What is an Active Directory (AD)?

The Microsoft Windows 2003 Active Directory glossary defines an Active Directory as "a structure supported by Windows 2003 that lets any object on a network be tracked and located. Active Directory is the directory service used in Windows 2003 Server and provides the foundation for Windows 2003 distributed networks." A directory service "provides the methods for storing directory data and making this data available to network users and administrators. For example, Active Directory stores information about user accounts, such as names, phone numbers, and so on, and enables other authorized users on the same network to access this information."

The AD, or Active Directory, is a database based on the LDAP (Lightweight Directory Access Protocol) standard, which makes the information contained within the AD easily available to other applications across different platforms. The AD contains user accounts, computer accounts, organizational units, security groups, and group policy object - all of which have a unique name and a unique path. All unique objects in the AD use a domain contained within the AD as a means of authentication.

What is a domain?

The Microsoft Windows 2003 Active Directory glossary defines a domain as "a single security boundary of a Windows NT-based computer network. Active Directory is made up of one or more domains. On a standalone workstation, the domain is the computer itself. A domain can span more than one physical location. Every domain has its own security policies and security relationships with other domains. When multiple domains are connected by trust relationships and share a common schema, configuration, and global catalog, they constitute a domain tree. Multiple domain trees can be connected together to create a forest."

What is a tree?

The Microsoft Windows 2003 Active Directory glossary defines a tree as "a set of Windows NT domains connected together through transitive, bidirectional trust, sharing a common schema, configuration, and global catalog. The domains must form a contiguous hierarchical namespace such that if a.com is the root of the tree, b.a.com is a child of a.com, c.b.a.com is a child of b.a.com, and so on."

What is a forest?

The Microsoft Windows 2003 Active Directory glossary defines a forest as "a group of one or more Active Directory trees that trust each other. All trees in a forest share a common schema, configuration, and global catalog. When a forest contains multiple trees, the trees do not form a contiguous namespace. All trees in a given forest trust each other through transitive bidirectional trust relationships. Unlike a tree, a forest does not need a distinct name. A forest exists as a set of cross-referenced objects and trust relationships known to the member trees. Trees in a forest form a hierarchy for the purposes of trust."

What is a schema?

The Microsoft Windows 2003 Active Directory glossary defines a schema as "the definition of an entire database; the universe of objects that can be stored in the directory is defined in

the schema. For each object class, the schema defines what attributes an instance of the class must have, what additional attributes it may have, and what object class can be a parent of the current object base."

What is a global catalog (GC)?

The Microsoft Windows 2003 Active Directory glossary defines a global catalog (GC) as "the global catalog contains a partial replica of every Windows 2003 domain in the directory. The GC lets users and applications find objects in an Active Directory domain tree given one or more attributes of the target object. It also contains the schema and configuration of directory partitions. This means the global catalog holds a replica of every object in the Active Directory, but with only a small number of their attributes. The attributes in the global catalog are those most frequently used in search operations (such as a user's first and last names, logon names, and so on), and those required to locate a full replica of the object. The GC allows users to find objects of interest quickly without knowing what domain holds them and without requiring a contiguous extended namespace in the enterprise. The global catalog is built automatically by the Active Directory replication system."

What is an organizational unit (OU)?

The Microsoft Windows 2003 Active Directory glossary defines an organizational unit as "a container object that is an Active Directory administrative partition. OUs can contain users, groups, resources, and other OUs. Organizational Units enable the delegation of administration to distinct subtrees of the directory."

What is a group policy?

The Microsoft Windows 2003 Active Directory glossary states that a group policy "refers to applying policy to groups of computers and/or users contained within Active Directory containers. The type of policy includes not only registry-based policy found in Windows NT Server 4.0, but is enabled by Directory Services to store many types of policy data, for example: file deployment, application deployment, logon/logoff scripts and startup/shutdown scripts, domain security, Internet Protocol security (IPSec), and so on. The collections of policies are referred to as Group Policy objects (GPOs)."

A group policy object (GPO) is defined as "a virtual collection of policies. It is given a unique name, such as a globally unique identifier (GUID). GPOs store group policy settings in two locations: a Group Policy container (GPC) (preferred) and a Group Policy template (GPT). The GPC is an Active Directory object that stores version information, status information, and other policy information (for example, application objects). The GPT is used for file-based data and stores software policy, script, and deployment information. The GPT is located on the system volume folder of the domain controller. A GPO can be associated with one or more Active Directory containers, such as a site, domain, or organizational unit. Multiple containers can be associated with the same GPO, and a single container can have more than one associated GPO."

A GPO is broken into two major sections, the Computer Configuration and the User Configuration. The Computer Configuration holds policies that are relevant only to the machine itself. The Computer Configuration can control printers, network settings, Startup and Shutdown scripts. One of the more useful policies based under the Computer Configuration setting is the loopback policy, which allows User Configurations policies to be applied to a computer, regardless of the user (unless the user is denied the GPO). Under the

User Configuration, logon and logoff scripts can be configured, folders can be redirected, and security settings can be tweaked.

What is an access control list (ACL)?

The Microsoft Windows 2003 Active Directory glossary defines an access control list as "a set of data associated with a file, directory, or other resource that defines the permissions that users and/or groups have for accessing it. In the Active Directory™ service, an ACL is a list of access control entries (ACEs) stored with the object it protects. In the Windows NT® operating system, an ACL is stored as a binary value, called a security descriptor."

What is an access control entry (ACE)?

The Microsoft Windows 2003 Active Directory glossary states that "each ACE contains a security identifier (SID), which identifies the principal (user or group) to whom the ACE applies, and information on what type of access the ACE grants or denies."

P01 - Can we add a Server within Windows Server 2003 in a 2000 Domain ?

Yes, DC under Windows Server 2000 and Windows Server 2003 can cohexist.

Before doing this you have to prepare the AD schema ,with adprep /forestprep

P02 - How to name an AD domain ?

The rules are mainly given from DNS : acceptable naming conventions for domain names include the use of alphanumeric characters (the letters A through Z and numerals 0 through 9) and the hyphen (-). A period (.) in a domain name is always used to separate the discrete parts of a domain name commonly known as labels. Each domain label can be no longer than 63 bytes. The first label may not be a number.

Extra restrictions must be considered :

_ If you want that the NetBIOS domain name corresponding to your domain reman simple, use less than 15 characters.
_ don't use the same domain that you use on the internet, but in order to avoid that it happens after, book the domain you use internaly on the internet
_ don't use the prefixe .local

Q01 - How to create a forest with a domain ?

1. Click Start, Run, and type dcpromo.
2. On the Welcome page, click Next.
3. On the Operating System Compatibility page, click Next.
4. On the Domain Controller Type page, click Domain controller for a new domain and click Next.
5. On the Create New Domain page, click Domain in a new forest and click Next.
6. Type the full DNS name for the new domain and click Next.
7. Verify the NetBIOS name and click Next.
8. Specify a location and click Next.

9. Choose a location and click Next.
10. Verify an existing DNS server or click Install and configure…, and then click Next.
11. Specify whether or not to assign default permissions.
12. When prompted, specify a password.
13. Review the Summary page, and click Next.
14. When prompted, restart the computer.

Q02 - How to add a DC (Domain Controler) to an existing domain ?

1. Run dcpromo.
2. On the Domain Controller Type page, select the Additional domain controller for an existing domain checkbox.
3. On the Network Credentials page, type the user name, password, and user domain.
4. On the Database and Log Folders page, type the location in which you want to install the database and log folders, or click Browse.
5. On the Shared System Volume page, type the location in which you want to install the SYSVOL folder, or click Browse.
6. On the Directory Services Restore Mode Administrator Password page, type and confirm the Directory Services Restore Mode password and click Next.
7. Review the Summary page, and then click Next.
8. When prompted, restart the computer.

Q03 - How to rename a Domain Controler ?

1. In the Control Panel, double-click System.
2. In the System Properties dialog box click Change.
3. When prompted, confirm that you want to rename the domain controller.
4. Enter the full computer name and click OK.

Q04 - How to delete (remove from domain) a Domain Controler ?

Delete a DC :
To remove a domain controller that is online and is no longer required:
1. Open the Active Directory Installation Wizard (Run dcpromo).
2. On the Remove Active Directory page select the This server is the last domain controller in the domain check box, and then click Next.
3. On the Administrator Password page type your new administrator password, and then click Next.
4. On the Summary page, review the summary, and then click Next.

To remove a domain controller that is damaged and cannot be started from Active Directory:
In this case, you have to use ntdsutil , read the
http://support.microsoft.com/default.aspx?scid=kb;en-us;216498

Q05 - How to check the correct initialisation of Active Directory ?

After you have performed an upgrade, you can verify the promotion of a server to a domain controller by verifying the following items.

- **Default Containers**
  These are created automatically when the first domain is created. Open the Active Directory Users and Computers Microsoft Management Console (MMC), and then verify that the following containers appear here: Computers, Users, ForeignSecurityPrincipals

- **Default Domain Controllers Organizational Unit**
  Open Active Directory Users and Computers, and then verify that this organizational unit appears here.

- **Default-First-Site-Name**
  You can verify this item by using Active Directory Sites and Services.

- **Active Directory Database**
  Your Ntds.dit file is the Active Directory database. Verify that it resides in the %Systemroot%\Ntds folder.

- **Global Catalog Server**

  By default, the first domain controller becomes a global catalog server. To verify this item:

  1. Click **Start**, click **Administrative Tools**, and then click **Active Directory Sites and Services**.
  2. Double-click **Sites**, expand **Servers**, and then select your domain controller.
  3. Double-click the domain controller to expand the server contents.
  4. Below the server, an **NTDS Settings** object is displayed. Right-click the object, and then click **Properties**.
  5. On the **General** tab, make sure that the **Global Catalog** check box is selected (this is the default setting).

- **Root Domain**

  To verify this role, use the net accounts command. The computer role should be "primary" or "backup," depending on whether the computer is the first domain controller in the domain.

- **Shared System Volume**

  A Windows Server 2003 domain controller should have a shared system volume located in the %Systemroot%\Sysvol\Sysvol folder.

- **SRV Resource Records**
  You must have a DNS server installed and configured for Active Directory and the associated client software to function correctly. Use the DNS Manager MMC snap-in to verify that the correct zones and resource records are created for each DNS zone. Active Directory creates its SRV RRs in the following folders:
    - _Msdcs/Dc/_Sites/Default-first-site-name/_Tcp
    - _Msdcs/Dc/_Tcp

  In these locations, an SRV RR is displayed for the following services:

    - _kerberos
    - _ldap

Q06 - How to create a child domain ?

You can't use a DC which manage the root domain as DC for a child domain, setup a new server and then follow the instructions :
1. Run dcpromo.
2. On the Domain Controller Type page, Click Child domain in an existing domain tree.
3. Type the user name, password, and user domain of the user account you want to use.
4. Verify the parent domain, and then type the new child domain name.

Q07 - How to create a new tree ? -

1. Run dcpromo.
2. On the Domain Controller Type page, click Domain tree in an existing forest.
3. Type the user name, password, and user domain of the user account you want to use.
4. Type the full DNS name for the new domain.

Q10 - How to Determine the RID, PDC, and Infrastructure FSMO Holders of a Selected Domain ?

1. Click **Start**, click **Run**, type dsa.msc, and then click **OK**.
2. Right-click the selected Domain Object in the top left pane, and then click **Operations Masters**.
3. Click the **PDC** tab to view the server holding the PDC master role.
4. Click the **Infrastructure** tab to view the server holding the Infrastructure master role.
5. Click the **RID Pool** tab to view the server holding the RID master role.

Q11 - How to Determine the Schema FSMO Holder in a Forest ? -

1. Click **Start**, click **Run**, type mmc, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, click **Add**, double-click **Active Directory Schema**, click **Close**, and then click **OK**.
3. Right-click **Active Directory Schema** in the top left pane, and then click **Operations Masters** to view the server holding the schema master rle.

Q12 - How to create a trust relationship beetween two forest ? - to

1. Open Active Directory Domains and Trusts.
2. Click Properties for forest root domain shortcut trust domain, external trust domain, or realm trust domain.
3. Click New Trust, then Next, on the Trust tab.
4. Click Next on the Welcome page.
5. Type DNS name on the appropriate Trust Name page and click Next.
6. Select the desired trust type on the Trust Type Page and click Next.
7. Select the desired trust direction on the Direction of Trust page,then follow wizard instructions.

Q13 - How to check trust relationships ? -

Using Active Directory Domains and Trusts:
1. Right-click the desired domain and click Properties.
2. Click the desired trust, then click Properties.
3. Click Validate, click No, do not….
4. Repeat steps 1 through 3 for the other domain in the relationship.

Using netdom:

NETDOM TRUST trusting_domain_name /Domain:trusted_domain_name /Verify

Q14 - How to delete trust relationships ? -

Using Active Directory Domains and Trusts:
1. Right-click the desired domain and click Properties.
2. Click the desires trust, then click Remove.
3. Repeat steps 1 and 2 for the other domain in the relationship.

Q15 - How to Create and Configure Sites and Subnets ?

To use sites to manage replication between sites, you create additional sites and subnets and delegate control of sites. Creating a site involves providing a name for the new site and associating the site with a site link. To create sites, you must log on as a member of the Enterprise Admins group or the Domain Admins group in the forest root domain.

To create a site, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu.
2. In the console tree, right-click **Sites**, and then click **New Site**.
3. In the **Name** box, type the name of the new site.
4. Click a site link object, and then click **OK** twice.

To create a subnet object, perform the following steps:

1. In Active Directory Sites and Services, in the console tree, double-click **Sites**, right-click **Subnets**, and then click **New Subnet**.
2. In the **Address** box, type the subnet IP address.
3. In the **Mask** box, type the subnet mask that describes the range of addresses for the subnet.
4. Select a site to associate the subnet with, and then click **OK**.

To associate a site with a subnet object, perform the following steps:

1. In Active Directory Sites and Services, expand **Sites**, expand **Subnets**, and then in the console tree, right-click the subnet that you want to associate the site with, and then click **Properties**.

2. On the **General** page, in the **Site** box, click the site that you want to associate with this subnet, and then click **OK**.

Q16 - How to move a DC to a different site ?

To move a domain controller to a different site, perform the following steps:

1. In Active Directory Sites and Services, expand **Sites**, expand the site that the domain controller is in, expand **Servers**, and then in the console tree, right-click the domain controller, and then click **Move**.
2. In the **Move Server** dialog box, in the **Site Name** list, select the site that you want to move the domain controller to, and then click **OK**.

Q17 - How to Create and Configure Site Links ?

You create site links in Active Directory to map connections between two or more sites. When you configure site links, you can define the site link properties, which include the cost, replication interval, schedule, and sites that the link is associated with.
To create a site link, perform the following steps:

1. In Active Directory Sites and Services, expand **Sites**, expand **Inter-Site Transports**, right-click **IP** or **SMTP**, depending on which protocol the site link you will use, and then click **New Site Link**.
2. In the **Name** box, type a name for the link.
3. Click two or more sites to connect, click **Add**, and then click **OK**.

To configure site links, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand **Inter-Site Transports**, and then click **IP** or **SMTP**, depending on which protocol the site link is configured to use.
2. Right-click the site link, and then click **Properties**.
3. On the **General** page of the **Properties** dialog box, change the values for site associations, cost, replication interval, and schedule as required, and then click **OK**.
4. Perform one of the following as appropriate:
   - In the **Sites not in this site link** box, click the site you want to add, and then click **Add**.
   - In the **Sites in this site link** box, click the site you want removed and then click **Remove**.
   - In the **Cost** box, enter a value for the cost of replication.
5. Click **Change Schedule**, select the block of time you want to schedule, and then click either **Replication Not Available** or **Replication Available**, and then click **OK**.

If you want to Create a Site Link Bridge
Before you can create new site link bridges, you must first disable default bridging of all site links to permit the creation of new site link bridges.
To disable default bridging of all site links, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand **Inter-Site Transports**, right-click either **IP** or **SMTP**, depending on the protocol for which you want to disable bridging of all site links, and then click **Properties**.
2. In the **Properties** dialog box, clear the **Bridge all site links** check box, and then click **OK**.

To create a site link bridge, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand **Inter-Site Transports**, right-click either **IP** or **SMTP**, depending on the protocol that

you want to create a site link bridge for, and then click **New Site Link Bridge**.
2. In the **Name** box, type a name for the site link bridge.
3. Click two or more site links to be bridged, click **Add**, and then click **OK**.

Q18 - How to Manage a Site Topology ?

How to Manage a Site Topology ?

To create a preferred bridgehead server, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand the site that contains the server that you want to configure, expand **Servers**, and then in the console tree, right-click the domain controller that you want to make a preferred bridgehead server, and then click **Properties**.
2. Choose the intersite transport or transports to designate the computer a preferred bridgehead server, click **Add**, and then click **OK**.

To determine the domain controller that holds the role of the intersite topology generator in the site, perform the following steps:

1. In Active Directory Sites and Services, expand **Sites**, and then select the site.
2. In the details pane, right-click **NTDS Site Settings**, and then click **Properties**.

To force the KCC to run, perform the following steps:

1. In Active Directory Sites and Services, in the console tree, expand **Sites**, expand the site that contains the server on which you want to run the KCC, expand **Servers**, and then select the server object for the domain controller that you want to run the KCC on.
2. In the details pane, right-click **NTDS Settings**, click **All Tasks**, and then click **Check Replication Topology**.

You use the Active Directory Sites and Services to force replication over a connection. You may be required to force replication if the event log displays replication inconsistencies or if you receive a message on the domain controller console alerting you to replication problems. To force replication over a connection, perform the following steps:

1. In Active Directory Sites and Services, expand the domain controller for the site that contains the connection that you use to replicate directory information.
2. In the console tree, click **NTDS Settings**.
3. In the details pane, right-click the connection that you use to replicate directory information, and then click **Replicate Now**.

Q19 - How to Transfer the Schema Master Role ?

Use the Active Directory Schema Master snap-in to transfer the schema master role.

1. Click **Start**, click **Run**, type mmc in the **Open** box, and then click **OK**.
2. On the **File**, menu click **Add/Remove Snap-in**.
3. Click **Add**.
4. Click **Active Directory Schema**, click **Add**, click **Close**, and then click **OK**.
5. In the console tree, right-click **Active Directory Schema**, and then click **Change Domain Controller**.
6. Click **Specify Name**, type the name of the domain controller that will be the new role holder, and then click **OK**.
7. In the console tree, right-click **Active Directory Schema**, and then click **Operations Master**.

8. Click **Change**.
9. Click **OK** to confirm that you want to transfer the role, and then click **Close**.

Q20 - How to transfer the Domain Naming Master Role ?

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. Right-click **Active Directory Domains and Trusts**, and then click **Connect to Domain Controller**.

   NOTE: You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.
3. Do one of the following:
   - In the **Enter the name of another domain controller** box, type the name of the domain controller that will be the new role holder, and then click **OK**.

     -or-
   - In the **Or, select an available domain controller** list, click the domain controller that will be the new role holder, and then click **OK**.
4. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Operations Master**.
5. Click **Change**.
6. Click **OK** to confirm that you want to transfer the role, and then click **Close**.

Q21 - How to Transfer the RID Master, PDC Emulator, and Infrastructure Master Roles ?

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click **Active Directory Users and Computers**, and then click **Connect to Domain Controller**.

   NOTE: You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.
3. Do one of the following:
   - In the **Enter the name of another domain controller** box, type the name of the domain controller that will be the new role holder, and then click **OK**.

     -or-
   - In the **Or, select an available domain controller** list, click the domain controller that will be the new role holder, and then click **OK**.
4. In the console tree, right-click **Active Directory Users and Computers**, point to **All Tasks**, and then click **Operations Master**.
5. Click the appropriate tab for the role that you want to transfer (**RID**, **PDC**, or **Infrastructure**), and then click **Change**.
6. Click **OK** to confirm that you want to transfer the role, and then click **Close**.

Q22 - How to backup AD ?

AD is backed Up when you save the System State on a DC with the Backup accessory.

1. Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. Click the **Backup** tab.
3. Click to select the **System State** check box. (All of the components to be backed up are listed in the right pane. You cannot individually select each item.)

   NOTE: During the system state backup, you must select to back up the Winnt\Sysvol folder. You must also select this option during the restore operation to have a working sysvol after the recovery.

The following information applies only to domain controllers. You can restore member servers the same way, but in normal mode.

If any of the following conditions are not met, the system state is not restored. Backup attempts to restore the system state, but does not succeed.

- The drive letter on which the %SystemRoot% folder is located must be the same as when it was backed up.
- The %SystemRoot% folder must be the same folder as when it was backed up.
- If sysvol or other Active Directory databases were located on another volume, they must exist and have the same drive letters also. The size of the volume does not matter.

Q23 - How to restore AD ?

There is different methods, depending with the state of your AD :
Normal : if you have lost only one DC, you have to restore DC and then datas
Authoritative : with many DCs, you can restaure whatever you want and select it.

How to Perform a Normal Restore
To perform a primary restore, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate permissions. If the computer is in a domain, members of the Domain Admins group can perform this procedure.
To perform a primary restore of Active Directory, perform the following steps:

1. Restart your domain controller in Directory Services Restore Mode.
2. Start the Backup utility.
3. On the **Welcome to the Backup or Restore Wizard** page, click **Advanced Mode**.
4. On the **Welcome to Backup Utility Advanced Mode** page, on the **Restore and Manage Media** tab, select what you want to restore, and then click **Start Restore**.
5. In the **Warning** dialog box, click **OK**.
6. In the **Confirm Restore** dialog box, click **Advanced**.
7. In the **Advanced Restore Options** dialog box, click **When restoring replicated data sets, mark the restored data as the primary data for all replicas**, and then click **OK** twice.
   Important
   Selecting this option ensures that the File Replication Service (FRS) data is

replicated to the other servers. Select this option only when you want to restore the first replica set to the network.
8. In the **Restore Progress** dialog box, click **Close**.
9. In the **Backup Utility** dialog box, click **Yes**.

Warning
When you restore the system state data, the Backup utility erases the system state data that is on your computer and replaces it with the system state data that you are restoring, including system state data that is not related to Active Directory. Depending on how old the system state data is, you may lose configuration changes that you recently made to the computer. To minimize this risk, back up the system state data regularly.

How to Perform an Authoritative Restore
Unlike a normal restore, an authoritative restore requires the use of a separate command-line tool, Ntdsutil. No backup utilities, including the Windows Server 2003 system utilities, can perform an authoritative restore.
To perform an authoritative restore, perform the following steps:

1. Restart your domain controller in Directory Services Restore Mode.
2. Restore Active Directory to its original location.
3. If you must perform an authoritative restore on the SYSVOL folder, restore Active Directory to an alternate location by using the Backup utility, but do not restart the computer when prompted after the restore. If you are not performing an authoritative restore on SYSVOL, skip to step 4.
4. At the command prompt, run **Ntdsutil.exe**.
5. At the **ntdsutil** prompt, type **authoritative restore**.
6. At the authoritative restore prompt, type **.restore subtree** *distinguished_name_of_object* (where *distinguished_name_of_object* is the distinguished name, or path, to the object).
   For example, to restore an organizational unit called Sales, which existed directly below the domain called contoso.msft, type **.restore subtree OU=Sales,DC=contoso,DC=msft**.
7. Type **quit** and then press ENTER.
8. Type **quit** again, and then press ENTER to exit ntdsutil.
9. Restart the domain controller.
10. After FRS publishes the SYSVOL folder, copy the SYSVOL folder and only those Group Policy folders that correspond to the restored Group Policy objects from the alternate location to the existing locations.

To verify that the copy operation was successful, examine the contents of the SYSVOL*Domain* folder, where *Domain* is the name of the domain.

Q30 - How to Delegate Administrative Control for Managing Group Policy Links ?

You can delegate the ability to manage Group Policy links by selecting Manage Group Policy links in the Delegation of Control Wizard to enable a user to link and unlink GPOs.
To delegate administrative control for managing Group Policy links, perform the following steps:

1. Open Group Policy Management.
2. Browse to the forest and domain in which you want to delegate administrative control for managing Group Policy links, and then click the link.
3. In the details pane, on the Delegation tab, click Add.
4. In the Select User, Computer, or Group dialog box, in the Enter the object name to select (examples) box, type the security principal, click Check Names, and then click OK.

5. In the Add Group or User dialog box, in the Permissions box, select the appropriate permission, and then click OK.

If you prefer the flexibility of the Properties dialog box, it is still available in Group Policy Management by clicking Advanced on the Delegation tab.

Q31 - How to Delegate Administrative Control for Creating and Editing GPOs

You use the Delegation of Control Wizard to delegate administrative control to create and edit GPOs.

To delegate administrative control for creating GPOs, perform the following steps:

1. Open Group Policy Management.
2. Browse to the forest and domain in which you want to delegate administrative control for creating GPOs, and then click Group Policy Objects.
3. In the details pane, on the Delegation tab, click Add.
4. In the Select User, Computer, or Group dialog box, in the Enter the object name to select (examples) box, type the security principal, click Check Names, and then click OK.

To delegate administrative control for editing GPOs, perform the following steps:

1. Open Group Policy Management.
2. Browse to the forest and domain in which you want to delegate administrative control for editing GPOs, and then click the link.
3. In the details pane, on the Delegation tab, click Add.
4. In the Select User, Computer, or Group dialog box, in the Enter the object name to select (examples) box, type the security principal, click Check Names, and then click OK.
5. In the Add Group or User dialog box, in the Permissions box, select the appropriate permission, and then click OK.

Q50 - I can't add another DC to the AD Domain. What can I check ?

Steps for fixing the problem when DCPROMO does not find the domain.

1. Verify that the existing domain controller is pointing to a Windows 2000 DNS server. Do not point it to any external ISP DNS servers.

2. Open the DNS MMC, double click forwarders so that you can see the zone for your domain.

3. Right click on this zone and select properties. Verify that your zone is set to allow dynamic updates, if not change it so that it does.

4. Double click your zone to expand it. You should have 4 subfolders (_MSDCS, _SITES, _TCP, _UDP) and a few records.

5. If the zones do not exist you should open a command prompt.

6. Type IPconfig /registerdns and enter

7. Type net stop netlogon

8. Type net start netlogon (restarting netlogon will force the service to register its SRV records with the DNS zone thus create the missing subfolders. The records that will be registered are in winnt\system32\config\netlogon.dns).

9. After restarting netlogon go back into your DNS zone and verify that you have the subfolders that were mentioned in 4. above.

10. If the folders are not there you may want to try running netdiag.exe /fix from the support tools. Or try restarting netlogon again.

11. On the DC that you are trying to promote verify that it is pointing to the Windows 2000 DNS server that we have been working on for DNS.