Basics

Windows Server 2008 Editions: Compare and Contrast, Compare different version of Windows Server 2008

Windows Web Server 2008

This version is designed as a dedicated web server. It has all the features you need to deploy as a web server. Compared to other editions, this version only includes web hosting specific features—IIS, ASP.NET, etc.

Windows Server 2008 Standard Edition

This is a basic version for Server 2008. It includes features such as .NET framework, IIS 7 and Active Directory for small to medium size businesses and supports up to two processors and 4GB of memory.

Windows Server 2008 Enterprise Edition

This version is designed for companies that need an enterprise class system. It has all the features of the Standard Edition as well as support for up to eight processors, clustering, from 64GB RAM for x86 version up to 2TB of RAM for x64 version and hot swappable memory.

Windows Server 2008 Datacenter Edition

As the name implies, this version is designed for data centers. In addition to featuring all those of the Enterprise edition, it also supports hot swappable processors and processors from 8 to 32.

Active Directory Domain Functional Level Features

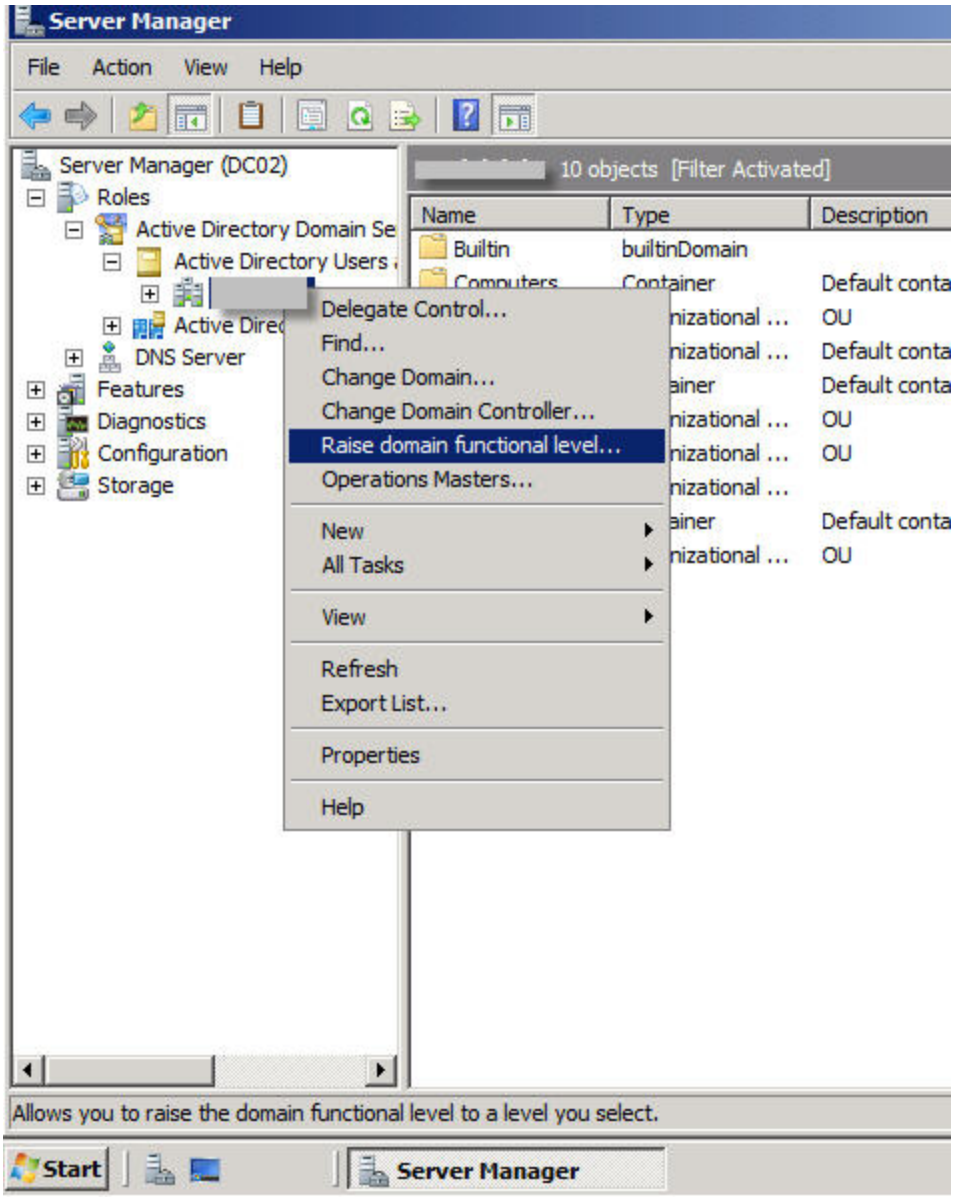
Windows Server 2003 Domain Functional Level Features:

- **Domain rename capability**
  Windows Server 2003 functional level supports rename of Active Directory domain.
- **Cross-forest transitive trusts**
  Windows Server 2003 functional level supports transitive trusts between two or more Active Directory forests.
- **Universal group caching**
  Windows Server 2003 functional level supports Universal group caching which eliminate the need for local global catalog server
- **Intersite topology generator (ISTG) improvements**
  More efficient ISTG algorithm allows support for extremely large numbers of sites.

- **Multivalued attribute replication improvements**
  This allows incremental membership changes.
- **Lingering objects (zombies) detection**
  Windows Server 2003 ability to detect zombies, or lingering objects.
- **AD-integrated DNS zones in application partitions**
  This allows storing of DNS data in AD application partition for more efficient replication.

Windows Server 2008 Domain Functional Level Features:

- **Fine-grained password policies**
  Allows multiple password polices to be applied to different users in the same domain.
- **Read-Only Domain Controllers**
  Allows implementation of domain controllers that only host read-only copy of NTDS database.
- **Granular auditing**
  Allows history of object changes in Active Directory.
- **Distributed File System Replication (DFSR)**
  Allows SYSVOL to replicate using DFSR instead of older File Replication Service (FRS). It provides more robust and detailed replication of SYSVOL contents.



How to Backup and Restore DHCP in Windows Server 2008

In Windows Server 2008, backup of DHCP database and settings has gotten simpler. You may want to backup your DHCP server from time to time to prepare for disaster recovery scenarios or when migrating DHCP server role to a new hardware.

Backup DHCP Server

1. Open Server Manager > DHCP role
2. Right click server name, choose Backup..
3. Choose a location for backup, click OK

Restore DHCP Server

1. Open Server Manager > DHCP role
2. Right Click server name, choose Restore
3. Choose the location of the backup, click OK
4. Restart the DHCP Service

New Active Directory Changes from Server 2003 SP1 to Server 2008

Changes to Active Directory from Server 2003 SP1 to Server 2008:

- Verbose Auditing: Server 2008 log values on changes that are made to AD objects.
- Restartable Active Directory Services.
- Fine-grained password policies.
- Read-only Domain Controllers.
- Improvements in AD Installation Wizard (dcpromo.exe).

New Roles in Server 2008:

- Read-only Domain Controller (RODC)
  As the name implies, Read-only domain controller only contains read only copy of Active Directory database. This allows IT administrators to place domain controller in insecure physical location such as branch offices.

- Active Directory Lightweight Directory Service (ADLDS)
  ADLDS is a Lightweight Directory Access Protocol (LDAP) directory service application. It is previously known as “Active Directory Application Mode (ADAM)” in Server 2003.

- Active Directory Rights Management Service (ADRMS)
  ADRMS provides information protection service to organizations. For example, email can be restricted to read-only; it cannot be printed, duplicated, or forwarded.

- Active Directory Federation Services (ADFS)
  ADFS allows cross-forest authentication to external resources, such UNIX environment or another forest.

Roles and Features Supported on Server 2008 Server Core Support

Server Core version on Server 2008 supports the following Roles:

- Active Directory Domain Services Role
- Active Directory Lightweight Directory Services Role
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS) Services Role
- File Services Role

- Hyper-V Role
- Print Services Role
- Web Services (IIS) Role

Server Core version on Server 2008 supports the following Features:

- Backup
- BitLocker
- Failover Clustering
- Multipath I/O
- Network Time Protocol (NTP)
- Removable Storage Management
- Simple Network Management Protocol (SNMP)
- Subsystem for Unix-based applications
- Telnet Client
- WINS

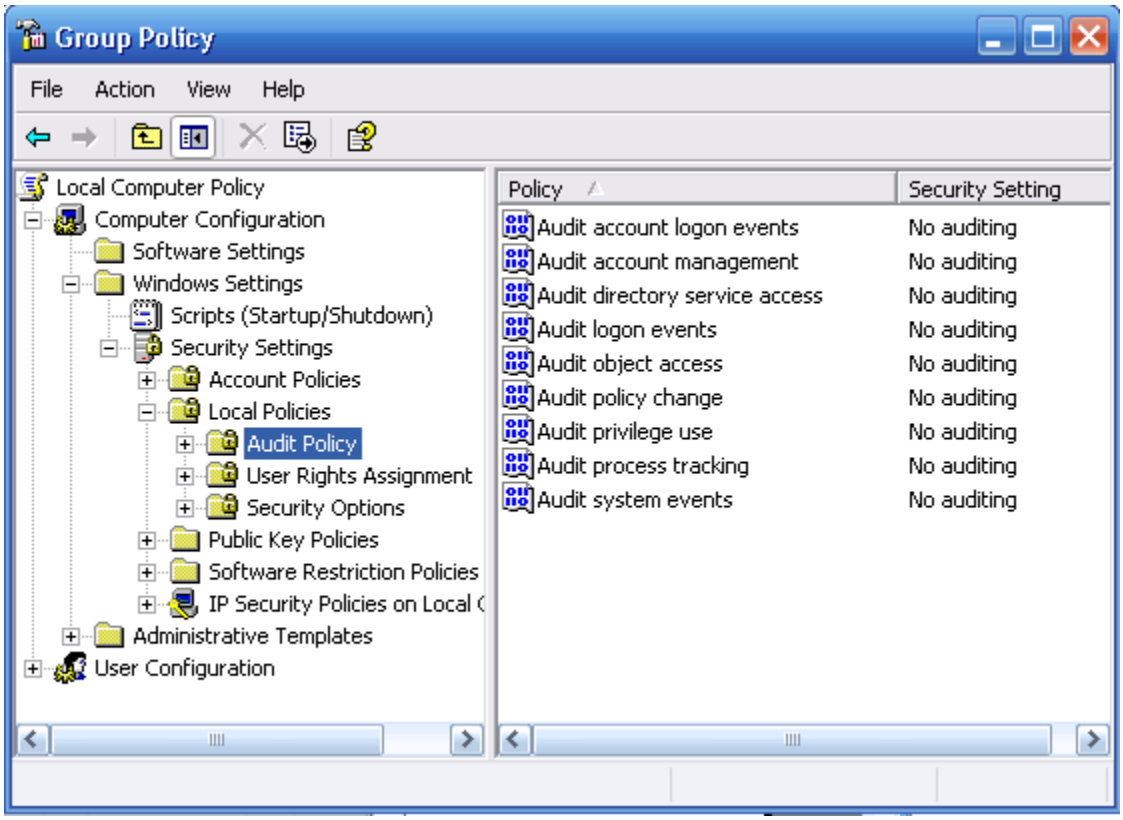
Auditing Windows Server 2008

Auditing allows IT administrators to keep track of activity on Server 2008 and Active Directory environment. Since auditing cause the event log to fill out very quickly, auditing is disabled by default. IT administrators should enable audit policies as needed since too many audit logs make it hard to review them. Audit polices can be configured in Group Policy Management Console under "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy". See screenshot. Auditing events can be viewed from Event Viewer.

Type of Audit Policies on Server 2008:

- **Audit account logon events**
  This policy logs events when user attempts to logon to a system.
- **Audit account management**
  This policy logs events when an account is changed.
- **Audit directory service access**
  This policy logs events when user attemps to access an Active Directory object.
- **Audit logon events**
  This policy logs logon events over the network or by service accounts.
- **Audit object access**
  This policy logs events when user attempts to access an object, such as file, shared folder or printer.
- **Audit policy change**
  This policy logs events when user attempts to change a policy, such as audit polices.
- **Audit privilege use**
  This policy logs events when a user attempts to exercise their privilege, such as changing the date or granting another use an admin privilege.

- **Audit process tracking**
  This policy logs events when user executes a process, application or a program when accessing the computer.
- **Audit system events**
  This policy logs system specific events such as startup and shutdown.



Administration

Server 2008 Remote Administration Tools

Remote Server Administration Tools (also known as RSAT) in Server 2008 replaces Adminpack.msi in Server 2003 and Windows XP.

List of the tools you will find in RSAT:

Role Administration Tools:

- Active Directory Certificate Services Tools
- Active Directory Domain Services (AD DS) Tools
- Active Directory Lightweight Directory Services (AD LDS) Tools
- DHCP Server Tools

- DNS Server Tools
- File Services Tools
- Network Policy and Access Services Tools
- Terminal Services Tools
- Universal Description, Discovery, and Integration (UDDI) Services Tools

Feature Administration Tools:

- BitLocker Drive Encryption Tools
- Failover Clustering Tools
- Group Policy Management Tools
- Network Load Balancing Tools
- SMTP Server Tools
- Storage Manager for SANs Tools
- Windows System Resource Manager Tools

And these tools also fully supported managing Windows Server 2003 servers:

- Active Directory Domain Services (AD DS) Tools
- Active Directory Lightweight Directory Services (AD LDS) Tools
- Active Directory Certification Authority Tools
- DHCP Server Tools
- DNS Server Tools
- Terminal Services Tools
- Universal Description, Discovery, and Integration (UDDI) Services Tools
- Group Policy Management Tools
- Network Load Balancing Tools

Install/Remove Server 2008 Roles and Features from Command Line

ServerManagerCmd.exe command-line tool can be used to Install / Remove Server 2008 Roles and Features from command line. This command-line tool can be integrated into a script to manage roles and features. Below is the output you will from ServerManagerCmd.exe /?

Usage: ServerManagerCmd.exe
Installs and removes roles, role services and features. Also displays the list of all roles, role services, and features available, and shows which are installed on this computer. For additional information about the roles, roles services, and features that you can specify using this tool, refer to the Help for Server Manager.

- query [<query.xml>] [-logPath <log.txt>]
- install <name>
  [-resultPath <result.xml> [-restart] | -whatIf] [-logPath <log.txt>]
  [-allSubFeatures]
- remove <name>
  [-resultPath <result.xml> [-restart] | -whatIf] [-logPath <log.txt>]

- inputPath <answer.xml>
  [-resultPath <result.xml> [-restart] | -whatIf] [-logPath <log.txt>]
- help | -?
- version

Switch Parameters:

- query [<query.xml>]
  Display a list of all roles, role services, and features available,
  and shows which are installed on this computer. (Short form: -q)
  If <query.xml> is specified, the information is also saved to a
  query.xml file with additional information.
- inputPath <answer.xml>
  Installs or removes the roles, role services, and features specified
  in an XML answer file, the path and name of which is represent by
  <answer.xml>. (ShortForm: -ip)
- install <name>
  Installs the role, role service, or feature on the computer that
  is specified by the <name> parameter. Multiple roles, role services or
  features must be separated by spaces. (ShortForm: -i)
- allSubFeatures
  Used with the -install parameter to install all subordinate
  role services and features along with the role, role service, or
  feature named with the -install parameter. (Short form: -a)
- remove <name>
  Removes the role, role service, or feature from the computer that
  is specified by the <name> parameter. Multiple roles, role services or
  features must be separated by spaces. (ShortForm: -r)
- resultPath <result.xml>
  Saves the result of the ServerManagerCmd.exe operation to a <result.xml>
  file, in XML format. (Short form: -rp)
- restart
  Restarts the computer automatically, if restarting is necessary to
  complete the operation.
- whatIf
  Display the operations to be performed on the current computer
  that are specified in the answer.xml file. (Short form: -w)
- logPath <log.txt>
  Specify the non-default location for the log file. (Short form: -l)
- help
  Display help information. (Short form: -?)
- version
  Display the version of the Server Manager command that is running,
  Microsoft trademark information, and the operating system.
  (Short form: -v)

Examples:

ServerManagerCmd.exe -query

ServerManagerCmd.exe -install Web-Server -resultPath installResult.xml

ServerManagerCmd.exe -inputPath install.xml -whatIf

How to Constrain Application CPU/Memory Usage on Windows Server 2008

Requirement: Windows Server 2008 Enterprise or Datacenter Edition
Prerequisites: Windows System Resource Manager Feature

1. Verify that Windows System Resource Manager is installed. If not, choose "Add Features" and install Windows System Resource Manager.
2. Go to Start > Administrative Tools > Windows System Resource Manager.
3. Connect to your computer.
4. Right click Process Matching Criteria and click "New Process Matching Criteria".
5. Type in Criteria Name (This is just a display name).
6. Click "Add" to add a new rule.
7. Under "Included files or command lines," choose Application.
8. Browse to the application you wish to constrain.
9. Under "users and groups" tab, add "BUILTIN\Users".
10. Click OK, click OK.
11. ----------
12. On System Resource Manager, right click "Resource Allocation Policies." Choose "New Resource Allocation Policy".
13. 13. Under "Policy Name", enter the name of your policy.
14. Click "Add." Select the Process Matching Criteria you just created.
15. Under "Percentage of processor" enter the maximum percentage that the process can consume.
16. You can also configure memory consumption using the "Memory" tab.

How to Disable Dynamic DNS Registration

At times, you may not want your host to register arecord automatically using dynamic DNS. If this is the case, simply run the following command on Server 2008 to disable dynamic DNS.

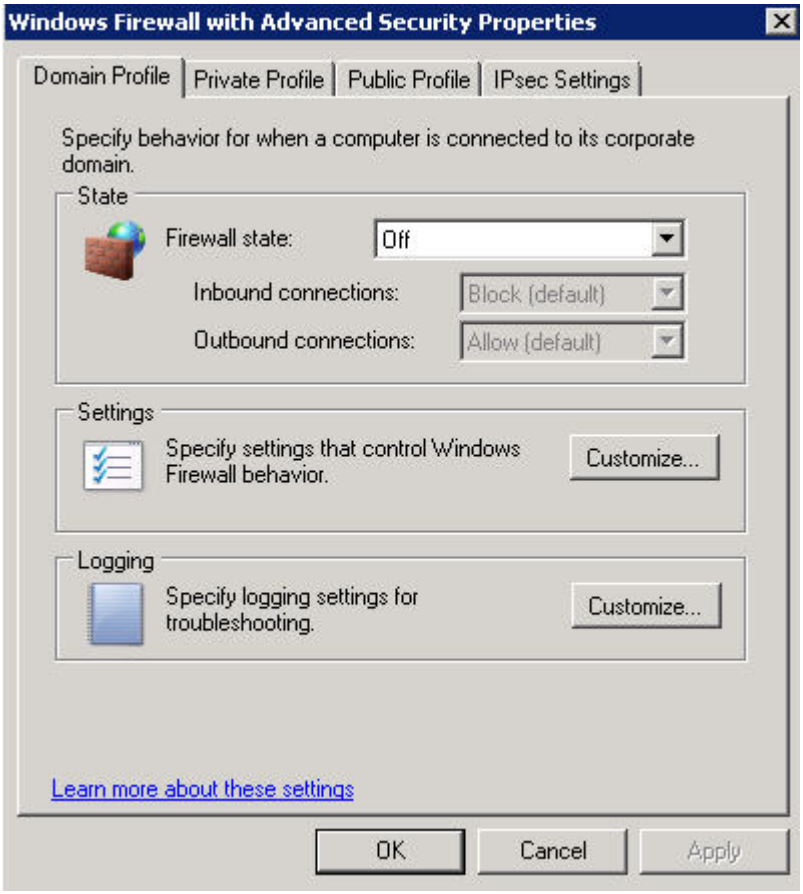
reg add hklm\system\currentcontrolset\services\tcpip\parameters /v DisableDynamicUpdate /t REG_DWORD /d 1 /f

Windows Server 2008 Firewall Profiles

On Server 2008 and Windows Vista, there are three types of firewall profiles—Domain, Private, Public profile. You can set a Firewall state(rules) for each profile and each firewall profile

applies depending on your network location. This allows you to set different firewall rules depending on your network location.

- **Domain Profile** – applied automatically when your server is connected to the Active Directory domain.
- **Private Profile** – you can assign this profile manually when your server is connected to any private address (192.168.x.x, 10.x.x.x, 172.31.x.x, etc.)
- **Public Profile** – applied by default when your first connect the server to any unknown network.



Windows Server 2008 Support Tools Download

You may ask where is the Windows Server 2008 support tools? On Server 2008 support tools are located in "support\tools" directory on the Windows Server 2008 CD, extract support.cab to the directory on your server.

UPDATE: I just spoke to someone from Microsoft. Most of Support Tools for Server 2008 should be included in "Remote Server Administration Tools". **Go to Add Features > Install Remote Server Administration Tools.**

Windows Server 2008 Network Load-Balancing (NLB) Explained

Network load-balancing (NLB)
Best for: Application Servers
Examples: Web Servers, VPN Servers, Exchange 2003 Front-end servers, Exchange 2007 CAS Servers

NLB provides a simple solution that allows high TCP/IP availability for application servers. NLB distribute the load among servers in the cluster group. When using NLB It is very important that Server OS and applications patch level are the identical to provide best user experience. You can install Server 2008 Network load-balancing (NLB) from Server Manager > “Add Features”.

Server 2008 Core Commands

> How to Configure Windows Server 2008 Server Core
> Configure Server Roles from Command Line

When you logon to Server Core, you will see a command prompt only.

Change the Administrator Password
Net user Administrator mypassword

Set IP on Network Interface
Use following command to view all network adapters on the server:
Netsh interface ipv4 show interfaces

Note the Idx # of the network adapter you want to configure
Use following command to configure IP of 10.0.1.2/24 on Idx 2.
Netsh interface ipv4 set address name=2 source=static address=10.0.1.2 mask=255.255.255.0 gateway=10.0.1.1

Use following commands to configure DNS server
Netsh interface ipv4 add dnsserver name=2 address=10.0.1.110

Activate the Server
Run Slmgr.vbs –ato

Rename the Server using WMI
wmic computersystem where name="%computername%" rename name="Server1"

Join the Server to the Domain
Netdom join %computername% /domain:domainname /userd:domainadmin /password:domainadminpassword

Adding Server Roles

1. Adding and Configuring the DNS Server Role
Use following command to install DNS Server role:
Start /w ocsetup DNS-Server-Core-Role

Once the DNS Server Role is installed, you can use DNS MMC from different computer or dnscmd.exe from command line to configure DNS.

2. Adding and Configuring the DHCP Server Role

Use following command to install DNS Server role:
Start /w ocsetup DHCPServerCore

Once the DHCP Server Role is installed, you can use DHCP MMC from different computer or netsh.exe from command line to configure DHCP.

3. Adding and Configuring the File Services

To install Distributed File System, run
start /w ocsetup DFSN-Server

To install File Replication Service
start /w ocsetup FRS-Infrastructure

To install Distributed File System Replication
start /w ocsetup DFSR-Infrastructure-ServerEdition

To install Network File System
start /w ocsetup ServerForNFS-Base
start /w ocsetup ClientForNFS-Base

4. Adding and Configuring the Active Directory Domain Services Role

Use following command to install Active Directory role
Dcpromo /unattend:c:\unattend.txt

*you must create c:\unattend.txt using notepad(notepad.exe is built-in to Server Core).

Adding and configuring Features

To install WINS (Windows Internet Name Service)
start /w ocsetup WINS-SC

To install Microsoft Failover Clustering
start /w ocsetup FailoverCluster-Core

To install SNMP (Simple Network Management Protocol)
start /w ocsetup SNMP-SC

To install Windows Backup
start /w ocsetup WindowsServerBackup

To install Multipath IO
start /w ocsetup MultipathIo

To install NLB (Network Load Balancing)
start /w ocsetup NetworkLoadBalancing HeadlessServer

To Install Hyper-V
start /w ocsetup Microsoft-Hyper-V

Server 2008 WinRM and WinRS explained

Windows Remote Management (WinRM) allows administrator to manage remote server via command line interface. The commands are sent remotely and executed locally on remote computer. On Server 2008 WinRM listen port 80 and 443 and uses /wsman URL. It is important to note that IIS role doesn't need to be installed for WinRM to work.

For example, you want to access EX01 remotely. You can simply configure WinRM by running **winrm quickconfig** on EX01. Now, you can connect to EX01 remotely by running **winrs –r:http://EX01.domain.com shutdown /r /t 1**. Previous command restarts EX01 remotely.

Accessing Server 2008 remotely using Windows Remote Shell

Run following command to Enable WinRM on remote computer,
WinRM quickconfig

You can use WinRS to connect to a remote server using following command,
Winrs –r:remoteservername cmd

*make sure firewall is not blocking remote connections

Below is the help file from Microsoft

Windows Remote Management Command Line Tool

Configuration for WinRM is managed using the winrm command line or through GPO. Configuration includes global configuration for both the client and service.

The WinRM service requires at least one listener to indicate the IP address(es) on which to accept WS-Management requests. For example, if the machine has multiple network cards, WinRM can be configured to only accept requests from one of the network cards.

Global configuration
winrm get winrm/config
winrm get winrm/config/client
winrm get winrm/config/service
winrm enumerate winrm/config/service/certmapping
winrm enumerate winrm/config/winrs/customremoteshell

Network listening requires one or more listeners.
Listeners are identified by two selectors: Address and Transport.

Address must be one of:
* - Listen on all IPs on the machine
IP:1.2.3.4 - Listen only on the specified IP address
MAC:... - Listen only on IP address for the specified MAC

Note: All listening is subject to the IPv4Fitler and IPv6Filter under
config/service.
Note: IP may be an IPv4 or IPv6 address.

The configuration that allows a client to run a remote shell and
arguments based on a URI is stored in the CustomRemoteShell table.
The table is identified by the following resource URI:

winrm/config/winrs/customremoteshell

Each entry in this table contains three properties:
URI - The URI of the shell resource.
Shell - The executable to be launched.
Arguments - The arguments to be passed to the shell Shell.

The URI is the key and is case-insensitive; wildcards, internal whitespaces
and '?' character are not allowed.

The shell executable must be specified as a full path.
It can contain environment variables; the environment
variables are expanded on the remote machine.

Example: To see the current CustomRemoteShell configuration
winrm enumerate winrm/config/winrs/customremoteshell

Example: To create an entry for PowerShell:
winrm create winrm/config/winrs/customremoteshell?uri=shell/Microsoft.Powershell @{
Shell="%windir%\system32\windowspowershell\v1.0\PowerShell.exe";Arguments="-s -
nologo"}

Transport must be one of:
HTTP - Listen for requests on HTTP (port 80)
HTTPS - Listen for requests on HTTPS (port 443)

Note: HTTP traffic by default only allows messages encrypted with
the Negotiate or Kerberos SSP.

When configuring HTTPS, the following properties are used:
Hostname - Name of this machine; must match CN in certificate.
CertificateThumbprint - hexadecimal thumbprint of certificate appropriate for
Server Authentication.

Note: If only Hostname is supplied, WinRM will try to find an appropriate certificate.

Example: To listen for requests on HTTP on all IPs on the machine:
winrm create winrm/config/listener?Address=*+Transport=HTTP

Example: To disable a given listener
winrm set winrm/config/listener?Address=IP:1.2.3.4+Transport=HTTP @{Enabled="false"}

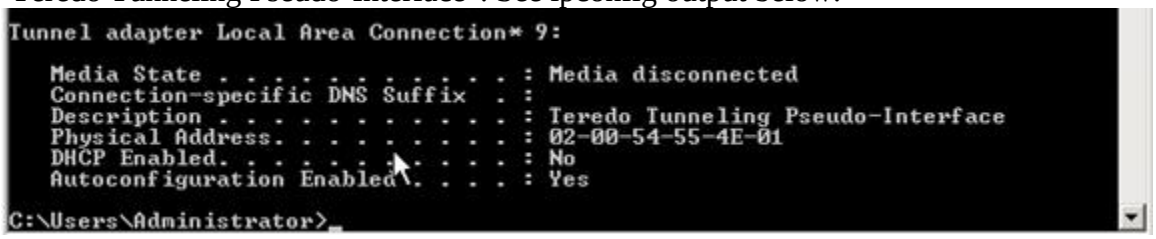
Example: To enable basic authentication on the client but not the service:
winrm set winrm/config/client/auth @{Basic="true"}

Example: To enable Negotiate for all workgroup machines.
winrm set winrm/config/client @{TrustedHosts="<local>"}

See also:
winrm help uris
winrm help aliases
winrm help certmapping
winrm help input
winrm help switches

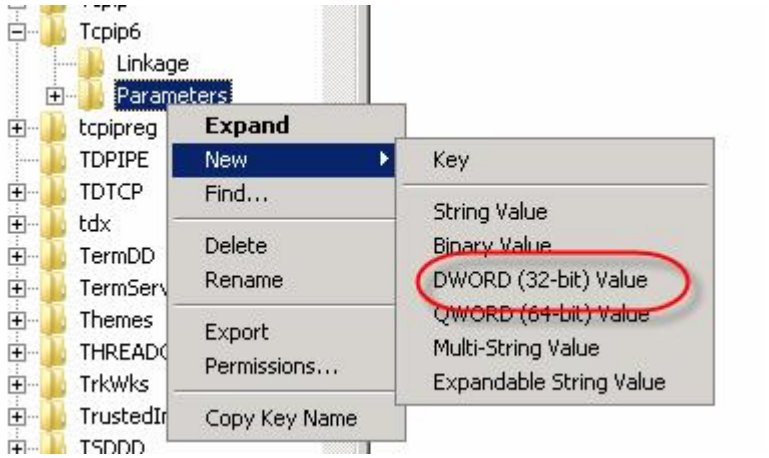
Server 2008 Disable IPV6

How to uninstall TCP/IPv6 on Server 2008. You may want to uninstall TCP/IPv6 for a number of reasons. When you uninstall TCP/IPv6 on Server 2008, it removes Tunnel adapter named "Teredo Tunneling Pseudo-Interface". See ipconfig output below.

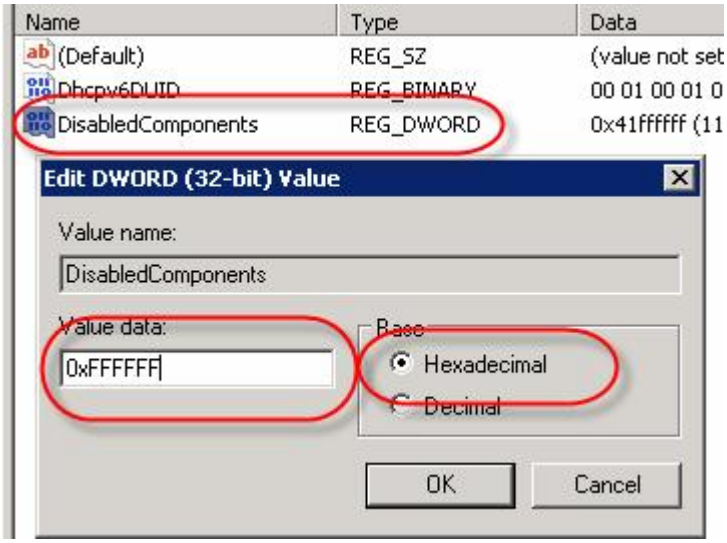


Disable TCP/IPv6

1. Uncheck "Internet Protocol version 6 (TCP/IPv6)" from all of your connections and adapters and component in the list under "This connection uses the following items."
2. Open Registry Editor, Regedit.exe
3. Browse to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
4. Right click on "Parameters", choose "New", choose "DWORD (32-bit) Value"



5. Change the name of the key to “DisabledComponents”, set the value to 0xFFFFFFFF, Hexadecimal



6. Restart the computer for the registry value to take effect.

File Services

Windows Server 2008 File Services

How to implement NFS on Windows Server 2008 File Services
Windows Server 2008 File Services allows you to implement and manage a file server. New features such as Storage Utilization Monitoring allow you to monitor disk usage and run reports.

Add Windows Server 2008 "File Server" Role:

1. Open Server Manager, click on "Add Roles".
2. choose "File Services", click Next.
3. On "Select Role Services" screen, choose File Server, File Server Resource Manager. Click Next.
   Note: choose "Services for Network File System", if you need to serve files to UNIX systems.
4. On "Configure Storage Utilization Monitoring" screen, choose the volume you want to monitor.
5. Click Install at the end.

Create a Share Using "Provision a Shared Folder Wizard"

1. 1. Open Server Manager, on the left pane, expend Roles > File Services > Share and Storage Management.
2. Click "Provision Share link" on the right pane.
3. On "Shared Folder Location" Screen, Browse to the location you want to share, click Next.
4. On "NTFS Permissions" screen, select "Yes, change NTFS permissions", click "Edit permission" and add appropriate users.
5. On "Share Protocols", check "SMB", enter Share name.
   Note: Check "NFS", if you need to serve files to UNIX systems via NFS.
6. On "SMB Settings" screen, Click Next.
7. On "SMB Permissions" screen, you can configure share-level permissions. These permissions apply to users browsing the shares over the network.
8. On "Quota Policy" screen, you can configure disk quota.
9. On "File Screen Policy" screen, you can configure types of files that is not allowed on the share.
10. On "DFS Namespace Publishing" screen, you may configure DFS if needed.
11. On "Review Settings and Create Share" screen, click Create.

Windows Server 2008 Permissions Explained

- **Read** – Allows users to read the object
- **Write** – Allows users to write to existing objects or create new objects.
- **Read and Execute** – Allows users to read attributes of a object and read its contents.
- **List Folder Contents** – Allows users to list contents.
- **Modify** – Allows users to read, write, execute and delete objects.
- **Full Control** - Allows users to read, write, execute, delete objects and change permissions on the object.

How to configure snapshot (volume shadow copy) on Windows Server 2008 File Server.

Previous versions in Windows Server 2008 allows you restore files to certain points in time when user accidentally modify the file. **This feature is enabled for you by default in Windows Server 2008**, unlike earlier versions. **To configure the snapshot schedule, follow below directions**.

1. Open Computer, Right click on the Volume, choose properties
2. On Shadow Copies tab, select the disk, click the Settings button
3. Click the schedule button and you may change the schedule from there.

Server 2008 DFS

The Distributed File System (DFS) allows you consolidate multiple shares on multiple servers to one logical place. This allows users to simply access all the shares from one central location. In a way, it is very similar to how we create short cut on our desktop to different locations. DFS replication also allows file replication with compression, throttling and scheduling.

Create a DFS namespace (Central Share)

Prerequisites: File Services role with DFS installed.
1. Open Server Manager, expend File Services role
2. Right click on the Namespace node in the left pane and select New Namespace
3. On “Namespace Server” screen, enter the name of the server, click Next
4. On “Namespace Name and Settings page” screen, enter the name of the namespace. I would name this something meaningful, (IT, Accounting, etc.)
5. On “Namespace Type”, choose “Domain-based namespace” if you have active directory, if not choose “Stand-alone namespace”
6. On “Review Settings and Create Namespace” screen, click Create. Add folder targets to namespace (distributed shares on multiple servers)7. Simply right click on the name of the namespace and select New Folder.

Now you can access all folder targets from step #7, by using namespace from step #4.

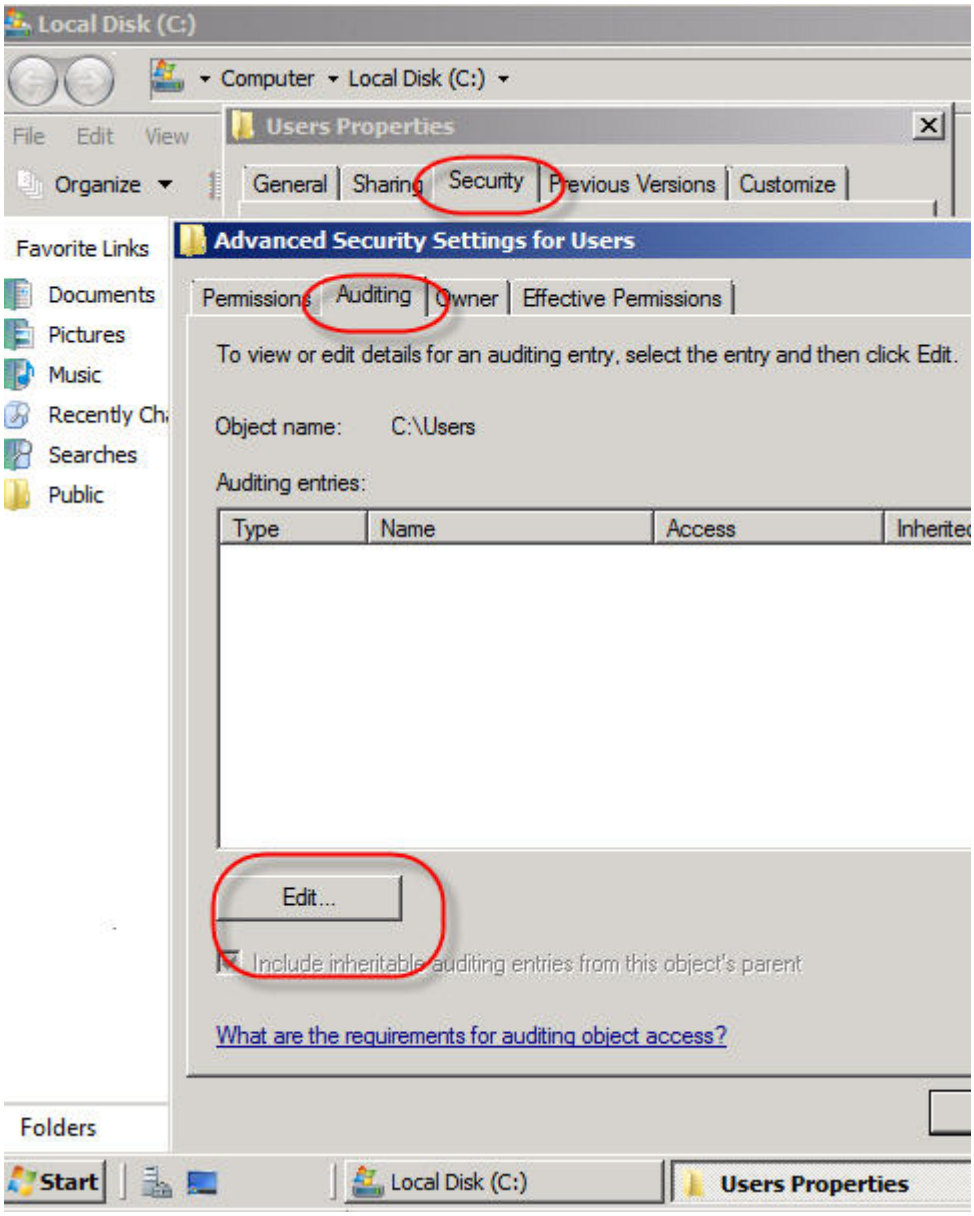
Audit File access on Server 2008

On important files and folder, you may want to configure auditing to keep an access log. It allows logging of who is accessing a directory.

Configure auditing on a folder on Server 2008

1. Right click folder which you want to audit
2. Select Security tab
3. Click the Advanced button.
4. Select Auditing tab.
5. Click the Edit button
6. Click the Add button, enter the Everyone group
7. Select types of access that you want audited.
8. Click OK to apply, Click Ok to save the settings

Now, you may view the auditing log from the Event Viewer.



IIS 7

Installing IIS 7.0 on Server 2008 from command line / Script

You can install IIS from command line on Server 2008 using pkgmgr.exe.

Start /w pkgmgr.exe /iu:IIS-WebServerRole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI

IIS 7.0 Configuration Files Explained

IIS 7.0 use configuration files instead of
the IIS metabase. IIS 7.0 configuration consist of four files.

1. Machine.config – These settings apply globally.
2. ApplicationHost.config – These settings are specific to IIS. Found in %systemroot%\system32\inetsrv
3. Web.config, root-level – These settings are shared by .NET applications. Found in %systemroot%\ Microsoft.NET\Framework\versionNumber\CONFIG.
4. Web.config, application-level – These settings apply to a specific .NET application.

Managing IIS 7.0 from command line on Server 2008

You can use %WINDIR%\system32\inetsrv\APPCMD.EXE to manage IIS 7.0 from command line in Server 2008.

Examples:
List all sites and its details
Appcmd.exe list SITE

List Default Web Site
APPCMD.EXE list SITE "Default Web Site"

List started sites
APPCMD.EXE list SITE /state:started

List all start / stopped application pools
APPCMD.EXE list apppools /state:started
APPCMD.EXE list apppools /state:stopped

Add a site called MySite on Port 80 in c:\inetpub\MySite
APPCMD.EXE add site /name:"MySite" /id:123 /bindings:"http:/*:80:" /physicalPath:"C:\inetpub\MySite"

List real time HTTP requestes
APPCMD.EXE list requests

List IIS configuration
APPCMD.EXE list config

Backup IIS configuration
APPCMD.EXE add backup IISBACKUP

Restore IIS configuration
APPCMD.EXE restore backup IISBACKUP

Installing IIS 7.0 on Server 2008 from command line / Script

You can install IIS from command line on Server 2008 using pkgmgr.exe.

Start /w pkgmgr.exe /iu:IIS-WebServerRole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI

Active Directory

What is the difference between Active Directory Forest and Domain?

Active Directory Forest and Active Directory Domain Explained.

Forest: Forest is the top level container of Active Directory infrastructure. A forest can consist of one or more domains and those domains are connected through transitive trust. A forest shares a single schema database, single Exchange organization, single global address list and a security boundary. Note: You may allow access to resources of only those in the same forest. You may want multiple forest if you need:

- more than one Exchange organization

- different forest functional levels

- separate security boundary

Domain: Domain is one level below Active Directory Forest. A domain can consist of one or more organization unit. A domain shares a single administrator group (Domain Admins security group) and same set of objects. Even when a domain shares a single administrator group, you may delegate control over each organization unit (OU).

Domain controller: Every domain consists of one or more domain controllers. Domain controller holds a directory database of its perspective domain. The directory database consists of user objects, computer objects and much more.

Organization unit (OU) is folder/container within a domain. OU can be used to organize set of computers or users. OUs are very useful when implementing different set of polices to a group of users or computers within a domain.

Active Directory Security Groups Explained

You may be wondering what the differences are among domain local groups, domain global, and universal groups. There are four types of security groups and each has its own security scope.

- **Machine local groups**
  This type of group can be created on a local computer. The security scope of this group is limited to this local machine. This group can include members that are Domain local groups, domain global groups and users within its domain and forest.

- **Domain local groups**
  This type of group can be created on a domain controller of its perspective domain. This group can only be used to assign permission on resources within the same domain. This group can include user accounts, universal groups, and global groups from any domain.

- **Domain global groups**
  This type of group can be created on a domain controller of its perspective domain. This group can be used to assign permission on resources in any trusted domain. This group can include user accounts, universal groups, and global groups from any domain.

- **Universal groups**
  This type of group can be created on a domain controller of its perspective domain that is running in mixed mode or higher. This group is known as "jack-of-all-trade" because it is used to assign permissions to resources in multiple domains. This group can include user accounts, universal groups, and global groups from any domain.

Server 2008 Domain Controller

Windows Server 2008 Active Directory prerequisites:

- If you are adding Windows Server 2008 Domain Controller to existing Windows 2000 or Windows Server 2003 forest, you must run **adprep /forestprep** on schema master.
- If you are adding Windows Server 2008 Domain Controller to existing Windows 2000 or Windows Server 2003 Domain, you must run **adprep /domainprep /gpprep** on infrastructure master.
- If you plan to use RODC (read-only domain controller), you must also run adprep /rodcprep

* You will find adprep tool in .\sources\adprep folder of the Windows Server 2008 CD.

Once all the prerequisites are met, you can run **dcpromo /adv** from Server 2008, follow the on screen directions.

Verify successful Windows Server 2008 Domain Controller promotion:

- Check directory service and File Replication event log to make sure there are no errors
- Open DNS Console, make sure all the SRV Records are created in _msds.YOURDOMAIN.NET zone
- Open Active Directory Users and Computers, make sure you can access the objects.

Windows Server 2008 Active Directory Certificate Services (AD CS) Explained

Windows Server 2008 Active Directory Certificate Services (AD CS) is known as Certificate Services in Server 2003. In Server 2003, Certificate Services is installed from ADD/REMOVE Windows components. In Server 2008, Active Directory Certificate Services (AD CS) is

installed from +Add Roles. AD CS is a low cost method of issuing digital certificates internally and maintaining a Certificate Authority (CA) infrastructure.

Active Directory Certificate Services Roles

- **Enterprise root certification authority**
  This is the top level, most trusted CA in an organization which should be installed before any other roles. This role should be highly protected as this is a most important role in CA infrastructure.
- **Enterprise subordinate certification authority**
  Enterprise subordinate CA can be used to off load work from Enterprise root CA. This CA can issue digital certificates internally but it must get a certificate from Enterprise root CA.
- **Stand-alone root certification authority**
  As the name implies, this is the top level CA that is independent from Enterprise root CA. Stand-alone root CA can be deploy for testing or particular purposes.
- **Stand-alone subordinate certification authority**
  As the name implies, subordinate CA can be used to off load work from Stand-alone root CA. This CA can issue digital certificates but it must get a certificate from Stand-alone root CA.

How to Install Windows Server 2008 Active Directory Certificate Services (AD CS)

1. Open Server Manager
2. Click on Add Roles
3. Click Next, chose “Active Directory Certificate Services”, click Next, click Next
4. Choose required roles services.
5. Choose Enterprise CA
6. Choose Root CA
7. Choose create new private key
8. Choose default settings for private key encryption settings
9. Choose the name of the CA, example: Organization-RootCA
10. Choose 5-year validity period.
11. Choose certificate database and log location
12. Confirm selections and click Install

After Enterprise root CA is install, it can be managed from Certification Authority console, Start>All
Programs>Administrative Tools>Certification Authority

Server 2008 Active Directory Sites Explained

From Active Directory perspective Site is well connected group of physical subnets which define internal replication boundary. Organizations usually create multiple Sites depending on their WAN infrastructure to control replication. It can also be use as a security scope to delegate authority to an administrator and used as an object to apply Group Policy. A Site contains Site name, Subnets that are associated to the Site, Site Links that are use to connect to other sites and DCs within the Site. Note: The term Intrasite replication refers to replication of DCs within the same site. The term Intersite replication refers to replication of DCs at different sites.

Relationship between Active Directory Sites and Domains

It is important to understand that Active Directory Sites and Domains can overlap. Active Directory Sites are independent to Active Directory Domains and vice versa. Multiple domains can exist within a single site as single domain can expand to multiple sites.

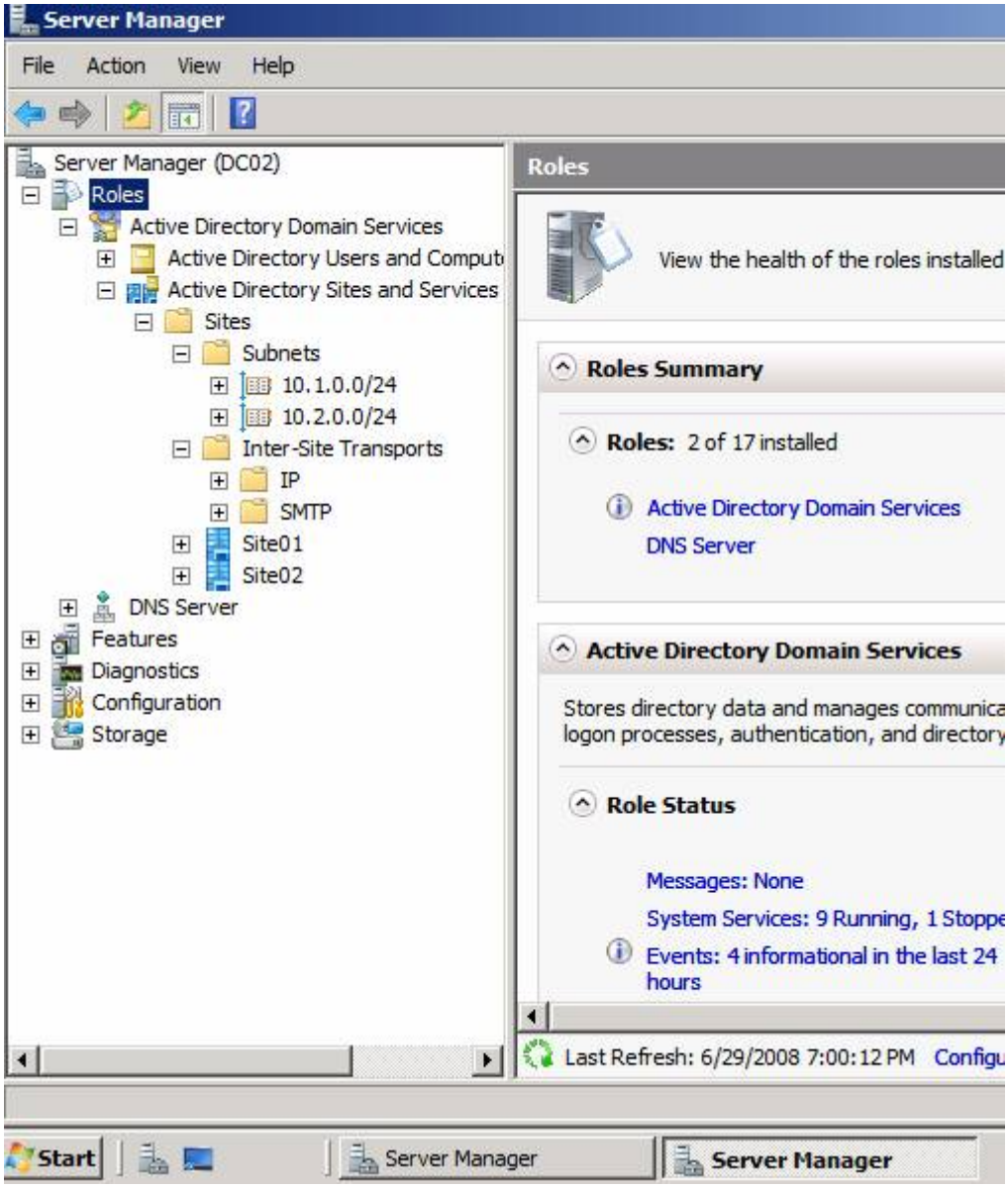
Server 2008 Active Directory Site Components

- Subnets
Subnets include list of well connected networks in the same site. I define “well connected” when speed is faster than 100/mbps. When a client—workstation looks for a Global Catalog, it prefers a Global Catalog in a same site / subnet as oppose to others. If subnets are not associated with a Site, clients can Global Catalog server in a different Site over WAN causing unnecessary traffic.

- Site Links
Site Links are the transport mechanism for Active Directory replication between sites. Site Links should be configured to mimic physical WAN connections between Sites. Replication interval and costs can be configured on Site Links. Active Directory Knowledge Consistency Checker (KCC) uses Site Links to build connections to make sure that replication occurs in efficient manner.

How to create a Site in Server 2008 Active Directory

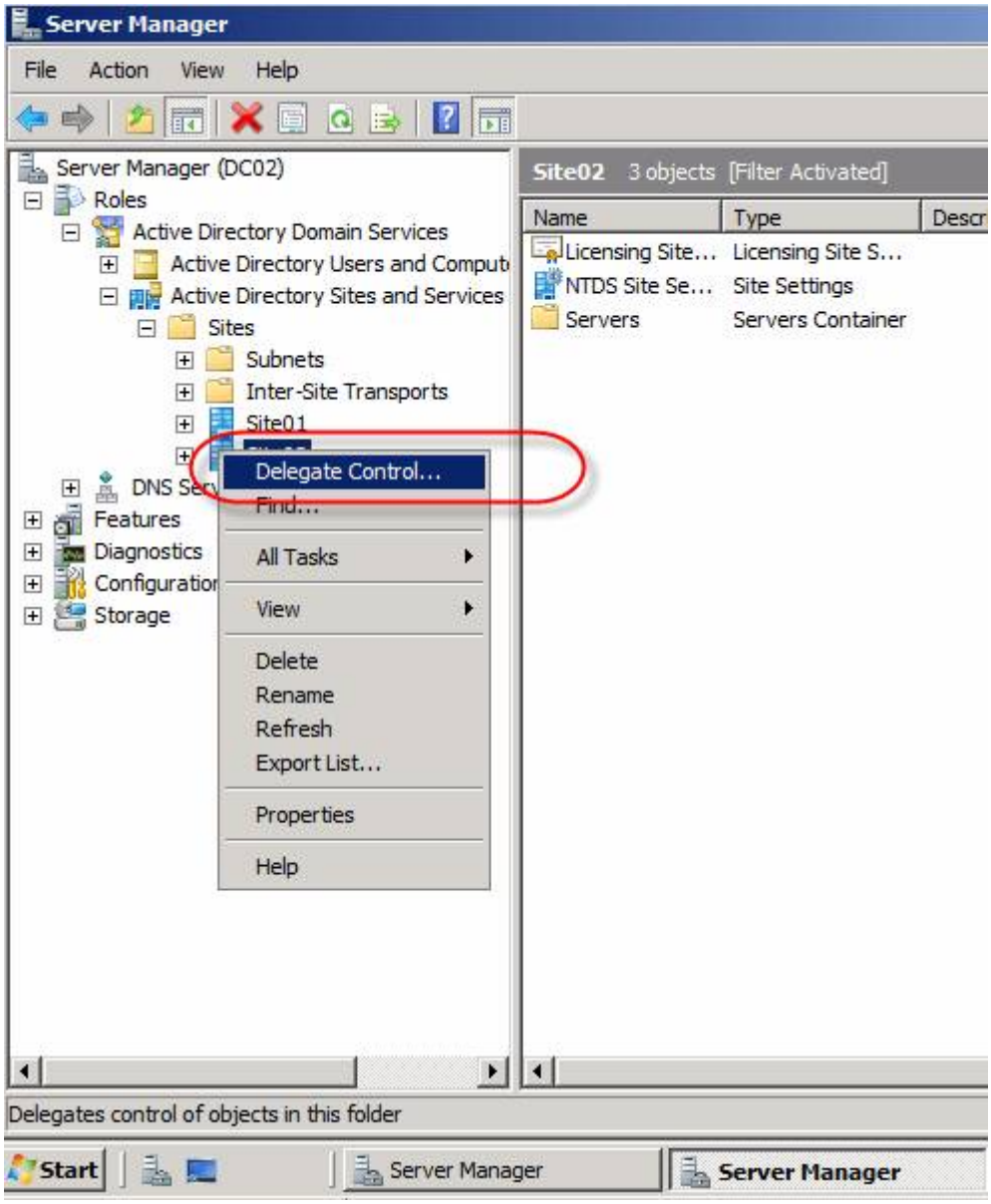
1. Open Active Directory Sites and Services console on a domain controller
2. Right click the Sites container and chose New Site.
3. Name the site choose a Site Link, lick Ok
4. To create a subnet, right click the Subnets container, and choose New Subnet.
5. Enter the network range, example: 192.168..1.0/24
6. Choose the proper Site from the list to associate with the new subnet.



Active Directory Delegation

We are most familiar with delegating administers control at OU level or Domain level in Active Directory. How to delegate control at Active Directory Site Level. You can also use this method to deny an administrator at Active Directory Site Level. Follow below steps to delegate control at Active Directory Site Level.

1. Open Active Directory Sites and Services console on a domain controller
2. Right click the Sites container and choose Delegate Control.
3. Click Next, use Add button to select the user or group, click Next
4. On the Active Directory Object Type screen, choose defaults
5. Click Next, On the Permissions screen, check the desired permissions type check boxes.
6. Click Next and Finish



Server 2008 Domain Controller

Windows Server 2008 Active Directory prerequisites:

- If you are adding Windows Server 2008 Domain Controller to existing Windows 2000 or Windows Server 2003 forest, you must run **adprep /forestprep** on schema master.
- If you are adding Windows Server 2008 Domain Controller to existing Windows 2000 or Windows Server 2003 Domain, you must run **adprep /domainprep /gpprep** on infrastructure master.
- If you plan to use RODC (read-only domain controller), you must also run adprep /rodcprep

* You will find adprep tool in .\sources\adprep folder of the Windows Server 2008 CD.

Once all the prerequisites are met, you can run **dcpromo /adv** from Server 2008, follow the on screen directions.

Verify successful Windows Server 2008 Domain Controller promotion:

- Check directory service and File Replication event log to make sure there are no errors
- Open DNS Console, make sure all the SRV Records are created in _msds.YOURDOMAIN.NET zone
- Open Active Directory Users and Computers, make sure you can access the objects.

Windows Server 2008 RODC (Read-Only Domain Controller) Explained

Pros and Cons of Windows Server 2008 RODC (Read-Only Domain Controller)

Facts:
- stores read-only copy of Active Directory NTDS.dit database, except passwords
- support caching of universal groups
- When user authenticate, RODC verifies that account exists then forward it to a regular DC

Pros:
- Perfect for branch offices that doesn't have IT staff on site
- Can be used by third-party applications to prevent accidental changes

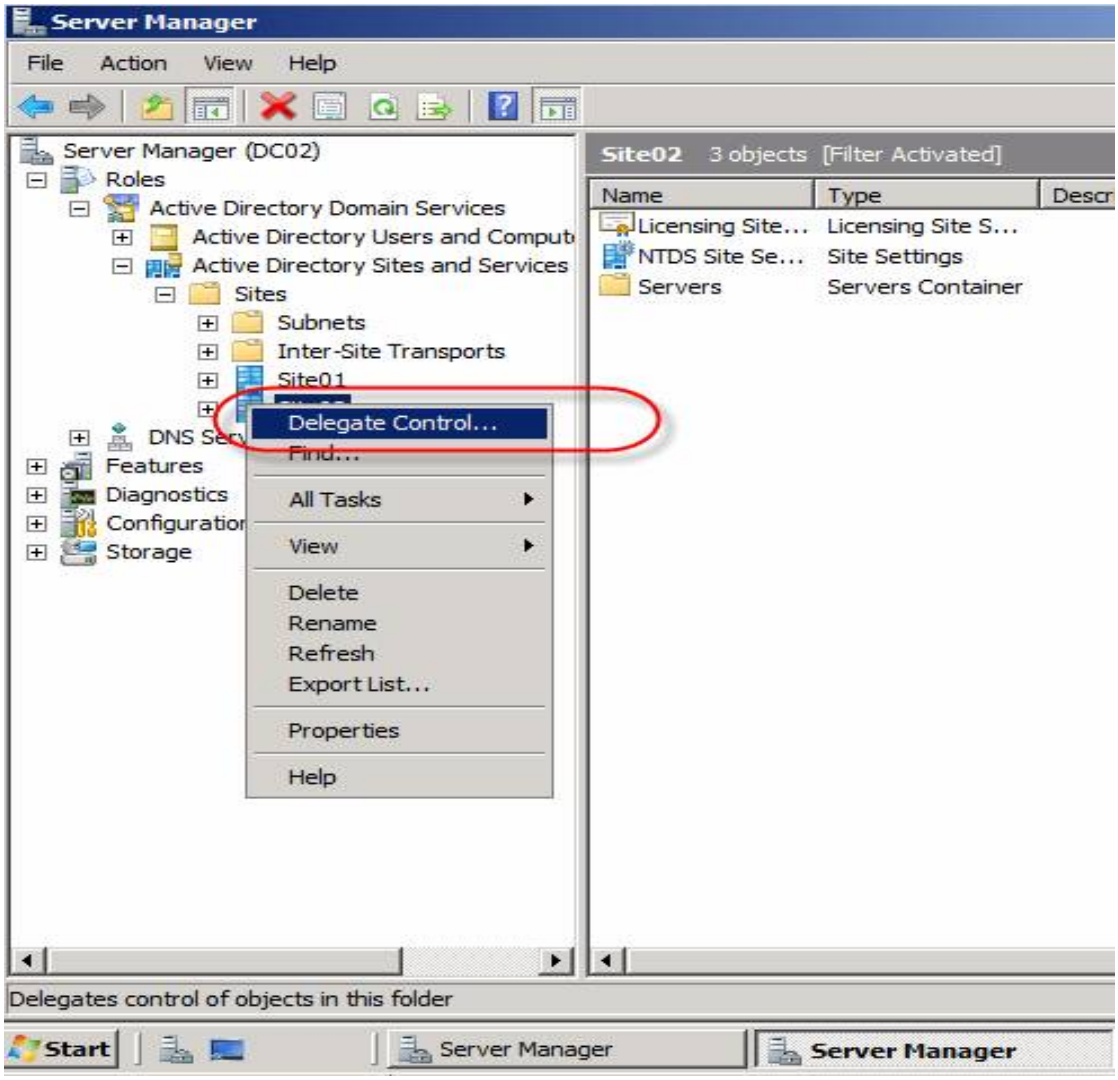
Cons:
- Branch office administrators cannot modify Active Directory objects.
- extra traffic may occur due to excessive authentication packets to regular DC.

How to audit changes to your active directory on Windows Server 2008 > How to audit account access on Windows Server 2008

In server 2008, you can track attribute changes that let you track old attributes and new attributes.

You can configure active directory auditing by editing the default domain controller policy. On Group Policy Management Editor, expend Computer Configuration > Windows Settings > Security settings > Local Policies > Audit Policy

You can view all the audit events from Windows Security Event Log. The cool thing is attribute changes—both the old value and new value is written to the event log.



How to Restore Server 2008 Active Directory (non-authoritative)

1. On Server 2008 DC, open the command prompt on the server
2. Run below commands to enter Directory Services Restore Mode (DSRM):
bcdedit /set safeboot dsrepair
shutdown –r –t 1
3. Login using .\administrator and DSRM password
4. Run below command (note that d: is the drive letter of your backup), this will show you the version identifier of the backup.
Wbadmin get versions –backuptarget:d:
5. Run below command to start the restore.
Wbadmin start sysstaterecovery –version:01/01/2008-22:30 –backuptarget :d:
6. After the restore process is completed, run following commands to reboot.
Bcedit /deletevalue safeboot
Shutdown –t 0 -r

How to Restore Server 2008 Active Directory if Someone Accidentally Deletes an Object. (authoritative restore)

1. Restore Server 2008 Active Directory (non-authoritative), do not reboot the server
2. Open command prompt, run following commands, where CN=VIPuser,CN=Users,DC=MYDOMAIN,DC=NET is the object you wish to restore.
ntdsutil
activate instance NTDS
authoritative restore
restore object "CN=VIPuser,CN=Users,DC=MYDOMAIN,DC=NET"

3. Once it's completed. Type quit
4. After the restore process is completed, run following commands to reboot.
Bcedit /deletevalue safeboot
Shutdown –t 0 -r

How to Forward DNS Queries for Specific Domain to a Specific DNS Server

This goal can be achieved using Conditional forwarding that is supported in Windows Server 2003 and Windows Server 2008.

Configure Conditional Forwarding on Windows Server 2003 or Windows Server 2008 DNS Server

1. Open Server Manager, expend to DNS under roles (on Server 2003 open DNS console)
2. Right Click on the DNS Server and choose "Properties"
3. On "Forwarders" tab, click "New"
4. Enter the domain name and press OK
5. In DNS Domain box, Click the domain name and add list of DNS server,
6. Then Click Apply or OK

As you can see, this will help you control DNS queries for specific domain to a specific DNS server.

How to Forward DNS Queries for Specific Domain to a Specific DNS Server

This goal can be achieved using Conditional forwarding that is supported in Windows Server 2003 and Windows Server 2008.

Configure Conditional Forwarding on Windows Server 2003 or Windows Server 2008 DNS Server

1. Open Server Manager, expend to DNS under roles (on Server 2003 open DNS console)
2. Right Click on the DNS Server and choose "Properties"

3. On “Forwarders” tab, click “New”
4. Enter the domain name and press OK
5. In DNS Domain box, Click the domain name and add list of DNS server,
6. Then Click Apply or OK

As you can see, this will help you control DNS queries for specific domain to a specific DNS server.

How to Add Child Domain to Active Directory

It is very important to have a concrete step by step plan when adding a child domain to active directory. You cannot easily recover active directory from fatal errors, especially in large Active Directory environments. I will walk through how to add child domain to active directory and properly configure DNS. The best practice is to delegate child DNS domain to child DNS Server.

Design Child Domain DNS Infrastructure

Terminology:

Root DNS Server
This is the DNS server that holds the DNS for root domain. For example: mylab.com

Child DNS Server (also Child DC)
This is the DNS server that holds the DNS for child domain. For example: sub1.mylab.com

How DNS Delegation Works
Delegation of child DNS domain allows root DNS server to forward DNS queries for Child DNS domain to Child DNS Server. When a client request for a lookup on resource on child DNS domain against root DNS Server, the root DNS Server forwards the query to child DNS Server.

Create DNS Delegation for Child Domain:

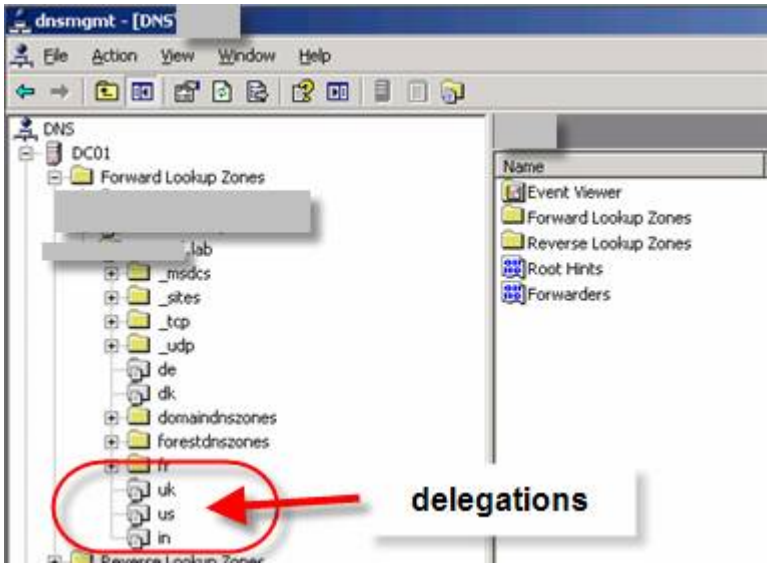
On root DNS Server,

1. Open DNS management console.
2. Right click on root zone, choose “New Delegation”, click Next.
3. Enter the child DNS server, click Next.

On child DNS Server.

4. Confirm child DNS server is using the root DNS server as the only DNS Server.
5. Install DNS Server from Add/remove Windows Components.
6. Open DNS management console
7. Create Standard Primary, Forward lookup zone (right click DNS server, choose New Zone)
8. Enter the name of the child zone example: sub1.mylab.com

9. Click Next, click Finish
10. Make sure the zone allow dynamic updates
11. Promote child DNS Server to Domain Controller (start > Run, type “dcpromo”)



How manage Server 2008 DNS from command line using dnscmd.exe

Dnscmd.exe can be found in Support\Tools directory on the Windows Server 2008 CD. You can copy dnscmd from support.cab to any location you wish.

Add a new standard zone called infotechguyz.com
dnscmd dc01.infotechguyz.local /ZoneAdd infotechguyz.com /Primary /file infotechguyz.com.dns

Create a new A record for Server name EX01 with an IP of 10.1.0.50
Dnscmd dc01.infotechguyz.local /RecordAdd infotechguyz.com EX01 A 10.1.0.50

Enumerate all zones
Dnscmd dc01.infotechguyz.local /enumzones

Clear the Cache on the server
Dnscmd dc01.infotechguyz.local /clearcache

Restart DNS service
Dnscmd dc01.infotechguyz.local /restart

How to enable GlobalNames Zones on Server 2008 DNS Server

Run “dnscmd <ServerName> /config /Enableglobalnamessupport 1”

How to create GlobalNames Zone

1. Open DNS Manager from Administrative Tools.
2. expend the DNS server, right-click “Forward Lookup Zones”, and choose “New Zone”
3. Click Next
4. Choose “Primary zone” (Store zone in Active Directory), click Next
5. Choose the Active Directory Zone Replication Scope. Click Next
6. On Zone Name, screen, enter “GlobalNames”, click Next
7. On Dynamic Update screen, choose “Do not allow dynamic updates”, click Next
8. Click Finish

How To Set Active Directory Verbose Logging

Often times you may want to turn on Active Directory Verbose logging to troubleshoot Active Directory (AD) related issues. By default, Active Directory only logs critical and error events.

You must configure following registry key to set Active Directory Verbose logging

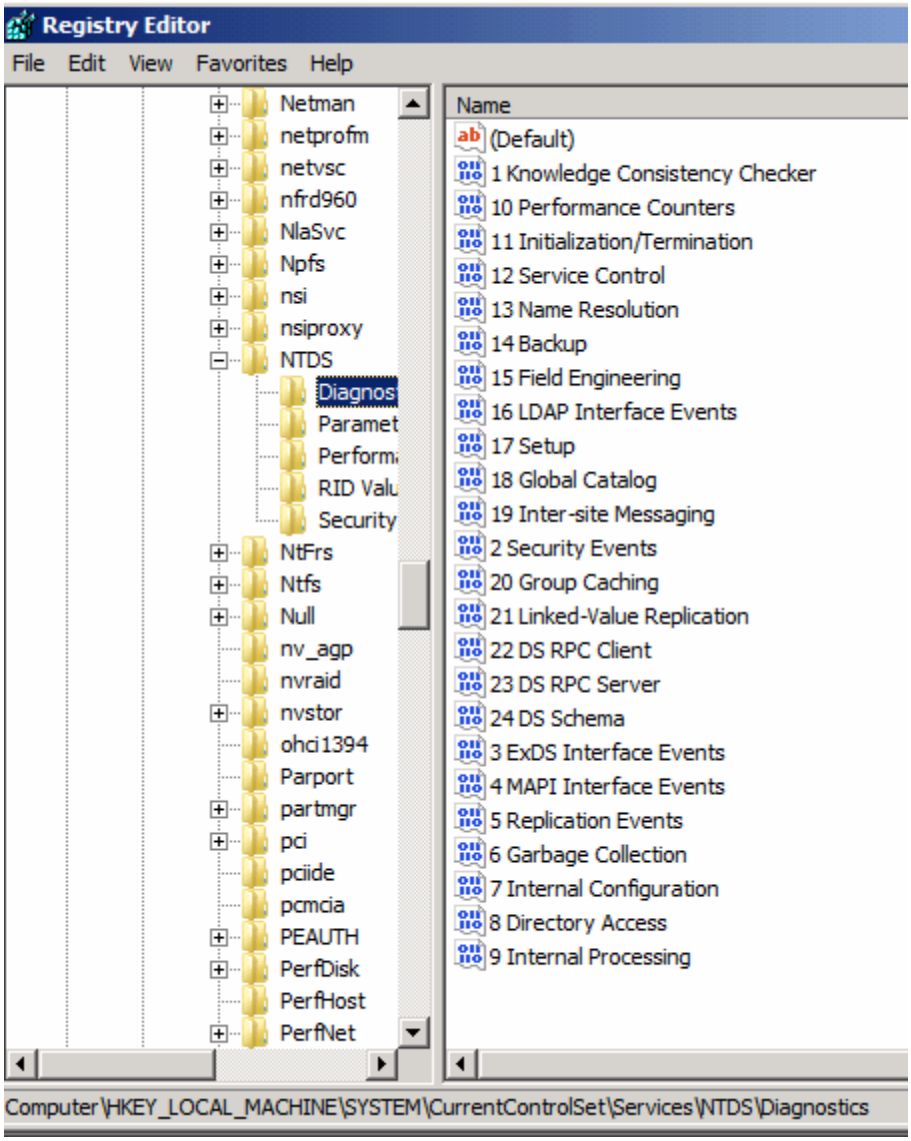
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

Events that can be set:

Knowledge Consistency Checker (KCC)
Security Events
ExDS Interface Events
MAPI Interface Events
Replication Events
Garbage Collection
Internal Configuration
Directory Access
Internal Processing
Performance Counters
Initialization/Termination
Service Control
Name Resolution
Backup
Field Engineering
LDAP Interface Events
Setup
Global Catalog
Inter-site Messaging
Group Caching
Linked-Value Replication
DS RPC Client
DS RPC Server
DS Schema

Logging Levels (from Microsoft Support):

- 0 (None): Only critical events and error events are logged at this level. This is the default setting for all entries, and it should be modified only if a problem occurs that you want to investigate.
- 1 (Minimal): Very high-level events are recorded in the event log at this setting. Events may include one message for each major task that is performed by the service. Use this setting to start an investigation when you do not know the location of the problem.
- 2 (Basic)
- 3 (Extensive): This level records more detailed information than the lower levels, such as steps that are performed to complete a task. Use this setting when you have narrowed the problem to a service or a group of categories.
- 4 (Verbose)
- 5 (Internal:): This level logs all events, including debug strings and configuration changes. A complete log of the service is recorded. Use this setting when you have traced the problem to a particular category of a small set of categories.



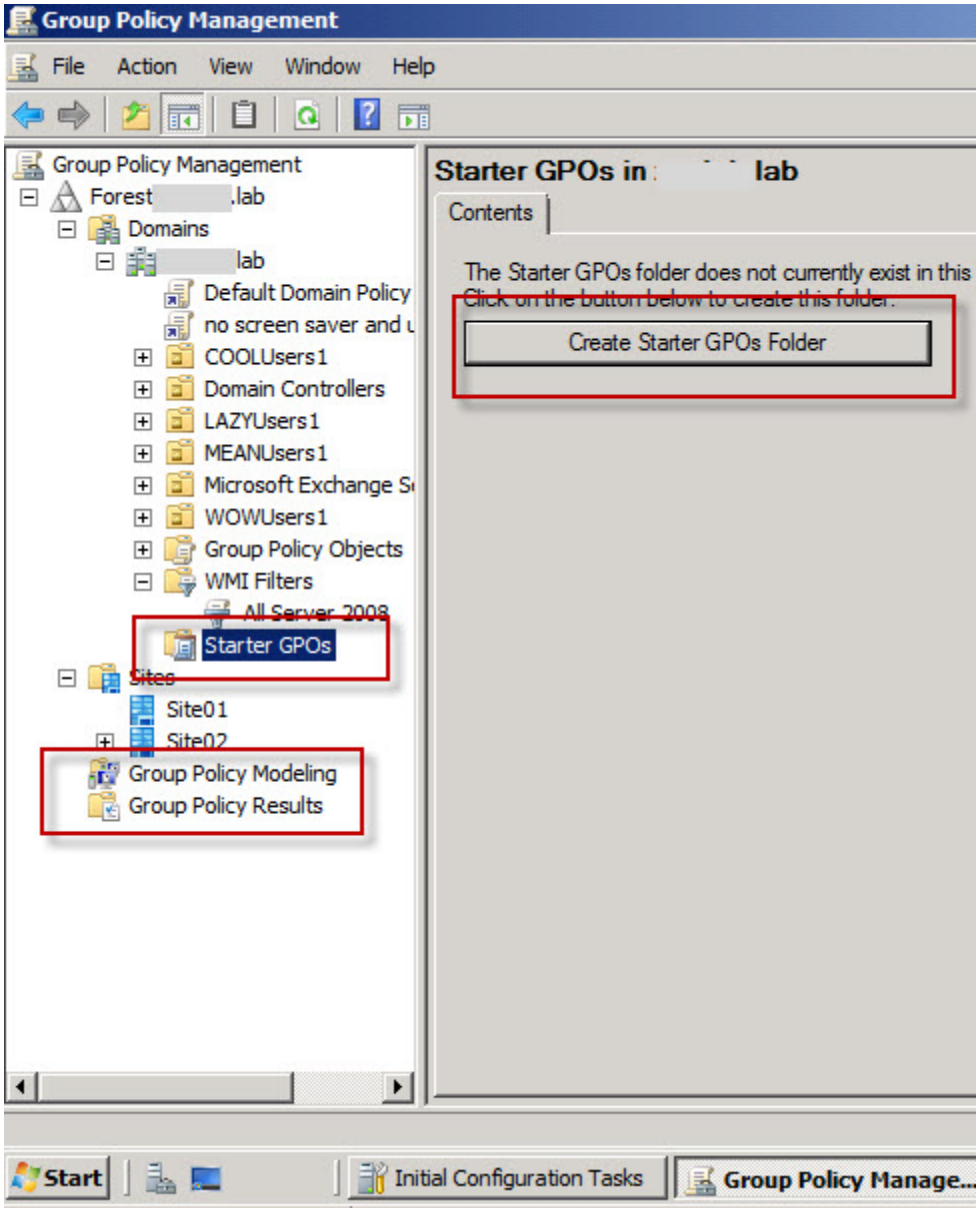
Group Policy

New Group Policy features in Server 2008

New Server 2008 Group Policy Management Console (GMPC) has new features below:

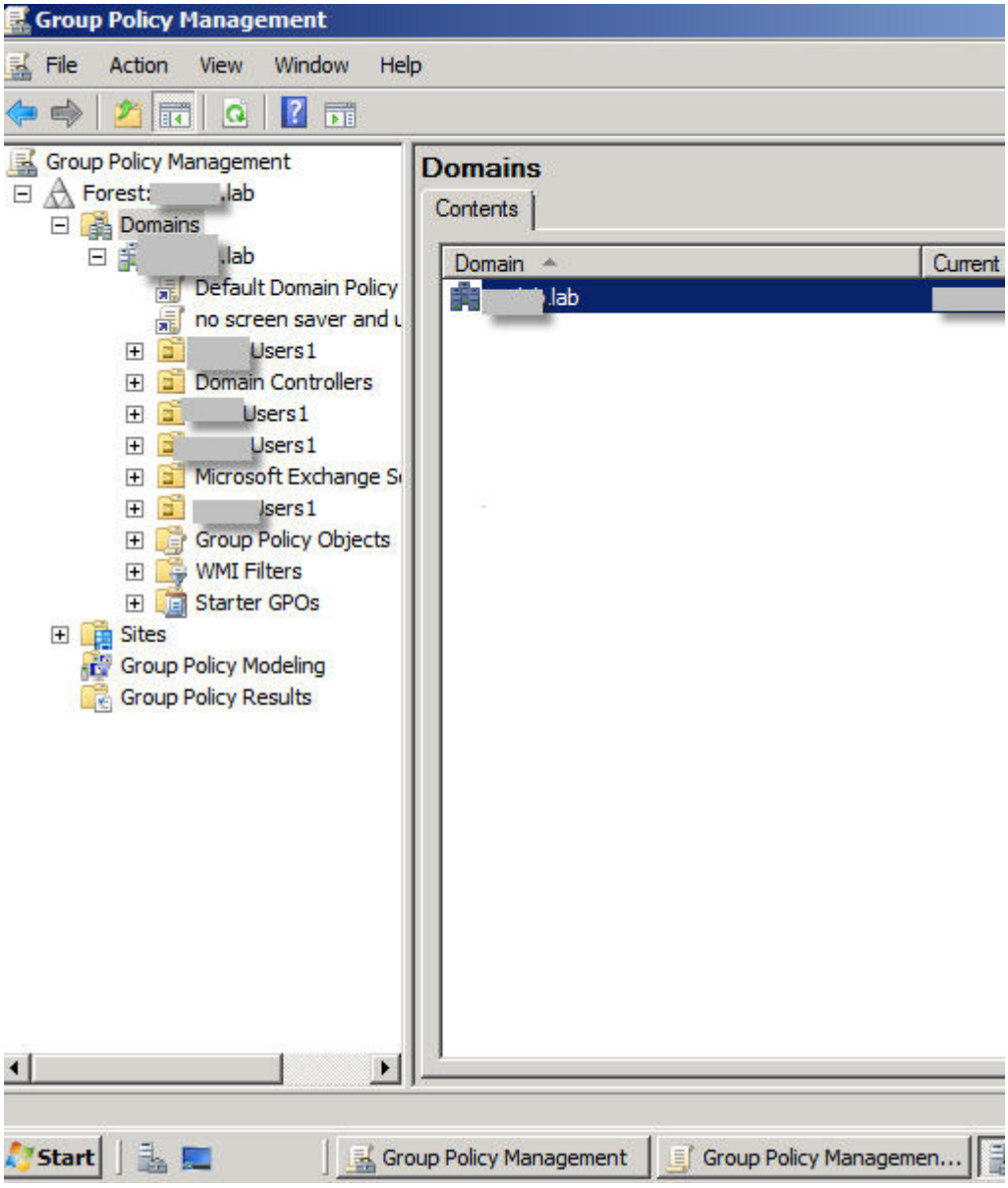
1. Create new starter GPOs
2. Backup and restore start GPOs in a domain
3. Manage GPO link enforcement
4. Manage GPO processing order
5. Resultant Set of Policy tool for planning operations

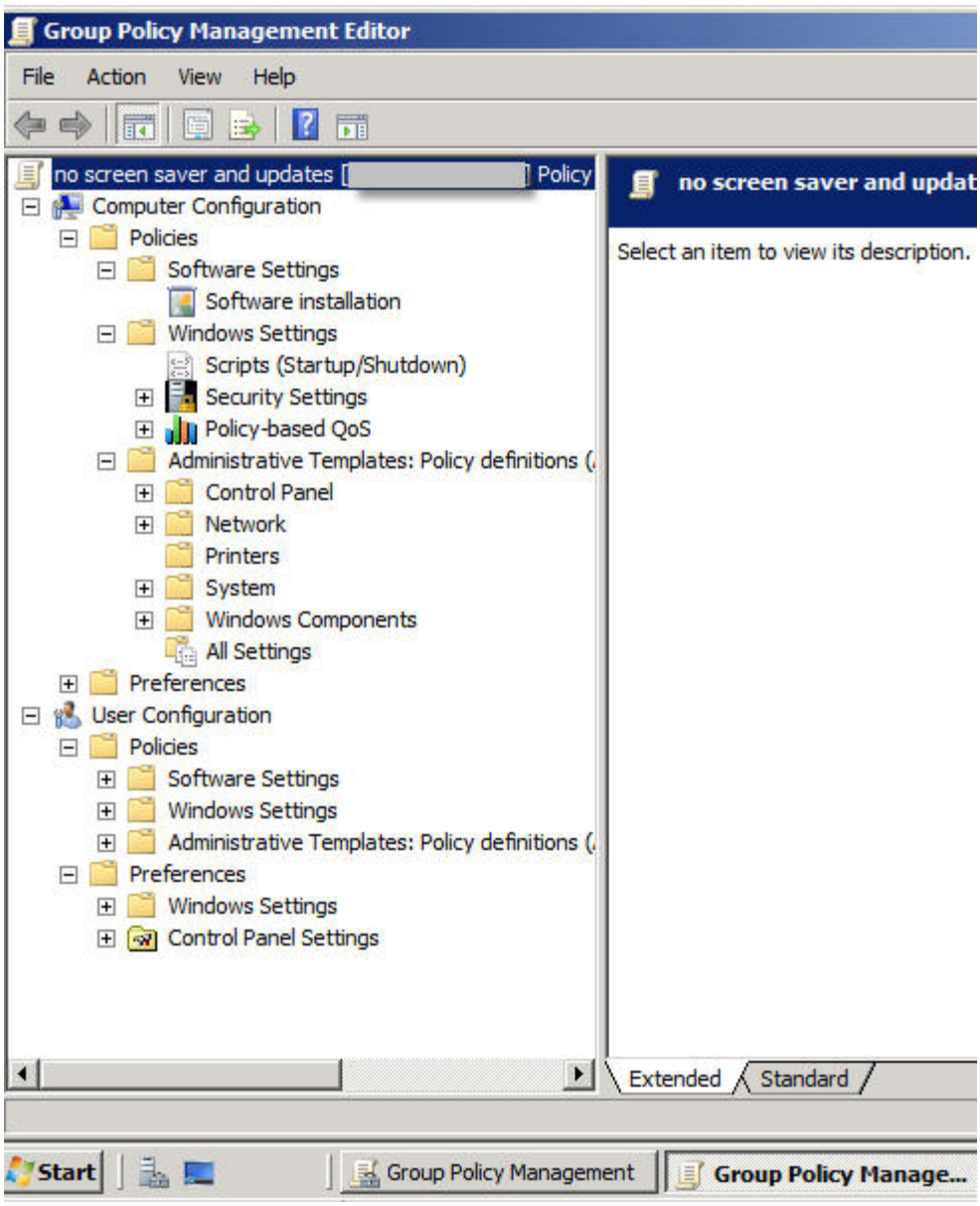
In depth explanation of Server 2008 Group Policy can be found here.



Server 2008 Group Policy Explained

Windows Server 2008 Active Directory allows implementation of Group Policy for centralized management of Users and Computer Settings. Group Policy is a method used to centrally configure and deploy a common set of computer and user settings, security settings, and, deploy software to Windows servers, Windows Clients and users in an Active Directory domain. A single Group Policy is used to configure settings on specified collection of computers, users, groups, site, organizational unit or domain. For example, you can use Group Policy to configure Automatic Updates on collection computer in specific Organizational Unit.

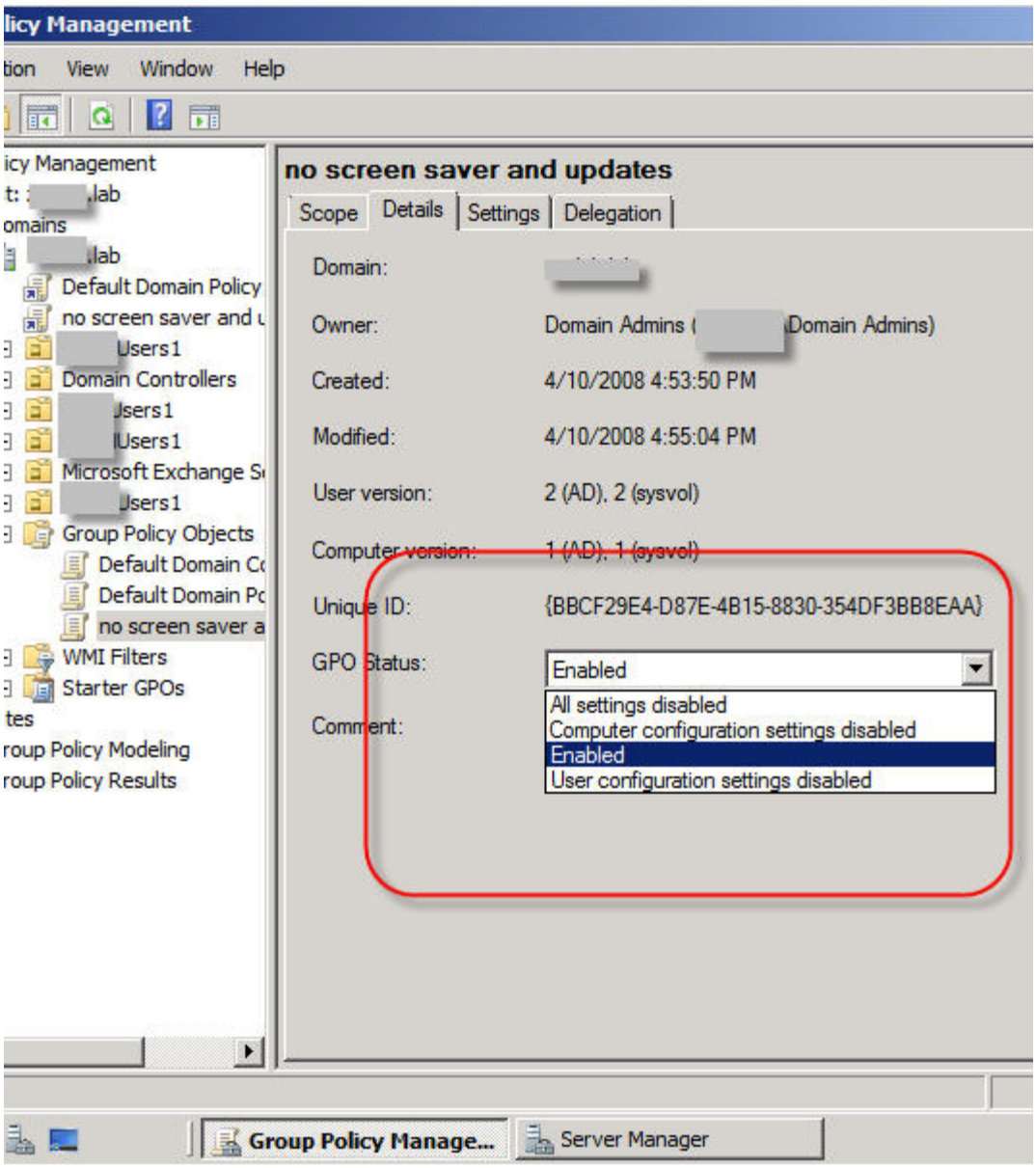

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: .lab
Domains
.lab
Default Domain Policy
no screen saver and u
Users1
Domain Controllers
Users1
Users1
Microsoft Exchange S
sers1
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Domains
Contents
Domain
Current
.lab
Start
Group Policy Management
Group Policy Managemen...

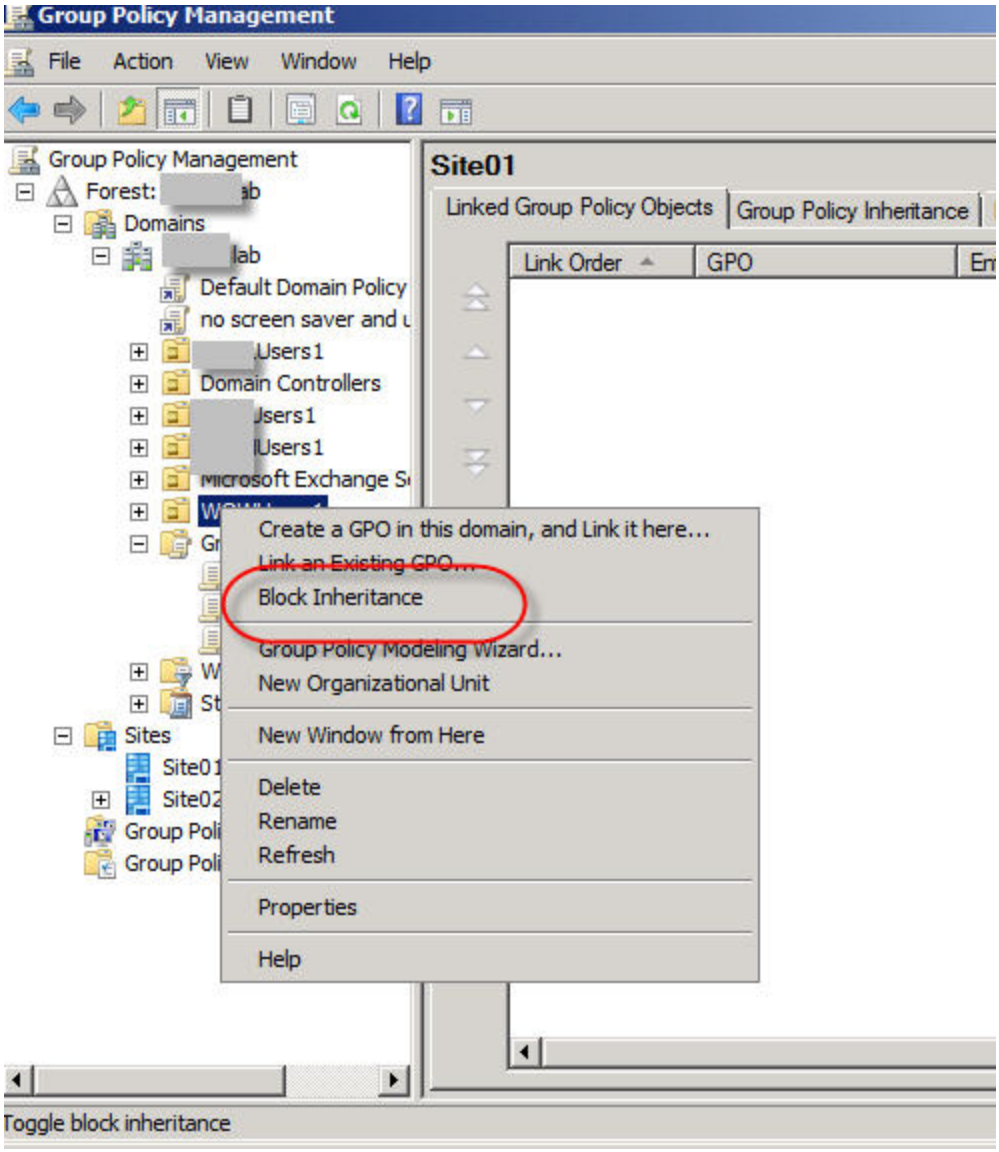


Optimizing Group Policy Performance

A few things that can improve Group Policy processing

1. Disable used policy settings (either user or computer), see screenshot below.
2. Consolidate multiple Group Polices to increase faster processing.
3. Block unneeded Group Policies at OU, Site or Domain level using “Block Policy Inheritance” setting.


licy Management
tion View Window Help
icy Management
t: lab
omains
lab
Default Domain Policy
no screen saver and u
Users1
Domain Controllers
Users1
Users1
Microsoft Exchange S
Users1
Group Policy Objects
Default Domain Co
Default Domain Po
no screen saver a
WMI Filters
Starter GPOs
tes
roup Policy Modeling
roup Policy Results
no screen saver and updates
Scope Details Settings Delegation
Domain:
Owner: Domain Admins (Domain Admins)
Created: 4/10/2008 4:53:50 PM
Modified: 4/10/2008 4:55:04 PM
User version: 2 (AD), 2 (sysvol)
Computer version: 1 (AD), 1 (sysvol)
Unique ID: {BBCF29E4-D87E-4B15-8830-354DF3BB8EAA}
GPO Status: Enabled
Comment:
All settings disabled
Computer configuration settings disabled
Enabled
User configuration settings disabled
Group Policy Manage...
Server Manager



Server 2008 Group Policy in depth

Basic explanation of Group Policy can be found here.

Group Policies are applied to computer / users objects during startup, shutdown and according to refresh interval—90 minutes by default. Gpupdate.exe command-line utility can be used to refresh Group Policy manually. Every GPO—Group Policy Object include a revision number, GPO processing is skipped if it hasn't changed since last application. This rule doesn't apply to login and logoff scripts within GPO since they need to be applied regardless.

GPO Processing of computer configuration
GPO is applied to a computer during startup, shutdown and according to refresh interval—90

minutes by default on members servers and 5 minutes on domain controllers. GPO is processed during startup by contacting the domain controller. GPO Processing of computer configuration can be qualified by OU—Organization Unit, security filtering—Security groups and WMI Filters – hardware or software configuration. WMI filters are advanced concept but very powerful. For example, you can apply a particular GPO to all computers in the domain that runs Server 2008 version 6.0.6001. WMI filter would be something like "select * from win32_operatingsystem where version=' 6.0.6001'"

See Screenshot

GPO Processing of user configuration
GPO Processing of user configuration is very simlar to computer processing. GPO is applied to a user during logon/logoff instead of startup, shutdown. GPO Processing of user configuration can be qualified by OU—Organization Unit and security filtering—Security groups.

See Screenshot

Local Computer Policy *vs* Active Directory Group Policy
Local Computer Policy can be found of most Windows systems. You can run gpedit.msc to open Local Computer Policy. Local Computer Policy allows configuration that is usually cannot be configured by control panel or commandline. Windows Server 2008 and Windows Vista now allow multiple local polices.

See Screenshot #3

Active Directory Group Policy is applied when a computer is joined to Active Directory domain. This allows centralized management of Group Policy settings by administrator.

Server 2008 Group Policy Components:

GPO -- Group Policy Objects
Group Policy Object refers to a file/object that defines set of user configuration and computer configuration. Group Policy Management Console is used to edit Group Policy Object to define user and computer configuration.

ADM folder
This folder only exist when older GPOs are imported from administrative temples. This includes GPOs created by Windows XP, Server 2003, etc.

Group Policy Object, User folder
The user folder in Group Policy Object contains settings, msi installers, scripts and any settings that relates to the user configuration of the object.

Group Policy Object, Machine folder
The machine folder in Group Policy Object contains settings, msi installers, scripts and any settings that relates to the machine configuration of the object.

Registry.pol Files
Most settings within the GPO is configured by using registry keys. These registry keys and values are stored within registry.pol files which can exist in both user and machine folders.

Gpt.ini File
This file can be found at the root of GPO folder in SYSVOL share. This contains the revision number which tracks the changes made to the GPO. As mention above, the revision number is used to save processing time by the client.

SYSVOL, FRS and DFSR
Active Directory stores GPO information in domain naming context partition of the NTDS database. The GPO settings are located in SYSVOL folder share of all domain controllers. The specific location is SYSVOL\yourdomain.net\Polices folder, which you will also find the GUID of the GPO. Windows Server 2003 uses FRS—File Replication Service to replicate the SYSVOL folder but Server 2008 uses DFSR—Distributed File System Replication for better efficiency. By default, intra-site replication occurs every 5 minutes between domain controllers and inter-site replication depends on your Active Directory Site link settings.

See Screenshot (screenshot of sysvol)

Group Policy Administrative Templates
Administrative Templates are a set of settings often used by administrators. This file can be a set of text or XML based files.

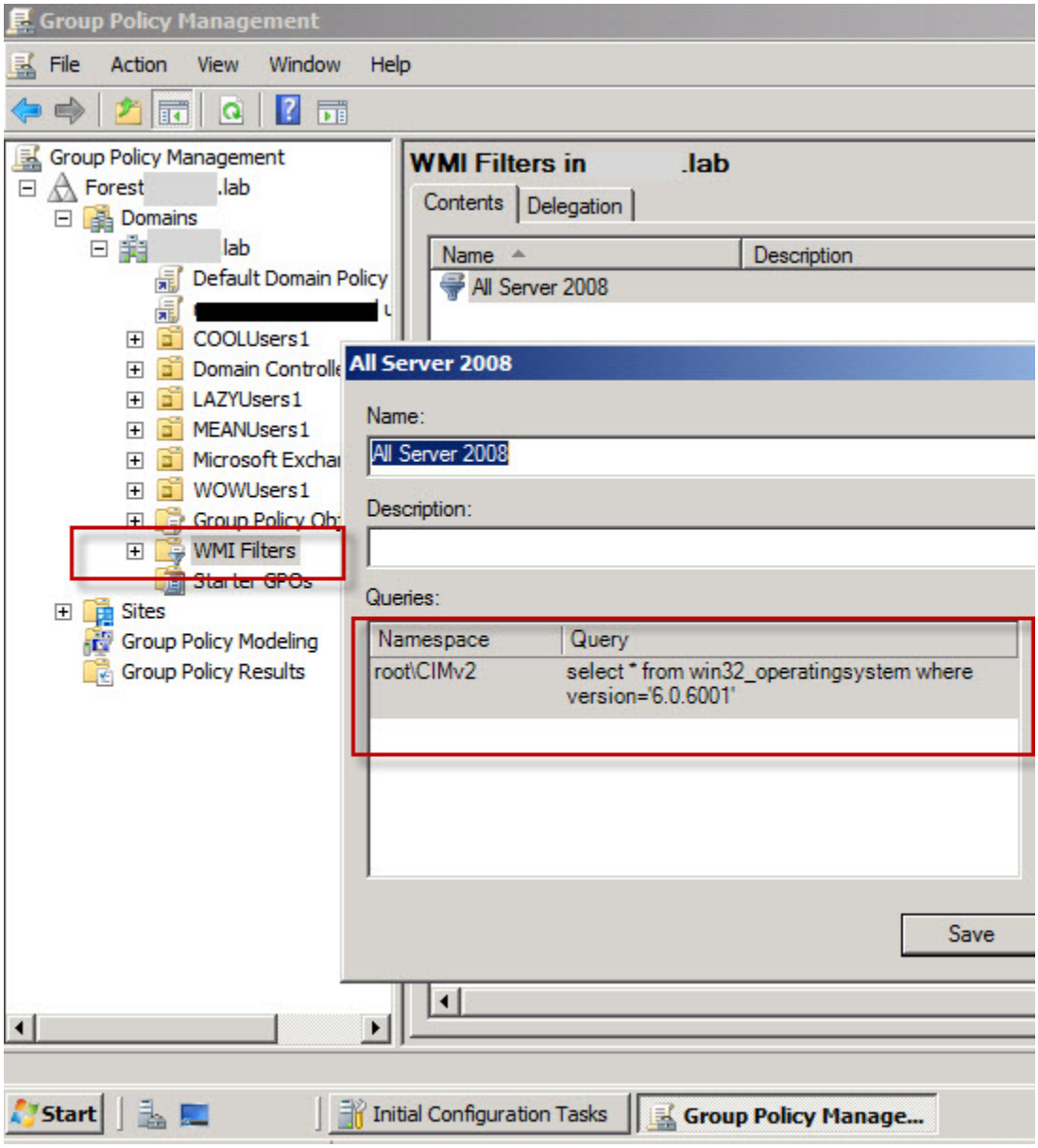
Server 2008 Central Store
This is the centralized store of administrative templates which is part of Server 2008 Group Policy infrastructure. Administrator can create GPO Central Store in SYSVOL folder to store ADMX and ADML administrative templates.

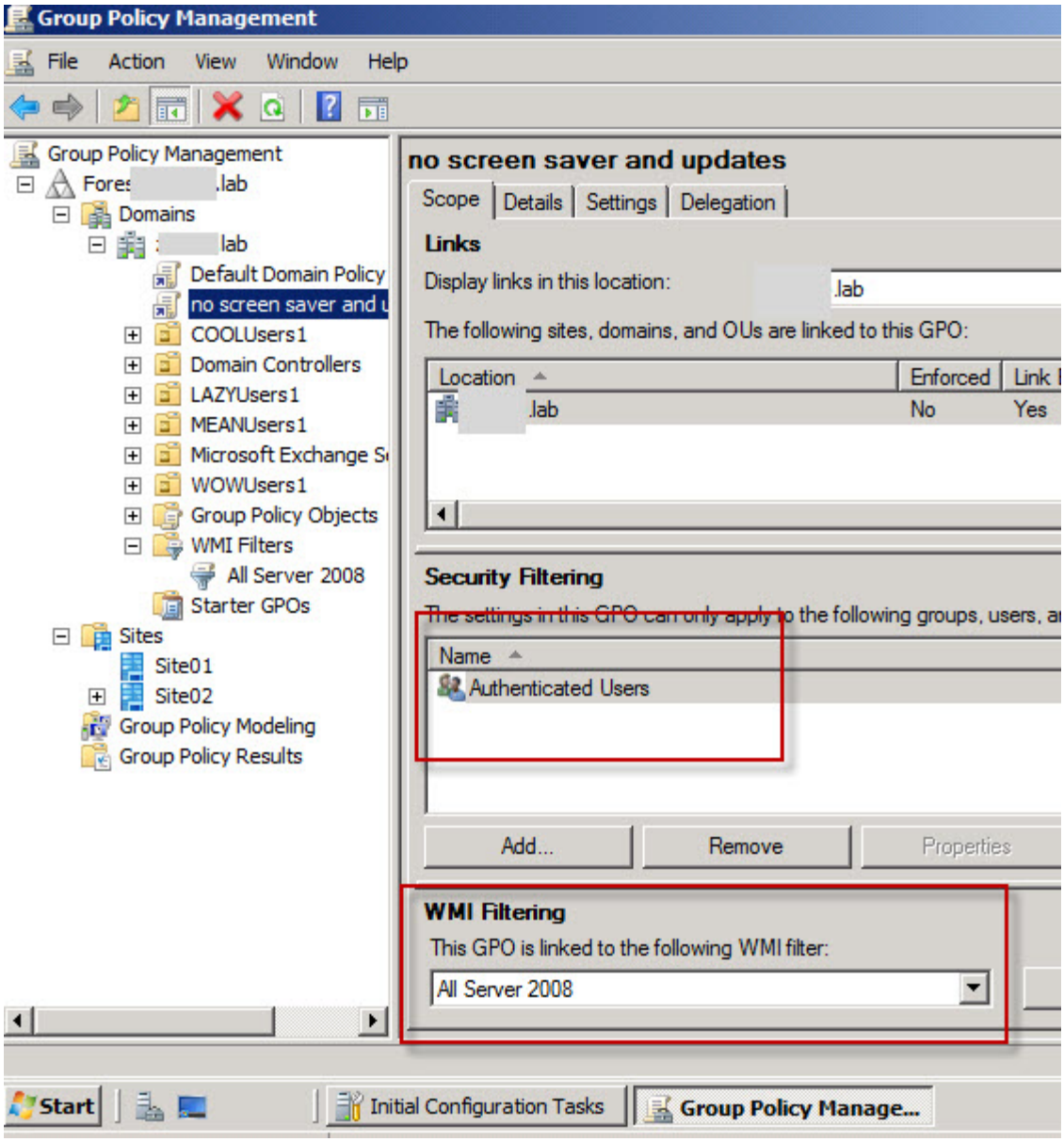
Starter GPOs
Start GPO allows storage of policy settings into a single object so it can be restored into new GPOs. This eliminates re-configuration of common settings when creating new GPOs. This also allows importing and exporting of GPOs between Active Directory forests.

Group Policy Link Enforcement
Group Policy Link Enforcement is a way to enforce a GPO even when Group Policy inheritance is blocked.

Group Policy Loopback Processing

Group Policy Loopback allows processing of both the Computer Configuration and User Configuration nodes within a policy only if one object is within linked containers.





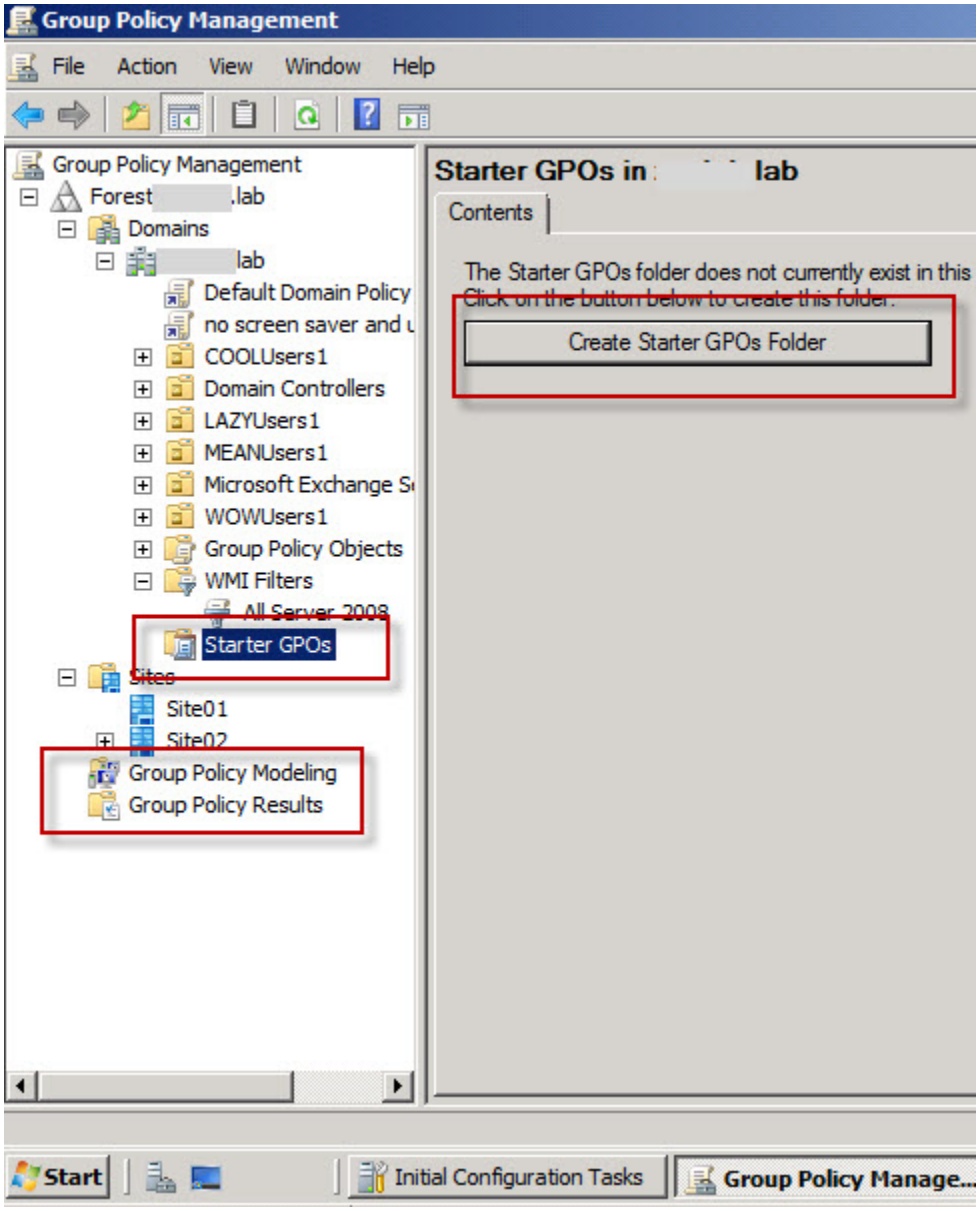
Starter GPO (Group Policy Object)

Server 2008 Group Policy Management Console allows creation of Starter GPO. It can be used to preload / prepopulate GPO settings into a GPO as a baseline.

Create a Starter GPO

1. Open Group Policy Management Console on Server 2008
2. Under domain, select the Starter GPO container
3. Click “Create Start GPOs Folder” on the right pane
4. Right click on the Starter GPO container and choose New

5. Right click the GPO, choose Edit to open the GPO in the Group Policy Starter GPO Editor.
6. Once configured, close the Group Policy Starter GPO Editor.
7. To backup the starter GPO, right click the recently created starter GPO and choose Backup.



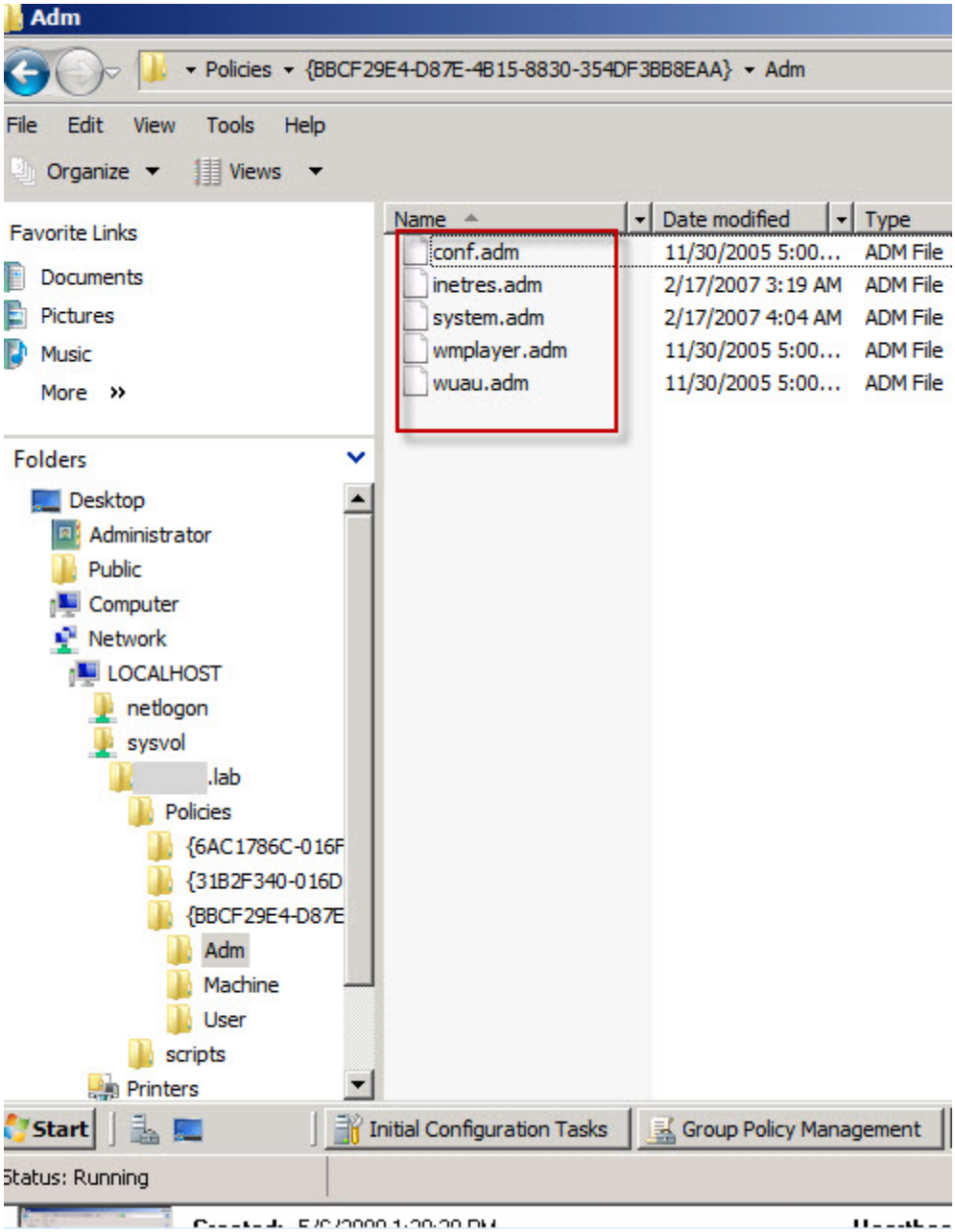
Server 2008 Group Policy Administrative Templates Explained

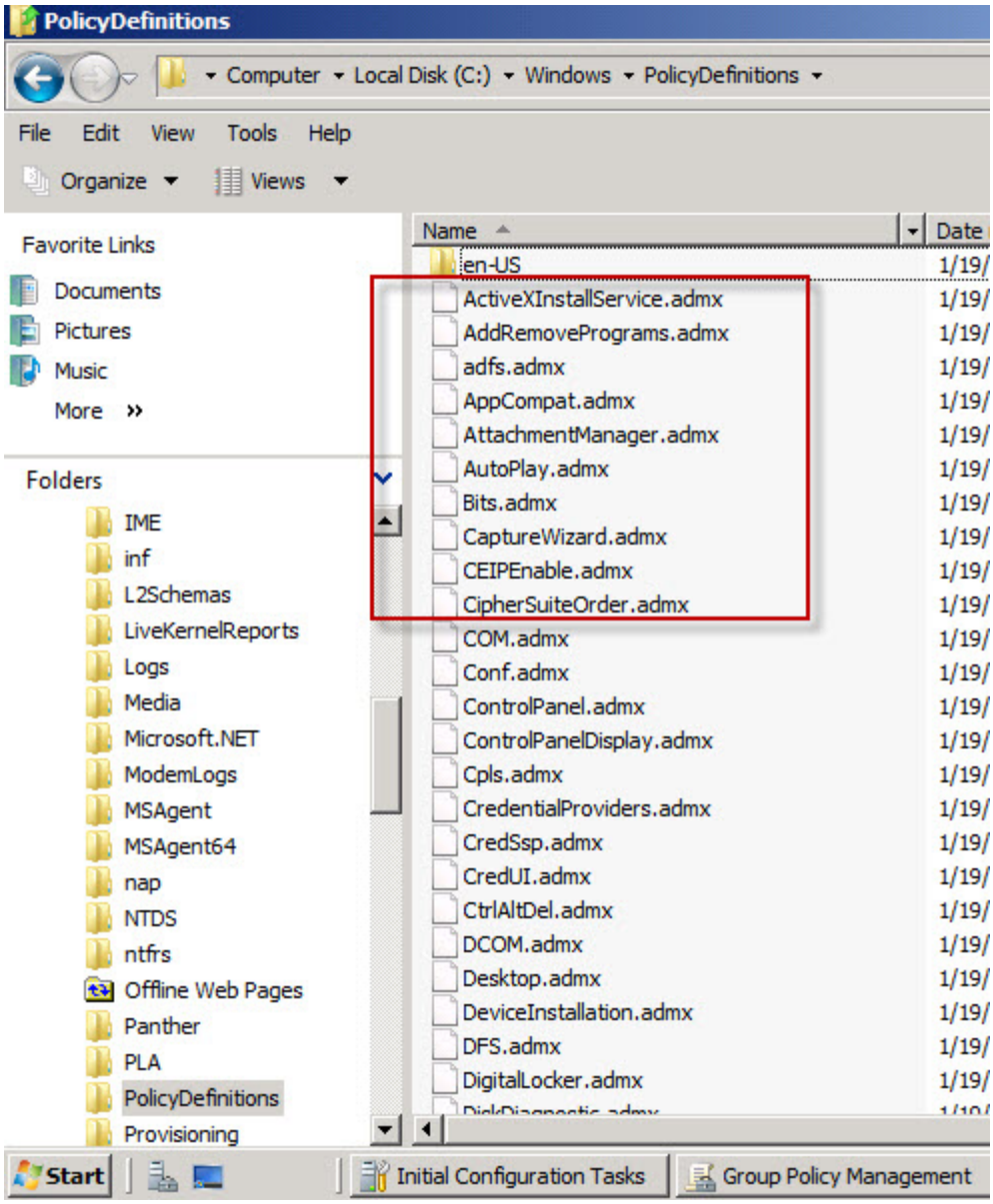
Group Policy administrative template contains collection of settings / registry keys for user configuration or computer configuration. ADM files are used in Server 2000 / 2003 environment. Server 2008 and Windows Vista use ADMX and ADML files.

When GPO is created by Server 2003 Windows XP tools, it creates set of ADM files in the SYSVOL GPO folder. In Server 2003, each GPO has copy of the same common template files within each GPO folder. If existing GPO is opened for viewing or editing, ADM files are compared and newer version is copied to SYSVOL GPO folder. As you may have guessed, this can cause a lot of problems in large Active Directory environments. For example, if an administrator using Windows XP SP2 view the GPO that was created using Windows XP SP1, ADM template will automatically get updated. Then the domain controller would replicate the changes to all domain controllers. This feature can be turned off by configuring the domain GPO, under *User Configuration\Policies\Administrative\Templates\System\Group Policy*

A lot of changes are made to Group Policy in Server 2008 and Windows Vista. The ADM files are not split into two files—ADMX administrative template settings file and ADML administrative template language file. GPO created by Server 2008 or Windows Vista Group Policy Management tool creates ADMX file and not the administrative template files as in Server 2003. This reduces the size of SYSVOL folder and save replication bandwidth. So when a GPO is created by the Windows Vista Group Policy Management Console, GPO folder makes use of the ADMX/ADML files. When a GPO is created by Windows XP and Windows Server 2003 Group Policy tools, it copies the ADM files to SYSVOL GPO folder.

Screenshot of ADM files
Screenshot ADMX files


Adm
Policies
{BBCF29E4-D87E-4B15-8830-354DF3BB8EAA}
Adm
File
Edit
View
Tools
Help
Organize
Views
Favorite Links
Documents
Pictures
Music
More
Name
Date modified
Type
conf.adm
11/30/2005 5:00...
ADM File
inetres.adm
2/17/2007 3:19 AM
ADM File
system.adm
2/17/2007 4:04 AM
ADM File
wmplayer.adm
11/30/2005 5:00...
ADM File
wuau.adm
11/30/2005 5:00...
ADM File
Folders
Desktop
Administrator
Public
Computer
Network
LOCALHOST
netlogon
sysvol
.lab
Policies
{6AC1786C-016F
{31B2F340-016D
{BBCF29E4-D87E
Adm
Machine
User
scripts
Printers
Start
Initial Configuration Tasks
Group Policy Management
Status: Running



Group Policy Central Store

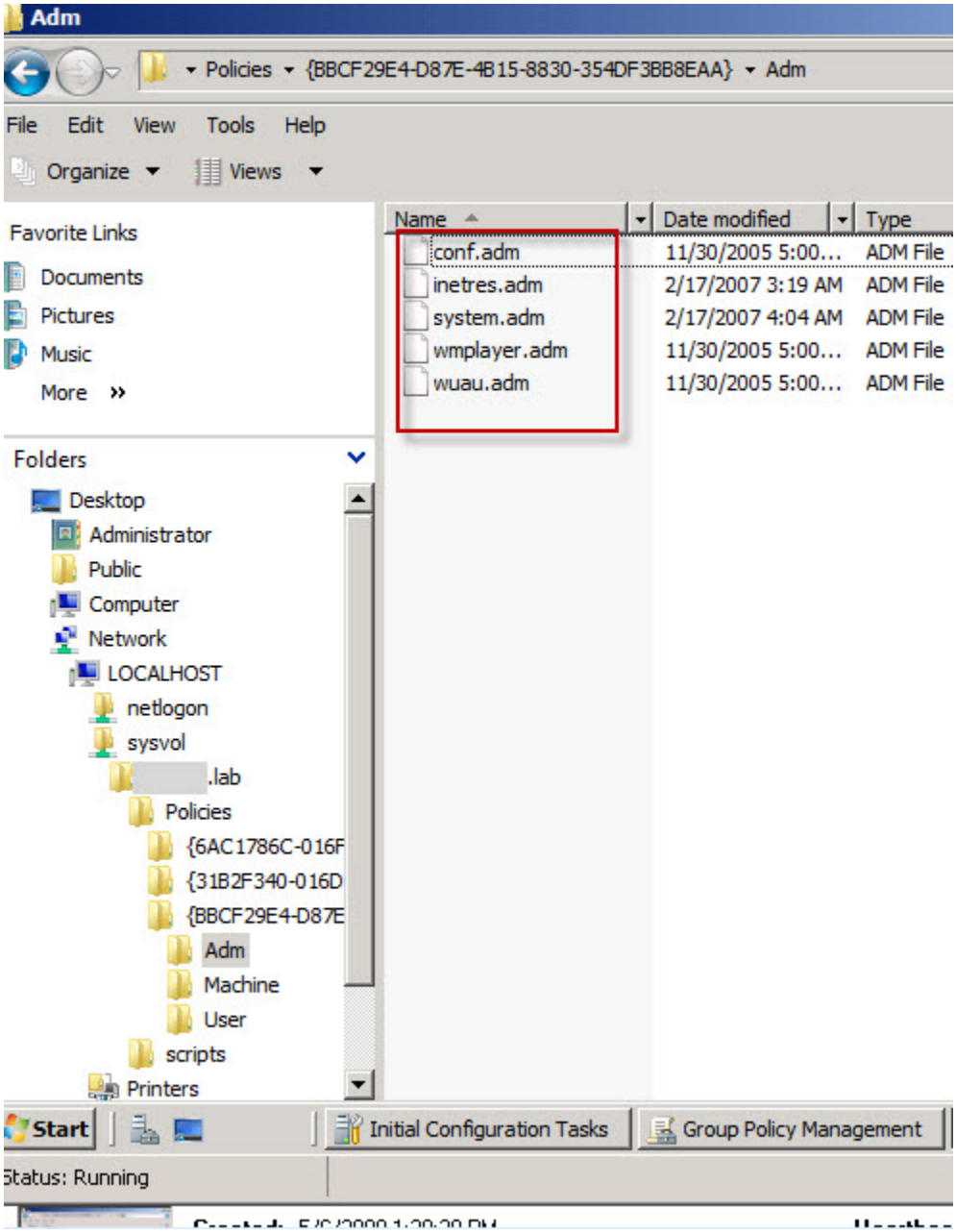
Group Policy Central Store contains all of the necessary ADMX and ADML files. Group Policy Central Store provides a simple and effective way to manage administrative templates from the SYSVOL folder. More information on Group Policy Central Store can be found here.

Create a Group Policy Central Store

1. Browse to C:\Windows\ folder on Server 2008.
2. Copy PolicyDefinitions folder from Server 2008.
3. Brose to your SYSVOL folder -- \\yourdomain.net\sysvol\yourdomain.net\policies.
4. Paste PolicyDefinitions folder from Server 2008 to SYSVOL folder.

Verify Group Policy Central Store

5. Open Group Policy Management Console on Server 2008.
6. Browse to Forest > Domains > Group Policy Objects , select a policy
7. On the right pane, click on “Settings” tab
8. Under Administrative Templates, it will tell you that Policy definitions (ADMX files) retrieved from the central store.



Server 2008 Group Policy: How to Design a Group Policy Infrastructure

Group Policy can be a great way to manage group of users and computers centrally from one console. This topic really comes down to two questions, what AD objects can I link group policy to? and how can I organize my resources—AD objects ?

What AD objects can I link group policy to?

Group Policy Object can be linked to

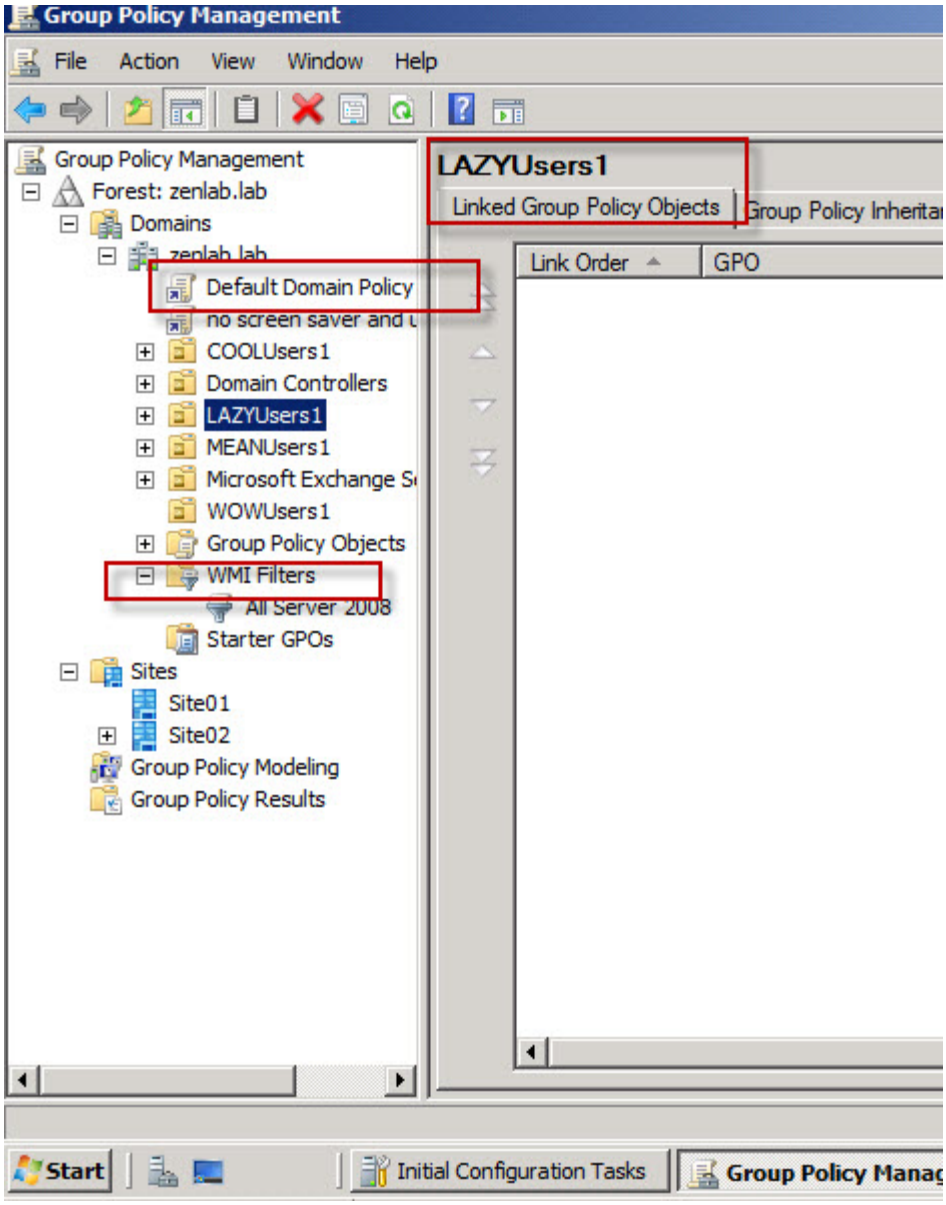
1. Active Directory domain
2. Active Directory Site
3. Active Directory Organizational Units
4. Active Directory Security Groups

Active Directory Domain
When a group policy is linked to a Domain, GPO is applied to every Active Directory objects within a domain. This is regardless of the Site or OU where user/computer object is located.

Active Directory Site
When a group policy is linked to a Site, the GPO is applied to every Active Directory objects within a Site. This is regardless of the domain or OU where user/computer object is located.

Active Directory Organizational Units
When a group policy is linked to an OU, the GPO is applied to every Active Directory objects within an OU. Administrators use OU to organize Active Directory objects usually by departments. This allows granular configuration of user and computers within a department.

Active Directory Security Groups
When a group policy is linked to a Security group, the GPO is applied to every Active Directory objects that is a member of a Security group. This is regardless of the Site, domain or OU where user/computer object is located.



How to assign a Group Policy to Users and Computers

Assign Group Policy to Active Directory Domain

1. Open Group Policy Management console on Server 2008
2. Right click on domain and choose “Create a GPO in this domain, and Link it here…” see screenshot here.

Assign Group Policy to Active Directory Site

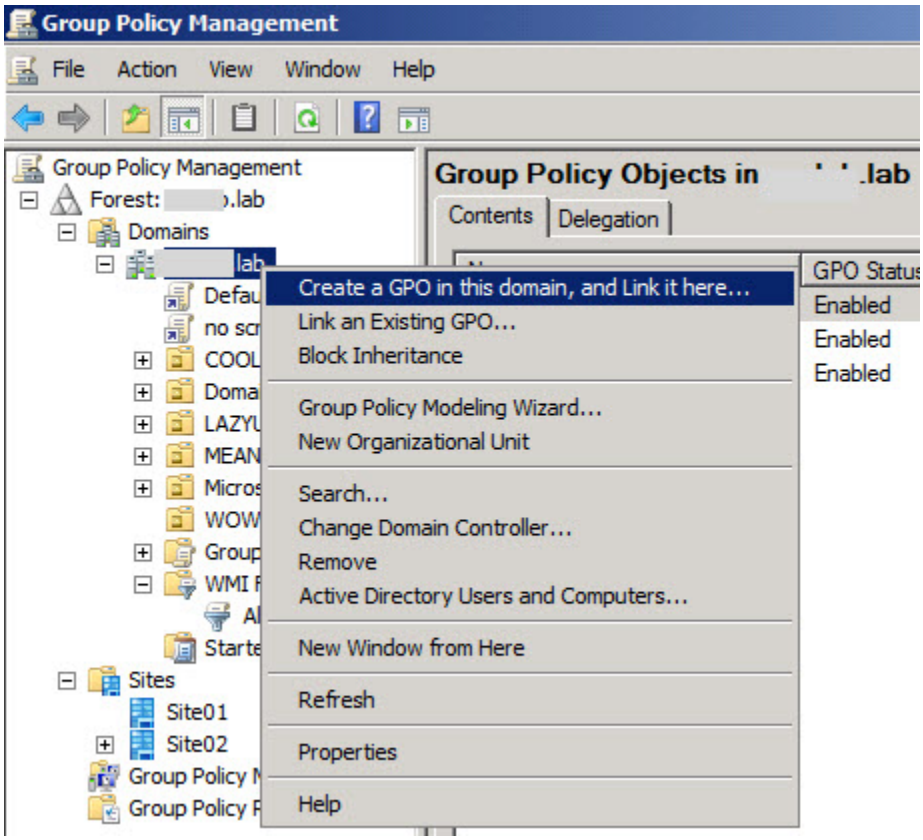
1. Open Group Policy Management console on Server 2008
2. Right click on the Site and choose “Link an Existing GPO…”

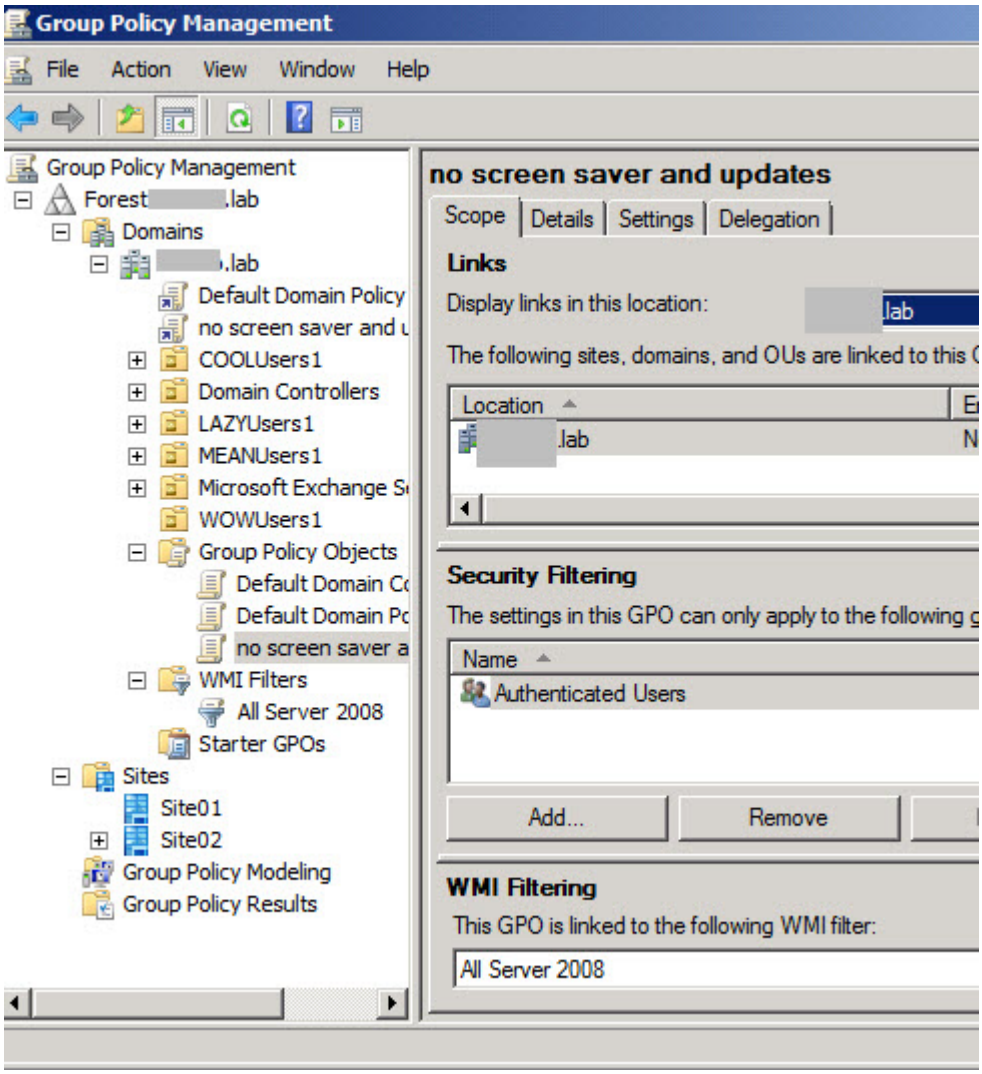
Assign Group Policy to Active Directory Organizational Units

1. Open Group Policy Management console on Server 2008
2. Right click on Organizational Unit and choose “Create a GPO in this domain, and Link it here…”

Assign Group Policy to Active Directory Security Groups

1. Open Group Policy Management console on Server 2008
2. Choose a Group Policy Object under “Group Policy Objects”
3. Under Security Filtering, Choose the group you want Group Policy to apply to. See screenshot here.

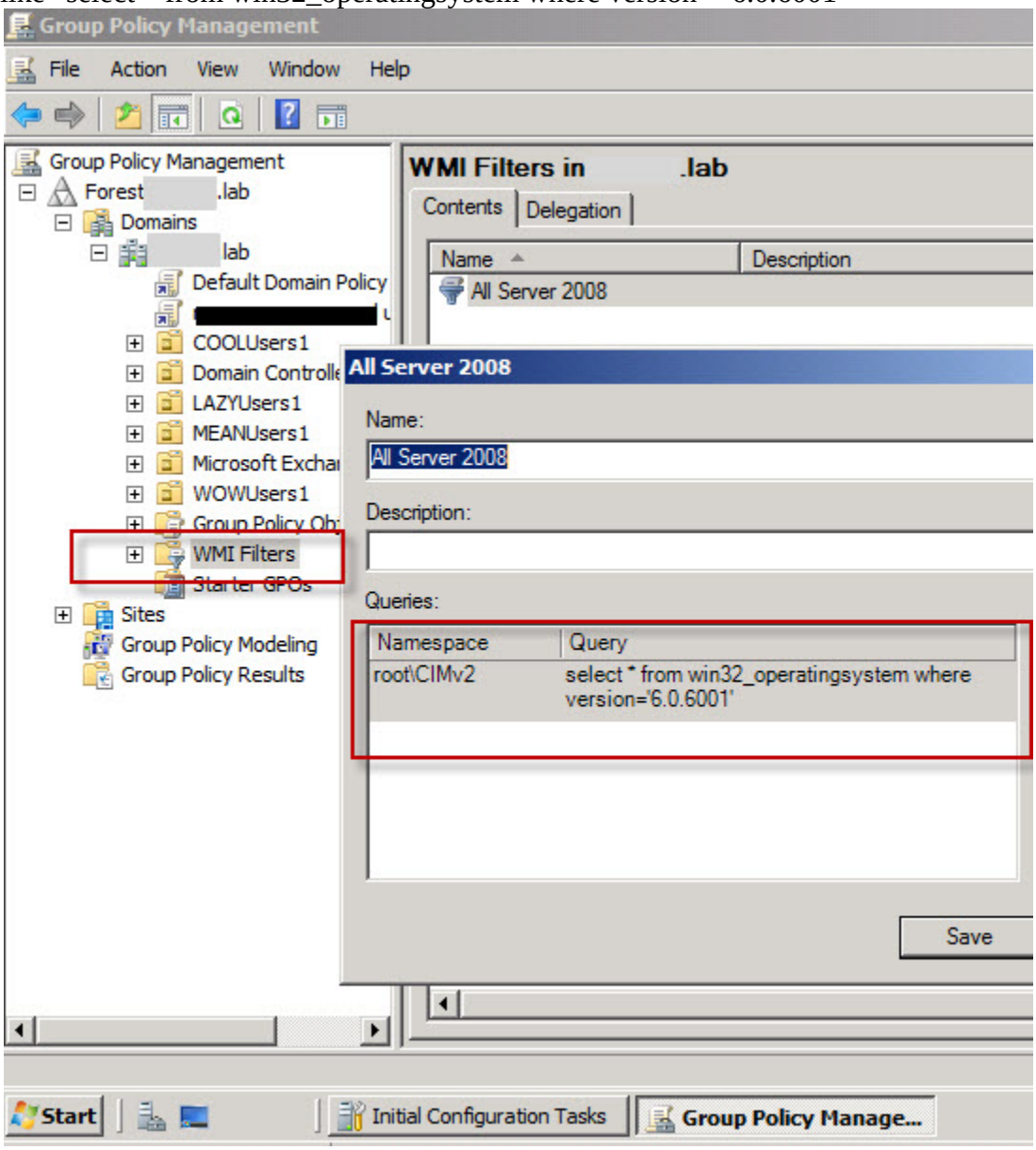




How to assign a Group Policy to Computers using WMI

Most advanced way to apply Group Policy is to use WMI filtering. This allows administrators to define set of computers using WMI query. For example, you can apply a particular GPO to all computers in the domain that runs Server 2008 version 6.0.6001. WMI filter would be something

like “select * from win32_operatingsystem where version=’ 6.0.6001'



How to block / restrict software access using Group Policy

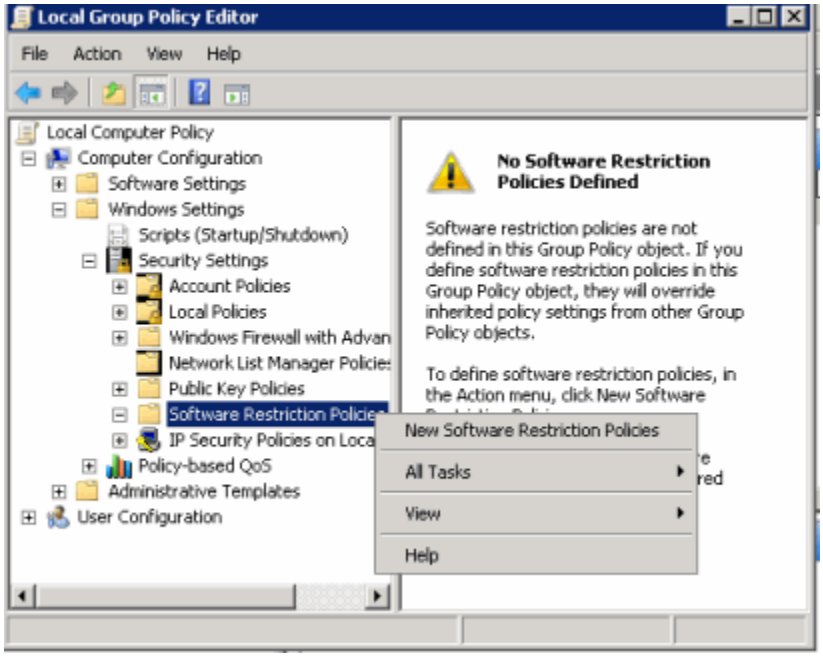
This article describes how to restrict software access from end users using Group Policy. IT administrators may prevent users from accessing certain software due to security reasons or business requirement. This requirement can be easily achieved by using Group Policy in Active Directory environment. Software Restriction Policy Group Policy setting can prevent end users from accessing certain software.

How to create Software Restriction Policy

1. Open Group Policy Management Console on Server 2008

2. Create a new GPO
3. Browse to:
   Computer Configuration > Windows Settings > Security Settings > Software Restrictions Polices

This policy allows IT administrators to enforce software policies and increase end users' productivity.



Publish Printers in Active Directory

Deploying printers to end users can be one of the most challenging tasks. This task is performed manually most of the time. IT Administrators may use logon scripts to deploy printers but it can be very time consuming also. Windows Server 2008 includes Print Management Console which allows simple management of Printers.

Deploy Printer Using Print Management Console

1. Open Print Management Console from Administrative Tools (Print Management Console is included in Server 2003 R2 and Server 2008)
2. Expand "Print Servers" to view print server within domain. (you can add new printers by right clicking on "Print Server' and choose "Add Servers")
3. Expand the printers and select the printers.
4. In Printers pane, right click on the Printer you want to deploy, select "Deploy with Group Policy"
5. Select the Group Policy Object this printer will be attached to, using the "Browse" button.
6. Check the appropriate check under "Deploy this printer connection to the following:"
7. Click OK to save changes

Use pushprinterconnections.exe to Push the Printers

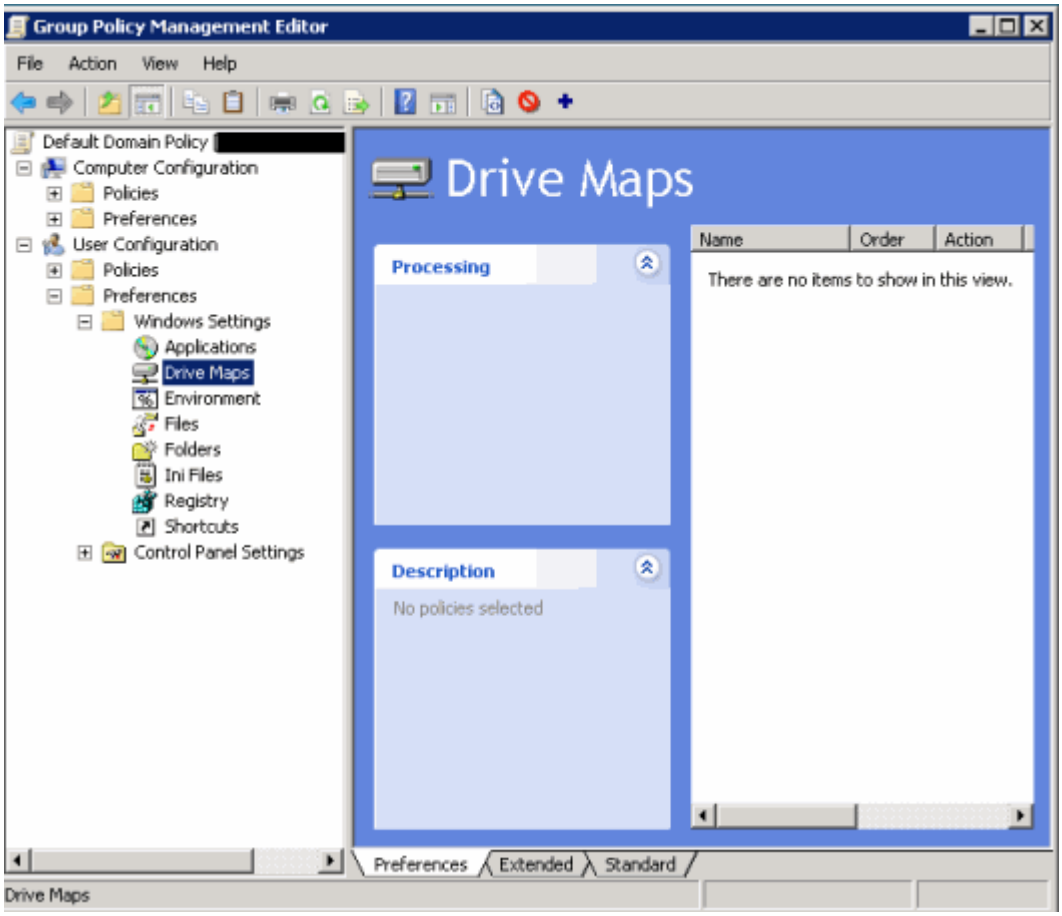
8. Browse to the c:\Windows\System32 folder.
9. Copy pushprinterconnections.exe to the domain Netlogon share -- \\mycompany.com\Netlogon.
10. Open the Printer GPO using Group Policy Object Editor
11. if printers are deployed per-machine, go to **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**
    if printers are deployed per-user, go to **User Configuration** > **Windows Settings** > **Scripts (Logon/Logoff)**
12. In **Logon Properties** or **Startup Properties** , add **PushPrinterConnections.exe** in the "Script Name" field

How to deploy drive mapping in Active Directory environment

Server 2008 introduces new feature Preferences Drive Maps extension in domain group policies. It allows IT administrators to map network drives for end users without writing scripts.

Map Drives Using User Drive Maps Preferences Extension

1. Open Group Policy Management Console on Server 2008
2. Create a new GPO, name "Userdrives"
3. Edit the new GPO, browse to User Configuration > Preferences > Windows Settings > select Drive Maps. Right click the setting, choose New – Mapped Drive.
4. Follow on screen instructions



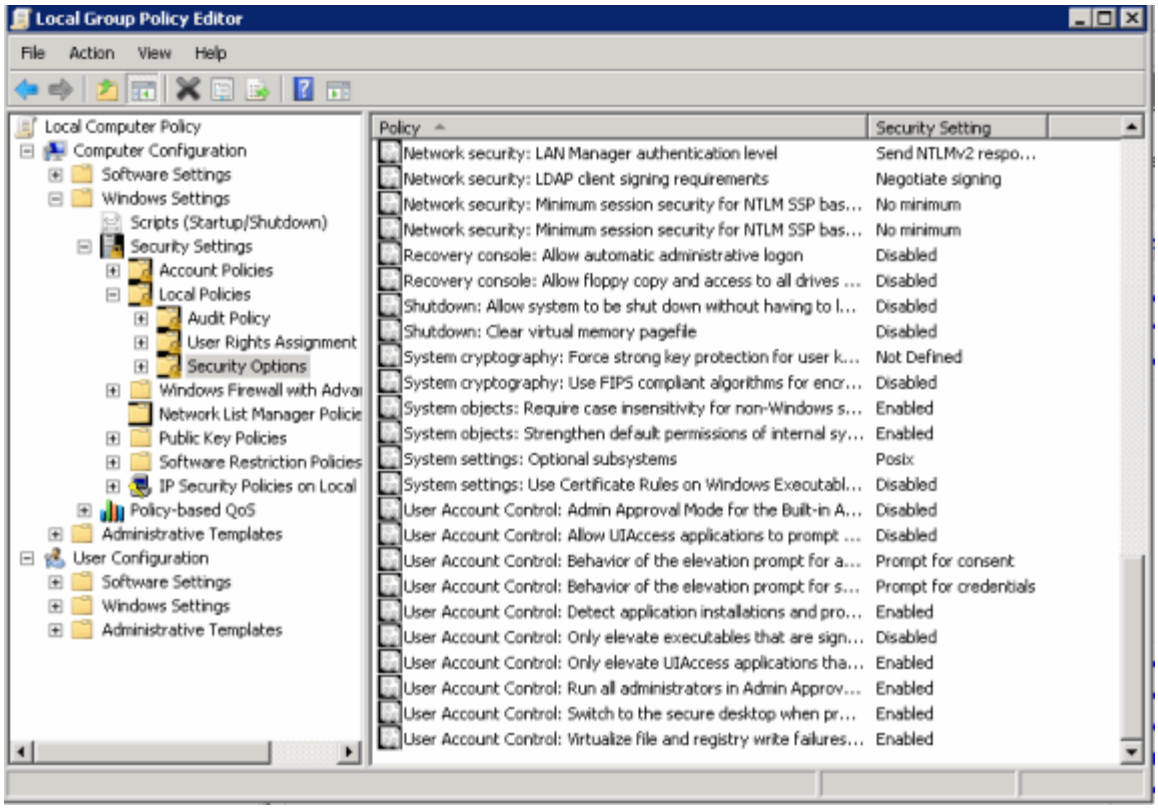
As you can see drive mapping is now very simple and effective. Server 2008 new feature Preferences Drive Maps extension allows IT administrators to map network drives for end users without writing scripts.

Manage User Account Control using Group Policy

A new security feature called User Account Control (UAC) is introduced in Windows Vista and Windows 2008. It is designed to reduce unauthorized access to the operating system by malicious viruses. When an administrator or user attempts to access an application that can result in a system configuration change, UAC prompts for authorization. This can be very annoying and reduce productivity for administrators. Use following method to centrally manage User Account Control via Group Policy.

1. Open Group Policy Management Console on Server 2008
2. Create a new GPO
3. Browse to:
   Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > User Account Control settings

Above GPO setting allows you to disable and enable User Account Control (UAC) from Group Policy.



Hyper-V

How to Install Hyper-V on Server 2008

Hyper-V is a virtualization platform from Microsoft that is comparable to VMware Server. Hyper-V is the next generating of Virtual Server 2005. The main limitation of Virtual Server 2005 was lack of support for 64-bit guest OS. Server 2008 Hyper-V requires that host machine where Hyper-V is installed support Virtualization technology. Virtualization technology for Intel processors is known as VT technology and it can be enabled from BIOS.

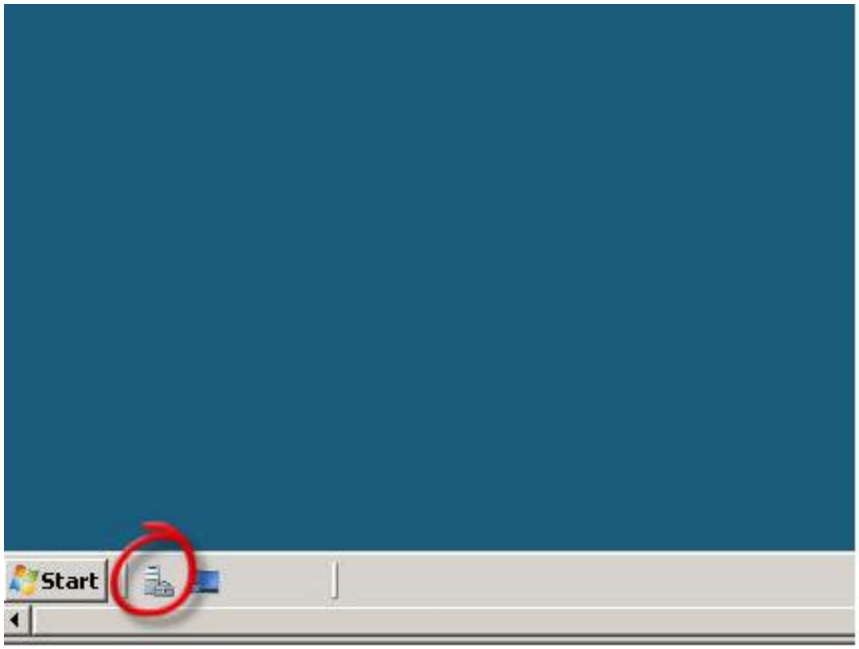
Install Hyper-V on Server 2008:

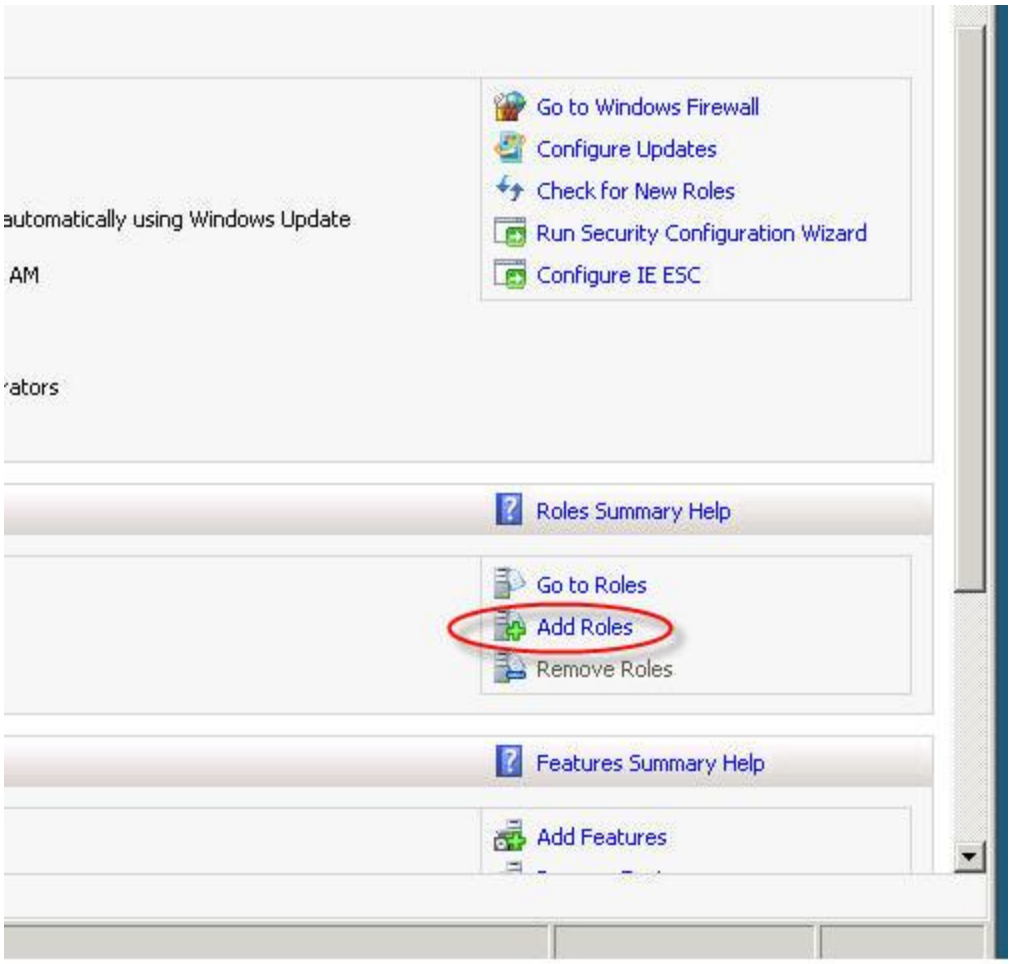
1. Open Server Manager
2. Click Add Roles
3. Choose Hyper-V role, Network Policy and Access Services (this enable routing two VM networks)
4. Choose sub services
5. Click Next
6. Leave the network adapters uncheck (new networks can be created later), Click Next
7. Click Next and Restart the computer when prompted.

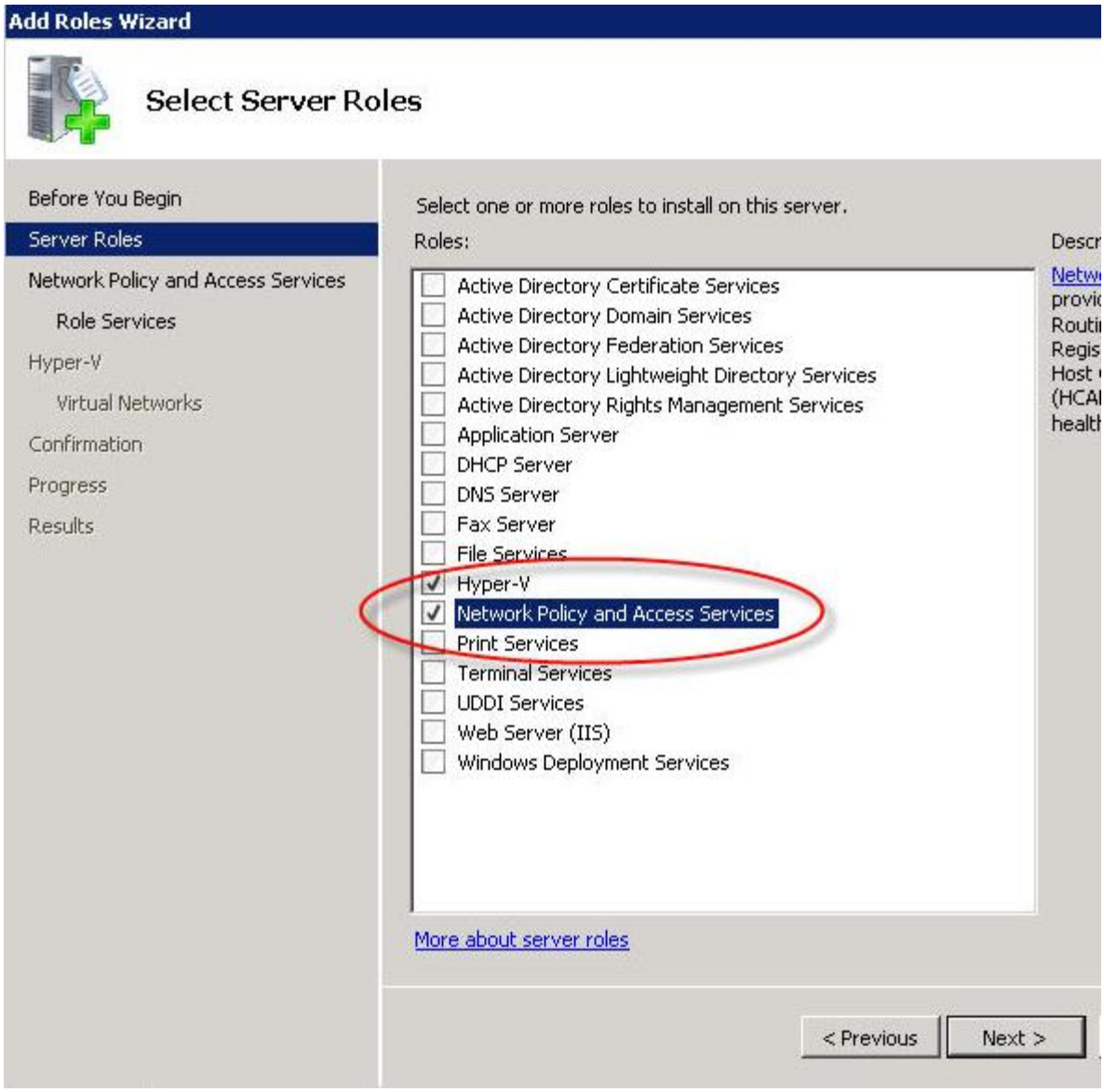
Now can manage Hyper-V role from Server Manager

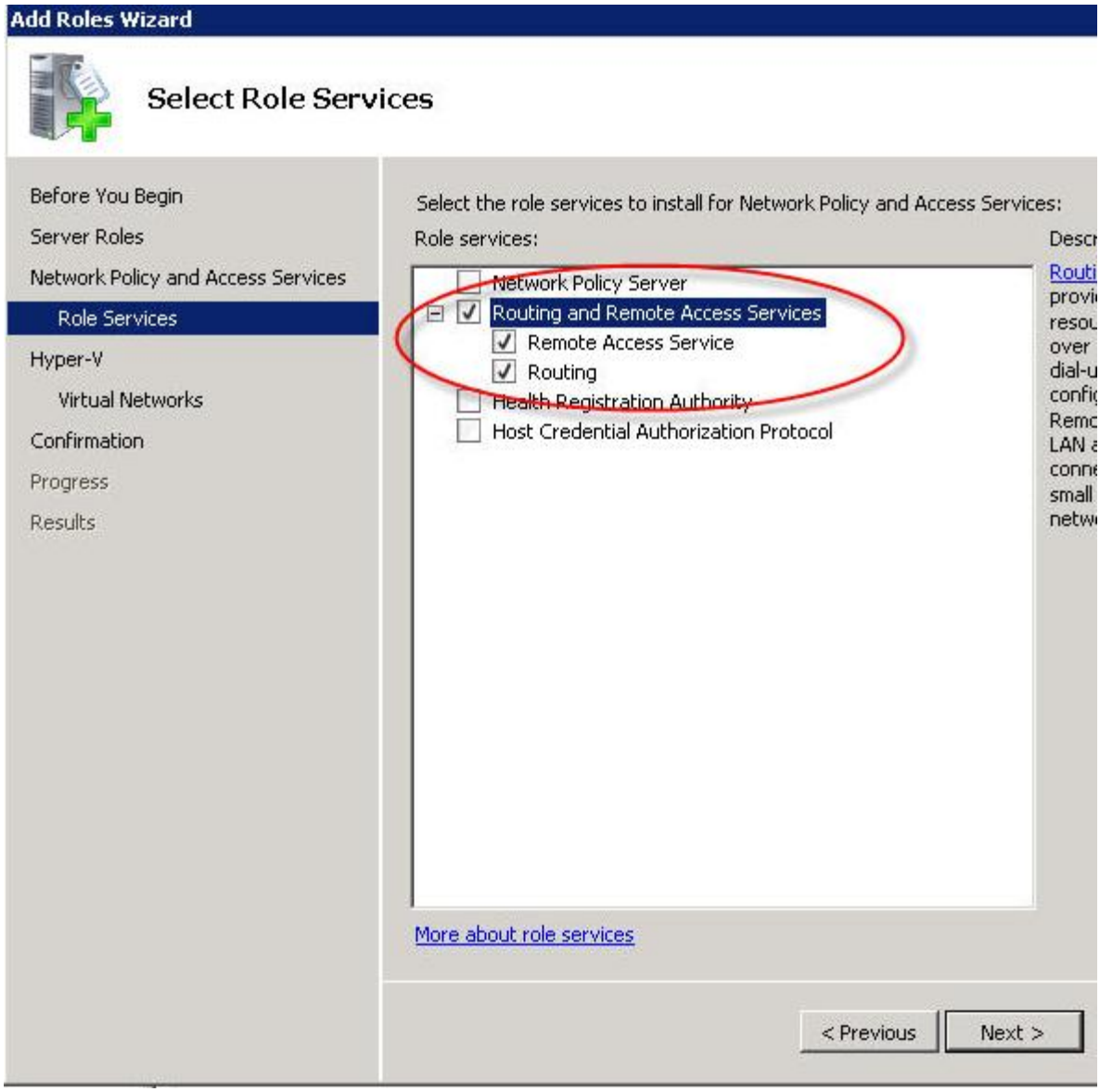
Related Links: Andrew from Techsack.com has written an article on running Hyper-V on Dell PowerEdge 2900

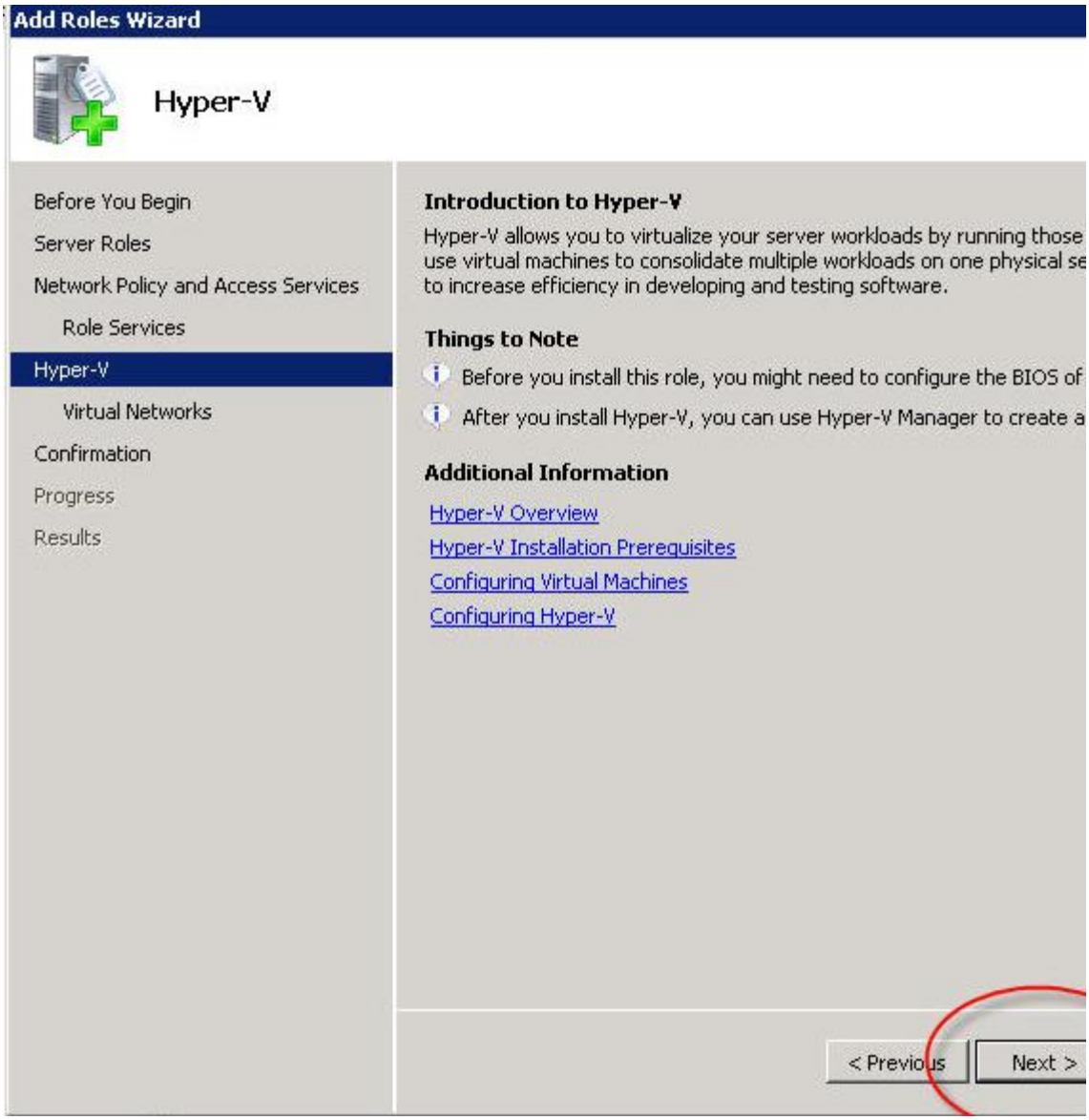
HYPER-V INSTALL SCREEN SHOTS

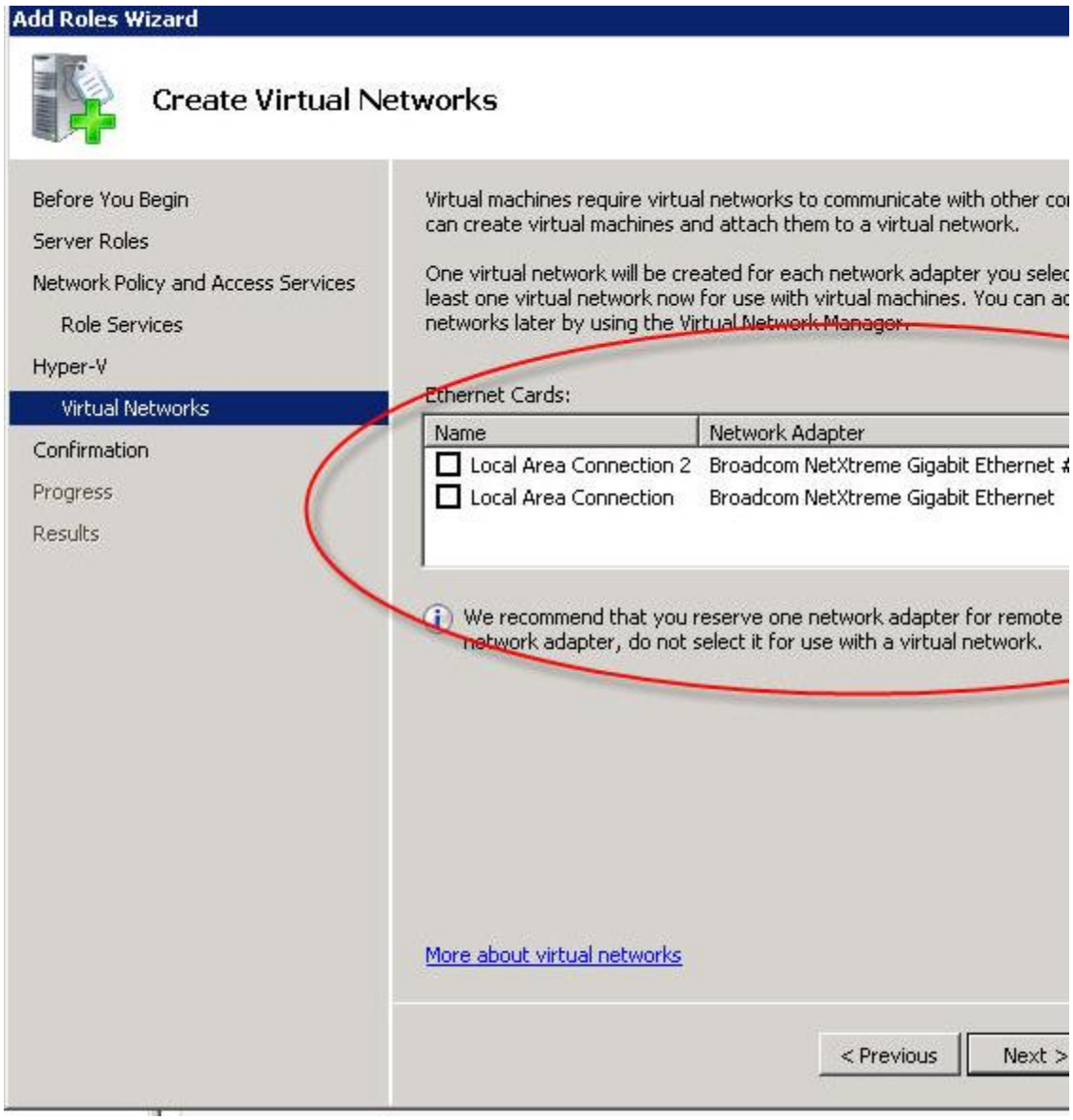



Go to Windows Firewall
Configure Updates
Check for New Roles
Run Security Configuration Wizard
Configure IE ESC
automatically using Windows Update
AM
ators
Roles Summary Help
Go to Roles
Add Roles
Remove Roles
Features Summary Help
Add Features

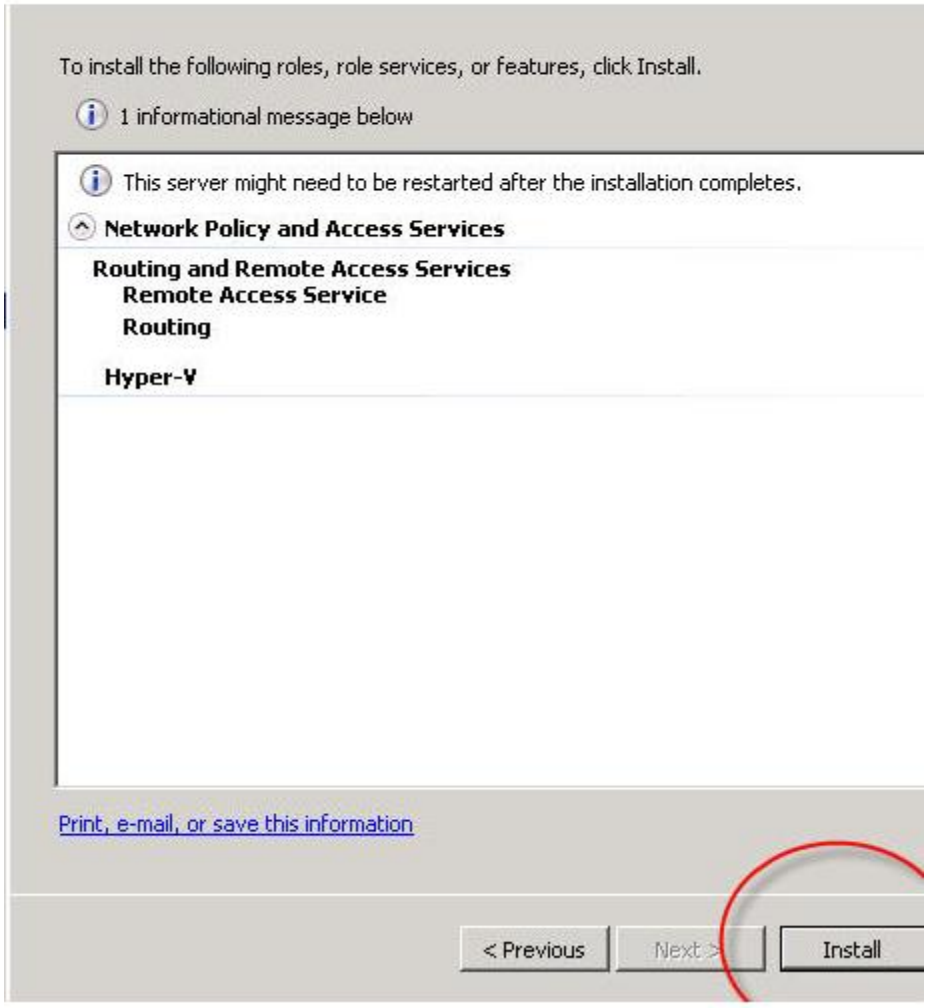

Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Hyper-V
Virtual Networks
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
More about server roles
< Previous
Next >

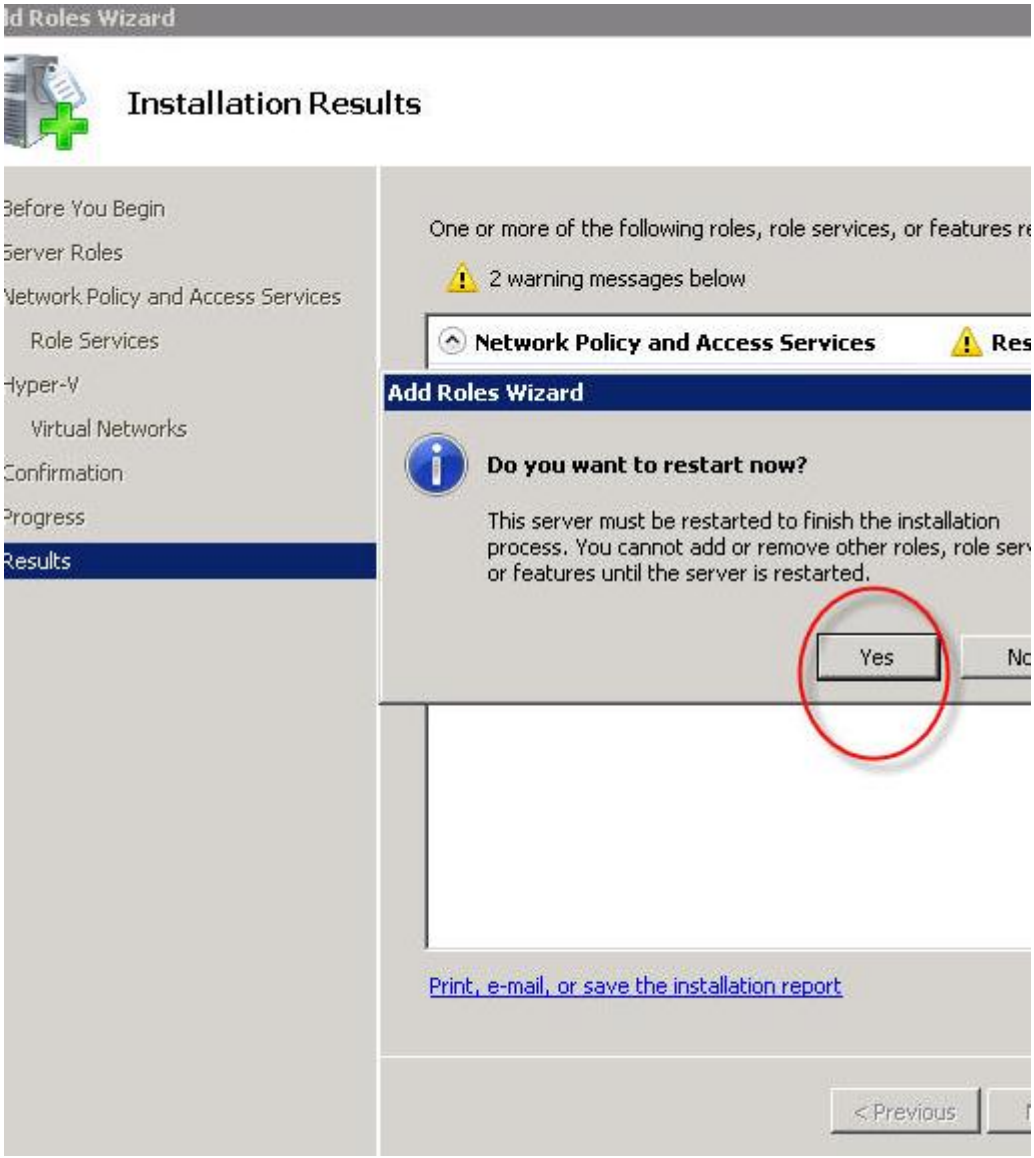

Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Hyper-V
Virtual Networks
Confirmation
Progress
Results
Select the role services to install for Network Policy and Access Services:
Role services:
Network Policy Server
Routing and Remote Access Services
Remote Access Service
Routing
Health Registration Authority
Host Credential Authorization Protocol
More about role services
< Previous
Next >

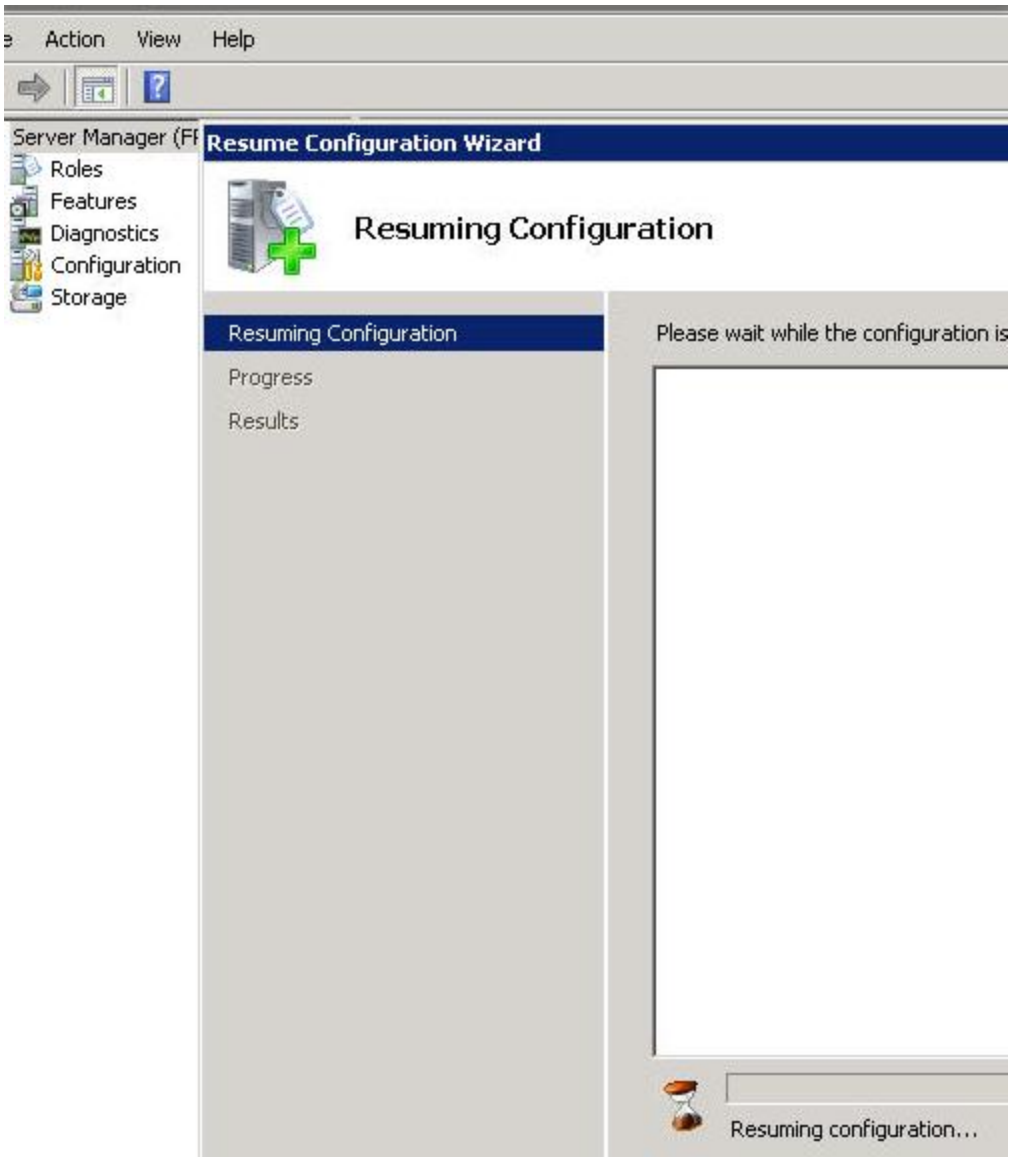

Add Roles Wizard
Hyper-V
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Hyper-V
Virtual Networks
Confirmation
Progress
Results
Introduction to Hyper-V
Hyper-V allows you to virtualize your server workloads by running those
use virtual machines to consolidate multiple workloads on one physical se
to increase efficiency in developing and testing software.
Things to Note
Before you install this role, you might need to configure the BIOS of
After you install Hyper-V, you can use Hyper-V Manager to create a
Additional Information
Hyper-V Overview
Hyper-V Installation Prerequisites
Configuring Virtual Machines
Configuring Hyper-V
< Previous
Next >


Add Roles Wizard
Create Virtual Networks
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Hyper-V
Virtual Networks
Confirmation
Progress
Results
Virtual machines require virtual networks to communicate with other co
can create virtual machines and attach them to a virtual network.
One virtual network will be created for each network adapter you selec
least one virtual network now for use with virtual machines. You can ac
networks later by using the Virtual Network Manager.
Ethernet Cards:
Name
Network Adapter
Local Area Connection 2
Broadcom NetXtreme Gigabit Ethernet #
Local Area Connection
Broadcom NetXtreme Gigabit Ethernet
We recommend that you reserve one network adapter for remote
network adapter, do not select it for use with a virtual network.
More about virtual networks
< Previous
Next >

tion Selections




d Roles Wizard
Installation Results
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Hyper-V
Virtual Networks
Confirmation
Progress
Results
One or more of the following roles, role services, or features re
2 warning messages below
Network Policy and Access Services
Res
Add Roles Wizard
Do you want to restart now?
This server must be restarted to finish the installation process. You cannot add or remove other roles, role serv or features until the server is restarted.
Yes
No
Print, e-mail, or save the installation report
< Previous



How to Migrate Virtual Server 2005 Virtual Machines to Windows Server 2008 Hyper-V

> How VM from Virtual Server 2005 to Windows Server 2008 Hyper-V

Hyper-V Guest OS Requirements: Windows server 2003 sp2, Windows Server 2008 sp1

On Virtual Server 2005
1. Upgrade existing Virtual Server 2005 virtual machine to Windows server 2003 sp2.
2. Uninstall Virtual Machine additions on Virtual Server 2005 virtual machine from

ADD/REMOVE programs.
3. Shutdown Virtual Server 2005 virtual machine and copy the VHD to Hyper-V server

On Hyper-V
1. On Hyper-V, create a new virtual machine with the VHD copied from Virtual Server 2005 virtual machine.
2. On Hyper-V VM, right click to access Settings.
3. Go to Add Hardware, Add new Legacy Network Adapter. Remove "Network Adapter", click OK to save the settings (If you skip the step, you will lose the previous IP configuration)
4. Start the VM, Right click, Start.
5. When the VM is up, mouse input will be unavailable so you must use the keyboard. (you can use the "Tab" key navigate)
6. Logon to VM, cancel all "New hardware found" error messages
7. On Virtual Machine Connection console on the host, Click Action > Insert Integration Services Setup Disk. This will install VM Integration Services automatically. You may be asked to reboot several times.

How Route between two different virtual networks in Hyper-V

When new internal network is created from "Virtual Network Manager", new virtual "Local Area Connection X" is automatically created under "Control Panel > Network Connections". We can use RRAS (routing and remote access) to route between virtual "Local Area Connection".

1. Open Hyper-V console
2. Click on "Virtual Network Manager" under "Actions" Pane
3. Enter Name, choose "Internal", click "Add", click "OK"
4. You will noticed that new Local Area Connection is created under "Control Panel > Network Connections"
5. Right click on the newly created Local Area Connection, choose properties.
6. On TCP/IPv4 screen, enter IP: 10.1.0.1 , Subnet: 255.255.255.0 and no gateway. (Repeat step 2 to 6 if you would like to create multiple networks)

7. Open "Routing and Remote Access" console. (Server Manager > Network Policy and Access > Routing and Remote Access)

8. Right click on "Routing and Remote Access" and choose "Configure and Enable Routing and Remote Access"

9. Choose "Custom Configuration"

10. Choose "NAT" and "LAN routing", click Next
    NAT allows your VMs to access the internet without exposing them.
    LAN routing allows you route between Local Area Connections

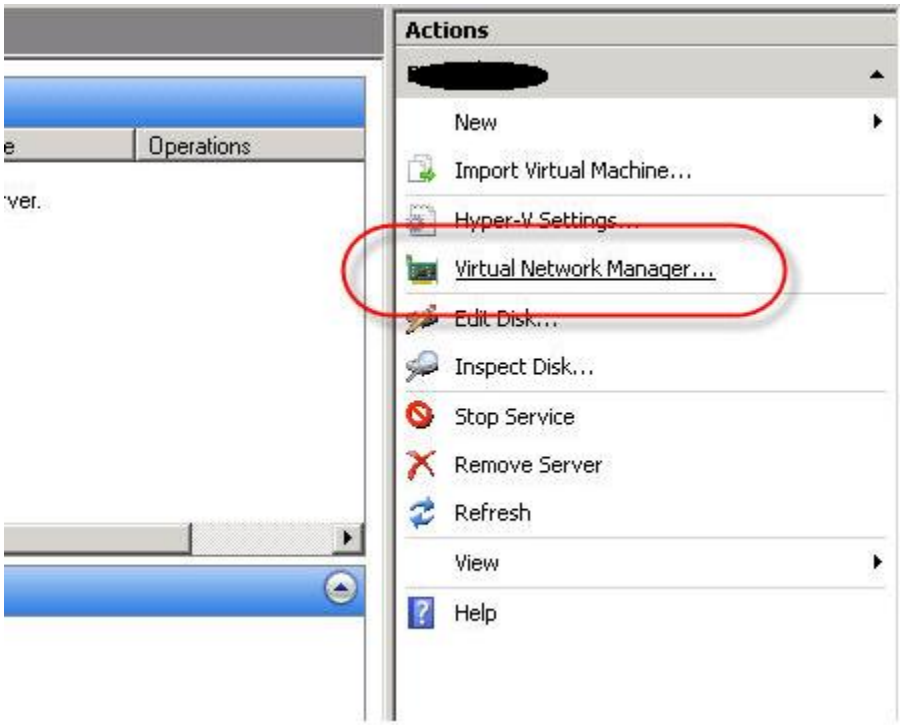
11. Click Finish and Start the service.

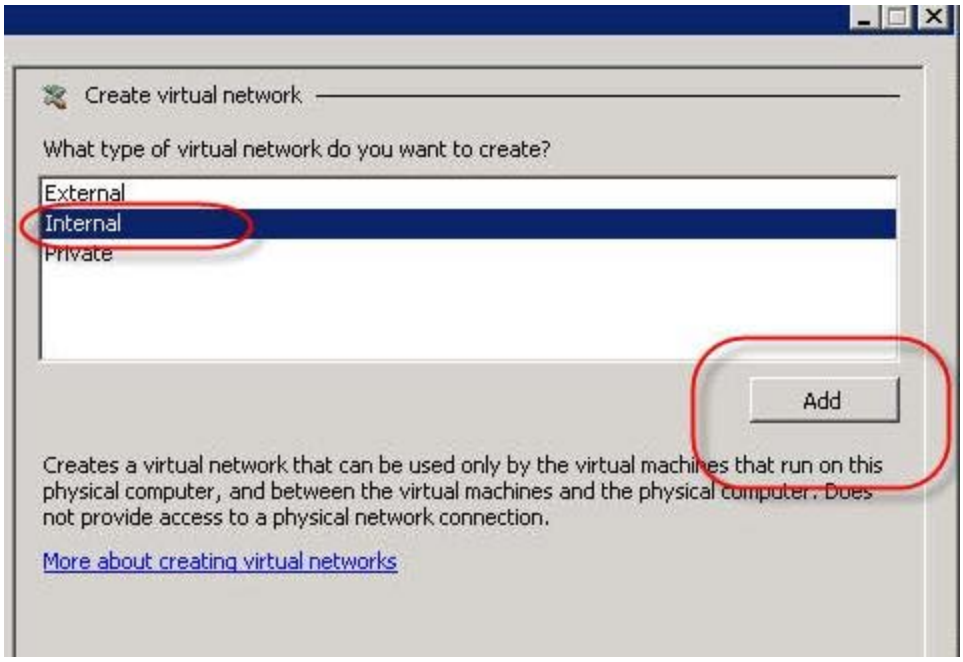
12. Browse to “NAT” under IPv4, Right click and choose “New Interface”, choose the interface that you use to connect to the internet.

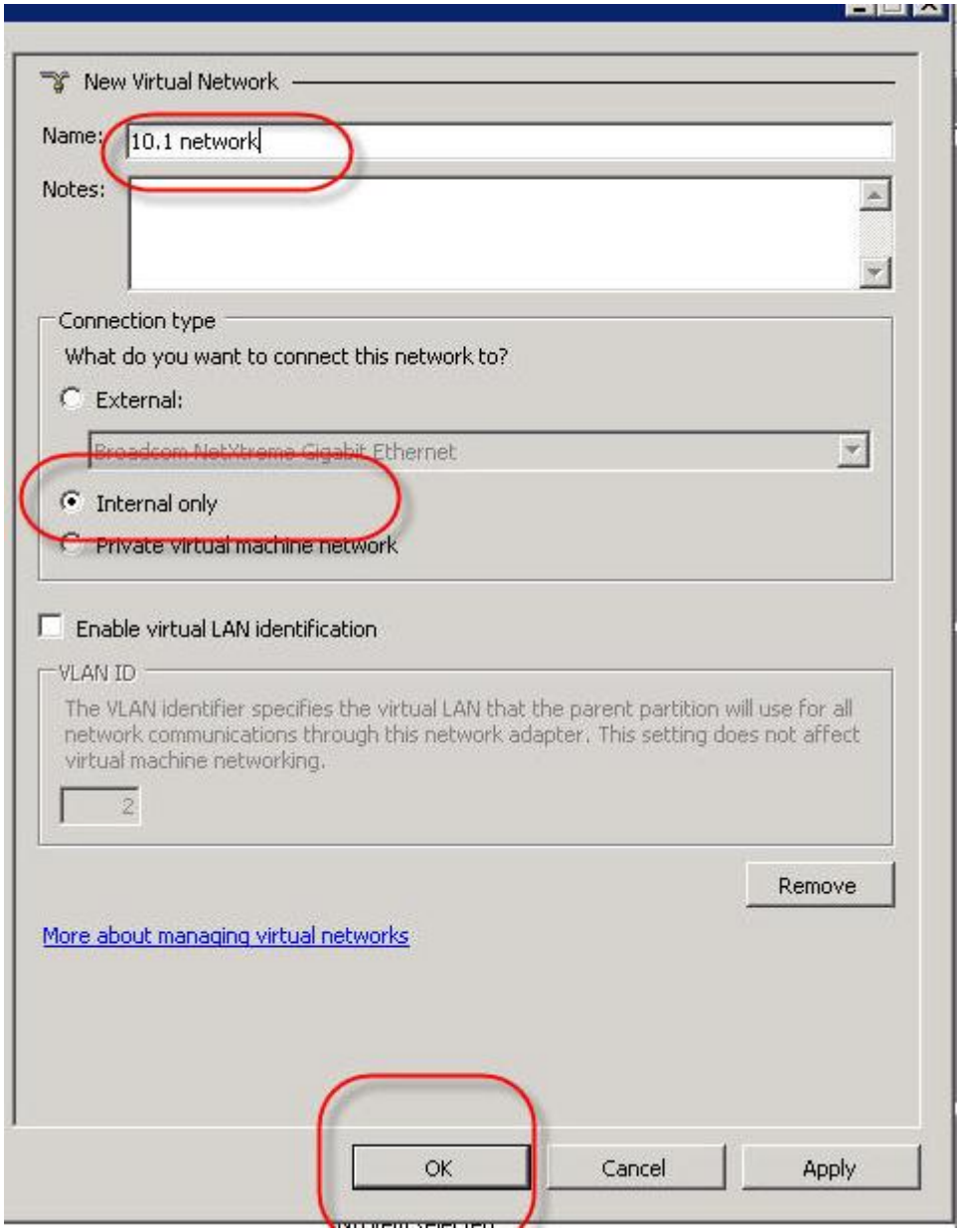
13. Choose “Public interface connected to the internet”, check “Enable NAT on this interface”, click OK

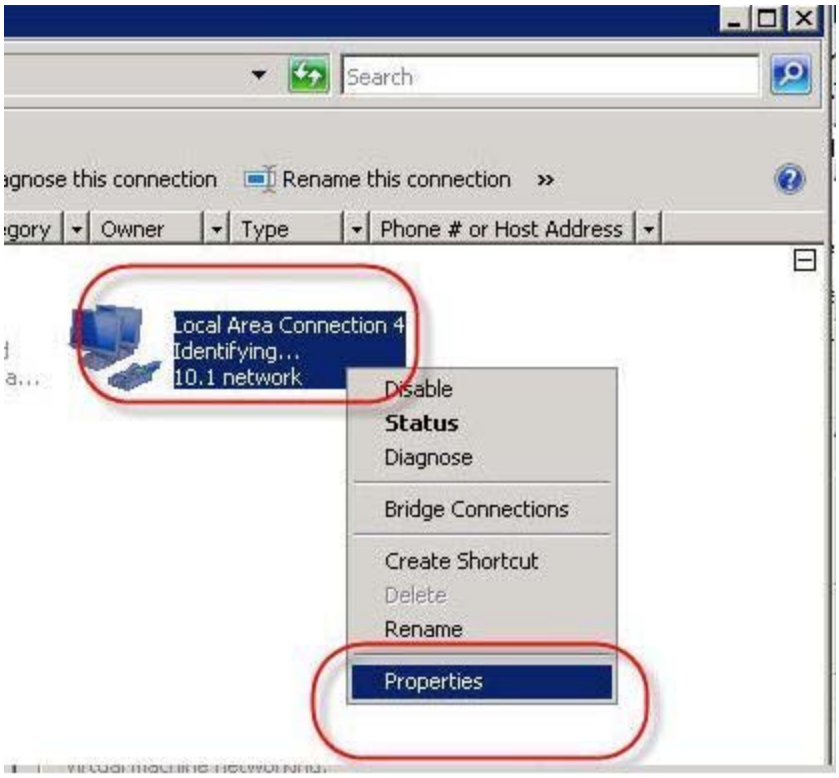
Now use 10.1.0.1 as the gateway on Hyper-V guest VM and you will be able to access the internet and to other subnets.

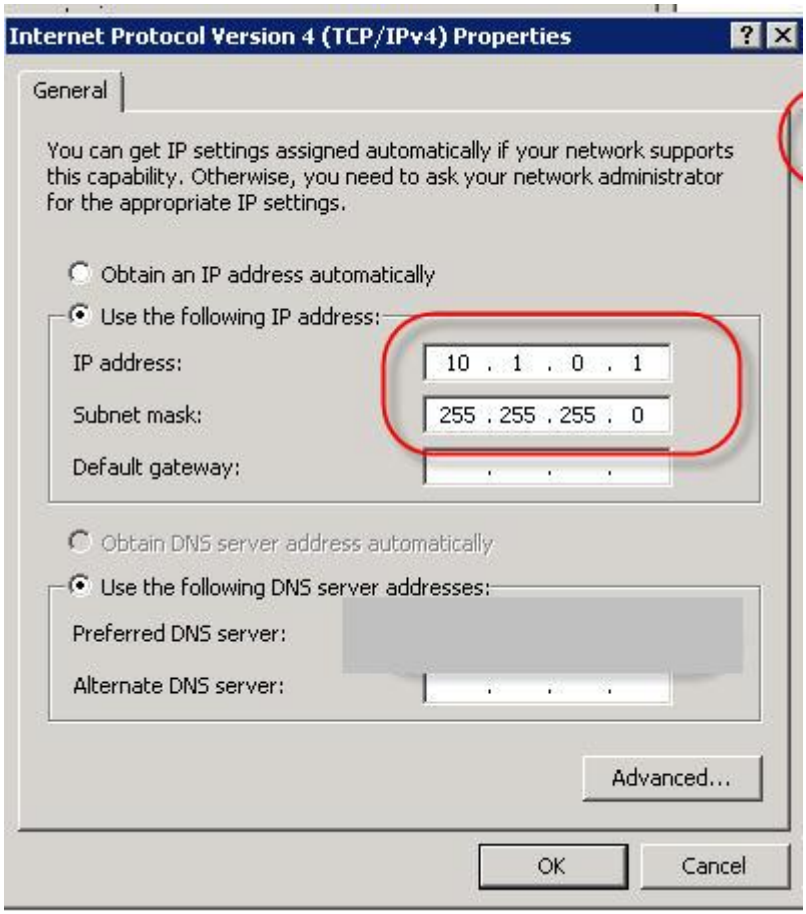
SCREENSHOTS

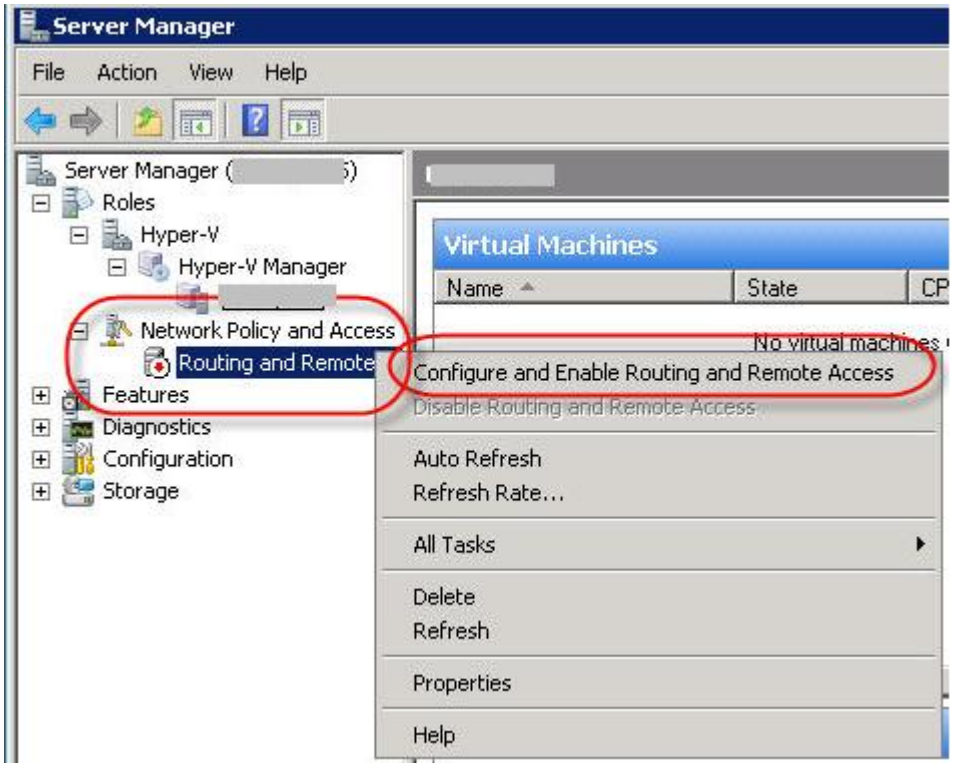


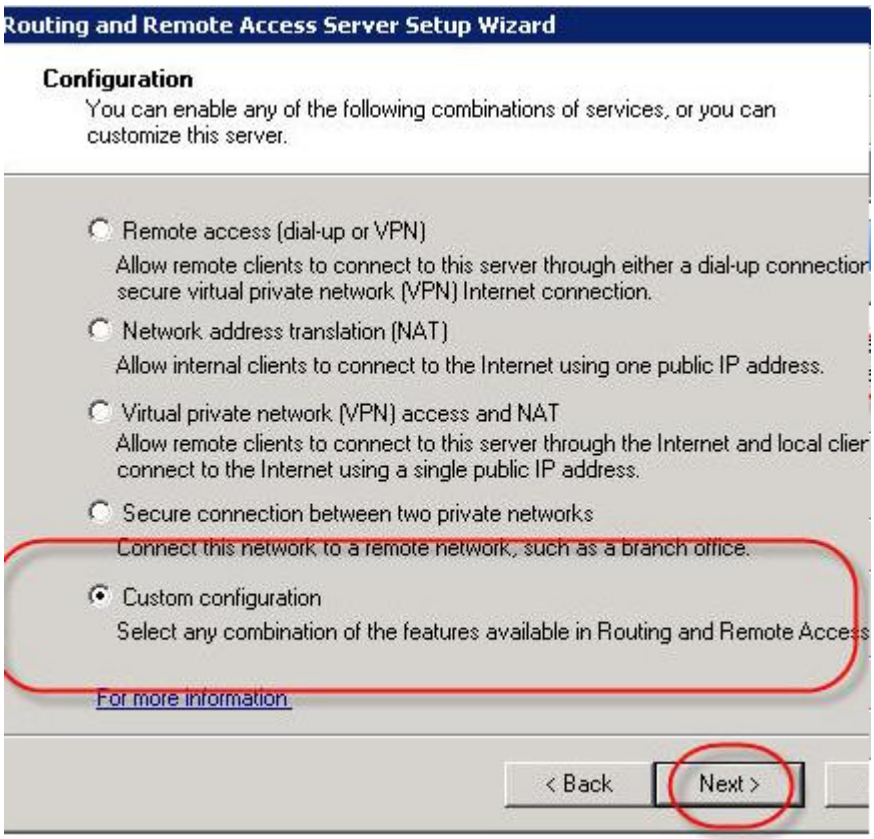

Create virtual network
What type of virtual network do you want to create?
External
Internal
Private
Add
Creates a virtual network that can be used only by the virtual machines that run on this physical computer, and between the virtual machines and the physical computer. Does not provide access to a physical network connection.
More about creating virtual networks

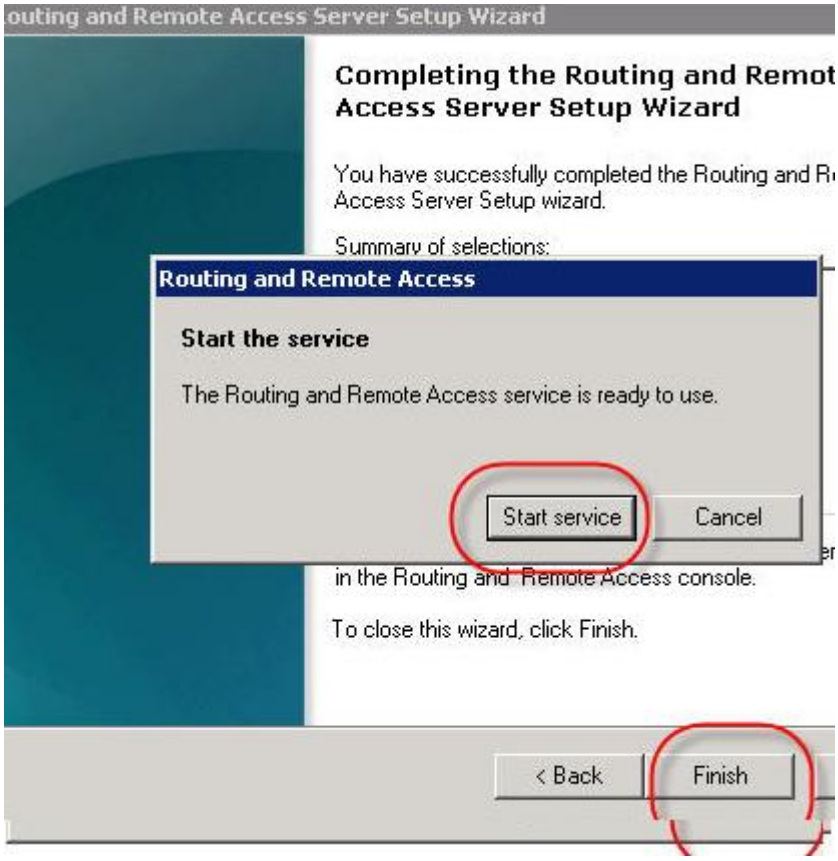

New Virtual Network
Name:
10.1 network
Notes:
Connection type
What do you want to connect this network to?
External:
Broadcom NetXtreme Gigabit Ethernet
Internal only
Private virtual machine network
Enable virtual LAN identification
VLAN ID
The VLAN identifier specifies the virtual LAN that the parent partition will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
More about managing virtual networks
OK
Cancel
Apply

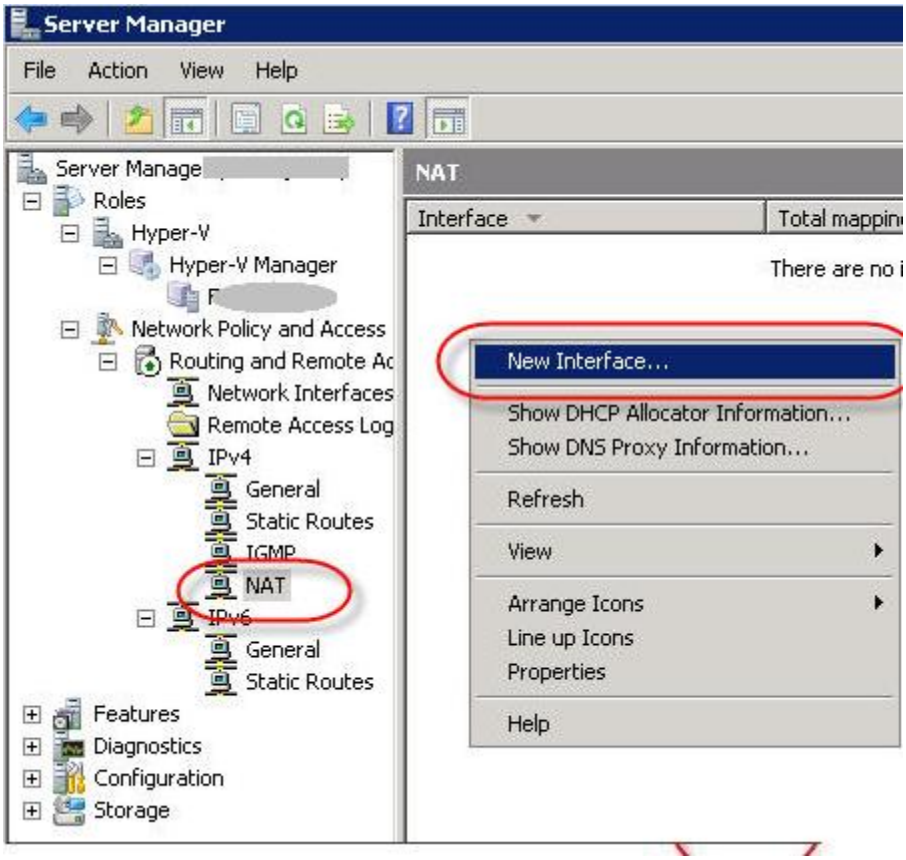

Search
gnose this connection
Rename this connection
»
gory
Owner
Type
Phone # or Host Address
Local Area Connection 4
Identifying...
10.1 network
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

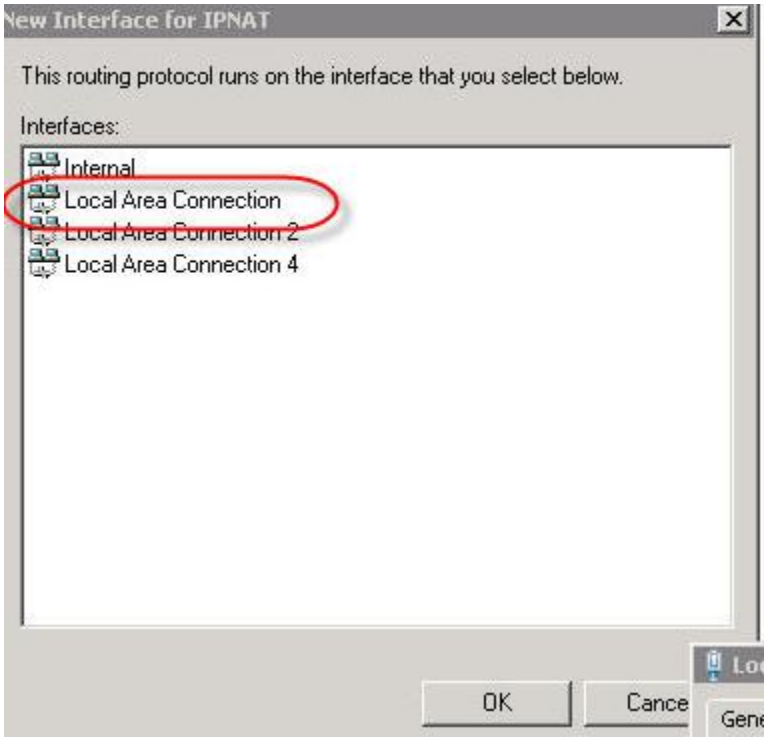

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 1 . 0 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

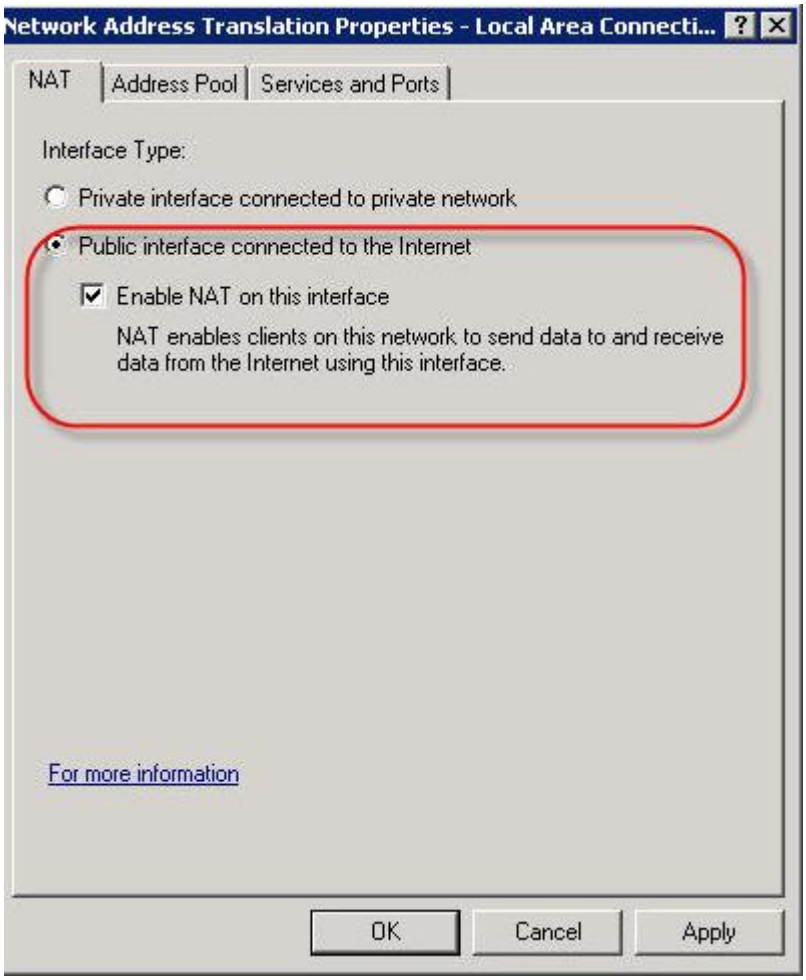

Server Manager
File
Action
View
Help
Server Manager (
Roles
Hyper-V
Hyper-V Manager
Network Policy and Access
Routing and Remote
Features
Diagnostics
Configuration
Storage
Virtual Machines
Name
State
No virtual machines
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
Auto Refresh
Refresh Rate...
All Tasks
Delete
Refresh
Properties
Help


Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection
secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clien
connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access
For more information
< Back
Next >


outing and Remote Access Server Setup Wizard
Completing the Routing and Remot
Access Server Setup Wizard
You have successfully completed the Routing and R
Access Server Setup wizard.
Summary of selections:
Routing and Remote Access
Start the service
The Routing and Remote Access service is ready to use.
Start service
Cancel
in the Routing and Remote Access console.
To close this wizard, click Finish.
< Back
Finish

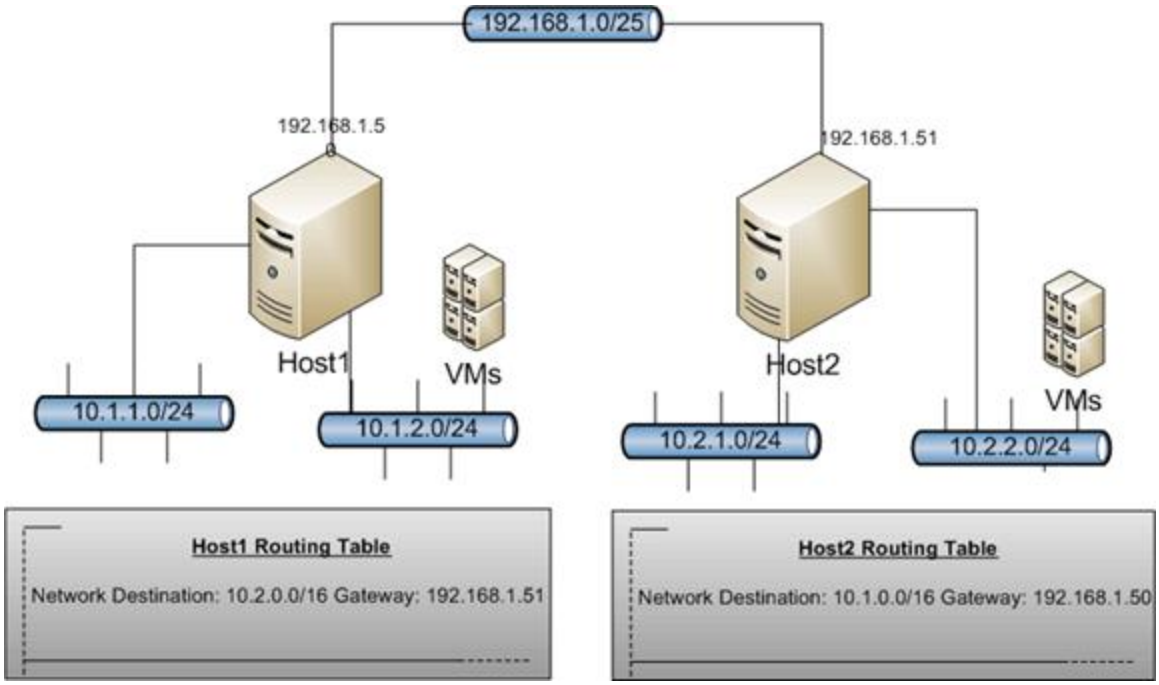

Server Manager
File
Action
View
Help
Server Manage
Roles
Hyper-V
Hyper-V Manager
Network Policy and Access
Routing and Remote Ac
Network Interfaces
Remote Access Log
IPv4
General
Static Routes
IGMP
NAT
IPv6
General
Static Routes
Features
Diagnostics
Configuration
Storage
NAT
Interface
Total mappin
There are no i
New Interface...
Show DHCP Allocator Information...
Show DNS Proxy Information...
Refresh
View
Arrange Icons
Line up Icons
Properties
Help


New Interface for IPNAT
This routing protocol runs on the interface that you select below.
Interfaces:
Internal
Local Area Connection
Local Area Connection 2
Local Area Connection 4
OK
Cance



How to route Hyper-V virtual networks between two hosts

This article explains how to route Hyper-V virtual networks between two physical hosts. This is a very advanced concept so I assume you have at least some experience with Hyper-V networking. This technique allows you scale a very large network / active directory environment across multiple physical hosts. You can deploy five to six VMs on each physical host and allow it to communicate while using its own IP address range. This technique is very useful when building a large Active Directory environment consisting multiple site and domains. You can assign different subnet to each virtual network and use this technique to allow communication between multiple hosts.



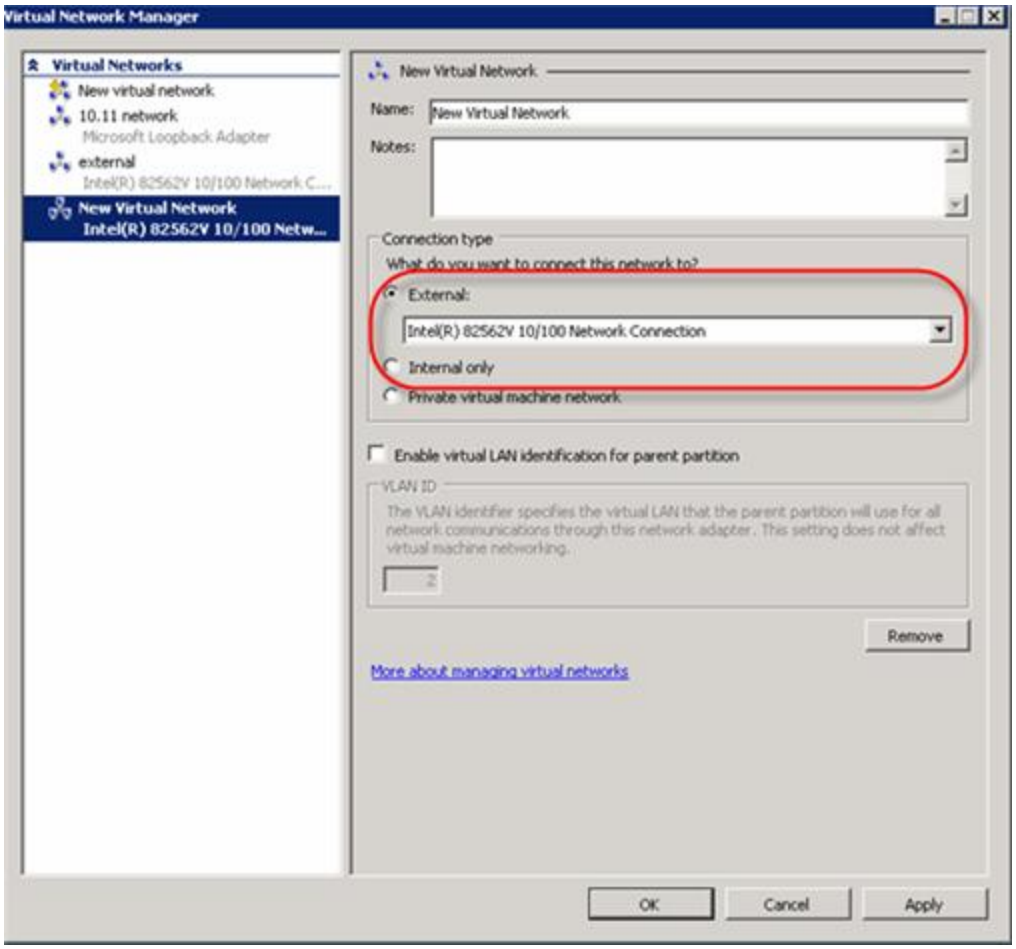
Step by step high level overview

1. Follow the instructions on how to route between two networks here.
2. create an external network and bind to physical NIC
3. configure RRAS for Routing and NAT
4. add static routes to both hosts
5. confirm network connectivity

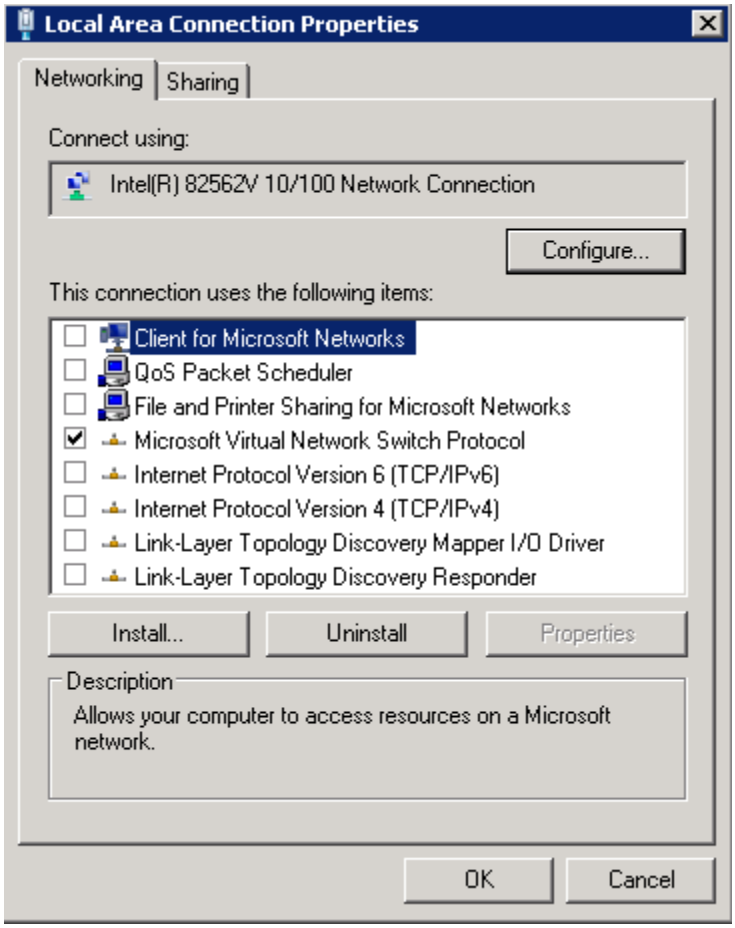
Step #1 - Follow the instructions on how to route between two virtual networks here.

Step #2 - create an external network and bind to physical NIC

1. Open Hyper-V manager, (Server Manager > Roles > Hyper-V)
2. On “Actions” pane, click Virtual Network Manager
3. Choose “New virtual network”, “External” click on “Add”
4. Enter network name, choose your primary physical network adapter. See screenshot
5. Click OK



Important note: Make sure your physical NIC bind to Microsoft Virtual Network Switch or else the packets will stop at the physical interface (running tracert can prove this). This is needed to route traffic that come in from your physical interface to the VM's loopback interface which is part of Microsoft Virtual Network Switch. You can do this by creating new External Virtual Network and selecting your physical adapter.



Step #3 - configure RRAS for Routing and NAT

1. Open “Routing and Remote Access” console. (Server Manager > Network Policy and Access > Routing and Remote Access)
2. Right click on “Routing and Remote Access” and choose “Configure and Enable Routing and Remote Access”
3. Choose “Custom Configuration”
4. Choose “NAT” and “LAN routing”, click Next
   NAT allows your VMs to access the internet without exposing them.
   LAN routing allows you route between Local Area Connections
5. Click Finish and Start the service.
6. Browse to “NAT” under IPv4, Right click and choose “New Interface”, choose the interface that you use to connect to the internet.
7. Choose “Public interface connected to the internet”, check “Enable NAT on this interface”, click OK

Step #4 - add static routes to both hosts

1. Use “route add” command or RRAS console to add static route for virtual networks (this allows the host to forward traffic to a physical host that is hosting the virtual network)

Step #5 - confirm network connectivity

1. use “Ping” and “tracert” to troubleshoot network connectivity between VMs, Virtual networks and hosts.

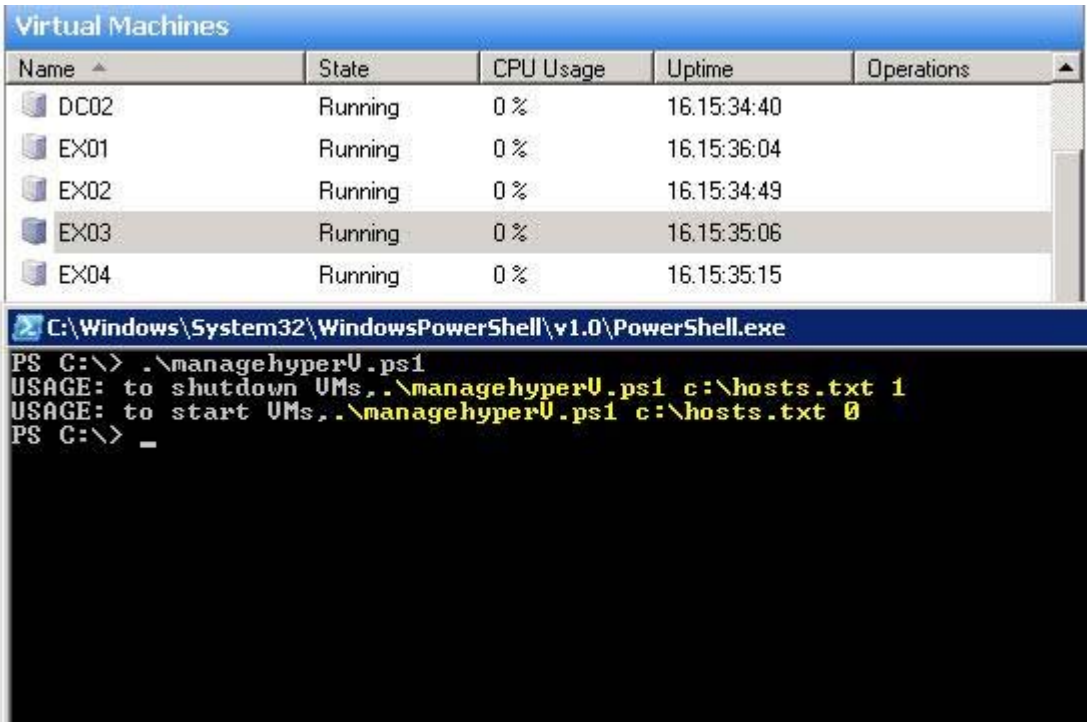
PowerShell Script to Manage Hyper-V VMs

Below is a script that will power on and power off Server 2008 Hyper-V VMs in sequential order from a text file. This Powershell script will read Hyper-V VM names from text file and turn them on.

1. Open notepad
2. Copy and paste below text to notepad
3. Save the file with .ps1 extension.

```
# ---------- SCRIPT STARTS HERE----------

$waitstart = 200
$waitshutdown = 120

if ($args[1] -match "0") {
$inputfile=get-content $args[0]
foreach ($guest in $inputfile) {
write-host "Starting $guest"
$vm = gwmi -namespace root\virtualization -query "select * from msvm_computersystem where
elementname='$guest'"
$result = $vm.requeststatechange(2)
if ($result.returnvalue -match "0") {
start-sleep -s $waitstart
write-host ""
write-host "$guest is started" -foregroundcolor green
write-host ""
}
else {
write-host ""
write-host "unable to start $guest" -foregroundcolor red
write-host ""
}}}

if ($args[1] -match "1") {
$inputfile=get-content $args[0]
foreach ($guest in $inputfile) {
write-host "shutting down $guest"
$vm = gwmi -namespace root\virtualization -query "select * from msvm_computersystem where
```

```
elementname='$guest'"
$vmname = $vm.name
$vmshut = gwmi -namespace root\virtualization -query "SELECT * FROM
Msvm_ShutdownComponent WHERE SystemName='$vmname'"
$result = $vmshut.InitiateShutdown("$true","no comment")
if ($result.returnvalue -match "0") {
start-sleep -s $waitshutdown
write-host ""
write-host "no error while shutting down $guest"
write-host "shutdown of $guest completed" -foregroundcolor green
write-host ""}

else {
write-host ""
write-host "unable to shutdown $guest" -foregroundcolor red
write-host ""
}}}

else {
write-host "USAGE: to shutdown VMs," -nonewline; write-host ".\managehyperV.ps1
c:\hosts.txt 1" -foregroundcolor yellow
write-host "USAGE: to start VMs," -nonewline; write-host ".\managehyperV.ps1 c:\hosts.txt 0" -
foregroundcolor yellow
}

# ---------- SCRIPT ENDS HERE----------
```



Terminal Server

Server 2008 Terminal Services Explained

Terminal Services allows consolidation and standardization of desktop applications or entire desktop. Terminal Services also allows enterprise applications to be made available from any location with an internet connection. In many cases, Terminal services can reduce total cost of ownership when deploying business applications to end users. This eliminates the need for installation of the application on every end user workstation. In a nutshell, Terminal Services allow users to access high performance applications in heterogeneous environments. It supports underpowered hardware, non-windows OS, terminals and thin clients to run as Terminal services clients.

Users utilize mstsc.exe (Remote Desktop Connection Client), RDC to connect to a Terminal Server to access applications. RDC uses Remote Desktop Protocol (RDP) to connect to terminal server on port TCP 3389. RDC Client keyboard and mouse events are redirected to Terminal Server via Remote Desktop Protocol. Terminal Sever then renders and redirects back display to RDC Client.

Terminal Services Modes:

Remote Desktop Mode
Remote Desktop mode allows only two users to connect to a server at one time. Remote Desktop Mode can be enabled by going to *System Properties* > *Remote tab*. The main purpose of Remote Desktop Mode is to allow remote administration of Server 2008. It has no intentions to use as Terminal Server as described above.

Terminal Server Mode
As mentioned above, Terminal Server mode allows consolidation and standardization of desktop applications. Terminal Server mode allows multiple users to connect and run an application or entire desktop. This mode requires the purchase of a Terminal Server client access license (CAL) for each user or session.

Terminal Service Client
Most Windows operating systems—Windows 2000, 2003, XP and Vista include a Remote Desktop Connection (RDC) client. This allows users to connect to a Terminal Server without installing extra application.

How to Install Applications on Server 2008 Terminal Server.

When you deploy a Terminal Server, it is most likely that you want to make an application available to remote users. Follow the steps below on how to install an application on Server 2008 Terminal Server.

To install an application on terminal server, you must change from Execute to Install mode.

1. Change to install mode by running command: **change user /install**
2. Install and configure the application you need.
3. Return to Execute mode; command: **change user /execute**

How to Publish Applications on Server 2008 Terminal Server

> How to make applications available to users on Server 2008 Terminal Server

1. Run "remoteprograms.msc"
2. Click "Add Remote Apps" from Actions list
3. Click Next
4. Select the application you wish you publish
5. Click Finish
6. Select Create .RDP File
7. Click Next
8. Click Finish
9. Select the application from Remote Programs list
10. Select "Create Windows Installer" from Actions menu
11. Click Next
12. Click Next again
13. On "Configure Distribution Package" screen, select "Desktop"and complete "Start menu folder" text box
14. Review settings and click Finish.
15. You may deliver the msi package under "C:\programs files\packaged programs"

How to Install Applications on Server 2008 Terminal Server.

When you deploy a Terminal Server, it is most likely that you want to make an application available to remote users. Follow the steps below on how to install an application on Server 2008 Terminal Server.

To install an application on terminal server, you must change from Execute to Install mode.

1. Change to install mode by running command: **change user /install**
2. Install and configure the application you need.
3. Return to Execute mode; command: **change user /execute**

How to Publish Applications on Server 2008 Terminal Server

> How to make applications available to users on Server 2008 Terminal Server

1. Run "remoteprograms.msc"
2. Click "Add Remote Apps" from Actions list
3. Click Next
4. Select the application you wish you publish
5. Click Finish
6. Select Create .RDP File
7. Click Next
8. Click Finish
9. Select the application from Remote Programs list
10. Select "Create Windows Installer" from Actions menu
11. Click Next
12. Click Next again
13. On "Configure Distribution Package" screen, select "Desktop"and complete "Start menu folder" text box
14. Review settings and click Finish.
15. You may deliver the msi package under "C:\programs files\packaged programs"

How to Install and Configure Windows Server 2008 Terminal Server Web Access

1. Open Server Manager
2. If you already have Terminal Services installed, select Terminal Services under Manage Roles
3. On Terminal Services Role Screen, click “Add Role Services”
4. Select “TS Web Access
5. if asked, choose “Add required Role Services”
6. On Introduction to Web Server (IIS) screen, Click Next
7. On Select Role Services screen., Click Next
8. Click Install.
9. When completed, click Close
10. You can access http://TsWebAccessServer/ts
11. Click on Configuration tab to configure.

Note: If the TS Web Access server is different from Terminal Services Server, you need add TS Web Access server to “TS Web Access Computers” security group on Terminal Services Server.

How to Remote Desktop to internal server securely over the internet.

> How to implement Terminal Services Gateway on Server 2008.

This goal can be achieved by implementing Terminal Services Gateway. Our main concern here is security. The traditional method of allowing remote desktop is to open port 3389 on the firewall, which is a huge security risk. By using Terminal Services Gateway which tunnels RDP traffic over HTTPS (very similar to RPC over HTTPS in Exchange 2003 and Outlook Anywhere in Exchange 2007), this will allow remote desktop access to your internal severs without using VPN.

Prerequisites:
Windows Server 2008
IIS 7
Network Policy Server
SSL Certificate
RPC over HTTP Proxy service

Install Terminal Services Gateway:
1. Click on "Add Roles" from server manager
2. On Select Server Roles screen, choose "Terminal Services" and click Next
3. On the Select Role Services screen, select TS Gateway.
4. Choose Certificate for SSL Encryption Later
5. Choose later to Create Authorization Policies for TS Gateway screen and click next
6. Confirm Network Policy Server is selected
7. Continue to click next and choose install

Misc. Services

Windows Server 2008 Network Access Protection (NAP) Explained

NAP is a Server 2008 feature that allows computers to be inspected against security polices set by an administrator. If the computer doesn't meet security requirements, it can be quarantined to a separate vlan. When using DHCP based enforcement, If the computer doesn't meet security requirements only IP address and subset of routes are provided.

NAP Components

Enforcement Client (EC)
Enforcement Client (EC) is a client—Windows Vista or Windows XP SP3 that is part of NAP infrastructure. This is usually a client that is being validated. Only Windows Vista and Windows XP3 is supported as Enforcement Client as System Health Agent component is pre-installed.

Enforcement Server (ES)
As the name implies, this server enforce security policies against the clients in NAP infrastructure. This is the Server 2008 with Network Policy Server (NPS) role installed

System Health Agent (SHA)
This is the agent/service on Enforcement Client (EC) that sends health information to Enforcement Server (ES). Windows System Health Validator SHA is included in Windows Vista and Windows XP SP3.

System Health Validator (SHV)
This is the service side component that validates information from the SHAs to enforce polices.

Remediation Server
This server provides remediation service for quarantined clients.

How Network Access Protection (NAP) Works
1. When computer obtain IP address automatically, it presents its health state to DHCP Server. System health agents (SHA) and system health validators (SHV) are included in Vista.
2. DHCP Server sends computer's health state to Microsoft Network Policy Server.
3. Microsoft Network Policy Server compare computer's health states with the policy set by an administrator and place the computer on the correct VLAN.

You can install implement Network Access Protection (NAP) from Server Manager > "Add Roles" > Network Policy Server role. Network Policy Server role is the Server 2008 role that handles NAP

How to Deploy a Server 2008 Network Policy Server

Installing Network Policy Server role on Server 2008 makes it an Enforcement Server and System Health Agent.

Network Policy Server Terminology:

802.1X authentication
Server 2008 Network Policy Server can validate clients and place them in 802.1X network. As Wikipedia explains it, **EEE 802.1X** is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

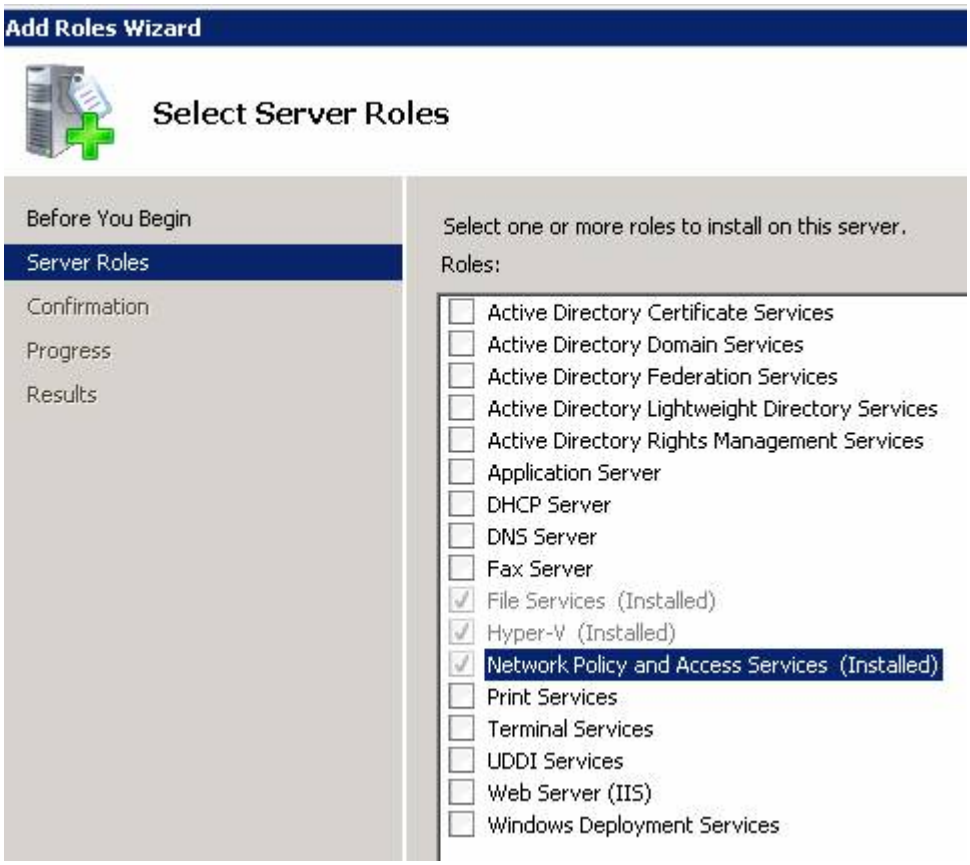
Internet Protocol Security (IPSec)
Server 2008 Network Policy Server can validate IPSec clients based on their health. As Wikipedia explains it, **IPsec** (**IP security**) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

Virtual private network (VPN) connections
Server 2008 Network Policy Server can validate VPN clients based on their health. As Wikipedia explains it, A **virtual private network (VPN)** is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case.

Dynamic Host Configuration Protocol (DHCP) addresses
Server 2008 Network Policy Server can validate DHCP clients and lease IP address based on their health status. As Wikipedia explains it, **Dynamic Host Configuration Protocol** (**DHCP**) is a protocol used by networked devices (*clients*) to obtain the parameters necessary for operation in an Internet Protocol network.

Install Network Policy Server Role

1. Open Server Manager
2. Click Add Roles
3. Click Next,
4. Choose, “Network Policy and Access Services”
5. Click Next
6. Choose “Network Policy Server”, “Routing and Remote Access Service”, Health Registration Authority
7. Choose to install a local CA or use a remote CA
8. Confirm settings and click Install



Enforcing Policies with Server 2008 Network Policy Server

Network Policy MMC console can be used to manage the Network Server. Start> All Programs> Administrative Tools> Network Policy Server. I won't go through the details but below is process of configuring Server 2008 Network Policy Server.

1. Create a System Health Validator.
2. Create a health policy for compliant clients.
3. Create a health policy for noncompliant clients.
4. Create a network policy for compliant clients.
5. Create a network policy for noncompliant clients.

Free system imaging solution ? Server 2008 Windows Deployment Services (WDS)?

Server 2008 Windows Deployment Services (WDS) replaces Remote Installation Services (RIS) offered in Windows Server 2003 and 2000. WDS use PXE and TFTP to boot from WDS server.

The main difference between Windows Deployment Services (WDS) and other imaging solutions like Ghost is that WDS uses file-based imaging format where others use sector based. WIM format uses single instance store which files are stored only once and referenced multiple times. As result, images are a lot smaller.

Windows Deployment Services (WDS) supported OSes:
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

How to install and configure Server 2008 Windows Deployment Services (WDS)

Server 2008 Windows Deployment Services (WDS) prerequisites

- WDS server must be a member server of an Active Directory domain
- DHCP must be configured for PXE boot to work
- DNS, you will mostly have this.
- OS media
- NTFS partition on the WDS server
- Server 2008

To install Windows Deployment Services (WDS) on Server 2008

open **server manager** > Click on **Add Roles** link > click **Next** > on the **Select Server Roles** screen, select **Windows Deployment Services**, and
then click **Next**.

On the Role Services screen, verify that Deployment Server and Transport Server are checked; then click Next, then click Install

Start > **Administrative Tools** > **Windows Deployment Services** to access the **Windows Deployment Services Management console**.
Choose the path to where images will stored.
Configure PXE Server settings, choose “Respond to all”, and Click finish.

Add a Boot Image to WDS Server

Boot image is the image file used during pre-installation OS, also known as boot OS and delivered via PXE boot.

1. Start > Administrative Tools > Windows Deployment Services to access the Windows Deployment Services Management console
2. Right click the Boot Images node. Then click Add Boot Image
3. Click Browse to locate the boot image you wish to add. (Use the Boot.wim from the Windows Server 2008 installation DVD)
4. Once completed, you should be able to see this image you when perform a PXE boot.

Create a Capture Boot Image

Capture Boot Image is a boot image used when capturing images. You will use capture image to boot a server/client to capture its image into a .wim file. You can create a capture boot image by using the Boot.wim from the Windows Server 2008 installation DVD.

1. Start > Administrative Tools > Windows Deployment Services to access the Windows Deployment Services Management console.
2. expand the Boot Images node
3. Right click the image you added earlier (See step 2 from Add a Boot Image to WDS Server)
4. Click Create Capture Boot Image
5. Once completed, click Finish.
6. Right click on boot image folder, choose "Add Boot Image"
7. Select the capture boot image we just created and click Next
8. Once completed, you should be able to use this boot image to capture Operating System images

Create an Install Image (create an image)

Install image includes the OS, custom applications and settings. It is most likely that you will have an install image for every OS you support.

1. Create a base computer (A computer that includes the OS, custom applications and settings).
2. Install sysprep.exe (If you are using windows 2003 or XP, you can find it deploy.cab of Installation CD,), note: sysprep is included by default in Server 2008
3. Run sysprep.exe on the base computer (on XP, sysprep –mini –reseal –forceshutdown)

4. Verify that the base computer is connected to the network and powered on the system
5. Perform a network boot (Often you can do this with the F12 key)
6. In the boot menu screen, select the capture boot image that you created earlier
7. Choose the source drive and enter a name and description for the image. Click Next. Note: only Sysprep drives will appear)
8. Choose "Browse" to select a destination for the image. Enter a name and click "Save", Select "Upload image to WDS Server"
9. Enter the name of the WDS server, and then click Connect.
10. Provide a user name and password if prompted
11. Select the "Image Group" from the list
12. Click "Finish"
13. Now, you should be able to install this image to a server/client via PXE boot.

Install an Install Image (restore an image)

This process restores the Install Image we created earlier.

1. Configure your BIOS to enable PXE boot (aka Network Boot)
2. Perform a network boot (usually by press F12)
3. Select the boot image from the boot menu.
4. WDS will load the computer into GUI and follow the wizard.

Different Types of Server 2008 WDS Images Explained

Boot Image
WDS Boot Image contain Windows Pre-installation Environment (Windows PE). This slim down operating system is used to connect to the WDS Server. The boot image can be found in Server 2008 installation media (search for boot.wim).

Discover Image
WDS Discover Image is created from boot image. This image allows an alternative way to load Windows PE and connect to a WDS server without using PXE boot. It can be stored on a physical media to load Windows PE and connect to WDS.

Capture Image
WDS Capture Image is created from boot image also. This image is used to capture a base system image that is ready for imaging.

Installation Image
WDS Installation Image consists of a file that contains Windows installation files. It make sense to have an Installation Image for every version of OS (XP, 2003, 2008, etc.)

How To Install WSUS on Windows Server 2008

Free Server 2008 patch management solution

WSUS allows administrators to control and distribute Windows updates from a central location. This free patch management solution can be installed on Server 2003 SP1 or Server 2008.

WSUS Prerequisites:

1. Server 2008 or Server 2003 SP1
2. BITS (Background Intelligent Transfer Service)
3. IIS (Internet Information Services)
4. MSDE database or SQL 2005 Database
5. .NET Framework 2.0 or higher

Install WSUS on Windows Server 2008

1. Open Server Manager > Add Roles
2. Install “Windows Server Update Services” Role

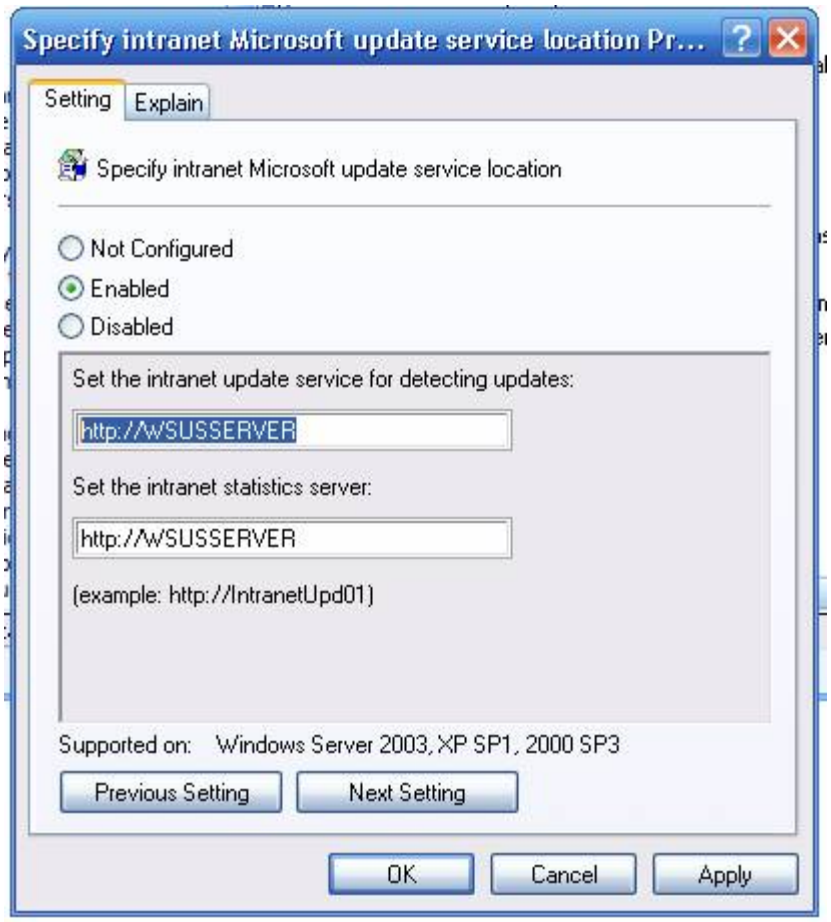
Configure on Windows Server 2008

1. On “Select Update Source” screen, check “Store updates locally” (ensure you have enough space to store large amounts of updates)
2. Use existing SQL 2005 Server or choose Windows Internal Database
3. Use the existing IIS site, click Next
4. Click Finish

Now you can further configure WSUS by using WSUS MMC. WSUS MMC can be accessed from Administrative Tools or Server manager.

Configure Automatic Update client via Group Policy
Use Group Policy to configure Automatic Update client to download from WSUS server.

1. Create a new Domain Policy on Computers OU
2. Expand to Computer Configuration>Administrative Templates>Windows Components>Windows Update
3. Click on “Configure Automatic Updates setting”, here configure Automatic Updates as you desire. Click OK
4. Click on “Specify intranet Microsoft update service location”, choose “Enabled ”, Configure intranet server in this format: http://WSUSSERVER
5. Once this Group Policy is propagated to the clients, clients will start to download from the WSUS server



Pros and Cons of Server 2008 SSTP VPN

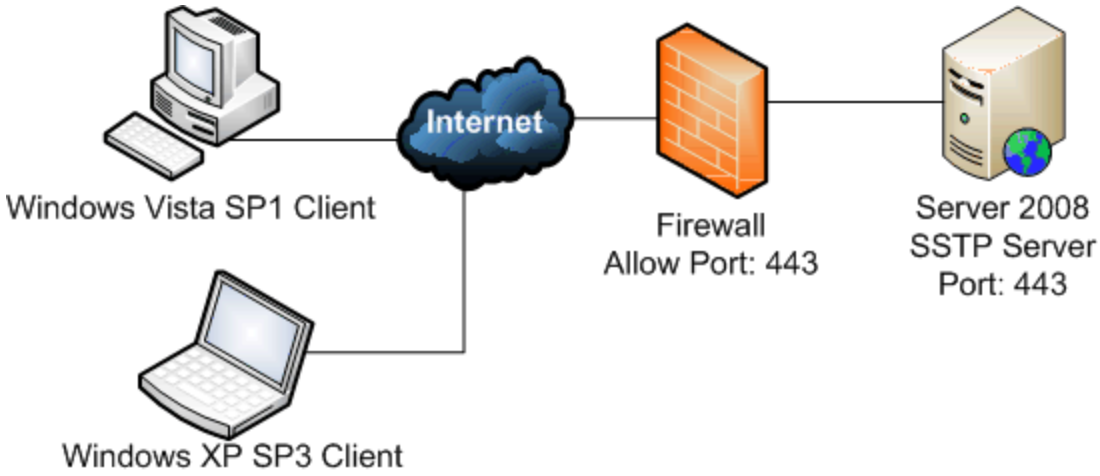
Windows Server 2008 includes support for new SSTP protocol. It allows clients to connect to corporate VPN overcoming many technical difficulties that's in PPTP and L2TP/IPSec.

Pros of SSTP VPN

SSTP VPN allows users to connect from anywhere. The advantage of SSTP VPN is that it only uses port 443 which is allowed by most firewalls. The predecessor PPTP had issues because a lot of corporation firewalls do not GRE traffic to pass through. SSTP VPN is perfect for Sales employees and executives who travel a lot that needs VPN connectivity from anywhere.

Cons of SSTP VPN

Since SSTP is SSL based, you will want to buy a Certificate from external CA such as Verisign. Also SSTP VPN Server must be Server 2008 and SSTP VPN Clients must be Windows XP SP3 and later or Windows Vista SP1 and later.



VPN Protocol	Protocol	Port	Description
SSTP	TCP	443	Allows VPN traffic via HTTPS to and from RRAS Server
PPTP	TCP	1723	PPTP tunnel maintenance traffic to and from RRAS
PPTP	IP	47	PPTP data to and from RRAS Server
L2TP	UDP	500	IKE traffic from and to RRAS Server
L2TP	UDP	4500	IPSec NAT-T traffic from and to RRAS Server
L2TP	IP	50	IPSec ESP traffic from and to RRAS Server

How to compile preconfigured Microsoft VPN Client

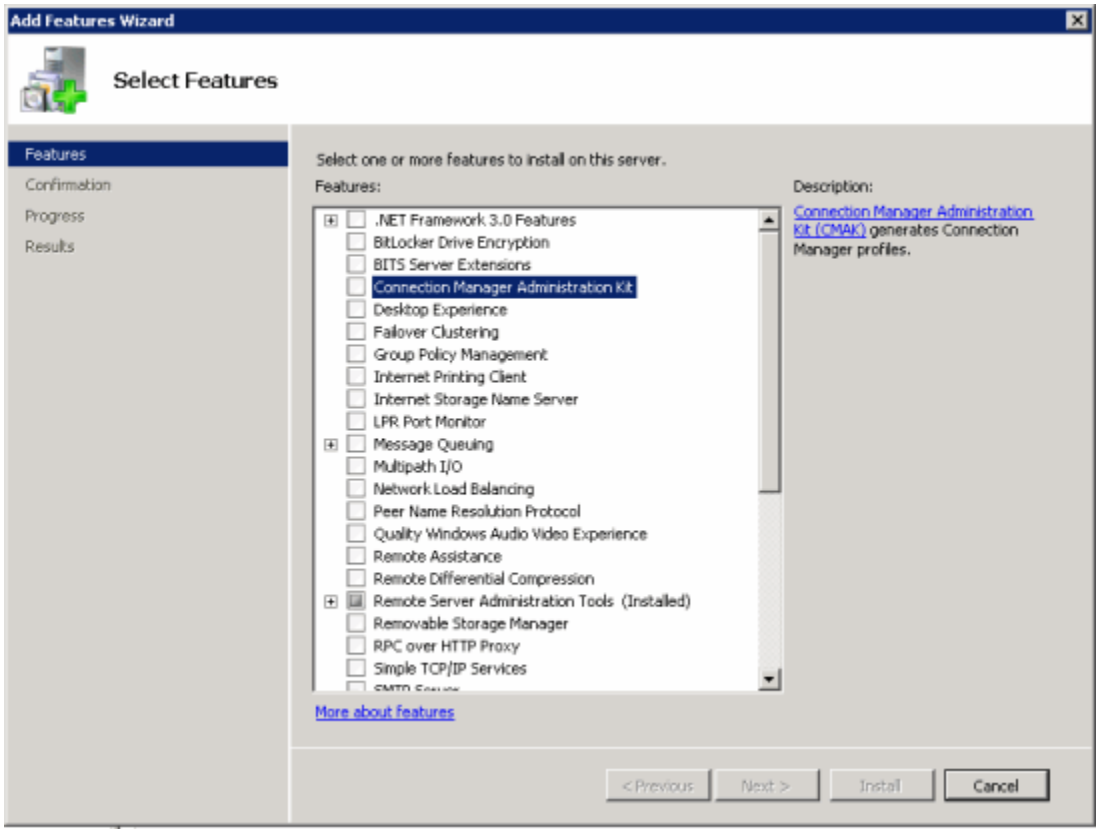
Complied version of the VPN simplifies installation and configuration for the end users. Connection Manager Administration Kit (CMAK) allows IT administrators to reconfigure VPN settings into the VPN client. This eliminate manual configuration of VPN server and other related settings.

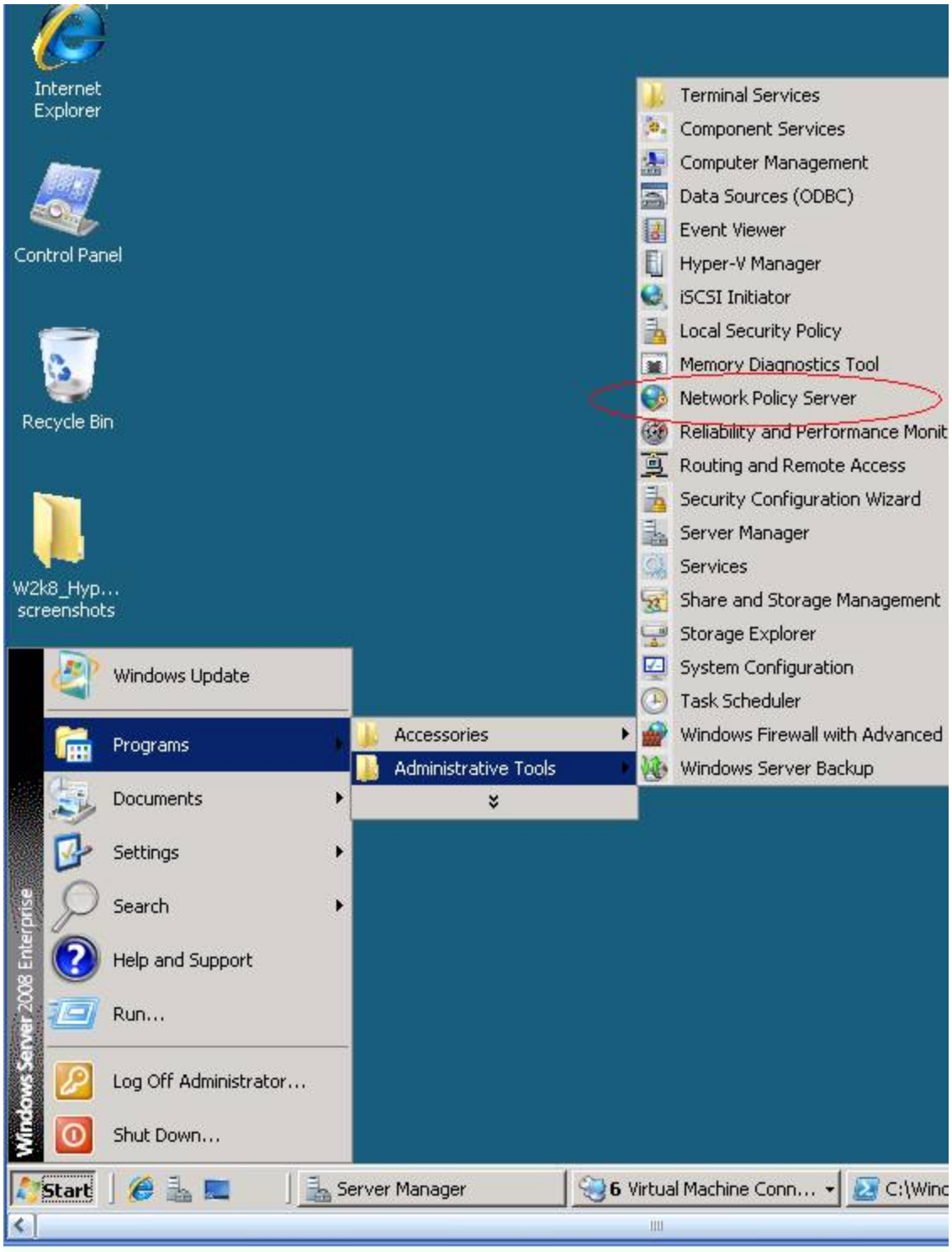
Install Connection Manager Administration Kit (CMAK) on Server 2008

1. Open Server Manager
2. Click “Add Features”
3. Choose “Connection Manager Administration Kit” , click Next

Access Connection Manager Administration Kit (CMAK) on Server 2008

1. Start > Administrative Tools > click Connection Manager Administration Kit




Internet Explorer
Control Panel
Recycle Bin
W2k8_Hyp... screenshots
Terminal Services
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
Hyper-V Manager
iSCSI Initiator
Local Security Policy
Memory Diagnostics Tool
Network Policy Server
Reliability and Performance Monit
Routing and Remote Access
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced
Windows Server Backup
Windows Update
Programs
Documents
Settings
Search
Help and Support
Run...
Log Off Administrator...
Shut Down...
Accessories
Administrative Tools
Windows Server 2008 Enterprise
Start
Server Manager
6 Virtual Machine Conn...
C:\Winc