



**Vendor: Microsoft**

**Exam Code: 70-640**

**Exam Name: TS: Windows Server 2008 Active Directory,  
Configuring**

**Version: Demo**

## QUESTION 1

Your company, Contoso Ltd, has offices in North America and Europe. Contoso has an Active Directory forest that has three domains.

You need to reduce the time required to authenticate users from the labs.eu.contoso.com domain when they access resources in the eng.na.contoso.com domain.

What should you do?

- A. Decrease the replication interval for all Connection objects.
- B. Decrease the replication interval for the DEFAULTIPSITELINK site link.
- C. Set up a one-way shortcut trust from eng.na.contoso.com to labs.eu.contoso.com.
- D. Set up a one-way shortcut trust from labs.eu.contoso.com to eng.na.contoso.com.

**Correct Answer: C**

### Explanation:

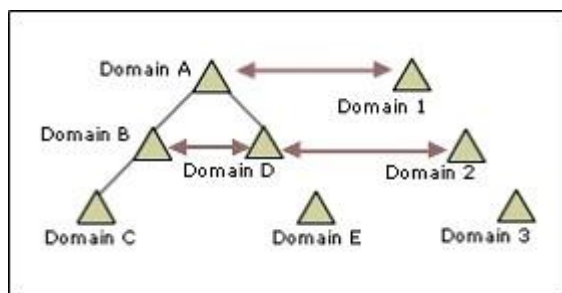
<http://technet.microsoft.com/en-us/library/cc754538.aspx>

Understanding When to Create a Shortcut Trust

When to create a shortcut trust

Shortcut trusts are one-way or two-way, transitive trusts that administrators can use to optimize the authentication process.

Authentication requests must first travel a trust path between domain trees. In a complex forest this can take time, which you can reduce with shortcut trusts. A trust path is the series of domain trust relationships that authentication requests must traverse between any two domains. Shortcut trusts effectively shorten the path that authentication requests travel between domains that are located in two separate domain trees. Shortcut trusts are necessary when many users in a domain regularly log on to other domains in a forest. Using the following illustration as an example, you can form a shortcut trust between domain B and domain D, between domain A and domain 1, and so on.



Using one-way trusts

A one-way, shortcut trust that is established between two domains in separate domain trees can reduce the time that is necessary to fulfill authentication requests--but in only one direction. For example, when a oneway, shortcut trust is established between domain A and domain B, authentication requests that are made in domain A to domain B can use the new

one-way trust path. However, authentication requests that are made in domain B to domain A must still travel the longer trust path.

Using two-way trusts

A two-way, shortcut trust that is established between two domains in separate domain trees reduces the time that is necessary to fulfill authentication requests that originate in either domain. For example, when a two-way trust is established between domain A and domain B, authentication requests that are made from either domain to the other domain can use the new, two-way trust path.

## QUESTION 2

You are installing an application on a computer that runs Windows Server 2008 R2.

During installation, the application will need to install new attributes and classes to the Active Directory database.

You need to ensure that you can install the application.

What should you do?

- A. Change the functional level of the forest to Windows Server 2008 R2.
- B. Log on by using an account that has Server Operator rights.
- C. Log on by using an account that has Schema Administrator rights and the appropriate rights to install the application.
- D. Log on by using an account that has the Enterprise Administrator rights and the appropriate rights to install the application.

**Correct Answer: C**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc756898%28v=ws.10%29.aspx>

Default groups

Default groups, such as the Domain Admins group, are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and delegate specific domain-wide administrative roles.

Groups in the Builtin container

The following table provides descriptions of the default groups located in the Builtin container and lists the assigned user rights for each group.

Group	Description	Default user rights
Server Operators	On domain controllers, members of this group can log on interactively, create and delete shared resources, start and stop some services, back up and restore files, format the hard disk, and shut down the computer. This group has no default members. Because this group has significant power on domain controllers, add users with caution.	Back up files and directories; Change the system time; Force shutdown from a remote system; Allow log on locally; Restore files and directories; Shut down the system.

### Groups in the Users container

The following table provides a description of the default groups located in the Users container and lists the assigned user rights for each group.

Group	Description	Default user rights
Schema Admins (only appears in the forest root domain)	Members of this group can modify the Active Directory schema. By default, the Administrator account is a member of this group. Because this group has significant power in the forest, add users with caution.	No default user rights.
Enterprise Admins (only appears in the forest root domain)	Members of this group have full control of all domains in the forest. By default, this group is a member of the Administrators group on all domain controllers in the forest. By default, the Administrator account is a member of this group. Because this group has full control of the forest, add users with caution.	Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.

### QUESTION 3

You have two servers named Server1 and Server2. Both servers run Windows Server 2008 R2. Server1 is configured as an enterprise root certification authority (CA).

You install the Online Responder role service on Server2.

You need to configure Server1 to support the Online Responder.

What should you do?

- A. Import the enterprise root CA certificate.
- B. Configure the Certificate Revocation List Distribution Point extension.
- C. Configure the Authority Information Access (AIA) extension.
- D. Add the Server2 computer account to the CertPublishers group.

**Correct Answer: C**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc732526.aspx>

Configure a CA to Support OCSP Responders

To function properly, an Online Responder must have a valid Online Certificate Status Protocol (OCSP)Response Signing certificate. This OCSP Response Signing certificate is also needed if you are using a non-Microsoft OCSP responder. Configuring a certification

authority (CA) to support OCSP responder services includes the following steps:

1. Configure certificate templates and issuance properties for OCSP Response Signing certificates.
2. Configure enrollment permissions for any computers that will be hosting Online Responders.
3. If this is a Windows Server 2003-based CA, enable the OCSP extension in issued certificates.
4. Add the location of the Online Responder or OCSP responder to the authority information access extension on the CA.
5. Enable the OCSP Response Signing certificate template for the CA.

#### **QUESTION 4**

Your company has an Active Directory domain that runs Windows Server 2008 R2. The Sales OU contains an OU for Computers, an OU for Groups, and an OU for Users.

You perform nightly backups. An administrator deletes the Groups OU.

You need to restore the Groups OU without affecting users and computers in the Sales OU.

What should you do?

- A. Perform an authoritative restore of the Sales OU.
- B. Perform a non-authoritative restore of the Sales OU.
- C. Perform an authoritative restore of the Groups OU.
- D. Perform a non-authoritative restore of the Groups OU.

**Correct Answer: C**

#### **Explanation:**

<http://technet.microsoft.com/en-us/library/cc816878%28v=ws.10%29.aspx>

#### Performing Authoritative Restore of Active Directory Objects

An authoritative restore process returns a designated, deleted Active Directory object or container of objects to its predeletion state at the time when it was backed up. For example, you might have to perform an authoritative restore if an administrator inadvertently deletes an organizational unit (OU) that contains a large number of users. In most cases, there are two parts to the authoritative restore process: a nonauthoritative restore from backup, followed by an authoritative restore of the deleted objects. If you perform a nonauthoritative restore from backup only, the deleted OU is not restored because the restored domain controller is updated after the restore process to the current status of its replication partners, which have deleted the OU. To recover the deleted OU, after you perform nonauthoritative restore from backup and before allowing replication to occur, you must perform an authoritative restore procedure. During the authoritative restore procedure, you mark the OU as authoritative and let the replication process restore it to all the other domain controllers in the domain. After an

authoritative restore, you also restore group memberships, if necessary.

#### **QUESTION 5**

An Active Directory database is installed on the C volume of a domain controller.

You need to move the Active Directory database to a new volume.

What should you do?

- A. Copy the ntds.dit file to the new volume by using the ROBOCOPY command.
- B. Move the ntds.dit file to the new volume by using Windows Explorer.
- C. Move the ntds.dit file to the new volume by running the Move-item command in Microsoft Windows PowerShell.
- D. Move the ntds.dit file to the new volume by using the Files option in the Ntdsutil utility.

**Correct Answer: D**

#### **Explanation:**

<http://technet.microsoft.com/en-us/library/cc816720%28v=ws.10%29.aspx>

Move the Directory Database and Log Files to a Local Drive

You can use this procedure to move Active Directory database and log files to a local drive.

When you move the files to a folder on the local domain controller, you can move them permanently or temporarily. Move the files to a temporary destination if you need to reformat the original location, or move the files to a permanent location if you have additional disk space. If you reformat the original drive, use the same procedure to move the files back after the reformat is complete. Ntdsutil.exe updates the registry when you move files locally. Even if you are moving the files only temporarily, use Ntdsutil.exe so that the registry is always current.

On a domain controller that is running Windows Server 2008, you do not have to restart the domain controller in Directory Services Restore Mode (DSRM) to move database files. You can stop the Active Directory Domain

Services (AD DS) service and then restart the service after you move the files to their permanent location.

To move the directory database and log files to a local drive:

7. At the ntdsutil prompt, type files, and then press ENTER.
8. To move the database file, at the file maintenance: prompt, use the following commands:

Further information:

<http://servergeeks.wordpress.com/2013/01/01/moving-active-directory-database-and-logs/>  
Moving Active Directory Database and Logs

Step 1

Start the server in Directory Services Restore Mode

Windows Server 2003/2008 Directory Service opens its files in exclusive mode. This means

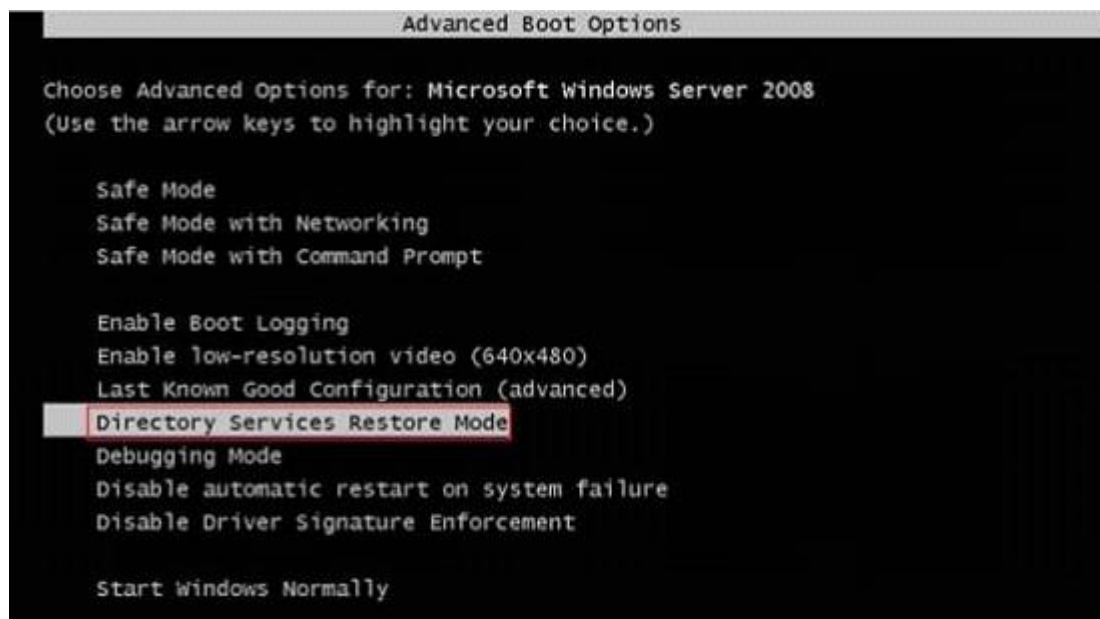
that the files cannot be managed while the server is operating as a domain controller. To perform any files movement related activities using ntdsutil, we need to start the server in Directory Services Restore Mode.

To start the server in Directory Services Restore mode, follow these steps:

Restart the computer.

After the BIOS information is displayed, press F8.

Use the DOWN ARROW to select Directory Services Restore Mode, and then press ENTER.



Log on with your local administrative account and password. (Not Domain Administrative account)



Note: using service control (SC.exe) you can verify quickly ntds services are running or stopped. In command prompt type SC query ntds



```
C:\>sc query ntds
SERVICE_NAME: ntds
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1  STOPPED
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
C:\>_
```

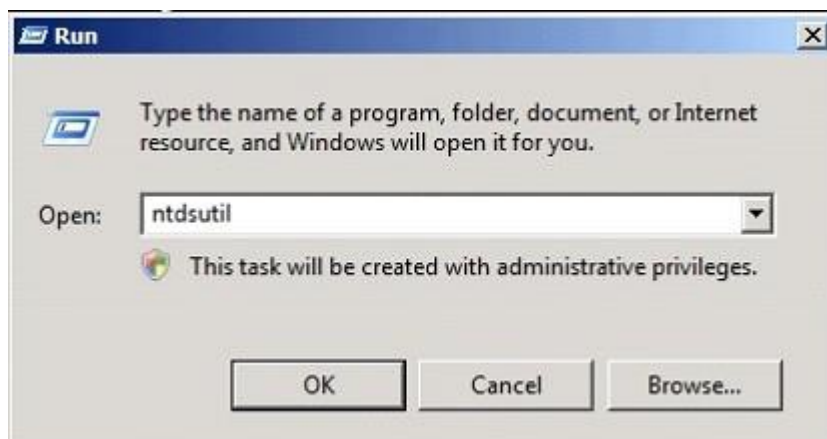
## Step 2

How to Move Active Directory Database and Logs

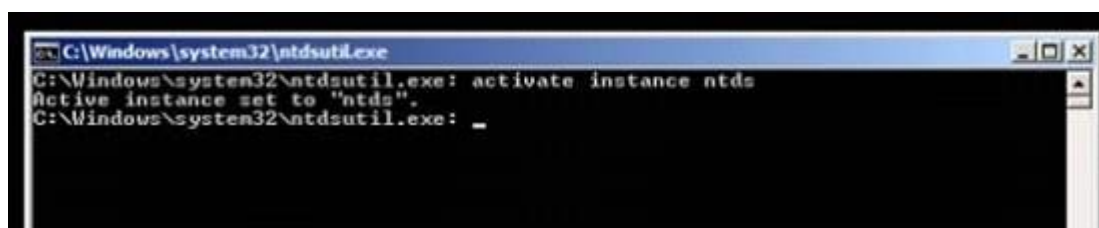
You can move the Ntds.dit data file to a new folder. If you do so, the registry is updated so that Directory

Service uses the new location when you restart the server. To move the data file to another folder, follow these steps:

Click Start, click Run, type ntdsutil in the Open box, and then press ENTER.



At the Ntdsutil command prompt, type activate instance ntds, and then press ENTER.



```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: _
```

At the Ntdsutil command prompt, type files, and then press ENTER.



```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: files
file maintenance:
```

At the file maintenance command prompt, type move DB to <new location> (where new location is an existing folder that you have created for this purpose) and then press ENTER. In this case, the new location for database is C:\AD\Database Now

```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: files
file maintenance: move DB to C:\AD\Database

Successfully updated the backup exclusion key.
Copying NTFS security from C:\Windows\NTDS to C:\AD\Database...
The previous NTDS database location C:\Windows\NTDS\dsadata.bak is unavailable.
The default NTFS security will be applied to NTDS folders.
Default NTFS security on NTDS folders will be set on reboot.
Copying NTFS security from C:\Windows\NTDS to C:\AD\Database...

Drive Information:
    C:\ NTFS <Fixed Drive  > free<119.1 Gb> total<126.9 Gb>

DS Path Information:
    Database      : C:\AD\Database\ntds.dit - 12.1 Mb
    Backup dir    : C:\AD\Database\DSADATA.BAK
    Working dir   : C:\AD\Database
    Log dir       : C:\Windows\NTDS - 40.0 Mb total
                   edbres00002.jrs - 10.0 Mb
                   edbres00001.jrs - 10.0 Mb
                   edb00001.log - 10.0 Mb
                   edb.log - 10.0 Mb

Move database is successful.
Please make a backup immediately else restore will not retain the new file
location.
file maintenance: _
```

Now to move logs , at the file maintenance command prompt, type move logs to <new location> (where new location is an existing folder that you have created for this purpose) and then press ENTER. In our case, the new location for database is C:\AD\Log

```
file maintenance# move logs to C:\AD\
Successfully updated the backup exclu
Copying NTFS security from C:\Windows
Drive Information#
      C:\ NTFS (Fixed Drive) Free
DS Path Information#
      Database      :: C:\AD\Database\
      Backup dir    :: C:\AD\Database\D
      Working dir   :: C:\AD\Database
      Log dir       :: C:\AD\logs - 40.
                       edbres00002.j
                       edbres00001.j
                       edb00001.log
                       edb.log - 10.
If move log files was successful,
please make a backup immediately else
will not retain the new file locatio
file maintenance#
```

To quit file maintenance, type quit. Again to Ntdsutl, type quit to close the prompt Restart the computer. AD database and Logs are moved successfully to new location.

#### QUESTION 6

Your company has a server that runs Windows Server 2008 R2. Active Directory Certificate Services (AD CS) is configured as a standalone Certification Authority (CA) on the server.

You need to audit changes to the CA configuration settings and the CA security settings.

Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Configure auditing in the Certification Authority snap-in.
- B. Enable auditing of successful and failed attempts to change permissions on files in the %SYSTEM32%\CertSrv directory.
- C. Enable auditing of successful and failed attempts to write to files in the %SYSTEM32%\CertLog directory.
- D. Enable the Audit object access setting in the Local Security Policy for the Active Directory Certificate Services (AD CS) server.

**Correct Answer:** AD

#### Explanation:

<http://technet.microsoft.com/en-us/library/cc772451.aspx>

Configure CA Event Auditing

You can audit a variety of events relating to the management and activities of a certification authority (CA):

Back up and restore the CA database.

Change the CA configuration.

Change CA security settings.

Issue and manage certificate requests.

Revoke certificates and publish certificate revocation lists (CRLs).

Store and retrieve archived keys.

Start and stop Active Directory Certificate Services (AD CS).

To configure CA event auditing

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the Action menu, click Properties.
4. On the Auditing tab, click the events that you want to audit, and then click OK.
5. On the Action menu, point to All Tasks, and then click Stop Service.
6. On the Action menu, point to All Tasks, and then click Start Service.

Additional considerations

To audit events, the computer must also be configured for auditing of object access. Audit policy options can be viewed and managed in local or domain Group Policy under Computer Configuration\Windows Settings\Security Settings\Local Policies.

## QUESTION 7

Your company has a single Active Directory domain named intranet.adatum.com. The domain controllers run Windows Server 2008 and the DNS server role. All computers, including non-domain members, dynamically register their DNS records.

You need to configure the intranet.adatum.com zone to allow only domain members to dynamically register DNS records.

What should you do?

- A. Set dynamic updates to Secure Only.
- B. Remove the Authenticated Users group.
- C. Enable zone transfers to Name Servers.
- D. Deny the Everyone group the Create All Child Objects permission.

**Correct Answer: A**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc753751.aspx>

Allow Only Secure Dynamic Updates

Domain Name System (DNS) client computers can use dynamic update to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address.

Dynamic updates can be secure or nonsecure. DNS update security is available only for

zones that are integrated into Active Directory Domain Services (AD DS). After you directory-integrate a zone, access control list (ACL) editing features are available in DNS Manager so that you can add or remove users or groups from the ACL for a specified zone or resource record.

Further information:

<http://technet.microsoft.com/en-us/library/cc771255.aspx>

Understanding Dynamic Update

## QUESTION 8

Your company has an Active Directory domain. All servers run Windows Server.

You deploy a Certification Authority (CA) server.

You create a new global security group named CertIssuers.

You need to ensure that members of the CertIssuers group can issue, approve, and revoke certificates.

What should you do?

- A. Assign the Certificate Manager role to the CertIssuers group
- B. Place CertIssuers group in the Certificate Publisher group
- C. Run the `certsrv -add CertIssuers` command prompt of the certificate server
- D. Run the `add -member-memberbtype memberset CertIssuers` command by using Microsoft Windows Powershell

**Correct Answer: A**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc779954%28v=ws.10%29.aspx>

Role-based administration

Role explanation

Role-based administration involves CA roles, users, and groups. To assign a role to a user or group, you must assign the role's corresponding security permissions, group memberships, or user rights to the user or group.

These security permissions, group memberships, and user rights are used to distinguish which users have which roles. The following table describes the CA roles of role-based administration and the groups relevant to role-based administration.

Roles and groups	Security permission	Description
CA Administrator	Manage CA permission	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate.
Certificate Manager	Issue and Manage Certificates permission	Approve certificate enrollment and revocation requests. This is a CA role. This role is sometimes referred to as CA Officer.
Backup Operator	Back up file and directories and Restore file and directories permissions	Perform system backup and recovery. This is an operating system role.
Auditor	Manage auditing and security log permission	Configure, view, and maintain audit logs. This is an operating system role.
Enrollees	Authenticated Users	Enrollees are clients who are authorized to request certificates from the CA. This is not a CA role.

Certificate Manager:

Delete multiple rows in database (bulk deletion)

Issue and approve certificates

Deny certificates

Revoke certificates

Reactivate certificates placed on hold

Renew certificates

Recover archived key

Read CA database

Read CA configuration information

### QUESTION 9

Your company has a single Active Directory domain named intranet.contoso.com. All domain controllers run Windows Server 2008 R2. The domain functional level is Windows 2000 native and the forest functional level is Windows 2000.

You need to ensure the UPN suffix for contoso.com is available for user accounts.

What should you do first?

- A. Raise the intranet.contoso.com forest functional level to Windows Server 2003 or higher.
- B. Raise the intranet.contoso.com domain functional level to Windows Server 2003 or higher.
- C. Add the new UPN suffix to the forest.
- D. Change the Primary DNS Suffix option in the Default Domain Controllers Group Policy Object (GPO) to contoso.com.

**Correct Answer: C**

**Explanation:**

<http://support.microsoft.com/kb/243629>

HOW TO: Add UPN Suffixes to a Forest

Adding a UPN Suffix to a Forest

Open Active Directory Domains and Trusts.

Right-click Active Directory Domains and Trusts in the Tree window pane, and then click

Properties.

On the UPN Suffixes tab, type the new UPN suffix that you would like to add to the forest. Click Add, and then click OK.

Now when you add users to the forest, you can select the new UPN suffix to complete the user's logon name.

APPLIES TO

Microsoft Windows 2000 Server

Microsoft Windows 2000 Advanced Server

Microsoft Windows 2000 Datacenter Server

### QUESTION 10

You have a Windows Server 2008 R2 Enterprise Root certification authority (CA).

You need to grant members of the Account Operators group the ability to only manage Basic EFS certificates.

You grant the Account Operators group the Issue and Manage Certificates permission on the CA.

Which three tasks should you perform next? (Each correct answer presents part of the solution. Choose three.)

- A. Enable the Restrict Enrollment Agents option on the CA.
- B. Enable the Restrict Certificate Managers option on the CA.
- C. Add the Basic EFS certificate template for the Account Operators group.
- D. Grant the Account Operators group the Manage CA permission on the CA.
- E. Remove all unnecessary certificate templates that are assigned to the Account Operators group.

**Correct Answer:** BCE

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc779954%28v=ws.10%29.aspx>

Role-based administration

Role explanation

Role-based administration involves CA roles, users, and groups. To assign a role to a user or group, you must assign the role's corresponding security permissions, group memberships, or user rights to the user or group.

These security permissions, group memberships, and user rights are used to distinguish which users have which roles. The following table describes the CA roles of role-based administration and the groups relevant to role-based administration.

Roles and groups	Security permission	Description
CA Administrator	Manage CA permission	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate.
Certificate Manager	Issue and Manage Certificates permission	Approve certificate enrollment and revocation requests. This is a CA role. This role is sometimes referred to as CA Officer.
Backup Operator	Back up file and directories and Restore file and directories permissions	Perform system backup and recovery. This is an operating system role.
Auditor	Manage auditing and security log permission	Configure, view, and maintain audit logs. This is an operating system role.
Enrollees	Authenticated Users	Enrollees are clients who are authorized to request certificates from the CA. This is not a CA role.

Certificate Manager:

Delete multiple rows in database (bulk deletion)

Issue and approve certificates

Deny certificates

Revoke certificates

Reactivate certificates placed on hold

Renew certificates

Recover archived key

Read CA database

Read CA configuration information

<http://technet.microsoft.com/en-us/library/cc753372.aspx>

Restrict Certificate Managers

A certificate manager can approve certificate enrollment and revocation requests, issue certificates, and manage certificates. This role can be configured by assigning a user or group the Issue and Manage Certificates permission. When you assign this permission to a user or group, you can further refine their ability to manage certificates by group and by certificate template. For example, you might want to implement a restriction that they can only approve requests or revoke smart card logon certificates for users in a certain office or organizational unit that is the basis for a security group.

This restriction is based on a subset of the certificate templates enabled for the certification authority (CA) and the user groups that have Enroll permissions for that certificate template from that CA.

To configure certificate manager restrictions for a CA:

1. Open the Certification Authority snap-in, and right-click the name of the CA.
2. Click Properties, and then click the Security tab.
3. Verify that the user or group that you have selected has Issue and Manage Certificates permission. If they do not yet have this permission, select the Allow check box, and then click Apply.
4. Click the Certificate Managers tab.
5. Click Restrict certificate managers, and verify that the name of the group or user is displayed.
6. Under Certificate Templates, click Add, select the template for the certificates that you want

this user or group to manage, and then click OK. Repeat this step until you have selected all certificate templates that you want to allow this certificate manager to manage.

7. Under Permissions, click Add, type the name of the client for whom you want the certificate manager to manage the defined certificate types, and then click OK.

8. If you want to block the certificate manager from managing certificates for a specific user, computer, or group, under Permissions, select this user, computer, or group, and click Deny.

9. When you are finished configuring certificate manager restrictions, click OK or Apply.

### **QUESTION 11**

Your company has a branch office that is configured as a separate Active Directory site and has an Active Directory domain controller.

The Active Directory site requires a local Global Catalog server to support a new application.

You need to configure the domain controller as a Global Catalog server.

Which tool should you use?

- A. The Server Manager console
- B. The Active Directory Sites and Services console
- C. The Dcpromo.exe utility
- D. The Computer Management console
- E. The Active Directory Domains and Trusts console

**Correct Answer: B**

#### **Explanation:**

<http://technet.microsoft.com/en-us/library/cc781329%28v=ws.10%29.aspx>

Configure a domain controller as a global catalog server

To configure a domain controller as a global catalog server

1. Open Active Directory Sites and Services.

Further information:

<http://technet.microsoft.com/en-us/library/cc728188%28v=ws.10%29.aspx>

What Is the Global Catalog?

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication.

Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

In addition to configuration and schema directory partition replicas, every domain controller in a forest stores a full, writable replica of a single domain directory partition. Therefore, a domain controller can locate only the objects in its domain. Locating an object in a different



domain would require the user or application to provide the domain of the requested object. The global catalog provides the ability to locate objects from any domain without having to know the domain name. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest. The additional domain directory partitions are partial because only a limited set of attributes is included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server. Note: A global catalog server can also store a full, writable replica of an application directory partition, but objects in application directory partitions are not replicated to the global catalog as partial, read-only directory partitions.

The global catalog is built and updated automatically by the AD DS replication system. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are defined by default by Microsoft. However, to optimize searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.

In Windows 2000 Server environments, any change to the PAS results in full synchronization (update of all attributes) of the global catalog. Later versions of Windows Server reduce the impact of updating the global catalog by replicating only the attributes that change.

In a single-domain forest, a global catalog server stores a full, writable replica of the domain and does not store any partial replica. A global catalog server in a single-domain forest functions in the same manner as a nonglobal-catalog server except for the processing of forest-wide searches.

## **QUESTION 12**

Your company has a domain controller that runs Windows Server 2008. The domain controller has the backup features installed.

You need to perform a non-authoritative restore of the domain controller using an existing backup file.

What should you do?

- A. Restart the domain controller in Directory Services Restore Mode and use wbadmin to restore critical volume
- B. Restart the domain controller in Directory Services Restore Mode and use the backup snap-in to restore critical volume
- C. Restart the domain controller in Safe Mode and use wbadmin to restore critical volume
- D. Restart the domain controller in Safe Mode and use the backup snap-in to restore critical volume

**Correct Answer:** A

**Explanation:**

Almost identical to B42

<http://technet.microsoft.com/en-us/library/cc816627%28v=ws.10%29.aspx>

Performing Nonauthoritative Restore of Active Directory Domain Services A nonauthoritative restore is the method for restoring Active Directory Domain Services (AD DS) from a system state, critical-volumes, or full server backup. A nonauthoritative restore returns the domain controller to its state at the time of backup and then allows normal replication to overwrite that state with any changes that occurred after the backup was taken. After you restore AD DS from backup, the domain controller queries its replication partners. Replication partners use the standard replication protocols to update AD DS and associated information, including the SYSVOL shared folder, on the restored domain controller.

You can use a nonauthoritative restore to restore the directory service on a domain controller without reintroducing or changing objects that have been modified since the backup. The most common use of a nonauthoritative restore is to reinstate a domain controller, often after catastrophic or debilitating hardware failures. In the case of data corruption, do not use nonauthoritative restore unless you have confirmed that the problem is with AD DS.

Nonauthoritative Restore Requirements You can perform a nonauthoritative restore from backup on a Windows Server 2008 system that is a standalone server, member server, or domain controller.

On domain controllers that are running Windows Server 2008, you can stop and restart AD DS as a service. Therefore, in Windows Server 2008, performing offline defragmentation and other database management tasks does not require restarting the domain controller in Directory Services Restore Mode (DSRM). However, you cannot perform a nonauthoritative restore after simply stopping the AD DS service in regular startup mode. You must be able to start the domain controller in Directory Services Restore Mode (DSRM). If the domain controller cannot be started in DSRM, you must first reinstall the operating system.

To perform a nonauthoritative restore, you need one of the following types of backup for your backup source:

System state backup: Use this type of backup to restore AD DS. If you have reinstalled the operating system, you must use a critical-volumes or full server backup. If you are restoring a system state backup, use the `wbadmin start systemstaterecovery` command.

Critical-volumes backup: A critical-volumes backup includes all data on all volumes that contain operating system and registry files, boot files, SYSVOL files, or Active Directory files. Use this type of backup if you want to restore more than the system state. To restore a critical-volumes backup, use the `wbadmin start recovery` command.

Full server backup: Use this type of backup only if you cannot start the server or you do not have a system state or critical-volumes backup. A full server backup is generally larger than a critical-volumes backup.

Restoring a full server backup not only rolls back data in AD DS to the time of backup, but it also rolls back all data in all other volumes. Rolling back this additional data is not necessary to achieve nonauthoritative restore of AD DS.

### **QUESTION 13**

Your company security policy requires complex passwords.

You have a comma delimited file named `import.csv` that contains user account information.

You need to create user account in the domain by using the import.csv file.

You also need to ensure that the new user accounts are set to use default passwords and are disabled.

What should you do?

- A. Modify the userAccountControl attribute to disabled. Run the `csvde i k f import.csv` command. Run the DSMOD utility to set default passwords for the user accounts.
- B. Modify the userAccountControl attribute to accounts disabled. Run the `csvde -f import.csv` command. Run the DSMOD utility to set default passwords for the user accounts.
- C. Modify the userAccountControl attribute to disabled. Run the `wscript import.csv` command. Run the DSADD utility to set default passwords for the imported user accounts.
- D. Modify the userAccountControl attribute to disabled. Run `ldifde -i -f import.csv` command. Run the DSADD utility to set passwords for the imported user accounts.

**Correct Answer: A**

**Explanation:**

Personal note:

The correct command should be:

```
csvde -i -k -f import.csv
```

<http://support.microsoft.com/kb/305144>

How to use the UserAccountControl flags to manipulate user account properties When you open the properties for a user account, click the Account tab, and then either select or clear the check boxes in the Account options dialog box, numerical values are assigned to the UserAccountControl attribute. The value that is assigned to the attribute tells Windows which options have been enabled.

You can view and edit these attributes by using either the Ldp.exe tool or the Adsiedit.msc snap-in.

The following table lists possible flags that you can assign. You cannot set some of the values on a user or computer object because these values can be set or reset only by the directory service. Note that Ldp.exe shows the values in hexadecimal. Adsiedit.msc displays the values in decimal. The flags are cumulative. To disable a user's account, set the UserAccountControl attribute to 0x0202 (0x002 + 0x0200). In decimal, this is 514 (2 + 512).

<http://technet.microsoft.com/en-us/library/cc732101%28v=ws.10%29.aspx>

Csvde

Imports and exports data from Active Directory Domain Services (AD DS) using files that store data in the comma-separated value (CSV) format. You can also support batch operations based on the CSV file format standard.

Syntax:

```
Csvde [-i] [-f <FileName>] [-s <ServerName>] [-c <String1> <String2>] [-v] [-j <Path>] [-t <PortNumber>] [-d <BaseDN>] [-r <LDAPFilter>] [-p <Scope>] [-l <LDAPAttributeList>] [-o <LDAPAttributeList>] [-
```

g] [-m] [-n] [-k] [-a

<UserDistinguishedName> {<Password> | \*} [-b <UserName> <Domain> {<Password> | \*}]

Parameters

-i

Specifies import mode. If not specified, the default mode is export.

-f <FileName> Identifies the import or export file name.

-k

Ignores errors during an import operation and continues processing.

<http://technet.microsoft.com/en-us/library/cc732954%28v=ws.10%29.aspx>

Dsmod user Modifies attributes of one or more existing users in the directory.

Syntax:

dsmod user <UserDN> ... [-upn <UPN>] [-fn <FirstName>] [-mi <Initial>] [-ln <LastName>] [-

display<DisplayName>] [-empid <EmployeeID>] [-pwd (<Password> | \*)] [-desc

<Description>] [-office <Office>] [-tel

<PhoneNumber>] [-email <E-mailAddress>] [-hometel <HomePhoneNumber>] [-pager

<PagerNumber>] [-mobile <CellPhoneNumber>] [-fax <FaxNumber>] [-iptel

<IPPhoneNumber>] [-webpg <WebPage>] [-title

<Title>] [-dept <Department>] [-company <Company>] [-mgr <Manager>] [-hmdir

<HomeDirectory>] [-hmdrv

<DriveLetter>:] [-profile <ProfilePath>] [-loscr <ScriptPath>] [-mustchpwd {yes | no}] [-

canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires

<NumberOfDays>] [-disabled {yes | no}] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p

{<Password> | \*}][-c] [-q] [{-uc | -uco | -uci}]

Parameters

<UserDN>Required. Specifies the distinguished names of the users that you want to modify.

If values are omitted, they are obtained through standard input (stdin) to support piping of output from another command to input of this command.

-pwd {<Password> | \*}

Resets the passwords for the users that you want to modify as Password or an asterisk (\*).

If you type \*, AD

DS prompts you for a user password.

#### QUESTION 14

Your company has an Active Directory domain. All servers run Windows Server 2008 R2.

Your company uses an Enterprise Root certification authority (CA) and an Enterprise Intermediate CA.

The Enterprise Intermediate CA certificate expires.

You need to deploy a new Enterprise Intermediate CA certificate to all computers in the domain.

What should you do?

- A. Import the new certificate into the Intermediate Certification Store on the Enterprise Root CA server.
- B. Import the new certificate into the Intermediate Certification Store on the Enterprise Intermediate CA server.
- C. Import the new certificate into the Intermediate Certification Store in the Default Domain Controllers group policy object.
- D. Import the new certificate into the Intermediate Certification Store in the Default Domain group policy object.

**Correct Answer: B**

**Explanation:**

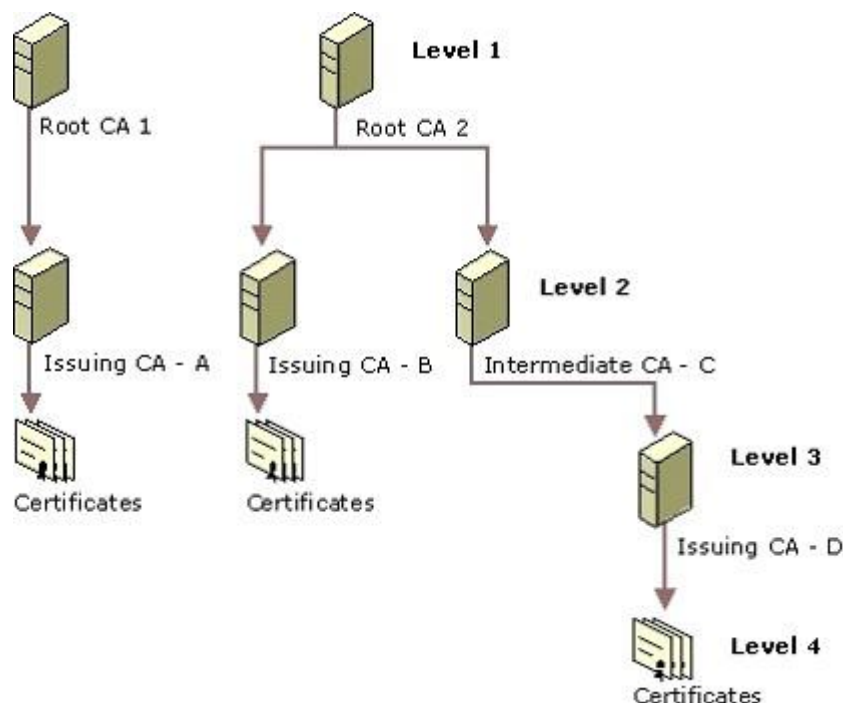
<http://technet.microsoft.com/en-us/library/cc962065.aspx>

Certification Authority Trust Model

Certification Authority Hierarchies

The Windows 2000 public key infrastructure supports a hierarchical CA trust model, called the certification hierarchy, to provide scalability, ease of administration, and compatibility with a growing number of commercial third-party CA services and public key-aware products. In its simplest form, a certification hierarchy consists of a single CA. However, the hierarchy usually contains multiple CAs that have clearly defined parent-child relationships.

Figure 16.5 shows some possible CA hierarchies.



You can deploy multiple CA hierarchies to meet your needs. The CA at the top of the hierarchy is called a root CA . Root CAs are self-certified by using a self-signed CA certificate. Root CAs are the most trusted CAs in the organization and it is recommended that they have

the highest security of all. There is no requirement that all CAs in an enterprise share a common top-level CA parent or root. Although trust for CAs depends on each domain's CA trust policy, each CA in the hierarchy can be in a different domain. Child CAs are called subordinate CAs. Subordinate CAs are certified by the parent CAs. A parent CA certifies the subordinate CA by issuing and signing the subordinate CA certificate. A subordinate CA can be either an intermediate or an issuing CA. An intermediate CA issues certificates only to subordinate CAs. An issuing CA issues certificates to users, computers, or services.

<http://social.technet.microsoft.com/Forums/en-US/winserversecurity/thread/605dbf9d-2694-4783-8002-c08b9c7d4149>

### QUESTION 15

Your company has a main office and three branch offices. The company has an Active Directory forest that has a single domain. Each office has one domain controller. Each office is configured as an Active Directory site.

All sites are connected with the DEFAULTIPSITELINK object.

You need to decrease the replication latency between the domain controllers.

What should you do?

- A. Decrease the replication schedule for the DEFAULTIPSITELINK object.
- B. Decrease the replication interval for the DEFAULTIPSITELINK object.
- C. Decrease the cost between the connection objects.
- D. Decrease the replication interval for all connection objects.

**Correct Answer: B**

#### **Explanation:**

Correct Answer: Decrease the replication interval for the DEFAULTIPSITELINK object.

Personal comment:

All sites are connected with the DEFAULTIPSITELINK object. <- this roughly translates into all sites are connected with the first domain controller in the forest So the topology is star shaped.

Thus, decreasing the cost between the connection objects will offer no benefit. We know we have multiple sites linked and are using a DEFAULTIPSITELINK object. Thus, the most plausible answer is to decrease the replication interval for DEFAULTIPSITELINK.

<http://www.informit.com/articles/article.aspx?p=26866&seqNum=5>

Understanding Active Directory, Part III

Replication

Active Directory replication between domain controllers is managed by the system administrator on a site-by-site basis. As domain controllers are added, a replication path must be established. This is done by the Knowledge Consistency Checker (KCC), coupled with

Active Directory replication components. The KCC is a dynamic process that runs on all domain controllers to create and modify the replication topology. If a domain controller fails, the KCC automatically creates new paths to the remaining domain controllers. Manual intervention with the KCC will also force a new path. The Active Directory replaces PDCs and BDCs with multimaster replication services. Each domain controller retains a copy of the entire directory for that particular domain. As changes are made in one domain controller, the originator communicates these changes to the peer domain controllers. The directory data itself is stored in the ntds.dit file.

Active Directory replication uses the Remote Procedure Call (RPC) over IP to conduct replication within a site. Replication between sites can utilize either RPC or the Simple Mail Transfer Protocol (SMTP) for data transmission. The default intersite replication protocol is RPC.

#### Intersite and Intrasite Replication

There are distinct differences in internal and intersite domain controller replication. In theory, the network bandwidth within a site is sufficient to handle all network traffic associated with replication and other Active Directory activities. By the definition of a site, the network must be reliable and fast. A change notification process is initiated when modifications occur on a domain controller. The domain controller waits for a configurable period (by default, five minutes) before it forwards a message to its replication partners. During this interval, it continues to accept changes. Upon receiving a message, the partner domain controllers copy the modification from the original domain controller. In the event that no changes were noted during a configurable period (six hours, by default), a replication sequence ensures that all possible modifications are communicated. Replication within a site involves the transmission of uncompressed data.

#### NOTE

Security-related modifications are replicated within a site immediately. These changes include account and individual user lockout policies, changes to password policies, changes to computer account passwords, and modifications to the Local Security Authority (LSA).

Replication between sites assumes that there are network-connectivity problems, including insufficient bandwidth, reliability, and increased cost. Therefore, the Active Directory permits the system to make decisions on the type, frequency, and timing of intersite replication. All replication objects transmitted between sites are compressed, which may reduce traffic by 10 to 25 percent, but because this is not sufficient to guarantee proper replication, the system administrator has the responsibility of scheduling intersite replication.

#### Replication Component Objects

Whereas the KCC represents the process elements associated with replication, the following comprise the Active Directory object components:

Connection object. Domain controllers become replication "partners" when linked by a connection object.

This is represented by a one-way path between two domain controller server objects.

Connection objects are created by the KCC by default. They can also be manually created by the system administrator.

NTDS settings object. The NTDS settings object is a container that is automatically created by the Active Directory. It contains all of the connection objects, and is a child of the server

object.

**Server object.** The Active Directory represents every computer as a computer object. The domain controller is also represented by a computer object, plus a specially created server object. The server object's parent is the site object that defines its IP subnet. However, in the event that the domain controller server object was created prior to site creation, it will be necessary to manually define the IP subnet to properly assign the domain controller a site. When it is necessary to link multiple sites, two additional objects are created to manage the replication topology.

**Site link.** The site link object specifies a series of values (cost, interval, and schedule) that define the connection between sites. The KCC uses these values to manage replication and to modify the replication path if it detects a more efficient one. The Active Directory DEFAULTIPSITELINK is used by default until the system administrator intervenes. The cost value, ranging from 1 to 32767, is an arbitrary estimate of the actual cost of data transmission as defined bandwidth. The interval value sets the number of times replication will occur: 15 minutes to a maximum of once a week (or 10080 minutes) is the minimum; three hours is the default. The schedule interval establishes the time when replication should occur. Although replication can be at any time by default, the system administrator may want to schedule it only during offpeak network hours.

**Site link bridges.** The site link bridge object defines a set of links that communicate via the same protocol. By default, all site links use the same protocol, and are transitive. Moreover, they belong to a single site link bridge. No configuration is necessary to the site link bridge if the IP network is fully routed. Otherwise, manual configuration may be necessary.

Further information:

<http://technet.microsoft.com/en-us/library/cc775549%28v=ws.10%29.aspx>

What Is Active Directory Replication Topology?

Replication of updates to Active Directory objects are transmitted between multiple domain controllers to keep replicas of directory partitions synchronized. Multiple domains are common in large organizations, as are multiple sites in disparate locations. In addition, domain controllers for the same domain are commonly placed in more than one site. Therefore, replication must often occur both within sites and between sites to keep domain and forest data consistent among domain controllers that store the same directory partitions. Site objects can be configured to include a set of subnets that provide local area network (LAN) network speeds. As such, replication within sites generally occurs at high speeds between domain controllers that are on the same network segment. Similarly, site link objects can be configured to represent the wide area network (WAN) links that connect LANs.

Replication between sites usually occurs over these WAN links, which might be costly in terms of bandwidth.

To accommodate the differences in distance and cost of replication within a site and replication between sites, the intrasite replication topology is created to optimize speed, and the intersite replication topology is created to minimize cost.

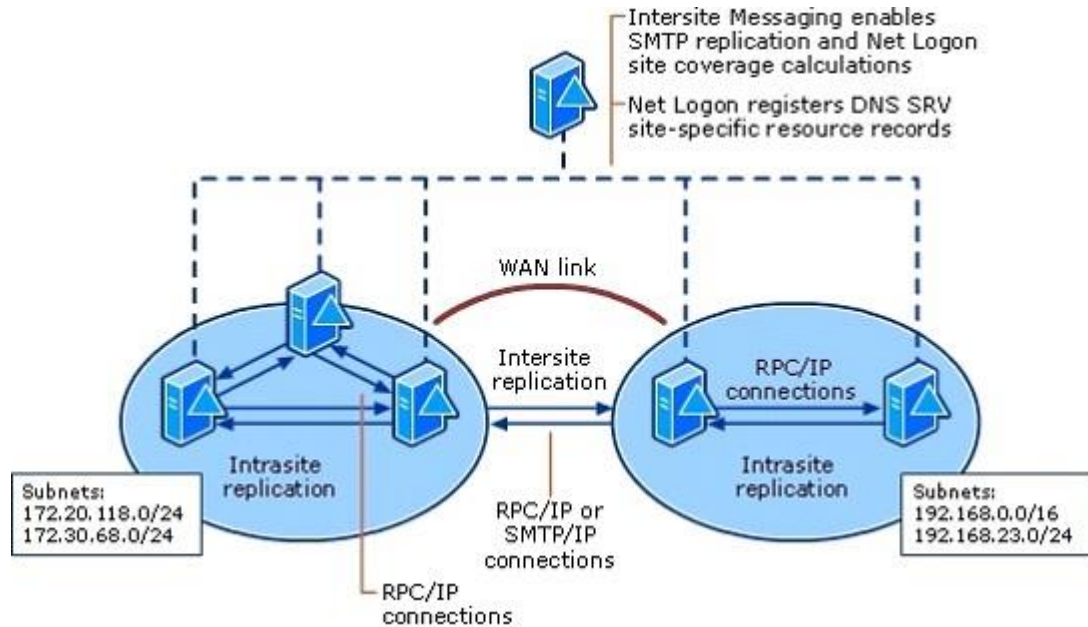
The Knowledge Consistency Checker (KCC) is a distributed application that runs on every domain controller and is responsible for creating the connections between domain controllers that collectively form the replication topology. The KCC uses Active Directory data to determine where (from what source domain controller to what destination domain controller)



to create these connections.

The following diagram shows the interaction of these technologies with the replication topology, which is indicated by the two-way connections between each set of domain controllers.

### Replication Topology and Dependent Technologies



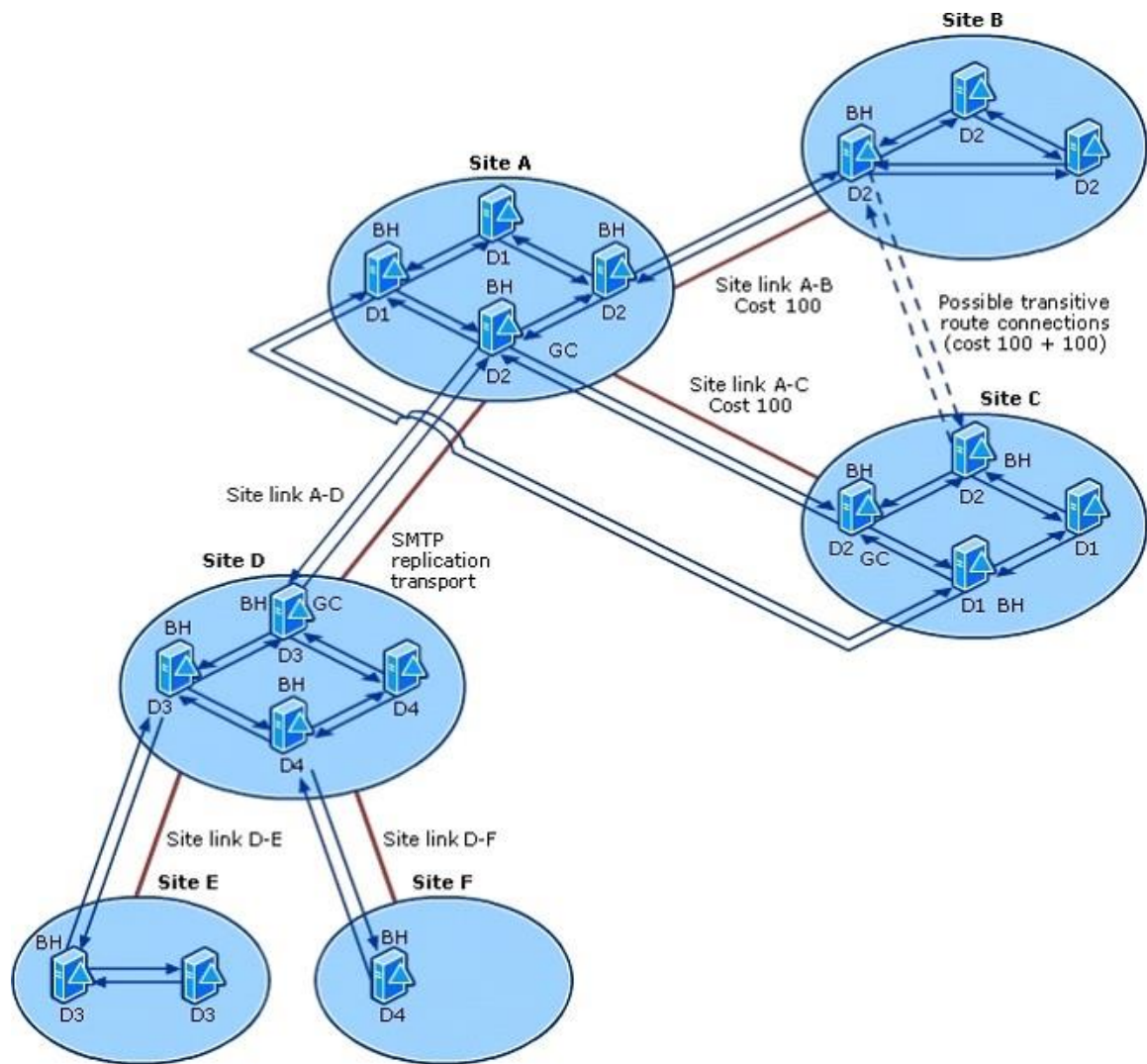
<http://technet.microsoft.com/en-us/library/cc755994%28v=ws.10%29.aspx>

### How Active Directory Replication Topology Works

#### Replication Topology Physical Structure

The Active Directory replication topology can use many different components. Some components are required and others are not required but are available for optimization. The following diagram illustrates most replication topology components and their place in a sample Active Directory multisite and multidomain forest. The depiction of the intersite topology that uses multiple bridgehead servers for each domain assumes that at least one domain controller in each site is running at least Windows Server 2003. All components of this diagram and their interactions are explained in detail later in this section.

#### Replication Topology Physical Structure



In the preceding diagram, all servers are domain controllers. They independently use global knowledge of onfiguration data to generate one-way, inbound connection objects. The KCCs in a site collectively create an intrasite topology for all domain controllers in the site. The ISTGs from all sites collectively create an intersite topology. Within sites, one-way arrows indicate the inbound connections by which each domain controller replicates changes from its partner in the ring. For intersite replication, one-way arrows represent inbound connections that are created by the ISTG of each site from bridgehead servers (BH) for the same domain (or from a global catalog server [GC] acting as a bridgehead if the domain is not present in the site) in other sites that share a site link. Domains are indicated as D1, D2, D3, and D4. Each site in the diagram represents a physical LAN in the network, and each LAN is represented as a site object in Active Directory. Heavy solid lines between sites indicate WAN links over which two-way replication can occur, and each WAN link is represented in Active Directory as a site link object. Site link objects allow connections to be created between bridgehead servers in each site that is connected by the site link. Not shown in the diagram is that where TCP/IP WAN links are available, replication between sites uses the RPC replication transport. RPC is always used within sites. The site link between Site A and Site D uses the SMTP protocol for the replication transport to replicate

the configuration and schema directory partitions and global catalog partial, read-only directory partitions. Although the SMTP transport cannot be used to replicate writable domain directory partitions, this transport is required because a TCP/IP connection is not available between Site A and Site D. This configuration is acceptable for replication because Site D does not host domain controllers for any domains that must be replicated over the site link A-D.

By default, site links A-B and A-C are transitive (bridged), which means that replication of domain D2 is possible between Site B and Site C, although no site link connects the two sites. The cost values on site links A-B and A-C are site link settings that determine the routing preference for replication, which is based on the aggregated cost of available site links. The cost of a direct connection between Site C and Site B is the sum of costs on site links A-B and A-C. For this reason, replication between Site B and Site C is automatically routed through Site A to avoid the more expensive, transitive route. Connections are created between Site B and Site C only if replication through Site A becomes impossible due to network or bridgehead server conditions.

#### Control Replication Latency and Cost

Replication latency is inherent in a multimaster directory service. A period of replication latency begins when a directory update occurs on an originating domain controller and ends when replication of the change is received on the last domain controller in the forest that requires the change. Generally, the latency that is inherent in a WAN link is relative to a combination of the speed of the connection and the available bandwidth.

Replication cost is an administrative value that can be used to indicate the latency that is associated with different replication routes between sites. A lower-cost route is preferred by the ISTG when generating the replication topology.

Site topology is the topology as represented by the physical network: the LANs and WANs that connect domain controllers in a forest. The replication topology is built to use the site topology. The site topology is represented in Active Directory by site objects and site link objects. These objects influence Active Directory replication to achieve the best balance between replication speed and the cost of bandwidth utilization by distinguishing between replication that occurs within a site and replication that must span sites. When the KCC creates replication connections between domain controllers to generate the replication topology, it creates more connections between domain controllers in the same site than between domain controllers in different sites.

The results are lower replication latency within a site and less replication bandwidth utilization between sites.

Within sites, replication is optimized for speed as follows:

Connections between domain controllers in the same site are always arranged in a ring, with possible additional connections to reduce latency.

Replication within a site is triggered by a change notification mechanism when an update occurs, moderated by a short, configurable delay (because groups of updates frequently occur together).

Data is sent uncompressed, and thus without the processing overhead of data compression.

Between sites, replication is optimized for minimal bandwidth usage (cost) as follows:

Replication data is compressed to minimize bandwidth consumption over WAN links. Store-and-forward replication makes efficient use of WAN links -- each update crosses an expensive link only once.

Replication occurs at intervals that you can schedule so that use of expensive WAN links is managed.

The intersite topology is a layering of spanning trees (one intersite connection between any two sites for each directory partition) and generally does not contain redundant connections.

#### Topology-Related Objects in Active Directory

Active Directory stores replication topology information in the configuration directory partition. Several configuration objects define the components that are required by the KCC to establish and implement the replication topology:

#### Site Link Objects

For a connection object to be created on a destination domain controller in one site that specifies a source domain controller in another site, you must manually create a site link object (class siteLink ) that connects the two sites. Site link objects identify the transport protocol and scheduling required to replicate between two or more sites. You can use Active Directory Sites and Services to create the site links. The KCC uses the information stored in the properties of these site links to create the intersite topology connections. A site link is associated with a network transport by creating the site link object in the appropriate transport container (either IP or SMTP). All intersite domain replication must use IP site links. The Simple Mail Transfer Protocol (SMTP) transport can be used for replication between sites that contain domain controllers that do not host any common domain directory partition replicas.

#### Site Link Properties

A site link specifies the following:

Two or more sites that are permitted to replicate with each other.

An administrator-defined cost value associated with that replication path. The cost value controls the route that replication takes, and thus the remote sites that are used as sources of replication information.

A schedule during which replication is permitted to occur.

An interval that determines how frequently replication occurs over this site link during the times when the schedule allows replication.

#### Default Site Link

When you install Active Directory on the first domain controller in the forest, an object named DEFAULTIPSITELINK is created in the Sites container (in the IP container within the Inter-Site Transports container). This site link contains only one site, Default-First-Site-Name.

### **QUESTION 16**

You have a domain controller that runs Windows Server 2008 R2 and is configured as a DNS server.

You need to record all inbound DNS queries to the server.

What should you configure in the DNS Manager console?

- A. Enable debug logging.
- B. Enable automatic testing for simple queries.
- C. Configure event logging to log errors and warnings.
- D. Enable automatic testing for recursive queries.

**Correct Answer: A**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc753579.aspx>

DNS Tools

Event-monitoring utilities

The Windows Server 2008 family includes two options for monitoring DNS servers:

Default logging of DNS server event messages to the DNS server log.

DNS server event messages are separated and kept in their own system event log, the DNS server log, which you can view using DNS Manager or Event Viewer.

The DNS server log contains events that are logged by the DNS Server service. For example, when the DNS server starts or stops, a corresponding event message is written to this log.

Most additional critical DNS Server service events are also logged here, for example, when the server starts but cannot locate initializing data and zones or boot information stored in the registry or (in some cases) Active Directory Domain Services (AD DS).

You can use Event Viewer to view and monitor client-related DNS events. These events appear in the System log, and they are written by the DNS Client service at any computers running Windows (all versions).

Optional debug options for trace logging to a text file on the DNS server computer. You can also use DNS Manager to selectively enable additional debug logging options for temporary trace logging to a text-based file of DNS server activity. The file that is created and used for this feature, Dns.log, is stored in the %systemroot%\System32\Dns folder.

<http://technet.microsoft.com/en-us/library/cc776361%28v=ws.10%29.aspx>

Using server debug logging options

The following DNS debug logging options are available:

Direction of packets

Send Packets sent by the DNS server are logged in the DNS server log file.

Receive Packets received by the DNS server are logged in the log file.

Further information:

<http://technet.microsoft.com/en-us/library/cc759581%28v=ws.10%29.aspx>

Select and enable debug logging options on the DNS server

## **QUESTION 17**

Your company has an Active Directory forest that contains Windows Server 2008 R2 domain controllers and DNS servers. All client computers run Windows XP SP3.

You need to use your client computers to edit domain-based GPOs by using the ADMX files that are stored in the ADMX central store.

What should you do?

- A. Add your account to the Domain Admins group.
- B. Upgrade your client computers to Windows 7.
- C. Install .NET Framework 3.0 on your client computers.
- D. Create a folder on PDC emulator for the domain in the PolicyDefinitions path. Copy the ADMX files to the PolicyDefinitions folder.

**Correct Answer: B**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc709647%28v=ws.10%29.aspx>

Managing Group Policy ADMX Files Step-by-Step Guide

Microsoft Windows Vista and Windows Server 2008 introduce a new format for displaying registry-based policy settings. Registry-based policy settings (located under the Administrative Templates category in the Group Policy Object Editor) are defined using a standards-based, XML file format known as ADMX files. These new files replace ADM files, which used their own markup language. The Group Policy tools --Group Policy Object Editor and Group Policy Management Console--remain largely unchanged. In the majority of situations, you will not notice the presence of ADMX files during your day-to-day Group Policy administration tasks.

<http://blogs.technet.com/b/grouppolicy/archive/2008/12/17/questions-on-admx-in-windows-xp-and-windows2003-environments.aspx>

Questions on ADMX in Windows XP and Windows 2003 environments

We had a question a couple of days ago about the usage of ADMX template formats in Windows XP/Server 2003 environments. Essentially the question was:

"...What's the supported or recommended way of getting W2k8 ADMX templates applying in a W2k3 domain with or with no W2k8 DCs. What I've done in test is, created a central store in the /Sysvol/domain/policies folder on the 2k3 DC (PDC) and created and edited a GPO using GPMC from the W2k8 member server applying to a W2k8 machine and it seems to work just fine. Is this the right way to do it?..."

The answer is Yes. Again this is one of those things that confuse people. The template format has nothing to do with the policy file that's created. Its just used to create the policy by the administrative tool itself. In the case of GPMC on Windows XP and Windows Server 2003 and previous this tool used the ADM file format. These ADM files were copied into every policy object on the SYSVOL, which represents about 4MB of duplicated bloat per policy. This was one of the areas that caused major problems with an issue called SYSVOL bloat.

In Vista and Server 2008 this template format changed to ADMX. This was a complete change towards a new XML based format that aimed to eliminate SYSVOL bloat. It doesn't copy itself into every policy object but relies on a central or local store of these templates (Note that even in the newer tools you can still import custom ADM files for stuff like Office etc).

In the question above, the person wanted to know if copying the local store, located under `c:/windows/ policydefinitions`, could be copied into a Windows Server 2003 domain environment as the central store and referenced by the newer admin tools. Again the domain functional mode has little to do with Group Policy. I talked about that one before. The things that we care about are the administrative tools and the client support for the policy functions. So of course it can.

Here's the confusion-reducing scoop - Group Policy as a platform only relies on two main factors. Active Directory to store metadata about the policy objects and to allow client discoverability for the location of the policy files. The other is the SYSVOL to store the policy files. So at its core that's LDAP and SMB file shares. Specific extensions on top of the policy platform may require certain domain functionality but that's very specific to that extension. Examples are the new Wireless policy and BitLocker extensions in Vista SP1. They require schema updates - not GP itself. So if you don't currently use them then you don't have to update schema.

So provided you're using Windows Vista SP1 with RSAT or Windows Server 2008 to administer the policies you get all the benefits to manage downlevel clients. That means eliminating SYSVOL bloat. That means all the joys of Group Policy Preferences. Honestly - it amazes us the amount of IT Pros that still haven't discovered GPP...especially with the power it has to practically eliminate logon scripts! As a last point - IT Pros also ask us when we will be producing an updated GPMC version for Windows XP to support all the new stuff. The answer is that we are not producing any updated GPMC versions for Windows XP and Server 2003. All the new administrative work is being done on the newer platforms. So get moving ahead! There are some really good benefits in the newer tools and very low impact to your current environment. You only need a single Windows Vista SP1 machine to start!

### **QUESTION 18**

Your company has an Active Directory domain. All servers run Windows Server 2008 R2.

Your company uses an Enterprise Root certificate authority (CA).

You need to ensure that revoked certificate information is highly available.

What should you do?

- A. Implement an Online Certificate Status Protocol (OCSP) responder by using an Internet Security and Acceleration Server array.
- B. Publish the trusted certificate authorities list to the domain by using a Group Policy Object (GPO).
- C. Implement an Online Certificate Status Protocol (OCSP) responder by using Network Load Balancing.
- D. Create a new Group Policy Object (GPO) that allows users to trust peer certificates. Link the GPO to the domain.

**Correct Answer: C**

**Explanation:**

<http://technet.microsoft.com/en-us/library/cc731027%28v=ws.10%29.aspx>

AD CS: Online Certificate Status Protocol Support

Certificate revocation is a necessary part of the process of managing certificates issued by certification authorities (CAs). The most common means of communicating certificate status is by distributing certificate revocation lists (CRLs). In the Windows Server 2008 operating system, public key infrastructures (PKIs) where the use of conventional CRLs is not an optimal solution, an Online Responder based on the Online Certificate Status Protocol (OCSP) can be used to manage and distribute revocation status information.

What does OCSP support do?

The use of Online Responders that distribute OCSP responses, along with the use of CRLs, is one of two common methods for conveying information about the validity of certificates.

Unlike CRLs, which are distributed periodically and contain information about all certificates that have been revoked or suspended, an Online Responder receives and responds only to requests from clients for information about the status of a single certificate. The amount of data retrieved per request remains constant no matter how many revoked certificates there might be.

In many circumstances, Online Responders can process certificate status requests more efficiently than by using CRLs.

Adding one or more Online Responders can significantly enhance the flexibility and scalability of an organization's PKI.

Further information:

<http://blogs.technet.com/b/askds/archive/2009/08/20/implementing-an-ocsp-responder-part-v-highavailability.aspx>

Implementing an OCSP Responder: Part V High Availability

There are two major pieces in implementing the High Availability Configuration. The first step is to add the OCSP Responders to what is called an Array. When OCSP Responders are configured in an Array, the configuration of the OCSP responders can be easily maintained, so that all Responders in the Array have the same configuration. The configuration of the Array Controller is used as the baseline configuration that is then applied to other members of the Array. The second piece is to load balance the OCSP Responders. Load balancing of the OCSP responders is what actually provides fault tolerance.

**QUESTION 19**

You have two servers named Server1 and Server2. Both servers run Windows Server 2008 R2. Server1 is configured as an Enterprise Root certification authority (CA).

You install the Online Responder role service on Server2.

You need to configure Server2 to issue certificate revocation lists (CRLs) for the enterprise root CA.



Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Import the enterprise root CA certificate.
- B. Import the OCSP Response Signing certificate.
- C. Add the Server1 computer account to the CertPublishers group.
- D. Set the Startup Type of the Certificate Propagation service to Automatic.

**Correct Answer:** AB

**Explanation:**

Further information:

<http://technet.microsoft.com/en-us/library/cc770413%28v=ws.10%29.aspx>

Online Responder Installation, Configuration, and Troubleshooting Guide Public key infrastructure (PKI) consists of multiple components, including certificates, certificate revocation lists (CRLs) and certification authorities (CAs). In most cases, applications that depend on X.509 certificates, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL) and smart cards, are required to validate the status of the certificates used when performing authentication, signing, or encryption operations. The certificate status and revocation checking is the process by which the validity of certificates is verified based on two main categories: time and revocation status.

Although validating the revocation status of certificates can be performed in multiple ways, the common mechanisms are CRLs, delta CRLs, and Online Certificate Status Protocol (OCSP) responses.

<http://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx>

Active Directory Certificate Services Step-by-Step Guide

<http://blogs.technet.com/b/askds/archive/2009/09/01/designing-and-implementing-a-pki-part-i-design-andplanning.aspx>

Designing and Implementing a PKI: Part I Design and Planning

<http://technet.microsoft.com/en-us/library/cc725937.aspx>

Set Up an Online Responder

<http://technet.microsoft.com/en-us/library/cc731099.aspx>

Creating a Revocation Configuration

**QUESTION 20**

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2.

You need to identify the Lightweight Directory Access Protocol (LDAP) clients that are using the largest amount of available CPU resources on a domain controller.

What should you do?

- A. Review performance data in Resource Monitor.
- B. Review the Hardware Events log in the Event Viewer.
- C. Run the Active Directory Diagnostics Data Collector Set. Review the Active Directory Diagnostics report.
- D. Run the LAN Diagnostics Data Collector Set. Review the LAN Diagnostics report.

**Correct Answer: C**

**Explanation:**

<http://servergeeks.wordpress.com/2012/12/31/active-directory-diagnostics/>

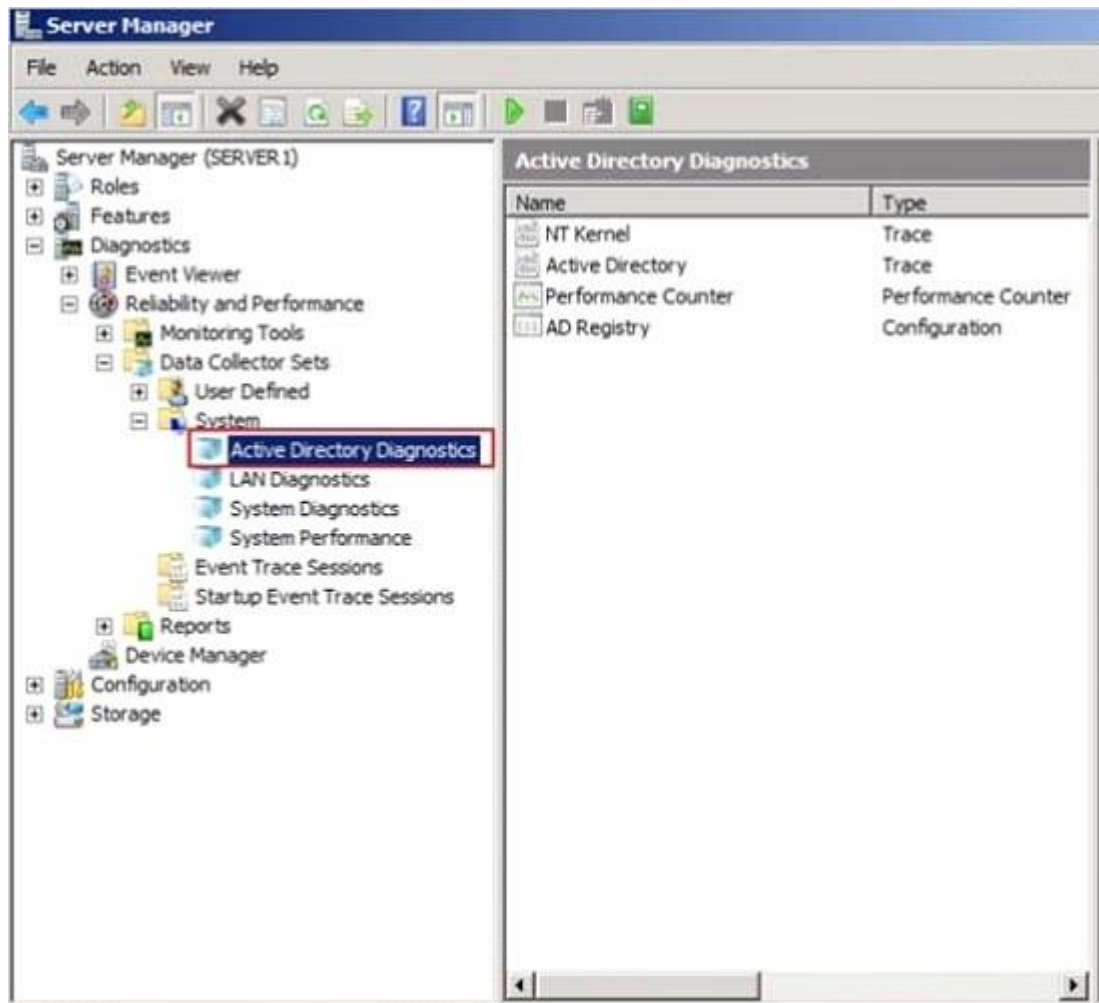
Active Directory Diagnostics

Prior to Windows Server 2008, troubleshooting Active Directory performance issues often required the installation of SPA. SPA is helpful because the Active Directory data set collects performance data and it generates XML based diagnostic reports that make analyzing AD performance issues easier by identifying the IP addresses of the highest volume callers and the type of network traffic that is placing the most loads on the CPU. Download SPA tool:

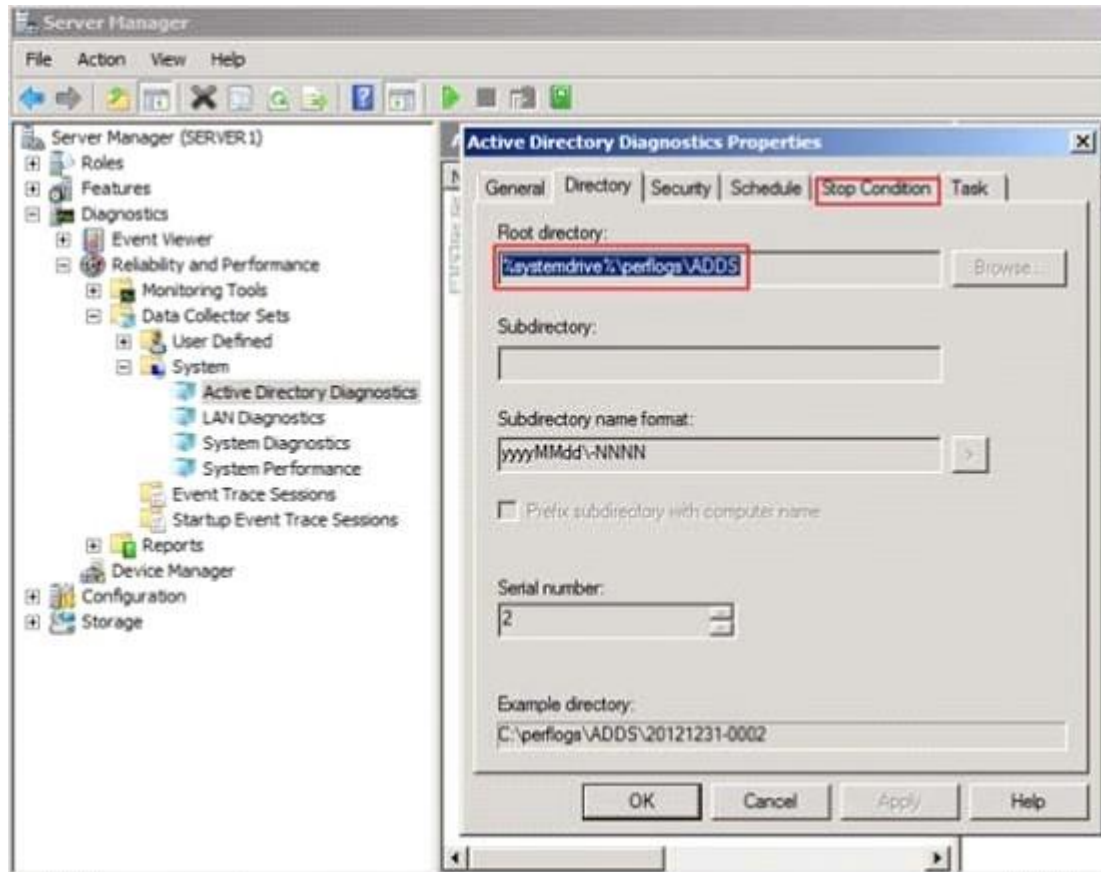
<http://www.microsoft.com/en-us/download/details.aspx?id=15506>

Now the same functionality has been built into Windows Server 2008 and Windows Server 2008 R2 and you don't have to install SPA anymore.

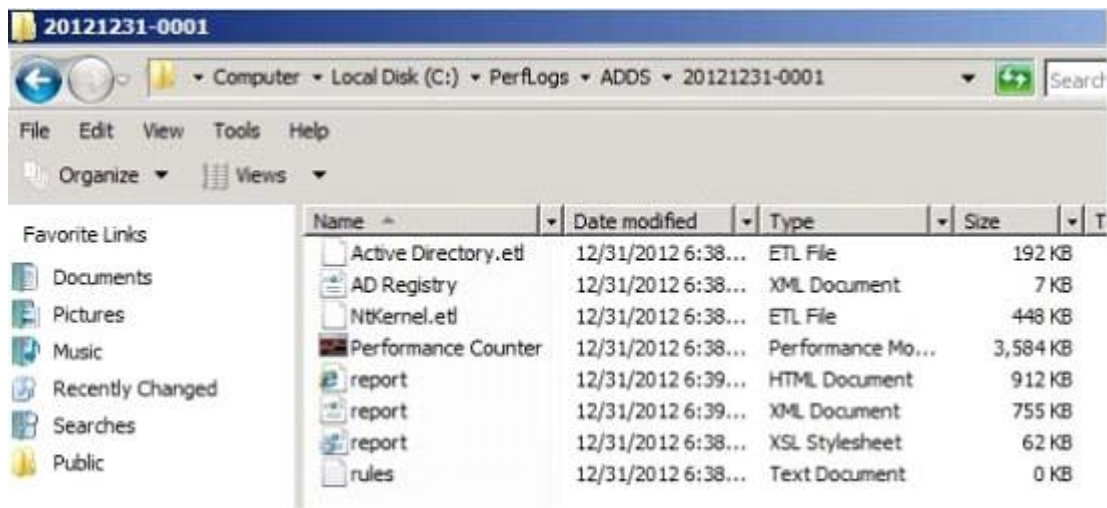
This performance feature is located in the Server Manager snap-in under the Diagnostics node and when the Active Directory Domain Services Role is installed the Active Directory Diagnostics data collector set is automatically created under System as shown here.



When you will check the properties of the collector you will notice that the data is stored under %systemdrive %\perflogs, only now it is under the \ADDS folder and when a data collection is run it creates a new subfolder called YYYYMMDD-#### where YYYY = Year, MM = Month and DD=Day and #### starts with 0001 . Active Directory Diagnostics data collector set runs for a default of 5 minutes. This duration period cannot be modified for the built-in collector. However, the collection can be stopped manually by clicking the Stop button or from the command line.



To start the data collector set, you just have to right click on Active Directory Diagnostics data collector set and select Start. Data will be stored at %systemdrive%\perflogs location.



Once you've gathered your data, you will have these interesting and useful reports under Report section, to aid in your troubleshooting and server performance trending.



Further information:

<http://technet.microsoft.com/en-us/library/dd736504%28v=ws.10%29.aspx>

Monitoring Your Branch Office Environment

<http://blogs.technet.com/b/askds/archive/2010/06/08/son-of-spa-ad-data-collector-sets-in-win2008-andbeyond.aspx>

Son of SPA: AD Data Collector Sets in Win2008 and beyond