Windows Server 2008 Active Directory, Configuring

Microsoft 70-640 Dumps Available Here at:

Question 1

Your company has an Active Directory forest that contains a single domain. The domain member server has an Active Directory Federation Services (AD FS) role installed. You need to configure AD FS to ensure that AD FS tokens contain information from the Active Directory domain. What should you do?

Options:

A. Add and configure a new account partner.

B. Add and configure a new resource partner.

C. Add and configure a new account store.

D. Add and configure a Claims-aware application.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc732095.aspx
Understanding Account Stores
Active Directory Federation Services (AD FS) uses account stores to log on users and extract security claims for those users. You can configure multiple account stores for a single Federation Service. You can also define their priority. The Federation Service uses Lightweight Directory Access Protocol (LDAP) to communicate with account stores. AD FS supports the following two account stores:
Active Directory Domain Services (AD DS)
Active Directory Lightweight Directory Services (AD LDS)

Question 2

You network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. You need to reset the Directory Services Restore Mode (DSRM) password on a domain controller.

What tool should you use?

Options:

A. Active Directory Users and Computers snap-in

B. ntdsutil

C. Local Users and Groups snap-in

D. dsmod

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc753343%28v=ws.10%29.aspx
Ntdsutil
Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the ntdsutil commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for use by experienced administrators.
..
Commands set DSRM password - Resets the Directory Services Restore Mode (DSRM) administrator password.
Further information:
http://technet.microsoft.com/en-us/library/cc754363%28v=ws.10%29.aspx
Set DSRM password
Resets the Directory Services Restore Mode (DSRM) password on a domain controller. At the Reset DSRM
Administrator Password: prompt, type any of the parameters listed under "Syntax." This is a subcommand of Ntdsutil and Dsmgmt. Ntdsutil and Dsmgmt are command-line tools that are built into Windows Server 2008 and Windows Server 2008 R2. Ntdsutil is available if you have the Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS) server role installed.
Dsmgmt is available if you have the AD LDS server role installed. These tools are also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT).

Question 3

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers. A domain controller named DC1 has a standard primary zone for contoso.com. A domain controller named DC2 has a standard secondary zone for contoso.com. You need to ensure that the replication of the contoso.com zone is encrypted. You must not lose any zone data. What should you do?

Options:

A. Convert the primary zone into an Active Directory-integrated stub zone. Delete the secondary zone.

B. Convert the primary zone into an Active Directory-integrated zone. Delete the secondary zone.

C. Configure the zone transfer settings of the standard primary zone. Modify the Master Servers lists on the

secondary zone.

D. On both servers, modify the interface that the DNS server listens on.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc771150.aspx
Change the Zone Type
You can use this procedure to change make a zone a primary, secondary, or stub zone. You can also use it to integrate a zone with Active Directory Domain Services (AD DS). http://technet.microsoft.com/en-us/library/cc726034.aspx Understanding Active Directory Domain Services Integration The DNS Server service
is integrated into the design and implementation of Active Directory Domain Services (AD DS). AD DS provides an enterprise-level tool for organizing, managing, and locating resources in a network.
Benefits of AD DS integration
For networks that deploy DNS to support AD DS, directory-integrated primary zones are strongly recommended. They provide the following benefits:
DNS features multimaster data replication and enhanced security based on the capabilities of AD DS. In a standard zone storage model, DNS updates are conducted based on a single-master update model. In this model, a single authoritative DNS server for a zone is designated as the primary source for the zone. This server maintains the master copy of the zone in a local file. With this model, the primary server for the zone represents a single fixed point of failure. If this server is not available, update requests from DNS clients are not processed for the zone. With directory-integrated storage, dynamic updates to DNS are sent to any AD DS-integrated DNS server and are replicated to all other AD DS-integrated DNS servers by means of AD DS replication. In this model, any AD DS-integrated DNS servercan accept dynamic updates for the zone. Because the master copy of the zone is maintained in the AD DS database, which is fully replicated to all domain controllers, the zone can be updated by the DNS servers operating at any domain controller for the domain. With the multimaster update model of AD DS, any of the primary servers for the directoryintegrated zone can process requests from DNS clients to update the zone as long as a domain controller is available and reachable on the network.
..
Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an AD DS domain.
By integrating storage of your DNS zone databases in AD DS, you can streamline database replication

planning for your network.

Directory-integrated replication is faster and more efficient than standard DNS replication. http://technet.microsoft.com/en-us/library/ee649124%28v=ws.10%29.aspx Deploy IPsec Policy to DNS Servers

You can deploy IPsec rules through one of the following mechanisms:

Domain Controllers organizational unit (OU): If the DNS servers in your domain are Active Directoryintegrated, you can deploy IPsec policy settings using the Domain Controllers OU. This option is recommended to make configuration and deployment easier. DNS Server OU or security group: If you have DNS servers that are not domain controllers, then consider creating a separate OU or a security group with the computer accounts of your DNS servers. Local firewall configuration: Use this option if you have DNS servers that are not domain members or if you have a small number of DNS servers that you want to configure locally. http://technet.microsoft.com/en-us/library/cc772661%28v=ws.10%29.aspx Deploying Secure DNS

Protecting DNS Servers

When the integrity of the responses of a DNS server are compromised or corrupted, or when the DNS data is tampered with, clients can be misdirected to unauthorized locations without their knowledge. After the clients start communicating with these unauthorized locations, attempts can be made to gain access to information that is stored on the client computers. Spoofing and cache pollution are examples of this type of attack. Another type of attack, the denial-of-service attack, attempts to incapacitate a DNS server to make DNS infrastructure unavailable in an enterprise. To protect your DNS servers from these types of attacks:

Use IPsec between DNS clients and servers.

Monitor network activity.

Close all unused firewall ports.

Implementing IPsec Between DNS Clients and Servers

IPsec encrypts all traffic over a network connection. Encryption minimizes the risk that data that is sent between the DNS clients and the DNS servers can be scanned for sensitive information or tampered with by anyone attempting to collect information by monitoring traffic on the network. When IPsec is enabled, both ends of a connection are validated before communication begins. A client can be certain that the DNS server with which it is communicating is a valid server. Also, all communication over the connection is encrypted, thereby eliminating the possibility of tampering with client communication. Encryption prevents spoofing attacks, which are false responses to DNS client queries by unauthorized sources that act like a DNS server.

Further information:

http://technet.microsoft.com/en-us/library/cc771898.aspx Understanding Zone Types

The DNS Server service provides for three types of zones:

Primary zone

Secondary zone

Stub zone

Note: If the DNS server is also an Active Directory Domain Services (AD DS) domain controller, primary zones and stub zones can be stored in AD DS.

The following sections describe each of these zone types:

Primary zone When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named zone_name.dns and it is located in the % windir%\System32\Dns folder on the server. Secondary zone When a zone that this DNS server

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

zone data is stored in a text file, which can be found in system32\dns.

Question 4

Your company has a main office and a branch office. You deploy a read-only domain controller (RODC) that
runs Microsoft Windows Server 2008 to the branch office. You need to ensure that users at the branch office are able to log on to the domain by using the RODC. What should you do?

Options:

A. Add another RODC to the branch office.

B. Configure a new bridgehead server in the main office.

C. Decrease the replication interval for all connection objects by using the Active Directory Sites and

Services console.

D. Configure the Password Replication Policy on the RODC.

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/cc754956%28v=ws.10%29.aspx
RODC Frequently Asked Questions
What new attributes support the RODC Password Replication Policy? Password Replication Policy is the mechanism for determining whether a user or computer's credentials are allowed to replicate from a writable domain controller to an RODC. The Password Replication Policy is always set on a writable domain
controller running Windows Server 2008. What operations fail if the WAN is offline, but the RODC is online in the branch office? If the RODC cannot connect to a writable domain controller running Windows Server 2008 in the hub, the following branch office operations fail:
Password changes
Attempts to join a computer to a domain
Computer rename
Authentication attempts for accounts whose credentials are not cached on the RODC Group Policy updates that an administrator might attempt by running the gpupdate /force command What operations succeed if the WAN is offline, but the RODC is online in the branch office? If the RODC cannot connect to a writable domain controller running Windows Server 2008 in the hub, the following branch office operations succeed:
Authentication and logon attempts, if the credentials for the resource and the requester are already cached,
Local RODC server administration performed by a delegated RODC server administrator.

file at:

https://www.certification-questions.com/microsoft-pdf/70-640-pdf.html