EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!

Accurate study guides

High passing rate!

http://www.examgood.com

Exam : **070-640**

Title : Windows Server 2008
Active Directory. Configuring

Version : DEMO

1.You have a single Active Directory domain. All domain controllers run Windows Server 2008 and are configured as DNS servers. The domain contains one Active Directory-integrated DNS zone. You need to ensure that outdated DNS records are automatically removed from the DNS zone.
What should you do?
A. From the properties of the zone, modify the TTL of the SOA record.
B. From the properties of the zone, enable scavenging.
C. From the command prompt, run ipconfig /flushdns.
D. From the properties of the zone, disable dynamic updates.
Answer: B
Explanation:
http://technet.microsoft.com/en-us/library/cc753217.aspx
Set Aging and Scavenging Properties for the DNS Server
The DNS Server service supports aging and scavenging features. These features are provided as a mechanism for performing cleanup and removal of stale resource records, which can accumulate in zone data over time. You can use this procedure to set the default aging and scavenging properties for the zones on a server.
Further information:
http://technet.microsoft.com/en-us/library/cc771677.aspx
Understanding Aging and Scavenging

2.Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. The Audit account management policy setting and Audit directory services access setting are enabled for the entire domain. You need to ensure that changes made to Active Directory objects can be logged. The logged changes must include the old and new values of any attributes.
What should you do?
A. Run auditpol.exe and then configure the Security settings of the Domain Controllers OU.
B. From the Default Domain Controllers policy, enable the Audit directory service access setting and enable directory service changes.
C. Enable the Audit account management policy in the Default Domain Controller Policy.
D. Run auditpol.exe and then enable the Audit directory service access setting in the Default Domain policy.
Answer: A
Explanation:
http://technet.microsoft.com/en-us/library/cc731607%28v=ws.10%29.aspx
AD DS Auditing Step-by-Step Guide
In Windows Server 2008 you can now set up AD DS auditing with a new audit subcategory to log old and new values when changes are made to objects and their attributes.
..
The ability to audit changes to objects in AD DS is enabled with the new audit policy subcategory Directory Service Changes. This guide provides instructions for implementing this audit policy subcategory.
The types of changes that you can audit include a user (or any security principal) creating, modifying, moving, or undeleting an object. The new audit policy subcategory adds the following capabilities to auditing in AD DS:

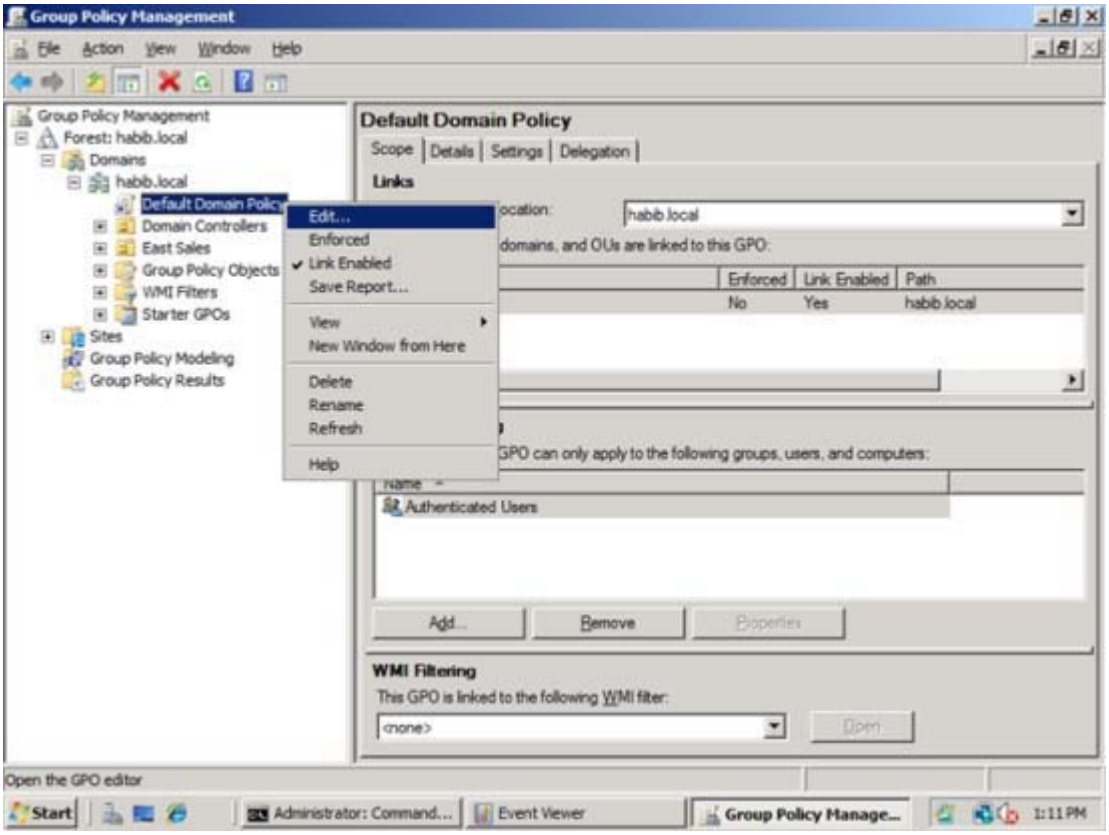
When a successful modify operation is performed on an attribute, AD DS logs the previous and current values of the attribute. If the attribute has more than one value, only the values that change as a result of the modify operation are logged.
If a new object is created, values of the attributes that are populated at the time of creation are logged. If the user adds attributes during the create operation, those new attribute values are logged. In most cases, AD DS assigns default values to attributes (such as samAccountName). The values of such system attributes are not logged.
If an object is moved, the previous and new location (distinguished name) is logged for moves within the domain. When an object is moved to a different domain, a create event is generated on the domain controller in the target domain.
If an object is undeleted, the location where the object is moved to is logged. In addition, if the user adds, modifies, or deletes attributes while performing an undelete operation, the values of those attributes are logged.
..
In Windows Server 2008, you implement the new auditing feature by using the following controls:
Global audit policy
System access control list (SACL)
Schema
Global audit policy
Enabling the global audit policy, Audit directory service access, enables all directory service policy subcategories. You can set this global audit policy in the Default Domain Controllers Group Policy (under Security Settings\Local Policies\Audit Policy). In Windows Server 2008, this global audit policy is not enabled by default. Although the subcategory Directory Service Access is enabled for success events by default, the other subcategories are not enabled by default.
You can use the command-line tool Auditpol.exe to view or set audit policy subcategories. There is no Windows interface tool available in Windows Server 2008 to view or set audit policy subcategories.
Further information:
http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx
Auditpol
Displays information about and performs functions to manipulate audit policies.
http://servergeeks.wordpress.com/2012/12/31/auditing-directory-services/
AD Scenario – Auditing Directory Services
Auditing of Directory Services depends on several controls, these are:
1. Global Audit Policy (at category level using gpmc.msc tool)
2. Individual Audit Policy (at subcategory level using auditpol.exe tool)
3. System ACLs – to specify which operations are to be audited for a security principal.
4. Schema (optional) – this is an additional control in the schema that you can use to create exceptions to what is audited.
In Windows Server 2008, you can now set up AD DS (Active Directory Domain Services) auditing with a new audit policy subcategory (Directory Service Changes) to log old and new values when changes are made to AD DS objects and their attributes. This can be done using auditpol.exe tool.
Command to check which audit policies are active on your machine: auditpol /get /category:*

```
Administrator: Command Prompt

C:\>auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             No Auditing
  System Integrity                      Success and Failure
  IPsec Driver                          No Auditing
  Other System Events                   Success and Failure
  Security State Change                 Success
Logon/Logoff
  Logon                                 Success and Failure
  Logoff                                Success
  Account Lockout                       Success
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         Success
  Other Logon/Logoff Events             No Auditing
  Network Policy Server                 Success and Failure
Object Access
  File System                           No Auditing
  Registry                              No Auditing
  Kernel Object                         No Auditing
  SAM                                   No Auditing
  Certification Services                No Auditing
  Application Generated                 No Auditing
  Handle Manipulation                   No Auditing
  File Share                            No Auditing
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         No Auditing
  Other Object Access Events            No Auditing
Privilege Use
  Sensitive Privilege Use               No Auditing
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
Detailed Tracking
  Process Termination                   No Auditing
  DPAPI Activity                        No Auditing
  RPC Events                            No Auditing
  Process Creation                      No Auditing
Policy Change
  Audit Policy Change                   Success
  Authentication Policy Change          Success
  Authorization Policy Change           No Auditing
```

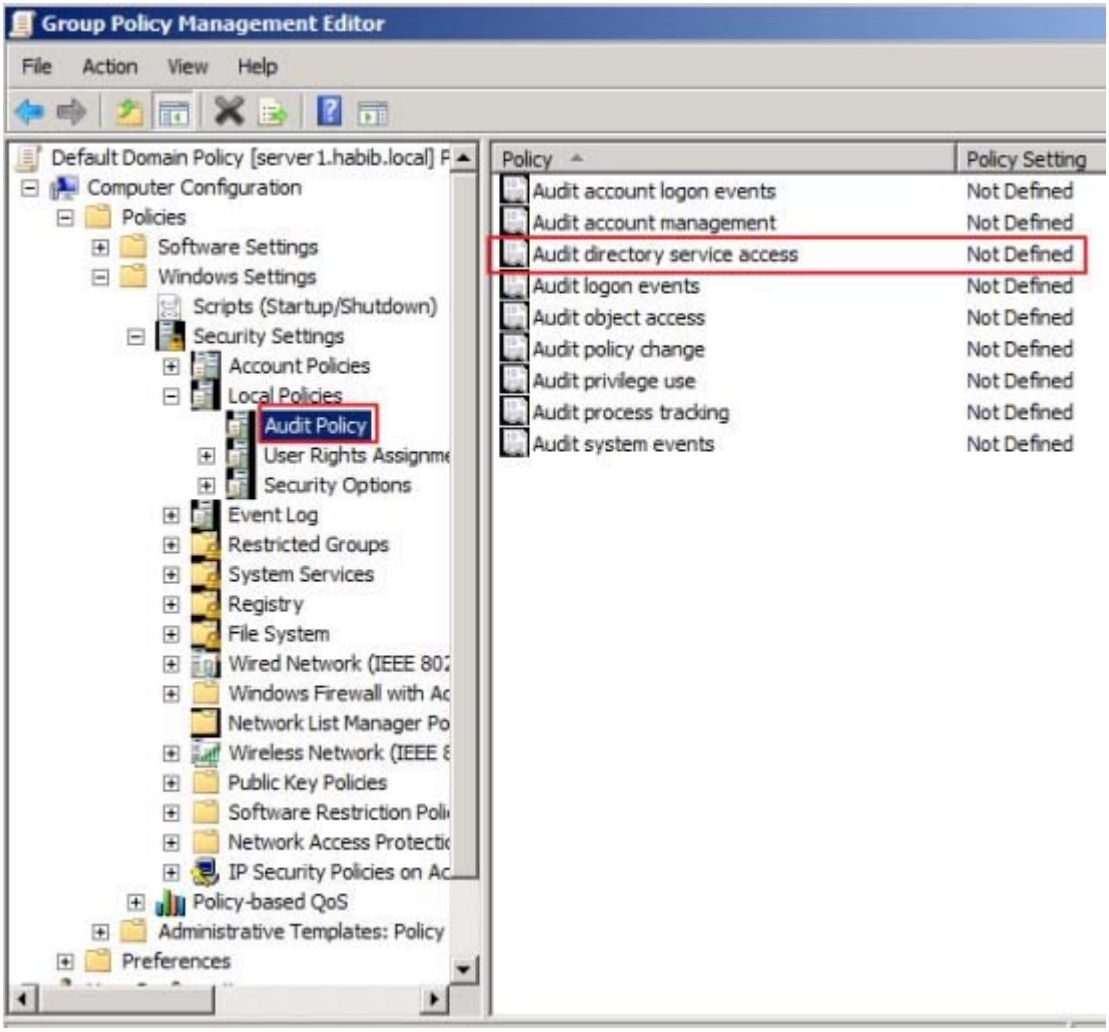
Command to view the audit policy categories and Subcategories:

```
Administrator: Command Prompt

C:\>auditpol /list /category
Category/Subcategory
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System

C:\>auditpol /list /subcategory:"DS Access"
Category/Subcategory
DS Access
  Directory Service Access
  Directory Service Changes
  Directory Service Replication
  Detailed Directory Service Replication

C:\>
```

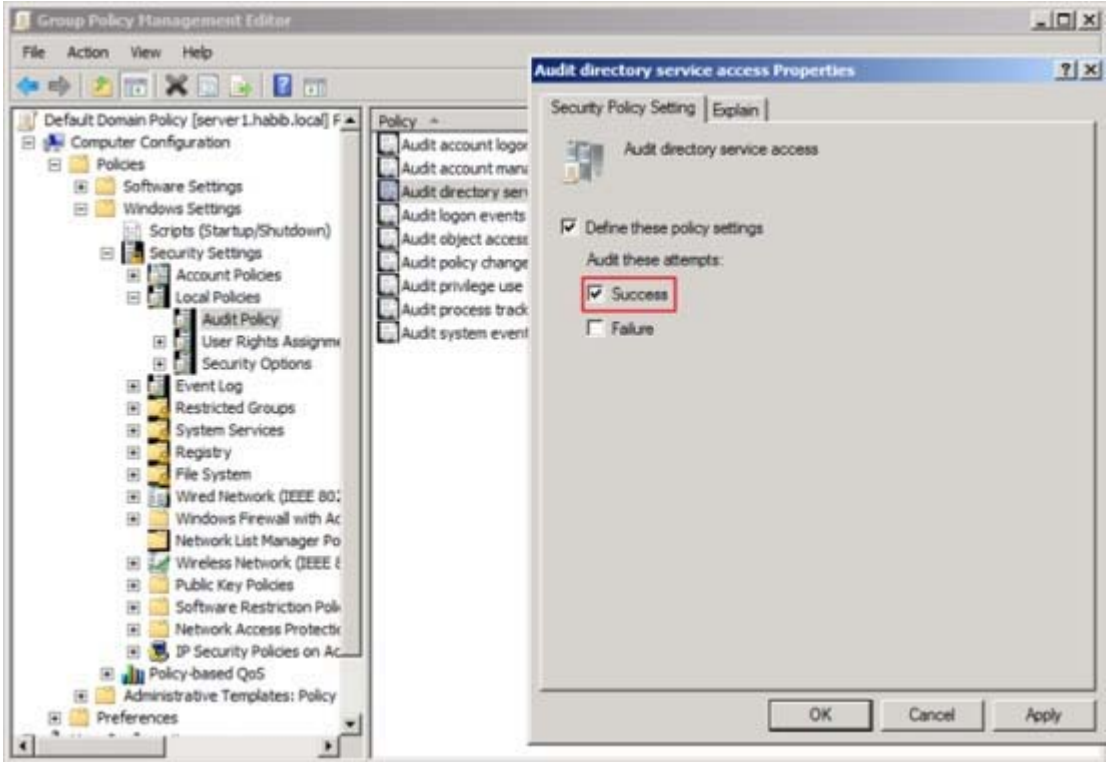
How to enable the global audit policy using the Windows interface i.e. gpmc tool
Click Start, point to Administrative Tools, and then Group Policy Management or run gpmc.msc command. In the console tree, double-click the name of the forest, double-click Domains, double-click the name of your domain, double-click Domain Controllers, right-click Default Domain Controllers Policy, and then click Edit.



Under Computer Configuration, double-click Policies, double-click Windows Settings, double-click Security Settings, double-click Local Policies, and then click Audit Policy.



In the details pane, right-click Audit directory service access, and then click Properties.
Select the Define these policy settings check box.
Under Audit these attempts, select the Success, check box, and then click OK.



How to enable the change auditing policy using a command line

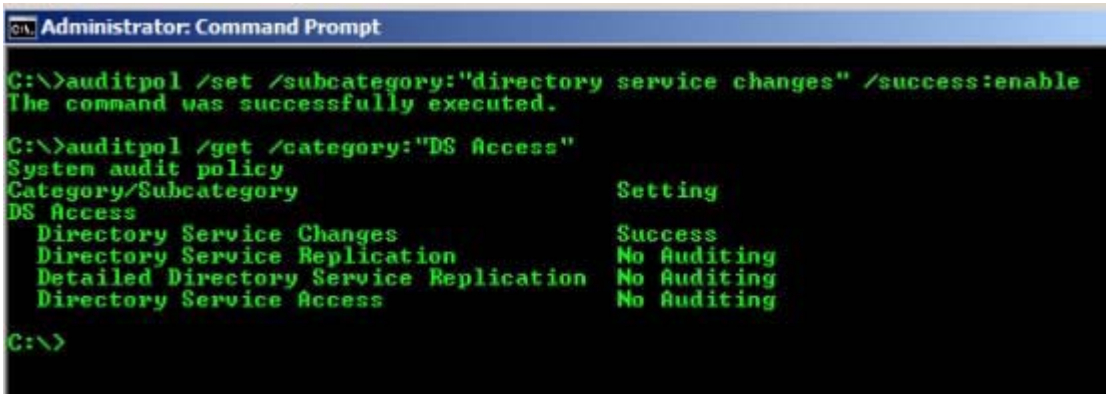
Click Start, right-click Command Prompt, and then click Run as administrator.

Type the following command, and then press ENTER:

auditpol /set /subcategory:"directory service changes" /success: enable

To verify if the auditing is enabled or not for "Directory Service Changes", you can run below command:

auditpol /get /category:"DS Access"

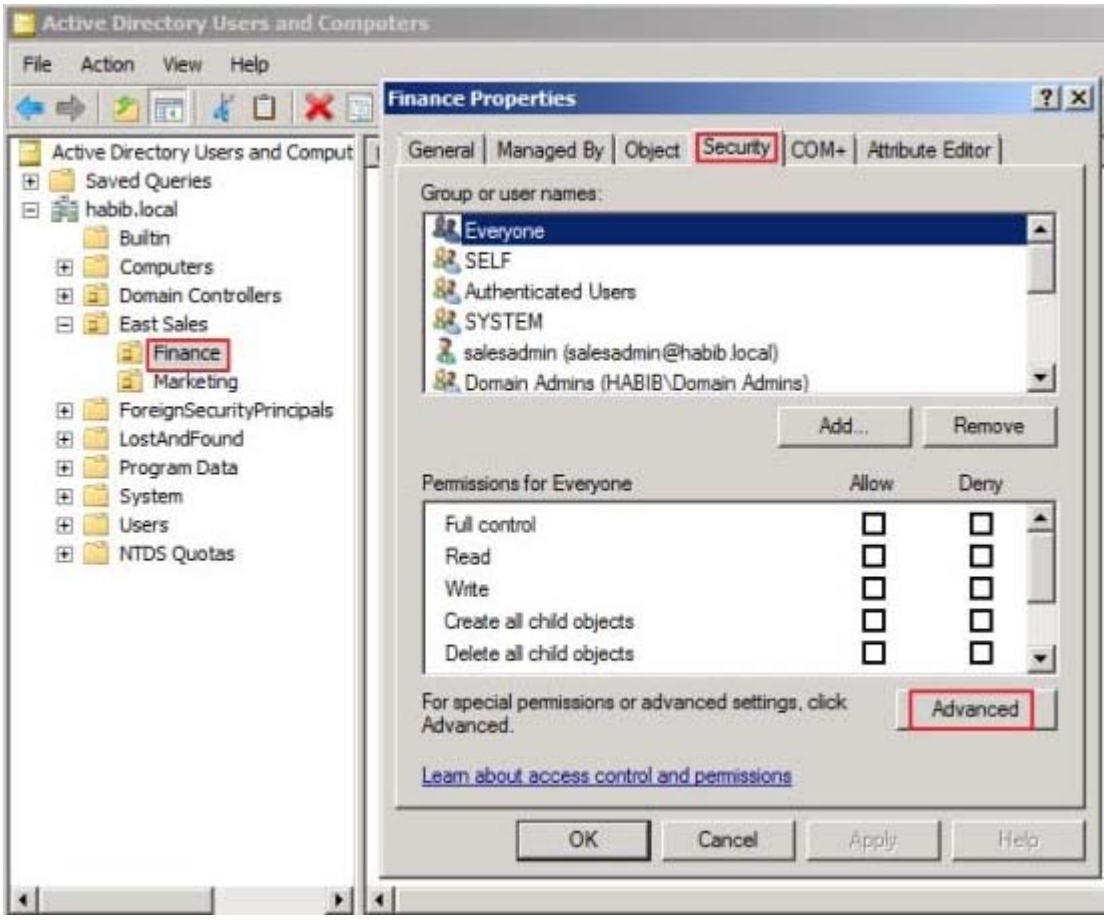


How to set up auditing in object SACLs

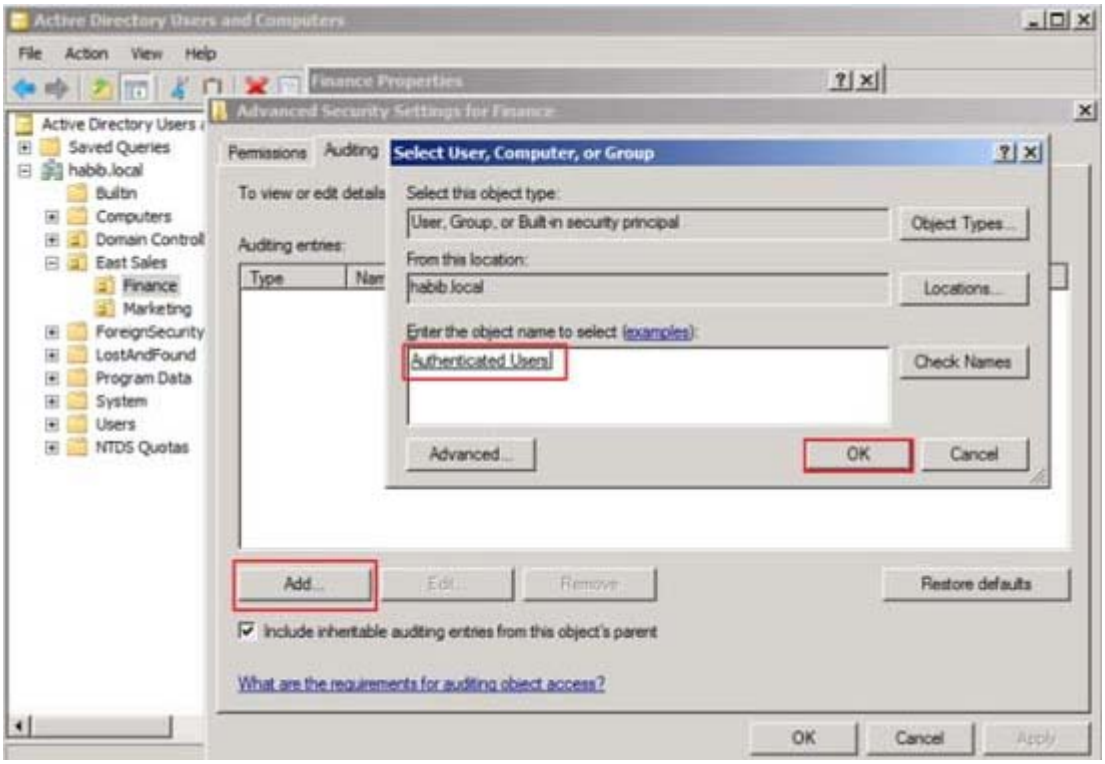
Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.

Right-click the organizational unit (OU) (or any object) for which you want to enable auditing, and then click Properties.

Click the Security tab, click Advanced, and then click the Auditing tab.

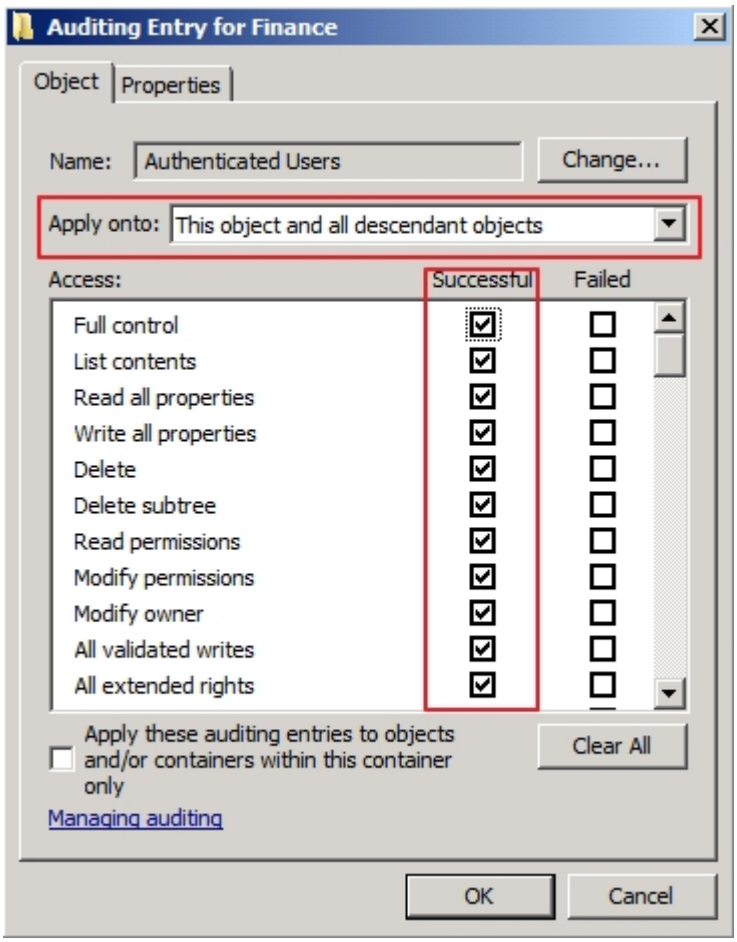


Click Add, and under Enter the object name to select, type Authenticated Users (or any other security principal) and then click OK.

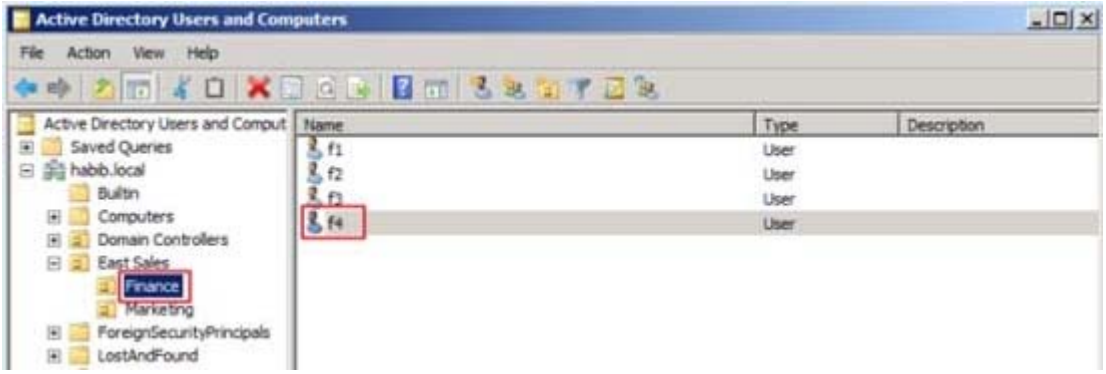


In Apply onto, click Descendant User objects (or any other objects).

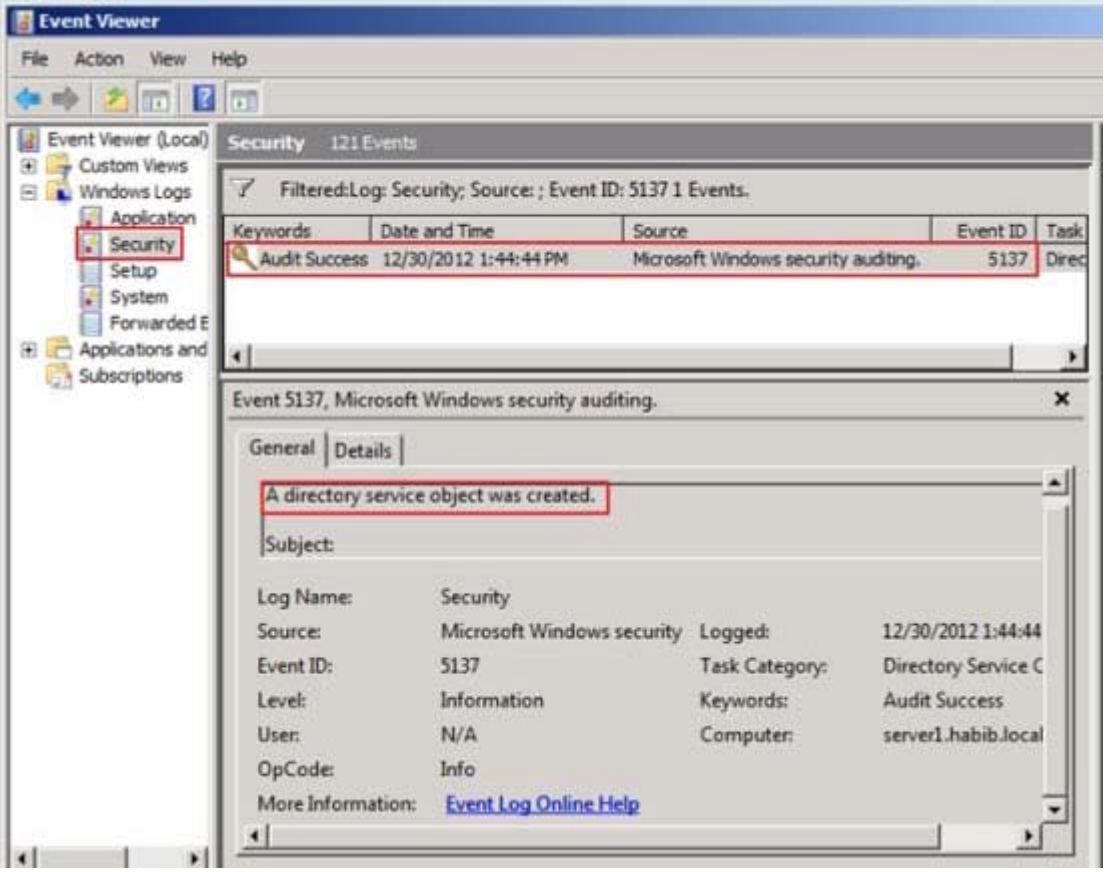
Under Access, select the Successful check box for Write all properties.
Click OK



Click OK until you exit the property sheet for the OU or other object.
To Test whether auditing is working or not, try creating or modifying objects in Finance OU and check the Security event logs.
I just created a new user account in Finance OU named f4.



If you check the security event logs you will find eventid 5137 (Create)
Note:
Once the auditing is enabled these eventids will appear in security event logs: 5136 (Modify), 5137 (Create), 5138 (Undelete), 5139 (Move).



3.Your company, Contoso Ltd has a main office and a branch office. The offices are connected by a WAN link. Contoso has an Active Directory forest that contains a single domain named ad.contoso.com. The ad.contoso.com domain contains one domain controller named DC1 that is located in the main office. DC1 is configured as a DNS server for the ad.contoso.com DNS zone. This zone is configured as a standard primary zone. You install a new domain controller named DC2 in the branch office. You install DNS on DC2. You need to ensure that the DNS service can update records and resolve DNS queries in the event that aWAN link fails.

What should you do?

A. Create a new stub zone named ad.contoso.com on DC2.

B. Create a new standard secondary zone named ad.contoso.com on DC2.

C. Configure the DNS server on DC2 to forward requests to DC1.

D. Convert the ad.contoso.com zone on DC1 to an Active Directory-integrated zone.

Answer: D

Explanation:

Answer Convert the ad.contoso.com zone on DC1 to an Active Directory-integrated zone.

http://technet.microsoft.com/en-us/library/cc726034.aspx

Understanding Active Directory Domain Services Integration

The DNS Server service is integrated into the design and implementation of Active Directory Domain Services (AD DS). AD DS provides an enterprise-level tool for organizing, managing, and locating resources in a network.

How DNS integrates with AD DS

When you install AD DS on a server, you promote the server to the role of a domain controller for a

specified domain. As part of this process, you are prompted to specify a DNS domain name for the AD DS domain which you are joining and for which you are promoting the server, and you are offered the option to install the DNS Server role. This option is provided because a DNS server is required to locate this server or other domain controllers for members of an AD DS domain.
Benefits of AD DS integration
For networks that deploy DNS to support AD DS, directory-integrated primary zones are strongly recommended. They provide the following benefits:
DNS features multimaster data replication and enhanced security based on the capabilities of AD DS. In a standard zone storage model, DNS updates are conducted based on a single-master update model. In this model, a single authoritative DNS server for a zone is designated as the primary source for the zone. This server maintains the master copy of the zone in a local file. With this model, the primary server for the zone represents a single fixed point of failure. If this server is not available, update requests from DNS clients are not processed for the zone.
With directory-integrated storage, dynamic updates to DNS are sent to any AD DS-integrated DNS server and are replicated to all other AD DS-integrated DNS servers by means of AD DS replication. In this model, any AD DS-integrated DNS servercan accept dynamic updates for the zone. Because the master copy of the zone is maintained in the AD DS database, which is fully replicated to all domain controllers, the zone can be updated by the DNS servers operating at any domain controller for the domain. With the multimaster update model of AD DS, any of the primary servers for the directoryintegrated zone can process requests from DNS clients to update the zone as long as a domain controller is available and reachable on the network.
Also, when you use directory-integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This security feature is not available with standard primary zones.
Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an AD DS domain.
By integrating storage of your DNS zone databases in AD DS, you can streamline database replication planning for your network.
Directory-integrated replication is faster and more efficient than standard DNS replication.
Further information:

4.Your company has a server that runs an instance of Active Directory Lightweight Directory Service (AD LDS). You need to create new organizational units in the AD LDS application directory partition.
What should you do?
A. Use the dsmod OU <OrganizationalUnitDN> command to create the organizational units.
B. Use the Active Directory Users and Computers snap-in to create the organizational units on the AD LDS application directory partition.
C. Use the dsadd OU <OrganizationalUnitDN> command to create the organizational units.
D. Use the ADSI Edit snap-in to create the organizational units on the AD LDS application directory partition.
Answer: D
Explanation:

Answer Use the ADSI Edit snap-in to create the organizational units on the AD LDS application directory partition.
http://technet.microsoft.com/en-us/library/cc773354%28v=ws.10%29.aspx
ADSI Edit (adsiedit.msc)
Active Directory® Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit.msc) provides a view of every object and attribute in an Active Directory forest. You can use ADSI Edit to query, view, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap-ins: Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema.
http://technet.microsoft.com/en-us/library/cc730701%28v=ws.10%29.aspx#BKMK_1
Step 4: Practice Managing AD LDS Organizational Units, Groups, and Users
Create an OU
To keep your AD LDS users and groups organized, you may want to place users and groups in OUs. In Active
Directory Domain Services (AD DS) and in AD LDS, as well as in other Lightweight Directory Access Protocol
(LDAP)–based directories, OUs are most commonly used for keeping users and groups organized.
To create an OU
1. Click Start, point to Administrative Tools, and then click ADSI Edit.
2. Connect and bind to the directory partition of the AD LDS instance to which you want to add an OU.
3. In the console tree, double-click the o=Microsoft,c=US directory partition, right-click the container to which you want to add the OU, point to New, and then click Object.
4. In Select a class, click organizationalUnit, and then click Next.
5. In Value, type a name for the new OU, and then click Next.
6. If you want to set values for additional attributes, click More attributes.
Further information:
http://technet.microsoft.com/en-us/library/cc754663%28v=ws.10%29.aspx
Step 5: Practice Working with Application Directory Partitions
The Active Directory Lightweight Directory Services (AD LDS) directory store is organized into logical directory partitions. There are three different types of directory partitions:
Configuration directory partitions
Schema directory partitions
Application directory partitions
Each AD LDS directory store must contain a single configuration directory partition and a single schema directory partition. The directory store can contain zero or more application directory partitions. Application directory partitions hold the data that your applications use. You can create an application directory partition during AD LDS setup or anytime after installation.

5.Your company has an Active Directory domain. The company has two domain controllers named DC1 and DC2. DC1 holds the Schema Master role. DC1 fails. You log on to Active Directory by using the administrator account. You are not able to transfer the Schema Master operations role. You need to ensure that DC2 holds the Schema Master role.
What should you do?

A. Configure DC2 as a bridgehead server.
B. On DC2, seize the Schema Master role.
C. Log off and log on again to Active Directory by using an account that is a member of the Schema Administrators group. Start the Active Directory Schema snap-in.
D. Register the Schmmgmt.dll. Start the Active Directory Schema snap-in.
Answer: B
Explanation:
Answer On DC2, seize the Schema Master role.
http://technet.microsoft.com/en-us/library/cc816645%28v=ws.10%29.aspx
Transfer the Schema Master
You can use this procedure to transfer the schema operations master role if the domain controller that currently hosts the role is inadequate, has failed, or is being decommissioned. The schema master is a forest-wide operations master (also known as flexible single master operations or FSMO) role.
..
Note: You perform this procedure by using a Microsoft Management Console (MMC) snap-in, although you can also transfer this role by using Ntdsutil.exe.
Membership in Schema Admins, or equivalent, is the minimum required to complete this procedure.
http://technet.microsoft.com/en-us/library/cc794853%28v=ws.10%29.aspx
Seize the AD LDS Schema Master Role
The schema master is responsible for performing updates to the Active Directory Lightweight Directory Services (AD LDS) schema. Each configuration set has only one schema master. All write operations to the AD
LDS schema can be performed only when connected to the AD LDS instance that holds the schema master role within its configuration set. Those schema updates are replicated from the schema master to all other instances in the configuration set.
Membership in the AD LDS Administrators group, or equivalent, is the minimum required to complete this procedure.
Caution: Do not seize the schema master role if you can transfer it instead. Seizing the schema master role is a drastic step that should be considered only if the current operations master will never be available again.

6.Your company has an Active Directory forest that runs at the functional level of Windows Server 2008. You implement Active Directory Rights Management Services (AD RMS). You install Microsoft SQL Server 2005. When you attempt to open the AD RMS administration Web site, you receive the following error message: "SQL Server does not exist or access denied."
You need to open the AD RMS administration Web site.
Which two actions should you perform? (Each correct answer presents part of the solution.
Choose two.)
A. Restart IIS.
B. Manually delete the Service Connection Point in AD DS and restart AD RMS.
C. Install Message Queuing.
D. Start the MSSQLSVC service.
Answer: A, D
Explanation:

http://technet.microsoft.com/en-us/library/cc747605%28v=ws.10%29.aspx#BKMK_1
RMS Administration Issues
"SQL Server does not exist or access denied" message received when attempting to open the RMS Administration Web site
If you have installed RMS by using a new installation of SQL Server 2005 as your database server the SQL Server Service might not be started. In SQL Server 2005, the MSSQLSERVER service is not configured to automatically start when the server is started. If you have restarted your SQL Server since installing RMS and have not configured this service to automatically restart RMS will not be able to function and only the RMS Global Administration page will be accessible.
After you have started the MSSQLSERVER service, you must restart IIS on each RMS server in the cluster to restore RMS functionality.

7.Your network consists of an Active Directory forest that contains one domain named contoso.com. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers. You have two Active Directory-integrated zones: contoso.com and nwtraders.com. You need to ensure a user is able to modify records in the contoso.com zone. You must prevent the user from modifying the SOA record in the nwtraders.com zone.
What should you do?
A. From the Active Directory Users and Computers console, run the Delegation of Control Wizard.
B. From the Active Directory Users and Computers console, modify the permissions of the Domain Controllers organizational unit (OU).
C. From the DNS Manager console, modify the permissions of the contoso.com zone.
D. From the DNS Manager console, modify the permissions of the nwtraders.com zone.
Answer: C
Explanation:
Answer From the DNS Manager console, modify the permissions of the contoso.com zone.
http://technet.microsoft.com/en-us/library/cc753213.aspx
Modify Security for a Directory-Integrated Zone
You can manage the discretionary access control list (DACL) on the DNS zones that are stored in Active Directory Domain Services (AD DS). You can use the DACL to control the permissions for the Active Directory users and groups that may control the DNS zones.
Membership in DnsAdmins or Domain Admins in AD DS, or the equivalent, is the minimum required to complete this procedure.
To modify security for a directory-integrated zone:
1. Open DNS Manager.
2. In the console tree, click the applicable zone.
Where?
DNS/applicable DNS server/Forward Lookup Zones (or Reverse Lookup Zones)/applicable zone
3. On the Action menu, click Properties.
4. On the General tab, verify that the zone type is Active Directory-integrated.
5. On the Security tab, modify the list of member users or groups that are allowed to securely update the applicable zone and reset their permissions as needed.
Further information:
http://support.microsoft.com/kb/163971

The Structure of a DNS SOA Record
The first resource record in any Domain Name System (DNS) Zone file should be a Start of Authority (SOA) resource record. The SOA resource record indicates that this DNS name server is the best source of information for the data within this DNS domain.
The SOA resource record contains the following information:
Source host - The host where the file was created.
Contact e-mail - The e-mail address of the person responsible for administering the domain's zone file. Note that a "." is used instead of an "@" in the e-mail name.
Serial number - The revision number of this zone file. Increment this number each time the zone file is changed. It is important to increment this value each time a change is made, so that the changes will be distributed to any secondary DNS servers.
Refresh Time - The time, in seconds, a secondary DNS server waits before querying the primary DNS server's SOA record to check for changes. When the refresh time expires, the secondary DNS server requests a copy of the current SOA record from the primary. The primary DNS server complies with this request. The secondary DNS server compares the serial number of the primary DNS server's current SOA record and the serial number in it's own SOA record. If they are different, the secondary DNS server will request a zone transfer from the primary DNS server. The default value is 3,600.
Retry time - The time, in seconds, a secondary server waits before retrying a failed zone transfer. Normally, the retry time is less than the refresh time. The default value is 600.
Expire time - The time, in seconds, that a secondary server will keep trying to complete a zone transfer. If this time expires prior to a successful zone transfer, the secondary server will expire its zone file. This means the secondary will stop answering queries, as it considers its data too old to be reliable. The default value is 86,400.
Minimum TTL - The minimum time-to-live value applies to all resource records in the zone file. This value is supplied in query responses to inform other servers how long they should keep the data in cache. The default value is 3,600.
http://technet.microsoft.com/en-us/library/cc787600%28v=ws.10%29.aspx
Modify the start of authority (SOA) record for a zone
..
Notes: To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.

8.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.

Answer: C
Explanation:
Answer Implement an Online Certificate Status Protocol (OCSP) responder by using Network Load Balancing.
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.

9.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.

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.

10.Your company has an Active Directory domain. A user attempts to log on to a computer that was turned off for twelve weeks. The administrator receives an error message that authentication has failed. You need to ensure that the user is able to log on to the computer.
What should you do?
A. Run the netsh command with the set and machine options.
B. Reset the computer account. Disjoin the computer from the domain, and then rejoin the computer to the domain.
C. Run the netdom TRUST /reset command.
D. Run the Active Directory Users and Computers console to disable, and then enable the computer account.
Answer: B
Explanation:
Answer Reset the computer account. Disjoin the computer from the domain, and then rejoin the computer to the domain.
http://social.technet.microsoft.com/wiki/contents/articles/9157.trust-relationship-between-workstation-and primary-domain-failed.aspx
Trust Relationship between Workstation and Primary Domain failed
What are the common causes which generates this message on client systems?
There might be multiple reasons for this kind of behaviour. Below are listed a few of them:
1. Single SID has been assigned to multiple computers.
2. If the Secure Channel is Broken between Domain controller and workstations
3. If there are no SPN or DNSHost Name mentioned in the computer account attributes
4. Outdated NIC Drivers.
How to Troubleshoot this behaviour?
..
2. If the Secure Channel is Broken between Domain controller and workstations
When a Computer account is joined to the domain, Secure Channel password is stored with computer account in domain controller. By default this password will change every 30 days (This is an automatic

process, no manual intervention is required). Upon starting the computer, Netlogon attempts to discover a DC for the domain in which its machine account exists. After locating the appropriate DC, the machine account password from the workstation is authenticated against the password on the DC.
If there are problems with system time, DNS configuration or other settings, secure channel's password between Workstation and DCs may not synchronize with each other.
A common cause of broken secure channel [machine account password] is that the secure channel password held by the domain member does not match that held by the AD. Often, this is caused by performing a Windows System Restore (or reverting to previous backup or snapshot) on the member machine, causing an old (previous) machine account password to be presented to the AD.
Resolution:
Most simple resolution would be unjoin/disjoin the computer from the domain and rejoin the computer account back to the domain. (this is a somewhat similar principle to performing a password reset for a user account)
Or
You can go ahead and reset the computer account using netdom.exe tool
http://technet.microsoft.com/en-us/library/cc772217%28v=ws.10%29.aspx
Netdom
Enables administrators to manage Active Directory domains and trust relationships from the command prompt.
Netdom is a command-line tool that is built into Windows Server 2008 and Windows Server 2008 R2. It is available if you have the Active Directory Domain Services (AD DS) server role installed. It is also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT).
You can use netdom to:
Join a computer that runs Windows XP Professional, Windows Vista, or Windows 7 to a Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows 2000, or Windows NT 4.0 domain.
Manage computer accounts for domain member workstations and member servers. Management operations include:
Establish one-way or two-way trust relationships between domains, including the following kinds of trust relationships:
Verify or reset the secure channel for the following configurations:
* Member workstations and servers.
* Backup domain controllers (BDCs) in a Windows NT 4.0 domain.
* Specific Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, or Windows 2000 replicas.
Manage trust relationships between domains.
Syntax
NetDom <Operation> [<Computer>] [{/d: | /domain :} <Domain>] [<Options>]
http://technet.microsoft.com/en-us/library/cc788073%28v=ws.10%29.aspx
Netdom reset Resets the secure connection between a workstation and a domain controller.
Syntax netdom reset <Computer> {/d: | /domain :}< Domain> [{/s: | /server :}< Server>] [{/uo: | /usero :}< User> {/po: | /
passwordo} {<Password>|*}] [{/help | /?}]
Further information:

http://technet.microsoft.com/en-us/library/cc835085%28v=ws.10%29.aspx
Netdom trust
Establishes, verifies, or resets a trust relationship between domains.
Syntax netdom trust <TrustingDomainName> {/d: | /domain:} <TrustedDomainName> [{/ud: | /userd:}[<Domain>\]<User> [{/pd: | /passwordd:}{<Password>|*}] [{/uo: | /usero:}<User>] [{/po: | /passwordo:}{<Password>|*}] [/verify] [/reset] [/passwordt:<NewRealmTrustPassword>] [/add [/realm]] [/remove [/force]] [/twoway] [/kerberos] [/transitive[:{YES|NO}]] [/oneside:{TRUSTED | TRUSTING}] [/force] [/quarantine[:{YES | NO}]] [/namesuffixes:<TrustName> [/togglesuffix:#]] [/EnableSIDHistory] [/ForestTRANsitive] [/SelectiveAUTH][/AddTLN][/AddTLNEX][/RemoveTLN] [/RemoveTLNEX][{/help | /?}]

11.Your company has an Active Directory forest that contains a single domain. The domain member server has an Active Directory Federation Services (AD FS) role installed. You need to configure AD FS to ensure that AD FS tokens contain information from the Active Directory domain.
What should you do?
A. Add and configure a new account partner.
B. Add and configure a new resource partner.
C. Add and configure a new account store.
D. Add and configure a Claims-aware application.
Answer: C
Explanation:
http://technet.microsoft.com/en-us/library/cc732095.aspx
Understanding Account Stores
Active Directory Federation Services (AD FS) uses account stores to log on users and extract security claims for those users. You can configure multiple account stores for a single Federation Service. You can also define their priority. The Federation Service uses Lightweight Directory Access Protocol (LDAP) to communicate with account stores. AD FS supports the following two account stores:
Active Directory Domain Services (AD DS)
Active Directory Lightweight Directory Services (AD LDS)

12.You network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. You need to reset the Directory Services Restore Mode (DSRM) password on a domain controller.
What tool should you use?
A. Active Directory Users and Computers snap-in
B. ntdsutil
C. Local Users and Groups snap-in
D. dsmod
Answer: B
Explanation:
http://technet.microsoft.com/en-us/library/cc753343%28v=ws.10%29.aspx
Ntdsutil
Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the ntdsutil commands to perform database maintenance of AD DS, manage and control single master operations,

and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for use by experienced administrators.
..
Commands set DSRM password - Resets the Directory Services Restore Mode (DSRM) administrator password.
Further information:
http://technet.microsoft.com/en-us/library/cc754363%28v=ws.10%29.aspx
Set DSRM password
Resets the Directory Services Restore Mode (DSRM) password on a domain controller. At the Reset DSRM Administrator Password: prompt, type any of the parameters listed under “Syntax.”
This is a subcommand of Ntdsutil and Dsmgmt. Ntdsutil and Dsmgmt are command-line tools that are built into Windows Server 2008 and Windows Server 2008 R2. Ntdsutil is available if you have the Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS) server role installed.
Dsmgmt is available if you have the AD LDS server role installed. These tools are also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT).

13.Your company has a main office and a branch office. You deploy a read-only domain controller (RODC) that runs Microsoft Windows Server 2008 to the branch office. You need to ensure that users at the branch office are able to log on to the domain by using the RODC.
What should you do?
A. Add another RODC to the branch office.
B. Configure a new bridgehead server in the main office.
C. Decrease the replication interval for all connection objects by using the Active Directory Sites and Services console.
D. Configure the Password Replication Policy on the RODC.
Answer: D
Explanation:
Answer Configure the Password Replication Policy on the RODC.
http://technet.microsoft.com/en-us/library/cc754956%28v=ws.10%29.aspx
RODC Frequently Asked Questions
What new attributes support the RODC Password Replication Policy?
Password Replication Policy is the mechanism for determining whether a user or computer's credentials are allowed to replicate from a writable domain controller to an RODC. The Password Replication Policy is always set on a writable domain controller running Windows Server 2008.
What operations fail if the WAN is offline, but the RODC is online in the branch office?
If the RODC cannot connect to a writable domain controller running Windows Server 2008 in the hub, the following branch office operations fail:
Password changes
Attempts to join a computer to a domain
Computer rename
Authentication attempts for accounts whose credentials are not cached on the RODC
Group Policy updates that an administrator might attempt by running the gpupdate /force command

What operations succeed if the WAN is offline, but the RODC is online in the branch office?
If the RODC cannot connect to a writable domain controller running Windows Server 2008 in the hub, the following branch office operations succeed:
Authentication and logon attempts, if the credentials for the resource and the requester are already cached, Local RODC server administration performed by a delegated RODC server administrator.

14.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.
Answer: A
Explanation:
Answer Set dynamic updates to Secure Only.
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

15.Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers. A domain controller named DC1 has a standard primary zone for contoso.com. A domain controller named DC2 has a standard secondary zone for contoso.com. You need to ensure that the replication of the contoso.com zone is encrypted. You must not lose any zone data.
What should you do?
A. Convert the primary zone into an Active Directory-integrated stub zone. Delete the secondary zone.
B. Convert the primary zone into an Active Directory-integrated zone. Delete the secondary zone.
C. Configure the zone transfer settings of the standard primary zone. Modify the Master Servers lists on the secondary zone.
D. On both servers, modify the interface that the DNS server listens on.
Answer: B

Explanation:
Answer Convert the primary zone into an Active Directory-integrated zone. Delete the secondary zone.
http://technet.microsoft.com/en-us/library/cc771150.aspx
Change the Zone Type
You can use this procedure to change make a zone a primary, secondary, or stub zone. You can also use it to integrate a zone with Active Directory Domain Services (AD DS).
http://technet.microsoft.com/en-us/library/cc726034.aspx
Understanding Active Directory Domain Services Integration
The DNS Server service is integrated into the design and implementation of Active Directory Domain Services (AD DS). AD DS provides an enterprise-level tool for organizing, managing, and locating resources in a network.
Benefits of AD DS integration
For networks that deploy DNS to support AD DS, directory-integrated primary zones are strongly recommended. They provide the following benefits:
DNS features multimaster data replication and enhanced security based on the capabilities of AD DS.
In a standard zone storage model, DNS updates are conducted based on a single-master update model. In this model, a single authoritative DNS server for a zone is designated as the primary source for the zone. This server maintains the master copy of the zone in a local file. With this model, the primary server for the zone represents a single fixed point of failure. If this server is not available, update requests from DNS clients are not processed for the zone.
With directory-integrated storage, dynamic updates to DNS are sent to any AD DS-integrated DNS server and are replicated to all other AD DS-integrated DNS servers by means of AD DS replication. In this model, any AD DS-integrated DNS servercan accept dynamic updates for the zone. Because the master copy of the zone is maintained in the AD DS database, which is fully replicated to all domain controllers, the zone can be updated by the DNS servers operating at any domain controller for the domain. With the multimaster update model of AD DS, any of the primary servers for the directoryintegrated zone can process requests from DNS clients to update the zone as long as a domain controller is available and reachable on the network.
..
Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an AD DS domain.
By integrating storage of your DNS zone databases in AD DS, you can streamline database replication planning for your network.
Directory-integrated replication is faster and more efficient than standard DNS replication.
http://technet.microsoft.com/en-us/library/ee649124%28v=ws.10%29.aspx
Deploy IPsec Policy to DNS Servers
You can deploy IPsec rules through one of the following mechanisms:
Domain Controllers organizational unit (OU): If the DNS servers in your domain are Active Directoryintegrated, you can deploy IPsec policy settings using the Domain Controllers OU. This option is recommended to make configuration and deployment easier.
DNS Server OU or security group: If you have DNS servers that are not domain controllers, then consider creating a separate OU or a security group with the computer accounts of your DNS servers.
Local firewall configuration: Use this option if you have DNS servers that are not domain members or if you have a small number of DNS servers that you want to configure locally.

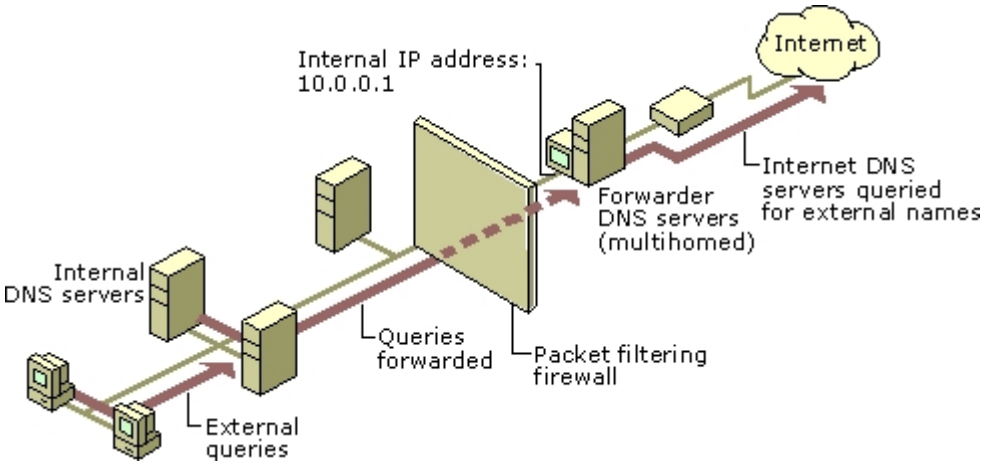
http://technet.microsoft.com/en-us/library/cc772661%28v=ws.10%29.aspx
Deploying Secure DNS
Protecting DNS Servers
When the integrity of the responses of a DNS server are compromised or corrupted, or when the DNS data is tampered with, clients can be misdirected to unauthorized locations without their knowledge. After the clients start communicating with these unauthorized locations, attempts can be made to gain access to information that is stored on the client computers. Spoofing and cache pollution are examples of this type of attack. Another type of attack, the denial-of-service attack, attempts to incapacitate a DNS server to make DNS infrastructure unavailable in an enterprise. To protect your DNS servers from these types of attacks:
Use IPsec between DNS clients and servers.
Monitor network activity.
Close all unused firewall ports.
Implementing IPsec Between DNS Clients and Servers
IPsec encrypts all traffic over a network connection. Encryption minimizes the risk that data that is sent between the DNS clients and the DNS servers can be scanned for sensitive information or tampered with by anyone attempting to collect information by monitoring traffic on the network. When IPsec is enabled, both ends of a connection are validated before communication begins. A client can be certain that the DNS server with which it is communicating is a valid server. Also, all communication over the connection is encrypted, thereby eliminating the possibility of tampering with client communication. Encryption prevents spoofing attacks, which are false responses to DNS client queries by unauthorized sources that act like a DNS server.
Further information:
http://technet.microsoft.com/en-us/library/cc771898.aspx
Understanding Zone Types
The DNS Server service provides for three types of zones:
Primary zone
Secondary zone
Stub zone
Note: If the DNS server is also an Active Directory Domain Services (AD DS) domain controller, primary zones and stub zones can be stored in AD DS.
The following sections describe each of these zone types:
Primary zone When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named zone_name.dns and it is located in the % windir%\System32\Dns folder on the server.
Secondary zone When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.
Stub zone
When a zone that this DNS server hosts is a stub zone, this DNS server is a source only for information

about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.
You can use stub zones to:
Keep delegated zone information current. By updating a stub zone for one of its child zones regularly, the DNS server that hosts both the parent zone and the stub zone will maintain a current list of authoritative DNS servers for the child zone.
Improve name resolution. Stub zones enable a DNS server to perform recursion using the stub zone's list of name servers, without having to query the Internet or an internal root server for the DNS namespace.
Simplify DNS administration. By using stub zones throughout your DNS infrastructure, you can distribute a list of the authoritative DNS servers for a zone without using secondary zones. However, stub zones do not serve the same purpose as secondary zones, and they are not an alternative for enhancing redundancy and load sharing.
There are two lists of DNS servers involved in the loading and maintenance of a stub zone:
The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.
The list of the authoritative DNS servers for a zone. This list is contained in the stub zone using name server (NS) resource records.
When a DNS server loads a stub zone, such as widgets.tailspintoys.com, it queries the master servers, which can be in different locations, for the necessary resource records of the authoritative servers for the zone widgets.tailspintoys.com. The list of master servers may contain a single server or multiple servers, and it can be changed anytime.
http://social.technet.microsoft.com/Forums/en-US/winserverNIS/thread/d352966e-b1ec-46b6-a8b4-317c2c3388c3/
Answered what is non-standard dns secondary zone?
Q: While passing through 70-291 exam prep questions, I encountered the term "standard secondary zone".
From the context of other questions I understood that "standard", in context of primary zone, mean "non-ADintegrated".
A: Standard means it is not an AD integrated zone. AD integrated zones are stored in the AD database and not in a text file.
Q: What does "standard" mean in context of DNS secondary zone?
A: It means the same thing in context of a Standard Primary Zone. Simply stated, "Standard" means the zone data is stored in a text file, which can be found in system32\dns.

16.You are decommissioning domain controllers that hold all forest-wide operations master roles. You need to transfer all forest-wide operations master roles to another domain controller.
Which two roles should you transfer? (Each correct answer presents part of the solution. Choose two.)
A. Domain naming master
B. Infrastructure master
C. RID master
D. PDC emulator
E. Schema master

Answer: A, E
Explanation:
Answer Schema master
Domain naming master
http://social.technet.microsoft.com/wiki/contents/articles/832.transferring-fsmo-roles-in-indows-server-2008.aspx
Transferring FSMO Roles in Windows Server 2008
One of any system administrator duties, would be to upgrade a current domain controller to a new hardware server. One of the crucial steps required to successfully migrate your domain controller, is to be able to successfully transfer the FSMO roles to the new hardware server. FSMO stands for Flexible Single Master
Operations, and in a forest there are at least five roles.
The five FSMO roles are:
Schema Master
Domain Naming Master
Infrastructure Master
Relative ID (RID) Master
PDC Emulator
The first two roles above are forest-wide, meaning there is one of each for the entire forest. The last three are domain-wide, meaning there is one of each per domain. If there is one domain in your forest, you will have five FSMO roles. If you have three domains in your forest, there will be 11 FSMO roles.

17.Contoso, Ltd. has an Active Directory domain named ad.contoso.com. Fabrikam, Inc. has an Active Directory domain named intranet.fabrikam.com. Fabrikam's security policy prohibits the transfer of internal DNS zone data outside the Fabrikam network. You need to ensure that the Contoso users are able to resolve names from the intranet.fabrikam.com domain.
What should you do?
A. Create a new stub zone for the intranet.fabrikam.com domain.
B. Configure conditional forwarding for the intranet.fabrikam.com domain.
C. Create a standard secondary zone for the intranet.fabrikam.com domain.
D. Create an Active DirectoryCintegrated zone for the intranet.fabrikam.com domain.
Answer: B
Explanation:
Answer Configure conditional forwarding for the intranet.fabrikam.com domain.
http://technet.microsoft.com/en-us/library/cc730756.aspx
Understanding Forwarders
A forwarder is a Domain Name System (DNS) server on a network that forwards DNS queries for external DNS names to DNS servers outside that network. You can also forward queries according to specific domain names using conditional forwarders.
You designate a DNS server on a network as a forwarder by configuring the other DNS servers in the network to forward the queries that they cannot resolve locally to that DNS server. By using a forwarder, you can manage name resolution for names outside your network, such as names on the Internet, and improve the efficiency of name resolution for the computers in your network.
The following figure illustrates how external name queries are directed with forwarders.



Conditional forwarders

A conditional forwarder is a DNS server on a network that forwards DNS queries according to the DNS domain name in the query. For example, you can configure a DNS server to forward all the queries that it receives for names ending with corp.contoso.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.

Further information:

http://technet.microsoft.com/en-us/library/cc794735%28v=ws.10%29.aspx

Assign a Conditional Forwarder for a Domain Name

http://technet.microsoft.com/en-us/library/cc754941.aspx

Configure a DNS Server to Use Forwarders

18.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.

Answer: D

19.Your company has file servers located in an organizational unit named Payroll. The file servers contain payroll files located in a folder named Payroll. You create a GPO. You need to track which employees access the Payroll files on the file servers.

What should you do?

A. Enable the Audit process tracking option. Link the GPO to the Domain Controllers organizational unit. On the file servers, configure Auditing for the Authenticated Users group in the Payroll folder.

B. Enable the Audit object access option. Link the GPO to the Payroll organizational unit. On the file servers, configure Auditing for the Everyone group in the Payroll folder.

C. Enable the Audit process tracking option. Link the GPO to the Payroll organizational unit. On the file servers, configure Auditing for the Everyone group in the Payroll folder.

D. Enable the Audit object access option. Link the GPO to the domain. On the domain controllers, configure Auditing for the Authenticated Users group in the Payroll folder.

Answer: B
Explanation:
Answer Enable the Audit object access option. Link the GPO to the Payroll organizational unit. On the file servers, configure Auditing for the Everyone group in the Payroll folder.
http://technet.microsoft.com/en-us/library/dd349800%28v=ws.10%29.aspx
Audit Policy
Establishing an organizational computer system audit policy is an important facet of information security. Configuring Audit policy settings that monitor the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.
There are nine different kinds of events for which you can specify Audit Policy settings. If you audit any of these kinds of events, Windows® records the events in the Security log, which you can find in Event Viewer.
..
Object access. Audit this to record when someone has used a file, folder, printer, or other object.
..
Process tracking. Audit this to record when events such as program activation or a process exiting occur.
..
When you implement Audit Policy settings:
..
If you want to audit directory service access or object access, determine which objects you want to audit access of and what type of access you want to audit. For example, if you want to audit all attempts by users to open a particular file, you can configure audit policy settings in the object access event category so that both successful and failed attempts to read a file are recorded.
Further information:
http://technet.microsoft.com/en-us/library/hh147307%28v=ws.10%29.aspx
Group Policy for Beginners
Group Policy Links
At the top level of AD DS are sites and domains. Simple implementations will have a single site and a single domain. Within a domain, you can create organizational units (OUs). OUs are like folders in Windows Explorer.
Instead of containing files and subfolders, however, they can contain computers, users, and other objects. For example, in Figure 1 you see an OU named Departments. Below the Departments OU, you see four subfolders: Accounting, Engineering, Management, and Marketing. These are child OUs. Other than the Domain Controllers OU that you see in Figure 1, nothing else in the figure is an OU.
What does this have to do with Group Policy links? Well, GPOs in the Group Policy objects folder have no impact unless you link them to a site, domain, or OU. When you link a GPO to a container, Group Policy applies the GPO's settings to the computers and users in that container.

20.Your company uses a Windows 2008 Enterprise certificate authority (CA) to issue certificates. You need to implement key archival.
What should you do?
A. Configure the certificate for automatic enrollment for the computers that store encrypted files.
B. Install an Enterprise Subordinate CA and issue a user certificate to users of the encrypted files.

C. Apply the Hisecdc security template to the domain controllers.
D. Archive the private key on the server.
Answer: D
Explanation:
Answer Archive the private key on the server.
http://technet.microsoft.com/en-us/library/cc753011.aspx
Enable Key Archival for a CA
Before a key recovery agent can use a key recovery certificate, the key recovery agent must have enrolled for the key recovery certificate and be registered as the recovery agent for the certification authority (CA).
You must be a CA administrator to complete this procedure.
To enable key archival for a CA:
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. Click the Recovery Agents tab, and then click Archive the key.
5. In Number of recovery agents to use, type the number of key recovery agents that will be used to encrypt the archived key.
The Number of recovery agents to use must be between one and the number of key recovery agent certificates that have been configured.
6. Click Add. Then, in Key Recovery Agent Selection, click the key recovery certificates that are displayed, and click OK.
7. The certificates should appear in the Key recovery agent certificates list, but their status is listed as Not loaded.
8. Click OK or Apply. When prompted to restart the CA, click Yes. When the CA has restarted, the status of the certificates should be listed as Valid.
Further information:
http://technet.microsoft.com/en-us/library/ee449489%28v=ws.10%29.aspx
Key Archival and Management in Windows Server 2008
http://technet.microsoft.com/en-us/library/cc730721.aspx
Managing Key Archival and Recovery