STUDY GUIDE

Microsoft

70-640

TS: Windows Server 2008 Active Directory, Configuring

Michael W. Krout

ExamForce

About the Author

Michael W. Krout (MCTS, MCSE, MCT) is an IT consultant and trainer with over 21 years of experience with technology. In addition he has owned and operated independent consulting and training firms, serving such prestigious clients as the U.S. Military and the Pentagon. In addition, he has hands-on experience with Microsoft products, dating back to DOS, as a programmer and database engineer, Windows server experience since NT version 3.51 and even Novell and IBM mainframe. These skills, in addition to university level instruction, educational content development and authoring and real world “know-how”, stand as credits to his knowledge and mastery of technical subjects.

Additional Contributor(s)

Brianne Havlik (A+, MCP)

About the Exam

There are six major topic areas that make up this exam:

- Configuring Domain Name System (DNS) for Active Directory (16%)
- Configuring the Active Directory Infrastructure (25%)
- Configuring Additional Active Directory Server Roles (9%)
- Creating and Maintaining Active Directory Objects (24%)
- Maintaining the Active Directory Environment (13%)
- Configuring Active Directory Certificate Services (13%)

This guide will walk you through all the skills measured by the exam, as published by Microsoft.

Objectives

Chapter 1: Configuring Domain Name System (DNS) for Active Directory

Configure zones.

- May include but is not limited to: Dynamic DNS (DDNS), Non-dynamic DNS (NDDNS), and Secure Dynamic DNS (SDDNS), Time to Live (TTL), GlobalNames, Primary, Secondary, Active Directory Integrated, Stub, SOA, zone scavenging, forward lookup, reverse lookup

Configure DNS server settings.

- May include but is not limited to: forwarding, root hints, configure zone delegation, round robin, disable recursion, debug logging, server scavenging

Configure zone transfers and replication.

- May include but is not limited to: configure replication scope (forestDNSzone, domainDNSzone), incremental zone transfers, DNS Notify, secure zone transfers, configure name servers, application directory partitions

Chapter 2: Configuring the Active Directory Infrastructure

Configure a forest or a domain.

- May include but is not limited to: remove a domain, perform an unattended installation, Active Directory Migration Tool (ADMT) v3, raise forest and domain functional levels, interoperability with previous versions of Active Directory, alternate user principal name (UPN) suffix, forestprep, domainprep

Configure trusts.

- May include but is not limited to: forest trust, selective authentication versus forest-wide authentication, transitive trust, external trust, shortcut trust, SID filtering

Configure sites.

- May include but is not limited to: create Active Directory subnets, configure site links, configure site link costing, configure sites infrastructure

Configure Active Directory replication.

- May include but is not limited to: Distributed File System, one-way replication, Bridgehead server, replication scheduling, configure replication protocols, force intersite replication

Configure the global catalog.

- May include but is not limited to: Universal Group Membership Caching (UGMC), partial attribute set, promote to global catalog

Configure operations masters.

- May include but is not limited to: seize and transfer, backup operations master, operations master placement, Schema Master, extending the schema, time service

Chapter 3: Configuring Additional Active Directory Server Roles

Configure Active Directory Lightweight Directory Service (AD LDS).

- May include but is not limited to: migration to AD LDS, configure data within AD LDS, server core, Windows Server 2008 Hyper-V

Configure Active Directory Rights Management Service (AD RMS).

- May include but is not limited to: certificate request and installation, self-enrollments, delegation, Active Directory Metadirectory Services (AD MDS), Windows Server virtualization

Configure the read-only domain controller (RODC).

- May include but is not limited to: unidirectional replication, Administrator role separation, read-only DNS, BitLocker, credential caching, password replication, syskey, Windows Server virtualization

Configure Active Directory Federation Services (AD FS).

- May include but is not limited to: install AD FS server role, exchange certificate with AD FS agents, configure trust policies, configure user and group claim mapping, Windows Server virtualization

Chapter 4: Creating and Maintaining Active Directory Objects

Automate creation of Active Directory accounts.

- May include but is not limited to: bulk import, configure the UPN, create computer, user, and group accounts (scripts, import, migration), template accounts, contacts, distribution lists

Maintain Active Directory accounts.

- May include but is not limited to: configure group membership, account resets, delegation, AGDLP/AGGUDLP, deny domain local group, local versus domain, Protected Admin, disabling accounts versus deleting accounts, deprovisioning, contacts, creating organizational units (OUs), delegation of control

Create and apply Group Policy objects (GPOs).

- May include but is not limited to: enforce, OU hierarchy, block inheritance, and enabling user objects, group policy processing priority, WMI, group policy filtering, group policy loopback

Configure GPO templates.

- May include but is not limited to: user rights, ADMX Central Store, administrative templates, security templates, restricted groups, security options, starter GPOs, shell access policies

Configure software deployment GPOs.

- May include but is not limited to: publishing to users, assigning software to users, assigning to computers, software removal

Configure account policies.

- May include but is not limited to: domain password policy, account lockout policy, fine-grain password policies

Configure audit policy by using GPOs.

- May include but is not limited to: audit logon events, audit account logon events, audit policy change, audit access privilege use, audit directory service access, audit object access

Chapter 5: Maintaining the Active Directory Environment

Configure backup and recovery.

- May include but is not limited to: using Windows Server Backup, back up files and system state data to media, back up and restore by using removable media, perform an authoritative or non-authoritative Active Directory restore, linked value replication, Directory Services Recovery Mode (DSRM) (reset admin password), back up and restore GPOs

Perform offline maintenance.

- May include but is not limited to: offline defragmentation and compaction, Restartable Active Directory, Active Directory database storage allocation

Monitor Active Directory.

- May include but is not limited to: Network Monitor, Task Manager, Event Viewer, ReplMon, RepAdmin, Windows System Resource Manager, Reliability and Performance Monitor, Server Performance Advisor, RSOP

Chapter 6: Configuring Active Directory Certificate Services

Install Active Directory Certificate Services.

- May include but is not limited to: standalone versus enterprise, CA hierarchies—root versus subordinate, certificate requests, certificate practice statement

Configure CA server settings.

- May include but is not limited to: key archival, certificate database backup and restore, assigning administration roles

Manage certificate templates.

- May include but is not limited to: certificate template types, securing template permissions, managing different certificate template versions, key recovery agent

Manage enrollments.

- May include but is not limited to: network device enrollment service (NDES), autoenrollment, Web enrollment, smart card enrollment, creating enrollment agents

Manage certificate revocations.

- May include but is not limited to: configure Online Responders, Certificate Revocation List (CRL), CRL Distribution Point (CDP), Authority Information Access (AIA)

Chapter 1 - Configuring Domain Name System (DNS) for Active Directory

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Configure zones.

Information in this section may include but is not limited to: Dynamic DNS (DDNS), Non-dynamic DNS (NDDNS), and Secure Dynamic DNS (SDDNS), Time to Live (TTL), GlobalNames, Primary, Secondary, Active Directory Integrated, Stub, SOA, zone scavenging, forward lookup, reverse lookup

Dynamic DNS (DDNS)

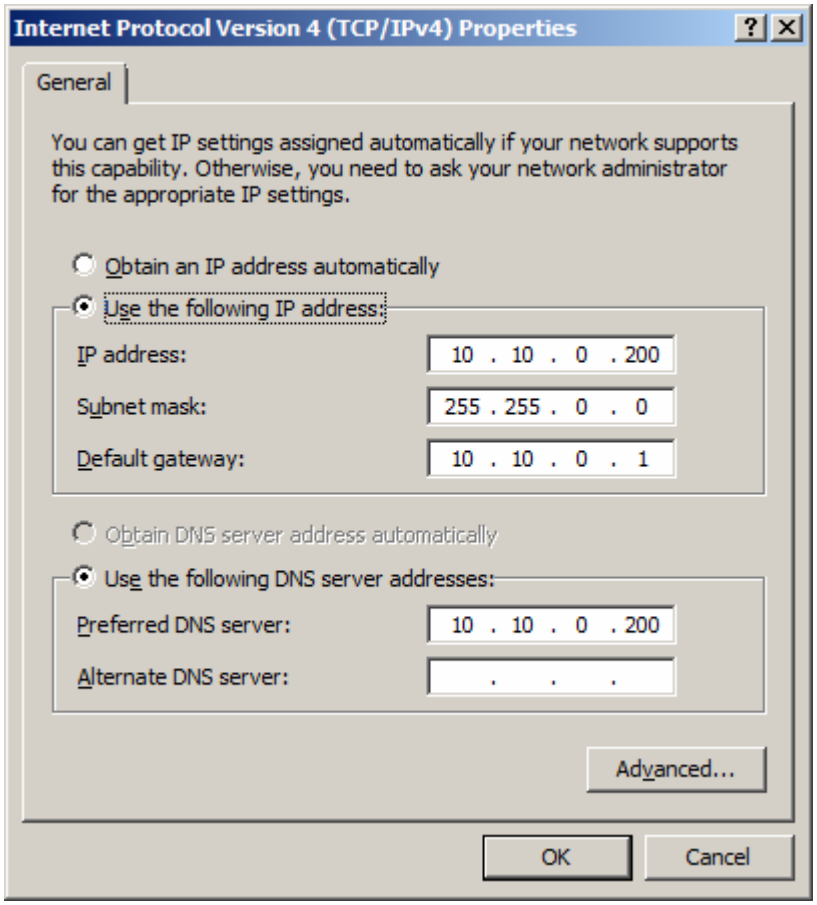
Dynamic DNS was introduced in Windows 2000 and allows resource records to be updated in real-time. When a user goes to the command prompt and types ipconfig/registerdns, this triggers the DNS server to accept the registration. This only happens if the computer is part of the domain. It is possible to control how the records are going to be accepted in the domain by making changes to the domain properties. Dynamic DNS requires less Administrative overhead because DNS registrations are done automatically. This is one of the requirements that DNS must pass before Directory Services can be installed into the environment.

One of the other uses is to replace the old WINS (Windows Internet Name Servers). Before DDNS DNS was static and stored in text files. This type of DNS was inherent into the Windows NT family of Operating Systems. The only way to make DNS dynamic was to integrate it with WINS. On the other hand, to update the DNS you would manually copy the file on to the other DNS machines within the network With the advent of DDNS, which integrates into Active Directory, this step is no longer necessary. The first version of DDNS appeared in Windows 2000 and has evolved with each release of the Windows Server platform.

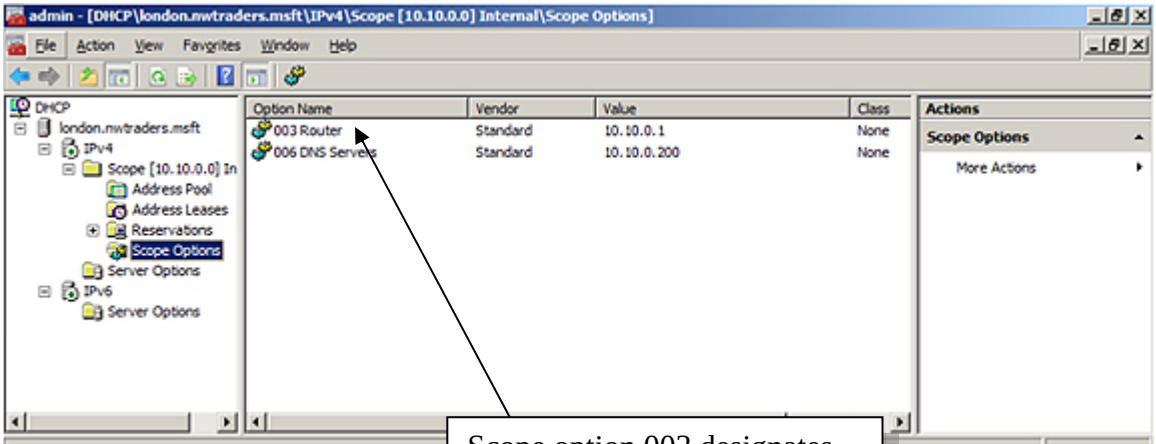
When IP addresses are leased to client machines the DNS is automatically updated with this information. Registration may be forced by typing from the command prompt:

```
C:\Users\Administrator>ipconfig /registerdns
```

This will force the DNS server to update the information of the client. To make this happen ensure that there are the correct DNS entries in the IPv4 settings. If not, the client will not be able to communicate with the DNS server.



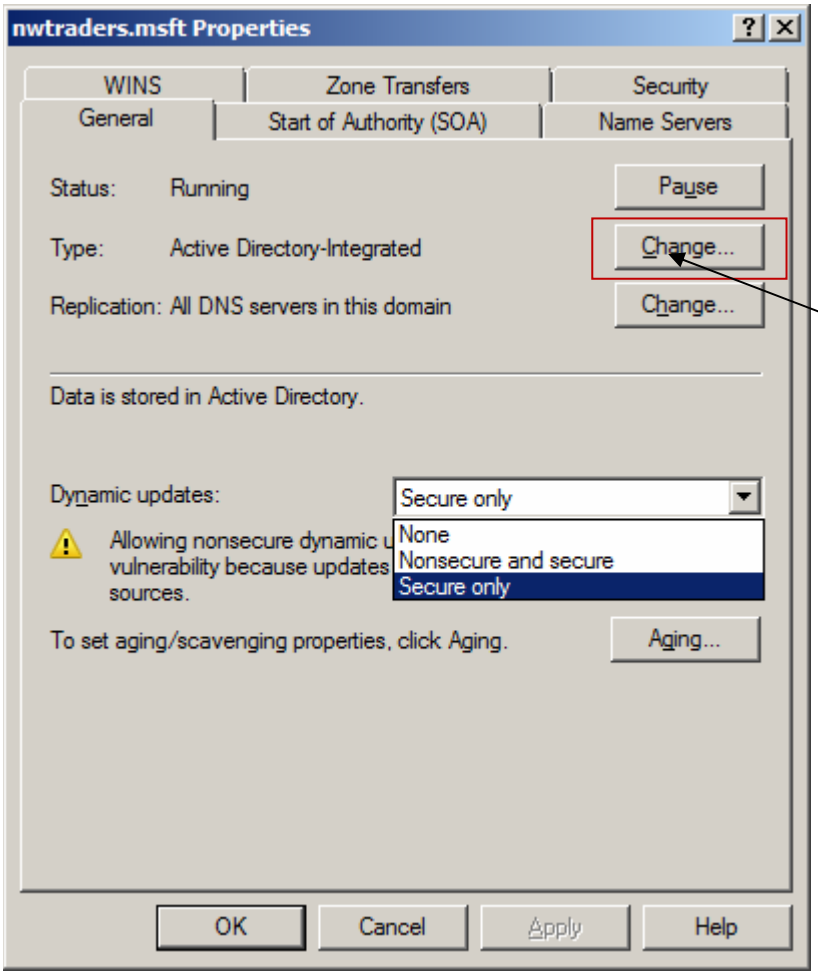
In this example the Preferred DNS server is set to 10.10.0.200. When the ipconfig/registerdns command is executed, it will interact with the 10.10.0.200 server. If the information was assigned through the DHCP server, then the information would be updated based on the Scope Option 006, which identifies the DNS server.



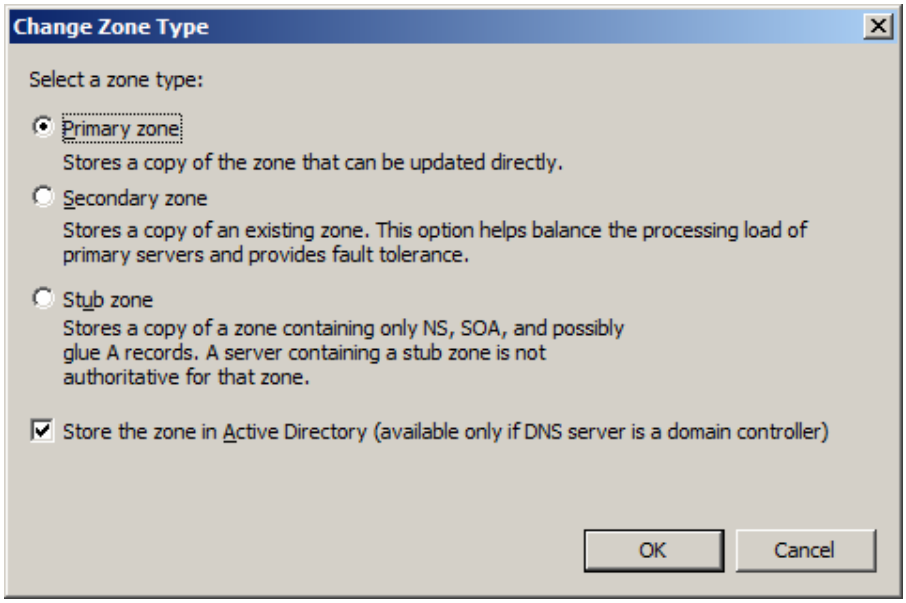
Scope option 003 designates the Default Gateway entry and 006 designates the DNS

Non-dynamic DNS (NDDNS)

Non-dynamic DNS is a representation of the original version of DNS. It has to be updated manually. The text file containing DNS entries is located under %SystemRoot%\System32\DNS.



By clicking the Change button it is possible to change the type of DNS that is being used. Dynamic DNS is considered best practice for implementing a Windows 2008 DNS server and have it integrate with Active Directory.

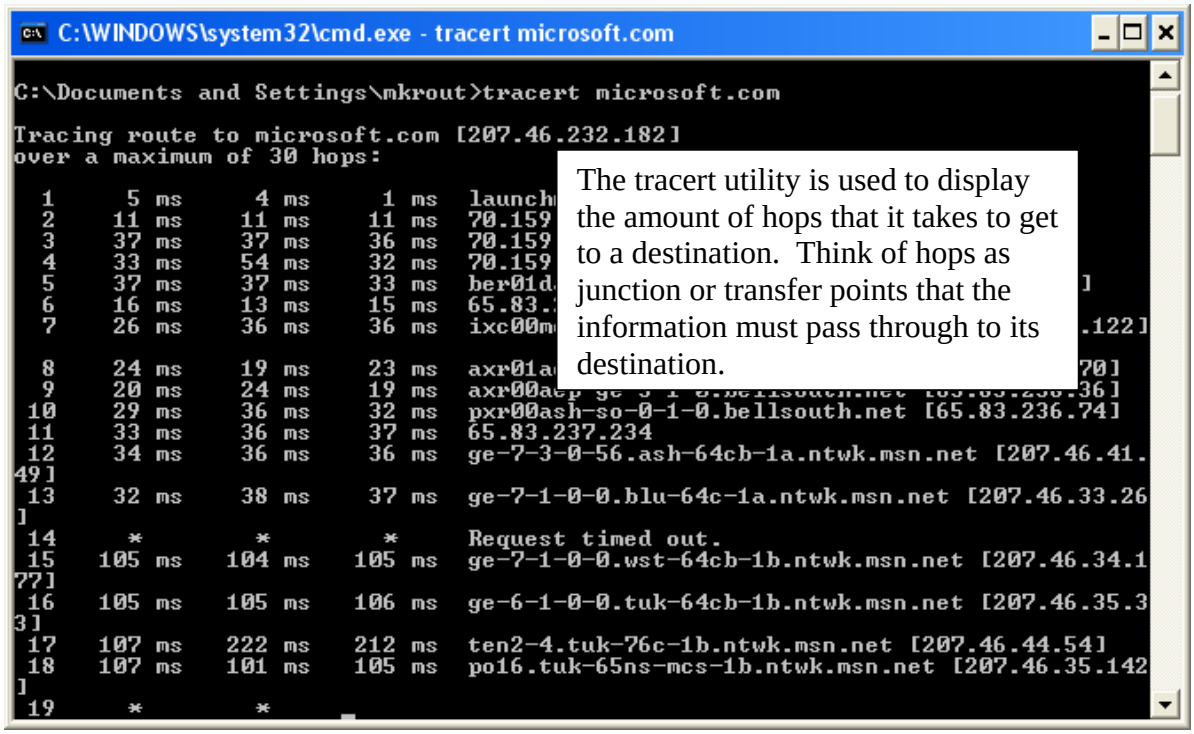


Secure Dynamic DNS (SDDNS)

Secure DNS is DNS that is updated over a secure channel. When transfers are initiated, the DNS server will check to see if the DNS server trying to forward an update is on the allowed list. This prevents poison entries (falsified records) from infecting the DNS environment. When an Active Directory integrated zone is set up, this feature is automatically initiated.

Time to Live (TTL)

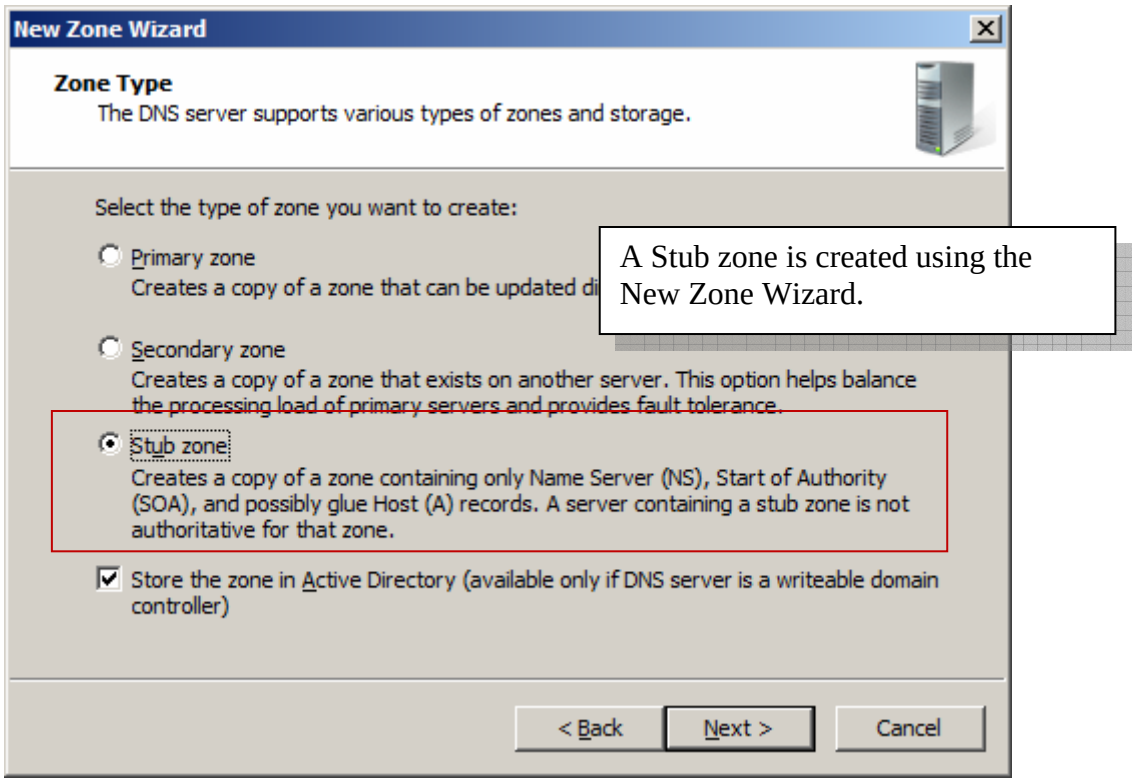
TTL is the amount of time a packet will survive on a network before it is discarded. In the following example the Minimum TTL is set to 1 Hour. The TTL for the SOA is set for 1 day.



Stub zone

A Stub zone serves as a source of current information for the Primary DNS zone server and authoritative zones for the network. Here are some reasons to use a Stub zone:

- Keep delegated zone information current
- Improve name resolution
- Simplify DNS Administration

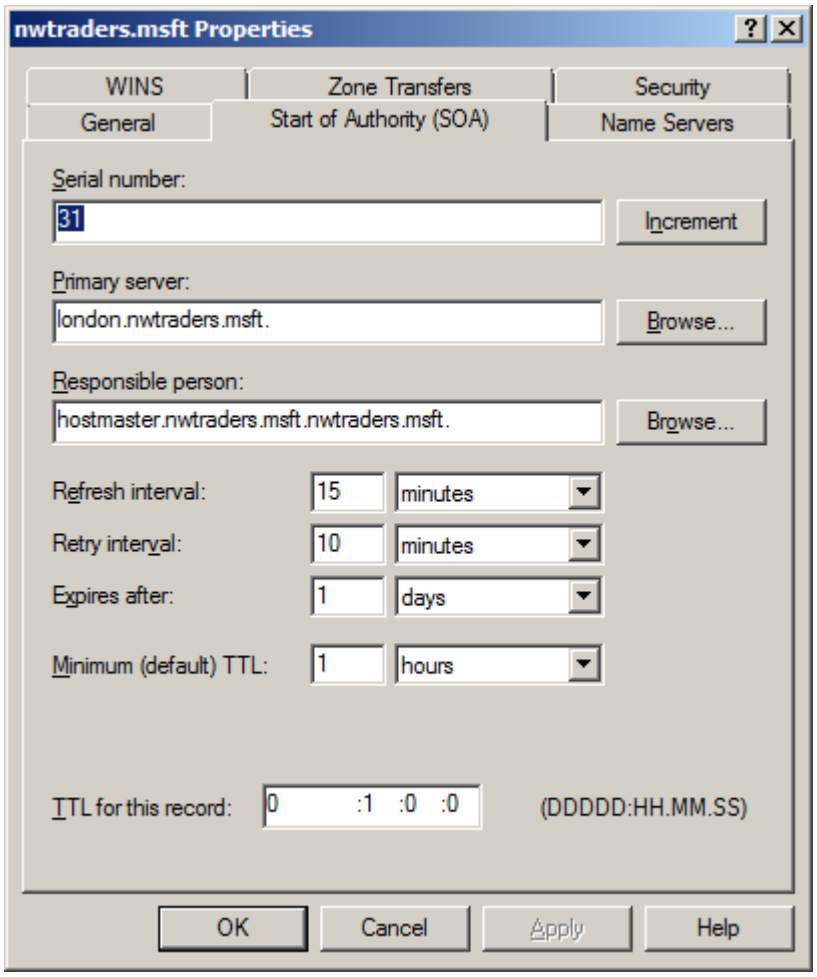


SOA

Start of Authority defines which DNS server is in charge of a zone. In the graphic below, notice the properties of the nwtraders.msft zone and the settings for the SOA record.

The SOA record specifies the following for the zone:

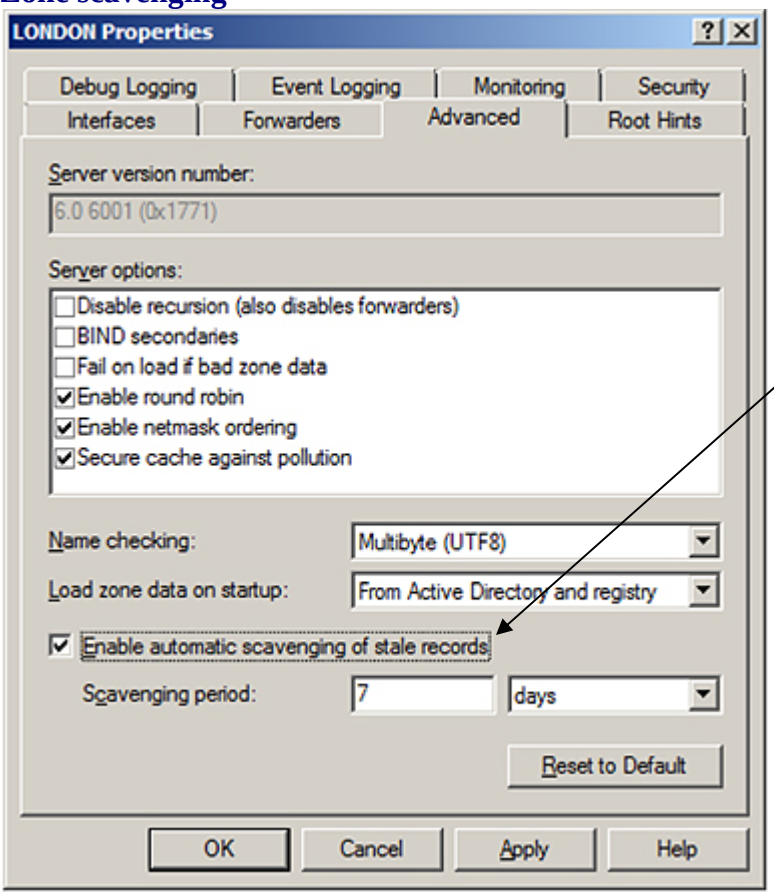
- Primary Server
- Zone Administrator's email address
- Secondary zone expiration values
- Minimum default TTL values for zone resource records



Global Names

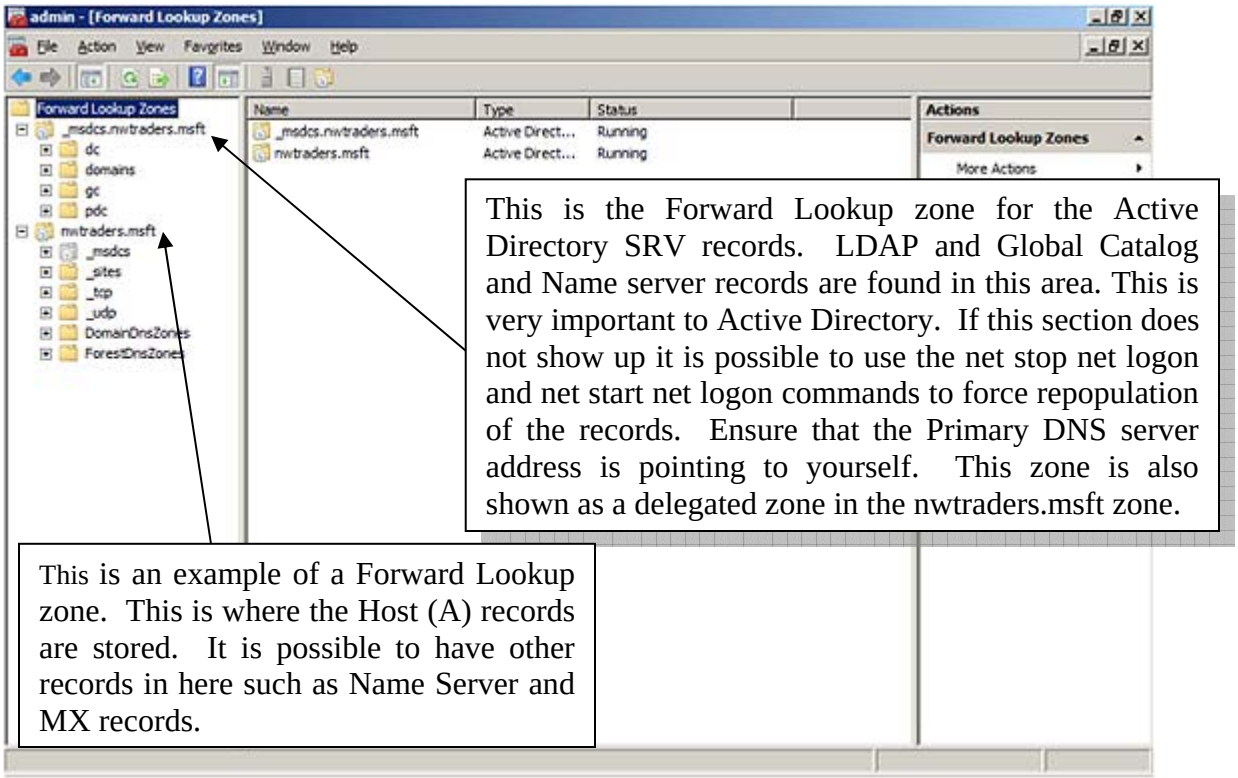
Global Name Zone (GNZ) is designed to enable the resolution of single-label, static, global names for servers using DNS. GNZ is intended to aide retirement of WINS. The purpose of a DNS server is to house different information, such as IP addresses which are associated to domain names. When website is looked up such as http://www.microsoft.com, the DNS server in the internal network will query the other DNS servers to find out who is www or it will check to see what is the IP address of the www (A Record). The DNS server will Global Names zone that is associated with the host name. If it is not available or is not found the authoritative zone records are checked. If the authoritative zone does not have the answer a query is sent to the next DNS. Once a record is found the information is returned to the client and the client can connect to the server. In this instance, it is the web server.

Zone scavenging



This is the setting within the DNS server properties that controls when records are removed from the DNS server. These are records that are considered to be invalid. This process is known as Zone Scavenging.

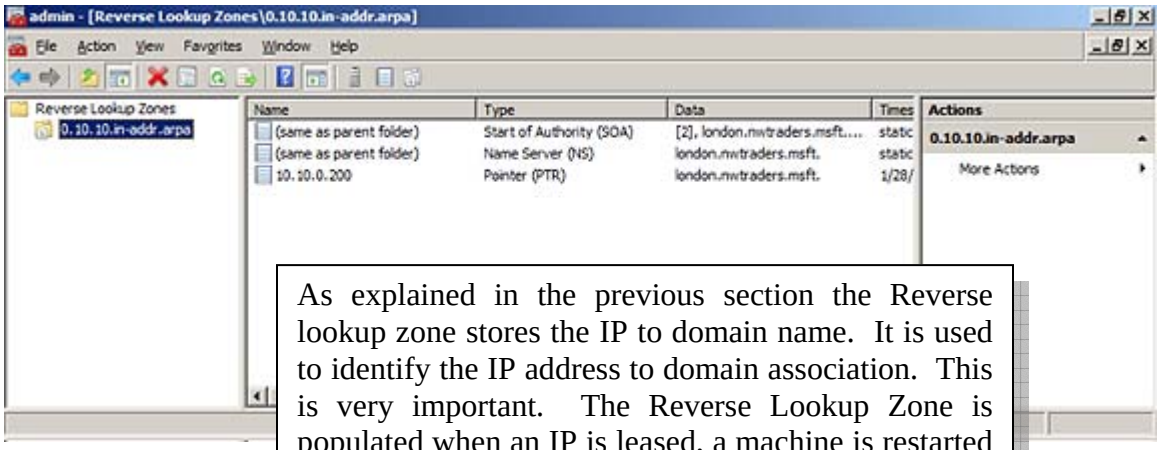
Forward Lookup



This is the Forward Lookup zone for the Active Directory SRV records. LDAP and Global Catalog and Name server records are found in this area. This is very important to Active Directory. If this section does not show up it is possible to use the net stop net logon and net start net logon commands to force repopulation of the records. Ensure that the Primary DNS server address is pointing to yourself. This zone is also shown as a delegated zone in the nwtraders.msft zone.

This is an example of a Forward Lookup zone. This is where the Host (A) records are stored. It is possible to have other records in here such as Name Server and MX records.

Reverse Lookup



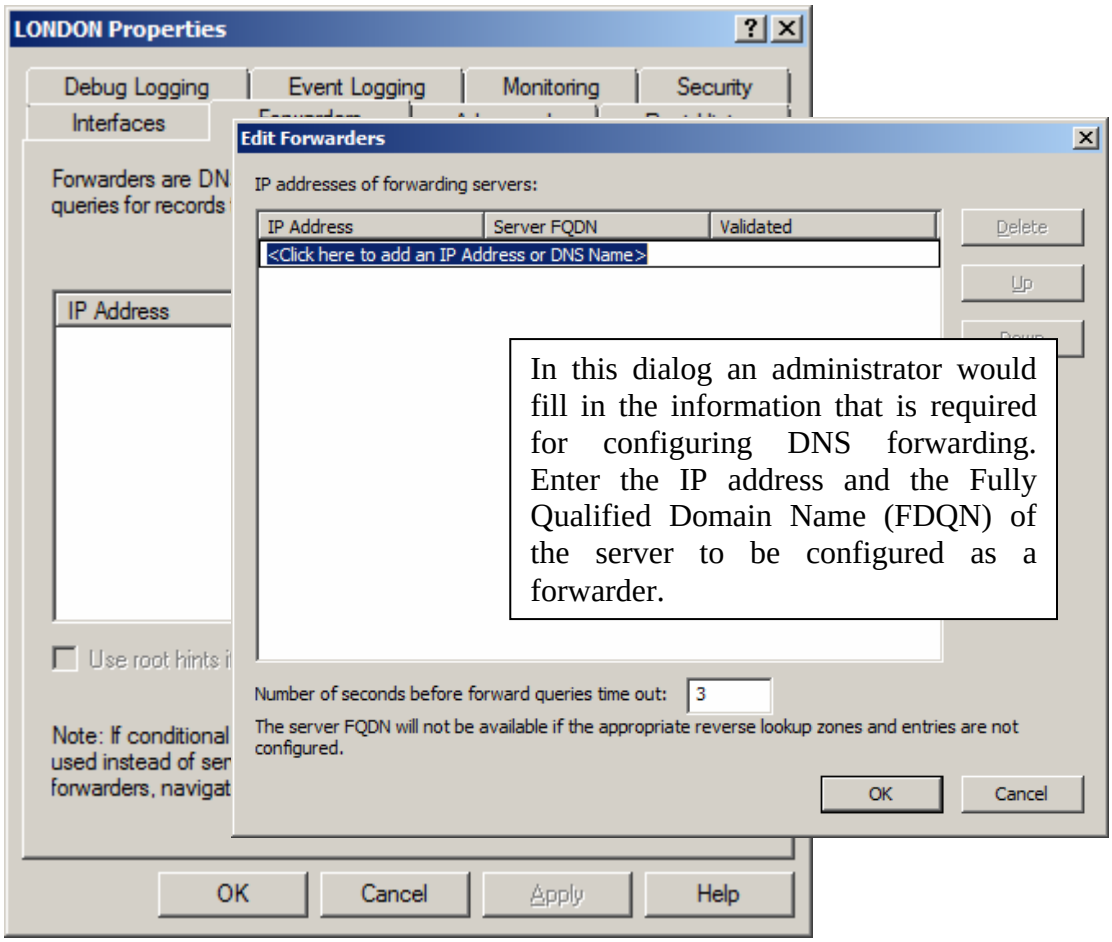
As explained in the previous section the Reverse lookup zone stores the IP to domain name. It is used to identify the IP address to domain association. This is very important. The Reverse Lookup Zone is populated when an IP is leased, a machine is restarted or when ipconfig/registerdns is executed from a given host.

Configure DNS server settings.

Information in this section may include but is not limited to: forwarding, root hints, configure zone delegation, round robin, disable recursion, debug logging, server scavenging.

Forwarding

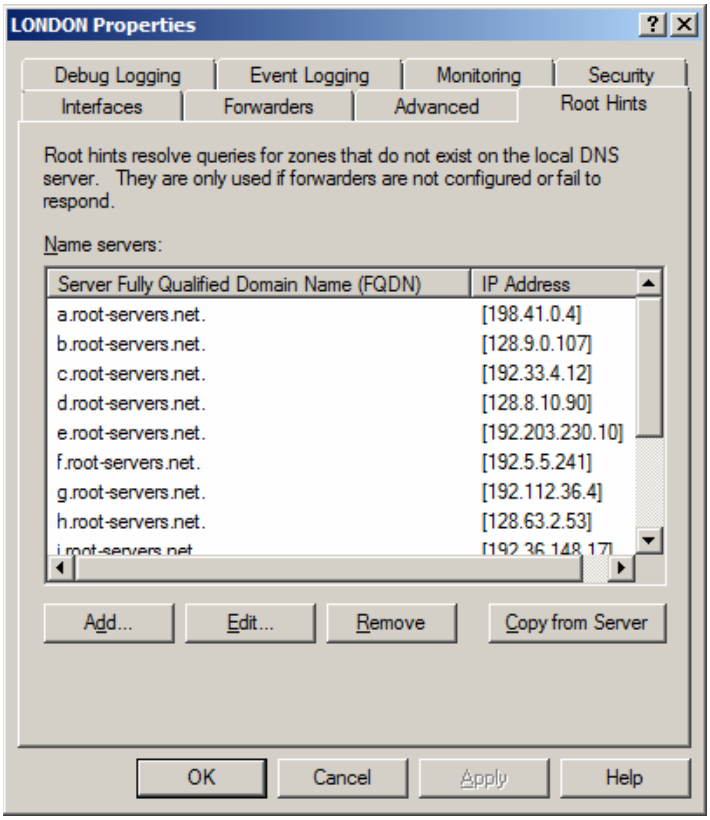
When a request is forwarded to a DNS server its database is being searched for the specific record. No DNS server maintains records for the entire Internet or an Intranet environment, therefore requests are sent to a DNS server to find the DNS server that is authoritative for a given zone.



In this dialog an administrator would fill in the information that is required for configuring DNS forwarding. Enter the IP address and the Fully Qualified Domain Name (FDQN) of the server to be configured as a forwarder.

Root Hints

Root Hints are important in configuring a DNS Server. If a server receives a query for an unknown domain, the root hints give a clue as to where to search for the answer. Root Hints provide a link between a DNS Server and top level DNS Servers on the internet. Because these IP addresses remain constant, Microsoft automatically loads them into the DNS Server's root hints. Everything works correctly unless a server is not allowed to connect to the internet, in which case a '.' local Root domain needs to be created.

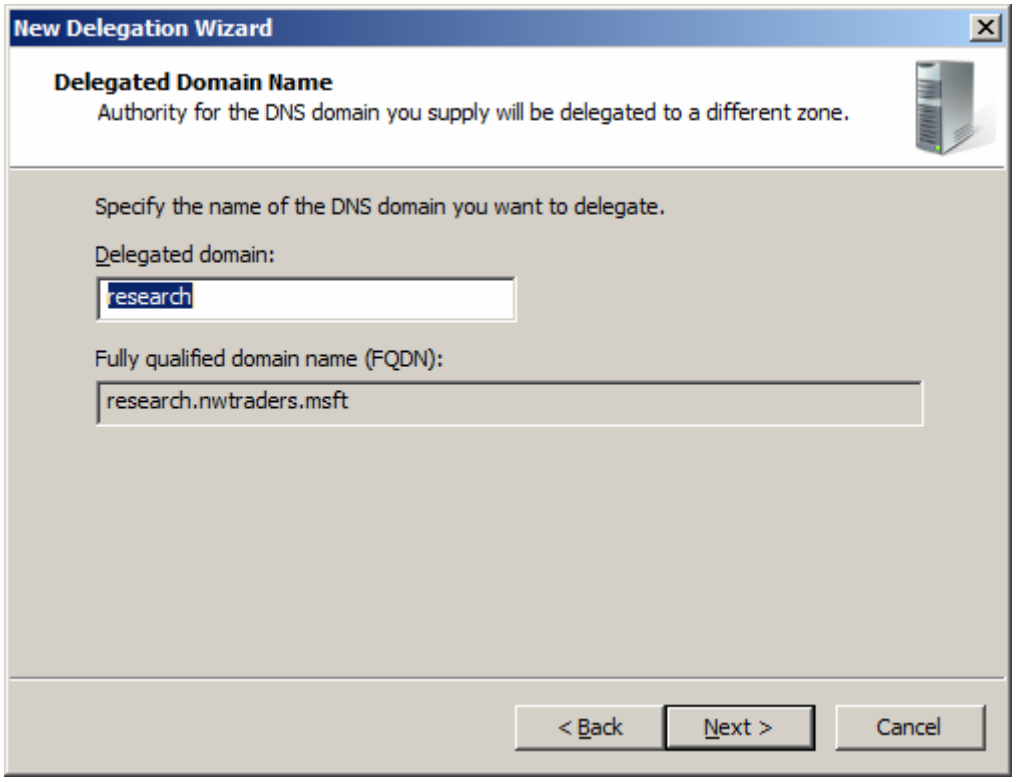


Configure zone delegation

The DNS utility gives the option of dividing up namespaces into one or more zones, which can be stored, distributed, and replicated to other DNS servers. Some reasons to use additional zones include:

- To delegate responsibility to another organization or department
- To break up a large namespace into to smaller sections to aid in management
- To extend the namespace and add additional sub-domains at once

When a zone is delegated, remember that for each new zone that is created, delegation records are needed in other zones that point to the authoritative DNS servers for the new zone. The reason these records are needed is to transfer authority and provide correct referral to other DNS Servers. Also, clients of the new servers that are being made authoritative for the new zone will be updated. A user must be an Administrator to complete the delegation of a zone.

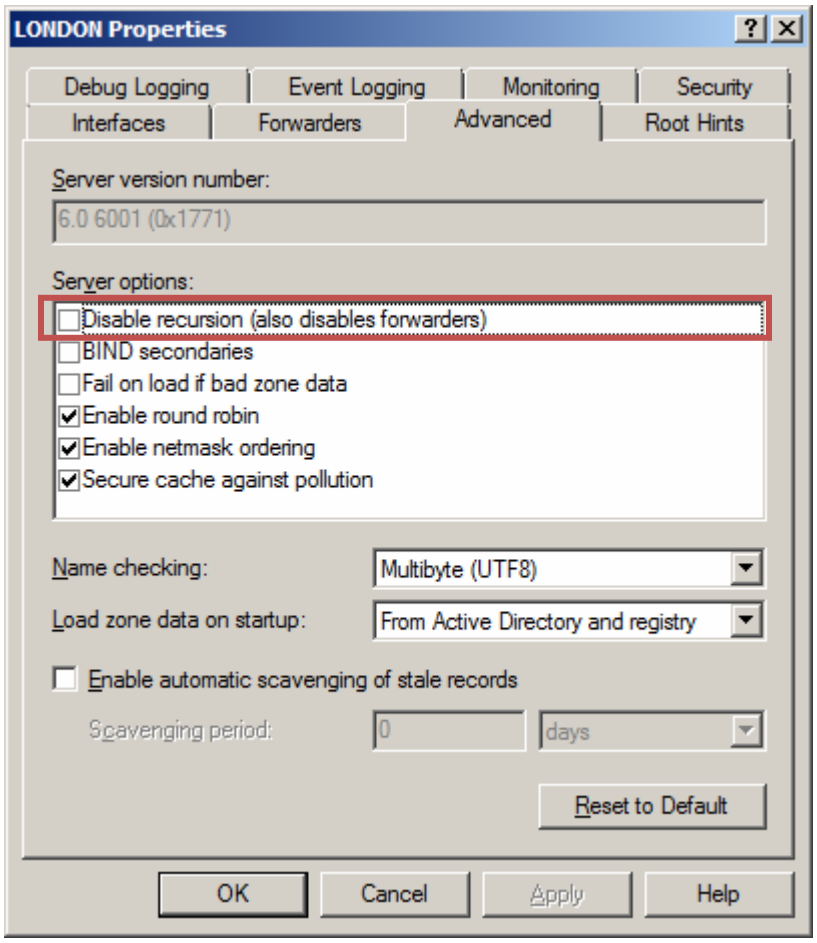


Round Robin

Round Robin is a load balancing technique in which balance of power is placed on the DNS Server instead of on the actual machine itself as in Network Load Balancing (NLB). Round Robin works on a rotating basis. IP addresses are given out and then return to the end of the list. This is done in a looping fashion. This is typically used with Web Servers but has been replaced by Network Load Balancing (NLB). When a user connects to a Web server the first IP address is given out and then it is sent to the end of the list. The next user connects and is given another IP address of another Web Server. For this to work the content needs to be on both Web Servers. This ensures that if a Web Server is not available another can take the load.

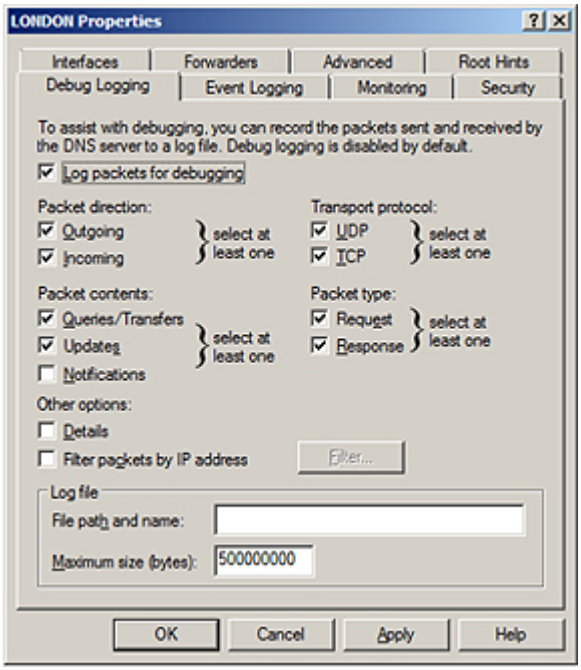
Disable Recursion

When this setting is activated in a DNS server it will not forward requests to any other server or answer any requests from any other server. This is a security technique and is used in protected environments.



Debug logging

Debug logging is used to troubleshoot DNS problems. This option is turned off by default.



Packet Contents

Standard queries - Standard queries (per RFC 1034) are logged in the DNS server log file.

Updates - Dynamic updates (per RFC 2136) are logged in the DNS server log file.

Notifies - Notifications (per RFC 1996) are logged in the DNS server log file.

- **Transport protocol**

UDP - Sent and received packets over UDP are logged in the DNS server log file.

TCP - Sent and received packets over TCP are logged in the DNS server log file.

- **Type of packet**

Request - A request packet is characterized by a QR bit set to 0 in the DNS message header and are logged in the DNS server log file.

Response - A response packet is characterized by a QR bit set to 1 in the DNS message header and are logged in the DNS server log file

- **Filter packets by IP address** – This Provides additional filtering of packets logged in the DNS server log file. This option allows logging of packets sent from specific IP addresses to a DNS server, or from a DNS server to specific IP addresses.

Server scavenging

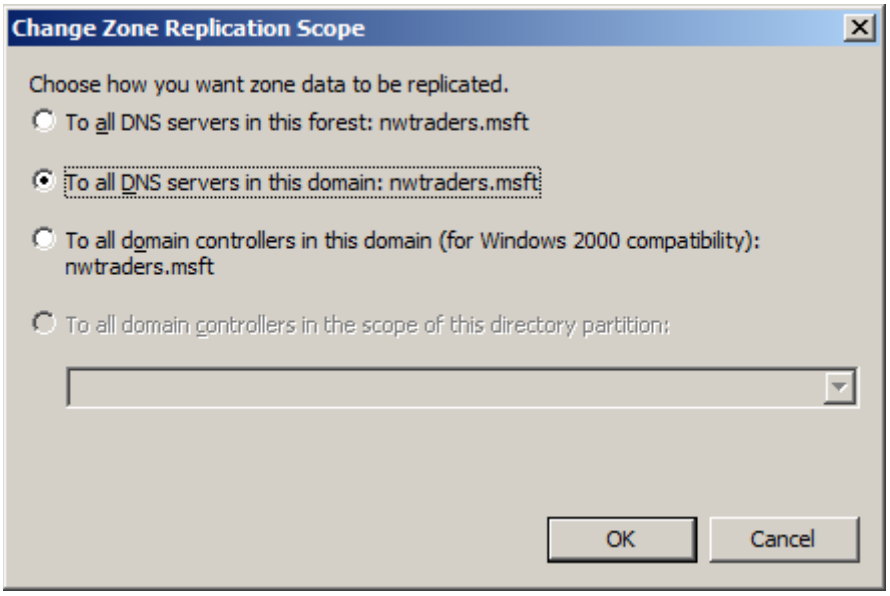
Server scavenging is the process of getting rid of stale DNS records. This service can be stopped, started and customized via a script. Sample scripts to perform these tasks can be found on Microsoft's website.

Configure zone transfers and replication.

Information in this section may include but is not limited to: configure replication scope (forestDNSzone, domainDNSzone), incremental zone transfers, DNS Notify, secure zone transfers, configure name servers, application directory partitions.

Configure replication scope (forestDNSzone, domainDNSzone)

When DNS is integrated with Active Directory there are two containers that are created. The first container is the forestDNSzone. It is used to store all the information for the forest. When an administrator selects what to replicate all information through the forest this zone is replicated. The second zone is the domainDNSzone. This is used for domain wide replication. When an administator selects what they want replicated to only within the domain this partition is used in the replication.

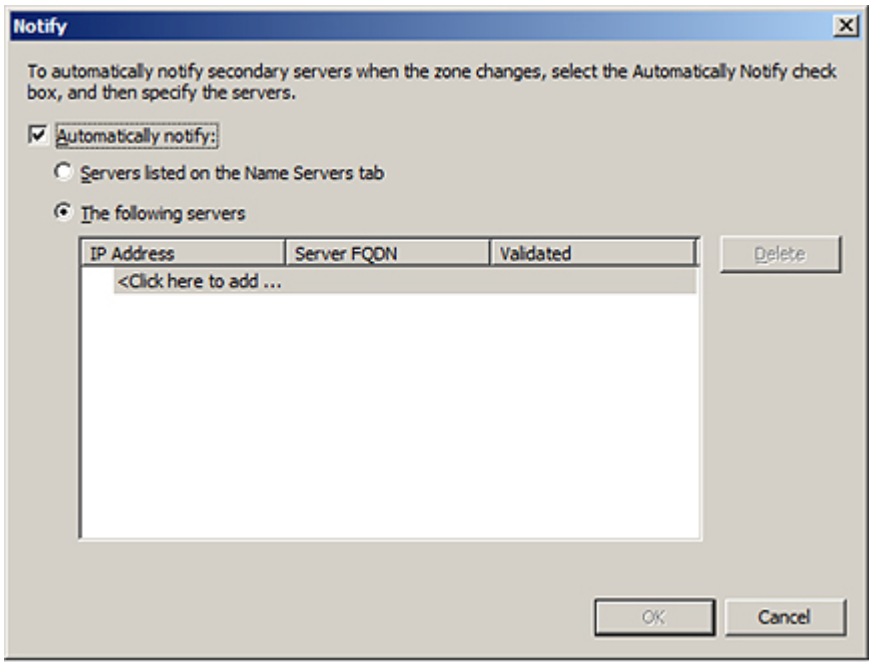


Incremental zone transfers

An incremental zone transfer involves replicating only changes in DNS to another DNS server. Instead of replicating all zones to the DNS zone partners only changes are replicated.

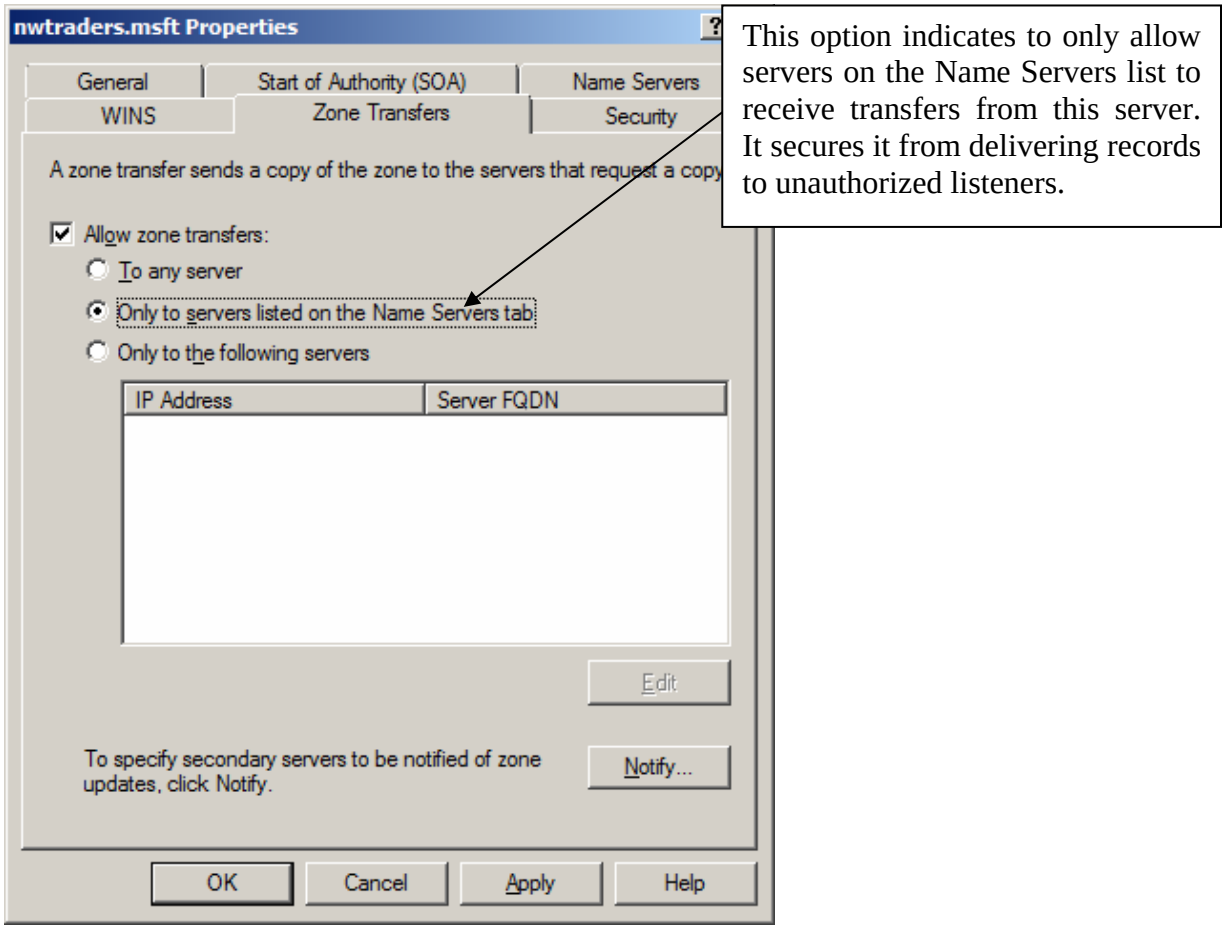
DNS Notify

DNS notify occurs when there are changes to the DNS and there have been servers set up to accept zone transfers. The DNS server will notify the other servers that changes have been made to the DNS server and need to be sent to update the records.



Secure zone transfers

Secure zone transfers are used to protect DNS data from being intercepted. When DNS is integrated with Active Directory it designates that only secure zone transfers are desired.



Configure name servers

Name Servers are the actual DNS servers that host that zone. They also designate DNS servers that communicate with the DNS servers. This will prevent zone transfers from going to non-authorized servers.

Application directory partitions

The application directory partition holds data that is specific to one or more directory-enabled applications. Application directory partitions can contain any type of object. The application data partition is only replicated to certain domain controllers. The member of the replication will have a replica of the data. Administrators can use Ntdsutils to create application directory partitions for testing purposes. The ForestDNSZone is an example of an application directory partition. The information in this partition is replicated to all domain controllers in the forest.

Chapter 2 - Configuring the Active Directory Infrastructure

Configure a forest or a domain.

May include but is not limited to: remove a domain, perform an unattended installation, Active Directory Migration Tool (ADMT) v3 (pruning and grafting), raise forest and domain functional levels, interoperability with previous versions of Active Directory, alternate user principal name (UPN) suffix, forestprep, domainprep

Remove a domain.

Removing a domain from Active Directory can be accomplished by using the dcpromo command line utility. It is also necessary to identify if there are any additional domain controllers that may be Global Catalog servers. When Active Directory is removed from a domain controller, it reverts back to SAM (Security Accounts Manager) and will lose all the security features of Directory Services.

Perform an unattended installation.

An unattended installation is used to roll out new domain controllers into an existing forest. An answer file should be created that will automatically respond to the normal questions asked during the installation. To start the unattended installation, use dcpromo and switches such as /answer /unattend. For more information type dcpromo /?.

Active Directory Migration Tool (ADMT)

Active Directory Migration tool makes it a simple process to migrate data from:

- Different Forests
- Same Forests
- Domains

It is widely used in migration for Exchange Servers such as Exchange 2000 to Exchange 2003.

Raise forest and domain functional levels.

The default functional level for Windows 2008 Forest and Domain is Windows 2000 native mode. There are certain limitations and benefits for raising to the next functional level. Keep in mind that all domain controllers must be changed to support each of the different functional levels. Example: There is a domain that has NT, 2000, Windows 2003, and Windows 2008 domain controllers and you are in Windows 2003 Interim and want to move to Windows 2003 server mode. All domain controllers would need to be upgraded to Windows 2003 and above.

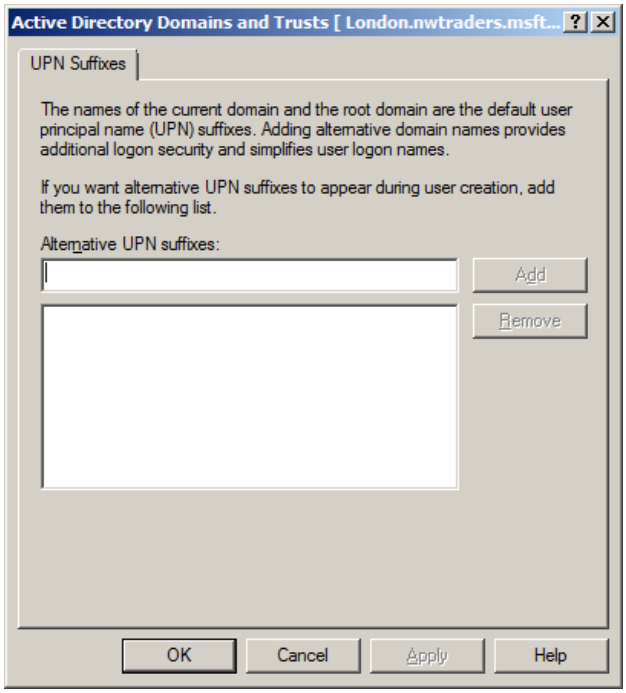
It is possible to change the domain functional level using the Active Directory Users and Computers, Active Directory Sites and Services and Active Directory Domains and Trusts. To raise the functional level of the forest use the Active Directory Domains and Trusts. To raise the forest functional level ensure that all domains are at the required level before attempting to accomplish this task. All domains for a Windows 2003 server mode must be Windows 2003 server mode before it is possible to raise the functional level of the Forest.

Interoperability with previous versions of Active Directory.

The different versions of Active Directory will work together but depending on the changes it is possible to experience differences. The changes from Windows 2003 to Windows 2008 are not significant. There is not much benefit from raising the Domain and Forest functional levels to Windows 2008 from Windows 2003. However, raising from Windows 2000 to Windows 2008 will produce significant benefits.

Alternate user principal name (UPN) suffix

There are instances when if a system is hosting email or domains for other organizations that where an alternate UPN suffix may be needed. This is configured using the Active Directory Domains and Trusts.



One of the uses would be to provide additional email addresses for an Exchange 2003 organization. This has been replaced in Exchange Server 2007.

Forestprep

Forestprep is the command that is used to ready the Forest for a new application such as Exchange Server or Windows 2008. Run this command to modify the Schema of Active Directory. This updates the classes and attributes within Active Directory to support the new services. Forestprep needs to be done where the Forest root domain controller is located. This will be the first domain controller installed into the Forest.

Domainprep

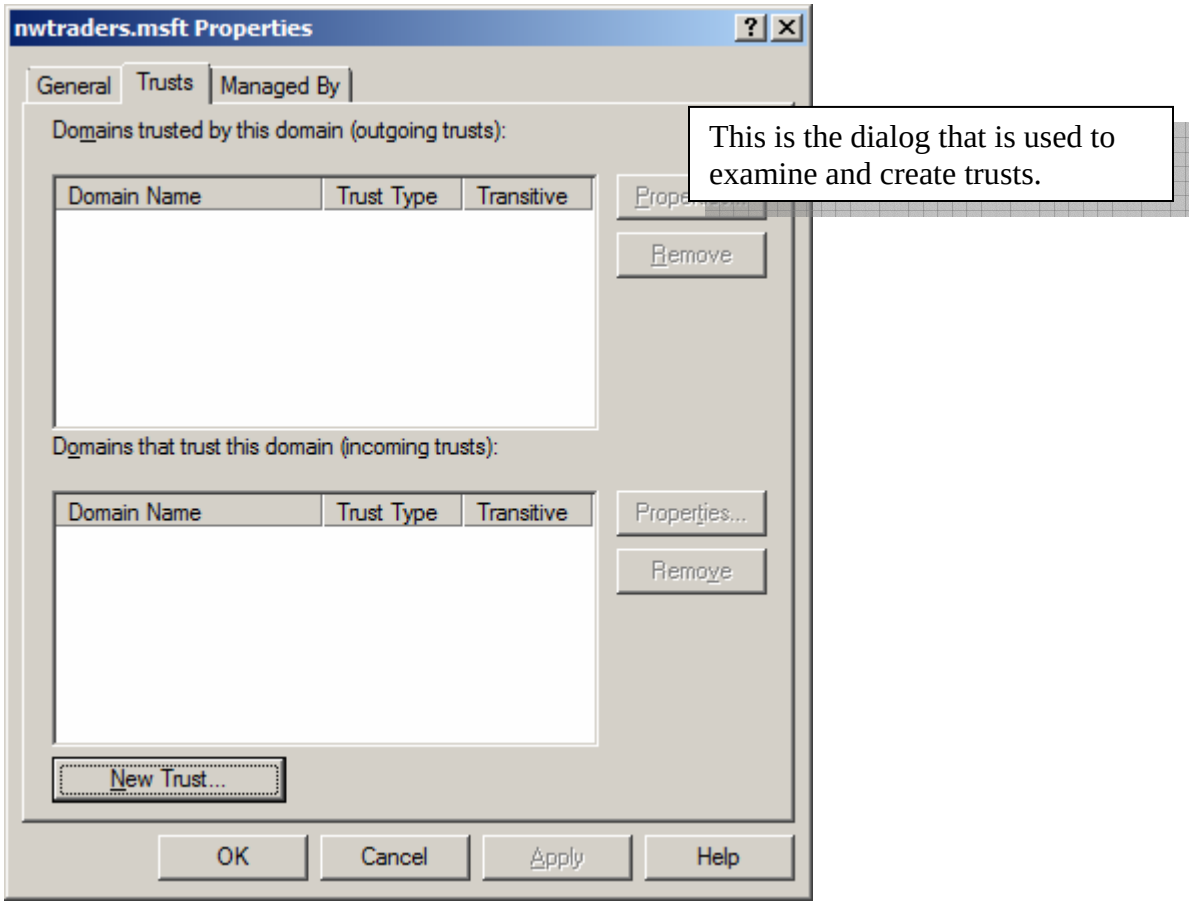
Domainprep is used to ready the domain for a new application. Domainprep creates the new security groups that are need to support the application. This needs to run in each of the domains that is going to be used with the new application.

Configure trusts.

May include but is not limited to: forest trust, selective authentication versus forest-wide authentication, transitive trust, external trust, shortcut trust, SID filtering

Forest trust

A reason to create Forest Trusts is to share resources between forests. If a forest trust is a two-way trust, authentication requests that are made in either forest can reach the other forest.



Some of the benefits of using trust are as follows:

- Simplified management across two forests
- Complete two-way trust relationships with every domain in each forest
- Access to forest authentication using a User Principal name (UPN)
- Flexibility of administration

Forest trusts are limited to only two Forests at a time. Both of the Forests must be of the same Level. It is recommended they be Windows 2008.

Selective authentication versus forest-wide authentication

Forest wide authentication allows anyone to connect or authenticate based on the permissions that are set in place within the Forest. Selective authentication allows the administrators to approve who is connected to the Forest ahead of time. This ensures that only individuals that are supposed to have access to resources have that access granted to them.

Transitive trust

A trust is transitive when both sides trust each other automatically. When a new domain is added to an existing Forest the new domain will have a transitive relationship to the Forest Root. When an additional domain is added to another domain the domain will have a transitive trust with the parent domain.

External trust

An external trust is used to provide access to resources that are located on a Windows NT 4.0 domain or domain that is located in a separate forest that is not joined by a forest trust.

Shortcut trust

Use shortcut trusts to improve user logon times between two domains within a Windows Server 2008 forest. This is useful when two domains are separated by two domain trees.

SID filtering

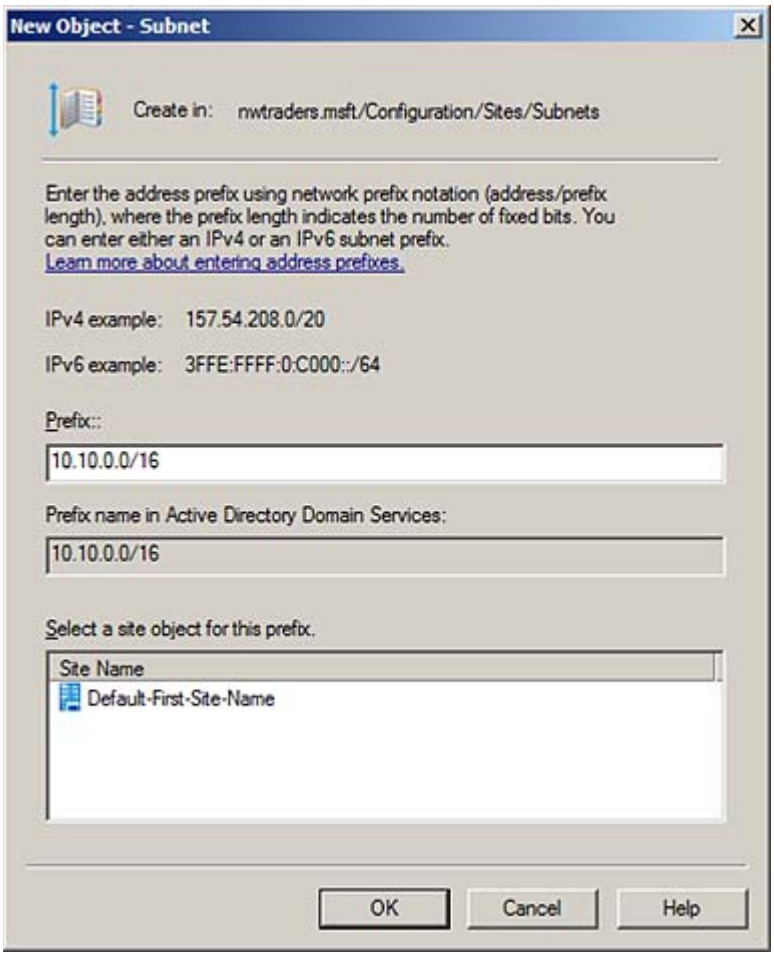
SID Filtering is used with external trusts. When security principals are created in a domain, the domain SID is included in the security principal's SID to identify the domain in which the security principal was create. The domain SID is important because it identifies a security principal home. Outgoing trusts that are created from the trusting domain use SID filtering to verify that incoming authentication requests are coming from a trusted source. This is accomplished by comparing the Domain SID's of the security principals. If the SID's do not compare then the offending SID is removed.

Configure sites.

May include but is not limited to: create Active Directory subnets, configure site links, configure site link costing, configure sites infrastructure.

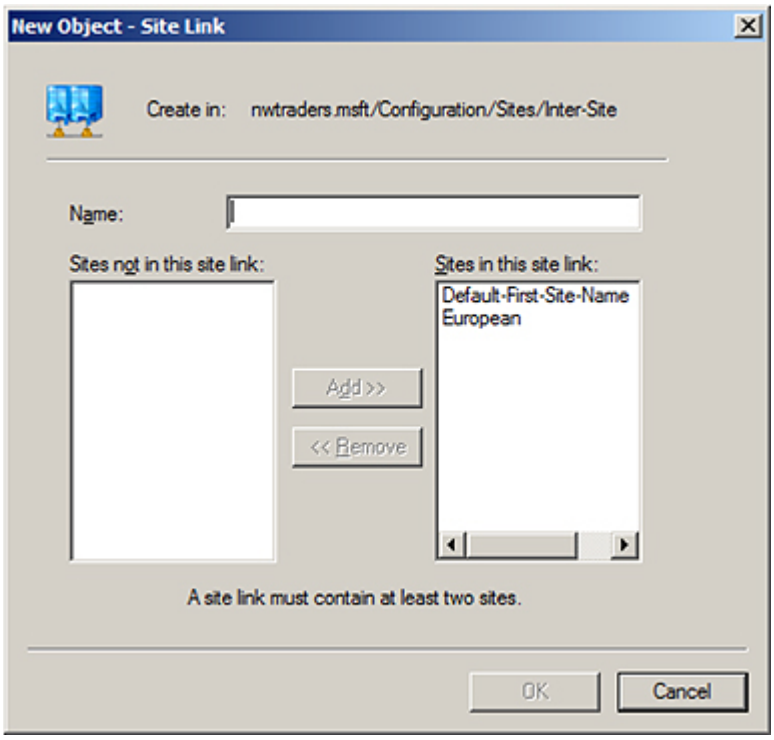
Create Active Directory subnets

When examining Active Directory there are two ways of approaching it. It is possible to look at the logical configuration (known as the Domain and Forest topology), or it is possible to look at the physical configuration. The physical configuration of Active Directory involves IP subnets. IP subnets are created by using the Active Directory Sites and Services utility.



Configure site links

Site Links represent the connection object between two Active Directory sites. This is used to provide a replication path.



This is the dialog box that used to create Site Links. A site link controls the traffic of replication through out the environment.

Configure site link costing

Configure site link costing is used to control what type of traffic and the frequency of the traffic being replicated to the domain controllers across the Site links. It is possible to control which link to use by raising the cost of the link. If it is a link that is highly taxed with traffic then it may be advisable to direct the traffic to another site link. The higher the cost the less probability this link will be used. It works the same as a routing algorithm.

Configure sites infrastructure

To configure the site infrastructure an administrator would configure subnets and connect those to sites. Then from the sites they connect a site link. This will configure the replication of Active Directory data so that all domain controllers are up to date with changes made in the environment.

Configure Active Directory replication.

May include but is not limited to: Distributed File System, one-way replication, Bridgehead server, replication scheduling, configure replication protocols, force intersite replication

Distributed File System

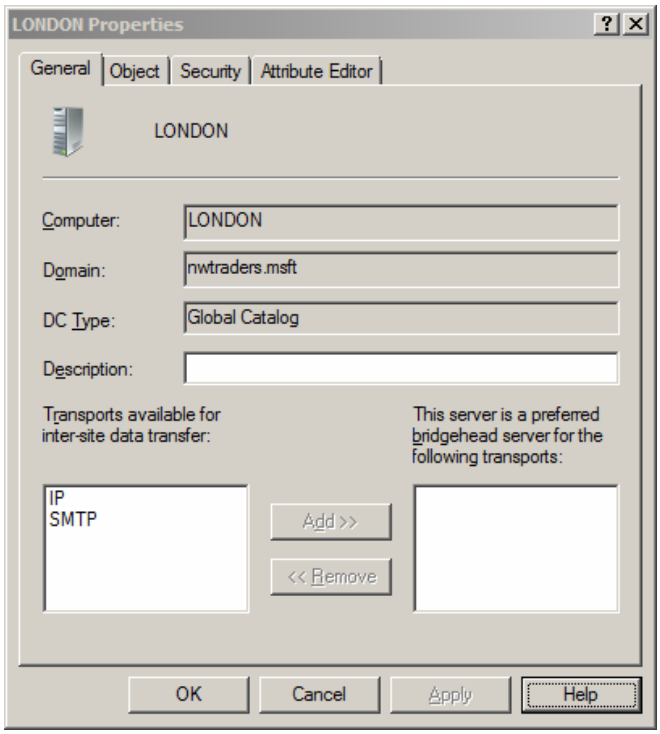
The Distributed File System is used to allow the creation of universal shares that are replicated to other servers. When one server is not available it will be directed to an available replica. It is possible to create a Domain based DFS which is replicated through Active Directory or create a Stand-alone DFS infrastructure.

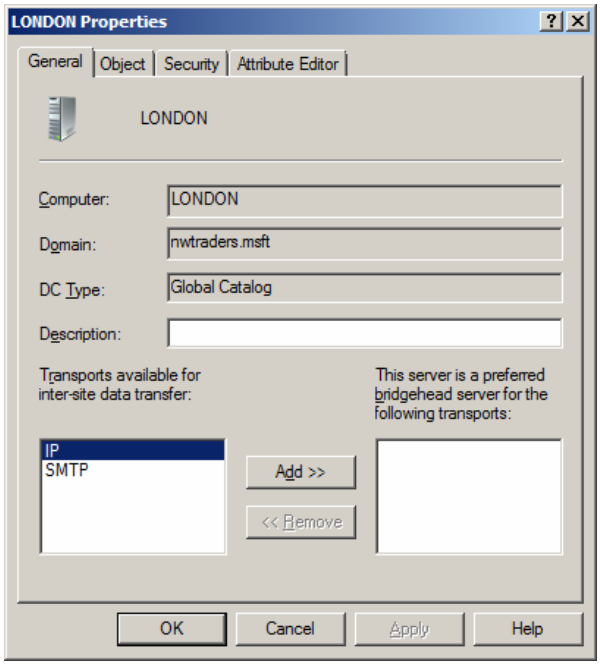
One-way replication

One way replication is used when a RODC (Read Only Domain Controller) has been implemented. These types of servers are used for Branch Offices. Only changes from the main domain controllers are replicated to the RODC. The RODC does not replicate any changes because it is read only.

Bridgehead server

The bridgehead server is a domain controller that has been either administratively assigned or automatically chosen to replicate changes collected. The bridgehead server is responsible for controlling replication. The replication topology generator automatically chooses the server to act as a bridgehead server. Select the bridgehead server through the dialog box shown below.



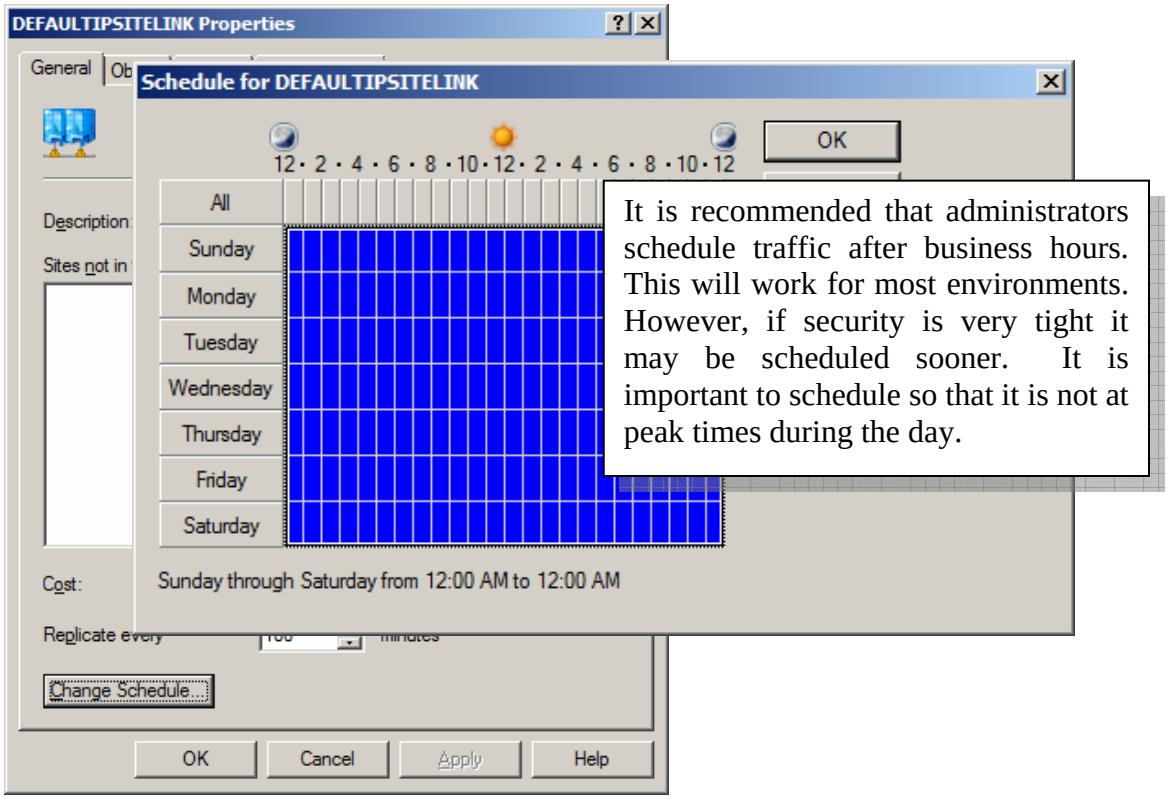


This is the dialog box that is used to configure Bridgehead servers. Select which transport protocol to use. Then add it in the Bridgehead server box. This will select the current server as the Bridgehead server. It is recommended to have more than one Bridgehead to provide redundancy.

This is done through the server properties.

Replication scheduling

Replication scheduling is used to control when replication should take place across the site links that have been configured. It is possible to set the site link cost and schedule replication traffic to more efficiently use your environment.



It is recommended that administrators schedule traffic after business hours. This will work for most environments. However, if security is very tight it may be scheduled sooner. It is important to schedule so that it is not at peak times during the day.

Configure replication protocols

Active Directory replication can utilize one of two protocols to send replication data between domain controllers:

- Remote Procedure Call (RPC): This is the main protocol used by Active Directory to send replication data.
- Simple Mail Transport Protocol (SMTP): SMTP is typically utilized for sending replication data in bulk, and for sending replication data over unreliable network connections.

IP is the default communications used to replicate Active Directory traffic. SMTP is used as a backup.

Force intersite replication

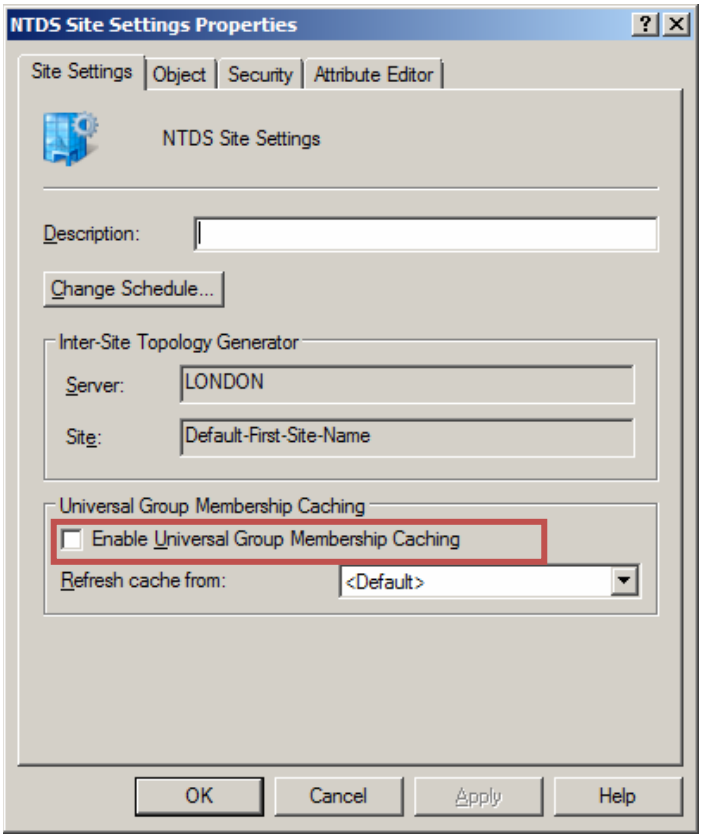
When changes have been made that need to take effect right away in Active Directory it is possible to use the Active Directory Sites and Services to force intersite replication to take place.

Configure the global catalog.

May include but is not limited to: Universal Group Membership Caching (UGMC), partial attribute set, promote to global catalog

Universal Group Membership Caching (UGMC)

On domain controllers running Windows 2003 or Windows 2008 in a site that has no global catalog server, it is possible to use universal group membership caching to reduce the need to contact a global catalog server. It can reduce the need to contact a global catalog server in a different site. When this feature is enabled, the first time a user logs on to a domain where universal groups are available, the user's universal group membership information is cached on the domain controller. The domain controller uses cached memberships to process the logon. Some of the potential benefits include faster logon, no need to upgrade hardware, and minimized bandwidth usage.

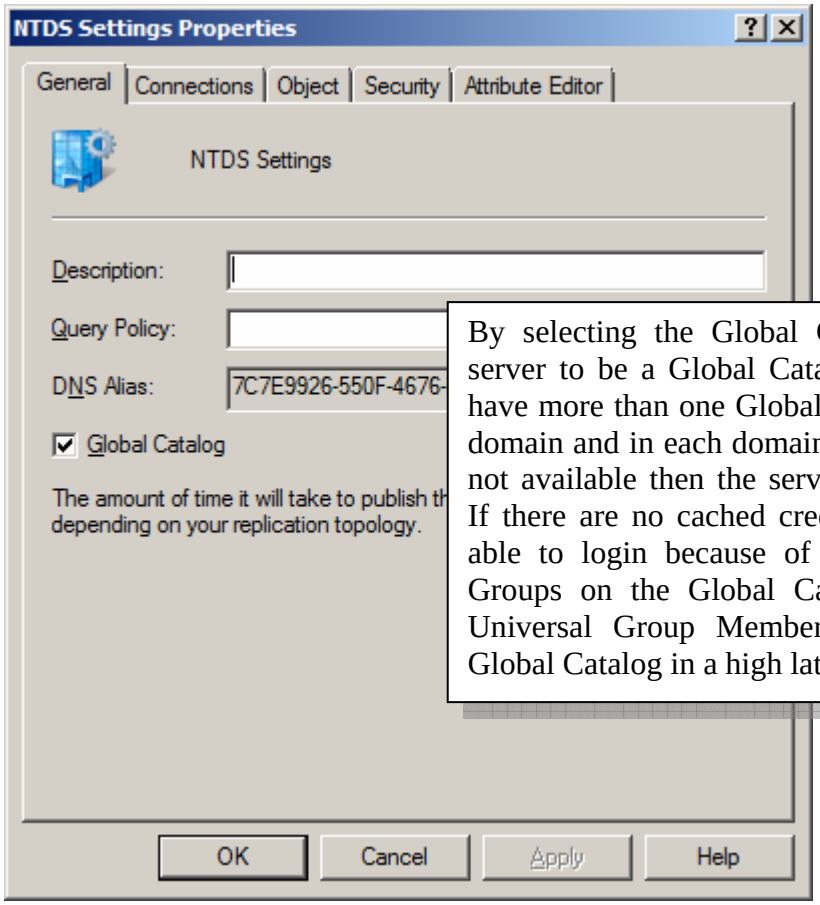


Partial attribute set

When information is replicated through the forest, attributes are replicated. With Windows 2008 only a partial set of attributes are replicated unlike the previous versions of Active Directory. This minimizes the amount of replication traffic.

Promote to global catalog

A Global Catalog has a subset of information for the entire forest. This server responds to requests from different servers including Exchange Server 2003 and Exchange Server 2007.



By selecting the Global Catalog box it designates the server to be a Global Catalog server. It is important to have more than one Global Catalog for each Site that in a domain and in each domain. If a Global Catalog server is not available then the server will use cached credentials. If there are no cached credentials then users will not be able to login because of the dependency of Universal Groups on the Global Catalog. It is possible to use Universal Group Membership Caching to replace the Global Catalog in a high latency area.

Configure operations masters.

May include but is not limited to: seize and transfer, backup operations master, operations master placement, Schema Master, extending the schema, time service

Seize and transfer

There are times when it may be necessary to seize or transfer a FSMO roler. Remember there are 5 roles. Schema and Domain Naming Masters are located on the Forest root and Infrastructure master, PDC Emulator and RID Master on the domain. It is possible to seize or transfer master's using GUI or command line.

Backup operations master

There is not an automatic way of configuring backup operations master. An administrator would designate a server as being the replacement if one of the FSMO servers fails.

Operations master placement

The default configuration for the FSMO's is sufficient depending on the amount of users in the domain. It is possible to move the FSMO's on to other servers. It is not advisable to move the Schema and Domain Naming Masters unless needed. The PDC and Infrastructure should be on different servers.

Schema Master

The Schema Master, by default, is installed on the Forest Root server which is the first server installed in the Forest. It controls updates to the Schema. Use the Forestprep command to make changes for Exchange or Windows 2008 into an existing domain.

Extending the schema

When the schema is extended additional classes and attributes are added to the schema. The schema is a database. The classes would be considered the Tables and attributes would be the Fields. Extending the schema is used to make changes to the schema to support different applications such as Exchange or custom applications.

Time service

The Time service is controlled by the PDC Emulator. It is very important because if servers are not in sync with each other, replication errors will occur. Administrators designate one server as the master time server and each server then syncs with that server.

Chapter 3 - Configuring Additional Active Directory Server Roles

Configure Active Directory Lightweight Directory Service (AD LDS).

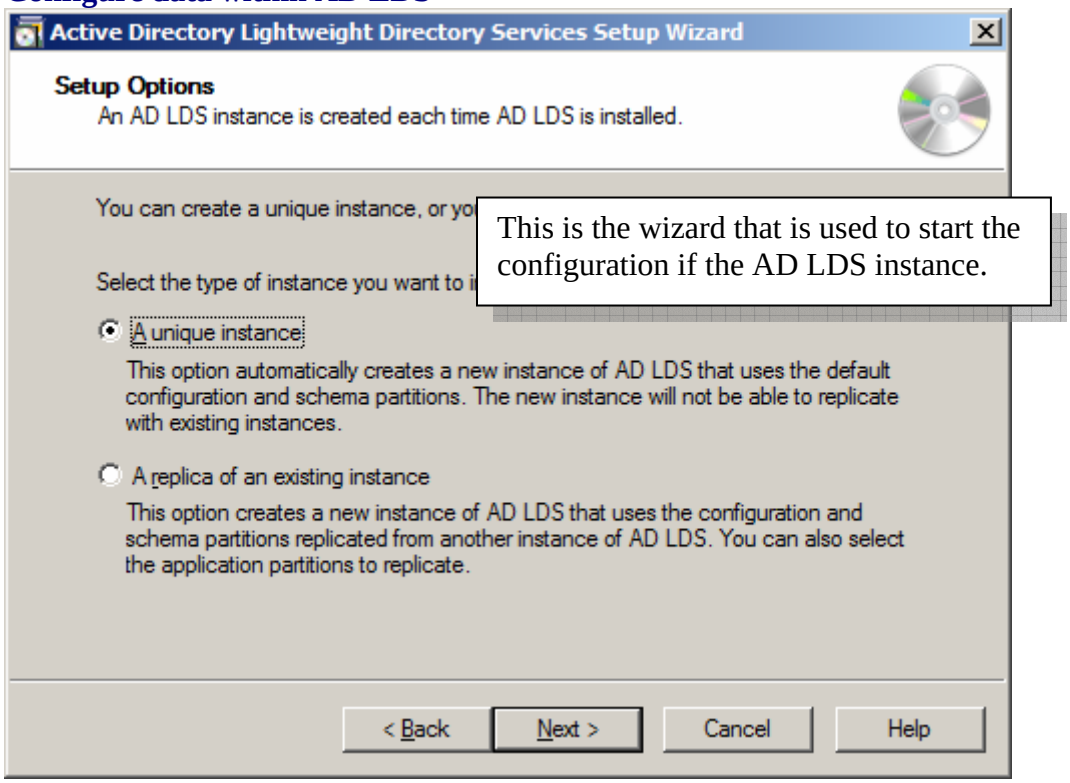
May include but is not limited to: migration to AD LDS, configure data within AD LDS, configure an authentication server, server core, Windows Server 2008 Hyper-V

Migration to AD LDS

The Active Directory Lightweight Directory Services (AD LDS) role (formerly known as Active Directory Application Mode (ADAM)) enables administrators to provide directory services for directory-enabled applications without incurring the overhead of domains and forests and the requirements of a single schema throughout a forest.

The AD LDS server role provides directory services specifically for directory-enabled applications. AD LDS does not require or rely on Active Directory domains or forests. However, if AD DS exists, AD LDS can use AD DS for the authentication of Windows security principals.

Configure data within AD LDS



This is the wizard that is used to start the configuration if the AD LDS instance.

Server core

Windows 2008 comes in two flavors, GUI and non-GUI. The Non-GUI version is known as the Server Core. When installing the Server Core you are installing a minimal version of the Operating System. The Server Core can still be managed using GUI tools remotely but in front of the server command line utilities are used. The server core is used for things such as DHCP, DNS and even Domain Controllers.

Windows Server 2008 Hyper-V

Windows Server 2008 Hyper-V was designed to compete with VMware and some of the other virtual server products. The Hyper-V allows companies to run several different servers on one box. The only requirements are that there must be enough resources on the host such as memory and hard drive space. Hyper-V also provides the ability to run other products such as Linux and use the full power of the 64-bit processor technology. By utilizing Hyper-V it is possible to lower the Total Cost of Ownership of the Operating System because less hardware is need. It is also easier to create test environments.

Configure Active Directory Rights Management Service (AD RMS).

May include but is not limited to: certificate request and installation, self-enrollments, delegation, Active Directory Metadirectory Services (AD MDS), Windows Server virtualization

Certificate request and installation

The Active Directory Certificate Services server is the used to create a PKI type environment. This needs to be added as a server role. Once this server role has been installed it is possible to start to distribute certificates to an organization. The CA can be installed as an Enterprise, Subordinate Enterprise or Standalone. The most effective would be the Subordinate because it is using a 3rd Party CA to self-sign certificates that are being given out.

Self-enrollments

It is possible to use web enrollment websites to acquire certificates from an Enterprise Certificate Authority.

Delegation

When there are several different branches of a company it may be necessary to give them the ability to manage parts of the network. This is known as delegating or passing responsibility to another party.

Active Directory Metadirectory Services (AD MDS)

MIIS (Microsoft Identity Integration System) allows environments to coexist with Sun and other OS's. It is built into Windows 2008. It allows administrators to create one account and propagate it to other OS's such as Novell, Sun and Unix.

Windows Server virtualization

Windows Server virtualization provides the ability of running multiple servers off of one platform. Also see Hyper-V.

Configure the read-only domain controller (RODC).

May include but is not limited to: unidirectional replication, Administrator role separation, read-only DNS, BitLocker, credential caching, password replication, syskey, Windows Server virtualization

Unidirectional replication

RODC's do not store writeable information. To keep current with users and groups there must be a way of updating this information. To update the information on a RODC the Master set of domain controllers will replicate the changes to the RODC. The replication is a one way replication from the Master to the RODC and not vice versa which is known as unidirectional.

Administrator role separation

Administrator role separation allows domain administrators to delegate the installation and administration of an RODC to non-administrative users.

Read-only DNS

When a RODC is installed it is also possible to install DNS. Clients can query the server just like any other DNS server. Updates to the DNS server are done through referrals. The DNS is read-only so it cannot accept updates directly. The update will be sent in a single-object replication. If there are any other changes they will happen the same way.

BitLocker

Bitlocker is a new technology that is unlike EFS. Instead of protecting a file or folder Bitlocker protects the whole drive. Bitlocker encrypts the entire system drive, including the Windows system files necessary for startup and logon. It is possible to logon and work with a file normally, but Bitlocker can help block hackers from accessing system files which they use to intercept password or access a hard drive by removing it from the computer. Bitlocker can only protect the files that are located on the drive that Windows is loaded on.

Credential catching

The RODC doesn't store any user or computer credentials. That is why it is called a Read Only Domain Controller. The only thing that it holds is the computer account of the RODC itself and a special "krbtgt" account that each RODC has.

It is possible to configure RODC to cache passwords. This is handled by the Password Replication Policy. This policy determines if replication from the writeable DC to the RODC is allowed for user or computer credentials. When a user logs on the credentials are checked to see if the user is allowed. If user is authorized the user's credentials are cached on the RODC at login.

An account is authenticated against a RODC if the RODC attempts to contact a writeable Domain Controller at the Hub site. If a password is not cached, the RODC will forward the authentication request to a writeable DC. The DC receiving the request recognizes that the request is coming from an RODC and checks with the Password Replication Policy.

Password protection is one of the benefits of Credential Caching at branch offices and minimizes exposure of credentials if the RODC is compromised. If a RODC is stolen, when using Credential Caching the user account and computer account can have their passwords reset, based on the RODC they belong to.

Credential Caching can be left disabled and this will limit the eventual exposure. On the other hand an increase WAN traffic will result of not using Credential Caching since all authentication requests will be forwarded to the writeable DCs in the main HUB site.

Password replication

When the RODC is initially deployed, the Password Replication Policy needs to be configured on the writeable domain controller that will be setup as the replication partner. The Password Replication Policy performs like an access control list (ACL), by determining if an RODC should be allowed to cache a password. When the RODC receives an authentication request or a computer begins to logon, it checks the Password Replication Policy to see if the account information should be cached. Once this is done, any other attempts to authenticate will be allowed without a problem because the credentials are cached on the server.

The accounts that are permitted to be cached and explicitly denied are located on the Password Replication Policy. The list does not contain the actual cached password. This can differ depending on which accounts and computers have attempted authentication. An Administrator does have the power to add accounts to the RODC for which they want to grant access. This is helpful when a connection is not available to the hub site.

Syskey

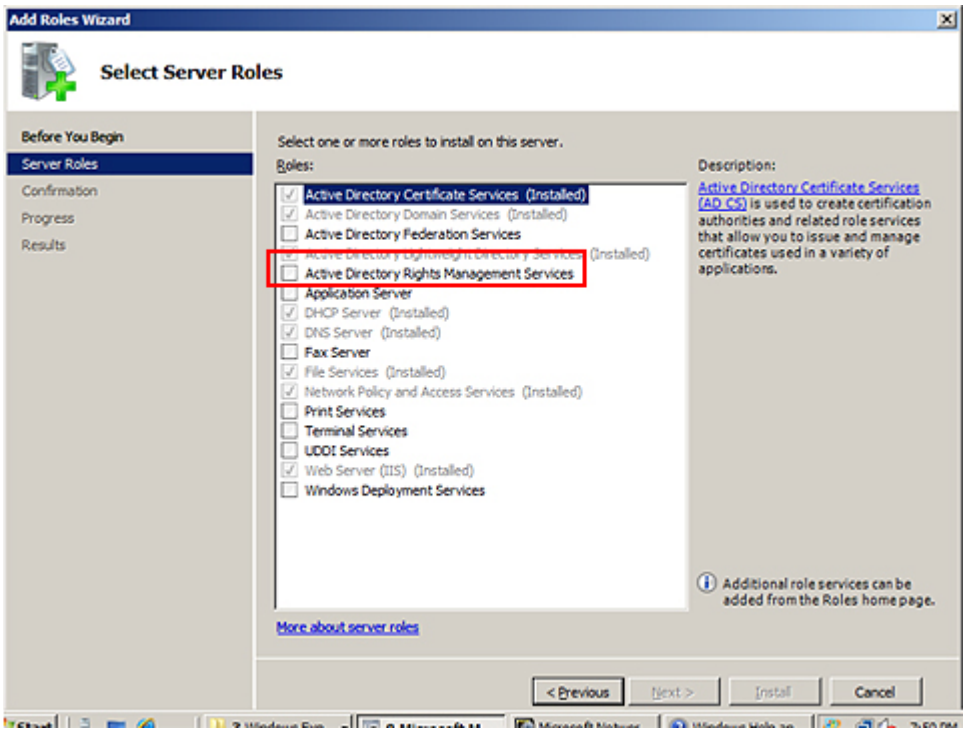
SYSKEY is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

Configure Active Directory Federation Services (AD FS).

May include but is not limited to: install AD FS server role, exchange certificate with AD FS agents, configure trust policies, configure user and group claim mapping, Windows Server virtualization

Install AD FS server role

The Active Directory Federation Service (AD FS) is installed through the Server Manager and selecting Server roles. The AD FS is used to create an identity access solution that can operate across multiple platforms, including both Windows and non-Windows environments. It provides browser based clients a "one prompt" access to one or more applications even if they are in completely different networks or organizations. AD FS makes the use of secondary accounts and their credentials unnecessary by providing trust relationships that you can use to project a user's identity and access rights to a trusted partners organization. AD FS can also project and accept other organizations credentials.



Exchange certificate with AD FS agents

The WS-* Web services architecture is supported by the Active Directory Federation Services and provides a standards-based solution that interoperates with other identity federation products. Passive Requestor Interoperability Profile is used by the AD FS with the WS-Federation. ADFS can interoperate with environments that might not use the Windows identity model by implementing the WS-Federation specification.

Here is an example:

There are two companies: Company A and Company B. They want to setup a Federation. Company B has information that they want Company A to have. Company B creates a new agreement that Company A can have access to the information. Company B is the resource partner because they have the information. Company A is the account partner because they have the accounts.

TLS/SSL is used to secure the exchanges and redirects of information. When a user in Company A accesses the Company B web site the user will be redirected to Company B's AD FS. Federation Service may present the user with an interface for selecting an account partner membership if this is the user's first time. This process is known as Home Realm Discovery. This is necessary if Company B had more than one partnership. This process may be changing by adjusting the code. The interface can be customized to make it more user friendly.

The user is then redirected after selecting Company A account partner. This then authenticates the user using the appropriate technology which can include integrated forms or a certificate. The Company A AD FS gives the client a signed security token based on the trust policy that is set in place and is redirected back to the Company B AD FS.

Company A's digital signature is verified by Trey Research and examines the claim. Company B will then refer to the trust policy for each of the claims in the security token. Once all the claims have been mapped to their local equivalents, a new security token is created containing the claims local to Company B. The token is then sent back to the client where they are redirected to the Company B AD FS enabled web application.

The digital signature and security token of the Company B AD FS are verified by the Web application. The claims in the token can be used to identify the user and make any necessary authorization decisions after the signature has been verified.

Configure trust policies

The Trust Policy node in AD FS snap-in represents the trust policy configuration information that is stored in an .xml file. This is created during the setup of the first federation server in the federation server farm. The path the trust policy is located in the web.config file. This should be stored on a network share to provide easy access.

Configure user and group claim mapping

The following procedure should be used to create group claim:

1. Access the AD FS from the Administrative Tools.
2. Double-Click the Federation services.
3. Double-Click the Trust Policy.
4. Double-Click the Organizations Claims.
5. Point to New.
6. Click on Organization claim.
7. Enter in the Claim Name in the New Organization Claim dialog.
8. Make sure that Group Claim has been selected and click on OK.

Chapter 4 - Creating and Maintaining Active Directory Objects

Automate creation of Active Directory accounts.

May include but is not limited to: bulk import, configure the UPN, create computer, user, and group accounts (scripts, import, migration), template accounts, contacts, distribution lists

Bulk import

There are several different ways to import data into Windows Server 2008 Directory Services. It is possible to use CSVDE which can do imports and exports, or LDIFDE can be used which can do imports, exports and changes. The PowerShell utility may also be used.

Configure the UPN

The User Principal Name looks like an email address. jdoe@nwtraders.msft. Additional UPN suffixes can be configured by accessing the Active Directory Domains and Trusts.

Create computer, user, and group accounts (scripts, import, migration)

It is possible to create Active Directory objects by using any of the GUI utilities, creation of VBscripts or PowerShell Scripts. Also, the Active Directory Migration Tool can be employed to import objects from another domain or Forest.

Template accounts

A template account is a model account that is used to create multiple accounts with common settings quickly. Items can be saved such as Group Membership and passwords criteria settings. However, passwords cannot be saved.

Contacts

A Collection is information about a person or organization. Contacts are stored in the contacts folder and can contain information such as phone, email, state, city and company.

Distribution lists

Distribution lists are used for sending information to multiple people that are part of a group. A distribution list can be used for newsletters or invitations.

Maintain Active Directory accounts.

May include but is not limited to: configure group membership, account resets, delegation, AGDLP/AGGUDLP, deny domain local group, local versus domain, Protected Admin, disabling accounts versus deleting accounts, deprovisioning, contacts, creating organizational units (OUs), delegation of control

Configure group membership

Groups are used for security purposes. They allow administrators to distribute permissions to multiple individuals by being part of the group. It is better to assign permissions to a group of individuals then to the individual themselves. A-G-L-P is a handy mnemonic device that can help to recall this basic organizational strategy. It means: ACCOUNTS go into GLOBAL groups which go into LOCAL groups which are assigned PERMISSIONS.

Account resets

Resetting an account refers to the act of re-associating a computer or user account with the physical object to which it belongs. In the case of a user, for example, this often means clearing and setting a new basic password. In the case of a computer account, this usually means resetting its SAM (Security Accounts Manager) entry.

AGDLP/AGGUDLP

These are acronyms for Accounts Global Domain Local Permissions and Accounts Global Global Universal Groups Domain Local permissions. They describe group nesting.

Deny domain local group

A deny permission takes precedence over all other permissions. When a person or object is part of an Active Directory group they inherit the rights and permissions of the group. However, if a specific privilege is assigned an explicit Deny, this means no matter what they will not be able to do the action or perform the right.

Local versus domain

A Local account is stored in the SAM (Security Accounts Manager). The SAM has all of the local accounts. When there is a Domain the accounts are stored in the Directory Services database.

Protected Admin

The protected Admin is an account that has limited abilities. Even when a user is logged into Windows 2008 with an administrator account they do not have all the rights available and are limited on certain tasks. This makes it so that viruses cannot take over the administrator account and destroy the system.

Disabling accounts versus deleting accounts,

The rule of thumb is to not delete an account unless absolutely sure the rights and permissions are not needed. When an account is deleted it is deleting the SID. This SID can be connected different files and folders within the environment and by deleting the account it can delete access to those resources. It is better to disable the account and rename it to another person so that all the rights and permissions to resources are not lost.

Deprovisioning

Deprovisioning refers to the deactivating of an Active Directory account. This is typically associated with user accounts. An example would be when a user leaves a company. This allows the associated information to be archived instead of outright deleted. A recommended best practice is to create an OU (Organizational Unit) for deprovisioned accounts and move them there via an automatic script.

Creating organizational units (OUs)

OU's are created in Active Directory Users and Computers. OU's are container objects and can contain other Active Directory objects. It is possible to then connect a Group Policy Object to the OU to control aspects of the objects within the OU.

Delegation of control

Administrators can delegate control of objects by using the delegation and control wizard within Directory Services. This utility will allow administrators to assign certain rights to parts of the Active Directory.

Create and apply Group Policy objects (GPOs).

May include but is not limited to: enforce, OU hierarchy, block inheritance, and enabling user objects, group policy processing priority, WMI, group policy filtering, group policy loopback

Enforce

When a Group Policy Object is created there are times when it may be necessary to make sure that everyone gets those settings or an application. It is possible to enforce a GPO to pass through a block that has been put on a OU, Site or Domain. Example: A GPO is created to push out a virus package. The package is critical to network security. The policy is implemented and users call saying that they have not received the package. The package was not delivered because of a block put on that OU. The administrator would need to enforce the policy so that it is delivered no matter what.

OU hierarchy

OU hierarchy means the order in which OU's are created. There might be a FL OU that has Admin, Sec, Exec and Workers. These OU's are under the FL OU so it is said to be their parent.

Block inheritance

Block inheritance is used to stop the deliverance of Group Policy Objects. This might be used to filter out a certain OU. This should be used sparingly because it will block all GPO's and not just one. It is possible to force a GPO by putting enforcement on the GPO. This will then bypass the Block Inheritance.

Enable user objects

When an object is enabled it means that it is able to read a GPO.

Group policy processing priority

GPOs that apply to a user or computer do not all have the same precedence. Settings that are applied later can override settings were applied previously. Group Policy settings are processed in the following order:

- Local Group policy object
- Site
- Domain
- Organizational Unit

To summarize, the Local GPO is processed first, and the organizational unit to which the computer or user belongs (the one that it is a direct member of) is processed last. All of this processing is subject to the following conditions:

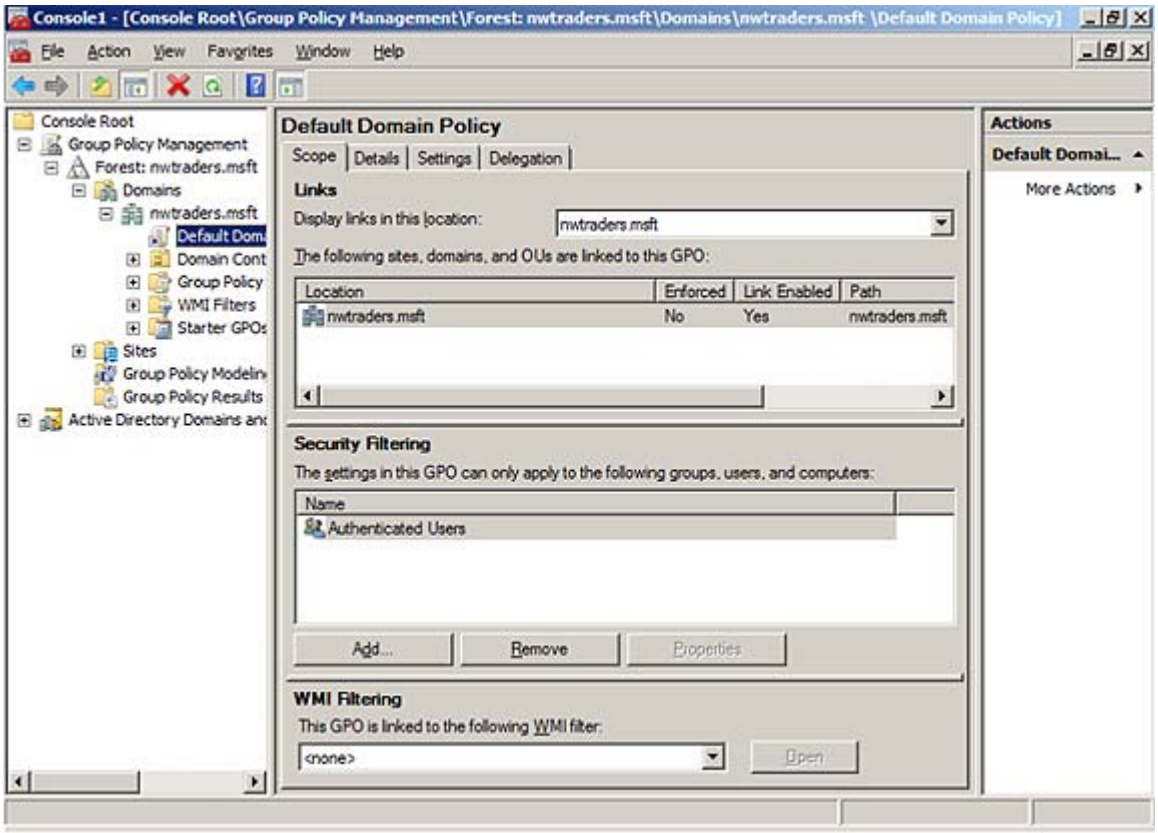
- Has there been WMI or Security filtering applied
- Has any GPO been enforced
- Has any Organizational Unit applied a Block Inheritance setting

WMI

Windows Management Instrumentation (WMI) is the main source of management data and functionality on local and remote computers that run Microsoft Windows operating system. WMI management data can be obtained directly through scripts and applications or through enterprise tools such as Microsoft Operations Manager (MOM) and Systems Management Server (SMS). Scripts written in any scripting language that can work with Windows Script Host may be used.

Group policy filtering

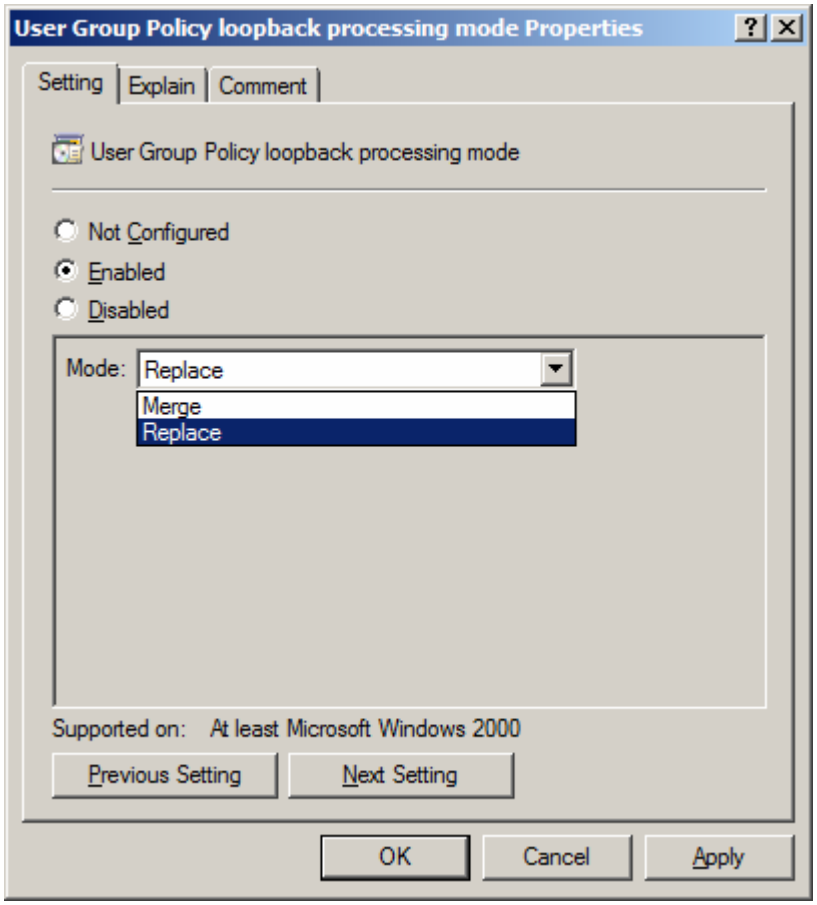
By default, a GPO affects all users and computers that are contained in the linked site, domain, or organizational unit. The administrator can further specify the computers and users that are affected by a GPO by using membership in security groups. It is possible to filter who is affected by group policies by using WMI filters and also through security filtering.



Group policy loopback

Group policy loopback is set within the GPO. It directs the system to apply the set of GPOs for the computer to any user who logs on to a computer affected by the setting. It is used for special locales such as public places, labs, and classrooms where settings need to be modified based on the computer that is being used. By default, the users GPO settings determine the settings but if this option is selected there are several things that can happen:

- Replace - The user settings on the computer will replace the user settings of the GPO
- Merge - The user settings are merged with the computer user settings.

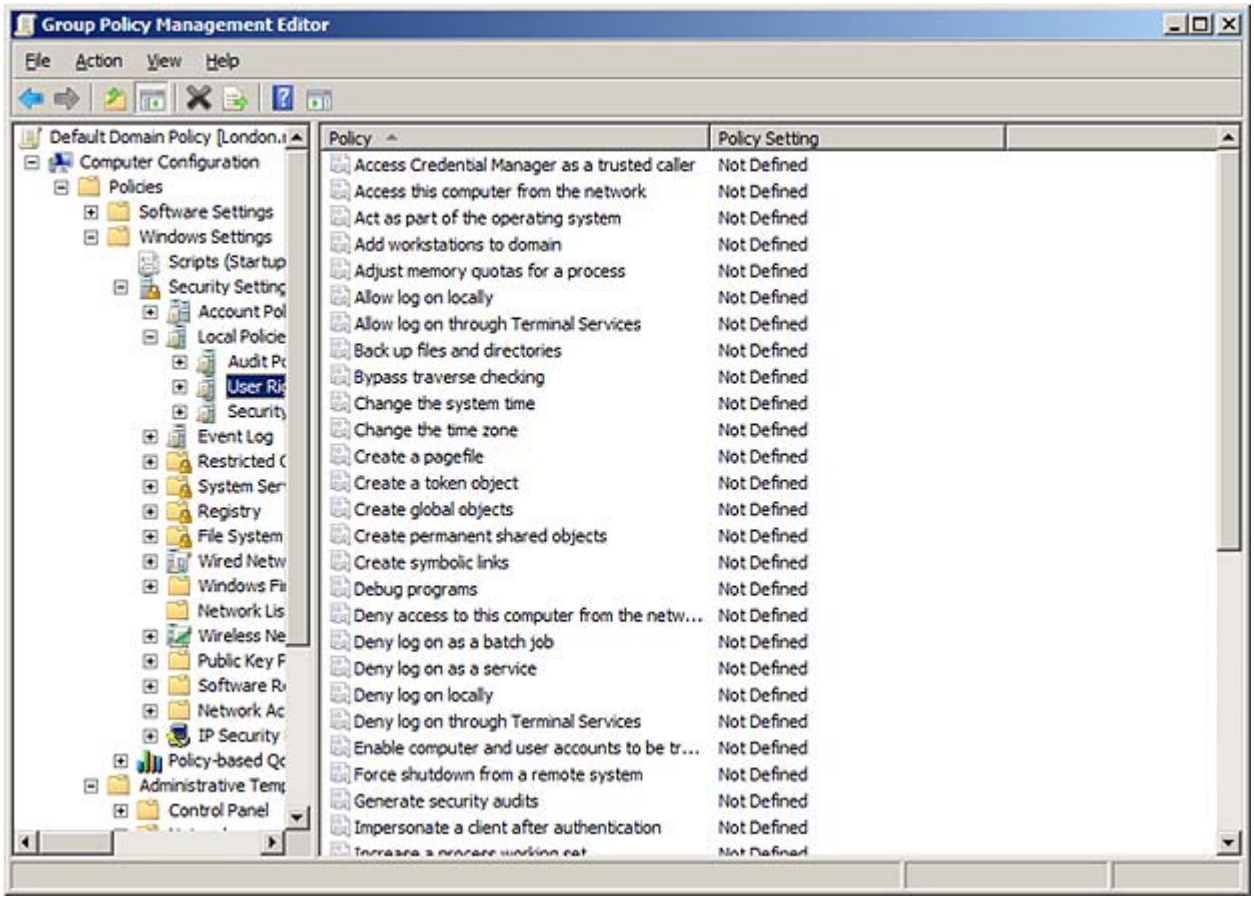


Configure GPO templates.

May include but is not limited to: user rights, ADMX Central Store, administrative templates, security templates, restricted groups, security options, starter GPOs, shell access policies

User rights

User Rights describes the tasks that a user is permitted to perform on a computer. Rights are controlled by the security settings on the computer and are usually set by the Administrator.



ADMX Central Store

The ADMX central store is one of the main benefits associated with ADMX files. The ADMX files replace the older ADM files. The central store design reduces the amount of space that is required to store GPO definitions. In addition to storing the ADMX files shipped in the operating system in the central store, it is possible to share a custom ADMX file by copying the file to the central store. This makes it available automatically to all Group Policy administrators in a domain.

Administrative templates

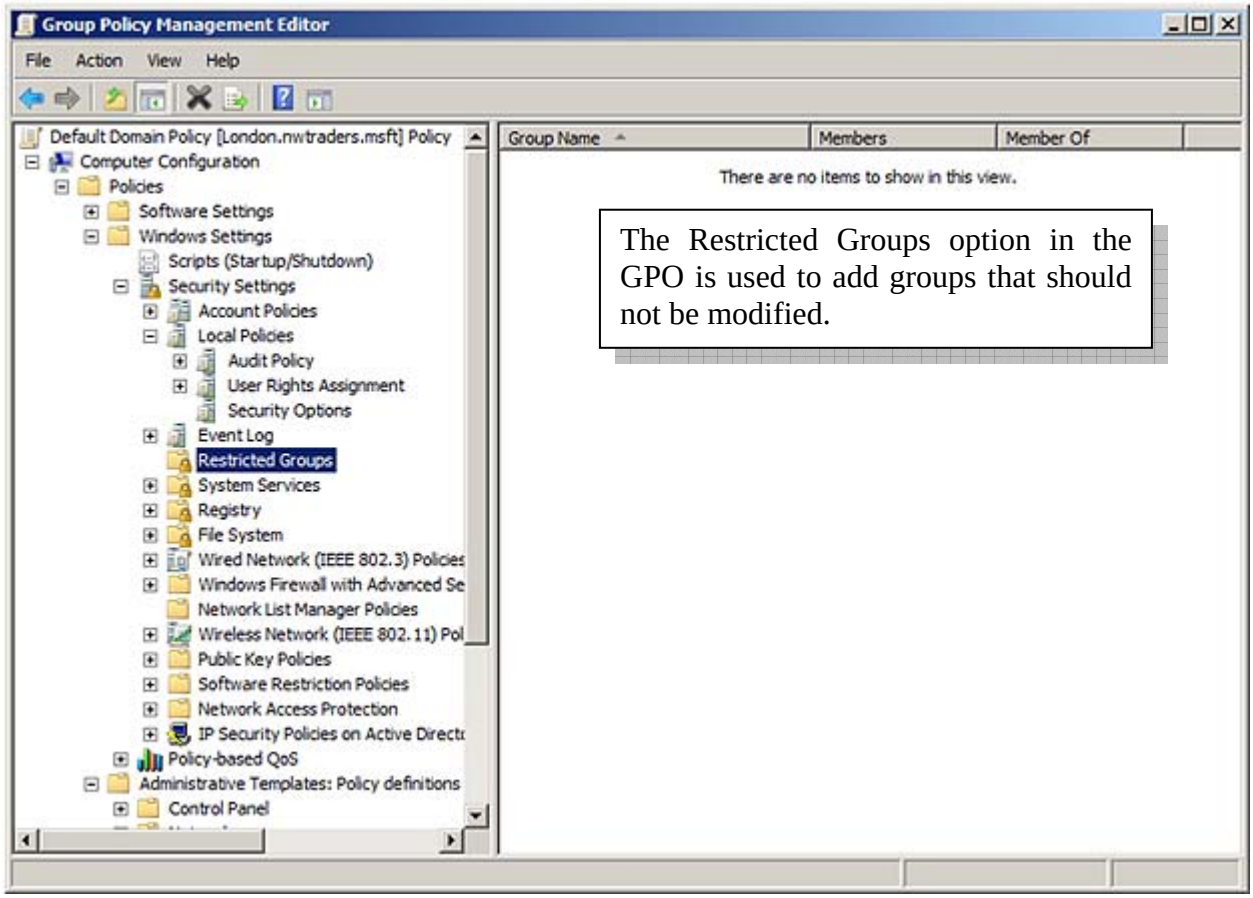
The Group Policy Administrative Templates node contains all registry-based policy information. User configurations are saved in HKEY_CURRENT_USER (HKCU), and computer configurations are saved in HKEY_LOCAL_MACHINE (HKLM). The software policy settings include Group Policy for programs as well as for the Windows 2000 operating system and its components. The namespace under the Administrative Templates node is populated by using .adm files or by an extension to Group Policy. When this node is used for the first time, the .adm files are automatically installed.

If an administrator plans to create entries for the Administrative Templates node, they should populate the namespace using the following naming convention, which is also used in the registry: *\CompanyName\product\version* (or *\CompanyName\product&version*)

Security templates

A security template has security configuration information that is stored in file. Security templates can be applied to a local computer. It is also possible to import to a Group Policy object, or it can be used to analyze security with the Security Configuration Wizard.

Restricted groups



Starter GPOs

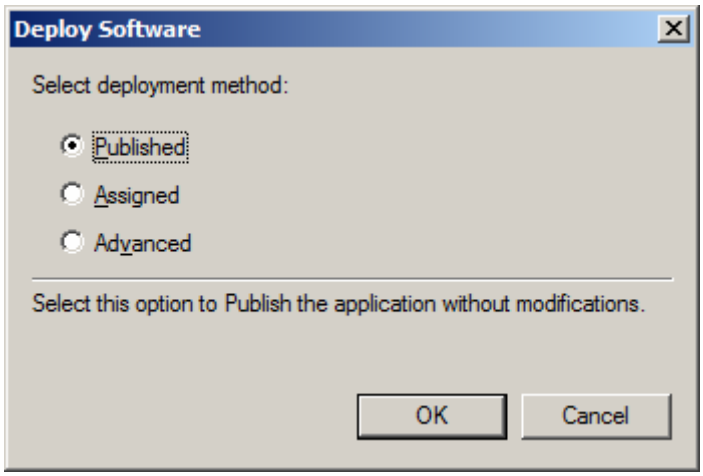
Starter Group Policy objects are derived from a Group Policy object. They provide the ability to store a collection of Administrative Templates policy settings in a single object. It is possible to import and export these Starter GPO's making them easy to distribute to other environments. When a new object is created from the Starter GPO the Administrative settings are set automatically to the settings of the Starter GPO.

Configure software deployment GPOs.

May include but is not limited to: publishing to users, assigning software to users, assigning to computers, software removal

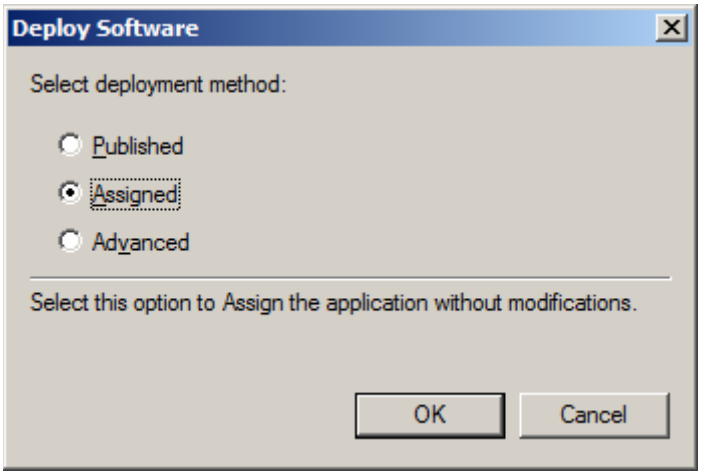
Publishing to users

There are two ways to distribute s software GPO: assign or publish it. Publishing means that it is advertising the software in the Add and Remove Programs or can be executed by association of the file extension. An example would be activating Word by association of a .doc. When a user tries to open a Word Document the Office Package would be installed on their machine.



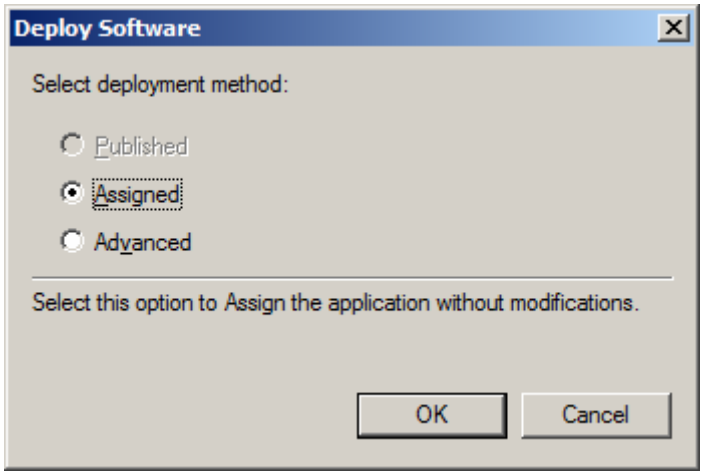
Assigning software to users

There are two ways to distribute software GPOs: assign or publish it to a user. Assigning means installing the software on the machine. It will be ready for use from the Programs menu. It will also associate software when it is opened such a Word .doc documents. Assigning means that whatever user logs on to the computer and each computer they log on to the software will follow.



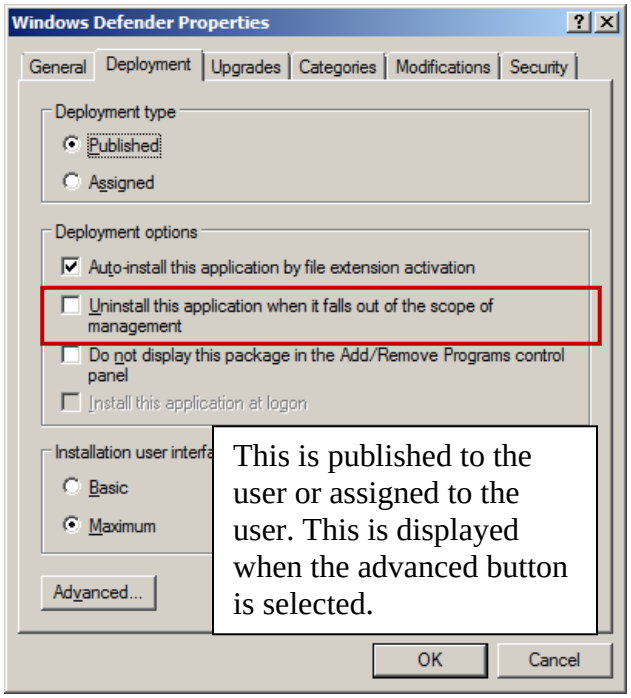
Assigning to computers

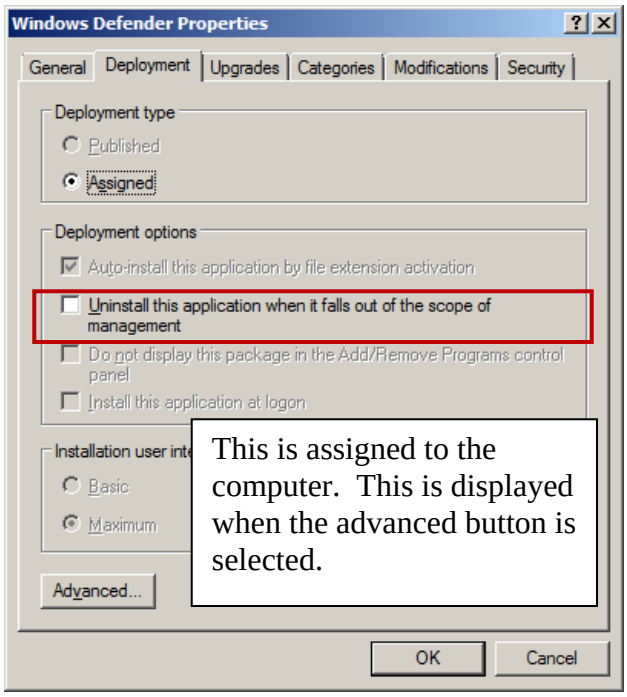
Assigning is the only way to distribute software to a computer. When a package is assigned to a computer it means that it is installing the software on the machine. When the computer starts up the assigned software will be installed automatically.



Software removal

When an administrator removes a GPO that is assigning or publishing software they have the option of allowing the software to remain or force removal.

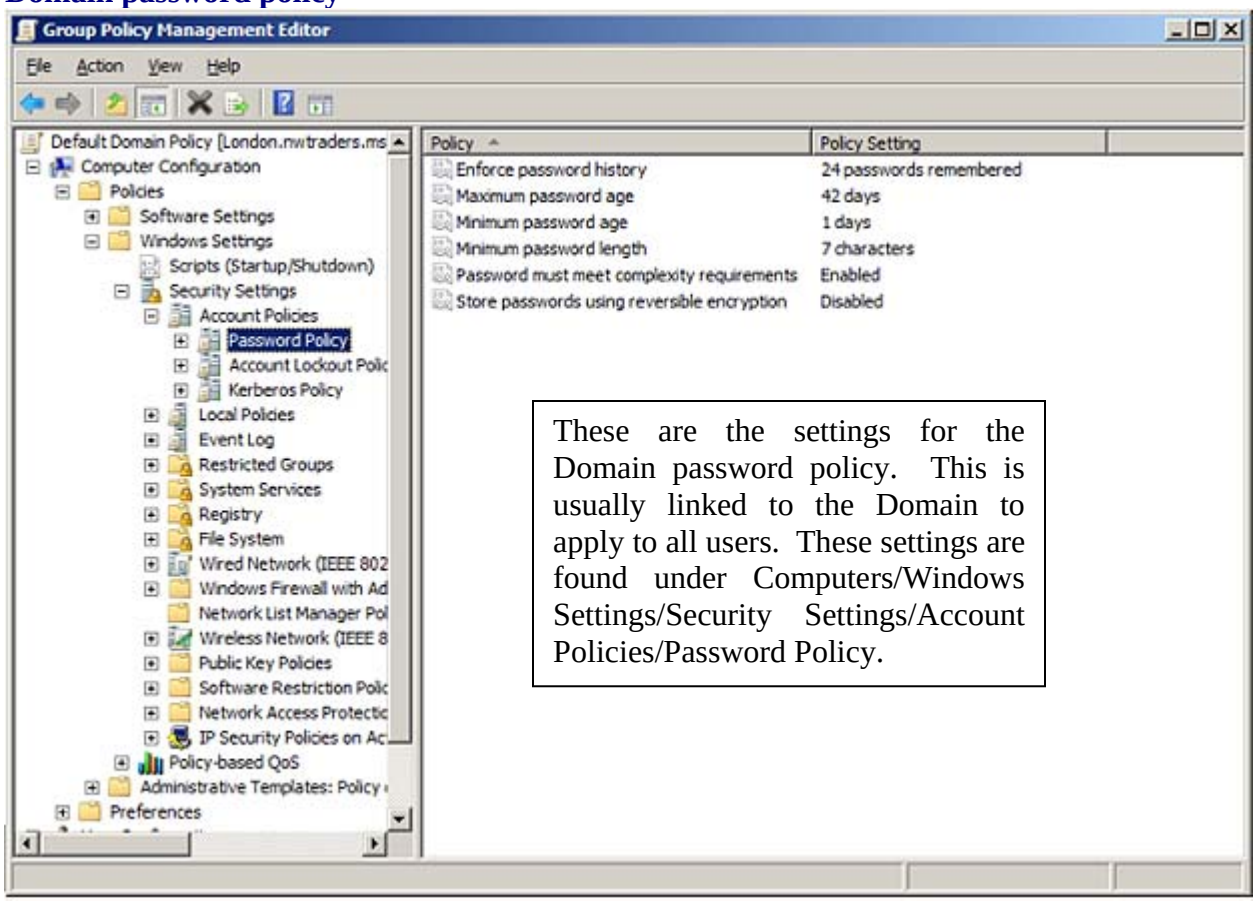




Configure account policies.

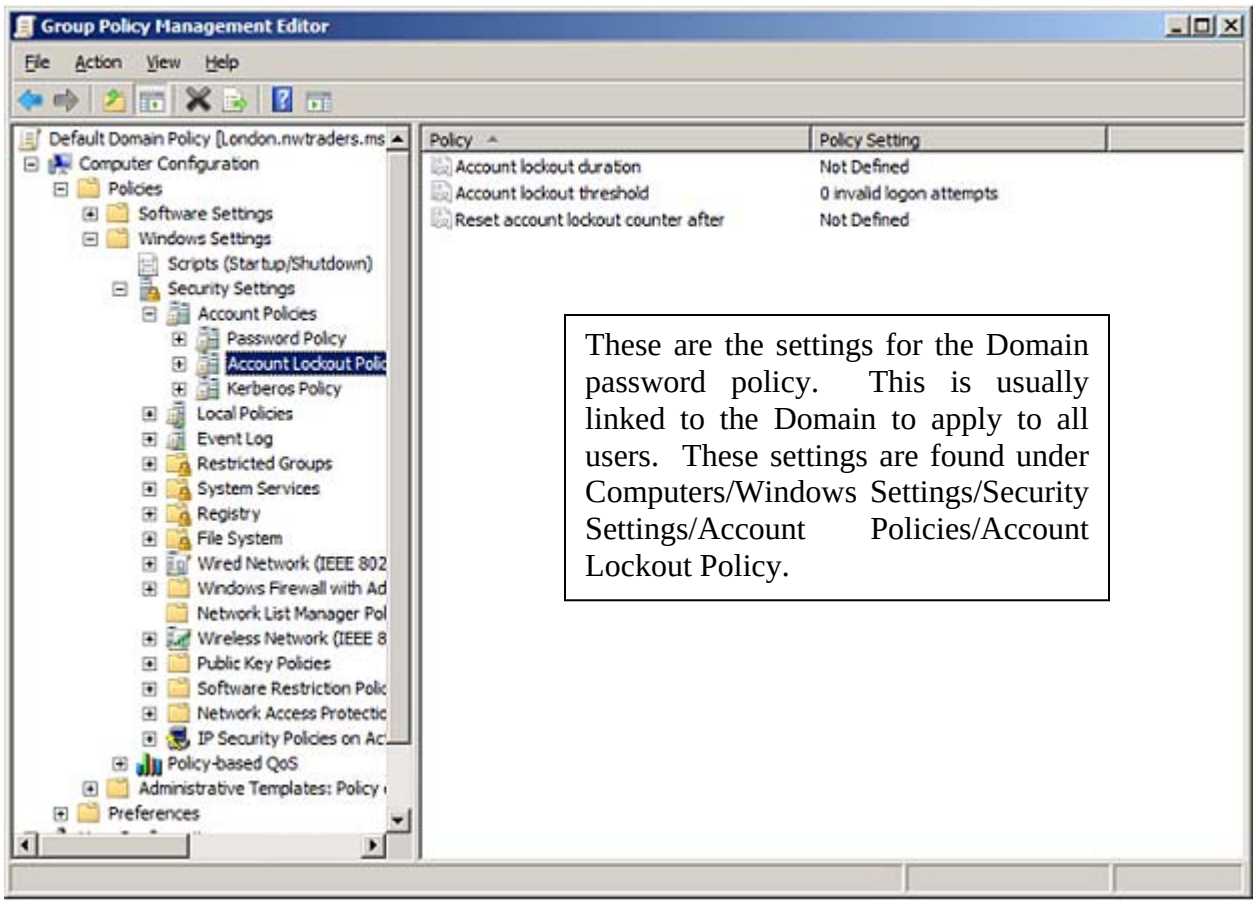
May include but is not limited to: domain password policy, account lockout policy, fine-grain password policies

Domain password policy



These are the settings for the Domain password policy. This is usually linked to the Domain to apply to all users. These settings are found under Computers/Windows Settings/Security Settings/Account Policies/Password Policy.

Account lockout policy



These are the settings for the Domain password policy. This is usually linked to the Domain to apply to all users. These settings are found under Computers/Windows Settings/Security Settings/Account Policies/Account Lockout Policy.

Fine-grain password policies

Administrators are not limited to implement a single Set of Password Settings to the whole domain (and therefore implement different domains if different Password Settings are needed). They are able to apply Password Settings on a Group and User basis.

After migrating to Windows Server 2008 on DCs, it is possible to incorporate this feature.

It is possible to configure the Password Settings and Account Settings like in Group Policies, but on a granular level. The basic concept is that there is a new object in Active Directory - the "Password Settings Object" which it's LDAP-Name msDS-PasswordSettings. For a new set of Password Settings simply create one of those objects underneath the container "cn=Password Settings, cn=System, dc=example, dc=com". This can be done using adsiedit.msc. The mandatory attributes must be filled in, and are listed in the following table:

Attribute	GPO Branch	Meaning
msDS-PasswordSettingsPrecendence	Password Setting	This is just a virtual number that can be made up which defines which Password Settings are taking effect.
msDS-PasswordReversibleEncryptionEnabled	Password Setting	This attribute is boolean and defines whether to store the passwords.
msDS-PasswordHistoryLength	Password Setting	This setting defines how many old passwords the user cannot reuse again
msDS-PasswordComplexityEnabled	Password Setting	This attribute is a boolean again, and defines if the password needs to be complex.
msDS-MinimumPasswordLength	Password Setting	This attribute defines the minimum length of a Password in characters.
msDS-MinimumPasswordAge	Password Setting	Also msDS-MinimumPasswordAge does just what its name suggests - defining the minimum age for Passwords.
msDS-MaximumPasswordAge	Password Setting	This is just the opposite and defines when to change a password.
msDS-LockoutThreshold	Account Lockout	Defines after how many failed attempts entering a password the user-object will be locked.
msDS-LockoutObservationWindow	Account Lockout	After which time should the "bad password counter" been reset?
msDS-LockoutDuration	Account Lockout	How long should a password being locked?

These settings are not available through GPO’s.

Configure audit policy by using GPOs.

May include but is not limited to: audit logon events, audit account logon events, audit policy change, audit access privilege use, audit directory service access, audit object access

Audit logon events

Domain controllers generate Account logon events for domain account activity and on local computers for local account activity. Domain controllers generate an account logon event if both account logon and logon audit policy categories are enabled, logons that use a domain account generate a logon or logoff event on the workstation or server.

When a user logs on to a server or workstation this is known as an interactive logon. When the user logs on to a member server or workstation that uses a domain account the logon will generate a logon event on the domain controller.

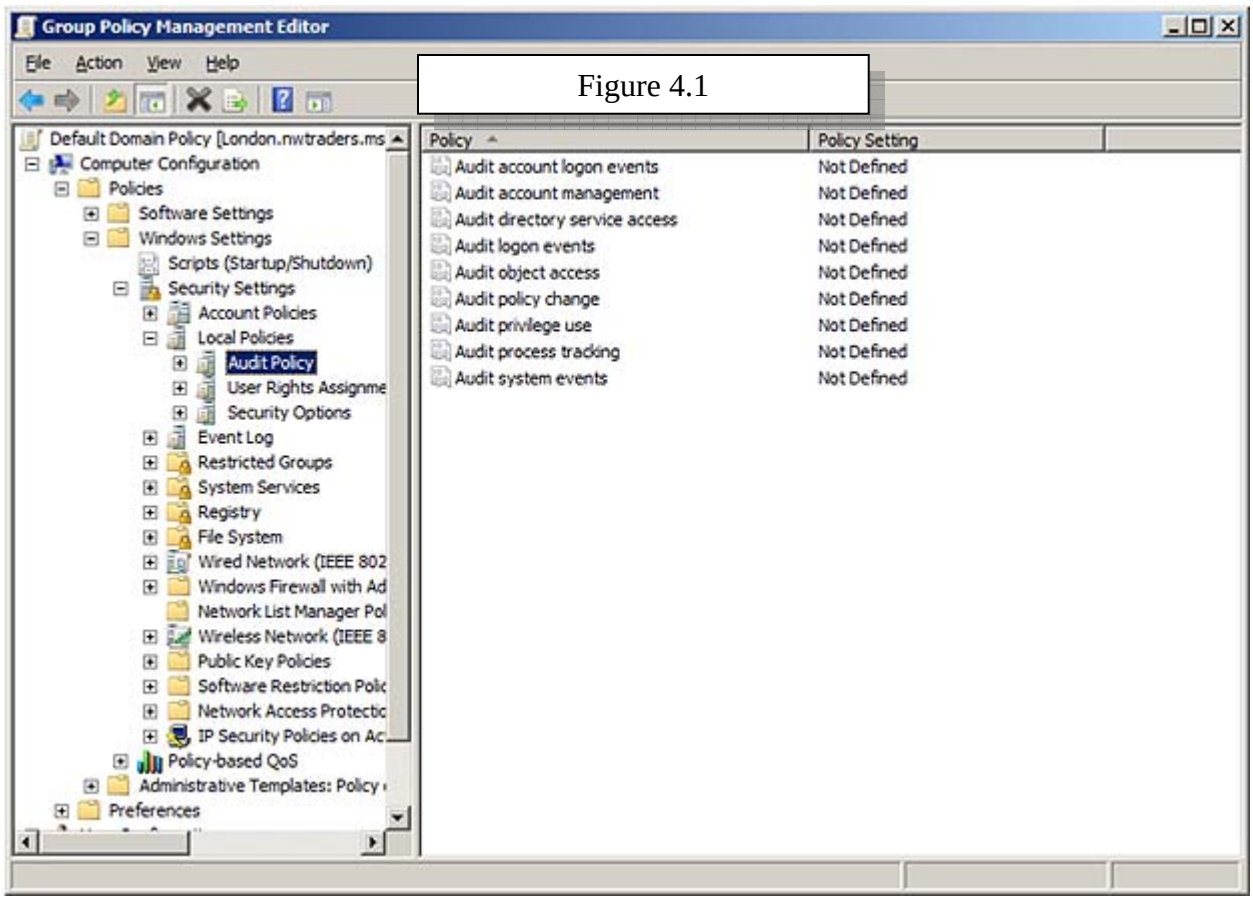


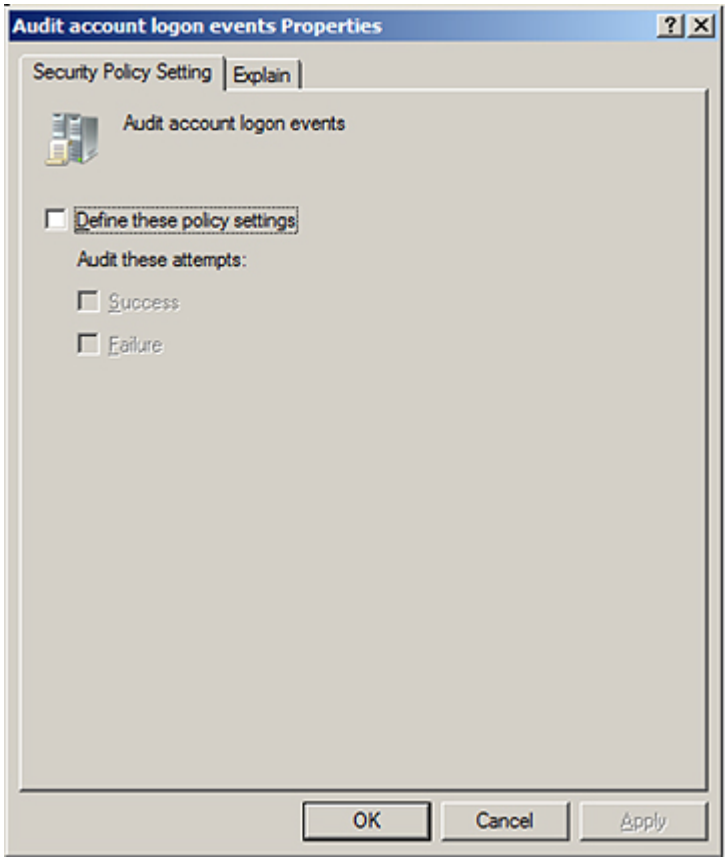
Figure 4.1

Audit account logon events

When a user is logging on to or logging off a computer the security setting determines whether to audit each instance. When a user is validated against a domain controller an Account logon event is generated. Domain controller log contains the event. When a local user is authenticated on a local computer logon events are generated. The local security log contains there events. Events are not generated for Account logoff.

It is possible to specify whether to audit successes, audit failures, or not audit any events in the policy settings. When an account succeeds in authenticating a success audit event is generated in the Security log. When an account fails to authenticate a failure audit event is generated in the Security log. To run off auditing, clear the success and failure boxes.

An entry is logged for each user who is authenticated against a domain controller; this is even true when the user is actually logging on to a workstation that is joined to the domain, if success auditing for account logon events is enabled on a domain controller.



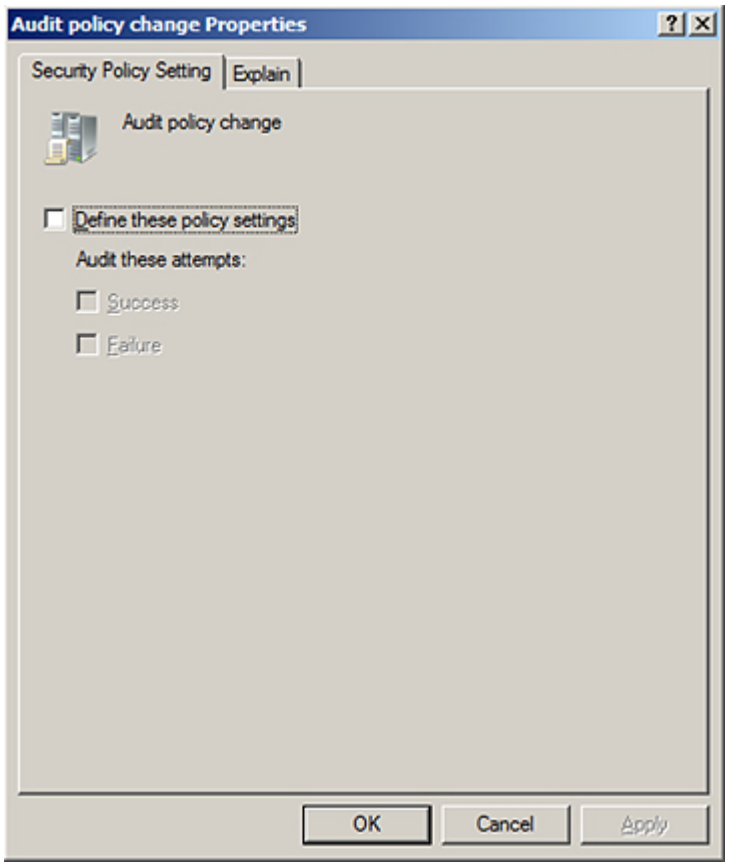
Audit policy change

Whenever a change is made to a policy it is possible to track these changes by enabling auditing of policy changes. Policy changes cover user rights assignments policies, audit polices and trust policies.

Administrators can specify whether to audit successes, audit failures, or not audit anything when they define this policy setting. When changes are made to a user rights assignment policies, audit policies or trust policies and they are successful a success audit entry is added to the Security log. When changes are made to user rights assignment policies, audit policies or trust policies and they are fail a failure audit entry is added to the Security log. To not audit anything, clear the check boxes for success and failure.

The default settings are as follows:

- Successes on domain controllers are tracked
- No auditing on member servers



Audit access privilege use

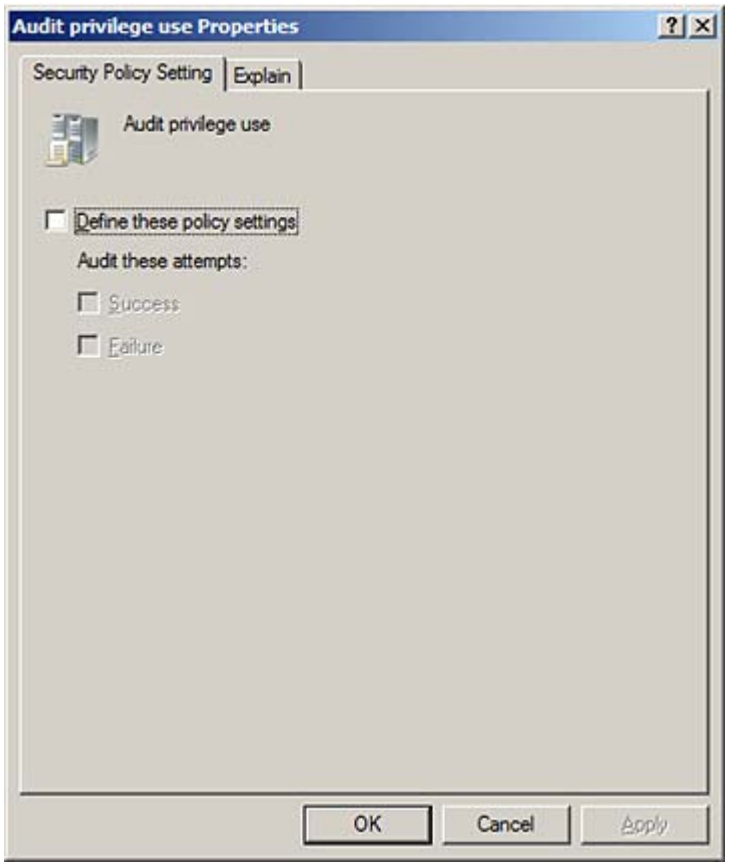
When this setting is enabled it is possible to suit successes and failures of a user exercising a user right.

Administrators can specify whether to audit successes, audit failures, or not audit anything when they define this policy. When a user exercises a right and it succeeds then a success audit generates in the Security log. When a user exercises a right and it fails then a failure audit generates in the Security log.

To set the properties to not audit anything clear the check boxes for Success and Failure. The default settings for the policy is no auditing.

The following are rights that are not audited:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace a process level token
- Generate security audits
- Backup files and directories
- Restore files and directories



Audit directory service access

When this security feature is enabled it will track Active Directory object access as long as the settings are turned on the object. The default setting for this option is no auditing which is represented in the Default Domain Controllers Group Policy.

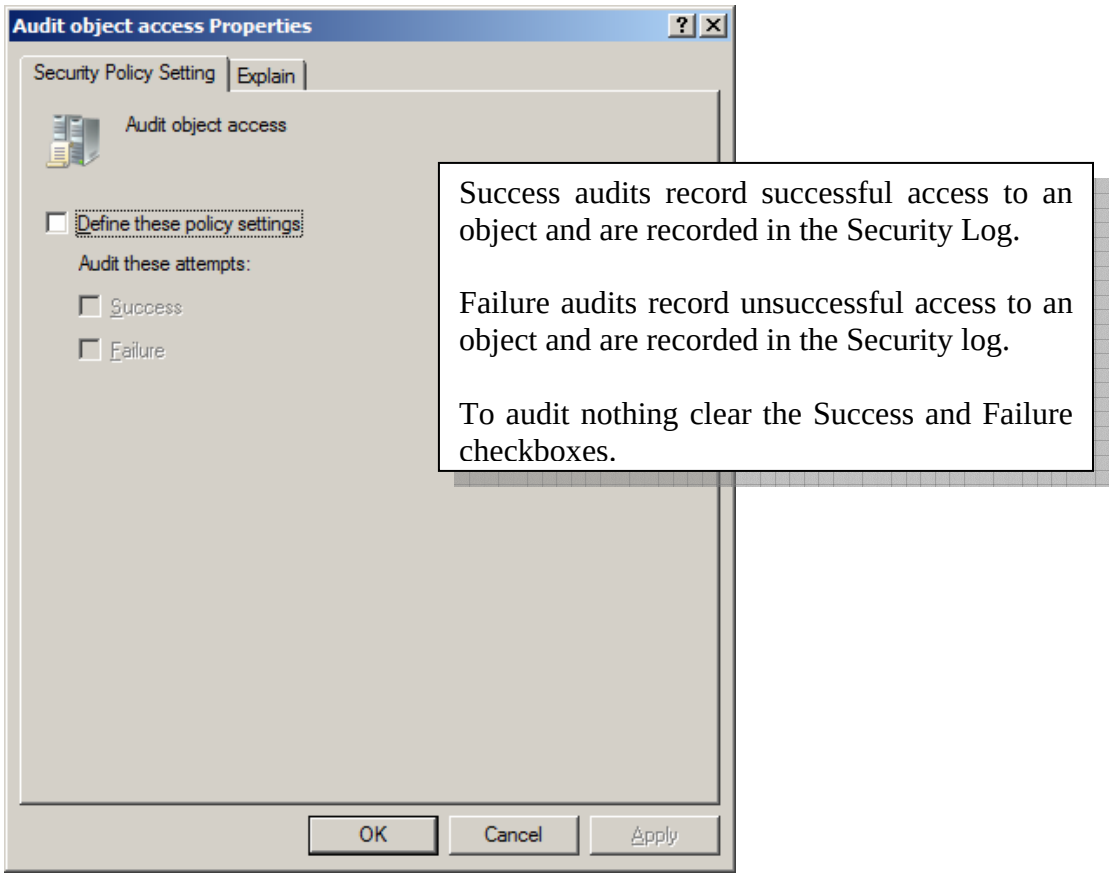
It is possible to specify whether to audit successes, audit failures, or not audit the evens at all. When a user successfully access an Active Directory object that has a SACL specified then a success audit will be logged in the Security log. When a user fails to access an Active Directory object that has a SACL specified then a failure audit will be logged in the Security log.

To set the auditing to audit nothing clear the Success and Failure checkboxes for the object.

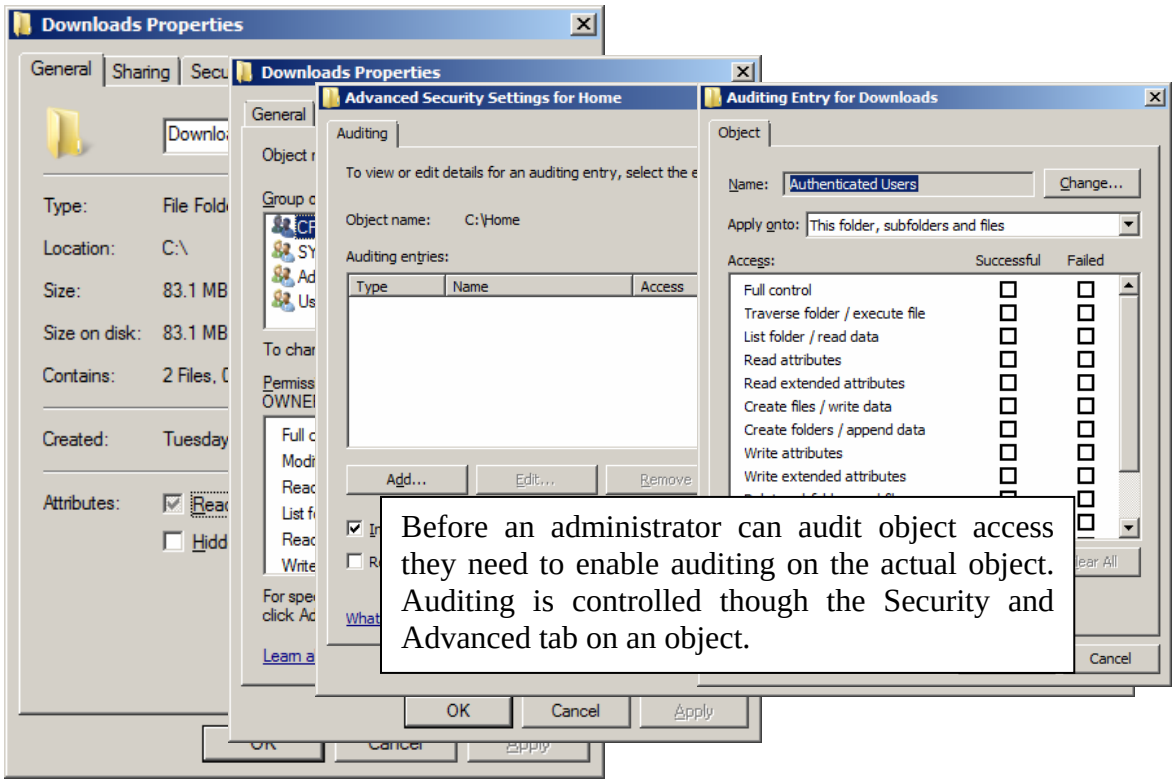
The actual setting needs to be defined in the Security Tab and Advanced properties. Then define who will be audited. This is the same as object access.

Audit object access

The audit object access setting tracks events that occur on an object such as file, folder, registry key, or printer. Administrators first have to enable the policy with a GPO. The GPO should be attached to the domain.



After the Security Policy is enabled the users or groups need to be tracked and decisions on what should be audited need to be made.



Before an administrator can audit object access they need to enable auditing on the actual object. Auditing is controlled though the Security and Advanced tab on an object.

Chapter 5 - Maintaining the Active Directory Environment

Quick Jump To:

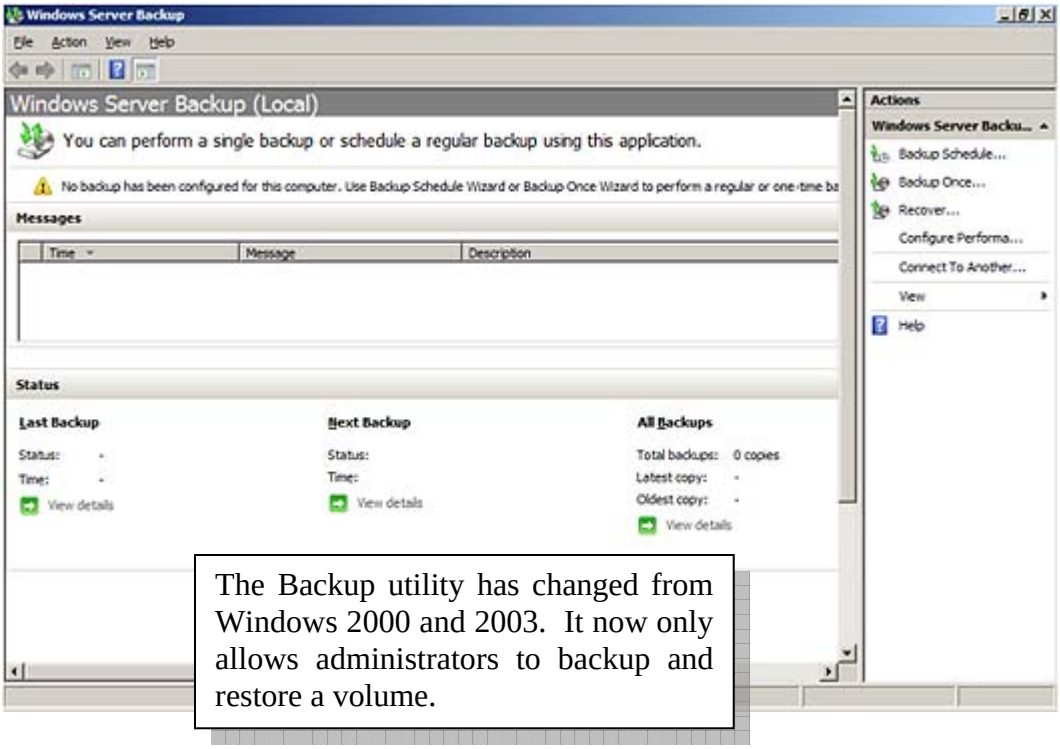
- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6

Configure backup and recovery.

May include but is not limited to: using Windows Server Backup, back up files and system state data to media, back up and restore by using removable media, perform an authoritative or non-authoritative Active Directory restore, linked value replication, Directory Services Recovery Mode (DSRM) (reset admin password), back up and restore GPOs

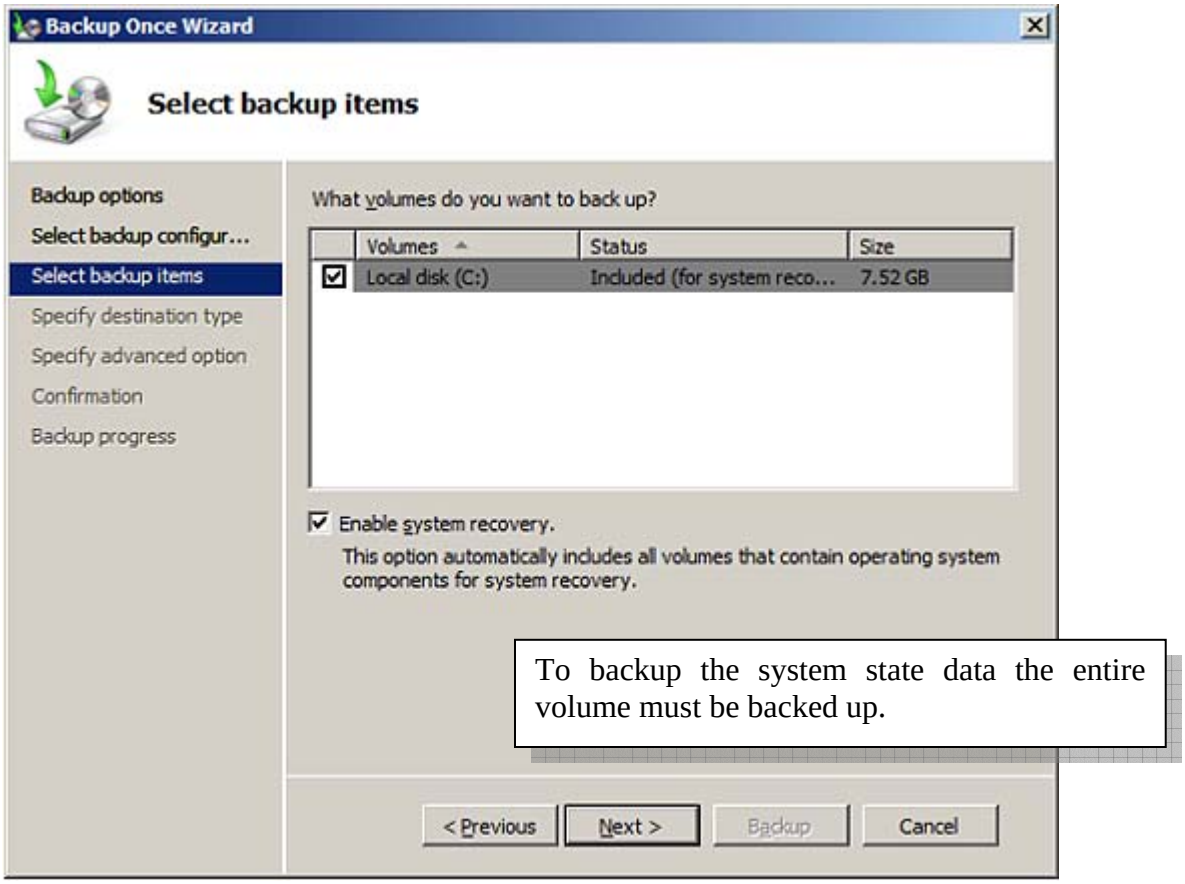
Using Windows Server Backup

This utility allows backup of information on the server. To install this feature Windows Server Backup role must be installed on the server.



The Backup utility has changed from Windows 2000 and 2003. It now only allows administrators to backup and restore a volume.

Back up files and system state data to media



Back up and restore by using removable media

This scenario explains how to manually back up volumes to DVD. This type of backup helps recover all volumes that are contained in the backup. It is used only when entire volumes need to be recovered. (It is not possible to recover individual files and folders or application data directly from backups stored on DVD.) For example, this type of backup might need to be performed to recover the operating system, or as protection in case of disk failure or a natural disaster.

Backups are compressed when stored on a DVD. As a result, the size of the backup on a DVD might be smaller than the volume on the server.

When a DVD backup contains all critical volumes (volumes with system components needed to restore the operating system), it is possible to use that backup to recover the server operating system by performing a volume recovery.

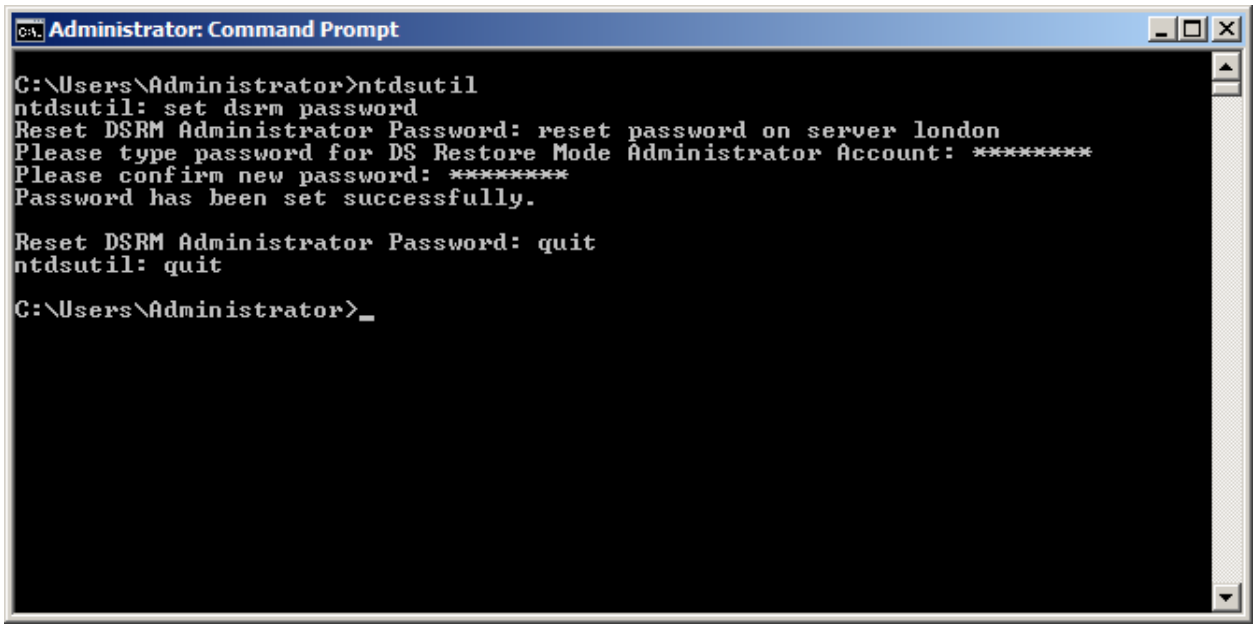
Perform an authoritative or non-authoritative Active Directory restore

To create an authoritative backup start Windows 2008 in Directory Restore Mode. This is accessed by restarting the server and pressing F8. Then select Directory Restore Mode. Enter the administrator password that was set up when installing Directory Services. Restore the backup. Use the ntdsutil to mark items as authoritative. This will make sure that they are not replaced by normal replication. To do a non authoritative backup follow the same steps but do not run ntdsutil.

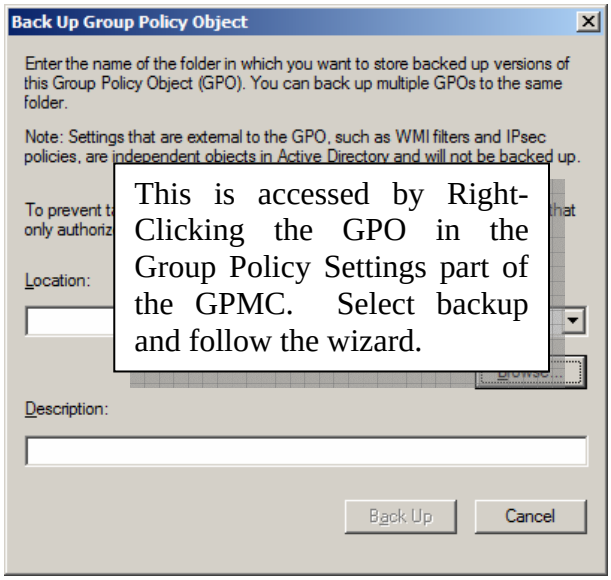
Directory Services Recovery Mode (DSRM) (reset admin password)

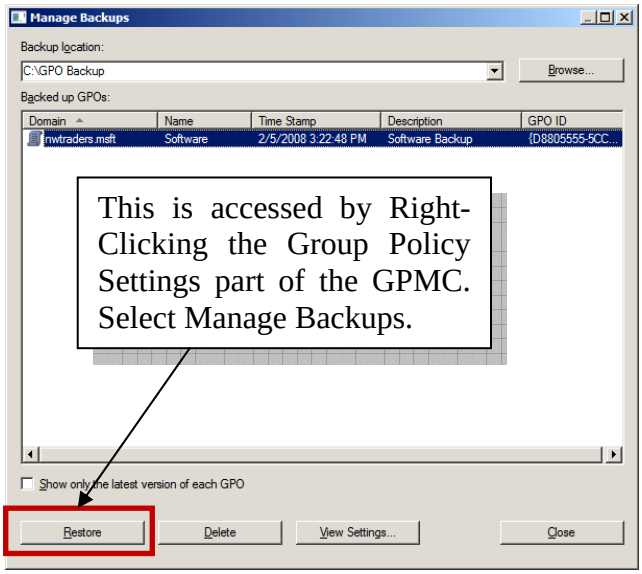
The DSRM password is the password that was created when the domain controller was first created. At some point it may be necessary to reset this password. To do this follow the steps listed below:

1. Access the command prompt on a domain controller
2. Type Ntdsutil {press Enter}
3. Type set-dsrm password {press Enter}
4. Type Reset password on server (server name) {press Enter}
5. Type {New Password} {press Enter}
6. Type {New Password to confirm} {press Enter}
7. Type quit {press Enter}
8. Type quit {press Enter}



Back up and restore GPOs





Perform offline maintenance.

May include but is not limited to: offline defragmentation and compaction, Restartable Active Directory, Active Directory database storage allocation

Offline defragmentation and compaction

Offline defragmentation should only be done when online defragmentation fails. During the defragmentation process the database integrity is checked. When offline defragmentation is performed the process creates a new, compacted version of the database in a location specified. This location can be on the same computer or a network mapped drive. However, there are potential problems that can arise due of network issues, so it is better to do it locally. After the procedure is completed copy the original Ntds.dit file to a backup file that looks similar to ntds.bak. Then take the new compacted database and copy it in to the original location. This whole process needs to be either in DSRM (Directory Service Restore Mode) or the new Restartable Active Directory may be used by stopping the Directory Services. You must be an administrator and have read and write access on the destination location.

Restartable Active Directory

Restartable Active Directory is a new feature in Windows 2008 and reduces the time that is required to perform certain operations. When updating a domain controller the Directory Services can be stopped. It is not necessary to go into DSRM and the other services such as DNS. DHCP can continue to service clients. This minimizes downtime which lowers the Total Cost of Ownership (TCO) of the Operating System.

Active Directory database storage allocation

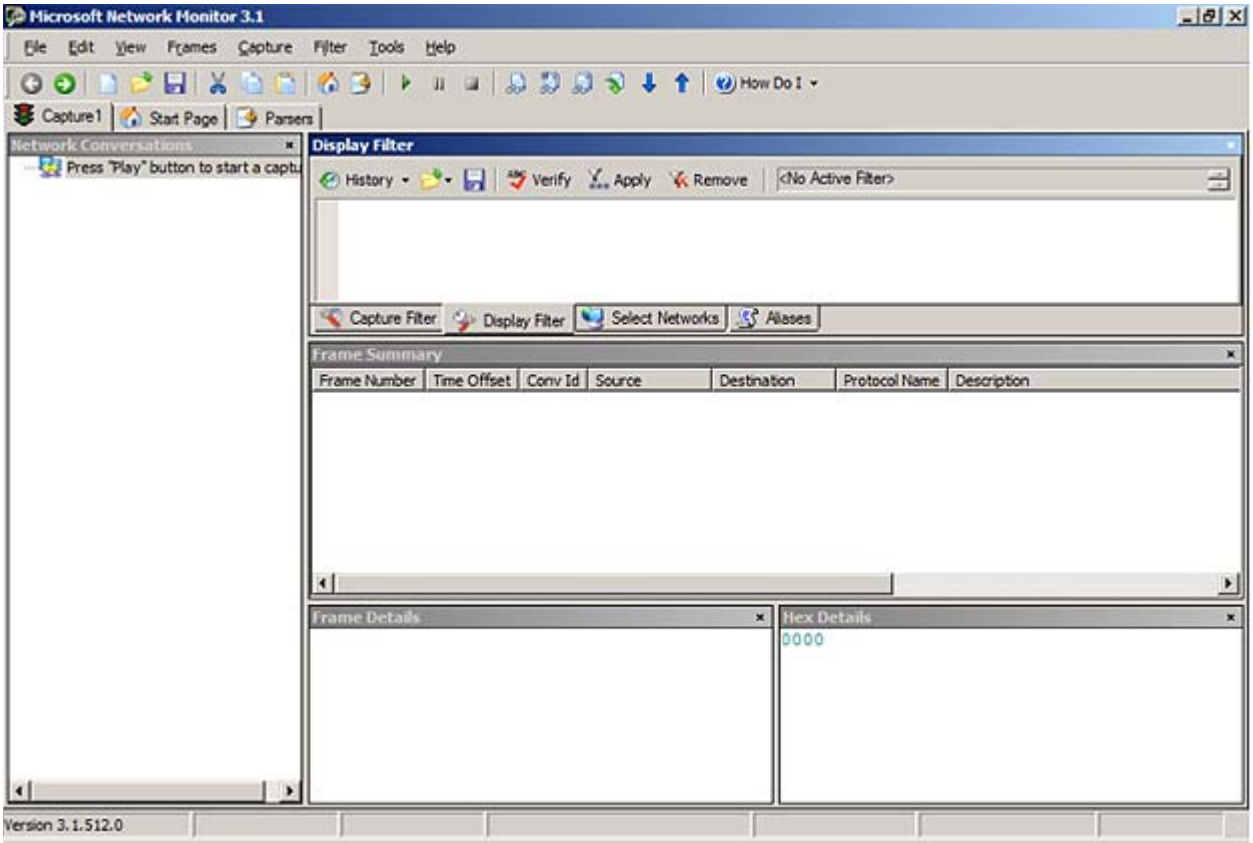
Active Directory database storage allocation is the amount of space that is going to be required to support the Directory Services database. This will vary for each organization.

Monitor Active Directory.

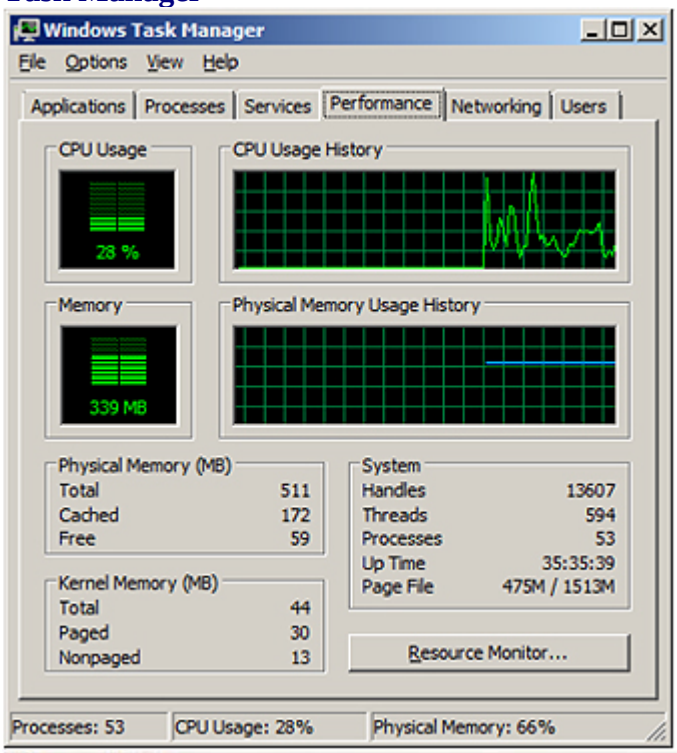
May include but is not limited to: Network Monitor, Task Manager, Event Viewer, ReplMon, RepAdmin, Windows System Resource Manager, Reliability and Performance Monitor, Server Performance Advisor, RSOP

Network Monitor

One of the utilities that can be used to troubleshoot a network is the Network Monitor. The Network Monitor 3.1 is a download that can be installed on the Windows 2008 server that works as a protocol analyzer. The Network Monitor allows administrators to capture traffic that is destined to the local machine. However, it is not able to capture traffic from another machine.



Task Manager



The Task manager is now redesigned with more information at administrators' finger tips.

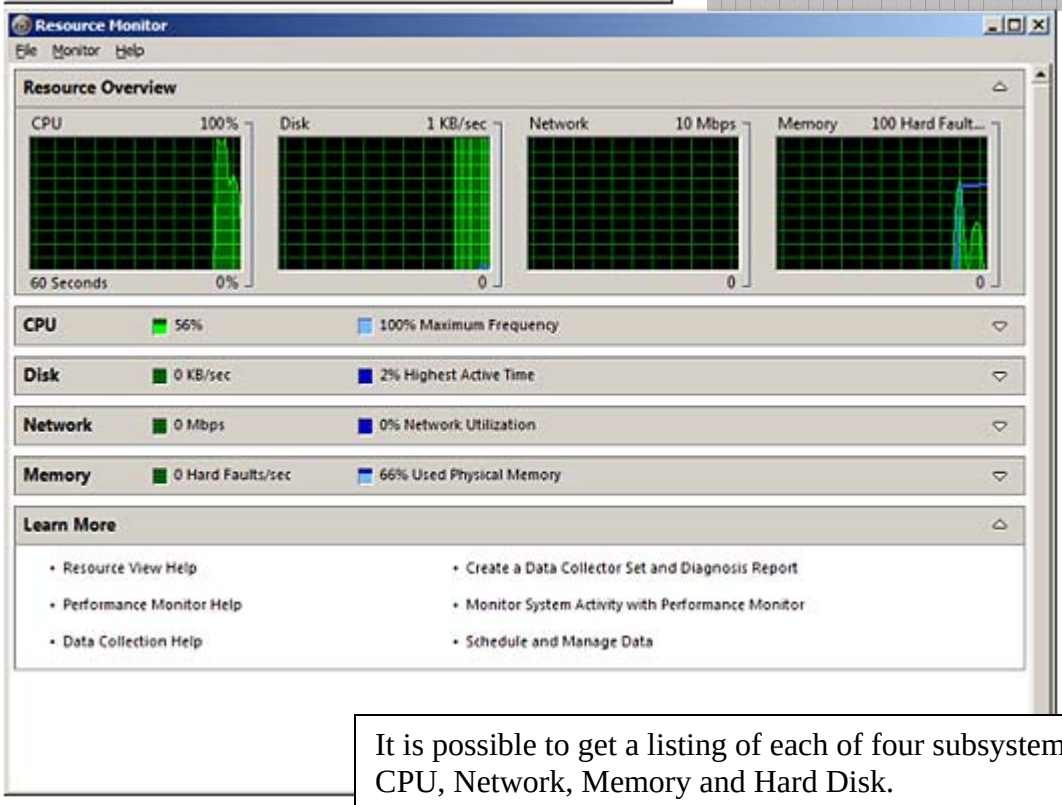
Applications – Shows what applications are running and allows shutdown of misbehaving applications.

Processes – Shows what processes are currently being used. This feature also allows shutdown of misbehaving processes.

Services - Shows what services are currently being used. Services can be stopped and started from this tab.

Performance – Shows a real time view of the resources being used and now has the resource monitor which can be used to see all of the resources at once. See Figure 5.1.

Network – Shows the network traffic to the server.



It is possible to get a listing of each of four subsystems: CPU, Network, Memory and Hard Disk.

Event Viewer

The Event Viewer is a Microsoft Management Console (MMC) snap-in that enables administrators to browse and manage event logs. It is an indispensable tool for monitoring the health of systems and troubleshooting issues when they arise.

Event Viewer enables the following tasks to be performed:

- View events from multiple event logs
- Save useful event filters as custom views that can be reused
- Schedule a task to run in response to an event

When the Event Viewer is used to troubleshoot a problem, it is important to locate events related to the problem, regardless of which event log they appear in. Event Viewer enables administrators to filter for specific events across multiple logs. That makes it easy to display all events potentially related to an issue that is being investigated. To specify a filter that spans multiple logs, a custom view needs to be created.

When working with Event Logs, the primary challenge is to narrow the set of events to just those that you are interested in. Sometimes this is easy. Other times this involves a great deal of effort; effort that is lost if there is not some way to save the view of the logs that were worked on. Event Viewer supports the idea of custom views. Once an administrator has queried and sorted their way to just the events they wanted to analyze, it is possible to save that work as a named view and it will be available for reuse in the future. The view can even be exported and used on other computers or shared with other people.

ReplMon

It is possible to troubleshoot Active Directory replication. Administrators can view level status of Active Directory replication and force synchronization between domain controllers using the Replmon utility. The Replmon utility is a GUI tool. Here are some of the things that can be accomplished using this tool:

- View replication traffic to investigate replication failures
- View the history of successful and failed replication changes
- View the properties of directory replication partners
- It is possible to script the Replmon and create application based on the API
- View snapshot of the configuration of replication partners
- Locate all transitive replication partners on the network
- View the replication topology

RepAdmin

The Replmon is the GUI version of the RepAdmin utility. The RepAdmin utility assists Administrators in diagnosing replication problems between Windows domain controllers.

To view replication topology Administrators can use Repadmin as seen from the domain controller. It is possible to force replication between replication partners and view the replication metadata and up-to-date replication vectors. The Repadmin tool can be used for monitoring the status of the Active Directory Forest.

Reliability and Performance Monitor

Reliability Monitor provides a system stability overview and trend analysis with detailed information about individual events that may affect the system's overall stability, such as software installations, operating system updates, and hardware failures. It begins collecting data at the time of system installation.

Performance Monitor provides a visual display of built-in Windows performance counters, either in real time or as a way to review historical data. It is possible to add performance counters to Performance Monitor by dragging and dropping, or by creating custom Data Collector Sets. It features multiple graph views that enable administrators to visually review performance log data. It is possible to create custom views in Performance Monitor that can be exported as Data Collector Sets for use with performance and logging features.

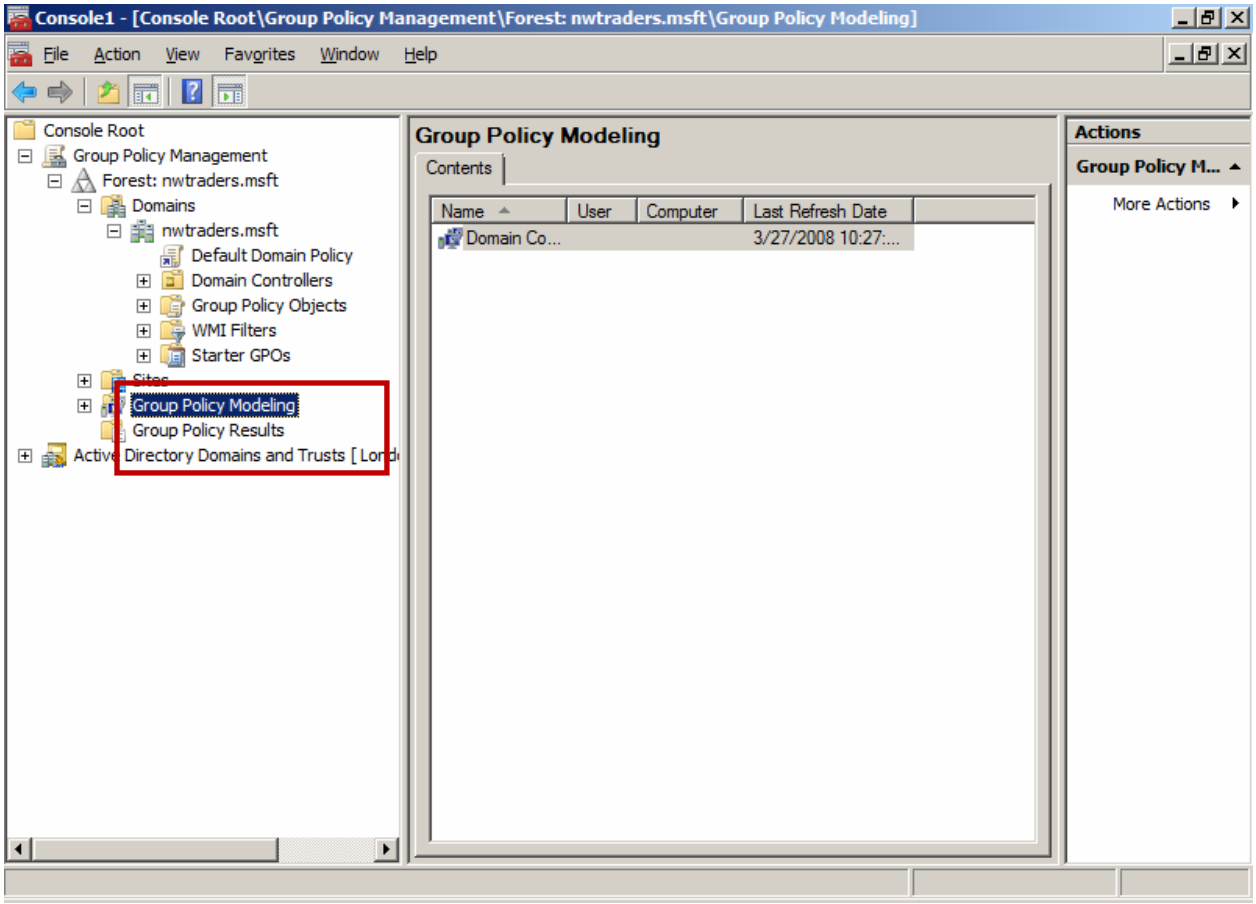
Server Performance Advisor

It is possible to diagnose the root causes of performance problems in a Microsoft Windows 2008 deployment using the Server Performance Advisor. Server Performance Advisor generates comprehensive diagnostic reports that provide the data to easily analyze problems and develop corrective actions from collected data.

RSOP

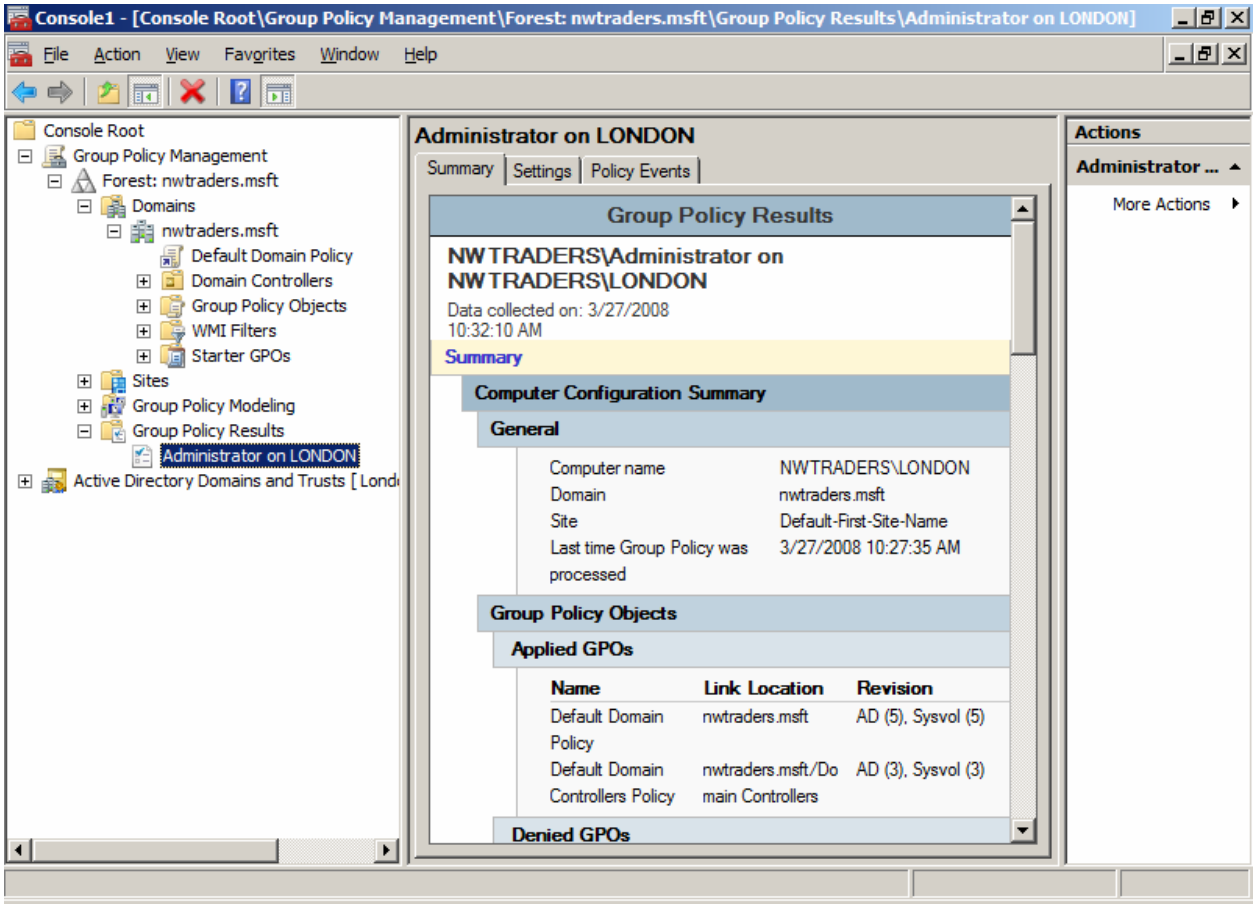
It is possible to use the Resultant Set of Policy(RSOP) snap-in to create detail reports about applied policy settings in two modes:

- Logging mode
  Logging mode displays policy settings that are applied to computers and users that are in an Organizational Unit, Domain or Site that have logged on.
- Planning mode
  This is used to simulate a implementation of a GPO and show the effects that will take place based on the configured policy settings.



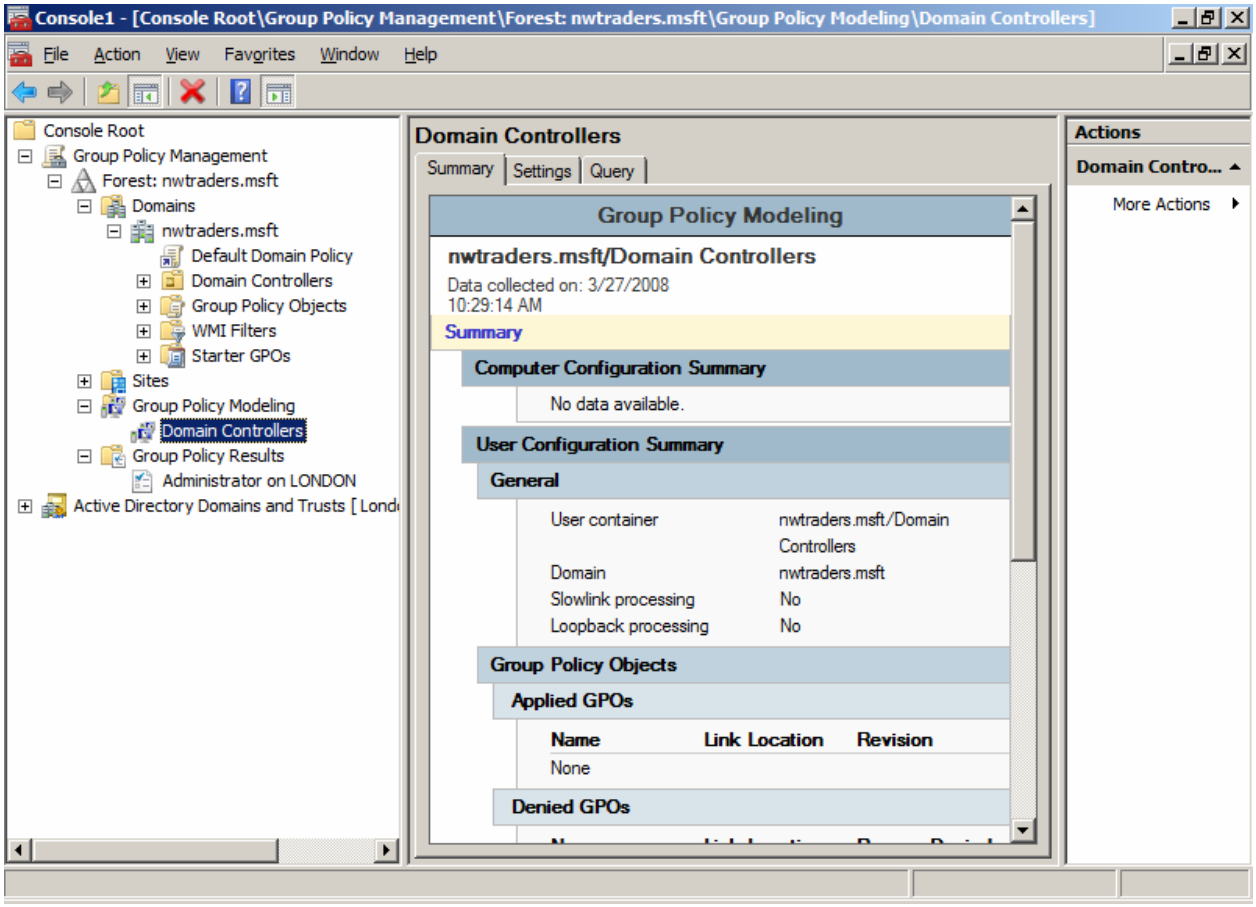
Logging Mode

Logging mode displays policy settings that are applied to computers and users that are in an Organizational Unit, Domain or Site that have logged on.



Planning Mode

This is used to simulate a implementation of a GPO and show the effects that will take place based on the configured policy settings.



Chapter 6 - Configuring Active Directory Certificate Services

Install Active Directory Certificate Services.

May include but is not limited to: standalone versus enterprise, CA hierarchies—root versus subordinate, certificate requests, certificate practice statement

Standalone versus enterprise

When a standalone CA is used Administrators must manually distribute certificates to clients. This is because the standalone CA is not part of the domain and does not have access to local or domain user accounts. The Enterprise CA adds flexibility and ability to the network by automatically publishing and handing out certificates to clients that need them. This can be done by the client requesting a certificate through the internet or through an application. The Enterprise Certificate Authority serves the whole Enterprise.

CA hierarchies—root versus subordinate

The root is the most protected. The subordinate is a second level below the root.

Certificate requests

This is a message sent to a CA asking for a certificate for protecting a server or allowing access certificate to access a protected resource such as a smartcard certificate.

Certificate practice statement

A Certification Practice Statement, or CPS, is a public statement of the practices for issuing and validating Certificates and for supporting reliance on Certificates. This is such a document, and this subsection further explains the nature and purpose of this document.

Configure CA server settings.

May include but is not limited to: key archival, certificate database backup and restore, assigning administration roles

Key archival

The private key portion of a public-private key pair may be archived and recovered. This process is known as Key recovery. The Administrator has to assume the role of a user for data access or data recovery purposes and this allows recovery of missing or corrupted keys. If a key is missing or damaged, the data will not be accessible until the key is recovered.

Certificate database backup and restore

To backup the Certificate database an administrator would perform a system state backup, which is done using the Windows Server backup utility.

Manage certificate templates.

May include but is not limited to: certificate template types, securing template permissions, managing different certificate template versions, key recovery agent

Certificate template types

The security requirements that are specific to an organization impact the types of certificates that they issue. It is possible to streamline distribution of the certificates by saving common settings into templates. The certificate template will be the starting point of a new certificate. Windows 2008 provides default certificate templates that can be used to base future creation of certificates. The certificate templates that are stored in Active Directory cannot be used on standalone CA's.

Managing different certificate template versions

Microsoft certification authorities (CA) support three types of certificate templates:

- Version 1: Provided for backwards compatibility and support general needs for subject certification
- Version 2: Allow customization of most settings in the template which provides flexibility for Administrators
- Version 3: This type of certificate allows Administrators to add Suite B cryptographic settings to their certificates

Key recovery agent

A key recovery agent is a person who is authorized to recover a certificate on behalf of an end user. It is recommended to only use trusted individuals to fulfill this responsibility because of sensitive data. To identify a key recovery agent, an administrator must configure the key recovery agent certificate template to allow the person delegated with this responsibility to enroll for a key recovery agent certificate.

Manage enrollments.

May include but is not limited to: network device enrollment service (NDES), autoenrollment, Web enrollment, smart card enrollment, creating enrollment agents

Network device enrollment service (NDES)

The Network Device Enrollment Service allows software on routers and other network devices running without domain credentials to obtain certificates based on the Simple Certificate Enrollment Process (SCEP).

Autoenrollment

There are many certificates that may need to be distributed without the client even being aware that enrollment is taking place. These can include most types of certificates issued to computers and services, as well as many certificates issued to users.

To automatically enroll clients for certificated in a domain environment these are the requirements:

- Configure a certificate template with Autoenroll permissions
- Configure an autoenrollment policy for the domain

Web enrollment

Windows 2008 AD CS has web pages available for users and administrators. These can be used to perform a variety of tasks related to requesting certificated. The pages are located at http://servername/certsrv.

Smart card enrollment

A smart card enrollment station is what is used to enroll Windows 2008 smart card clients. This can be a designated person or agent to issue smart cards from one centralized workstation or from one of any number of designated workstations. Using a smart card enrollment station and enrollment agents simplifies the physical preparation of the card to be issued, reduces the chance for certificate service interruption, and prevents users and managers from validating their own identification and issuing their own certificates. This is especially important in areas which different in levels of security and access exist.

Creating enrollment agents

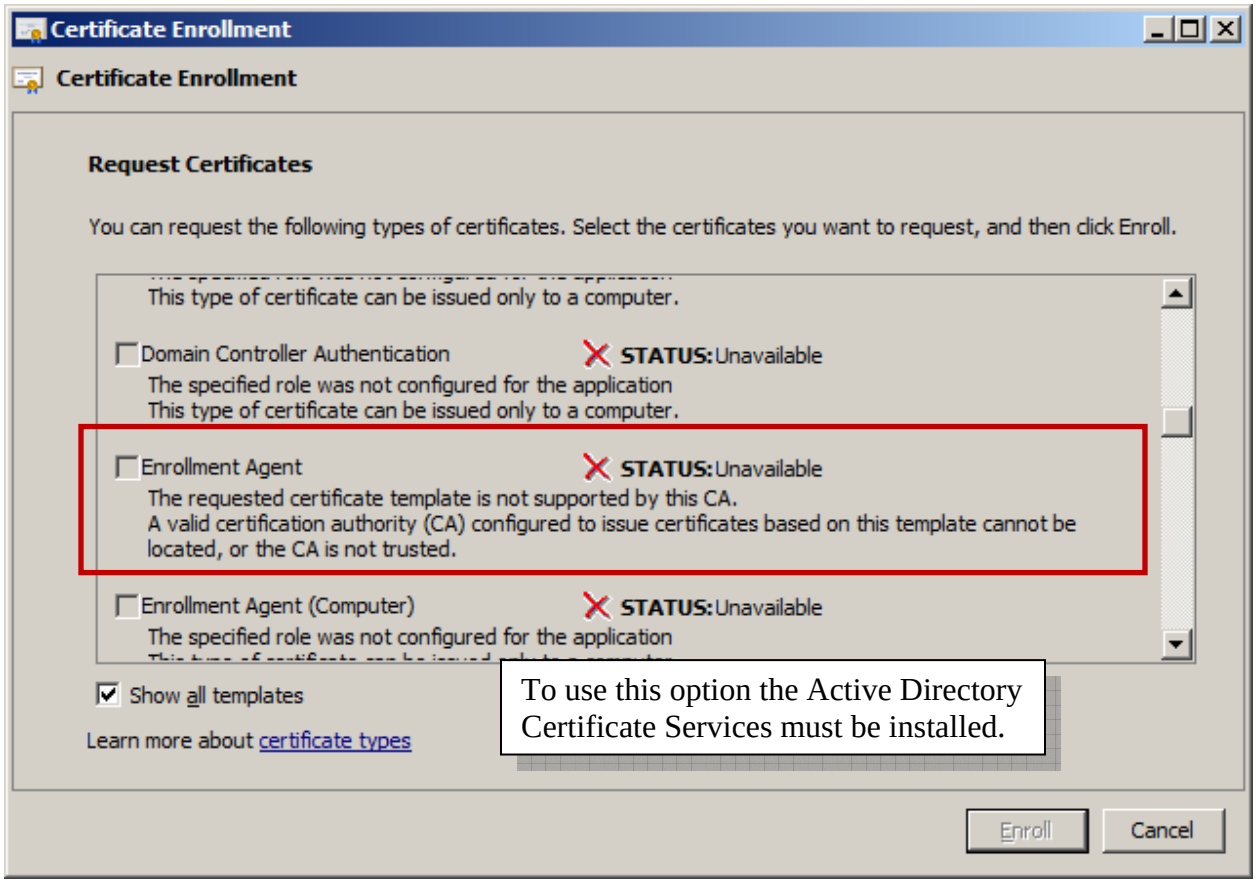
Windows 2008 includes three certificate templates that enable different enrollment agents:

- Enrollment agent
- Enrollment agent computer
- Exchange Enrollment agent (Offline Request)

The steps to create an enrollment station are:

1. Add the Certificates snap-in to a MMC
2. Click on My user account
3. Click Close
4. Double Click Certificates – Current User
5. Click on Personal in the tree
6. On the action menu point to All Tasks and click Request New Certificate
7. In the Certificate Enrollment Wizard click Enrollment Agent

8. When prompted click Install Certificate



Manage certificate revocations.

May include but is not limited to: configure Online Responders, Certificate Revocation List (CRL), CRL Distribution Point (CDP), Authority Information Access (AIA)

Configure Online Responders

The Online Responder is a trusted server that receives and responds to individual client requests for information about the status of a certificate. Unlike the CRL the Online Responder only responds to individual queries for certificate information. This is installed through adding services under the Active Directory Certificate Services server role.

Certificate Revocation List (CRL)

Certificate revocation lists are used to distribute information about revoked certificates to individuals, computers and applications attempting to verify the validity of certificates.

CRL Distribution Point (CDP)

The CRL Distribution Point is a URL pointing to the location of the CRL. You must be a CA Administrator to make changes to a CRL Distribution Point in certificates that have been issued.