Global Catalog & Flexible Single Master Operations (FSMO)
Topics for this Unit

- Functions of the Global Catalog
- Functions of Universal Group Membership Caching
- The Five FSMO roles
- Management of FSMO roles
- Transfer and seizing of FSMO roles
Global Catalog

• Critical component of Active Directory
• Acts as a central repository by holding
  – A complete copy of objects from the host server’s local domain
  – A partial copy of objects from other domains within the same forest
• Used for logon, object searches, and universal group memberships
• By default, the first domain controller installed in the forest root domain is designated as a global catalog server
• Any or all domain controllers in a domain can be designated as global catalog server
Global Catalog

• Where you put the global catalog depends on
  – The speed and reliability of the WAN link
  – The amount of traffic that will be generated by replication
  – The size of the global catalog database
• Active Directory searches are automatically sent to TCP port 3268
• Global catalogs are identified by DNS through SRV records (global catalog, or _gc, service)
Universal Group Membership Caching

- Server 2003 and Windows Server 2008
- Used for sites that do not have a global catalog server available
- Stores universal group memberships on a local domain controller so no global catalog is needed provided
  - The user successfully logged on at some point
  - Universal group caching was turned on
- Enabled on a per-site basis
- By default, cache is refreshed every eight hours
- If caching not available and link down, can’t login
Adding a Global Catalog Server

- Use Active Directory Sites and Services from the Administrative Tools folder
Enabling Univ Group Membership Caching

- Use Active Directory Sites and Services
FSMO Roles

- First domain controller in a new forest holds both of the forest-wide FSMOs and the three domain-wide FSMOs
- Flexible Single Master Operations (FSMO) roles
  - Relative Identifier Master
  - Infrastructure Master
  - Primary Domain Controller (PDC) Emulator
  - Domain Naming Master
  - Schema Master
FSMO Roles

• Relative Identifier (RID) Master
  – One per domain
  – Responsible for assigning relative identifiers to domain controllers in the domain
  – Relative identifiers are variable-length numbers assigned by a domain controller when a new object is created

• Infrastructure Master
  – One per domain
  – Responsible for reference updates to other domains
  – Assists in tracking which domains own which objects
FSMO Roles

• PDC Emulator
  – one per domain
  – Provides backward compatibility with Microsoft Windows NT 4.0 domains and other down-level clients
  – Manages account lockouts
  – Manages time synchronization for the domain
  – Managers password changes and replicates immediately
  – Managing edits to Group Policy Objects (GPO)

• Schema Master
  – One per forest
  – Responsible for managing changes to the Active Directory schema
FSMO Roles

- Domain Naming Master
  - One per forest
  - Has the authority to manage the creation and deletion of domains, domain trees, and application data partitions in the forest
  - When any of these is created, the Domain Naming Master ensures that the name assigned is unique to the forest
MANAGING FSMO ROLES

- Active Directory Users And Computers
  - RID master
  - Infrastructure master
  - PDC emulator

- Active Directory Domains And Trusts—domain naming master

- Microsoft Management Console (MMC) Schema snap-in—schema master

- Repadmin

- NTDSUtil—All roles
Managing FSMO Roles

• Role seizure - Used only when you have experienced a failure of a domain controller that holds a FSMO role and you forced an ungraceful transfer
  – Use the ntdsutil command to access the fmso maintenance prompt and use the seize command

• Role transfer - Used to move a FSMO role gracefully from one domain controller to another
Transferring Schema Master FSMO Role

- Open the Active Directory Schema snap-in
- Right-click Active Directory Schema from the console tree and select Change Operations Master
- Remember that before you can access the Active Directory Schema snap-in, you need to register the schmmgmt.dll DLL file using the following syntax

  regsvr32 schmmgmt.dll
FAILURE

- Schema master – can’t change the schema but has no effect on users
- Domain naming master – can’t add or delete domains
- PDC emulator – users that logon through the PDC emulator will not be able to log on
- RID master – can’t move objects from one domain to another and if all the RIDs are used up you can’t create new objects
- Infrastructure master – the active directory database can become corrupted
Summary

• The global catalog server acts as a central repository for Active Directory by holding
  – Complete copy of all objects within its local domain
  – Copy of all objects from other domains within the same forest

• The global catalog has three main functions
  – Do searches for objects in the forest
  – Resolve UPN names
  – Provide universal group membership information
Summary

• A global catalog should be placed in each site when possible.

• If not possible, universal group membership caching can be enabled for the site to facilitate logon requests.

• Global catalog placement
  – Speed and reliability of the WAN link
  – Amount of traffic that will be generated by replication
  – Size of the global catalog database
Summary

- Operations master roles are assigned to domain controllers to perform single-master operations.
- The Schema Master and Domain Naming Master roles are forest-wide.
  - Every forest must have one and only one of each of these roles.
- The RID Master, PDC Emulator, and Infrastructure Master roles are domain-wide.
  - Every domain must have only one of each of these roles.
Summary

- FSMO roles can be managed in two ways:
  - Role transfer - Transfer a FSMO role to other domain controllers in the domain or forest to
    - balance the load among domain controllers
    - accommodate domain controller maintenance and hardware upgrades
  - Role seizure - Seize a FSMO role assignment when a server holding the role fails and you do not intend to restore it
    - Seizing a FSMO role is a drastic step that should be considered only if the current FSMO role holder will never be available again
Summary

- Use repadmin to check the status of the update sequence numbers (USNs) when seizing the FSMO role from the current role holder
- Use ntdsutil to actually perform a seizure of the FSMO role
Lab 4

- Create a Global Catalog Failure
- Enable Universal Group Membership Caching
- Transfer FSMO Roles