2.1. Active Directory Design

An efficient Active Directory domain simplifies security administration while providing the needed level of access control. As you create a security plan, examine the Active Directory structure and make modifications where necessary to improve performance and administration. In particular, do the following to prepare for Active Directory design.

- Identify areas that have different Account Policy requirements.
- Identify departments that have a different administrative approach.
- Identify users and their network resource access needs. Group users who have similar access needs.

With this information on hand, you can structure Active Directory to accommodate your security requirements. The following table describes design considerations for Active Directory.

Component	**Description**
Domain	The domain is the basic administrative unit of an Active Directory structure. In many cases, a single domain will be sufficient for the network. You might need to create multiple domains to: • Implement different Account Policies settings. • Manage cultural or country differences or large, dispersed geographic regions. • Grant 99% administrative independence to the domain. • Integrate existing NT domains into the domain structure. • Accommodate an existing DNS namespace that is not contiguous. • Divide the directory database for more effective partitioning.

Organizational Unit (OU)	Use organizational units to delegate network administration and simplify permission assignments. Divide domain resources into organizational units to: • Delegate administrative control to the objects within the OU. • Apply Group Policy Objects (GPOs). ***Note:*** *A generic container is not an OU and can't have group policy objects assigned to it. A good practice is to move objects out of generic containers and into an OU. For example, you can move the computers out of the Computers container and into an OU where group policy can be applied.*
Trees and Forests	By default, all domains in a forest: • Share the same schema. • Share global catalogs. • Have automatic two-way transitive trusts. For these reasons, you will typically only need one forest for a network. However, you might want multiple forests to: • Divide administration and prevent sharing between domains in different forests. • Have different schemas or global catalogs in place. • Limit trusts between domains. • Prepare for an eventual split of a portion of the network. For example, if one part of the network represents a business unit that might eventually be sold to another company. • Create a test forest for schema-enabled applications. • Connect two independent organizations. This can result from a merger or acquisition, and it can be temporary (until one forest is migrated to the other) or permanent. • Grant 100% independence by creating a completely independent unit (for testing or administration). Administration does not cross forest boundaries.

	Note: *Tree boundaries are automatic and based on the DNS namespace. You will typically not need to design tree boundaries.* A good security practice is to separate the root domain of a forest by creating an empty root. Limit access to the empty root to prevent users from accessing the default administrator account of the root domain, which is by default a member of Enterprise Admins. This means that users with access to the administrator account of the root domain have full control over the forest.
Sites	Use sites to: • Control domain controller replication across WAN links. • Localize resource access. Use the following guidelines to identify site objects: • Divide sites based on slow WAN links. • Include multiple LANs or subnets within a site only if the links between networks are fast. • Make sure each site has at least one domain controller. Combine sites without domain controllers with other sites.

2.2. Group Policy Design

Group Policy lets you define common settings or policies that are applied to User or Computer objects. Through Group Policies, you can design consistent interface and security settings throughout the network. Group Policy settings are stored in Group Policy objects. Each object contains both computer and user settings.

GPO Category	Description
Computer Configuration	Computer policies (also called machine policies) are enforced for the entire computer. Computer policies are initially applied as the computer boots, and are enforced before any user logs on.
User Configuration	User policies are enforced for specific users. User policies are initially applied as the user logs on, and often customize Windows based on user preferences.

Policy settings are enforced for specific computers or users by associating (linking) the Group Policy object with an Active Directory container. Settings in the local Group Policy may also be applied. For any given user or computer, multiple Group Policies might apply. By default, policies associated with a container are applied to all objects within or below that container. In addition, a single container might have multiple associated Group Policy objects. Policy settings are both inheritable and cumulative.

GPOs can be linked to Active Directory sites, domains, or organizational units (OUs). The table below describes the order in which GPOs are applied:

Order	Location
1	**L** -- The Local Group Policy on the computer.
2	**S** -- GPOs linked to the site where the user's computer is located.
3	**D** -- GPOs linked to the domain that contains the User or Computer object
4	**OU** -- GPOs linked to the organizational unit(s) that contain(s) the User or Computer object (from the highest-level OU to the lowest-level OU).

Settings in Group Policy objects have the following characteristics:

- GPO settings are cumulative. If multiple GPOs apply to a specific object, settings in all GPOs are combined and applied.
    - If a setting is defined in one GPO and undefined in another, the defined setting will be enforced (regardless of the position of the GPO in the application order).
    - If a setting is configured in two GPOs, the setting in the last-applied GPO will be used.
- GPO settings are inherited to objects in or below a container. Settings in the GPO for a parent OU flow down to child OUs. However, settings defined in a GPO on a child OU can override settings inherited from parent OUs.
- If a single object (site, domain, or OU) has multiple linked GPOs, they are applied in the reverse order that they are listed (the GPO at the top takes precedence).

The table below describes six exceptions to the order in which GPOs are applied.

Exception	Description
Account Policies	Account policies include the following: • Password policies • Account lockout policies • Kerberos settings You should be aware of how Account Policy settings are applied in various situations. The Account Policy settings that are used depend on the type of logon (domain or local) and whether the computer is a domain controller. • When a user logs on to a domain, the Account Policy stored in the default domain Group Policy is used. These settings apply to all computers in the domain. • When a user logs on locally, if the computer is a member of a domain, the Account Policy of the parent OU (if it exists) is used. • When a user logs on locally, if the computer is not a domain member, the Account Policy in the local Group Policy is used. (In a workgroup environment, control Account Policy settings through the local Group Policy.)

	• Because you cannot log on locally to a domain controller, the Account Policy stored in the default domain Group Policy is always used for a domain controller. ***Note:*** *Account Policy settings are not cumulative. Either the domain Account Policy, an Account Policy associated with the Organizational Unit, or the Local Account Policy is used. Settings in the Local Account Policy are not combined with other Account Policy settings.*
Blocking Inheritance	You can block inheritance to prevent group policies from higher levels from descending through the order of application.
No Override	On a per policy basis, you can allow policies to pass through blocks.
Loopback	You can choose to have the user settings apply to the machine a user logs on to. This allows you to apply the same settings for all users.
WMI Filtering	You can define specific filter criteria that determine the circumstances under which group policies are applied.
ACL Filtering	Using the access control list, you can turn on or off the **Apply** setting for specific users and groups.

As you design Group Policy, keep in mind the following facts and guidelines:

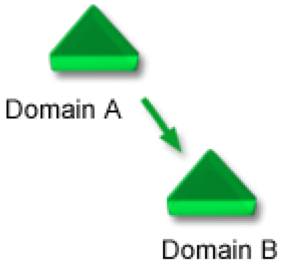
- Minimize the number of GPOs applied for any given object. Avoid linking GPOs to every OU and site in the domain.
- Use the **Block Inheritance** and **No Override** options to control inheritance sparingly. Using these options can greatly increase the complexity of the settings that are applied to a specific object.
- Because Account Policies are set only at the domain level, you must create multiple domains if two divisions in the same organization have different Account Policy needs.
- Although you can link a single GPO to multiple domains, link GPOs only to objects in the same domain to improve performance.
    - Place the configuration files on the Netlogon share of a domain controller.

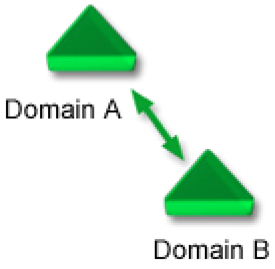
- To control security in a workgroup environment, you must modify the local Group Policy for each system. (Workgroup computers are not members of a domain and therefore do not inherit Group Policy settings through Active Directory.)

2.3. Trust

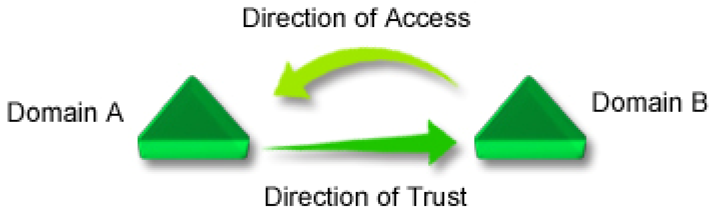
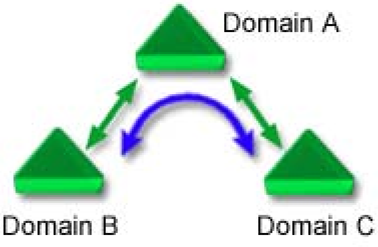
The domain is the basic security division in Active Directory. Typically, security settings and access control lists in one domain do not apply to other domains. A trust relationship identifies another domain as trusted, enabling members in one domain to access resources in another domain.

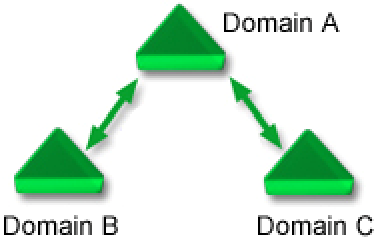
You should understand the following properties of trusts:

<table>
<tr><th>Characteristic</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">Direction of Trust</td><td colspan="2">The direction of the arrow identifies the direction of trust. For example, if Domain A trusts Domain B, the arrow would point from Domain A to Domain B. Domain A is the <i>trusting</i> domain, and Domain B is the <i>trusted</i> domain. The direction can be one-way or two-way.</td></tr>
<tr><td><b>One-way Trust</b>


Domain A trusts Domain B. Domain B does not trust Domain A.</td><td><b>Two-way Trust</b>


Domain A trusts Domain B. Domain B trusts Domain A.
<b><i>Note:</i></b> <i>A two-way trust is the same as two one-way trusts in opposite directions.</i></td></tr>
</table>

<table>
<tr>
<td><b>Direction of Resource Access</b></td>
<td colspan="2">Resource access is granted opposite of the direction of trust. For example, if Domain A trusts Domain B, users in Domain B have access to resources in Domain A (remember that users in the trusted domain have access to resources in the trusting domain).

 </td>
</tr>
<tr>
<td rowspan="2"><b>Transitivity</b></td>
<td colspan="2"><i>Transitivity</i> defines whether trust between domains flows or is inherited to other trusted domains.</td>
</tr>
<tr>
<td>A transitive trust allows the trust relationship to flow among domains.


Domain A trusts Domain B.
Domain A trusts Domain C.
Therefore, Domain B trusts Domain C.</td>
<td>With a non-transitive trust, trust relationships must be explicit between domains.


Domain A trusts Domain B.
Domain A trusts Domain C.
Domain B does <i>not</i> trust Domain C.</td>
</tr>
</table>

By default, Active Directory creates two-way transitive trusts between parent and child domains in the tree or forest. These are known as Active Directory trusts or Kerberos trusts. You must manually create trusts with domains outside of the forest, or between other forests.

2.4. Trust Design

By default, Active Directory creates automatic, two-way, transitive trusts between all domains in the forest. In most cases, the default trusts will be sufficient. You might want to create trust relationships manually to:

- Enable sharing between domains in different forests.
- Establish trusts with Kerberos realms.
- Explicitly control trust relationships (i.e. not accept the default trusts so you can establish only the trusts that are necessary).

The following table describes the characteristics of each trust type.

Trust	Description
Tree root	• Automatically established between two trees in the same forest. • Trusts are transitive and two-way. • Uses Kerberos and NTLM for authentication.
Parent/child	• Automatically created between child and parent domains. • Trusts are transitive and two-way. • Uses Kerberos and NTLM for authentication.
Forest root	• Manually created between the two root domains or two forests. • Transitive within the two forests. Non-transitive between other forests (forest A trusts forest B and forest B trusts forest C, but forests A and C don't share trust). • Can be either one-way or two-way. • Uses Kerberos and NTLM for authentication. • Use to grant access to resources in other forests. • All forest domain controllers must be at 2003 functional level.

External	• Manually created between domains in different forests or UNIX domains (Kerberos realms). • Trusts are not transitive. • Trusts are one-way, although you can create two one-way trusts to simulate a two-way trust. • Uses NTLM for authentication.
Shortcut	• Manually created between two domains in the same forest. • Trusts are transitive, and can be either one-way or two-way. • Uses Kerberos and NTLM for authentication. • Create a shortcut trust to reduce the amount of Kerberos traffic on the network due to authentication. The shortcut trust allows quicker response between the domains by enabling domains to pass authentication requests directly between themselves.
Realm	• Manually created between Active Directory and non-Windows Kerberos realms. • Can be transitive or non-transitive. • Can be either one-way or two-way. • Uses Kerberos for authentication. The non-Windows realm must use Kerberos V5.

There are two ways to control authentication when using a forest trust:

- With forest authentication, any user can be given access to resources in the other forest. This is an open access model.
- With selective authentication, you can lock down resources using the following methods:
    - Restrict access to domains using domain suffix routing.
    - Restrict access to computers by granting the **Allowed to Authenticate** permission on users, groups, or the Other Organization group.

2.5. CA Design

To plan a certificate authority structure, you need to consider the CA hierarchy role, the CA type, and the CA access as described in the following table.

CA Hierarchy Role	Description
Root	The root CA is the top-level CA. All other CAs in the hierarchy are below the root CA. The root CA: • Issues its own certificate (a self-signed certificate). • Issues CA certificates to subordinate CAs. • Typically, does not issue certificates directly to users or computers.
Subordinate	Subordinate CAs are certification authorities below the root CA. A subordinate CA: • Receives its certificate from the root CA or another subordinate CA. • Can be authorized to issue certificates to other CAs, users, or computers.
CA Type	**Description**
Enterprise	Enterprise CAs are integrated with Active Directory. Enterprise CAs: • Can issue certificates to users and computers in Active Directory automatically. • Use certificate templates to simplify requesting and issuing certificates. Use an enterprise CA to issue certificates to users within your organization.

Standalone	A standalone CA is not integrated with Active Directory. - Information in certificate requests must be validated manually. - Certificates must be approved and issued manually. Use a standalone CA to issue certificates to users outside of your organization (such as customers or users who do not have Active Directory accounts).
Third-party	A third-party CA is a certification authority that is maintained by an outside organization. Third-party CAs are trusted on the Internet, and are used to obtain certificates that are used to prove identity outside of your organization or to the public. Use a third-part CA to: - Receive a certificate for Web servers to identify them to the general public. - Digitally sign software distributed to the public (such as Active X controls made available to the general public).

CA Access	Description
Online	An online CA is one that is electronically accessible through the network. Because it is online, requests can be submitted and granted automatically through auto-enrollment. ***Note:*** *Because an enterprise CA requires Active Directory, enterprise CAs should be online.*
Offline	With an offline CA, certificate request must be manually submitted. Approved certificates must be manually approved, and the certificate exported and imported to the requesting user or computer. Because the CA cannot be accessed through the network, an offline CA is more secure than an online CA. ***Note:*** *Root CAs are often offline in order to minimize the attack exposure of the root CA.*

Most PKI infrastructure designs use multiple CAs with varying configurations and roles. Two common designs are as follows:

Configuration	Description
Offline standalone root CA with online enterprise subordinate CAs	If you are designing your own PKI for internal use, you will typically have at least two CAs: • The root CA is offline to protect the CA. Because it is offline, it is configured as a standalone CA. • One or more online enterprise subordinate CAs are configured to support certificate templates and autoenrollment.
Internal PKI for internal certificates and a third-party CA for external certificates	Using an internal PKI for certificates is often less expensive than obtaining all certificates from a third-party CA. However, even if you have your own internal PKI, you will likely need to obtain some certificates from a third-party CA for those certificates that are used by the public. • Configure the internal PKI to issue certificates to users and for signing software that is only used internally. • Obtain third-party certificates for signing code that is made available to the public or for validating the identity of public servers (such as a public Web server).

Certification Authorities issue certificates that are used to validate user identity and message integrity. For this reason, you should safeguard your CAs to ensure that certificates and private keys are not compromised. Consider the following actions to safeguard CAs.

- Prevent unauthorized access to the physical systems to prevent compromise of certificates.
- Protect your root CA from physical failure. If the root CA fails, you might have to reissue all certificates in the certificate hierarchy.

- Have a CA recovery plan (regular backups and a restore procedure).
- In particular, protect the root CA from compromise. For maximum security, make the root CA offline. This means that physical access to the root CA is required to issue subordinate certificates.
- Periodically audit certificates.
- Immediately revoke certificates that have been compromised. Publish a new Certificate Revocation List (CRL).
  - The CA periodically publishes the CRL to notify other computers of revoked certificates. Although a Windows CA automatically publishes its CRL at regular intervals, you can publish it at any time by using the CRL Publication wizard.
  - Each certificate issued by a Windows CA specifies a CRL distribution point (the network location of the CRL). This lets the client automatically retrieve and cache the CRL. Once the client has a copy of the CRL, it will no longer recognize certificates on the list as valid.
  - By default, Windows Workstation and Server machines check the CRL before accepting a certificate.
  - Windows Servers allows you to publish *delta* CRLs. Delta CRLs list only changes made to the CRL since the CRL was published. Be aware that Windows systems older than XP cannot use delta CRLs.

2.6. Certificate Distribution Design

A certificate template identifies a certificate type and describes the rules the CA follows when issuing a certificate based on the template. Templates also give instructions to the user on how to create and submit a certificate request.

You can use certificate templates to simplify certificate management.

- Each template includes settings for certificates that are used for specific functions.
- Certificate templates are stored in Active Directory. All CAs in the forest share the same set of certificate templates. Changes made to templates are available to all CAs.
- Because certificate templates are stored in Active Directory, only Enterprise CAs can use certificate templates.
- Certificate templates are identified by a version number. The following table describes the characteristics of each version.

Version	Description
Version 1 templates	o Can be used by Windows 2000 or 2003 CAs. o Have very few settings that can be customized.
Version 2 templates	o Can only be used by Windows 2003 CAs that are running an Enterprise or Datacenter version of Windows. All settings can be customized.
Version 3 templates	o Can only be used by Windows 2008 or 2008 R2 CAs that are running an Enterprise or Datacenter version of Windows. All settings can be customized.
Version 4 templates	o Can only be used by Windows 2012 or 2012 R2 CAs that are running an Enterprise or Datacenter version of Windows. All settings can be customized.

Use the following process to implement certificate templates:

1. (Recommended) Copy an existing certificate template to create a new template.
2. Modify the template properties. In particular, uses must have the Read and Enroll permissions in order to request a certificate of that type.
3. Publish the certificate template on the server. This enables the server to respond to certificate requests for that type of certificate.

As part of the PKI design process, you will have to decide how users and computers will request certificates and how those requests will be handled. The following table lists various methods for distributing certificates.

Method	Description
Autoenrollment	With autoenrollment, certificates can be requested, issued, or renewed without user intervention. Autoenrollment automatically downloads and manages certificates from Active Directory into the local machine registry for all users who log on to domain-joined machines. Autoenrollment requires you to have the following hardware: • Windows 2003 or later domain controllers • Windows XP/2003 or later clients • Windows 2003 or later enterprise CA To configure autoenrollment: • Use version 2 or later certificate templates. If necessary, copy a version 1 template to create a version 2 or later template. • Grant users or computers the Read, Enroll, and Autoenroll permissions. • Edit Group Policy and enable autoenrollment for computers, users, or both. You can also configure whether certificates are automatically renewed or updated.

Enrollment Web Pages	With the enrollment Web pages, users submit requests using a special Web site. Depending on the configuration of the CA, certificates might be issued automatically, or users might need to manually install the certificate after it is approved. To allow Web-based enrollment, • Your CA must be running Windows Server 2003 or later Certificate Services and IIS 6.0 or later. • The CA must be installed with the Web Enrollment application. This allows users to request and receive certificates from standalone and enterprise CAs. Use the Web enrollment pages to submit manual requests, or to enable certificate requests when the clients or the servers do not support autoenrollment.
Manual Request	You can submit manual certificate requests through a variety of wizards included with certain utilities (such as IIS or the CA installation process). Use a manual request when you have an offline CA or when you need to request a single certificate for a single user or computer and when autoenrollment is not supported. To obtain a certificate manually: 1. Use the Web Enrollment Pages, the Certificate Request Wizard, or **Certreq.exe** to prepare the request. The request will be saved as a file. 2. Import the request file into the CA. 3. Approve the request, making it a certificate. Save the certificate as a file. 4. Import the certificate file into the system that requested it.

2.7. Management Tools

The following table lists various security issues related to remote administration tools.

Method	Description
Remote Desktop (RDP)/Terminal Server connection	With a Remote Desktop connection, administrators can view and interact with the server console using the graphical interface. • Remote Desktop uses 56-bit or 128-bit RC4 encryption. Encryption is enabled by default. • For additional protection, enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy to use 128-bit 3DES encryption. • To control which users can connect using Remote Desktop, modify the membership of the Remote Desktop Users group. In addition, members of the local Administrators group always have Remote Desktop access.
MMC consoles	You can use the Microsoft Management Console (MMC) to remotely administer most client and server functions. Simply add the remote computer to the console or connect to the computer within the console. • The Windows 2003 administrative tools or RSAT 2008 or later use LDAP signing to authenticate and encrypt packets. • You can create your own consoles to limit the features available to other administrators. Add only the snap-ins required for the administrative task, then save the console in a user mode to prevent adding additional snap-ins.

	• Use the following Group Policy category to control which snap-ins users can access: **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins**. • You can also use NTFS permissions to control access to predefined snap-ins.
Remote Administration Website	The Remote Administration Website is a browser-based tool that you can use to manage IIS. It cannot be used to manage other server functions or services. • The remote administration tools are configured by adding the component to IIS in Add/Remove Windows Components. • Adding the component creates a new Web site. • To securely manage the Web site through the HTML interface, use port 8098 (uses SSL). SSL is enabled when the Web site is created--you do not need to add a server certificate for SSL.
Remote Assistance	With Remote Assistance, users can request help from their desktops. Assistants can view and remotely control user desktops. • By default, users must request assistance and then agree to allow administrators to control the desktop. • Use Group Policy to enable or disable remote assistance, allow unsolicited help, or to take control of a desktop without permission. • For most remote administrative tasks, use Remote Desktop.

Telnet	Telnet is a text-based administration tool that allows you to submit commands to a remote server. • To administer Microsoft servers and clients, use Remote Desktop or an MMC console instead of Telnet. • If you must use Telnet to administer non-Microsoft systems, use SSH (the secure version of Telnet that uses SSL), use IPSec, or establish a VPN before running the utility.

Each of the management tools described here are in-band tools, meaning that they work through a normal network connection to the destination server. With Microsoft's Emergency Management Services (EMS), you can use an out-of-band connection to remotely administer the server. For example, you can use EMS to:

- Manage servers that are inaccessible through a network connection, for example when the network card has failed.
- Manage servers when operating system or other conditions prevent it from responding to normal administration tools.
- Create a secure administration network that operates outside of the normal network connection.
- Create *headless* servers that have no keyboard, monitor, or mouse.

Out-of-band management uses three different methods to enable you to remotely manage the console.

Method	Description
Firmware console redirection	Some systems include a feature in the BIOS whereby console screens can be redirected to a different port. With this method, you will be able to see the text-based startup messages associated with POST and system startup.

Operating system redirection	With Microsoft's EMS, once the operating system loads it assumes control of console redirection. With EMS, you can use a console commands to: • Gather information about the server such as its IP address, running processes, and loaded drivers. • View logs. • Shut down or restart the system. • Change process priority. Note: EMS gives you a text-based console. It does not show you the GUI Windows interface.
Service processor	A service processor is a special processor, either built onto the motherboard or added through a PCI expansion slot, that performs console redirection tasks. EMS can typically redirect output through these service processors. In addition, some service processors might come with additional features not included in EMS.

Console output is typically redirected to a serial port or a special port provided on an expansion card. With a terminal concentrator, you can link multiple servers together to a single console for out-of-band management. Then use Telnet or SSH at the console to connect to a specific server.

Note: *When using an out-of-band solution, make sure to implement strict physical security to secure the server consoles.*

2.8. Administration Design

An important part of network security is to strictly limit the privileges of authorized users. For administrators, this means enforcing the principle of least privilege--assigning only those privileges that are necessary for the administrator to do the job.

When designing administration, begin by identifying the administrative approach:

Administrative Model	**Description**
Centralized	With a *centralize*d approach, a single IT department manages the entire network. Centralization ensures standardization and guarantees a certain amount of expertise available for all network administration tasks.
Decentralized	With a *decentralized* approach, localized IT departments handle administration tasks locally. Decentralization may improve crisis response times and reduce indirect expenses such as travel required to fix problems in distant locations.

Most large organizations use a combined approach where some tasks (such as system-wide tasks) are centralized and other tasks are decentralized (such as administering user accounts and files).

Approach	**Typical Tasks**
Centralized	• Designing a global network infrastructure • Designing the DNS namespace • Designing naming standards • Installing the first Active Directory domain controller (forest root domain) • Modifying the Active Directory schema • Monitoring global network needs • Creating upper-level OUs

Often Centralized	• Designing security policies • Designing backup and restore policies • Designing replication topology and schedules • Authorizing DHCP servers • Installing/configuring Active Directory domain controllers • Installing/configuring DHCP servers • Installing/configuring DNS servers • Repairing mistakes created by lower-level administrators
Often Decentralized	• Supporting end users • Creating/deleting user accounts • Modifying user passwords and configuring other user account properties • Installing/configuring member servers • Monitoring individual servers and subnets • Administering computers and printers

You can use the following three processes to design an administrative strategy:

Process	**Description**
Define Administrative Roles	To define a role, identify the actions administrators of each role must perform on specific objects or object attributes. For example, you might have the following roles: • Department administrator • Workstation administrator (create and manage workstations) • User administrator (create and delete user accounts) • Password administrator (modify passwords) • User information administrator (modify phone numbers and addresses for user accounts)

	Create a group for each role, then make the necessary user accounts members of that role.
Define Administrative Boundaries	To simplify assigning permissions, use OUs to group objects under a single administrative control. • Divide the network into multiple domains only if necessary. For most applications, a single domain is sufficient. • Use organizational units to subdivide the network based on administrative boundaries. Administrative boundaries might be: • Geographical, if different administrators are in charge of different locations. • Departmental, if you have different administrators for each logical division. • Resource-based, if you have administrators who are responsible for a specific Active Directory object type such as users, computers, or servers.
Assign Permissions to Enable Administrative Access	As a rule, you should assign only the permissions to the objects or attributes needed to fulfill the administrative role. As you assign permissions, keep in mind the following: • Assign permissions to groups rather than users to simplify administration. • Assign permissions as high up in the structure as necessary, taking advantage of inheritance. • For department administrators, assign Full Control to the OU representing the administrative boundary. • For lower-level administrators, assign necessary permissions to specific attributes. To simplify creating administrators, use the Delegation of Control Wizard.

Keep in mind the following guidelines when designing an administrative strategy:

- You should rarely, if ever, make administrators members of administrator groups, such Enterprise Admins, Domain Admins, or even local Administrators. Instead, create your own groups for specific administrative roles.
- Assign administrators two accounts:
    - An account for normal, non-administrative use.
    - An account that gives them access to elevated privileges. Have administrators use the **Run as** command to log on with this account only when necessary.
- Set up special administrator workstations in physically secure locations. For added security on these workstations:
    - Require IPSec to all connections with the workstation.
    - Add a smart card reader and allow logon only with smart cards. Configure the system to automatically log off users when the smart card is removed.
- If you give Full Control to an OU and if the group is inside the OU, the group members can change the group membership. For example, if you create a Research Admins group in the Research OU and assign the group Full Control over the OU, group members can make other users members of the group, thereby granting administrative privileges to other users. To prevent administrators from modifying the group membership, take one of the following actions:
    - Remove the Full Control permissions over the OU, then delegate administrative control over the OU, carefully identifying only the allowed actions that the group can perform.
    - Move the group outside of the OU. This means that group members can no longer manage the group itself.
- Consider preventing remote administration altogether for some tasks or servers.

2.9. Software Distribution Methods

Although you can deploy operating system updates and software manually, you will likely want to automate the process as much as possible. The following table compares different methods you can use to automate software distribution.

Update Deployment Method	**Description**
Windows Software Update Services (WSUS)	Windows Software Update Services (WSUS) is the preferred method for distributing Microsoft software updates. • WSUS works with operating system updates and also supports other Microsoft software updates (such as Office). • WSUS allows you to centrally manage and control the updates that will be applied to network computers. • WSUS allows you control network bandwidth by specifying local servers to use for downloading updates. • You cannot use WSUS to update drivers or non-Microsoft software.
Microsoft Update	Microsoft Update is a service that can be used to download and apply operating system updates automatically. • Using Group Policy, you can control the behavior of updates. For example, you can download updates automatically without user intervention. • Unlike WSUS, Microsoft Update does not require that you configure update servers on your network. All updates are downloaded from the Microsoft Web site. • With Microsoft Update, you cannot control which updates are installed.

Software Installation Policies in Group Policy	You can deploy software using the Software Installation node of a Group Policy object. • Software must have an installer file (.msi or other allowed installer file). • You can distribute Microsoft and third-party software. • You can control which users or computers get the software by linking GPOs to domains and OUs. In addition, you can use WMI filtering to ensure that the updates go only to the computers that need the updates. • You can force software to be installed (publish), or make the software available for installation through Add/Remove Programs (assign).
Scripting	You can automate software installation by writing custom scripts that can detect installed software and launch the appropriate installation files. • Scripts can be run automatically by linking the scripts to a Group Policy object. • You can create scheduled tasks to run scripts at specific times. • You can run scripts automatically following the operating system installation by editing the [GuiRunOnce] section of the Unattend.txt file.
Systems Management Server (SMS)	Systems Management Server (SMS) is a Microsoft service that provides application deployment, security patch management, and asset management. With SMS, you can easily distribute software using various criteria such as group membership or computer hardware characteristics.

2.10. WSUS Design

The preferred method of managing operating system updates is through WSUS. Be aware of the following facts regarding:

- WSUS supports updating additional Microsoft products including Office and Exchange. You cannot use WSUS to update other software products. Instead, use a software distribution policy or Systems Management Server (SMS) to distribute application updates.
- WSUS supports updating drivers, although the Automatic Updates client will detect and report them. You must install drivers manually from Microsoft Update.
- Each client computer must have the Windows Automatic Updates client software to utilize automatic updates. This software is included automatically with Windows Servers and Workstation systems.
- WSUS cannot uninstall hotfixes. You must manually uninstall hotfixes or write a script to perform the uninstall.
- WSUS requires IIS.

As you design a WSUS solution, make the following design decisions:

Decision	**Options**
Approval method	WSUS allows you to approve updates that will be applied. Only approved updates will be installed on client systems. Approval can be: • Centralized, where all approval happens on a single WSUS server. • Decentralized, where approval is delegated to location or department administrators.
Server topology	The server topology identifies the number and relationship of WSUS servers on the network. For example, you can have: • A single WSUS server for the entire network. • Multiple WSUS servers, each servicing a specific location or department.

	• A hub and spoke configuration, where clients connect to multiple WSUS servers that are linked with a central WSUS server.
Downloading updates	Using Microsoft Update, all updates are downloaded by the client from the Microsoft Web site. With WSUS, you can control where downloads are obtained. Controlling the download location improves download times and reduces WAN link use. Possible configurations include: • Clients download updates directly from the Microsoft Web site. With this configuration, the WSUS server is used to identify approved updates, but the server itself does not have a copy of the updates. • The WSUS server downloads the updates from the Microsoft Web site. Clients then download updates from the internal WSUS server. • A central WSUS server downloads updates from the Microsoft Web site. Additional WSUS servers copy the updates from the internal server, and clients download updates from local WSUS servers.
Client settings	By default, client computers are configured to use Microsoft Update for obtaining operating system updates. You must configure clients to point to the WSUS server for approval and to download updates. The most efficient method of managing these settings is through Group Policy. With Group Policy you can: • Point clients to the WSUS download location (identify the server that holds the updates to be downloaded). • Identify client-side groups (identify the client group so it gets only the updates approved for that group). ***Note:*** *You can configure non-domain members to use WSUS by editing the registry on each computer.*

The following table lists two common configuration scenarios for large SUS implementations:

Implementation	Description
Single site, centralized administration	For a large network at a single location, the following configuration centralizes administration while minimizing Internet traffic. • A single WSUS server is used to approve updates. Updates are downloaded from the Internet, and updates are periodically synchronized with the Internet. • Additional WSUS servers are located on different subnets. These WSUS servers are linked to the central WSUS server. Updates are synchronized from the internal WSUS server. • Clients are configured to point to the nearest WSUS server to download updates. Group Policy is used to point the clients to the correct WSUS server. • If there are multiple groups of computers with different update requirements: o Define multiple approval lists on the central WSUS server. o Use Group Policy to configure clients with client-side targeting. Client computers will identify their respective group and obtain only the updates approved for that group.
Multiple sites, decentralized administration	For a network with multiple physical locations, each with an Internet connection, the following design is typical: • An SUS server in each administrative location is configured with the appropriate approval list. Updates are downloaded to these WSUS servers. • Additional WSUS servers are placed in each location. These servers obtain the list of approved

	updates from the corresponding main WSUS server. o If the additional WSUS servers are in the same location as the main WSUS server, configure these servers to download updates from the main WSUS server. o If the additional WSUS servers are in different physical locations, configure these servers to download updates from the Internet. • Clients are configured to point to the closest WSUS server for the updates.

2.11. Patch Assessment Tools

The recommended method of checking the security vulnerabilities of a system in an enterprise network is using the Microsoft Security Baseline Analyzer (MBSA).

- Run **Mbsacli.exe** at the command line to start MBSA.
- MBSA checks for installed security updates (patches) and security vulnerabilities (such as user accounts without passwords and unsecure policy settings). MBSA does not check for non-security related operating system updates.
- You can use MBSA to compare a target system with a list of approved updates on an WSUS server.
- MBSA can scan a single or multiple computers. To scan multiple computers, install MBSA on one computer, then point the tool to the target computer(s).
- You can save the results of the scan to an XML file for later analysis.
- MBSA does not install security updates, it only checks the system to see if the recommended updates are installed.
- MBSA does not verify custom Group Policy settings or settings applied through a template. To compare a system to a baseline template, use **Secedit**.
- To use MBSA through a firewall, open:
    - TCP ports 135, 139, and 445.
    - UDP ports 137 and 138.

In addition, you can use the following other methods to check for operating system patch levels:

- Systems Management Server (SMS) also includes a scanning tool that performs functions similar to MBSA.
- Using the Microsoft Update Web site, you can scan a single computer (but not multiple computers).
- Command-line tools such as **Netdiag** and **Wmic qfe** can list applied patches on a single system. You can create simple batch files to run these commands and store the results locally.
- You can manually check the Add/Remove Windows Programs or the C:\Windows directory for installed patches.