers to focus on their primary role—processing messaging requests.

For more information on the Client Access server role and details on how to install and configure the role, review Chapter 17, "Implementing Client Access and Hub Transport Servers."

Hub Transport Servers—Routing the Mail

The Hub Transport server role is responsible for moving mail between Exchange Mailbox servers, similar to how bridgehead servers worked in the past. This role can be configured on a dedicated server or it can be deployed on an existing mailbox server.

A Hub Transport server must be deployed in each Active Directory site that contains an Exchange Server 2010 Mailbox server, as all message routing in other sites goes through one or more Hub Transport servers.

Even if the sender and recipient are on the same Mailbox server, the message will route through a local Hub Transport server. This ensures that all messages are subject to any transport rules that may be configured for the environment.

For more information on the Hub Transport server role and details on how to install and configure the role, review Chapter 17.

Unified Messaging Servers—Combining All the Data

The Unified Messaging server role was introduced with Exchange Server 2007. It acts as a gateway for combining email, voice, and fax data into a single mailbox. All this data can be accessed via the mailbox or a telephone.

For more information on the Unified Messaging server and detailed steps on installing and configuring the role, refer to Chapter 24, "Designing and Configuring Unified Messaging in Exchange Server 2010."

Mailbox Servers—What It's All About

The Mailbox server role is the core role within Exchange Server 2010. Without mailbox servers to store the user data, all of the other server roles would be without purpose.

The Mailbox servers host mailboxes and mail enabled objects such as contacts and distribution lists.

Understanding the Prerequisites for Exchange Server 2010

Before installing Exchange Server 2010, the administrator should become familiar with the prerequisites for each of the server roles. This section covers the prerequisites for the implementation of Exchange Server 2010 in a Windows networking environment.

Active Directory Infrastructure

Exchange Server 2010 relies on an Active Directory infrastructure to do its job. AD Sites and Services, DNS, Global Catalog Servers, Domain Controllers—all must be in place and configured properly for Exchange Server to function well.

The importance of each of these services, and the steps to deploy them, will be explained in greater detail later in the chapter.

Windows Server 2008—64-Bit All the Way

From inception through Exchange Server 2003, Exchange Server was always a 32-bit application. While this technology was able to handle the needs of organizations in the past, organizations today have more demanding messaging requirements.

In a world with ever-increasing message traffic, the need for highly available systems that allow access from multiple client technologies, through the Internet, and through continuous synchronization with wireless devices resulted in the desire for increased productivity through increased performance.

To address these growing needs, Microsoft released a 64-bit version of their Exchange Server 2007 server for production environments. While they still produced a 32-bit version of the product, it was intended primarily for non-production environments.

With Exchange Server 2010, 32-bit support has gone away, and the product is only being released in a 64-bit version.

By utilizing 64-bit architecture, Exchange Server has significantly enhanced processor and memory utilization. This ensures higher performance gains, the ability to handle an ever-increasing volume of messages, the capability of supporting more users per server, and more simultaneously connected mail clients. This last item is critical as more and more organizations take advantage of the capabilities of Outlook Web App (OWA) and ActiveSync.

The Exchange Server 2010 application can only be installed on a 64-bit edition of the Windows Server 2008 Service Pack 2 (or later) operating system. Either the standard or enterprise edition of Windows Server can be utilized; however, if you plan on taking advantage of some of the more advanced features of Exchange Server 2010 (such as database availability groups and mailbox database copies) you must use the Enterprise edition.

NOTE

The Exchange Server 2010 management tools can be installed on a 64-bit edition of the Windows Server 2008 Service Pack 2 (or later) operating system, or on the Windows Vista Service Pack 2 (or later) operating system.

Microsoft .NET Framework 3.5

The Microsoft .NET Framework is a Microsoft Windows component that allows the ability to build, deploy, and run Web Services and other applications. The .NET framework is a key offering from Microsoft, and most new applications created for the Windows platform rely on it in one way or another.

.Net Framework 3.5 builds on the features added in previous releases and includes service packs for both .NET Framework 2.0 and .NET Framework 3.0. Additionally, there are a number of new features which have been added.

Windows Server 2008 ships with .NET Framework 3.0 already installed. However, Exchange Server 2010 requires .NET Framework 3.5 or above. When applying updates to the Windows Server 2008 server, if you elect to apply all updates the latest version of .NET Framework will be installed. If you elect to selectively install updates, make *sure* you install this update.

Windows Remote Management 2.0

The Exchange Management Shell is a command line interface that enables you to manage your Microsoft Exchange organization without having to rely on a GUI interface.

The Windows Remote Management (WinRM) 2.0 is the transport mechanism that enables your local version of Windows PowerShell to connect to remote Exchange servers, whether that server is in the next rack or across the country. Utilizing WinRM 2.0, administrators can manage servers, devices, and applications throughout their organization from a single management server.

Windows Remote Management 2.0 can be downloaded and installed from the Internet, and instructions on how to do so are included later in this chapter.

Windows PowerShell V2

Administrators who are familiar with Exchange Server 2007 have most likely had some experience with Windows PowerShell. For many, the implementation of PowerShell addressed one of the most glaring shortcomings of older Windows installations—the lack of a usable command line interface for performing administrative tasks.

PowerShell is an extensible command-line shell and scripting language from Microsoft that integrates with the .NET Framework to allow administrators to perform just about any task in an Exchange environment from a command line. From simple to complex, scripts can be written using the PowerShell scripting language to save administrators from time consuming and repetitive tasks.

While some have found the PowerShell scripting language to be difficult to learn and challenging to implement, few who have seen the results of this product being put into action can complain about the results.

Windows PowerShell V2 introduces several new features to PowerShell 1.0 that extend its capabilities including:

▶ **PowerShell Remoting**—Allows scripts and cmdlets to be executed on a remote machine, or several remote machines

▶ **Windows PowerShell Integrated Scripting Environment (ISE)**—GUI-based PowerShell host that provides an integrated debugger, syntax highlighting, tab completion, and up to eight PowerShell consoles.

▶ **Script Debugging**—Allows breakpoints to be set in a PowerShell script or function.

▶ **Eventing**—Allows listening, forwarding, and acting on management and system events.

Windows PowerShell V2 can be downloaded and installed from the Internet, and instructions on how to do so are included later in this chapter.

Microsoft Management Console 3.0

The Microsoft Management Console (MMC) was originally released back in 1996 with the Windows NT 4.0 Option Pack. This was the first time Microsoft released a consistent and integrated management tool that aimed at standardizing the way administrators conducted administrative and operational tasks on Microsoft software. Since 1996, Microsoft has been updating and improving its management console and releasing new versions.

The Exchange Server 2010 Management Console utilizes MMC 3.0, but as Windows Server 2008 ships with the product already installed, it is not listed as a prerequisite and you do not have to install it separately.

Internet Information Services (IIS) 7.0

Internet Information Services (IIS) remains a critical component that allows users to connect to Exchange services over the Internet using Outlook Web App (OWA), Outlook Mobile Access (OMA) and ActiveSync.

As with the MMC above, IIS 7.0 is installed by default with Windows Server 2008.

Understanding High Availability and Site Resilience in Exchange Server 2010

In Exchange Server 2007, Microsoft introduced new technologies that allowed organizations to deploy their Exchange environments with improved availability. Known as "Continuous Replication," this technology was offered in three flavors—Local Continuous Replication (LCR), Cluster Continuous Replication (CCR), and Standby Continuous Replication (SCR).

Although these options were a significant improvement over previous technologies, organizations found that the technologies were challenging to implement, as they required a significant amount of time and experience to deploy. This was largely due to the fact that some parts of the technology were owned by the Windows operating system, and some parts were owned by Exchange Server.

Exchange Server 2010 has built on these technologies and combined the on-site data replication features of CCR with the off-site data replication features of SCR. This combination of technologies is known as a database availability group (DAG). This architecture is designed to provide recovery from disk-level, server-level and site-level failures.

A few characteristics of Mailbox Database copies follow:

▶ Designed for mailbox databases only. Public folder replication is still the preferred method of redundancy and high availability for public folders.

▶ Up to 16 copies of a mailbox database can be created on multiple servers.

▶ Mailbox servers in a DAG can host other Exchange Server roles (Client Access, Hub Transport, and Unified Messaging).

▶ Exchange Server 2010 mailbox databases can only be replicated to other Exchange Server 2010 servers within a DAG. You cannot replicate a database outside of the DAG, or to an Exchange Server 2007 server.

Exchange Server 2010 Hardware Requirements

Microsoft maintains a list of minimum hardware requirements to install Exchange Server 2010. For the latest list of requirements, go to http://technet.microsoft.com and search for "Exchange 2010 System Requirements."

Table 7.1 shows the minimum and recommended hardware requirements for Exchange Server 2010, as stated by Microsoft.

TABLE 7.1   Minimum Hardware Requirements

Hardware	Minimum Requirements
Processor	X64 architecture-based computer with Intel Processor that supports Intel 64 Intel Extended Memory 64 Technology (formerly known as Intel EM64T)
	AMD processor that supports AMD64 platform
	Note—Intel Itanium IA64 processors are NOT supported.

TABLE 7.1   Minimum Hardware Requirements

Hardware	Minimum Requirements
Memory	Edge Transport Server—Minimum: 2GB. Maximum: 16GB. **Recommended:** 1GB per core (2GB Minimum, 8GB Maximum) Hub Transport Server—Minimum: 2GB. Maximum: 16GB. **Recommended:** 1GB per core (2GB Minimum, 8GB Maximum) Client Access Server—Minimum: 2GB. Maximum: 16GB. **Recommended:** 2GB per core (8GB Minimum, 16GB Maximum) Unified Messaging Server—Minimum: 4GB. Maximum: 8GB. **Recommended:** 1GB per core (4GB Minimum, 8GB Maximum) Mailbox Server—Minimum: 2GB. Maximum: 64GB. **Recommended:** 2GB plus 2-4MB per mailbox Multiple Roles (combinations of Hub Transport, Client Access, and Mailbox Server Roles)—Minimum: 4GB Maximum: 64GB. Recommended: 8GB plus 2-4MB per mailbox.
Disk space	At least 1.2GB on the hard disk where Exchange Server 2010 will be installed. An additional 500MB for each Unified Messaging language pack that will be installed. 200MB on the system drive. A hard disk drive that stores the message queue databases on an Edge Transport server or Hub Transport server with at least 500MB.

> **NOTE**
>
> These hardware requirements from Microsoft are the bare minimum and should not be used in best-practice scenarios. In addition, hardware requirements can change because of features and functionality required by the company, for example, the implementation of Unified Messaging voice mail services or clustering on an Exchange Server 2010 server can require more memory. See Chapter 34, "Optimizing an Exchange Server 2010 Environment," for more tips and best practices on sizing the server for your environment.

Understanding the Active Directory Requirements for Exchange Server 2010

An Active Directory (AD) infrastructure running on Windows Server 2003 or Windows Server 2008 must be in place before an organization can deploy Exchange Server 2010. Exchange Server depends on the services provided by AD to successfully function and the design and implementation of the AD environment can have an enormous impact on the success of the Exchange Server deployment. Mistakes made in the planning or implementation of AD can be costly and difficult to correct later.

If AD is already deployed, it is important that the team designing the Exchange Server infrastructure have a solid understanding of the existing AD environment. Organizations with an AD infrastructure already in place need to evaluate how Exchange Server can fit into their environment. If AD has not been deployed, the organization or team designing Exchange Server needs to plan their implementation with a thought as to what their messaging infrastructure will look like.

This section is designed to give a basic understanding of the AD infrastructure required to support an Exchange Server 2010 implementation. Many facets are involved when planning a production AD infrastructure—forest model, domain model, group policies, and delegation of administration to name a few, and the information needed to design an AD infrastructure from end to end is beyond the scope of this book.

Some of the AD factors that should be considered when deploying Exchange Server 2010 include the following:

▶ Global Catalog Server Placement

▶ AD Sites and Services

▶ Forest and Domain Functional Levels

▶ Flexible Single Master Operations Role Placement

▶ Permissions Needed to Install Exchange

▶ Bandwidth and Latency in the Network

NOTE

For in-depth guidance on designing, implementing, and maintaining an AD infrastructure, refer to *Windows Server 2003 Unleashed, R2 Edition*, by Sams Publishing (ISBN: 0-672-32898-4), or *Windows Server 2008 Unleashed*, by Sams Publishing (ISBN: 0-672-32930-1).

Global Catalog Server Placement

As was the case in Exchange 2000 Server through Exchange Server 2007, Exchange Server 2010 requires a global catalog infrastructure to function. The global catalog maintains an index of the Active Directory database for objects within its domain. Additionally, it stores partial copies of data for all other domains within a forest.

Just as important, Exchange Server relies on global catalog servers to resolve email addresses for users within the organization. Failure to contact a global catalog server causes emails to bounce, as the recipient's name cannot be resolved.

Sizing a global catalog infrastructure and server placement is discussed in depth later in this chapter in the section entitled "Establishing a Proper Global Catalog Placement Strategy."

Active Directory Sites and Services

In Exchange Server 2003 and earlier, Exchange Server utilized dedicated routing topology for transporting messages throughout the organization. Beginning with Exchange Server 2007, Microsoft redesigned the product to be a "site-aware" application. This continues in Exchange Server 2010.

Site-aware applications are able to determine what site they (and other servers) belong to by querying Active Directory. The site attribute of all Exchange server objects is maintained by the Microsoft Exchange Active Directory Topology Service. Additionally, Exchange Server 2010 servers utilize site membership to identify which Domain Controllers and Global Catalog servers should be utilized to process Active Directory queries.

The Exchange Server 2010 servers utilize Active Directory site membership as follows:

Hub Transport Servers—Gather information from Active Directory to determine mail routing inside the organization. When a message hits the Microsoft Exchange Transport service, the Hub Transport server resolves the recipient's information and queries Active Directory to match an email address to the recipient's account. The result of this query includes the fully qualified domain name (FQDN) of the user's mailbox server.

From the FQDN, the AD site of the recipient's Mailbox server is determined and, if the Mailbox server is in the same site as the Hub Transport server, the message is delivered. If the Mailbox server is in another site, the message is relayed to a Hub Transport server in that site, and the message is then delivered to the user's mailbox server.

Client Access Servers—When a client access server receives a connection request from a user, it contacts AD to determine which mailbox server houses the user's mailbox and which site that server belongs to. If the mailbox server is in a different site, the connection is redirected to a client access server in the same site as the mailbox server.

Mailbox Servers—Query Active Directory to determine which Hub Transport servers are located in their site. Messages are submitted to local Hub Transport servers for routing and transport.

Unified Messaging Servers—Utilize Active Directory site membership information to determine what Hub Transport servers are located in the same site as the UM server. Messages for routing and transport are delivered to a Hub Transport server in the same site as the UM server.

Forest and Domain Functional Levels

With each new edition of the Windows Server and Exchange Server operating systems, new functionalities are introduced. Some of these enhancements require that the Active Directory infrastructure be upgraded before you can take advantage of the new capabilities. At times, these capabilities cannot be implemented until all domain controllers in an environment have been upgraded to the same level.

To support this, Active Directory has Forest and Domain functional levels that determine what enhancements are enabled or disabled. By raising the functional level of

an environment, new functionalities are enabled. By maintaining an older functional level, interoperability with older domain controllers is supported.

Forest Functional Levels

Windows Server 2003 supports three forest functional levels:

▶ **Windows 2000 Native**—Required while any Windows Server 2000 domain controllers remain in your forest. Supports domain controllers running Windows NT 4.0, Windows 2000 server, and Windows Server 2003.

▶ **Windows Server 2003 Interim**—A special functional level only implemented during NT 4.0 to Windows 2003 upgrades.

▶ **Windows Server 2003**—All DCs in the forest must be running Windows Server 2003, and all domains in the forest must be at the Windows 2003 Domain functional level before you can raise your forest functional level to Windows Server 2003.

Windows Server 2008 supports three forest functional levels:

▶ **Windows 2000 Native**—Supports Windows 2000, Windows Server 2003, and Windows Server 2008 domain controllers.

▶ **Windows Server 2003**—Allows for a mix of Windows Server 2003 and Windows Server 2008 functional level domains.

▶ **Windows Server 2008**—Ensures all domain controllers in the forest are running Windows Server 2008 and all domains have been raised to the Windows Server 2008 domain functional level.

> **NOTE**
>
> To install Exchange Server 2010, the Active Directory forest functional level MUST be Windows Server 2003 or higher.
>
> Windows 2000 Native and Windows Server 2003 Interim modes are NOT supported.

7

Domain Functional Levels

Windows Server 2003 supports four domain functional levels:

▶ **Windows 2000 Mixed**—Allows Windows Server 2003 domain controllers to interoperate with other domain controllers running Windows Server 2003, Windows 2000 Server, and Windows NT 4.0.

▶ **Windows 2000 Native**—Allows domain controllers running Windows Server 2003 to interact with domain controllers running either Windows Server 2003 or Windows 2000 Server.

▶ **Windows Server 2003 Interim**—Supports only domain controllers running Windows Server 2003 and Windows NT 4.0.

▶ **Windows Server 2003**—Supports only Windows Server 2003 domain controllers.

Windows Server 2008 supports three domain functional levels:

- ▶ **Windows 2000 Native**—Allows domain controllers running Windows Server 2008 to interact with domain controllers running either Windows Server 2008, Windows Server 2003, or Windows 2000 Server.

- ▶ **Windows Server 2003**—Supports an environment comprised of a mixture of Windows Server 2003 and Windows Server 2008 domain controllers.

- ▶ **Windows Server 2008**—Only available after all domain controllers in a domain are running Windows Server 2008.

NOTE

To install Exchange Server 2010, the Active Directory domain functional level MUST be Windows Server 2003 or higher for each domain in the Active Directory forest that will house an Exchange Server 2010 server.

Windows 2000 Mixed, Windows 2000 Native, and Windows Server 2003 Interim modes are NOT supported.

Understanding Flexible Single Master Operations Roles

Active Directory uses a multimaster replication scheme for replicating directory information between domain controllers; however, certain domain and enterprise wide operations are not well suited for a multimaster model. Some services are better suited to a single master operation to prevent the introduction of conflicts while an Operations Master is offline. These services are referred to as Operations Master or Flexible Single Master Operations (FSMO) roles.

FSMO roles can be either "forestwide" or "domainwide." The forestwide roles consist of the Schema Master and the Domain Naming Master. The domainwide roles consist of the Relative ID (RID) Master, the Primary Domain Controller (PDC) Emulator, and the Infrastructure Master. A brief description of each is as follows:

- ▶ **Schema Master**—Maintains all modifications to the schema throughout the Active Directory forest, as no other domain controller is allowed to write to the schema. The schema determines what types of objects are permitted in the forest and the attributes of those objects.

- ▶ **Domain Naming Master**—Maintains a list of the names of all domains in the forest and is required to add any new domains (or to remove existing ones).

- ▶ **RID Master**—Allocates security RIDs to domain controllers to assign to new AD security users, groups, or computer objects. RIDs are the part of the Security Identifier (SID) that identifies an account or group within a domain. The RID master also manages objects moving between domains.

- ▶ **PDC Emulator**—Processes all password changes in the domain. If a user logon attempt fails due to a bad password, the request is forwarded to the PDC emulator to check the password against the most recent one. This allows a user to log in

immediately after a password change instead of having to wait for that change to replicate throughout the active directory.

▶ **Infrastructure Master—**Maintains security identifiers, GUIDs, and DNS for objects referenced across domains. This role is also responsible for ensuring that cross-domain group-to-user references are correctly maintained.

When designing the FSMO role placement of an Active Directory environment, the following best practices should be considered:

▶ If a domain has only one domain controller, that domain controller holds all the domain roles. However, this configuration is not recommended (even for smaller organizations), as it creates a single point of failure.

▶ The Schema Master and Domain Naming Master should be placed on the same domain controller in the root or placeholder domain. This server can (and should) also be configured as a global catalog server.

▶ Place the RID and PDC emulator roles on the same domain controller. If the load on this server justifies separating the roles, place them on domain controllers in the same domain and AD site and ensure the two domain controllers are direct replication partners of each other.

▶ As a general rule, the infrastructure master should be deployed on a domain controller that is NOT also a global catalog server. This domain controller should have a direct connection to a GC server, preferably in the same Active Directory site. Global catalog servers hold a partial replica of every object in the forest and the infrastructure master, when placed on a global catalog server, will never update anything as it does not contain any references to objects that it does not hold. There are two exceptions to this rule:

   1. Single domain forest: In a forest with a single AD domain, there are no phantoms and the infrastructure master has no work to do. In this case, the infrastructure master can be placed on any domain, including those that are also global catalog servers.

   2. Multidomain forests where *every* domain controller is a global catalog server. When *every* domain controller in a domain that is part of a multidomain forest is configured as a global catalog server, there are no phantoms or work for the infrastructure master to do. The infrastructure master can be placed on any domain controller in the domain.

NOTE

As stated by Microsoft, to install Exchange Server 2010, the Schema master should have "the latest 32-bit or 64-bit edition of the Windows Server 2003 Standard or Enterprise operating system or the latest 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise operating system."

Additionally, in each Active Directory site where you plan to install Exchange Server 2010, you must have at least one Global Catalog server that meets the same criteria.

Understanding How DNS and AD Namespace Are Used in Exchange Server 2010

The first step in the actual design of the AD structure is the decision on a common domain name system (DNS) namespace that AD will occupy. AD revolves around (and is inseparable from) DNS and this decision is one of the most important ones to make. The namespace chosen can be as straightforward as companyabc.com, for example, or it can be more complex. Multiple factors must be considered, however, before this decision can be made. Is it better to register an AD namespace on the Internet and potentially expose it to intruders, or is it better to choose an unregistered, internal namespace? Is it necessary to tie in multiple namespaces into the same forest? These and other questions must be answered before the design process can proceed.

Impact Forests Have on an Exchange Server 2010 Design

An AD forest and an Exchange Server organization are tightly integrated. Exchange Server relies on AD as its directory repository for mailboxes, mail-enabled objects, Exchange servers, and much more. An AD forest can only host a single Exchange organization and an Exchange organization can only span one AD forest.

It is recommended that a single AD forest should be utilized to minimize complexity and administration when designing and implementing a company's Exchange Server implementation. However, there will be times when a single AD forest will not meet the company's business, security, or political requirements.

If multiple AD forests are necessary to satisfy the company's requirements, it must be decided on which forest the Exchange organization will be hosted. It is possible to have an Exchange Server reside in a single forest, a dedicated resource forest, or to implement multiple Exchange organizations in multiple forests.

The Role of a Domain in Exchange Server 2010

After the AD forest structure has been laid out, the domain structure can be contemplated. Unlike the forest structure, an Exchange Server 2010 organization can span multiple domains within the forest if needed. Therefore, a user mailbox, Exchange server, or other Exchange object can reside in any domain within the forest where Exchange Server 2010 has been deployed. A company can plan its domain model structure (single domain model or multiple domain model) based on their business and security requirements without a direct negative impact to the Exchange Server 2010 design.

While a single domain model is often considered due to its simplicity, most organizations prefer the placeholder domain model. The placeholder domain model has an isolated domain serving as the root domain in the forest. The user domain, which contains all production user accounts, would be located in a separate domain in the forest, as illustrated in Figure 7.1.
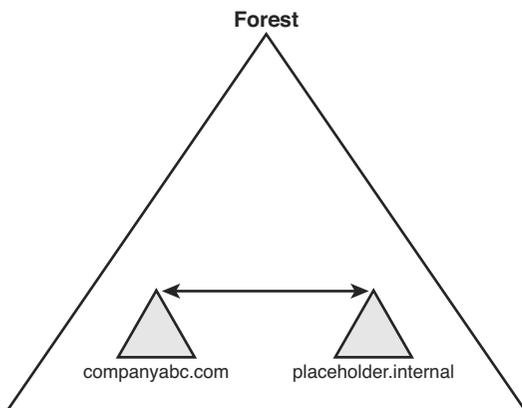
FIGURE 7.1   The placeholder domain model.

The placeholder domain structure increases security in the forest by segregating high-level schema-access accounts into a completely separate domain from the regular user domain. Access to the placeholder domain can be audited and restricted to maintain tighter control on the critical schema. The downside to this model, however, is the fact that the additional domain requires a separate set of domain controllers, which increases the infrastructure costs of the environment. Smaller organizations may have a difficult time justifying the extra infrastructure costs to provide the increased security, but whenever the budget allows, this model should definitely be considered.

Planning a Proper Sites and Services Architecture

As stated earlier, one of the major features of Exchange Server 2007 and Exchange Server 2010 is the ability to natively utilize Active Directory Sites and Services for routing mail, rather than having to implement and maintain an independent routing topology using connectors. To take advantage of this capability, you must first remove all pre-Exchange Server 2007 servers from your environment.

If Exchange Server 2010 will be installed into an existing Exchange Server 2003 organization, the administrators must configure routing group connectors to ensure that the Exchange Server 2010 servers are communicating to legacy servers.

For more information on coexistence of Exchange Server 2010 with legacy versions, review Chapter 15, "Migrating from Active Directory 2000/2003 to Active Directory 2008."

Administrators should be aware of the best practices for designing a proper Sites and Services architecture to support Exchange Server 2010. From a high-level perspective, within AD it is necessary for administrators to create sites, allocate subnets to sites, and then create site links between sites for communication to occur. Similar to Exchange 2000 and 2003, it is possible to set up redundant links between sites and allocate costs to control communication priorities.

Active Directory Sites

The basic unit of AD replication is known as the site. Not to be confused with physical sites or Exchange Server 5.5 sites, the AD site is simply a group of domain controllers connected by high-speed network connections. Each site is established to more effectively replicate directory information across the network. In a nutshell, domain controllers within a single site will, by default, replicate more often than those that exist in other sites. The concept of the site constitutes the centerpiece of replication design in AD.

Associating Subnets with Sites

In most cases, a separate instance of a site in AD physically resides on a separate subnet from other sites. This idea stems from the concept that the site topology most often mimics, or should mimic, the physical network infrastructure of an environment.

In AD, sites are associated with their respective subnets to allow for the intelligent assignment of users to their respective domain controllers. For example, consider the design shown in Figure 7.2.
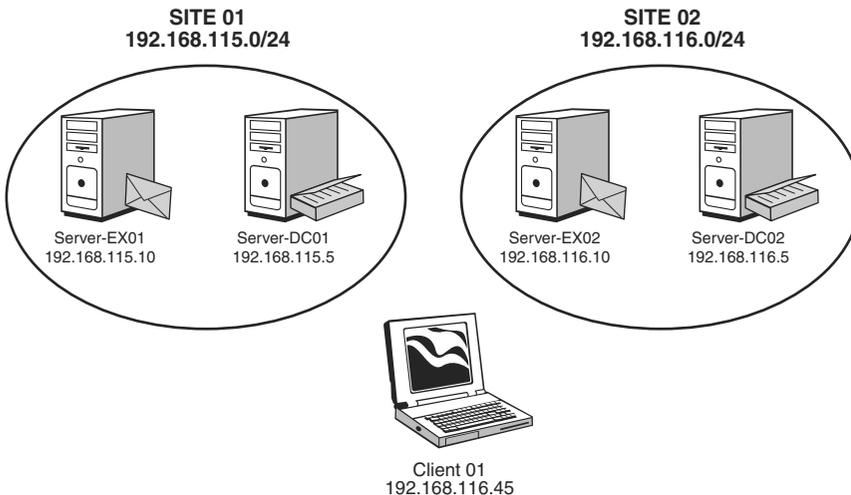
FIGURE 7.2   Sample Exchange Server and Client site assignment.

In this example, Server-EX01 is a physical member of the 192.168.115.0/24 subnet. Server-EX02 and Client01 are both members of the 192.168.116.0/24 subnet. Based on the subnets, Server-EX01 will automatically be assigned to the domain controller Server-DC01 in SITE01 and Server-EX02 and Client01 will be assigned to the domain controller Server-DC02 in SITE02.

Using Site Links

By default, the creation of two sites in AD does not automatically create a connection linking the two sites. This type of functionality must be manually implemented by the creation of a "site link."

A site link is essentially a connection that joins together two sites and allows for replication traffic to flow from one site to another. Multiple site links can be set up and should normally follow the wide area network (WAN) lines of your organization. Multiple site links also assure redundancy so that if one link goes down, replication traffic has an alternate path.

Site link replication schedules can be modified to fit the requirements of your organization. If, for example, the WAN link is saturated during the day, a schedule can be established to replicate information at night. This functionality allows you to easily adjust site links to the needs of any WAN design.

Exchange Server 2010 and Site Membership

After the AD site topology has been created, including adding the appropriate subnets to sites and creating site links between sites, an administrator can now take Exchange Server placement into consideration.

Similar to AD domain controllers, Exchange Server 2010 servers will be associated with sites in AD based on their IP address and subnet mask. As stated earlier, there should be at least one domain controller/global catalog server residing in each site that an Exchange Server 2010 server will be in.

For more information on creating an Exchange Server routing topology, refer to Chapter 4, "Architecting an Enterprise-Level Exchange Server Environment."

> **NOTE**
>
> If an AD infrastructure already exists prior to the design of the Exchange Server 2010 environment, there might be a need to make changes to the AD routing topology to support the Exchange routing requirements.

Establishing a Proper Global Catalog Placement Strategy

Another area of importance is the design and placement of global catalog servers within the environment. The importance of the global catalog server cannot be overstated. The global catalog is used for the address list that users see when they are addressing a message and by Exchange servers every time a message is delivered. If a global catalog server is not available, the recipient's address will not resolve when users address a message, and the message cannot be delivered.

There should be at least one global catalog server in every AD site that contains an Exchange Server 2010 server. The recommendation from Microsoft is as follows:

If Active Directory is running on a 32-bit system, the recommendation is 4:1—for every four processor cores in your mailbox servers, you should have one processor core in a global catalog server. For example, if you have 2 mailbox servers, each with dual quad-core processors, that is 16 processor cores. You should have at least 4 processor cores worth of global catalog computing, so 1 quad core server, or 2 dual core servers should do the trick.

If Active Directory is running on a 64-bit system, the recommended ratio is 1:8. However, you must have enough memory installed on the server to cache the entire Active

Directory database in memory. To confirm the size of your Active Directory database, look at the size of the `%WINDIR%\NTDS\NTDS.DIT` file.

For optimization, plan on having a global catalog server close to the clients to provide efficient address list access. Making all domain controller servers global catalog servers is recommended for an organization that has a single AD domain model and a single site. Otherwise, for multidomain models, all domain controllers can be configured as global catalog servers *except* for the domain controller hosting the Infrastructure Master FSMO role.

> **NOTE**
>
> It is a best practice to have a minimum of at least two global catalog servers within an AD infrastructure.

Understanding Role Based Access Control

Exchange Server 2010 uses the new *Role Based Access Control* (RBAC) permissions model on the Mailbox, Hub Transport, Unified Messaging, and Client Access server roles. At first glance, this RBAC may seem very similar to the Exchange Server 2007 server permissions model, but it actually allows for much greater flexibility.

Using RBAC allows you to easily control what your administrators and users can (and cannot) access. Rather than applying permissions directly to user accounts, the permissions are applied directly to the role. Members are added to a particular role when they need a particular level of permissions.

In addition, role assignments can be "scoped" to include only specific resources within the organization. The role (and the permissions associated with it) allows certain tasks to be accomplished, while the role scope determines what resources can be administered.

The RBAC model consists of:

- ▶ **Management Role**—A container for grouping management role entries.

- ▶ **Management Role Entries**—A cmdlet (including parameters) that is added to a management role. This process grants rights to manage or view the objects associated with that cmdlet.

- ▶ **Management Role Assignment**—The assignment of a management role to a particular user or a universal security group. This grants the user (or the members of the security group) the ability to perform the management role entries in the management role that they are assigned to.

- ▶ **Management Role Scope**—Used to target the specific object or objects that the management role assignment is allowed to control. A management role scope can include servers, organizational units, filters on server or recipient objects, and more.

As described by Microsoft, this process allows complete control of the *who* (management role assignment), the *what* (management role and management role entries), and the *where* (management role scope) in the security model.

Role Based Access Control is *not* used on Edge Transport servers, as these servers are designed to sit outside the domain.

Exchange Server 2010 provides several built-in management roles that cannot be modified, nor can the management role entries configured on them. However, the *scope* of the built-in management roles can be modified.

The following built-in management roles are included by default in Exchange Server 2010:

▶ **Organization Management**—Administrators assigned to this role have administrative access to the entire Exchange Server 2010 organization, and can perform almost any task against any Exchange Server 2010 object. Even if a task can only be completed by another role, members of the Organization Management role have the ability to add themselves to any other role.

As this role is very powerful, it is recommended that it only be assigned to users who are responsible for organizational level administration. Changes made by this role can potentially impact the entire Exchange organization.

▶ **View Only Organization Management**—This role is the equivalent to the Exchange View-Only Administrator role in Exchange Server 2007. Members of this role can view the properties of any object in the Exchange organization, but cannot modify the properties of any object.

Useful for personnel who need to be able to view the configuration of objects within the environment, but who do not need the ability to add new or modify existing objects.

▶ **Recipient Management**—Administrators assigned to this role have the ability to create, modify, or delete Exchange Server 2010 recipients within the organization.

▶ **Records Management**—Administrators assigned to this role have the ability to configure compliance features, including transport rules, message classifications, retention policy tags, and others.

Often assigned to administrators or members of an organization's legal department who need the ability to view and modify compliance features in an organization.

▶ **GAL Synchronization Management**—Administrators assigned to this role have the ability to configure global address list (GAL) synchronization between organizations.

Other built-in management roles include the Unified Messaging Management, Unified Messaging Recipient Management, Unified Messaging Prompt Management, and Discovery Management.

7

NOTE

Membership in the Organization Management Role should be limited to personnel who have advanced knowledge of the Exchange Server operating system and your particular network environment.

Planning Your Exchange Server 2010 Installation

Before installing Exchange Server, you should review the following chapters earlier in this book:

Chapter 1, "Exchange Server 2010 Technology Primer" covers what is new in Exchange Server 2010 and differences between the available versions.

Chapter 2, "Planning, Prototyping, Migrating, and Deploying Exchange Server 2010."

Chapter 3, "Understanding Core Exchange Server 2010 Design Plans."

Chapter 4, "Architecting an Enterprise-Level Exchange Server Environment" addresses the planning and design of an Exchange Server 2010 implementation for a small, medium, or large enterprise organization.

From these chapters, you will learn the industry best practices and recommendations for planning and deploying Exchange Server 2010.

Installing Exchange Server 2010 in a Test Environment

To reduce risks, prevent end-user downtime, and minimize the exposure of the production environment, it is typically recommended that the first implementation of Exchange Server 2010 be conducted in an isolated test lab rather than being installed into a production environment.

Having a test environment isolates functional errors so that if there are any problems they will not be injected into the existing production environment. In addition, the test environment acts as a "Proof of Concept" for the new Exchange Server 2010 design.

Occasionally, organizations attempt to repurpose their test environments into their production environment. Administrators should be cautious, as "shortcuts" are sometimes taken in the lab—the use of evaluation copies of software and/or underpowered hardware may work flawlessly in the lab, but transitioning the equipment to production results in inadequate performance and unnecessary downtime.

Production equipment should be rebuilt and deployed from scratch, not "moved" from a test environment.

Prototyping an Exchange Server 2010 Installation

Some of the steps an organization should go through when planning to build a test Exchange Server environment include the following:

▶ Building Exchange Server 2010 in a lab

▶ Testing email features and functionality

▶ Reviewing Exchange Server 2010 server roles

▶ Verifying design configuration

▶ Testing failover and recovery

▶ Selecting to install on physical hardware or virtual machines

Much of the validation and testing should occur during the testing process. It is much easier, for example, to test a disaster recovery rebuild of Exchange Server in an exclusive test environment than it is to do so in a production environment, where production servers or users could accidentally be impacted.

Additionally, testing application compatibility in a lab environment can be much more effective than attempting to do so in a production environment, where you might suddenly find business critical third-party fax, voice mail, or paging software non functional.

Other items to test and confirm in your lab environment include:

▶ **Sites and Services Configuration**—Ensure replication is completed as expected

▶ **Role Based Access Control**—Ensure the proposed security settings allow proper user and administrative access

Building an Exchange Server 2007 prototype test lab can be a costly affair for companies that want to simulate a large, global implementation. For companies with a global presence where it is necessary to provide messaging services for thousands of employees, in multiple sites throughout the world, mirroring their production site can prove a daunting task. However, without successfully prototyping the installation, upgrade strategy, and application compatibility before they move forward in production, they cannot be assured that the deployment will go smoothly.

The cost of building a lab of this magnitude using physical servers can be prohibitive; there can be AD domain controllers, Exchange 2003 and 2007 servers, and application servers. The cost of building the lab could eat up a large part of the overall budget allocated to the project.

However, with the improvements in server virtualization, companies can significantly lower the costs associated with the prototype phase. Server virtualization enables multiple virtual operating systems to run on a single physical machine, while remaining logically distinct with consistent hardware profiles. For further cost savings, the hardware utilized for the virtual lab can be purchased with an eye toward re-utilization in the production environment once the prototype phase is complete.

Upgrading from Previous Versions of Microsoft Windows

Many organizations already have an existing directory structure in place. It is great if a company has the opportunity to implement a new Windows Server 2003 or Windows Server 2008 AD environment from scratch; however, this is not usually possible for environments with previous versions of Exchange Server deployed.

When upgrading an existing Active Directory infrastructure, the deployment plan should be carefully thought out and tested before implementation in the production environment.

Deploying Active Directory from Scratch

Before installing Exchange Server 2010, there must be an existing Active Directory environment to support it. The environment can be running on either a Windows Server 2003 or Windows Server 2008 platform. The following sections will focus on the steps needed to install an Active Directory environment on a Windows Server 2008 platform from scratch. This example can be followed in a lab environment to prepare it for the deployment of Exchange Server 2010.

This sample deployment will consist of a single site and single domain controller, as might be found in a small organization. The steps we will deploy include:

▶ Installing the Windows Server 2008 operating system

▶ Promoting a Windows Server 2008 Server to a domain controller

▶ Configuring Active Directory Sites and Services

▶ Configuring a global catalog server

Installing the Windows Server 2008 Operating System

Microsoft Exchange Servers rely heavily on the Active Directory environment they are installed in.

For those experienced with installing previous versions of the Windows Server operating system, most of the concepts covered in this section will feel very familiar. The installation of Windows Server 2008 is straightforward, and takes approximately 30 minutes to an hour to complete. The following procedure is based on installing Windows Server from the standard media provided by Microsoft. Many hardware manufacturers include special installation instructions and procedures specific to their hardware platform, but the concepts should be roughly the same.

For our test lab, we will install Windows Server 2008 Enterprise Edition on two machines. One will be promoted later in the chapter to a domain controller. The other will have the Exchange Server 2010 software installed on it.

To install Windows Server 2008 (Standard or Enterprise Edition) perform the following steps:

1. Insert the Windows Server 2008 CD into the CD drive.

2. Power up the server and let it boot to the CD-ROM drive. If there is currently no operating system on the hard drive, it automatically boots into the CD-ROM-based setup.

3. Select the language you wish to install, the Time and Currency Format, and the Keyboard or input method. When ready, click Next to continue.

4. Click Install Now.

5. Select which version of the Windows Server 2008 Operating system you wish to install. For this example, we will be installing Windows Server 2008 Enterprise (Full Installation) on a 64-bit platform. When ready, click Next to continue.

6. Review the Microsoft Software License Terms, click the "I accept the license terms" check box, and click Next to continue.

7. Select Custom (advanced) to install a clean copy of Windows.

8. Select the physical disk on which Windows will be installed and click Next to continue.

The server will begin the installation process, rebooting several times during the process.

1. A default account called Administrator will be created, but you will have to set the password for this account. When prompted The User's Password Must Be Changed Before Logging on the First Time, click OK to continue.

2. Enter the new password for the Administrator account in both the New password and Confirm password fields, and then press Enter. When prompted Your password has been changed, click OK.

Once the installation process has completed and the server reboots, there will be an Initial Configuration Tasks screen. Perform the steps in the Provide Computer Information section as follows:

Set Time Zone

1. Click Set Time Zone. On the Date and Time tab, review the current Date, Time, and Time zone settings and configure them as needed.

2. If desired, up to two additional clocks can be configured for additional time zones with customized display names. If you wish to display more than one clock, select the Additional Clocks tab and configure them.

3. By default, Windows Server 2008 servers are configured to automatically synchronize with time.windows.com. The server is configured to synchronize once a week. If you need to change the source of your time updates, you can click the Internet Time tab.

4. Click OK to return to the Install Configuration Tasks screen.

Configure Networking

Windows Server 2008 has a completely redesigned implementation of the TCP/IP protocol stack which is known as the "Next Generation TCP/IP stack." This updated functionality applies to both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

1. Click Configure networking, double-click the Local Area Network Connection icon, and then click the Properties tab.

2. Double-click the Internet Protocol Version 4 (TCP/IPv4) option and configure an appropriate IP address, Subnet mask, Default gateway, and preferred DNS server for your environment.

3. Click OK to save your changes.

4. Perform the same steps to configure the Internet Protocol Version 6 (TCP/IPv6).

5. Save all settings and exit the Network Connections utility.

6. Launch Internet Explorer and confirm internet connectivity. Adjust your network settings if necessary to allow the computer access to the Internet.

Provide Computer Name and Domain

Each computer on a Windows network and in Active Directory must have a unique computer name. This name, known as the NetBIOS name, allows users, resources, and other computers to contact this computer on the network.

A standard NetBIOS name is limited to 15 characters and should only consist of letters (A-Z, a-z), digits (0-9), and hyphens (-). For example, weinhardt-dc is a standard computer name, but weinhardt_dc is nonstandard. Although the implementation of a DNS server will allow you to use nonstandard computer names and still find the resources in your environment, servers as critical as domain controllers and Exchange servers should only use standard computer names.

1. Click Provide Computer Name and Domain. If you have already closed your Initial Configuration Tasks screen, you can click Start, right-click Computer, select Properties; then, beside Computer Name, Domain, and Workgroup Settings, click Change Settings.

2. On the Computer Name tab, click Change.

3. Under Computer name, enter the computer name for this machine; then click OK to continue.

4. Acknowledge that you must restart your computer to apply these changes by clicking OK, and then click Close.

5. When prompted You Must Restart Your Computer, click Restart Now.

Enable Automatic Updating and Feedback

Windows Server allows you the option of automatically applying updates as they are released from Microsoft. While this option may be a good idea for some applications, most organizations require change control procedures before updating servers as business critical as domain controllers and Exchange servers.

1. Click on Enable Automatic Updating and Feedback. Although the first option, Enable Windows Automatic Updating and Feedback, states that it is "recommended," in this author's opinion, that setting is NOT recommended for domain controllers or Exchange servers. Instead, click on Manually Configure Settings.

2. Under Windows Automatic Updating, click Change Setting. Set the automatic updates according to your organization's policies. The author recommends selecting either Download Updates but Let Me Choose Whether to Install Them or Check for Updates but Let Me Choose Whether to Download and Install Them. Additionally, the author recommends Include Recommended Updates When Downloading, Installing, or Notifying Me about Updates, as shown in Figure 7.3.

3. When ready, click OK to continue.

4. Review the Windows Error Reporting and Customer Experience Improvement Program settings. The author recommends the default settings, as shown in Figure 7.4. When finished, click Close to continue.

5. Click Download and Install Updates; if prompted to Install new Windows Update Software, click Install Now. As part of the installation process, the Windows Updates application will automatically close and reopen and begin checking for updates.
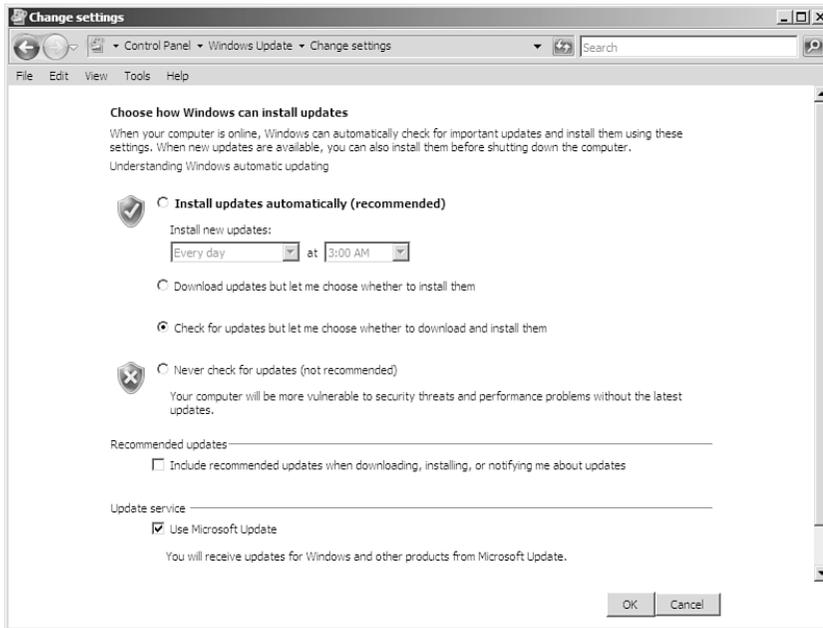
FIGURE 7.3   Configuring automatic updates.
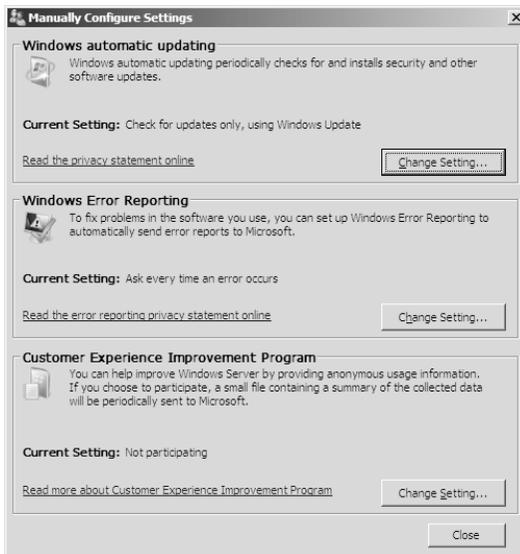
FIGURE 7.4   Configuring Windows Error Reporting and Customer Experience Improvement Program.

6. At this point, you can either click View Available Updates and select which ones to install or simply click Install Updates to automatically download and install all available updates.

7. Accept any license agreements and click Finish to begin installing available updates. Monitor the installation, as you may have additional prompts from the installation process. When finished, if a restart is required, click Restart Now.

8. When the server has rebooted, log on again and return to the Download and Install Updates section.

9. Click the option to Get Updates for More Products.

10. From the Microsoft Update site, place a check mark in the I Accept the Terms of Use box and click Next.

11. Select Use Current Settings and click Install; then on the User Account Control window, click Continue.

12. When complete, your server now checks for updates for all Microsoft products on the server (such as Exchange Server), and not just for the standard Windows updates. Close all windows to finish.

This concludes the installation of the Base operating system for both the Domain Controller and the Exchange Server 2010 server.

Promoting a Windows Server 2008 Server to a Domain Controller

As previously stated, in this example we are creating a new Active Directory environment, creating a new forest and domain, and installing a new domain controller in that domain. This is accomplished by using the Active Directory Domain Services Installation Wizard.

1. The installation wizard can be started from the Add Roles option on the Initial Configuration Tasks window, but the easiest way is simply to kick off the wizard from a command prompt. To do so, from the Start menu select Run, type DCPROMO in the text box, and then click OK. This installs the Active Directory Domain Services binaries and starts the Installation Wizard.

2. When the wizard starts, select Use Advanced Mode Installation and click Next.

NOTE

There are many improvements in the Active Directory Domain Services Installation Wizard in Windows Server 2008. While all of these improvements are available by default, some of the wizard pages will appear only if the administrator selects Use Advanced Mode Installation.

Advanced mode installation can also be selected by running the DCPROMO command with the /ADV switch (dcpromo /adv).

---

3. On the Operating System Compatibility screen, read the information and then click Next.

4. At the Choose a Deployment Configuration screen, for our purposes, we select Create a New Domain in a New Forest and click Next. Other available options enable you to modify an existing forest by adding a new domain controller in a new or existing domain.

5. Enter the fully qualified domain name (FQDN) of the Forest Root Domain and click Next. For our example, we use `companyabc.lab`.

6. Enter the Domain NetBIOS name. A default name is suggested for you, derived from the Forest Root Domain name in the previous step. In our example, the suggested domain name is COMPANYABC. When you have the domain name entered, click Next.

7. Set the Forest Functional Level. For our purposes, we cannot set the level to Windows 2000, as Exchange Server 2010 requires at least Windows Server 2003 or higher. If you are certain your environment will not contain any Windows Server 2003 domain controllers in the future, you can set it to Windows Server 2008. For our test installation, we select Windows Server 2003 and click Next to continue.

8. Set the Domain Functional Level. As above, we will select Windows Server 2003 and click Next.

9. Microsoft recommends that you install DNS server on the first domain controller, and requires that this server be a Global Catalog. Leave the default settings and click Next to continue. Electing to install Microsoft DNS on the new domain controller will also modify the server's TCP/IP properties to use the new DNS installation for name resolution.

10. If your computer has any IP addresses (either IPv4 or IPv6) that are assigned by a DHCP server, you will receive a notice that static IP addresses should be assigned to all network adapters. Check your IP settings and continue when ready.

11. If no authoritative parent DNS zone exists, you receive the warning shown in Figure 7.5.

FIGURE 7.5   DNS installation error message.

In our example, we are not integrating with an existing DNS infrastructure, so we will simply click Yes to continue.

12. Depending on your server configuration design, select the location where the AD databases will be located. Using the Browse buttons, select the locations for your Database, Log files, and SYSVOL folders. When ready, click Next.

NOTE

When configuring AD database locations, make sure that your server hardware configuration plan takes recoverability and performance into account.

For best performance, install the AD databases on a separate hard disk than the server operating system and server page file.

For best recoverability, use disk fault tolerance such as RAID or disk mirroring for the AD databases.

---

13. Assign a password to the Directory Services Restore Mode Administrator account. This account is used in the event that you have to start the domain controller in Directory Services Restore Mode. This password should be a strong password, containing a combination of upper and lower-case letters, numbers, and special characters. The password should be documented and stored in a secure location. Enter the Directory Services Restore Mode Administrator password and click Next.

14. Review the selections you have made. In the future, when creating additional domain controllers that will be similar to one another, you can export the settings to an "answer file" that you can use for future unattended installations. If you need to make any changes, use the Back button to go to the section you want to change, then use the Next button to return to the review screen. When ready, click Next to continue.

15. The installation wizard now installs DNS and the Active Directory Domain Services. When the installation has completed, click Finish to close the wizard, and then click Restart Now to restart the server.

When the server has rebooted, log on to the new domain. Your default administrator account will now be a domain administrator, and the password is the same. Take the time to review the server's Event Viewer application and system logs to identify any errors or potential problems with your installation before continuing.

Configuring Active Directory Sites and Services

As previously stated, in order for Exchange Server 2010 to successfully deliver mail, it relies heavily on Active Directory Sites and Services to determine what site particular servers belong to.

After the AD domain controller has been installed, it is necessary to configure Sites and Services to support the future Exchange Server deployment. In our example, we are going to configure two sites for a future installation of Exchange servers in two locations. We will cover how to rename the default first site, and how to create the second site from scratch.

Changing Site Properties

To change the AD Default-First-Site-Name, follow these steps:

1. On the domain controller, select Start\Administrative Tools\Active Directory Sites and Services.

2. Click the plus sign (+) to expand the Sites tree.

3. Right-click Default-First-Site-Name in the left pane of the console, and then click Rename.

4. Enter a name, and then press Enter, which changes the default site name to your custom site name. In our sample lab, we will choose FredericksburgVA.

Creating a New Active Directory Site

To create a new site in AD, follow these steps:

1. On the domain controller, open AD Sites and Services.

2. Click the plus sign (+) to expand the Sites tree.

3. Right-click Sites in the left pane of the console, and then click New and Site.

4. Enter the new site name in the New Object-Site dialog box. In this example, SunnyvaleCA was used for the new site name.

5. Click to highlight DEFAULTIPSITELINK, and then click OK.

6. Review the Active Directory Domain Services message box (shown in Figure 7.6) and ensure the configuration was successful, and then click OK.
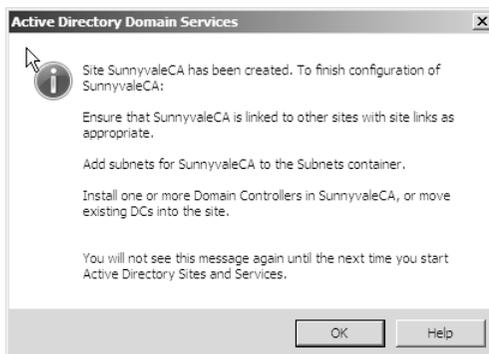
FIGURE 7.6   Active Directory Domain Services message box.

In AD, sites are associated with their respective subnets to allow for the intelligent assignment of users to their respective domain controllers.

To create a new subnet and associate it with a site, follow these steps:

1. Open AD Sites and Services.

2. Click the plus sign (+) to expand the Sites tree.

3. Right-click Subnets and choose New and Subnet.

4. Enter the address prefix using network prefix notation. This requires the address and the prefix length, where the prefix length shows the number of fixed bits in the subnet. The example shown in Figure 7.7 uses the 192.168.80.0/24 subnet, providing us with a Class C (255.255.255.0) subnet. Next, select a site to associate with the subnet and click OK.
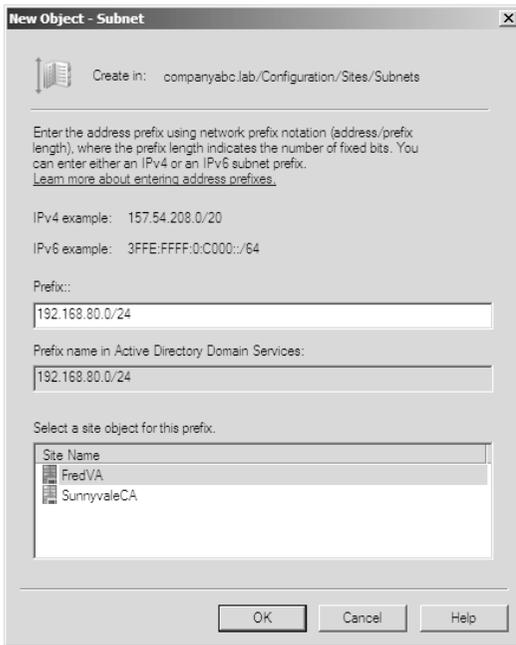
FIGURE 7.7   Associate a subnet to a site.

Perform the same steps to create a second subnet and associate it with the second site.

Configuring a Global Catalog Server

By default, the first domain controller in a domain is automatically configured as a global catalog server. Any additional domain controllers need to be configured manually.

To configure or verify that a domain controller is a global catalog server, follow these steps:

1. Open AD Sites and Services.
2. Click the plus sign (+) to expand the Sites tree.
3. Expand the desired site name, the Servers folder, and then the server object.

4. Right-click the NTDS Settings object, and then click Properties.

5. On the General Tab, ensure the Global Catalog check box is marked if you want the server to be a global catalog server (as illustrated in Figure 7.8). When ready, click OK.
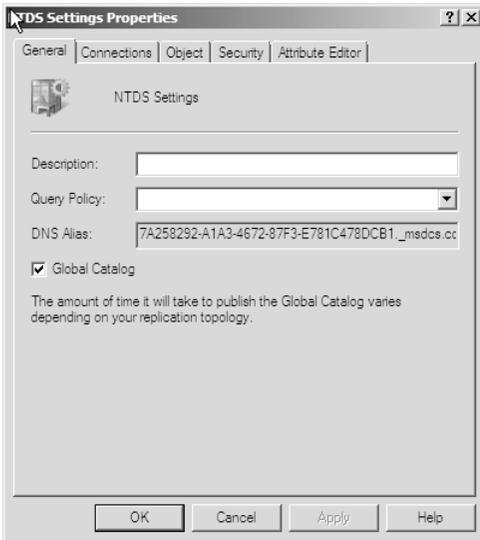
FIGURE 7.8   Configuring a global catalog server.

Preparing Your Environment for Exchange Server 2010

Before deploying Exchange Server 2010, there are several steps that must be done, and several more that *should* be done.

Performing an Active Directory Health Check

This is a step that *should* be done, especially if AD is not being set up from scratch (as it is in our scenario). The existing AD environment should be validated to ensure it is functioning correctly. Since Exchange Server relies so heavily on Active Directory, an extensive health check utilizing tools such as DCDIAG, NETDIAG, and Replication Monitor can help identify any underlying problems that will impact the installation or performance of Exchange Server. A combination of Windows Server 2003 and Windows Server 2008 Support tools can be utilized for these tasks.

For detailed instructions on performing an AD health check, see the Digital ShortCut titled *Performing an AD Health Check* (Sams Publishing, ISBN: 0-7686-6842-5), which can be purchased and downloaded from www.samspublishing.com/bookstore/ product.asp?isbn=0768668425.

Granting the Appropriate Permissions

To install Exchange Server 2010, you must make sure the domain account you will be using is a member of the following groups: Domain Admins, Enterprise Admins, and Schema Admins.

To do so, perform the following steps:

1. On the domain controller, from the Start menu, select Administrative Tools, then Active Directory Users and Computers.

2. Expand your domain name and select the Users organizational unit (OU).

3. Right-click Users and click Find. Enter the name of the account that you will be using to install Exchange Server 2010 and click Find Now.

4. Double-click the user account and select the Member Of tab.

5. Click Add. In the Enter the Object Names to Select field, type `Enterprise Admins;` `Domain Admins; Schema Admins` (separated by semicolons as shown). Click Check Names to ensure all group names are resolved, and then click OK. Ensure all three groups show in the Member Of section and click Apply. Click OK to exit the screen.

Installing the Base Operating System on Your Exchange Server

Exchange Server 2010 can be installed only on a 64-bit version of the Windows Server 2008 Operating System. Although either Standard or Enterprise can be used, the Enterprise version is required for some of the more advanced Exchange Server features.

After you complete the setup of the base operating system, perform the following steps to join the server to the domain:

1. Install Windows Server 2008 on your Exchange server by following the installation procedures earlier in this chapter in the section titled Installing Windows Server 2008. Do NOT continue with the installation of Active Directory on this server.

2. Configure your Domain Controller/DNS server as the Preferred DNS Server in the Internet Protocol Version 4 (TCP/IPv4) settings of your new Exchange Server.

3. From the Initial Configuration Tasks screen, click Provide Computer Name and Domain.

4. On the Computer Name tab, click Change.

5. In the Member Of section, select the Domain radio button and type the name of the domain you created. In our example, this is companyabc. Click OK to continue.

6. Enter the administrator name and password for your domain and click OK.

7. When prompted Welcome to the companyabc Domain, click OK; then click OK again to acknowledge that the computer must be restarted. Close all open windows and, when prompted, click Restart now.

8. After the computer restarts, from the log on screen, click Switch User; then click Other User and enter the domain administrator credentials in the following format:

–domain\administrator, where domain is the name of your domain, and adminis-trator is the administrative account for that domain.

Prepare Internet Explorer to Accept ActiveX Downloads

The default security settings of Windows Server 2008, combined with the default security settings of Internet Explorer 8.0, can result in some real challenges when attempting to download the prerequisite applications for Exchange Server. To ease the process, perform the following steps.

1. On the new Exchange server, log on with your domain administrative account.

2. Right-click the Internet Explorer icon and click Run as administrator. Ensure you have Internet connectivity by bringing up an Internet website. If you do not, trou-bleshoot your network settings and resolve any issues before continuing.

3. In Internet Explorer, select Tools, and then Internet Options. Select the Security tab and then the Trusted Sites icon, and click Sites.

4. In the Add This Website to the Zone field, type `https://connect.microsoft.com` and click Add. Then type `http://download.microsoft.com` and click Add. When finished, click Close.

5. Click the Internet icon and click Custom Level. Under the ActiveX Controls and Plug-Ins section, change Download Signed ActiveX Controls to Prompt (recommended).

6. Click OK and click Yes in response to the warning; then click OK again and exit Internet Explorer.

Installing the Prerequisites

There are some software applications that must be installed on the server before you can run the Exchange Setup Wizard. These applications must be installed regardless of which server role you are going to install. Follow the steps below to install these applications.

Installing Windows Remote Management 2.0

1. Log on to the workstation with your domain administrative account.

2. Insert the Exchange Server 2010 CD and allow Autorun to start the Microsoft Exchange Server 2010 Setup Wizard. You can also start the Wizard from a command prompt by typing `d:\setup` (assuming d:\ contains your E2010 installation media).

3. If you have installed all updates for the server, Step 1: Install .NET Framework 3.5 should already be completed.

4. Select Step 2: Install Windows Remote Management 2.0.

5. Select the WinRM on Vista and WS08 (x64) option, and click Download beneath the file. When prompted This Website Wants to Install the Following Add-On, right-click the Internet Explorer Information Bar and select Install This Add-on for All Users on This Computer.

6. Click Install to Install the Microsoft File Transfer Manager.

7. If the Language Update box appears, click OK and install the selected file.

8. When the Confirm Transfer Request box appears, browse to the location where you would like to store your prerequisite installation files. (Note: The browse feature does not allow you to create new folders, so if you are going to want to create a new folder for the storage of these files, do so in Explorer before trying to browse.) When you have selected the location, click Transfer.

9. Once the file has finished downloading, click Close. You can then go to the directory where you stored the download. Double-click the WinRM on Vista and WS08 (x64) Directory; then double-click the installation file. When prompted to Click OK to Install do so.

10. Accept the license terms by clicking I Accept.

11. Once completed, click Restart Now.

Installing Windows PowerShell v2

1. Log on to the workstation with your domain administrative account.

2. Insert the Exchange Server 2010 CD and allow Autorun to start the Microsoft Exchange Server 2010 Setup Wizard. You can also start the Wizard from a command prompt by typing d:\setup (assuming d:\ contains your E2010 installation media).

3. Select Step 3: Install Windows PowerShell v2.

4. From the download page for Windows PowerShell V2, locate the download files and click Download next to the "PowerShell_Setup_amd64.msi" file.

5. Click Run to run the file directly from the download page. If you receive a security warning, click Run again.

6. From the Windows PowerShell Setup Wizard, click Next.

7. On the License Agreement page, click I Accept the Terms in the License Agreement, then click Next, and then click Install.

8. Click Finish when complete and close the Internet Explorer window.

Installing the 2007 Office System Converter: Microsoft Filter Pack

This section is required only for Exchange Server 2010 servers that have the Mailbox role installed on them.

1. Log on to the workstation with your domain administrative account.

2. Open Internet Explorer and go to www.microsoft.com/downloads. Search for 2007 Office Converter Microsoft Filter Pack. Select the Microsoft Filter Pack from the available options.

3. Make sure you are on the 2007 Office System Converter: Microsoft Filter Pack page. Scroll down and click Download for the FilterPackx64.exe file. When prompted, click Run.

4. From the Welcome screen, click Next.

5. From the End-User License Agreement screen, click I Accept the Terms in the Licensing Agreement and click Next.

6. When complete, click OK to exit the installation.

Installing the Active Directory Services Remote Management Tools

These steps will allow an administrator to perform the Schema and Domain prep commands from your Windows Server 2008 server.

1. Open an administrator-enabled command prompt. Right-click Command Prompt and select Run as Administrator.

2. Run the following command:

   ```
   ServerManagerCmd –i RSAT-ADDS
   ```

   The progress of this command will sit at the <10/100> prompt for awhile—be patient and let it finish.

   Upon completion, you see two Warnings in yellow stating You Must Restart This Server to Finish the Installation.

3. After you have successfully installed the Role Administration Tools and the Active Directory Domain Services Tools, reboot the server as instructed.

NOTE

Simply running the `ServerManagerCmd` command above from a normal command prompt will result in a frustrating and poorly documented error:

WriteError: Failed to write the log file: Access to the path 'C:\Windows\logs\ServerManager.log' is denied.

The need to do this is the result of a newly added security component found in both Windows Server 2008 and Windows Vista that is known as "User Access Control" or "UAC." UAC allows administrators to enter their credentials while in a non-administrators user session to accomplish administrative tasks without having to switch users, log off, or utilize the "run as" command. UAC also utilized the Admin Approval Mode (AAM) for all accounts except the built-in Administrator account in Windows Server 2008. AAM is designed to prevent malicious applications from installing without the knowledge of the logged on user.

AAM allows administrators to log on and receive a split user access token—the administrator receives both a full access token and a filtered access token. The filtered access token is used to start Explorer.exe (the process that creates the user's desktop). All applications started by the Explorer.exe process inherit this filtered access token.

In short—with UAC enabled, administrators may have to confirm the installation of some applications or system changes, even when logged in with elevated privileges.

Preparing the Active Directory Forest, Domain, and Exchange Organization

Before you can install Exchange Server, the Active Directory Schema and Domain must be prepared.

Preparing the Schema

1. From the Exchange server, log on with your administrative account. This account must be a member of the Schema Administrators and Enterprise Administrators groups.

2. Copy the contents of your Exchange Server 2010 installation media to a directory on a local drive, such as c:\E2k10Install.

3. From an administrator-enabled command prompt, change to the drive and directory that holds your Exchange Server 2010 installation media and run the following command:

```
Setup /PrepareSchema or Setup /ps
```

> **NOTE**
>
> Depending on how you obtain the media for Exchange Server 2010, you may need to copy the installation media to a local drive and run the setup from that local drive. If you do not, your installation may result in the following error:
>
> *An error occurred while copying the file d:\\en\Setup\ServerRoles\Common \en\Details Templates Editor.msc. The error code was 5.*
>
> If you did not copy the installation media locally and you receive this error, delete the contents of the c:\%windir%\temp file, copy the media locally, and run the command again.

4. When completed, the screen should look like the one in Figure 7.9.

FIGURE 7.9   Preparing the Active Directory Schema.

5. When finished, leave your Command Prompt window open and continue with the next section.

Preparing the Domain and Organization

1. To prepare the Domain and Organization, log on to the Exchange server with your administrative account. This account must be a member of Enterprise Administrators and Domain Administrators groups.

2. From an administrator-enabled command prompt, change to the drive and directory that holds your Exchange Server 2010 installation media and run the following command:

```
Setup /PrepareAD /OrganizationName:SG or Setup /p /on:SG
```

where SG is the Organization Name for your environment. In our lab, we are using TestLab as the Organization Name, so the command will look like this:

```
Setup /PrepareAD /OrganizationName:TestLab
```

3. When completed, the screen should look like the one in Figure 7.10.
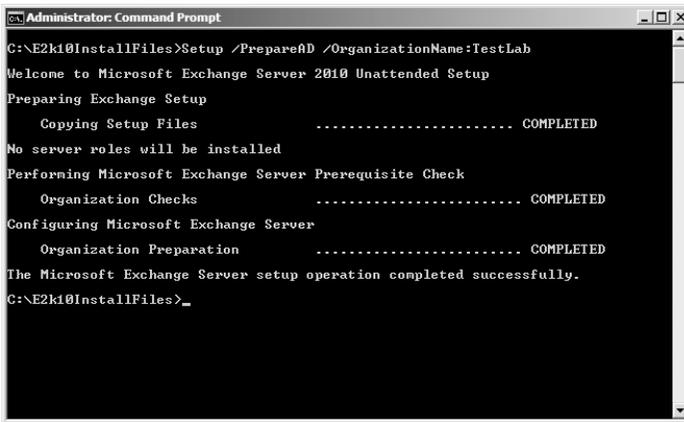
FIGURE 7.10   Preparing the Domain and Creating the Organization.

4. When finished, leave your Command Prompt window open and continue with the next section.

Installing Additional Required Operating System Components

There are several additional operating system components that are prerequisites for all Exchange Server 2010 roles. Additionally, there are specific prerequisites that are required for each of the individual roles.

To determine what prerequisites are needed for each role, review the Exchange Server 2010 Prerequisites document on Microsoft Technet. You can find this by going to http://technet.microsoft.com and searching for "Exchange 2010 Prerequisites."

The following components are required for a server that will contain the Hub Transport, Client Access, and Mailbox roles:

```
ServerManagerCmd -i Web-Server
ServerManagerCmd -i Web-ISAPI-Ext
ServerManagerCmd -i Web-Metabase
ServerManagerCmd -i Web-Lgcy-Mgmt-Console
ServerManagerCmd -i Web-Basic-Auth
```

```
ServerManagerCmd -i Web-Digest-Auth
ServerManagerCmd -i Web-Windows-Auth
ServerManagerCmd -i Web-Dyn-Compression
ServerManagerCmd -i NET-HTTP-Activation
ServerManagerCmd -I RPC-over-HTTP-proxy
```

To install these roles, perform the following steps:

1. Log on with your domain administrator account. From an administrator-enabled Command Prompt, run each of the commands above or, alternately, run the combined command as shown here:

   ```
   ServerManagerCmd –I Web-Server Web-ISAPI-Ext Web-Metabase Web-Lgcy-

   Mgmt-Console Web-Basic-Auth Web-Digest-Auth Web-Windows-Auth Web-Dyn

   -Compression NET-HTTP-Activation RPC-over-HTTP-proxy –Restart
   ```

   Note the addition of the –Restart at the end of the command to ensure the server does not try to restart between component installations.

   When complete, you should see Success: Installation Successful.

2. Reboot the server upon completion.

Installing Exchange Server 2010

Although the installation of all the Active Directory components, prerequisites, operating system components, updates, and hotfixes might seem to have taken forever, we are now finally ready to kick off the Exchange Server 2010 Installation.

Installing Exchange Server 2010 from the GUI Interface

Utilizing the Exchange Server 2010 Installation Wizard is the simplest way of deploying an Exchange server. The GUI interface is extremely intuitive and makes the installation a snap. To install Exchange Server using the Installation Wizard, perform the following tasks:

1. Log on with your domain administrator account. From your Exchange Server 2010 installation media, run the Exchange Installation Wizard (d:\setup.exe, for example).

2. Select Step 4: Choose Exchange Language Option. Select either Install All Languages from the Language Bundle or Install Only Languages from the DVD.

   If you select Install All Languages from the Language Bundle, another screen will appear giving you the option to either download the latest language pack bundle from the Internet or connect to a specific network path for the language files. When the language files have been installed, click Finish to return to the Exchange Server 2010 installation wizard.

3. Select Step 5: Install Microsoft Exchange.

4. From the Introduction screen, click Next to continue.

5. From the License Agreement screen, select I Accept the Terms in the License Agreement and click Next to continue.

6. On the Error Reporting screen, select whether you want to report installation errors to Microsoft. The default is No. Click Next to continue.

7. On the Installation Type screen, if you are installing specific roles, select Custom Exchange Server Installation. In our test environment, we are installing the Hub Transport, Client Access, and Mailbox server roles (as well as the Exchange Management Tools), so we select Typical Exchange Server Installation. Additionally, if you are not installing the Exchange Server application to the default location, click Browse to select the installation directory. When ready, click Next to continue.

8. On the Client Settings screen, if you have clients running either Outlook 2003 (or earlier) or Entourage, select Yes. Otherwise, select No. Selecting Yes creates a public folder database during the installation to support these clients. If No is selected, a public folder database can be created manually any time after the installation completes. When ready, click Next to continue.

9. The Configure Client Access Server External Domain screen is a new addition to the Exchange Installation Wizard (see Figure 7.11). If your client access server will be Internet facing, you can place a check in the box and enter the domain name that you will use (for example, mailservices.domain.com). If your client access server is NOT going to be Internet facing, leave this box unchecked. Click Next to continue.
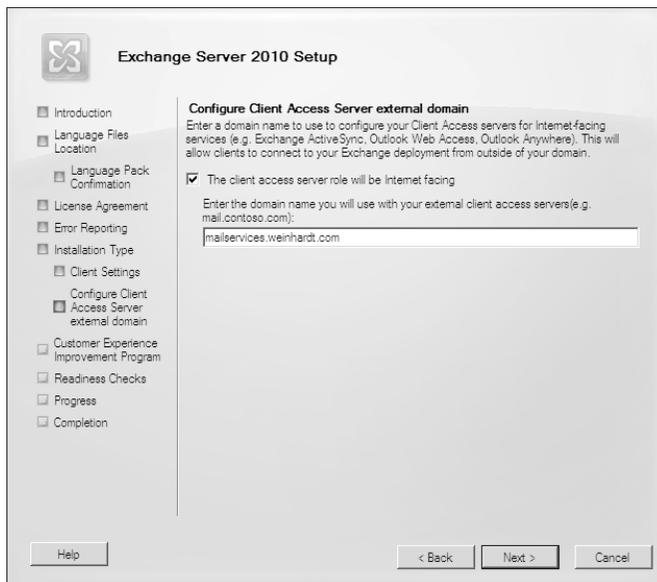
FIGURE 7.11   The New Configure Client Access Server External Domain screen.

10. On the Customer Experience Improvement Program screen, elect whether you want to join the Exchange Customer Experience Improvement Program. Make your selection and click Next to continue.

11. On the Readiness Checks screen, wait while the Install Wizard goes through the prerequisites for each of the selected roles. There may be hotfixes required for the roles being installed—if so, they will be identified as errors in the Readiness Check. Take the recommended actions to resolve them. When all readiness checks show as Completed, click Install to continue.

12. On the Completion screen, review the results of the installation. Ideally, you should see Successfully Installed. No Errors, as shown in Figure 7.12. When ready, uncheck the option to Finalize This Installation Using the Exchange Management Console and click Finish.
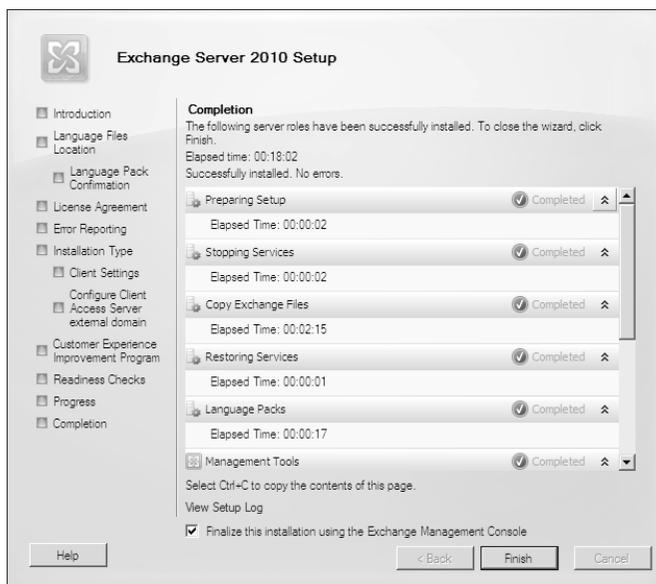
FIGURE 7.12   Completion screen reporting Successfully Installed. No Errors.

13. When you return to the Exchange Sever 2010 Installation Wizard, click Step 5: Get Critical Updates for Microsoft Exchange.

14. Install any available updates for Exchange Server and reboot the server if necessary.

Installing Exchange Server 2010 from the Command Prompt

In several situations (such as the deployment of an Exchange server in a remote location), administrators would prefer to install Exchange Server 2010 from the command prompt.

To do so, perform the following steps:

1. From an administrator-enabled command prompt, change to the drive and directory that contains your installation media.

2. Run the following command:

```
Setup.com /mode:<setup mode> /roles:<roles to install>
➥[/OptionalParameters]
```

For our purposes, we will simply run the following command:

```
Setup.com /mode:install /roles:H,C,M
```

The optional parameters cover all of the various configuration possibilities, including the organization name, target directory, source directory, default database name, and others.

All optional parameters can be viewed from the command line by typing:

```
Setup.com /help:install
```

Finalizing the Deployment

After completing the installation of the Exchange server software, there are several post-installation tasks that should be completed to ensure the installation completed successfully. These include the following:

▶ Exchange Server 2010 Post-Installation Tasks

▶ Review Exchange Installation Logs

▶ Review the Event Viewer for Errors and Warnings

▶ Verify Server Roles Were Successfully Installed

▶ Run the Microsoft Exchange Best Practice Analyzer

Exchange Server 2010 Post-Installation Tasks

After the Exchange installation has completed, open the Exchange Management Console and perform the Exchange Server 2010 Post-Installation Tasks. There are three sections:

▶ **Finalize Deployment Tasks—**Tasks required to complete the deployment of your Exchange organization. Apply to features that are enabled, but require additional configuration.

▶ **End-to-End Scenario Tasks—**Check list of the recommended tasks to perform after deploying Exchange Server.

▶ **Additional Post-Installation Tasks—**Optional steps for configuring Exchange Server features.

Reviewing Exchange Server Installation Logs

After the first Exchange Server 2010 server installation is complete, administrators should review the installation logs located on the root drive of the installation path selected. The typical location of the installation log file is C:\ExchangeSetupLogs.

The log files contain all the details pertaining to the installation of the Exchange server throughout the process.

Review the Event Viewer for Errors and Warnings

After an administrator has verified the installation logs for any anomalies and determined the implementation is a success, it is beneficial to review the Windows Event Viewer logs.

The Application Event Log can contain both positive and negative Exchange Server information about the installation. The Exchange Server events can consist of information, warning, and critical errors. The Application Event Log can be found by launching the Event Viewer included with Windows Server 2008.

Verify Server Roles Were Successfully Installed

Another recommended post-installation task is to verify that the appropriate server roles were installed. This can be conducted by running the `get-ExchangeServer ¦fl` command from within the Exchange Management Shell. Look at the ServerRole header to determine what roles are installed on the server.

Run the Microsoft Exchange Best Practice Analyzer

The final recommended post-installation task is to run the Exchange Best Practice Analyzer tool included with Exchange Server 2010. The Microsoft Exchange Best Practice Analyzer tool is designed for administrators to determine the overall health of the Exchange topology. The tool analyzes Exchange servers and verifies items that do not adhere to Microsoft best practices against a local repository.

The Exchange Best Practice Analyzer tool can be found by expanding the Toolbox node in the Exchange Management Console.

Summary

The installation of Exchange Server 2010 is a relatively simple process, thanks to the Exchange Server Installation Wizard. However, the key to a successful deployment is proper planning—administrators should know exactly what they are deploying before they begin, and the plan should be confirmed in a test environment before deployment.

A solid understanding of the prerequisites, testing the installation process, and carefully following the installation steps confirmed during the testing phase are critical to a smooth and error-free deployment.

Best Practices

The following are best practices from this chapter:

▶ Carefully review and complete all prerequisites before attempting to install Exchange Server 2010. The "trial and error" method is time consuming and frustrating. Proper planning before execution will greatly increase the chance of an error-free installation.

▶ For email messages to flow, you MUST install both the Mailbox server role and the Hub Transport server role in each Active Directory site that will house a mailbox server.

▶ You must install a client access server in each AD site that has a mailbox server.

▶ Use virtual servers when creating a test lab to simulate large production implementations and to minimize hardware costs.

▶ For small organizations, it is possible to install the Mailbox, Client Access, and Hub Transport roles all on the same server.

▶ Before installing Exchange Server 2007 into a production environment, it is beneficial to prototype the design in a test environment.

▶ To install Exchange Server 2010, the Active Directory forest functional level MUST be Windows Server 2003 or higher.