Lesson 4

Global Catalog and Flexible Single-Master Operations (FSMO) Roles

Knowledge Assessment

Fill in the Blank

1. Active Directory will tolerate a maximum of a 5-minute \_\_clock skew\_\_ between a client and the domain controller that authenticates it. P87

2. The \_\_ PDC Emulator\_\_ is responsible for managing time synchronization within a domain. P85

3. You can improve login times in a site that does not contain a global catalog server by implementing \_\_universal group membership caching\_\_. P81

4. To add or remove an application directory partition from Active Directory, the \_\_Domain Naming Master\_\_ needs to be accessible. P87

5. If a domain controller that holds a FSMO role fails and will not be returned to the network, you can \_\_seize\_\_ the FSMO role to another domain controller. P91

6. You can add additional attributes to the \_\_partial attribute set (PAS)\_\_ by modifying the Active Directory schema. P80

7. The \_\_security identifier (SID)\_\_ uniquely identifies an object within an Active Directory domain, but will change if an object is moved from one domain to another. P85

8. The \_\_ Infrastructure Master \_\_ FSMO role should not be housed on a domain controller that has been configured as a global catalog. P85

9. You can transfer the \_\_Domain Naming Master\_\_ FSMO from one domain controller to another using the Active Directory Domains and Trusts MMC snap-in. P87

10. Membership information for a(n) \_\_universal group\_\_ is stored on the global catalog. P81

Multiple Choice

1. What is the Active Directory component that contains a reference to all objects within Active Directory called?

a. Main database

b. Central catalog

c. Global database

d. Global catalog

The Global Catalog server contains a reference to each object within an Active Directory forest, regardless of which domain the GC belongs to or how many domains are configured within the forest. P80

2. Which of the following roles is a forest-wide FSMO role?

a. PDC Emulator

b. Infrastructure Master

c. Schema Master

d. Global catalog

The Schema Master and the Domain Naming Master are the forest-wide FSMO roles. Each Active Directory domain also has three domain-wide FSMOs: the PDC Emulator, the Infrastructure Master, and the RID Master. P87

3. To which port does the \_gc SRV record listen?

a. TCP 445

b. UDP 137

c. TCP 3268

d. UDP 445

The Global Catalog answers queries on TCP port 3268. Normal domain controller LDAP queries take place on TCP port 389. P.83

4. You are the administrator of an Active Directory forest that contains a forest root domain with three child domains. How many of each FSMO does this forest contain?

a. 1 Domain Naming Master, 1 Schema Master, 3 PDC Emulators, 3 Infrastructure Masters, 3 RID Masters

b. 3 Domain Naming Masters, 3 Schema Masters, 3 PDC Emulators, 3 Infrastructure Masters, 3 RID Masters

c. 1 Domain Naming Master, 1 Schema Master, 4 PDC Emulators, 4 Infrastructure Masters, 4 RID Masters

d. 1 Domain Naming Master, 1 Schema Master, 1 PDC Emulator, 1 Infrastructure Master, 1 RID Master

There is only one forest-wide Domain Naming Master and Schema Master per forest. Because there are four total domains in this example (the forest root domain and the three child domains), there will be four of each domain-wide FSMO role.

5. The Schema Master FSMO for your forest will be taken offline for a few hours so that your hardware vendor can replace the motherboard of the server. To allow your clients to continue to log in, what is the minimum that you need to do?

a. Transfer the Schema Master FSMO to another domain controller before taking it offline.

b. Seize the Schema Master FSMO to another domain controller before taking it offline.

c. Do nothing. Your clients will still be able to log in while the Schema Master is offline.

d. Disable the domain controller's computer account from Active Directory Users and Computers before taking it offline.

The Schema Master is only required when an application is installed that will extend the Active Directory schema. This FSMO role is not noticeable during day-to-day client logon operations and thus can be taken offline for a short period of time without impacting client activities.

6. You are a member of the Domain Admins group of a child domain on an Active Directory network. You have an application that requires you to configure an application directory partition, but you find that you are unable to do so. What could be preventing you from creating an application directory partition in your domain?

a. You must be a member of the Enterprise Admins group to create an application directory partition.

b. You must be a member of the Schema Admins group to create an application directory partition.

c. You must be a member of the Forest Admins group to create an application directory partition.

d. You must be a member of the DNS Admins group to create an application directory partition.

Only Enterprise Administrators can create application directory partitions because these have the potential to be replicated forest-wide.

7. The RID Master FSMO distributes RIDs to domain controllers in increments of \_\_\_\_.

a. 100

b. 250

c. 500

d. 1,000

By default, the RID Master FSMO role hands out Relative Identifiers (RIDs) to each domain controller in a domain in increments of 500. Each DC will go back to the RID Master to obtain a new supply of RIDs when their current allotment runs out. P85

8. You are logging onto an Active Directory child domain from a workstation running Windows Vista Business. By default, where will this workstation look to synchronize its clock with the domain?

a. The PDC Emulator for the child domain

b. The PDC Emulator for the forest root domain.

c. An external clock

d. The domain controller that authenticates the workstation

Active Directory time synchronization is hierarchical, wherein the PDC Emulator for each domain will synchronize its time with the PDC Emulator in the forest root domain. Each DC in a domain will synchronize its time with the PDC Emulator for its domain. Member servers and workstations in a domain will synchronize their time with the DC that authenticated them, which can be the PDC Emulator for that domain. P87

9. Each object's SID consists of two components: the domain portion and the \_\_\_\_\_\_\_\_.

a. remote identifier

b. globally unique identifier

c. relative identifier

d. global identifier

An object SID is comprised of the security identifier for the Active Directory domain, which will be the same for each security principal created within that domain, and a relative identifier, which will be unique to that security principal. P85

10. You can view and manage the PDC Emulator FSMO role holder using which utility?

a. Active Directory Users and Computers

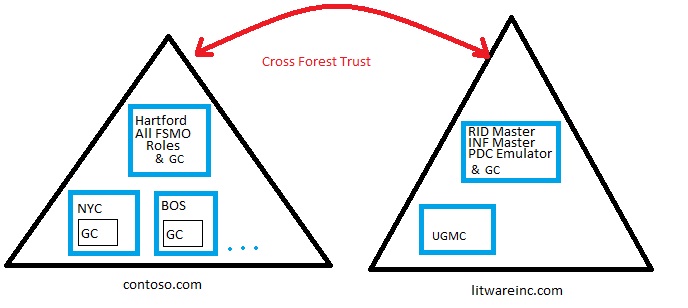
b. Active Directory Schema

c. Active Directory Sites and Services

d. Active Directory Domains and Trusts

To view the PDC Emulator, RID Master, and Infrastructure Master FSMO role holders, right-click the domain name in Active Directory Users and Computers and select the Operations Masters option from the context menu. P92

Case Scenarios



After Scenario 4-1 and 4-2

Scenario 4-1: FSMO Role Placement—I

Contoso Pharmaceuticals has 500 employees in 14 locations. The company headquarters is in Hartford, Connecticut. All locations are part of the contoso.com domain, contain at least two servers, and are connected by reliable links.

a. Which FSMO roles would you house at the Hartford location?

The Schema Master and the Domain Naming Master should be housed at the corporate headquarters, because these domain controllers should be heavily secured. ALL FSMO roles.

b. While trying to add new user accounts to the domain, you receive an error that the accounts cannot be created. You are logged on as a member of the Domain Admins group. What is most likely causing the problem?

The RID Master is likely unavailable.

c. What should you consider placing at each location to facilitate logons?

Place a global catalog server in each location.

Scenario 4-2: FSMO Role Placement—II

Contoso Pharmaceuticals is expanding to include several newly acquired companies. Although they will each become part of the contoso.com forest, each of these companies wants to maintain their own decentralized management strategy. To accommodate this request, you have installed the subsidiaries as separate domain structures. One of them is named litwareinc.com.

a. Which roles will this new domain need to accommodate?

Each domain will need to house a set of domain-wide FSMO roles: the PDC Emulator, the RID Master, and the Infrastructure Master.

b. If litwareinc.com decides to have a small satellite office included in their domain for several users, without having logon traffic using their available bandwidth to the parent domain, what should they do?

Enable universal group membership caching in the remote location.

c. In contoso.com, your server functioning as the Domain Naming Master has failed due to a power surge. You are unable to create a new child domain for a new location until this server is back online. Currently, it is not expected that the Domain Naming Master issue will be resolved in a reasonable amount of time. What steps should you take so that you can resolve this problem and create the necessary child domain?

Seize the Domain Naming Master to another domain controller. Be sure to reformat the existing Domain Naming Master before returning it to your production Active Directory.