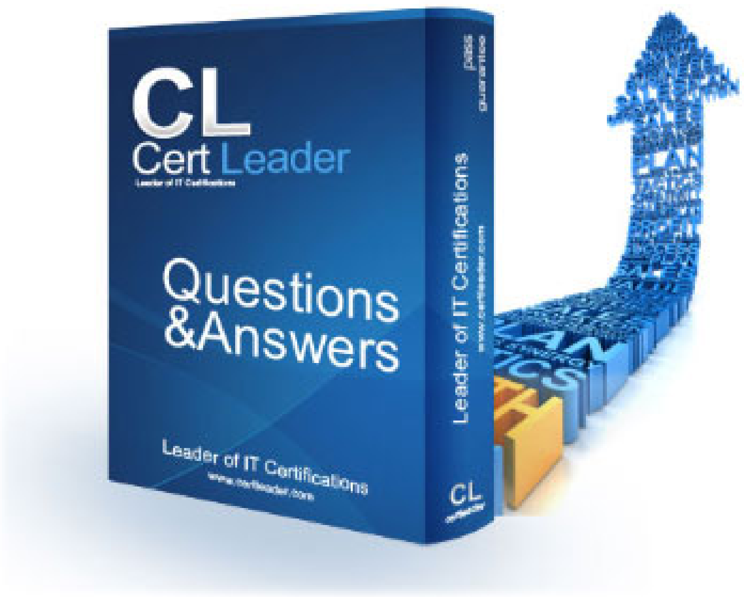
70-640 Dumps

TS: Windows Server 2008 Active Directory. Configuring

https://www.certleader.com/70-640-dumps.html

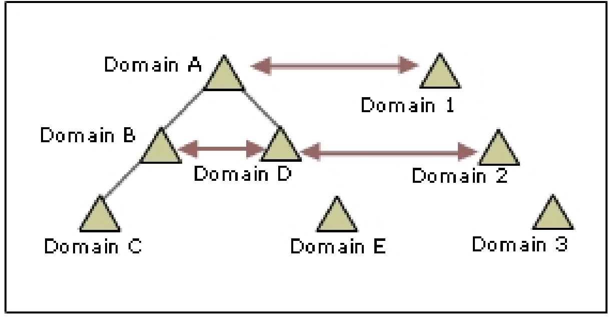


NEW QUESTION 1
Your company, Contoso Ltd, has offices in North America and Europe. Contoso has an Active Directory forest that has three domains.
You need to reduce the time required to authenticate users from the labs.eu.contoso.com domain when they access resources in the eng.na.contoso.com domain.
What should you do?

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

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.



C:\Documents and Settings\usernwz1\Desktop\1.PNG
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.

NEW QUESTION 2
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 certificat
B. Configure the Certificate Revocation List Distribution Point extensio
C. Configure the Authority Information Access (AIA) extensio
D. Add the Server2 computer account to the CertPublishers grou

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.

NEW QUESTION 3
Add the location of the Online Responder or OCSP responder to the authority information access extension on the CA.

Answer:

NEW QUESTION 4
At the ntdsutil prompt, type files, and then press ENTER.

Answer:

NEW QUESTION 5
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 highe
B. Raise the intranet.contoso.com domain functional level to Windows Server 2003 or highe
C. Add the new UPN suffix to the fores
D. Change the Primary DNS Suffix option in the Default Domain Controllers Group Policy Object (GPO) to contoso.co

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 forrest. 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

NEW QUESTION 6
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

Answer: B

Explanation:
Answer: The Active Directory Sites and Services console
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.

NEW QUESTION 7
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 disable
B. Run the csvde i k f import.csv comman
C. Run the DSMOD utility to set default passwords for the user account
D. Modify the userAccountControl attribute to accounts disable
E. Run the csvde -f import.csv comman
F. Run the DSMOD utility to set default passwords for the user account
G. Modify the userAccountControl attribute to disable
H. Run the wscript import.csv comman
I. Run the DSADD utility to set default passwords for the imported user account
J. Modify the userAccountControl attribute to disable
K. Run ldifde -i -f import.csv comman
L. Run the DSADD utility to set passwords for the imported user account

Answer: A

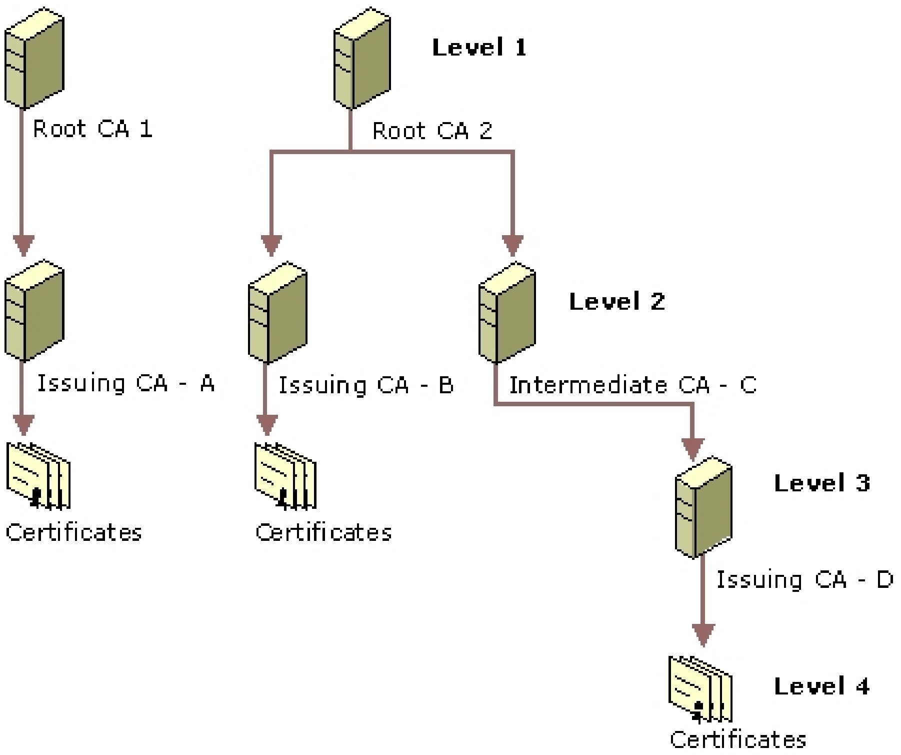
Explanation:
Personal note:
The correct command should be:
csvde - i -k -f import.csv
http://support.microsoft.com/kb/305144
How to use the UserAccountControl flags to manipulate user account properties When you open the properties for a user account, click the Account tab, and then either select or 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
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.

NEW QUESTION 8
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 serve
B. Import the new certificate into the Intermediate Certification Store on the Enterprise Intermediate CA serve
C. Import the new certificate into the Intermediate Certification Store in the Default Domain Controllers group policy objec
D. Import the new certificate into the Intermediate Certification Store in the Default Domain group policy objec

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.



C:\Documents and Settings\usernwz1\Desktop\1.PNG
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

NEW QUESTION 9
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 objec
B. Decrease the replication interval for the DEFAULTIPSITELINK objec
C. Decrease the cost between the connection object
D. Decrease the replication interval for all connection object

Answer: B

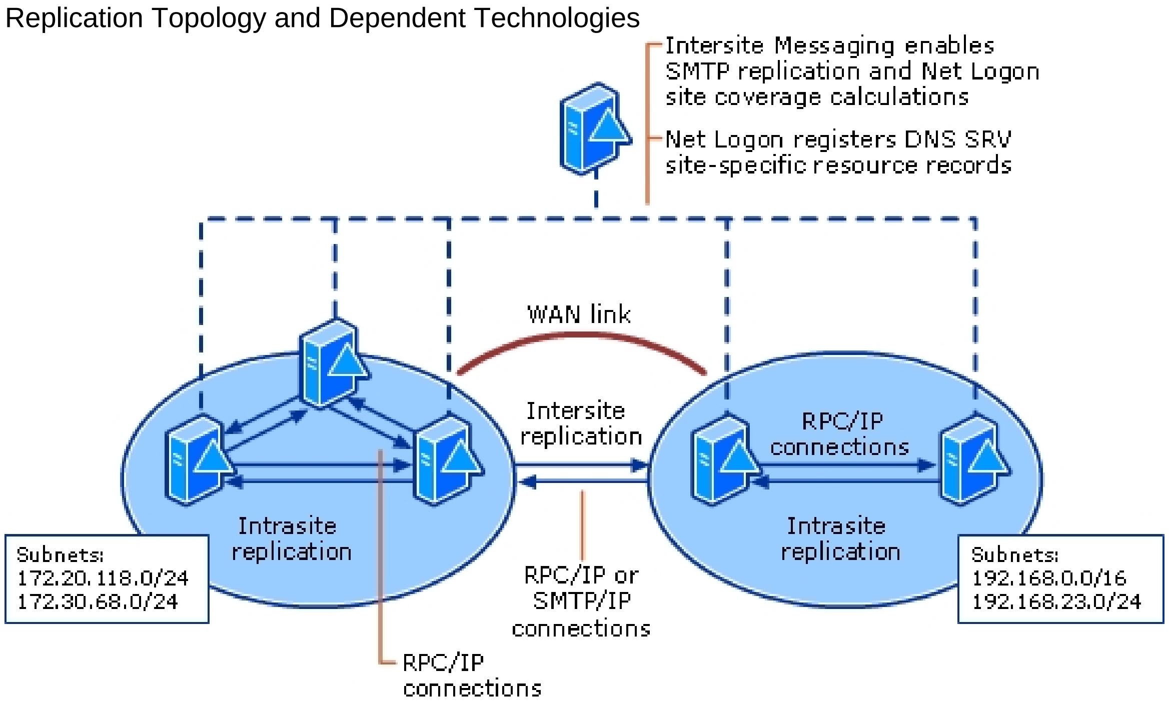
Explanation:
Answer: Decrease the replication interval for the DEFAULTIPSITELINK object.
Personal comment:
All sites are connected with the DEFAULTIPSITELINK object. <- this roughly translates into all sites are connected with the first domain controller in the forest
So the topology is star shaped.
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-bysite 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.

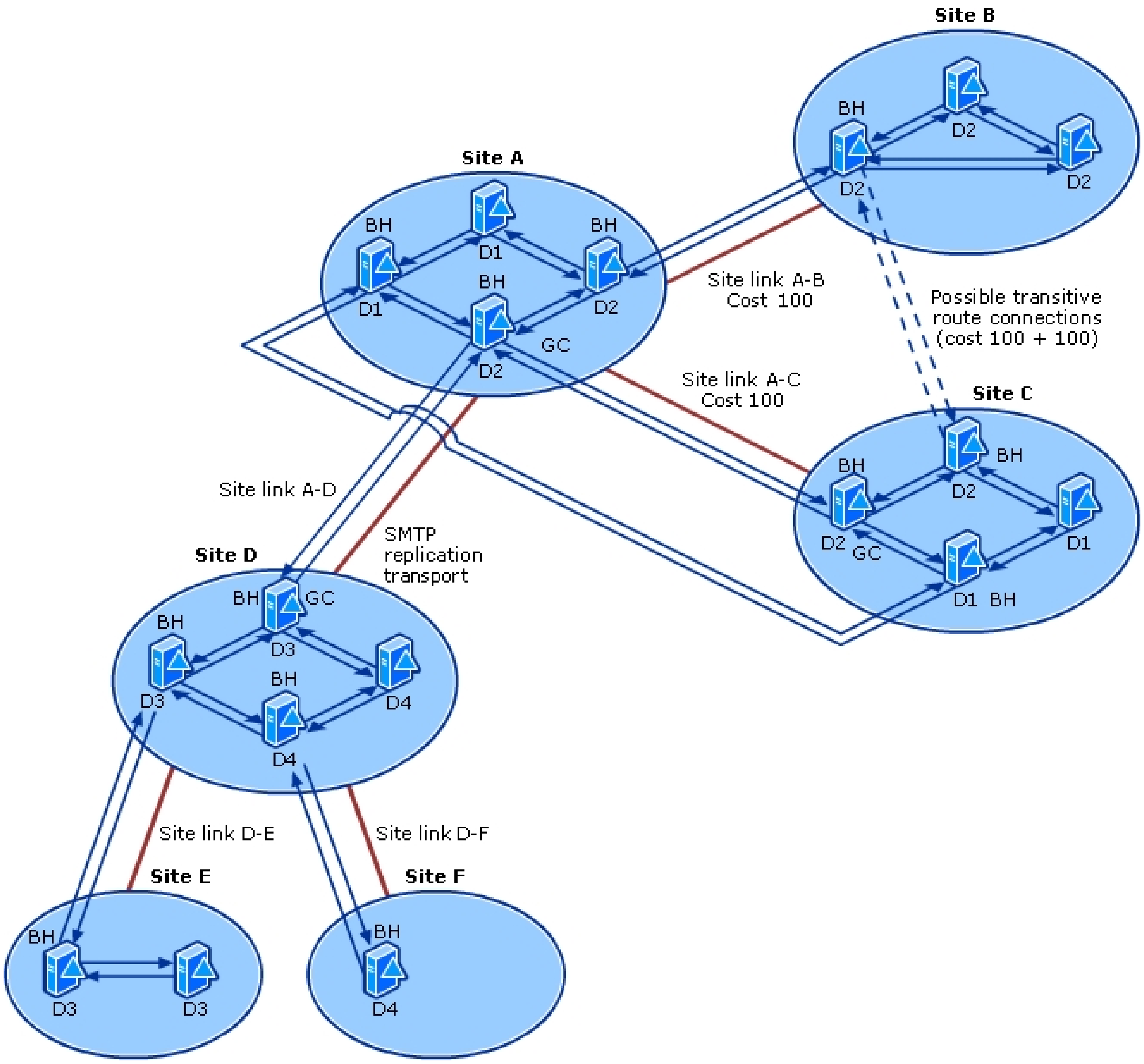
Replication Topology and Dependent Technologies



C:\Documents and Settings\usernwz1\Desktop\1.PNG

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



C:\Documents and Settings\usernwz1\Desktop\1.PNG

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 pExplanation 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.

NEW QUESTION 10
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 loggin
B. Enable automatic testing for simple querie
C. Configure event logging to log errors and warning
D. Enable automatic testing for recursive querie

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

NEW QUESTION 10
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 certificat
B. Import the OCSP Response Signing certificat
C. Add the Server1 computer account to the CertPublishers grou
D. Set the Startup Type of the Certificate Propagation service to Automati

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-

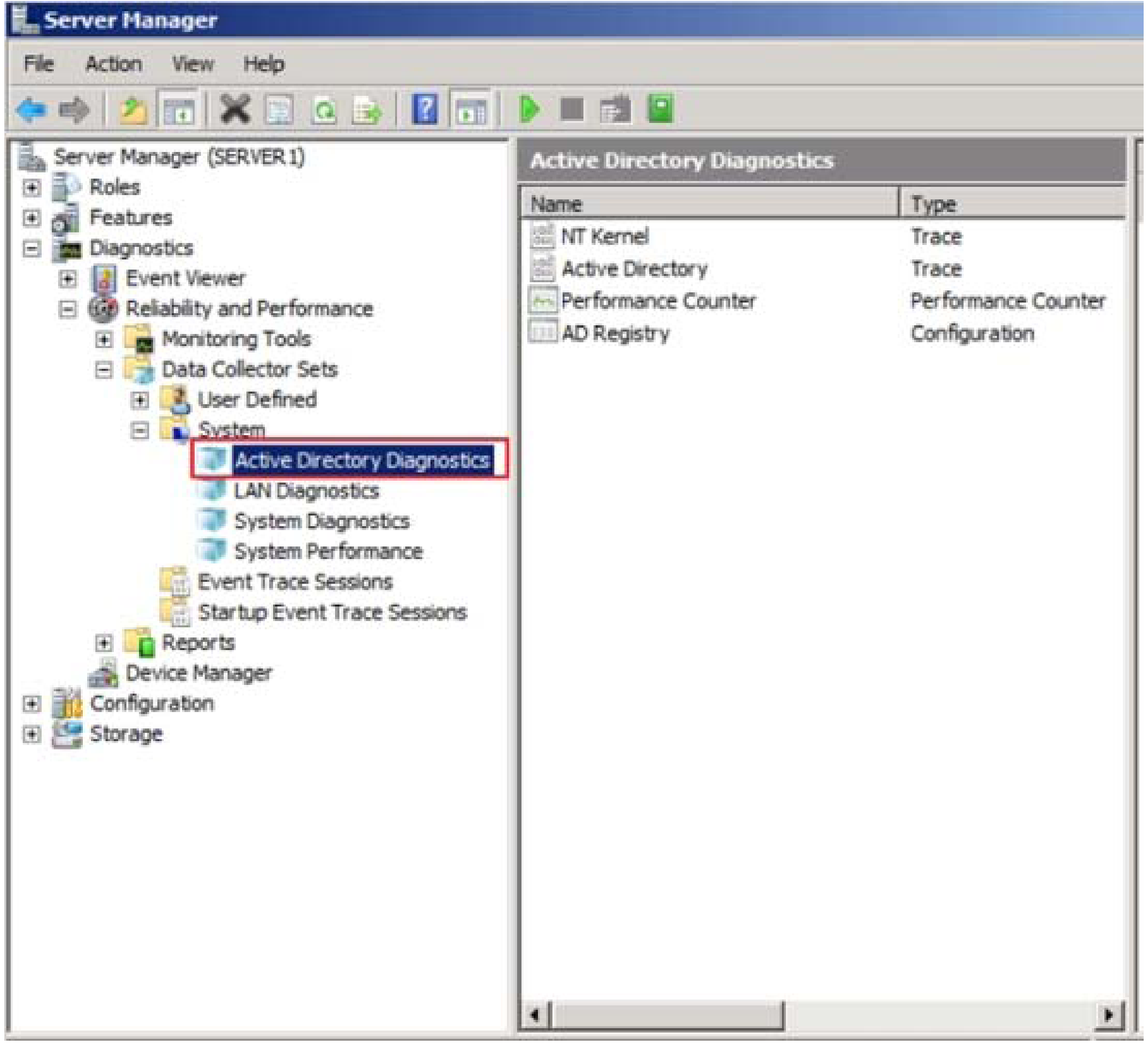
andplanning.aspx Designing and Implementing a PKI: Part I Design and Planning http://technet.microsoft.com/en-us/library/cc725937.aspx Set Up an Online Responder http://technet.microsoft.com/en-us/library/cc731099.aspx Creating a Revocation Configuration

NEW QUESTION 14
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 Monito
B. Review the Hardware Events log in the Event Viewe
C. Run the Active Directory Diagnostics Data Collector Se
D. Review the Active Directory Diagnostics repor
E. Run the LAN Diagnostics Data Collector Se
F. Review the LAN Diagnostics repor

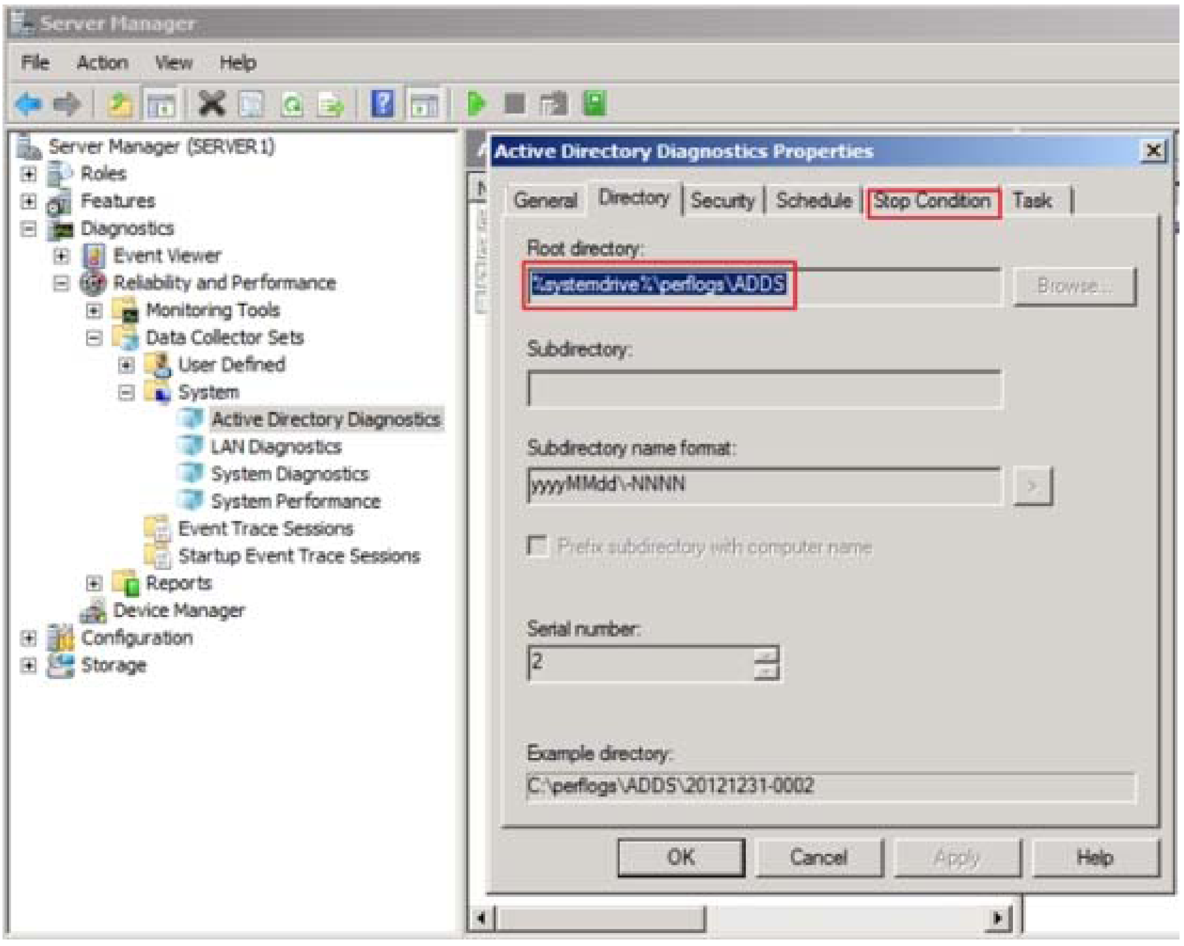
Answer: C

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.



Name	Type
NT Kernel	Trace
Active Directory	Trace
Performance Counter	Performance Counter
AD Registry	Configuration

C:\Documents and Settings\usernwz1\Desktop\1.PNG
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.



Root directory: %systemdrive%\perflogs\ADDS

Subdirectory:

Subdirectory name format: yyyyMMdd\-NNNN

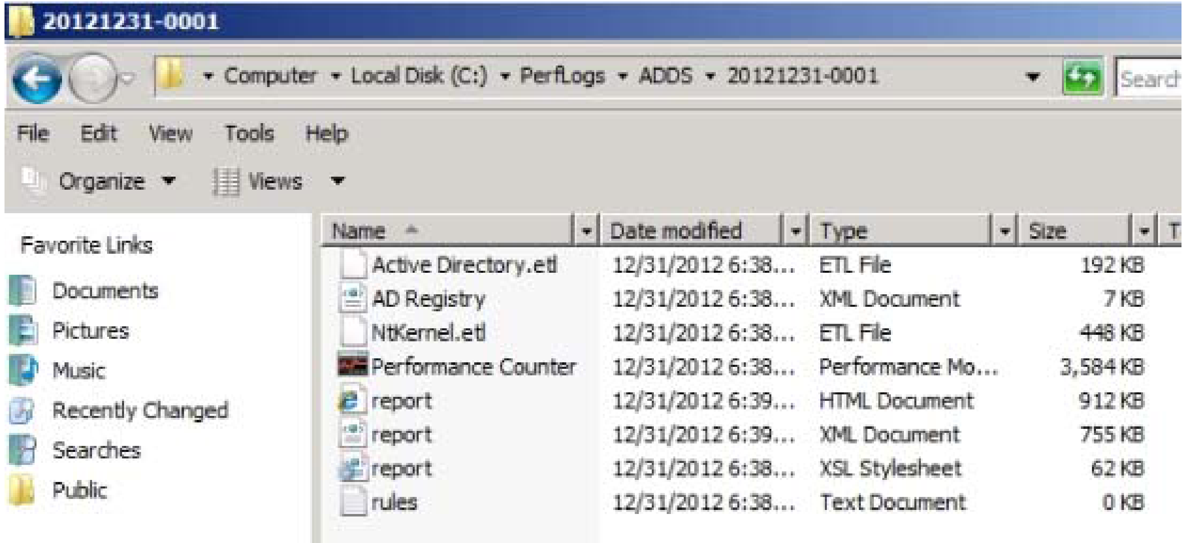
□ Prefix subdirectory with computer name

Serial number: 2

Example directory: C:\perflogs\ADDS\20121231-0002

C:\Documents and Settings\usernwz1\Desktop\1.PNG

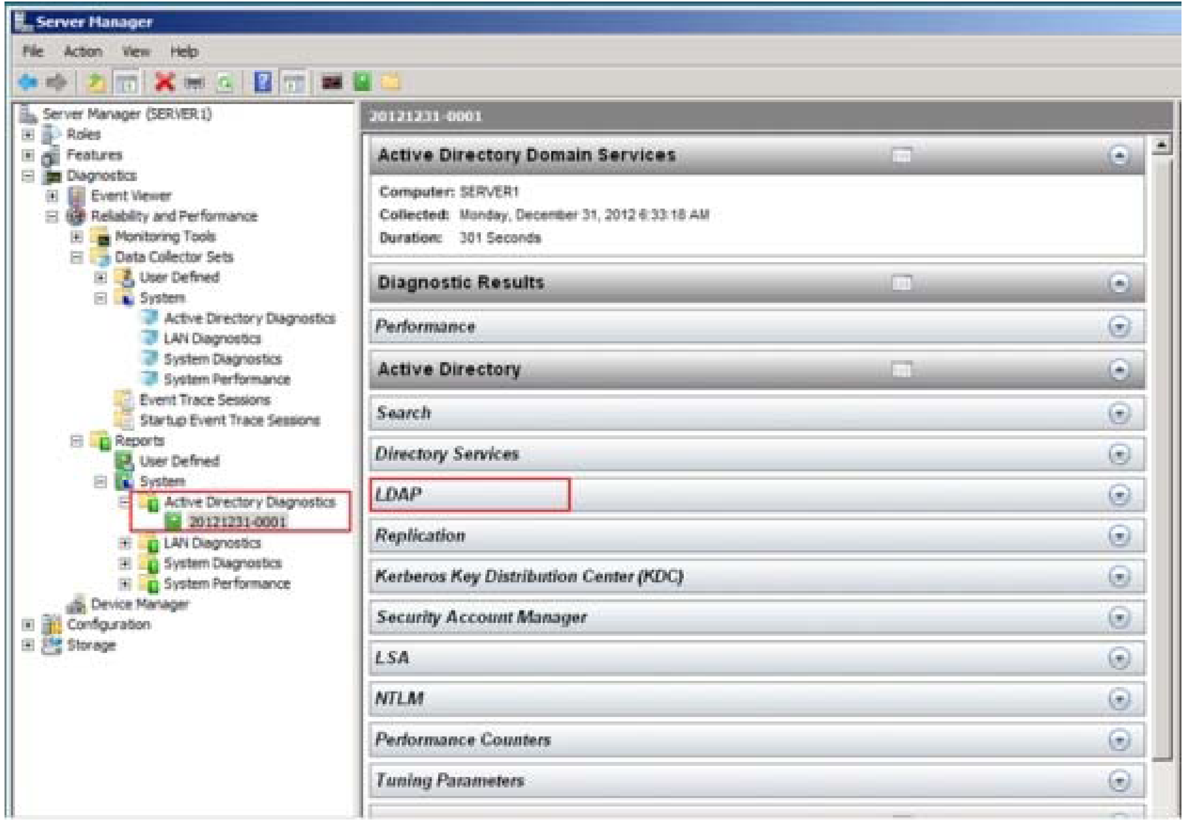
To start the data collector set, you just have to right click on Active Directory Diagnostics data collector set and select Start. Data will be stored at %systemdrive%\perflogs location.



Name	Date modified	Type	Size
Active Directory.etl	12/31/2012 6:38...	ETL File	192 KB
AD Registry	12/31/2012 6:38...	XML Document	7 KB
NtKernel.etl	12/31/2012 6:38...	ETL File	448 KB
Performance Counter	12/31/2012 6:38...	Performance Mo...	3,584 KB
report	12/31/2012 6:39...	HTML Document	912 KB
report	12/31/2012 6:39...	XML Document	755 KB
report	12/31/2012 6:38...	XSL Stylesheet	62 KB
rules	12/31/2012 6:38...	Text Document	0 KB

C:\Documents and Settings\usernwz1\Desktop\1.PNG

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.



Active Directory Domain Services

Computer: SERVER1
Collected: Monday, December 31, 2012 6:33:18 AM
Duration: 301 Seconds

Diagnostic Results

Performance

Active Directory

Search

Directory Services

LDAP

Replication

Kerberos Key Distribution Center (KDC)

Security Account Manager

LSA

NTLM

Performance Counters

Tuning Parameters

C:\Documents and Settings\usernwz1\Desktop\1.PNG

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

NEW QUESTION 19

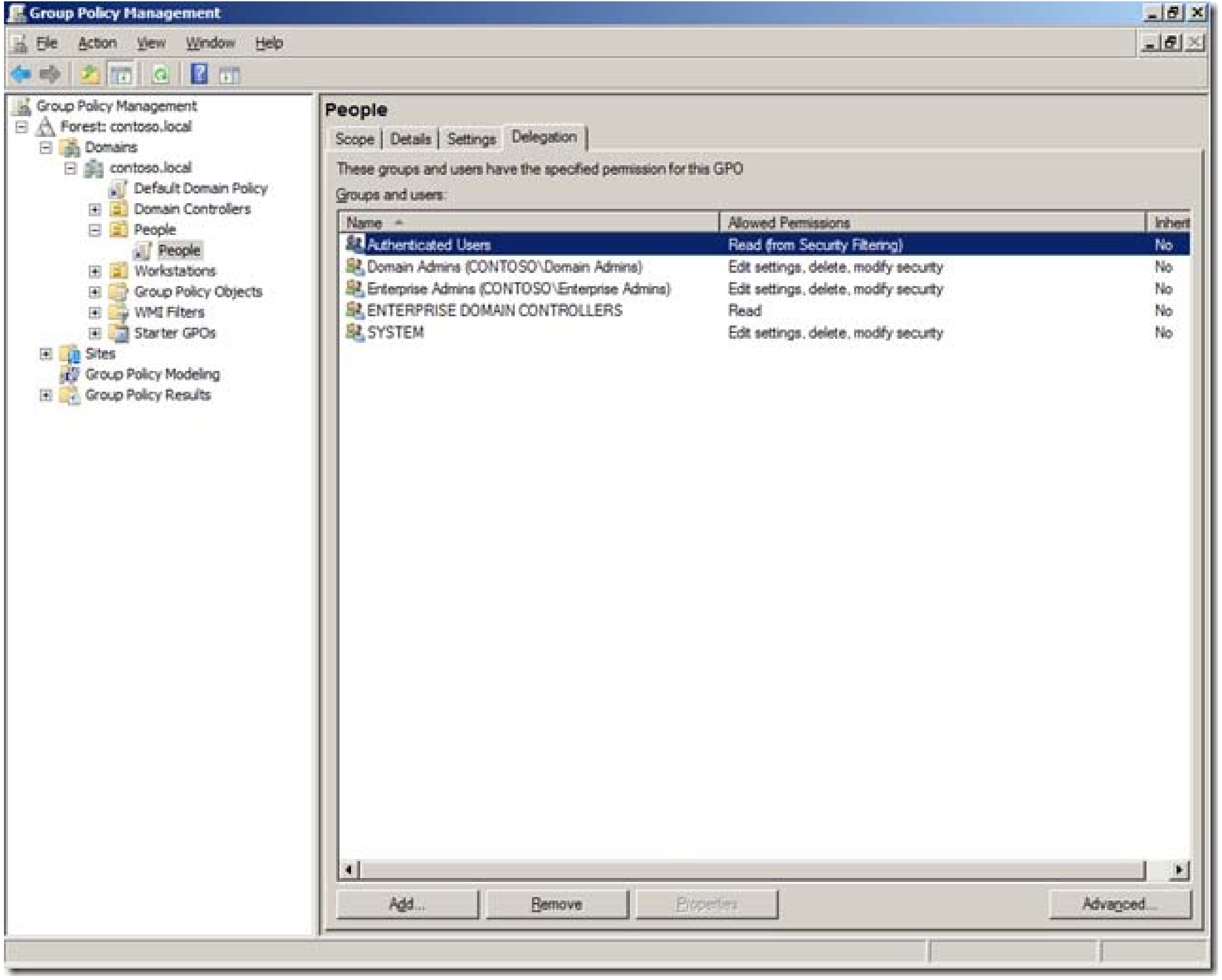
Your company has an Active Directory domain that has an organizational unit named Sales. The Sales organizational unit contains two global security groups

named sales managers and sales executives.
You need to apply desktop restrictions to the sales executives group.
You must not apply these desktop restrictions to the sales managers group.
You create a GPO named DesktopLockdown and link it to the Sales organizational unit.
What should you do next?

A. Configure the Deny Apply Group Policy permission for Authenticated Users on the DesktopLockdown GP
B. Configure the Deny Apply Group Policy permission for the sales executives on the DesktopLockdown GP
C. Configure the Allow Apply Group Policy permission for Authenticated Users on the DesktopLockdown GP
D. Configure the Deny Apply Group Policy permission for the sales managers on the DesktopLockdown GP

Answer: D

Explanation:
http://support.microsoft.com/kb/816100 How to prevent domain Group Policies from applying to certain user or computer accounts Typically, if you want Group Policy to apply only to specific accounts (either user accounts, computer accounts, or both), you can put the accounts in an organizational unit, and then apply Group Policy at that organizational unit level. However, there may be situations where you want to apply Group Policy to a whole domain, although you may not want those policy settings to also apply to administrator accounts or to other specific users or groups. http://www.grouppolicy.biz/2010/05/how-to-exclude-individual-users-or-computers-from-a-group-policy-object/ Best Practice: How to exclude individual users or computers from a Group Policy Object One of the common question I see on the forums from time to time is how to exclude a user and/or a computer from having a Group Policy Object (GPO) applied. This is a relatively straight forward process however I should stress this should be used sparingly and should always be done via group membership to avoid the administrative overhead of having to constantly update the security filtering on the GPO. Step 1. Open the Group Policy Object that you want to apply an exception and then click on the "Delegation" tab and then click on the "Advanced" button.

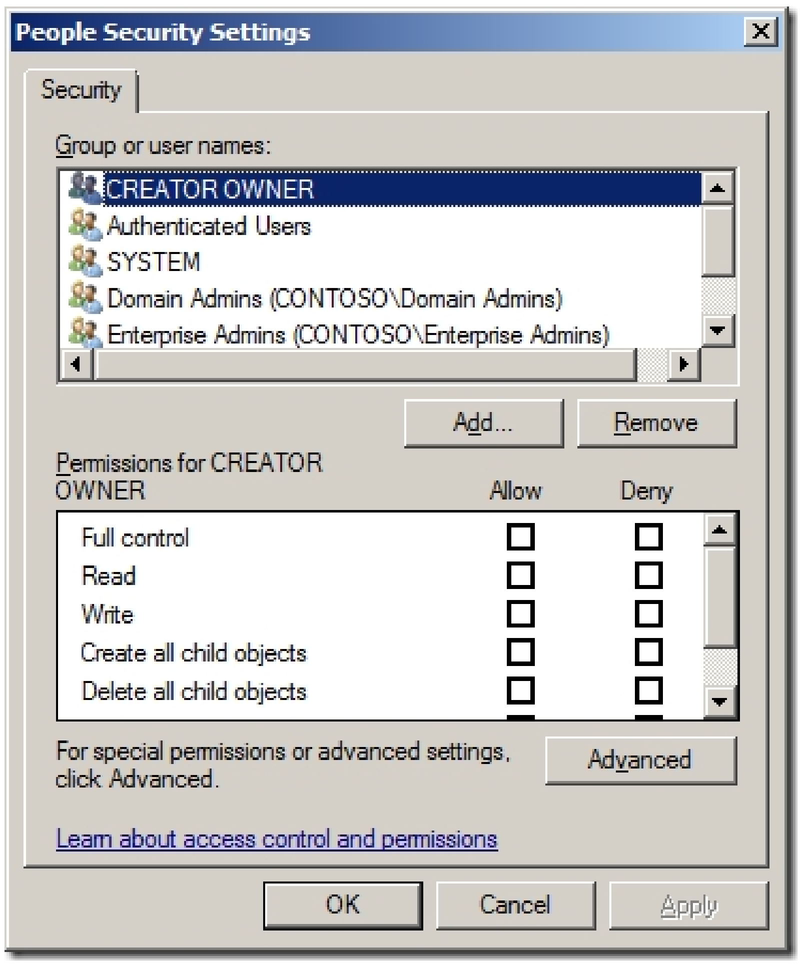


These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherit
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (CONTOSO\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (CONTOSO\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

C:\Documents and Settings\usernwz1\Desktop\1.PNG
Step 2. Click on the "Add" button and select the group (recommended) that you want to exclude from having this policy applied.


People Security Settings

Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)

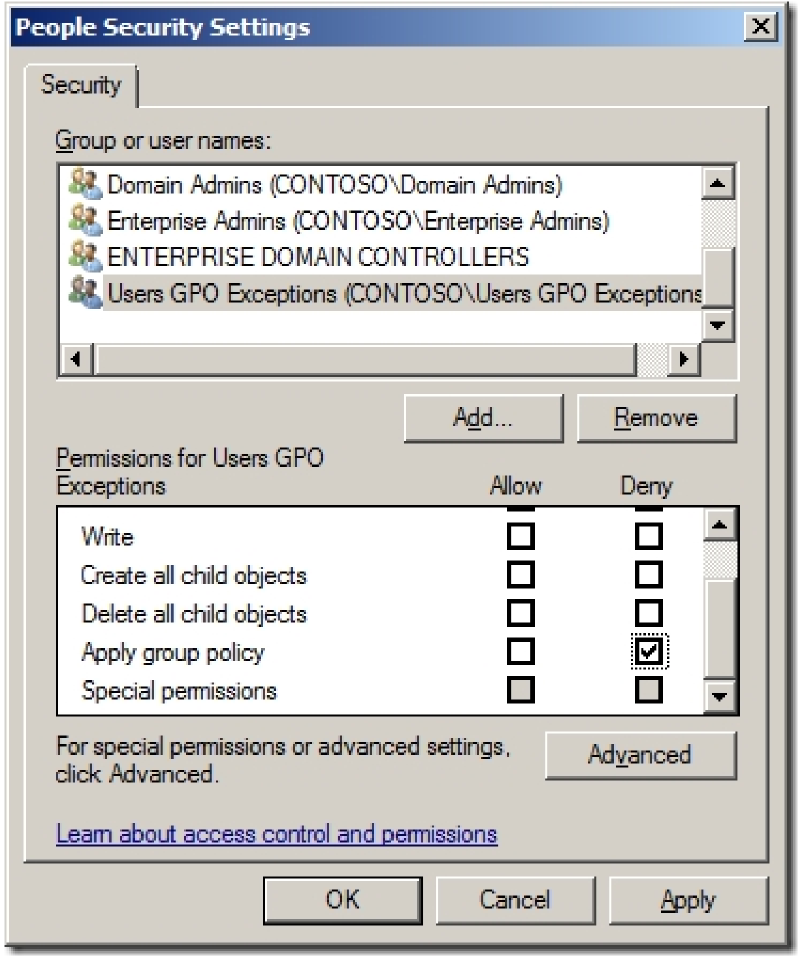
Permissions for CREATOR OWNER

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

C:\Documents and Settings\usernwz1\Desktop\1.PNG
Step 3. In this example I am excluding the “Users GPO Exceptions” group for this policy. Select this group in the “Group or user names” list and then scroll down the permission and tick the “Deny” option against the “Apply Group Policy” permission.


People Security Settings

Security

Group or user names:

- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- Users GPO Exceptions (CONTOSO\Users GPO Exceptions

Permissions for Users GPO Exceptions	Allow	Deny
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Apply group policy	□	☑
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

C:\Documents and Settings\usernwz1\Desktop\1.PNG
Now any members of this “User GPO Exceptions” security group will not have this Group Policy Object applied. Having a security group to control this exception makes it much easier to control as someone only needs to modify the group membership of the group to makes changes to who (or what) get the policy applied. This makes the delegation of this task to level 1 or level 2 support much more practical as you don’t need to grant them permission to the Group Policy Objects.

NEW QUESTION 24
Your network contains an Active Directory forest. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers.
You have an Active Directory-integrated zone for contoso.com.
You have a Unix-based DNS server.
You need to configure your Windows Server 2008 R2 environment to allow zone transfers
of the contoso.com zone to the Unix-based DNS server.
What should you do in the DNS Manager console?

A. Enable BIND secondaries
B. Create a stub zone
C. Disable recursion
D. Create a secondary zone

Answer: A

Explanation:
http://skibbz.com/understanding-of-advance-properties-settings-in-window-server-2003-and-2008-dns-serverbind-secondaries/ Understanding Of Advance Properties Settings In Window Server 2003 And 2008 DNS Server (BIND Secondaries) BIND Secondaries controls the zone transfer between different vendor

DNS server. It help verifies the type of format used zone transfer, whether it is fast or slow transfer (zone transfer). The full mean of BIND is Berkeley Internet Name domain (BIND). BIND is a based on UNIX operating system. Two window servers do not required BIND. BIND is only required when transfer dns zone between two different dns server vendors (UNIX and Microsoft Window). If you are using only Window server for dns and zone transfer you will have to disable this option in the window dns server. However if you want the server to perform a slow zone transfer and uncompressed data transfer then you will have to enable BIND in the dns server. To reiterate, BIND only provide slow dns zone transfer and data compression mechanism for DNS server. BIND is understood to have been introduced in window server to support UNIX. System admin will normally disable this option if they want the data in their dns zone transfer to between primary and secondary dns server to be transfer faster in order to improve dns queries efficiency within their network environment Bind is used in a DNS window server, when the needs to configured zone transfer between window server and UNIX server or operative system. Bind is enabled when a window server is configured as a primary dns server and a UNIX computer is configured as a secondary dns server for zone transfer. BIND Secondaries need to be configured to mitigate, the problem of interoperability between the two server operating system since they are from different vendors. Note that old version of the BIND was noted to be very slow and uses an uncompressed zone transfer format. However, BIND in window server 2008 and later has improved this problem. This is because it was noted that BIND in window server 2008 and later uses faster, compressed format during zone transfer between primary and secondary DNS server configured in for different server operating system (UNIX and Window server).

NEW QUESTION 27
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 optio
B. Link the GPO to the Domain Controllers organizational uni
C. On the file servers, configure Auditing for the Authenticated Users group in the Payroll folde
D. Enable the Audit object access optio
E. Link the GPO to the Payroll organizational uni
F. On the file servers, configure Auditing for the Everyone group in the Payroll folde
G. Enable the Audit process tracking optio
H. Link the GPO to the Payroll organizational uni
I. On the file servers, configure Auditing for the Everyone group in the Payroll folde
J. Enable the Audit object access optio
K. Link the GPO to the domai
L. On the domain controllers, configure Auditing for the Authenticated Users group in the Payroll folde

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.

NEW QUESTION 31
Your company has an Active Directory domain. The company has purchased 100 new computers. You want to deploy the computers as members of the domain.
You need to create the computer accounts in an OU.
What should you do?

A. Run the csvde -f computers.csv command
B. Run the ldifde -f computers.ldf command
C. Run the dsadd computer <computerdn> command
D. Run the dsmod computer <computerdn> command

Answer: C

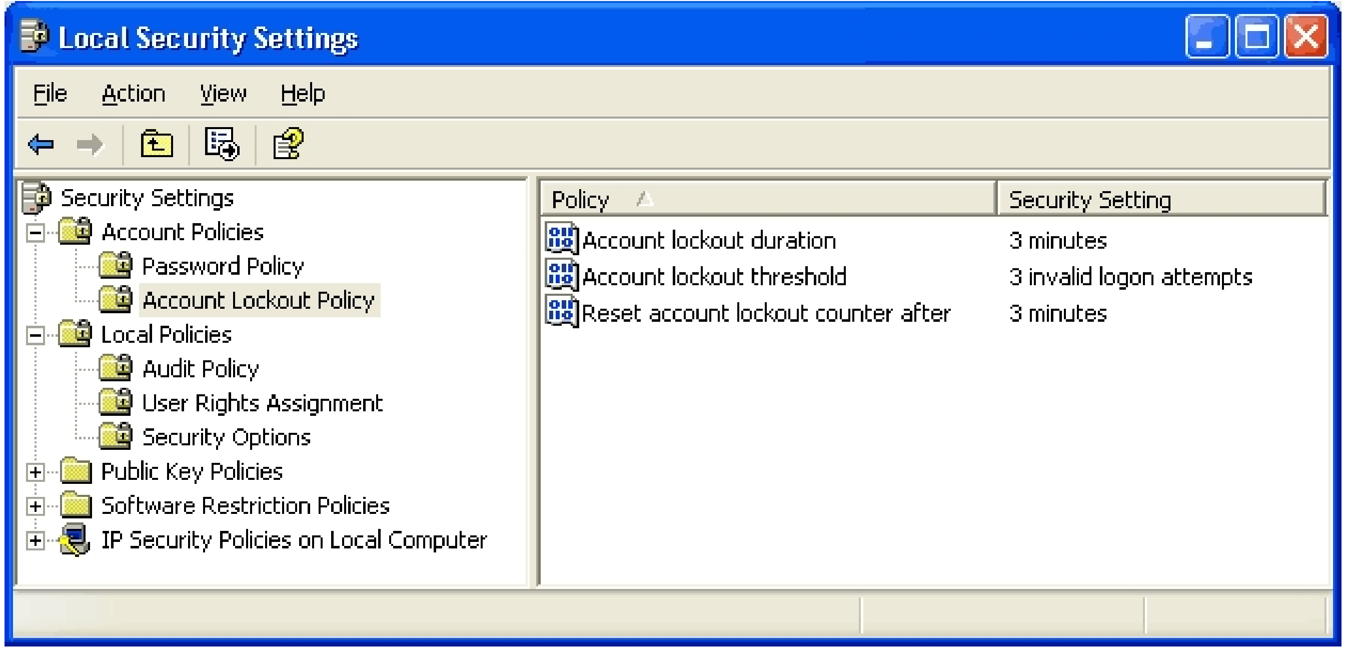
Explanation:
http://technet.microsoft.com/en-us/library/cc754539%28v=ws.10%29.aspx Dsadd computer Syntax: dsadd computer <ComputerDN> [-samid <SAMName>] [-desc <Description>] [-loc <Location>] [-memberof <GroupDN ...>] [{-s <Server> | -d <Domain>}] [-u <UserName>] [-p {<Password> | *}] [-q] [{-uc | -uco | -uci}] Personal comment: you use ldifde and csvde to import and export directory objects to Active Directory http://support.microsoft.com/kb/237677
http://technet.microsoft.com/en-us/library/cc732101%28v=ws.10%29.aspx

NEW QUESTION 35
You need to ensure that users who enter three successive invalid passwords within 5 minutes are locked out for 5 minutes.
Which three actions should you perform? (Each correct answer presents part of the solution.
Choose three.)

A. Set the Minimum password age setting to one da
B. Set the Maximum password age setting to one da
C. Set the Account lockout duration setting to 5 minute
D. Set the Reset account lockout counter after setting to 5 minute
E. Set the Account lockout threshold setting to 3 invalid logon attempt
F. Set the Enforce password history setting to 3 passswords remembere

Answer: CDE

Explanation:



Policy	Security Setting
Account lockout duration	3 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	3 minutes

C:\Documents and Settings\usernwz1\Desktop\1.PNG

NEW QUESTION 40
You need to relocate the existing user and computer objects in your company to different organizational units.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Run the move-item command in the Microsoft Windows PowerShell utilit
B. Run the Active Directory Users and Computers utilit
C. Run the Dsmove utilit
D. Run the Active Directory Migration Tool (ADMT).

Answer: BC

Explanation:
Personal note:
You can simply drag and drop objects when using the Active Directory Users and Computers utility or use the dsmove command.
http://technet.microsoft.com/en-us/library/cc731094%28v=ws.10%29.aspx
Dsmove Moves a single object, within a domain, from its current location in the directory to a new location, or renames a single object without moving it in the directory tree.

NEW QUESTION 43
Your company has an Active Directory forest. The company has servers that run Windows Server 2008 R2 and client computers that run Windows 7. The domain uses a set of GPO administrative templates that have been approved to support regulatory compliance requirements.
Your partner company has an Active Directory forest that contains a single domain. The company has servers that run Windows Server 2008 R2 and client computers that run Windows 7.
You need to configure your partner company's domain to use the approved set of administrative templates.
What should you do?

A. Use the Group Policy Management Console (GPMC) utility to back up the GPO to a fil
B. In each site, import the GPO to the default domain polic
C. Copy the ADMX files from your company's PDC emulator to the PolicyDefinitions folder on the partner company's PDC emulato
D. Copy the ADML files from your company's PDC emulator to the PolicyDefinitions folder on the partner company's PDC emulato
E. Download the conf.adm, system.adm, wuau.adm, and inetres.adm files from the Microsoft Updates Web sit
F. Copy the ADM files to the PolicyDefinitions folder on thr partner company's emulato

Answer: B

Explanation:
http://support.microsoft.com/kb/929841 How to create the Central Store for Group Policy Administrative Template files in Windows Vista Windows Vista uses a new format to display registry-based policy settings. These registry-based policy settings appear under Administrative Templates in the Group Policy Object Editor. In Windows Vista, these registry-based policy settings are defined by standards-based XML files that have an .admx file name extension. The .admx file format replaces the legacy .adm file format. The .adm file format uses a proprietary markup language. In Windows Vista, Administrative Template files are divided into .admx files and language-specific .adml files that are available to Group Policy administrators.
Administrative Template file storage In earlier operating systems, all the default Administrative Template files are added to the ADM folder of a Group Policy object (GPO) on a domain controller. The GPOs are stored in the SYSVOL folder. The SYSVOL folder is automatically replicated to other domain controllers in the same domain. A policy file uses approximately 2 megabytes (MB) of hard disk space. Because each domain controller stores a distinct version of a policy, replication traffic is increased.
Windows Vista uses a Central Store to store Administrative Template files. In Windows

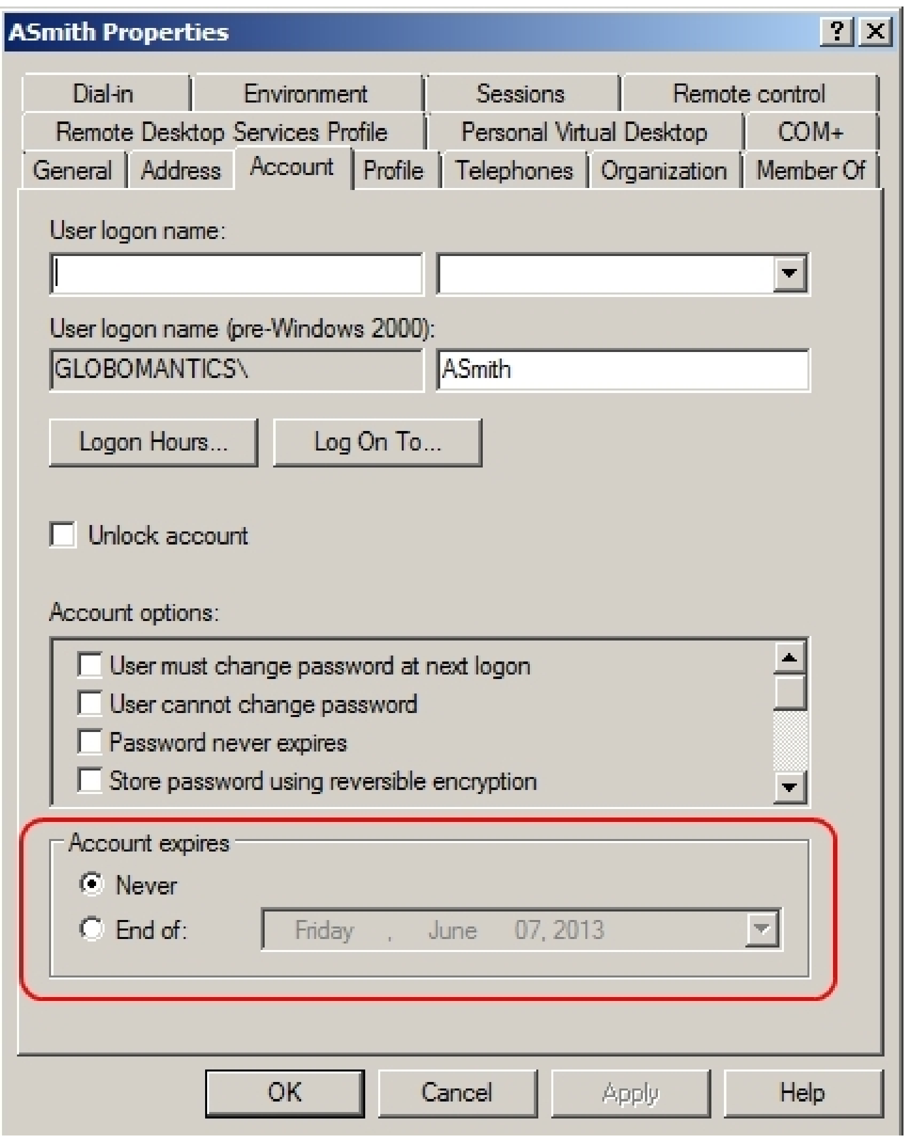
Vista, the ADM folder is not created in a GPO as in earlier versions of Windows. Therefore, domain controllers do not store or replicate redundant copies of .adm files.
The Central Store
To take advantage of the benefits of .admx files, you must create a Central Store in the SYSVOL folder on a domain controller. The Central Store is a file location that is checked by the Group Policy tools. The Group Policy tools use any .admx files that are in the Central Store. The files that are in the Central Store are later replicated to all domain controllers in the domain.
To create a Central Store for .admx and .adml files, create a folder that is named PolicyDefinitions in the following location:
\\FQDN\SYSVOL\FQDN\policies
Note: FQDN is a fully qualified domain name.
http://www.frickelsoft.net/blog/?p=31
How can I export local Group Policy settings made in gpedit.msc?
Mark Heitbrink, MVP for Group Policy... came up with a good solution on how you can "export" the Group
Policy and Security... settings you made in on a machine with the Local Group Policy Editor (gpedit.msc) to other machines pretty easy:
Normal settings can be copied like this:
1.) Open %systemroot%\system32\grouppolicy\
Within this folder, there are two folders - "machine" and "user". Copy these to folders to the "%systemroot%
\system32\grouppolicy - folder on the target machine. All it needs now is a reboot or a "gpupdate /force".
Note: If you cannot see the "grouppolicy" folder on either the source or the target machine, be sure to have your explorer folder options set to "Show hidden files and folders"…
For security settings:
1.) Open MMC and add the Snapin "Security Templates".
2.) Create your own customized template and save it as an "*inf" file.
3.) Copy the file to the target machine and import it via command line tool "secedit": secedit /configure /db %temp%\temp.sdb /cfg yourcreated.inf
Further information on secedit can be found here:http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/secedit_cmds.mspx?mfr=true
If you're building custom installations, you can pretty easy script the "overwriting" of the "machine"/"user"- folders or the import via secedit by copying these file to a share and copy and execute them with a script.

NEW QUESTION 46
The default domain GPO in your company is configured by using the following account policy settings:
Minimum password length: 8 characters
Maximum password age: 30 days
Enforce password history: 12 passwords remembered
Account lockout threshold: 3 invalid logon attempts
Account lockout duration: 30 minutes
You install Microsoft SQL Server on a computer named Server1 that runs Windows Server 2008 R2. The SQL Server application uses a service account named SQLSrv. The SQLSrv account has domain user rights.
The SQL Server computer fails after running successfully for several weeks. The SQLSrv user account is not locked out.
You need to resolve the server failure and prevent recurrence of the failure. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Reset the password of the SQLSrv user accoun
B. Configure the local security policy on Server1 to grant the Logon as a service right on the SQLSrv user accoun
C. Configure the properties of the SQLSrv account to Password never expire
D. Configure the properties of the SQLSrv account to User cannot change passwor
E. Configure the local security policy on Server1 to explicitly grant the SQLSrv user account the Allow logon locally user righ

Answer: AC

Explanation:
Personal comment:
Maximum password age: 30 days
The most probable cause for the malfunction is that the password has expired.
You need to reset the password and set it to never expire.



User logon name:

User logon name (pre-Windows 2000): GLOBOMANTICS\ ASmith

☐ Unlock account

Account options:

☐ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption

Account expires
● Never
○ End of: Friday , June 07, 2013

C:\Documents and Settings\usernwz1\Desktop\1.PNG

NEW QUESTION 49
Your company has an Active Directory domain and an organizational unit. The organizational unit is named Web.
You configure and test new security settings for Internet Information Service (IIS) Servers on a server named IISServerA.
You need to deploy the new security settings only on the IIS servers that are members of the Web organizational unit.
What should you do?

A. Run secedit /configure /db iis.inf from the command prompt on IISServerA, then run secedit /configure /db webou.inf from the comand promp
B. Export the settings on IISServerA to create a security templat
C. Import the security template into a GPO and link the GPO to the Web organizational uni
D. Export the settings on IISServerA to create a security templat
E. Run secedit /configure /db webou.inf from the comand promp
F. Import the hisecws.inf file template into a GPO and link the GPO to the Web organizational uni

Answer: B

Explanation:
http://www.itninja.com/blog/view/using-secedit-to-apply-security-templates Using Secedit To Apply Security Templates Secedit /configure /db secedit.sdb /cfg"c:\temp\custom.inf" /silent >nul This command imports a security template file, “custom.inf” into the workstation’s or server’s local security database. /db must be specified. When specifying the default secuirty database (secedit.sdb,) I found that providing no path worked best. The /cfg option informs Secedit that it is to import the .inf file into the specified database, appending it to any existing .inf files that have already been imported to this system. You can optionally include an /overwrite switch to overwrite all previous configurations for this machine. The /silent option supresses any pop-ups and the >nul hides the command line output stating success or failure of the action.

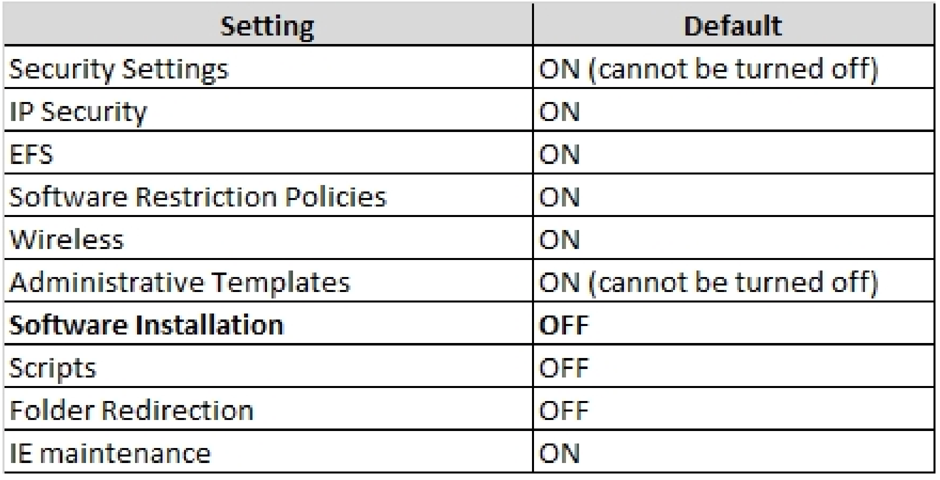
NEW QUESTION 50
Your company has an Active Directory forest. The forest includes organizational units corresponding to the following four locations:
. London
. Chicago
. New York
. Madrid
Each location has a child organizational unit named Sales. The Sales organizational unit contains all the users and computers from the sales department.
The offices in London, Chicago, and New York are connected by T1 connections. The office in Madrid is connected by a 256-Kbps ISDN connection.
You need to install an application on all the computers in the sales department.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create a Group Policy Object (GPO) named OfficeInstall that assigns the application to user
B. Link the GPO to each Sales organizational uni
C. Disable the slow link detection setting in the Group Policy Object (GPO).
D. Configure the slow link detection threshold setting to 1,544 Kbps (T1) in the Group Policy Object (GPO).
E. Create a Group Policy Object (GPO) named OfficeInstall that assigns the application to the computer
F. Link the GPO to each Sales organizational uni

Answer: BD

Explanation:

http://technet.microsoft.com/en-us/library/cc781031%28v=ws.10%29.aspx Specifying Group Policy for Slow Link Detection Administrators can partially control which Group Policy extensions are processed over a slow link. By default, when processing over a slow link, not all components of Group Policy are processed. Table 2.6 shows the default settings for processing Group Policy over slow links.



Setting	Default
Security Settings	ON (cannot be turned off)
IP Security	ON
EFS	ON
Software Restriction Policies	ON
Wireless	ON
Administrative Templates	ON (cannot be turned off)
Software Installation	**OFF**
Scripts	OFF
Folder Redirection	OFF
IE maintenance	ON

C:\Documents and Settings\usernwz1\Desktop\1.PNG

Administrators can use a Group Policy setting to define a slow link for the purposes of applying and updating Group Policy. The default value defines a rate slower than 500 Kbps as a slow link. http://technet.microsoft.com/en-us/library/cc783635%28v=ws.10%29.aspx Assigning and Publishing Software

Assigning software to computers After you assign a software package to computers in a site, domain, or OU, the software is installed the next time the computer restarts or the user logs on. Further information: http://technet.microsoft.com/en-us/library/cc978717.aspx Group Policy slow link detection

NEW QUESTION 53

Your company has a single Active Directory domain. All domain controllers run Windows Server 2003.
You install Windows Server 2008 R2 on a server.
You need to add the new server as a domain controller in your domain.
What should you do first?

A. On a domain controller run adprep /rodcpre
B. On the new server, run dcpromo /ad
C. On the new server, run dcpromo /createdcaccoun
D. On a domain controller, run adprep /forestpre

Answer: D

Explanation:

http://social.technet.microsoft.com/Forums/en-US/winserverDS/thread/9931e32f-6302-40f0-a7a1-2598a96cd0c1/ DC promotion and adprep/forestprep

Q: I've tried to dcpromo a new Windows 2008 server installation to be a Domain Controller, running in an existing domain. I am informed that, first, I must run adprep/forestprep ("To install a domain controller into this Active Directory forest, you must first perpare the forest using "adprep/forestprep". The Adprep utility is available on the Windows Server 2008 installation media in the Windows\sources\adprep folder"

A1:

You can run adprep from an existing Windows Server 2003 domain controller. Copy the contents of the \sources\adprep folder from the Windows Server 2008 installation DVD to the schema master role holder and run Adprep from there.

A2: to introduce the first W2K8 DC within an AD forest....
(1) no AD forest exists yet:
--> on the stand alone server execute: DCPROMO
--> and provide the information needed
(2) an W2K or W2K3 AD forest already exists:
--> ADPREP /Forestprep on the w2k/w2k3 schema master (both w2k/w2k3 forests)
--> ADPREP /rodcprep on the w2k3 domain master (only w2k3 forests)
--> ADPREP /domainprep on the w2k3 infrastructure master (only w2k3 domains)
--> ADPREP /domainprep /gpprep on the w2k infrastructure master (only w2k domains)
--> on the stand alone server execute: DCPROMO
--> and provide the information needed

NEW QUESTION 54

You have an Active Directory domain that runs Windows Server 2008 R2.
You need to implement a certification authority (CA) server that meets the following requirements:
Allows the certification authority to automatically issue certificates
Integrates with Active Directory Domain Services
What should you do?

A. Install and configure the Active Directory Certificate Services server role as a Standalone Root C
B. Install and configure the Active Directory Certificate Services server role as an Enterprise Root C
C. Purchase a certificate from a third-party certification authority, Install and configure the Active Directory Certificate Services server role as a Standalone Subordinate C
D. Purchase a certificate from a third-party certification authority, Import the certificate into the computer store of the schema maste

Answer: B

Explanation:

http://technet.microsoft.com/en-us/library/cc776874%28v=ws.10%29.aspx Enterprise certification authorities The Enterprise Administrator can install Certificate Services to create an enterprise certification authority (CA). Enterprise CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions), authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) and logging on to a Windows Server 2003 family domain using a smart card. An enterprise CA has the following features: An enterprise CA requires the Active Directory directory service. When you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. You must be a Domain Administrator or be an administrator with write access to Active

Directory to install an enterprise root CA. Certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards. The enterprise exit module publishes user certificates and the certificate revocation list (CRL) to Active Directory. In order to publish certificates to Active Directory, the server that the CA is installed on must be a member of the Certificate Publishers group. This is automatic for the domain the server is in, but the server must be delegated the proper security permissions to publish certificates in other domains. For more information about the exit module, see Policy and exit modules. An enterprise CA uses certificate types, which are based on a certificate template. The following functionality is possible when you use certificate templates: Enterprise CAs enforce credential checks on users during certificate enrollment. Each certificate template has a security permission set in Active Directory that determines whether the certificate requester is authorized to receive the type of certificate they have requested. The certificate subject name can be generated automatically from the information in Active Directory or supplied explicitly by the requestor. The policy module adds a predefined list of certificate extensions to the issued certificate. The extensions are defined by the certificate template. This reduces the amount of information a certificate requester has to provide about the certificate and its intended use. http://technet.microsoft.com/en-us/library/cc780501%28WS.10%29.aspx Stand-alone certification authorities You can install Certificate Services to create a stand-alone certification authority (CA). Stand-alone CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions) and authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS). A stand-alone CA has the following characteristics: Unlike an enterprise CA, a stand-alone CA does not require the use of the Active Directory directory service. Stand-alone CAs are primarily intended to be used as Trusted Offline Root CAs in a CA hierarchy or when extranets and the Internet are involved. Additionally, if you want to use a custom policy module for a CA, you would first install a stand-alone CA and then replace the stand-alone policy module with your custom policy module. When submitting a certificate request to a stand-alone CA, a certificate requester must explicitly supply all identifying information about themselves and the type of certificate that is wanted in the certificate request. (This does not need to be done when submitting a request to an enterprise CA, since the enterprise user's information is already in Active Directory and the certificate type is described by a certificate template). The authentication information for requests is obtained from the local computer's Security Accounts Manager database. By default, all certificate requests sent to the stand-alone CA are set to Pending until the administrator of the stand-alone CA verifies the identity of the requester and approves the request. This is done for security reasons, because the certificate requester's credentials are not verified by the stand-alone CA. Certificate templates are not used. No certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards, but other types of certificates can be issued and stored on a smart card. The administrator has to explicitly distribute the stand-alone CA's certificate to the domain user's trusted root store or users must perform that task themselves. When a stand-alone CA uses Active Directory, it has these additional features: If a member of the Domain Administrators group or an administrator with write access to Active Directory, installs a stand-alone root CA, it is automatically added to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. For this reason, if you install a stand-alone root CA in an Active Directory domain, you should not change the default action of the CA upon receiving certificate requests (which marks requests as Pending). Otherwise, you will have a trusted root CA that automatically issues certificates without verifying the identity of the certificate requester. If a stand-alone CA is installed by a member of the Domain Administrators group of the parent domain of a tree in the enterprise, or by an administrator with write access to Active Directory, then the stand-alone CA will publish its CA certificate and the certificate revocation list (CRL) to Active Directory.

NEW QUESTION 56
Your company has an Active Directory domain.
You plan to install the Active Directory Certificate Services (AD CS) server role on a member server that runs Windows Server 2008 R2.
You need to ensure that members of the Account Operators group are able to issue smartcard credentials.They should not be able to revoke certificates.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Create an Enrollment Agent certificat
B. Create a Smartcard logon certificat
C. Restrict enrollment agents for the Smartcard logon certificate to the Account Operator grou
D. Install the AD CS role and configure it as an Enterprise Root C
E. Install the AD CS role and configure it as a Standalone C
F. Restrict certificate managers for the Smartcard logon certificate to the Account Operator grou

Answer: BCD

Explanation:
http://technet.microsoft.com/en-us/library/cc753800%28v=ws.10%29.aspx AD CS: Restricted Enrollment Agent The restricted enrollment agent is a new functionality in the Windows Server. 2008 Enterprise operating system that allows limiting the permissions that users designated as enrollment agents have for enrolling smart card certificates on behalf of other users.
What does the restricted enrollment agent do? Enrollment agents are one or more authorized individuals within an organization. The enrollment agent needs to be issued an enrollment agent certificate, which enables the agent to enroll for smart card certificates on behalf of users. Enrollment agents are typically members of the corporate security, Information Technology (IT) security, or help desk teams because these individuals have already been trusted with safeguarding valuable resources. In some organizations, such as banks that have many branches, help desk and security workers might not be conveniently located to perform this task. In this case, designating a branch manager or other trusted employee to act as an enrollment agent is required to enable smart card credentials to be issued from multiple locations. On a Windows Server 2008 Enterprise-based certification authority (CA), the restricted enrollment agent features allow an enrollment agent to be used for one or many certificate templates. For each certificate template, you can choose which users or security groups the enrollment agent can enroll on behalf of. You cannot constrain an enrollment agent based on a certain Active Directory. organizational unit (OU) or container; you must use security groups instead. The restricted enrollment agent is not available on a Windows
http://technet.microsoft.com/en-us/library/cc776874%28v=ws.10%29.aspx
Enterprise certification authorities The Enterprise Administrator can install Certificate Services to create an enterprise certification authority (CA). Enterprise CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions), authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) and logging on to a Windows Server 2003 family domain using a smart card. An enterprise CA has the following features: An enterprise CA requires the Active Directory directory service. When you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. You must be a Domain Administrator or be an administrator with write access to Active Directory to install an enterprise root CA. Certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards. The enterprise exit module publishes user certificates and the certificate revocation list (CRL) to Active Directory. In order to publish certificates to Active Directory, the server that the CA is installed on must be a member of the Certificate Publishers group. This is automatic for the domain the server is in, but the server must be delegated the proper security permissions to publish certificates in other domains. For more information about the exit module, see Policy and exit modules.
An enterprise CA uses certificate types, which are based on a certificate template. The following functionality is possible when you use certificate templates: Enterprise CAs enforce credential checks on users during certificate enrollment. Each certificate template has a security permission set in Active Directory that determines whether the certificate requester is authorized to receive the type of certificate they have requested. The certificate subject name can be generated automatically from the information in Active Directory or supplied explicitly by the requestor.
The policy module adds a predefined list of certificate extensions to the issued certificate. The extensions are defined by the certificate template. This reduces the amount of information a certificate requester has to provide about the certificate and its intended use.
http://technet.microsoft.com/en-us/library/cc780501%28WS.10%29.aspx
Stand-alone certification authorities
You can install Certificate Services to create a stand-alone certification authority (CA). Stand-alone CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions) and authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS). A stand-alone CA has the following characteristics: Unlike an enterprise CA, a stand-alone CA does not require the use of the Active Directory directory service. Stand-alone CAs are primarily intended to be used as Trusted Offline Root CAs in a CA hierarchy or when extranets and

the Internet are involved. Additionally, if you want to use a custom policy module for a CA, you would first install a stand-alone CA and then replace the stand-alone policy module with your custom policy module. When submitting a certificate request to a stand-alone CA, a certificate requester must explicitly supply all identifying information about themselves and the type of certificate that is wanted in the certificate request. (This does not need to be done when submitting a request to an enterprise CA, since the enterprise user's information is already in Active Directory and the certificate type is described by a certificate template). The authentication information for requests is obtained from the local computer's Security Accounts Manager database. By default, all certificate requests sent to the stand-alone CA are set to Pending until the administrator of the stand-alone CA verifies the identity of the requester and approves the request. This is done for security reasons, because the certificate requester's credentials are not verified by the stand-alone CA. Certificate templates are not used. No certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards, but other types of certificates can be issued and stored on a smart card. The administrator has to explicitly distribute the stand-alone CA's certificate to the domain user's trusted root store or users must perform that task themselves. When a stand-alone CA uses Active Directory, it has these additional features: If a member of the Domain Administrators group or an administrator with write access to Active Directory, installs a stand-alone root CA, it is automatically added to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. For this reason, if you install a stand-alone root CA in an Active Directory domain, you should not change the default action of the CA upon receiving certificate requests (which marks requests as Pending). Otherwise, you will have a trusted root CA that automatically issues certificates without verifying the identity of the certificate requester.
If a stand-alone CA is installed by a member of the Domain Administrators group of the parent domain of a tree in the enterprise, or by an administrator with write access to Active Directory, then the stand-alone CA will publish its CA certificate and the certificate revocation list (CRL) to Active Directory.

NEW QUESTION 57
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 unit
B. Use the Active Directory Users and Computers snap-in to create the organizational units on the AD LDS application directory partitio
C. Use the dsadd OU <OrganizationalUnitDN> command to create the organizational unit
D. Use the ADSI Edit snap-in to create the organizational units on the AD LDS application directory partitio

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.

NEW QUESTION 60
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 II
B. Manually delete the Service Connection Point in AD DS and restart AD RM
C. Install Message Queuin
D. Start the MSSQLSVC servic

Answer: AD

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.

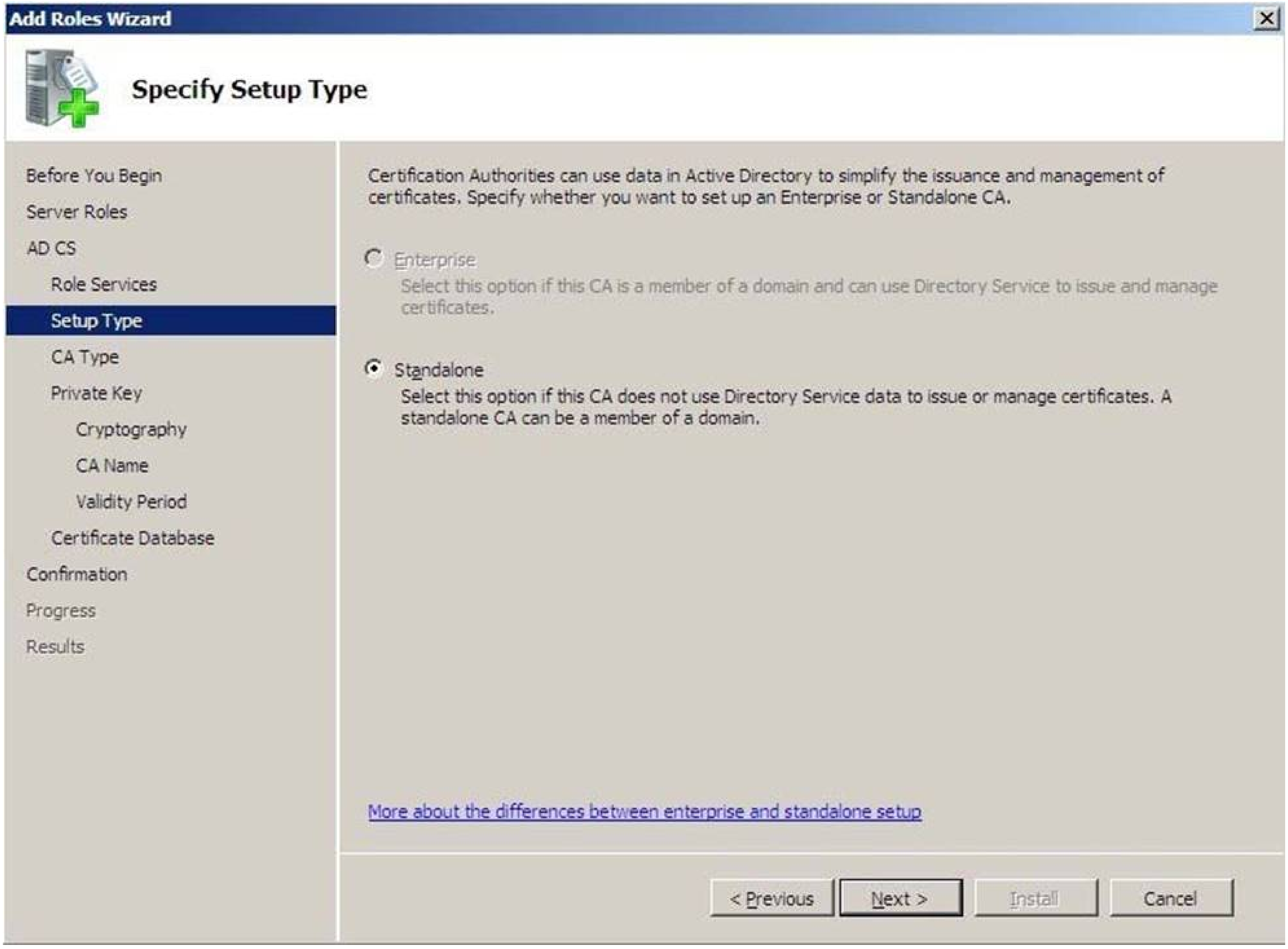
NEW QUESTION 65

Your company has an Active Directory forest.
You plan to install an Enterprise certification authority (CA) on a dedicated stand-alone server.
When you attempt to add the Active Directory Certificate Services (AD CS) role, you find that the Enterprise CA option is not available.
You need to install the AD CS role as an Enterprise CA.
What should you do first?

A. Add the DNS Server rol
B. Add the Active Directory Lightweight Directory Service (AD LDS) rol
C. Add the Web server (IIS) role and the AD CS rol
D. Join the server to the domai

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx
Active Directory Certificate Services Step-by-Step Guide
http://kazmierczak.eu/itblog/2012/09/23/enterprise-ca-option-is-greyed-out-unavailable/
Enterprise CA option is greyed out / unavailable Many times, administrators ask me what to do when installing Active Directory Certificate Services they cannot choose to install Enterprise Certification Authority, because it’s unavailable as in following picture:



Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

○ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

● Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

C:\Documents and Settings\usernwz1\Desktop\1.PNG
Well, you need to fulfill basic requirements: Server machine has to be a member server (domain joined). You can run an Enterprise CA on the Standard, Enterprise, or Data Center Windows Edition. The difference is the number of ADCS features and components that can be enabled. To get full functionality, you need to run on Enterprise or Data Center Windows Server 2008 /R2/ Editions. It includes functionality like Role separation, Certificate manager restrictions, Delegated enrollment agent restrictions, Certificate enrollment across forests, Online Responder, Network Device Enrollment. In order to install an Enterprise CA, you must be a member of either Enterprise Admins or Domain Admins in the forest root domain (either directly or through a group nesting). If issue still persists, there is probably a problem with getting correct credentials of your account. There are many thing that can cause it (network blockage, domain settings, server configuration, and other issues). In all cases I got, this troubleshooting helped perfectly: First of all, carefully check all above requirements. Secondly, install all available patches and Service Packs with Windows Update before trying to install Enterprise CA. Check network settings on the CA Server. If there is no DNS setting, Certificate Authority Server cannot resolve and find domain. Sufficient privileges for writing the Enterprise CA configuration information in AD configuration partition are required. Determine if you are a member of the Enterprise Admins or Domain Admins in the forest root domain. Think about the account you are currently trying to install ADCS with. In fact, you may be sure, that your account is in Enterprise Admins group, but check this how CA Server “sees” your account membership by typing whoami /groups. You also need to be a member of local Administrators group. If you are not, you wouldn’t be able to run Server Manager, but still needs to be checked. View C:\windows\certocm.log file. There you can find helpful details on problems with group membership. For example status of ENUM_ENTERPRISE_UNAVAIL_REASON_NO_INSTALL_RIGHTS indicates that needed memberships are not correct. Don’t forget to check event viewer on CA Server side and look for red lines. Verify that network devices or software&hardware firewalls are not blocking access from/to server and Domain Controllers. If so, Certificate Authority Server may not be communicating correctly with the domain. To check that, simply run nltest /sc_verify:DomainName Check also whether Server CA is connected to a writable Domain Controller. Enterprise Admins groups is the most powerful group and has ADCS required full control permissions, but who knows – maybe someone changed default permissions? Run adsiedit.msc on Domain Controller, connect to default context and first of all check if CN=Public Key Service,CN=Services,CN=Configuration,DC=Your,DC=Domain,DC=Com container does exist. If so, check permissions for all subcontainers under Public Key Service if Enterprise Admins group has full control permissions. The main subcontainers to verify are Certificate Templates, OID, KRA containers. If no above tips

help, disjoin the server from domain and join again. Ultimately reinstall operation system on CA Server.

NEW QUESTION 68
Your company has two Active Directory forests named contoso.com and fabrikam.com. Both forests run only domain controllers that run Windows Server 2008.
The domain functional level of contoso.com is Windows Server 2008. The domain functional level of fabrikam.com is Windows Server 2003 Native mode.
You configure an external trust between contoso.com and fabrikam.com.
You need to enable the Kerberos AES encryption option.
What should you do?

A. Raise the forest functional level of fabrikam.com to Windows Server 2008.
B. Raise the domain functional level of fabrikam.com to Windows Server 2008.
C. Raise the forest functional level of contoso.com to Windows Server 2008.
D. Create a new forest trust and enable forest-wide authenticatio

Answer: B

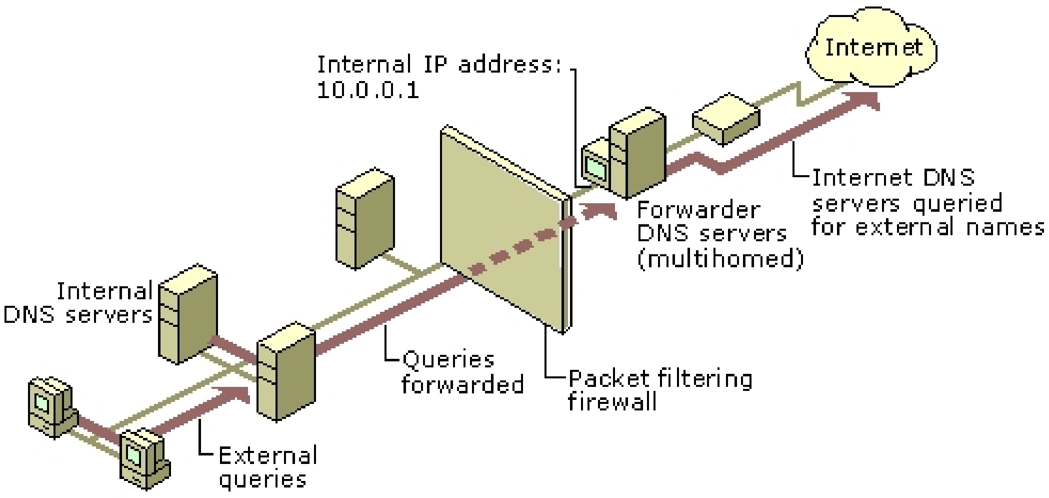
Explanation:
Answer: Raise the domain functional level of fabrikam.com to Windows Server 2008.
http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels%28v=ws.10%29.aspx Understanding Active Directory Domain Services (AD DS) Functional Levels Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities. They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest. However, functional levels do not affect which operating systems you can run on workstations and member servers that are joined to the domain or forest.
Features that are available at domain functional levels
Windows Server 2008 All of the default AD DS features, all of the features from the Windows Server 2003 domain functional level, and the following features are available:
* Advanced Encryption Standard (AES 128 and AES 256) support for the Kerberos protocol. In order for TGTs to be issued using AES, the domain functional level must be Windows Server 2008 or higher and the domain password needs to be changed.
Further information: http://technet.microsoft.com/en-us/library/cc749438%28WS.10%29.aspx Kerberos Enhancements
Requirements All Kerberos authentication requests involve three different parties: the client requesting a connection, the server that will provide the requested data, and the Kerberos KDC that provides the keys that are used to protect the various messages. This discussion focuses on how AES can be used to protect these Kerberos authentication protocol messages and data structures that are exchanged among the three parties. Typically, when the parties are operating systems running Windows Vista or Windows Server 2008, the exchange will use AES. However, if one of the parties is an operating system running Windows 2000 Professional, Windows 2000 Server, Windows XP, or Windows Server 2003, the exchange will not use AES.

NEW QUESTION 69
Your network consists of an Active Directory forest that contains two domains. All servers run Windows Server 2008 R2. All domain controllers are configured as DNS Servers.
You have a standard primary zone for dev.contoso.com that is stored on a member server.
You need to ensure that all domain controllers can resolve names from the dev.contoso.com zone.
What should you do?

A. On the member server, create a stub zon
B. On the member server, create a NS record for each domain controlle
C. On one domain controller, create a conditional forwarde
D. Configure the conditional forwarder to replicate to all DNS servers in the fores
E. On one domain controller, create a conditional forwarde
F. Configure the conditional forwarder to replicate to all DNS servers in the domai

Answer: C

Explanation:
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.


Internet
Internal IP address: 10.0.0.1
Internet DNS servers queried for external names
Forwarder DNS servers (multihomed)
Internal DNS servers
Queries forwarded
Packet filtering firewall
External queries

C:\Documents and Settings\usernwz1\Desktop\1.PNG
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

NEW QUESTION 71
Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2003.
You upgrade all domain controllers to Windows Server 2008.
You need to configure the Active Directory environment to support the application of multiple password policies.
What should you do?

A. Raise the functional level of the domain to Windows Server 2008.
B. On one domain controller, run dcpromo /ad
C. Create multiple Active Directory site
D. On all domain controllers, run dcpromo /ad

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc770842%28v=ws.10%29.aspx AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide This step-by-step guide provides instructions for configuring and applying fine-grained password and account lockout policies for different sets of users in Windows Server. 2008 domains. In Microsoft. Windows. 2000 and Windows Server 2003 Active Directory domains, you could apply only one password and account lockout policy, which is specified in the domain's Default Domain Policy, to all users in the domain. As a result, if you wanted different password and account lockout settings for different sets of users, you had to either create a password filter or deploy multiple domains. Both options were costly for different reasons. In Windows Server 2008, you can use fine-grained password policies to specify multiple password policies and apply different password restrictions and account lockout policies to different sets of users within a single domain. Requirements and special considerations for fine-grained password and account lockout policies Domain functional level: The domain functional level must be set to Windows Server 2008 or higher.

NEW QUESTION 76
Your company has an Active Directory forest. Each branch office has an organizational unit and a child organizational unit named Sales.
The Sales organizational unit contains all users and computers of the sales department.
You need to install an Office 2007 application only on the computers in the Sales organizational unit.
You create a GPO named SalesApp GPO.
What should you do next?

A. Configure the GPO to assign the application to the computer accoun
B. Link the SalesAPP GPO to the Sales organizational unit in each locatio
C. Configure the GPO to assign the application to the computer accoun
D. Link the SalesAPP GPO to the domai
E. Configure the GPO to publish the application to the user accoun
F. Link the SalesAPP GPO to the Sales organizational unit in each locatio
G. Configure the GPO to assign the application to the user accoun
H. Link the SalesAPP GPO to the Sales organizational unit in each locatio

Answer: A

NEW QUESTION 81
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 Wizar
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 zon
D. From the DNS Manager console, modify the permissions of the nwtraders.com zon

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.

NEW QUESTION 83
Your company has a main office and a branch office. The company has a single-domain Active Directory forest. The main office has two domain controllers named DC1 and DC2 that run Windows Server 2008 R2. The branch office has a Windows Server 2008 R2 read-only domain controller (RODC) named DC3.
All domain controllers hold the DNS Server role and are configured as Active Directory-integrated zones. The DNS zones only allow secure updates.
You need to enable dynamic DNS updates on DC3.
What should you do?

A. Run the Dnscmd.exe /ZoneResetType command on DC3.
B. Reinstall Active Directory Domain Services on DC3 as a writable domain controlle
C. Create a custom application directory partition on DC1. Configure the partition to store Active Directoryintegrated zone
D. Run the Ntdsutil.exe > DS Behavior commands on DC3.

Answer: B

Explanation:
Answer: Reinstall Active Directory Domain Services on DC3 as a writable domain controller.
http://technet.microsoft.com/en-us/library/cc754218%28WS.10%29.aspx#BKMK_DDNS Appendix A: RODC Technical Explanation Topics DNS updates for clients that are located in an RODC site When a client attempts a dynamic update, it sends a start of authority (SOA) query to its preferred Domain Name System (DNS) server. Typically, clients are configured to use the DNS server in their branch site as their preferred DNS server. The RODC does not hold a writeable copy of the DNS zone. Therefore, when it is queried for the SOA record, it returns the name of a writable domain controller that runs Windows Server 2008 or later and hosts the Active Directory–integrated zone, just as a secondary DNS server handles updates for zones that are not Active Directory–integrated zones. After it receives the name of a writable domain controller that runs Windows Server 2008 or later, the client is then responsible for performing the DNS record registration against the writeable server. The RODC waits a certain amount of time, as explained below, and then it attempts to replicate the updated DNS object in Active Directory Domain Services (AD DS) from the DNS server that it referred the client to through an RSO operation. Note: For the DNS server on the RODC to perform an RSO operation of the DNS record update, a DNS server that runs Windows Server 2008 or later must host writeable copies of the zone that contains the record. That DNS server must register a name server (NS) resource record for the zone. The Windows Server 2003 Branch Office Guide recommended restricting name server (NS) resource record registration to a subset of the available DNS servers. If you followed those guidelines and you do not register at least one writable DNS server that runs Windows Server 2008 or later as a name server for the zone, the DNS server on the RODC attempts to perform the RSO operation with a DNS server that runs Windows Server 2003. That operation fails and generates a 4015 Error in the DNS event log of the RODC, and replication of the DNS record update will be delayed until the next scheduled replication cycle. Further information: http://technet.microsoft.com/en-us/library/dd737255%28v=ws.10%29.aspx Plan DNS Servers for Branch Office Environments This topic describes best practices for installing Domain Name System (DNS) servers to support Active Directory Domain Services (AD DS) in branch office environments. As a best practice, use Active Directory–integrated DNS zones, which are hosted in the application directory partitions named ForestDNSZones and DomainDNSZones. The following guidelines are based on the assumption that you are following this best practice. In branch offices that have a read-only domain controller (RODC), install a DNS server on each RODC so that client computers in the branch office can still perform DNS lookups when the wide area network (WAN) link to a DNS server in a hub site is not available. The best practice is to install the DNS server when you install AD DS, using Dcpromo.exe. Otherwise, you must use Dnscmd.exe to enlist the RODC in the DNS application directory partitions that host Active Directory–integrated DNS zones. Note: You also have to configure the DNS client's setting for the RODC so that it points to itself as its preferred DNS server. To facilitate dynamic updates for DNS clients in branch offices that have an RODC, you should have at least one writeable Windows Server 2008 DNS server that hosts the corresponding DNS zone for which client computers in the branch office are attempting to make DNS updates. The writeable Windows Server 2008 DNS server must register name server (NS) resource records for that zone. By having the writeable Windows Server 2008 DNS server host the corresponding zone, client computers that are in branch offices that are serviced by RODCs can make dynamic updates more efficiently. This is because the updates replicate back to the RODCs in their respective branch offices by means of a replicate-singleobject (RSO) operation, rather than waiting for the next scheduled replication cycle. For example, suppose that you add a new member server in a branch office, Branch1, which includes an RODC. The member server hosts an application that you want client computers in Branch1 to locate by using a DNS query. When the member server attempts to register its host (A or AAAA) resource records for its IP address to a DNS zone, it performs a dynamic update on a writeable Windows Server 2008 or Windows Server 2008 R2 DNS server that the RODC tracks in Branch1. If a writeable Windows Server 2008 DNS server hosts the DNS zone, the RODC in Branch1 replicates the updated zone information as soon as possible from the writeable Windows Server 2008 DNS server. Then, client computers in Branch1 can successfully locate the new member server by querying the RODC in Branch1 for its IP address. If you do not have a writeable Windows Server 2008 DNS server that hosts the DNS zone, the update can still succeed against Windows Server 2003 DNS server if one is available but the updated record in the DNS zone will not replicate to the RODC in Branch1 until the next scheduled replication cycle, which can delay client computers that use the RODC DNS server for name resolution from locating the new member server.

NEW QUESTION 84
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 file
B. Install an Enterprise Subordinate CA and issue a user certificate to users of the encrypted file
C. Apply the Hisecdc security template to the domain controller
D. Archive the private key on the serve

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

NEW QUESTION 89
You need to identify all failed logon attempts on the domain controllers.
What should you do?

A. View the Netlogon.log fil
B. View the Security tab on the domain controller computer objec
C. Run Event Viewe
D. Run the Security and Configuration Wizar

Answer: C

Explanation:
http://support.microsoft.com/kb/174074 Security Event Descriptions This article contains descriptions of various security-related and auditing- related events, and tips for interpreting them. These events will all appear in the Security event log and will be logged with a source of "Security." Event ID: 529 Type: Failure Audit Description: Logon Failure: Reason: Unknown user name or bad password User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 530 Type: Failure Audit Description: Logon Failure: Reason: Account logon time restriction violation User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 531 Type: Failure Audit Description: Logon Failure: Reason: Account currently disabled User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 532 Type: Failure Audit Description: Logon Failure: Reason: The specified user account has expired User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 533 Type: Failure Audit Description: Logon Failure: Reason: User not allowed to logon at this computer User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 534 Type: Failure Audit Description: Logon Failure: Reason: The user has not been granted the requested logon type at this machine User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 535 Type: Failure Audit Description: Logon Failure: Reason: The specified account's password has expired User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 536 Type: Failure Audit Description: Logon Failure: Reason: The NetLogon component is not active User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6 Event ID: 537 Type: Failure Audit Description: Logon Failure: Reason: An unexpected error occurred during logon User Name: %1 Domain: %2 Logon Type: %3 Logon Process: %4 Authentication Package: %5 Workstation Name: %6

NEW QUESTION 91
You have a domain controller named DC1 that runs Windows Server 2008 R2. DC1 is configured as a DNS Server for contoso.com.
You install the DNS Server role on a member server named Server1 and then you create a standard secondary zone for contoso.com.
You configure DC1 as the master server for the zone.
You need to ensure that Server1 receives zone updates from DC1.
What should you do?

A. On DC1, modify the permissions of contoso.com zon
B. On Server1, add a conditional forwarde
C. On DC1, modify the zone transfer settings for the contoso.com zon
D. Add the Server1 computer account to the DNSUpdateProxy grou

Answer: C

Explanation: http://technet.microsoft.com/en-us/library/cc771652.aspx
Modify Zone Transfer Settings You can use the following procedure to control whether a zone will be transferred to other servers and which servers can receive the zone transfer.

To modify zone transfer settings using the Windows interface
1. Open DNS Manager.
2. Right-click a DNS zone, and then click Properties.
3. On the Zone Transfers tab, do one of the following:
To disable zone transfers, clear the Allow zone transfers check box.
To allow zone transfers, select the Allow zone transfers check box.
4. If you allowed zone transfers, do one of the following:
To allow zone transfers to any server, click To any server.
To allow zone transfers only to the DNS servers that are listed on the Name Servers tab, click Only to servers listed on the Name Servers tab.
To allow zone transfers only to specific DNS servers, click Only to the following servers, and then add the IP address of one or more DNS servers.

NEW QUESTION 96
All consultants belong to a global group named TempWorkers. You place three file servers in a new organizational unit named SecureServers. The three file servers contain confidential data located in shared folders.
You need to record any failed attempts made by the consultants to access the confidential data.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create and link a new GPO to the SecureServers organizational uni
B. Configure the Deny access to this computer from the network user rights setting for the TempWorkers global grou
C. Create and link a new GPO to the SecureServers organizational uni
D. Configure the Audit privilege use Failure audit policy settin
E. Create and link a new GPO to the SecureServers organizational uni
F. Configure the Audit object access Failure audit policy settin
G. On each shared folder on the three file servers, add the three servers to the Auditing ta
H. Configure the Failed Full control setting in the Auditing Entry dialog bo
I. On each shared folder on the three file servers, add the TempWorkers global group to the Auditing ta
J. Configure the Failed Full control setting in the Auditing Entry dialog bo

Answer: CE

Explanation:
Windows Server 2008 R2 Unleashed (SAMS, 2010) page 671
Auditing Resource Access
Object access can be audited, although it is not one of the recommended settings. Auditing object access can place a significant load on the servers, so it should only be enabled when it is specifically needed. Auditing object access is a two-step process: Step one is enabling “Audit object access” and step two is selecting the objects to be audited. When enabling Audit object access, you need to decide if both failure and success events will be logged. The two options are as follows:
Audit object access failure enables you to see if users are attempting to access objects to which they have no rights. This shows unauthorized attempts.
Audit object access success enables you to see usage patterns. This shows misuse of privilege.
After object access auditing is enabled, you can easily monitor access to resources such as folders, files, and printers.
Auditing Files and Folders
The network administrator can tailor the way Windows Server 2008 R2 audits files and folders through the property pages for those files or folders. Keep in mind that the more files and folders that are audited, the more events that can be generated, which can increase administrative overhead and system resource requirements.
Therefore, choose wisely which files and folders to audit. To audit a file or folder, do the following:
1. In Windows Explorer, right-click the file or folder to audit and select Properties.
2. Select the Security tab and then click the Advanced button.
3. In the Advanced Security Settings window, select the Auditing tab and click the Edit button.
4. Click the Add button to display the Select User or Group window.
5. Enter the name of the user or group to audit when accessing the file or folder. Click the Check Names button to verify the name.

NEW QUESTION 99
You have a Windows Server 2008 R2 Enterprise Root CA.
Security policy prevents port 443 and port 80 from being opened on domain controllers and on the issuing CA.
You need to allow users to request certificates from a Web interface. You install the Active Directory Certificate Services (AD CS) server role.
What should you do next?

A. Configure the Online Responder Role Service on a member serve
B. Configure the Online Responder Role Service on a domain controlle
C. Configure the Certificate Enrollment Web Service role service on a member serve
D. Configure the Certificate Enrollment Web Service role service on a domain controlle

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd759209.aspx Certificate Enrollment Web Service Overview The Certificate Enrollment Web Service is an Active Directory Certificate Services (AD CS) role service that enables users and computers to perform certificate enrollment by using the HTTPS protocol. Together with the Certificate Enrollment Policy Web Service, this enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain. Personal note: Since domain controllers are off-limits (regarding open ports), you are left to install the Certificate Enrollment Web Service role service on a plain member server

NEW QUESTION 100
Your company has an organizational unit named Production. The Production organizational unit has a child organizational unit named R&D. You create a GPO named Software Deployment and link it to the Production organizational unit.
You create a shadow group for the R&D organizational unit. You need to deploy an application to users in the Production organizational unit.
You also need to ensure that the application is not deployed to users in the R&D organizational unit.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Configure the Block Inheritance setting on the R&D organizational uni
B. Configure the Enforce setting on the software deployment GP
C. Configure security filtering on the Software Deployment GPO to Deny Apply group policy for the R&D security grou
D. Configure the Block Inheritance setting on the Production organizational uni

Answer: AC

Explanation:
Answer: Configure the Block Inheritance setting on the R&D organizational unit. Configure security filtering on the Software Deployment GPO to Deny Apply group policy for the R&D security group.
http://technet.microsoft.com/en-us/library/cc757050%28v=ws.10%29.aspx Managing inheritance of Group Policy
Blocking Group Policy inheritance You can block policy inheritance for a domain or organizational unit. Using block inheritance prevents GPOs linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. By default, children inherit all GPOs from the parent, but it is sometimes useful to block inheritance. For example, if you want to apply a single set of policies to an entire domain except for one organizational unit, you can link the required GPOs at the domain level (from which all organizational units inherit policies by default) and then block inheritance only on the organizational unit to which the policies should not be applied.
Enforcing a GPO link You can specify that the settings in a GPO link should take precedence over the settings of any child object by setting that link to Enforced. GPO-links that are enforced cannot be blocked from the parent container. Without enforcement from above, the settings of the GPO links at the higher level (parent) are overwritten by settings in GPOs linked to child organizational units, if the GPOs contain conflicting settings. With enforcement, the parent
GPO link always has precedence. By default, GPO links are not enforced. In tools prior to GPMC, "enforced" was known as "No override."
In addition to using GPO links to apply policies, you can also control how GPOs are applied by using security filters or WMI filters.
http://technet.microsoft.com/en-us/library/cc781988%28v=ws.10%29.aspx
Security filtering using GPMC
Security filtering Security filtering is a way of refining which users and computers will receive and apply the settings in a Group Policy object (GPO). Using security filtering, you can specify that only certain security principals within a container where the GPO is linked apply the GPO. Security group filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO.
Notes:
GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units. However, by using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer.
The location of a security group in Active Directory is irrelevant to security group filtering and, more generally, irrelevant to Group Policy processing.
Further information:
http://technet.microsoft.com/en-us/library/cc731076.aspx
Block Inheritance
http://en.wikipedia.org/wiki/Active_Directory#Shadow_groups
Active Directory
Shadow groups
In Microsoft's Active Directory, OUs do not confer access permissions, and objects placed within OUs are not automatically assigned access privileges based on their containing OU. This is a design limitation specific to Active Directory. Other competing directories such as Novell NDS are able to assign access privileges through object placement within an OU. Active Directory requires a separate step for an administrator to assign an object in an OU as a member of a group also within that OU. Relying on OU location alone to determine access permissions is unreliable, because the object may not have been assigned to the group object for that OU. A common workaround for an Active Directory administrator is to write a custom PowerShell or Visual Basic script to automatically create and maintain a user group for each OU in their directory. The scripts are run periodically to update the group to match the OU's account membership, but are unable to instantly update the security groups anytime the directory changes, as occurs in competing directories where security is directly implemented into the directory itself. Such groups are known as Shadow Groups. Once created, these shadow groups are selectable in place of the OU in the administrative tools. Microsoft refers to shadow groups in the Server 2008 Explanation documentation, but does not explain how to create them. There are no built-in server methods or console snap-ins for managing shadow groups.[5] The division of an organization's information infrastructure into a hierarchy of one or more domains and toplevel OUs is a key decision. Common models are by business unit, by geographical location, by IT Service, or by object type and hybrids of these. OUs should be structured primarily to facilitate administrative delegation, and secondarily, to facilitate group policy application. Although OUs form an administrative boundary, the only true security boundary is the forest itself and an administrator of any domain in the forest must be trusted across all domains in the forest.[6]

NEW QUESTION 103
......