Microsoft

Exam 70-640

Windows Server 2008 Active Directory, Configuring

Version: 41.0

[Total Questions: 631]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	100
Topic 6: Volume F	131

Topic 1, Volume A

Question No : 1 - (Topic 1)

Contoso, Ltd. has an Active Directory domain named ad.contoso.com. Fabrikam, Inc. has an Active Directory domain named intranet.fabrikam.com. Fabrikam's security policy prohibits the transfer of internal DNS zone data outside the Fabrikam network.

You need to ensure that the Contoso users are able to resolve names from the intranet.fabrikam.com domain.

What should you do?

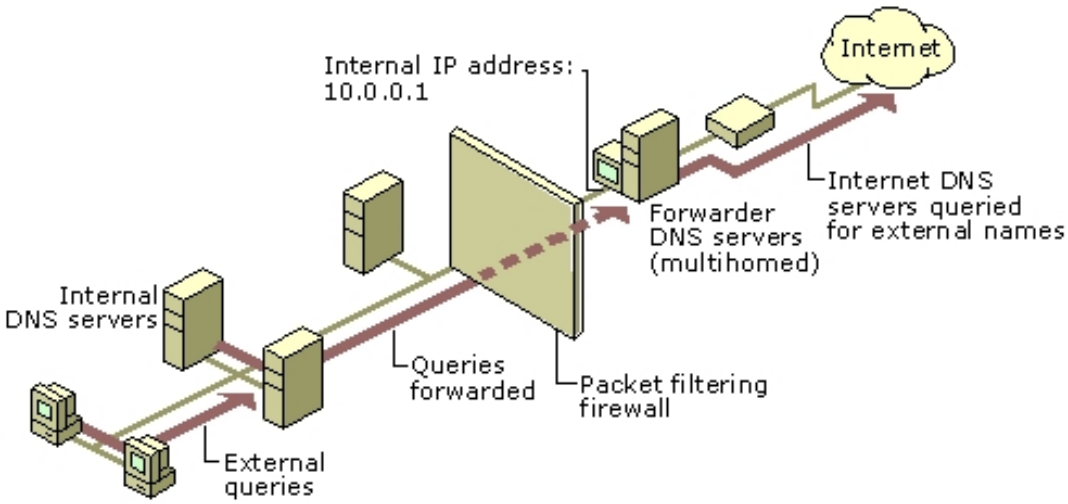
A. Create a new stub zone for the intranet.fabrikam.com domain.
B. Configure conditional forwarding for the intranet.fabrikam.com domain.
C. Create a standard secondary zone for the intranet.fabrikam.com domain.
D. Create an Active DirectoryCintegrated zone for the intranet.fabrikam.com domain.

Answer: B

Explanation:

Answer: Configure conditional forwarding for the intranet.fabrikam.com domain.

http://technet.microsoft.com/en-us/library/cc730756.aspx
Understanding Forwarders
A forwarder is a Domain Name System (DNS) server on a network that forwards DNS queries for external DNS names to DNS servers outside that network. You can also forward queries according to specific domain names using conditional forwarders.
You designate a DNS server on a network as a forwarder by configuring the other DNS servers in the network to forward the queries that they cannot resolve locally to that DNS server. By using a forwarder, you can manage name resolution for names outside your network, such as names on the Internet, and improve the efficiency of name resolution for the computers in your network.
The following figure illustrates how external name queries are directed with forwarders.



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

Question No : 2 - (Topic 1)

Your company has a main office and three branch offices. Each office is configured as a separate Active Directory site that has its own domain controller.

You disable an account that has administrative rights.

You need to immediately replicate the disabled account information to all sites.

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

A. From the Active Directory Sites and Services console, configure all domain controllers

as global catalog servers.

B. From the Active Directory Sites and Services console, select the existing connection objects and force replication.

C. Use Repadmin.exe to force replication between the site connection objects.

D. Use Dsmod.exe to configure all domain controllers as global catalog servers.

Answer: B,C

Explanation:

http://technet.microsoft.com/en-us/library/cc835086%28v=ws.10%29.aspx

Repadmin /syncall Synchronizes a specified domain controller with all of its replication partners.

http://ivan.dretvic.com/2012/01/how-to-force-replication-of-domain-controllers/

How to force replication of Domain Controllers From time to time its necessary to kick off AD replication to speed up a task you may be doing, or just a good too to check the status of replication between DC's.

Below is a command to replicate from a specified DC to all other DC's.

Repadmin /syncall DC_name /Aped By running a repadmin /syncall with the /A(ll partitions) P(ush) e(nterprise, cross sites) d(istinguished names) parameters, you have duplicated exactly what Replmon used to do in Windows 2003, except that you did it in one step, not many.And with the benefit of seeing immediate results on how the operations are proceeding.

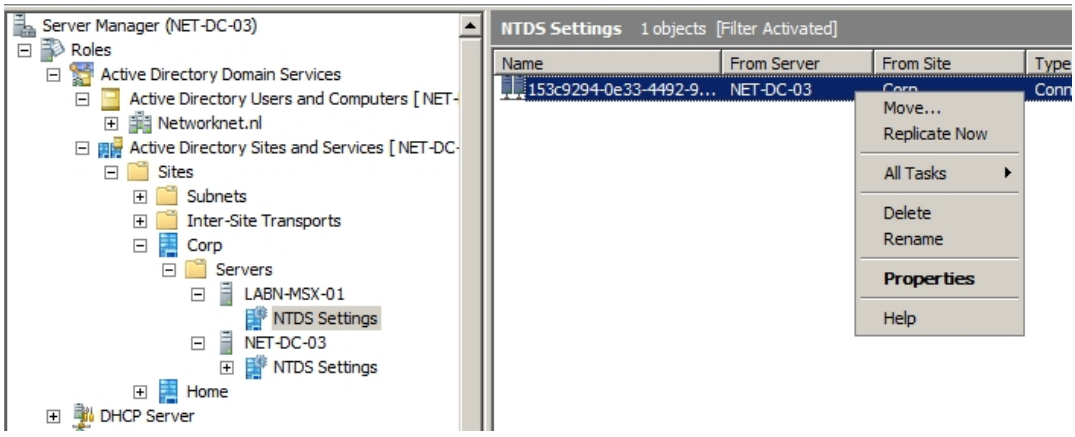
If I am running it on the DC itself, I don't even have to specify the server name.

http://technet.microsoft.com/en-us/library/cc776188%28v=ws.10%29.aspx

Force replication over a connection

To force replication over a connection

1. Open Active Directory Sites and Services.



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

Question No : 3 - (Topic 1)

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.

Question No : 4 - (Topic 1)

Your company has an Active Directory domain. You have a two-tier PKI infrastructure that contains an offline root CA and an online issuing CA. The Enterprise certification authority is running Windows Server 2008 R2.

You need to ensure users are able to enroll new certificates.

What should you do?

A. Renew the Certificate Revocation List (CRL) on the root CA. Copy the CRL to the CertEnroll folder on the issuing CA.
B. Renew the Certificate Revocation List (CRL) on the issuing CA, Copy the CRL to the SysternCertificates folder in the users' profile.
C. Import the root CA certificate into the Trusted Root Certification Authorities store on all

client workstations.

D. Import the issuing CA certificate into the Intermediate Certification Authorities store on all client workstations.

Answer: A

Explanation:

http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx

Offline Root Certification Authority (CA)

A root certification authority (CA) is the top of a public key infrastructure (PKI) and generates a self-signed certificate. This means that the root CA is validating itself (self-validating). This root CA could then have subordinate CAs that effectively trust it. The subordinate CAs receive a certificate signed by the root CA, so the subordinate CAs can issue certificates that are validated by the root CA. This establishes a CA hierarchy and trust path.

CA Compromise

If a root CA is in some way compromised (broken into, hacked, stolen, or accessed by an unauthorized or malicious person), then all of the certificates that were issued by that CA are also compromised. Since certificates are used for data protection, identification, and authorization, the compromise of a CA could compromise the security of an entire organizational network. For that reason, many organizations that run internal PKIs install their root CA offline. That is, the CA is never connected to the company network, which makes the root CA an offline root CA. Make sure that you keep all CAs in secure areas with limited access.

To ensure the reliability of your CA infrastructure, specify that any root and non-issuing intermediate CAs must be offline. A non-issuing CA is one that is not expected to provide certificates to client computers, network devices, and so on. This minimizes the risk of the CA private keys becoming compromised, which would in turn compromise all the certificates that were issued by the CA.

How Do Offline CAs issue certificates?

Offline root CAs can issue certificates to removable media devices (e.g. floppy disk, USB drive, CD/DVD) and then physically transported to the subordinate CAs that need the certificate in order to perform their tasks. If the subordinate CA is a non-issuing intermediate that is offline, then it will also be used to generate a certificate and that certificate will be placed on removable media. Each CA receives its authorization to issue certificates from the CA directly above it in the CA hierarchy. However, you can have multiple CAs at the same level of the CA hierarchy. Issuing CAs are typically online and used to issue certificates to client computers, network

devices, mobile devices, and so on. Do not join offline CAs to an Active Directory Domain Services domain Since offline CAs should not be connected to a network, it does not make sense to join them to an Active Directory Domain Services (AD DS) domain, even with the

Offline Domain Join [This link is external to TechNet Wiki. It will open in a new window.] option introduced with Windows 7 and Windows Server 2008 R2.
Furthermore, installing an offline CA on a server that is a member of a domain can cause problems with a secure channel when you bring the CA back online after a long offline period. This is because the computer account password changes every 30 days. You can get around this by problem and better protect your CA by making it a member of a workgroup, instead of a domain. Since Enterprise CAs need to be joined to an AD DS domain, do not attempt to install an offline CA as a Windows Server Enterprise CA.
http://technet.microsoft.com/en-us/library/cc740209%28v=ws.10%29.aspx
Renewing a certification authority
A certification authority may need to be renewed for either of the following reasons:
Change in the policy of certificates issued by the CA
Expiration of the CA's issuing certificate

Question No : 5 - (Topic 1)

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

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

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

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

Choose three.)

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

Answer: B,C,E

Explanation:

http://technet.microsoft.com/en-us/library/cc779954%28v=ws.10%29.aspx
Role-based administration
Role explanation
Role-based administration involves CA roles, users, and groups. To assign a role to a user or group, you must assign the role's corresponding security permissions, group memberships, or user rights to the user or group.
These security permissions, group memberships, and user rights are used to distinguish which users have which roles. The following table describes the CA roles of role-based administration and the groups relevant to role-based administration.

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

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

Certificate Manager:
Delete multiple rows in database (bulk deletion)
Issue and approve certificates
Deny certificates
Revoke certificates
Reactivate certificates placed on hold
Renew certificates
Recover archived key
Read CA database
Read CA configuration information

http://technet.microsoft.com/en-us/library/cc753372.aspx
Restrict Certificate Managers
A certificate manager can approve certificate enrollment and revocation requests, issue certificates, and manage certificates. This role can be configured by assigning a user or group the Issue and Manage Certificatespermission.
When you assign this permission to a user or group, you can further refine their ability to manage certificates by group and by certificate template. For example, you might want to implement a restriction that they can only approve requests or revoke smart card logon certificates for users in a certain office or organizational unit that is the basis for a security group.