Chapter 2

Implementing Active Directory

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. You can install Active Directory from the Windows command-line using the \_\_dcpromo\_\_ utility.

2. The \_Password Replication Policy\_ will configure which user accounts will or will not be cached on an RODC.

3. The \_nslookup\_ command allows you to troubleshoot DNS information from the command line.

4. To install Active Directory on a Server Core computer, you will need to use a(n) \_unattended installation\_.

5. You can use \_User Principal Names (UPNs)\_ to ease the user logon process in a large, multidomain environment.

6. The \_\_SYSVOL\_\_ shared folder is replicated to each domain controller and stores domain-wide information such as Group Policy Objects and login scripts.

7. Active Directory \_latency\_ refers to the amount of time it takes for changes to replicate to every domain controller in an environment.

8. \_Incremental\_ zone transfers allow modern DNS servers to replicate only records that have been changed, rather than the contents of an entire zone.

9. The Active Directory Domain Services \_\_binaries\_\_ are not installed on a Windows Server 2008 computer until you add the AD DS role to the computer.

10. If two SRV records have the same priority, the frequency by which they are accessed by clients will be determined by their relative \_weight\_.

Multiple Choice

Select the correct answer for each of the following questions. Choose all answers that are correct.

1. What mechanism within DNS is used to set up load balancing between multiple servers that are advertising the same SRV records?

a. Protocol

b. Domain name

c. Port

d. Priority

Clients will always use DNS records with a lower-numbered priority before one with a higher-numbered priority. Clients only use a host with a higher-numbered priority SRV record if hosts corresponding to lower-numbered SRV records are unavailable.

2. What security improvement allows you to begin the installation of an RODC from a secure central location before completing it at the remote site where the RODC will be housed?

a. Staged installation

b. Two-part installation

c. Part I installation

d. Multi-part installation

The staged installation of RODC allows you to delegate the ability to install an RODC without granting rights within Active Directory itself, which allows you to further secure the process of creating an RODC.

3. What does each class or attribute that you add to the Active Directory schema need to have?

a. Protocol

b. Object Identifier

c. Priority

d. Port

Each Object Identifier, represented by a dotted-decimal notation string such as 2.5.4.20, must be globally unique within an Active Directory forest.

4. Which Windows Server 2008 feature enables you to perform certain Active Directory maintenance functions without needing to reboot the domain controller?

a. Directory Services Restore Mode

b. Safe Mode

c. Safe Mode with Networking

d. Restartable Active Directory

Restartable Active Directory is a new feature of Windows Server 2008 that enables you to place the ntds.dit file in an offline mode, allowing you to start and stop Active Directory.

5. Which utility allows you to create, remove, and maintain Active Directory trust relationships from the command-line?

a. Repadmin

b. Nslookup

c. Netdom

d. Shstat

In Active Directory, you can manage trust relationships using the Active Directory Domains & Trusts MMC snap-in GUI interface. If you prefer to work from the command line, you can use the built-in netdom.exe utility.

6. What is the new unified tool, introduced by Windows Server 2008, for managing numerous aspects of a 2008 server?

a. Computer Management

b. Server Manager

c. Active Directory Users & Computers

d. Active Directory Domains & Trusts

Windows Server 2008 introduces the Server Manager console, which allows you to perform network configuration tasks, manage the Windows Firewall, and add and remove server roles and features from a single point of administration.

7. Although all writeable domain controllers use multimaster replication, there are certain sensitive operations that can only be controlled by one DC at a time. What is this functionality known as?

a. Flexible Single Master Operations (FSMO) roles

b. Flexible Multiple Master Operations (FMMO) roles

c. Flexible Single Operations Master (FSOM) roles

d. Flexible Multiple Operations Master (FMOM) roles

There are two forest-wide and three domain-wide FSMO roles. The first domain controller installed in a forest holds all five FSMO roles for the forest root domain; the first DC in any additional domains holds all three domain-wide FSMO roles for the new domain.

8. What Windows Server 2008 feature allows you to configure a user or group as the local administrator of an RODC without delegating any rights to the user or group within Active Directory?

a. Flexible Single Master Operations (FSMO) roles

b. Admin Role Separation

c Staged Installations

d. Active Directory Lightweight Domain Services (AD LDS)

The Admin Role Separation feature is only available on Read-Only Domain Controllers; you cannot configure this feature on writeable DCs because they still participate in multimaster replication.

9. What is a new installation option in Windows Server 2008 that features a minimal installation footprint designed to run specific infrastructure services?

a. RODC

b. FSMO

c. Server Core

d. Web Server Edition

The Server Core installation option in Windows Server 2008 runs almost entirely without a graphical user interface and needs to be administered primarily from the command line.

10. What term describes the length of time for which a DNS record is valid, after which it needs to be re-registered?

a. Protocol

b. Priority

c. Weight

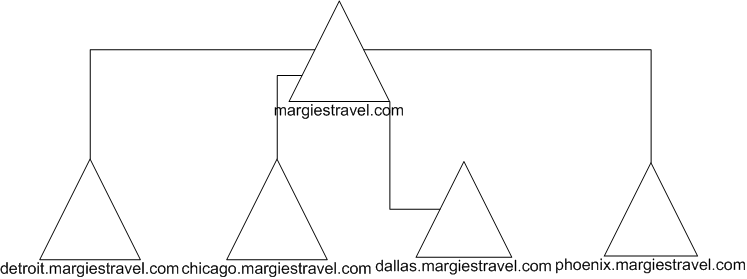
d. Time-to-Live

The TTL guards against scenarios in which out-of-date DNS records remain active within a DNS server. This field is referred to as the hop limit in IPv6.

Case Scenarios

Scenario 2-1: Designing Active Directory

Margie's Travel has decided to install a Windows Server 2003 network. They plan to use the name margiestravel.com as their DNS name, because it is already registered with the InterNic. The corporate headquarters is located in Detroit and branches are located in Chicago, Dallas, and Phoenix. Margie's Travel wants to maintain a separate child domain in the forest representing each of the branches for ease of management. Create a pen and paper drawing of how you would design this forest structure. Be sure to include the recommended domain names within the forest.



Scenario 2-2: Configuring Access Across Networks

The management of Margie's Travel has just released the names of several vendors that you must allow access to network resources. These vendors have Microsoft Windows 2000, Windows Server 2003, or Windows Server 2008 domains. You have established a domain that holds all the information that vendors will need to access within your forest. The vendors want to be able to gain access to these resources without permitting access for your company to their network. What do you need to do to make this happen?

Functional level is Windows 2000. Configure external trusts (one-way, nontransitive) between margiestravel.com and the partner organizations to ensure that data access only flows in one direction.

Scenario 2-3: Planning a Migration

You are an IT consultant working with a mid-sized corporation to improve its network. Currently the company is running six Windows 2000 servers in three separate domains. The workstations run various versions of Microsoft Windows, including Windows 2000 Professional and Windows XP Professional. Several new Windows Vista Business machines are being used by management. The company has decided to migrate to Windows Server 2008 using Active Directory to take advantage of centralized administration and better security. To help you consult with your customer, answer the following questions.

1. What considerations should you make during the migration planning?

Operating system level of current servers and workstations in the existing Active Directory environment.

2. What recommendations will you make?

Perform a complete inventory of all existing domain controllers, and document scheduled plans to upgrade or replace domain controllers that are running legacy operating systems.

3. What functional level should be set initially?

Windows 2000 Native at the domain and forest functional levels

Scenario 2-4: DNS Naming

The same client discussed in Scenario 2-3 already has a DNS name registered with the Internet. The client uses it for the company's Web site, which allows customers to access the product database and place orders online. Your client would like to use the same name for its internal network, but you have been advised that using the internal network may affect network security. What options would you suggest they explore to allow some naming consistency while providing internal network security?

You can configure the internal domain name using the .local extension rather than .com, .net, or .org to separate your internal from your external namespace.