Module 8: Flexible Single Master Operations (FSMO)

Lesson 1: FSMO Roles and Administration

Flexible Single Master Operations

Module 8 Lesson 1

Global Learning Services

Overview

Learn the different roles of an Active Directory® Domain Controller and how to change the properties.

What You Will Learn

After completing this lesson, you will be able to:

- Describe Flexible Single Master Operations (FSMO).
- Describe the responsibilities of the various FSMO roles.
- Identify which FSMO role a domain controller is performing.
- Transfer FSMO roles between domain controllers.
- Troubleshoot FSMO related issues.
- Determine a strategy for placing FSMO role holders.
- Describe how to deal with FSMO failures.

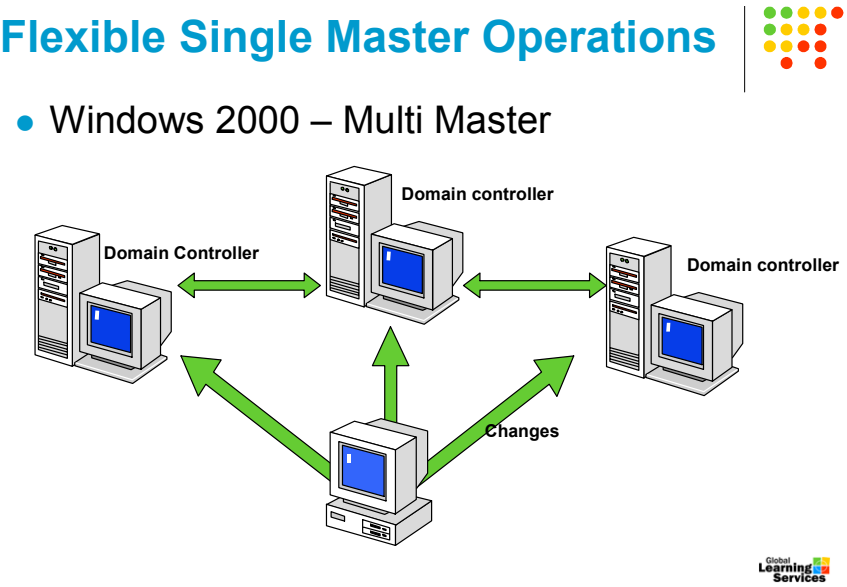
Related Topics Covered in this Lesson

- Designing strategies for placing Domain Controllers.

Recommended Reading

- *Distributed Systems Guide* of the Resource Kit

Flexible Single Master Operations



As noted previously, Active Directory supports multi-master replication. This means that changes can be made at any domain controller in the domain, even if that domain controller is disconnected from the rest of the network. It is possible for multiple users to submit similar changes to the database through different domain controllers resulting in updates that conflict with each other. In spite of the conflicting changes, multi-master replication ensures that all domain controllers will eventually converge to the same value through a process called conflict resolution.

Some conflicts are inappropriate to resolve in a multi-master environment. For example, if different domain controllers have conflicting versions of the directory schema, what happens to directory objects created in the schema that "loses"? In this situation it is a better strategy to prevent conflicts rather than trying to resolve them.

To address this type of problem, Active Directory performs certain types of updates in single-master fashion. Schema updates are an example of one type of single master operation. To avoid conflicting changes to the schema, only one domain controller is allowed to make the changes.

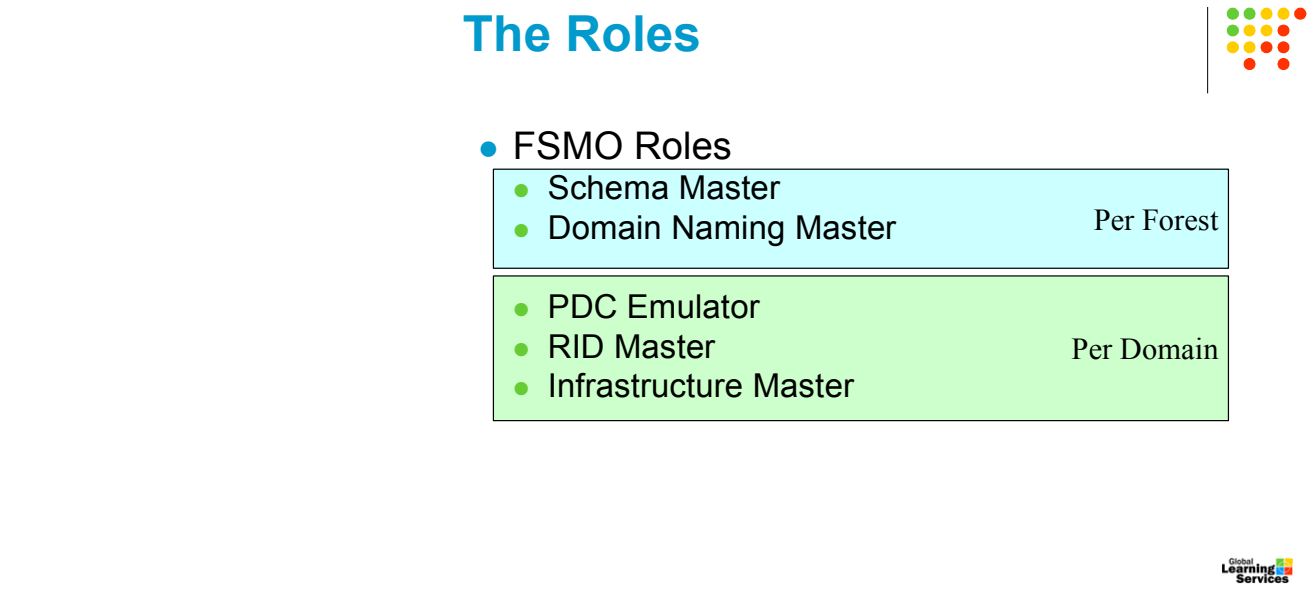
This is an example of flexible single-master operations—FSMO for short. All the changes are made at a single domain controller, referred to as the FSMO, and then replicated to the other domain controllers. The role of FSMO can be held by any single domain controller at one time. It is possible to assign the FSMO role to any domain controller in the domain thus allowing the location of the role to be flexible.

Since an update to the database is performed at the single-master, you may not perform the update if the master is unreachable. Generally, updates to the master are infrequent and not time-critical.

Note:

During the Windows 2000 Beta process, flexible single master operations were known as floating single master operations. In the released version of Active Directory, FSMOs are sometimes known as operations masters.

The Roles



There are five specific types of FSMO roles:

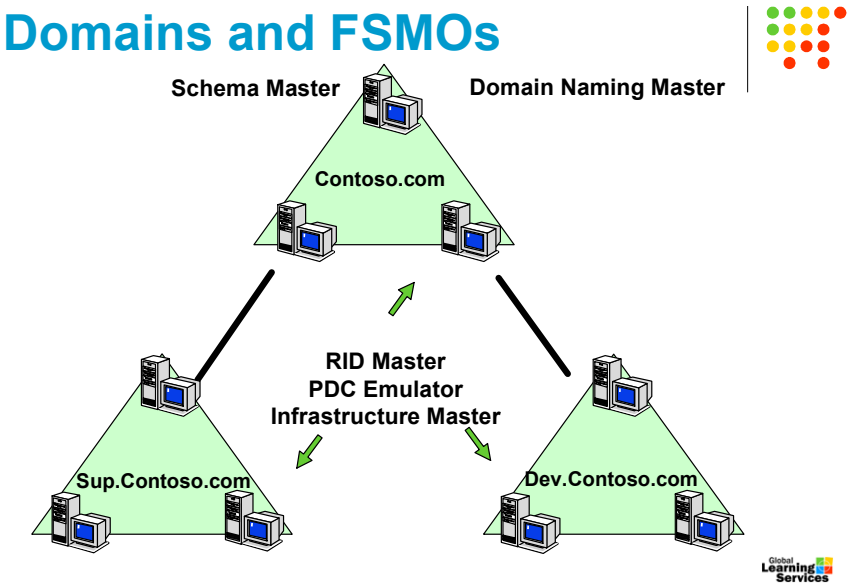
- The Schema Master – Manages all updates made to the schema.
- Domain Naming Master – Controls the addition and removal of domains to and from the directory.
- PDC Emulator – Acts as the Domain Master Browser, manages replication to downlevel domain controllers, and receives preferential password change replication.
- Relative Identifier (RID) Master – Manages the Domain RID allocation pool and moving domain objects.
- Infrastructure Master – Responsible for updating security identifiers (SIDs) and distinguished names (DNs) when objects that contain cross-domain references are moved.

Information is stored in the Active Directory by the creation of various objects. Attributes that define these objects are stored in the schema. The objects that represent the various FSMO roles are no exception. There is a specific object, called the primary role object that is associated with each FSMO role. The primary role object has an attribute, called the FSMO-Role-Owner, which contains a single value that identifies the domain controller that currently is assigned that FSMO role.

Since every domain controller has its own copy of the directory, there is no guarantee that all domain controllers agree on the value of the FSMO-Role-Owner at any one time. Due to latency in replication, it is certain that when the role holder changes, different domain controllers will disagree for a time on who holds the role. This is not really a problem because as replication cycles complete, the systems will eventually all agree. To avoid problems, the following conditions must be met:

- Two domain controllers must not assume a role at the same time.
- A domain controller that assumes a role must contain an up to date replica of the role object set.

Domains and FSMOs



Consider a directory with three domains:

- contoso.com
- sup.contoso.com
- dev.contoso.com

The total number of FSMO roles in a tree that contains three domains is 11: a schema master for the directory (1), a domain naming master for the directory (1), a RID master for each domain (3), a primary domain controller (PDC) emulator for each domain (3), and an infrastructure master for each domain (3).

A single domain controller can hold up to five FSMO roles, one of each. So it is possible to distribute the roles listed above among as few as three domain controllers or as many as eleven.

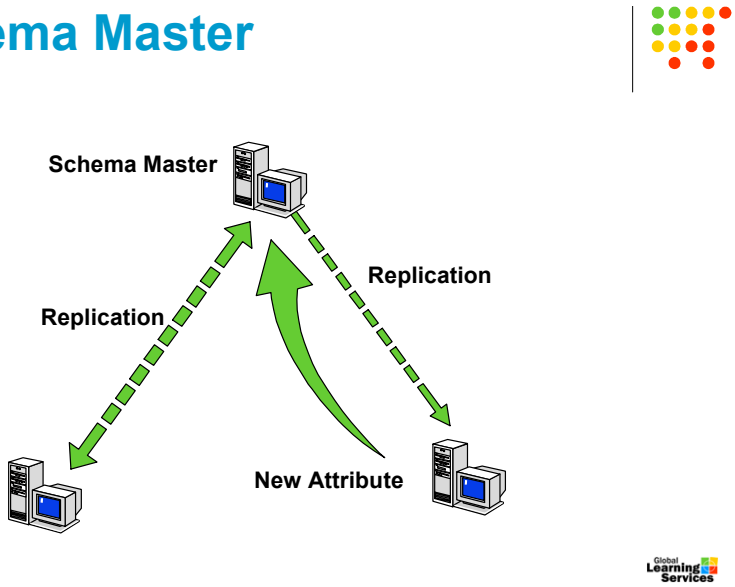
When the first Active Directory® domain controller is created, the system assigns all five roles to it. When the first Active Directory domain controller of an additional domain is created, the system assigns all three domain roles to it.

Only Active Directory domain controllers can hold FSMO roles.

There are administration tools that allow the viewing and transfer of these roles:

- Domains and Trusts Manager – Domain Naming FSMO
- Schema Manager – Schema FSMO
- Active Directory Users and Computers – PDC emulator, RID and Infrastructure master FSMO
- NTDSUtil.exe – All roles

Schema Master



To avoid conflicting changes being made to the schema by multiple domain controllers, all changes are managed by the domain controller filling the role of Schema Master. The schema contains the master list of the attributes used to define the entire directory. Since there is a single schema, there is one schema master per directory. This includes directories that consist of a single tree and directories that contain an entire forest.

Only the schema master can perform updates to the schema. Schema updates then replicate from the schema master to all other domain controllers for the directory.

The FSMO Schema-Master can be chosen in the Schema Management console by selecting Operations Master from the Active Directory Schema Manager. From this location, the present domain controller can be made a schema writable domain controller. This operation requires that the domain controller under focus by this tool is not currently the Schema Master FSMO.

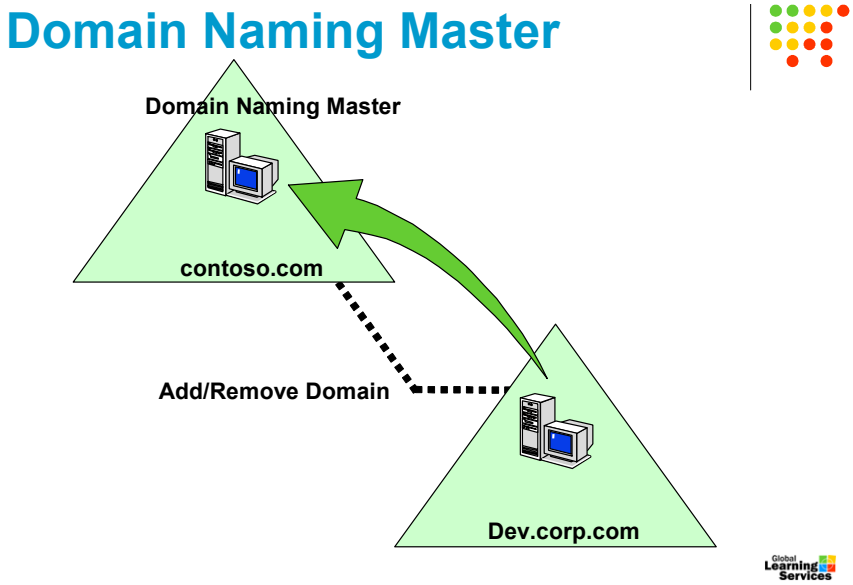
In Microsoft® Windows® 2000, the Schema Master computer should also have the following registry value set:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\
Schema Update Allowed

REG_DWORD 1

This key is not required on Microsoft® Windows Server™ 2003.

Domain Naming Master



When a new domain is added to the directory, the Partitions container of the Configuration naming context is modified to reflect the new addition. This process is managed by a single domain controller role, the domain naming master.

The domain controller that has the domain naming master role is the only domain controller that can do the following:

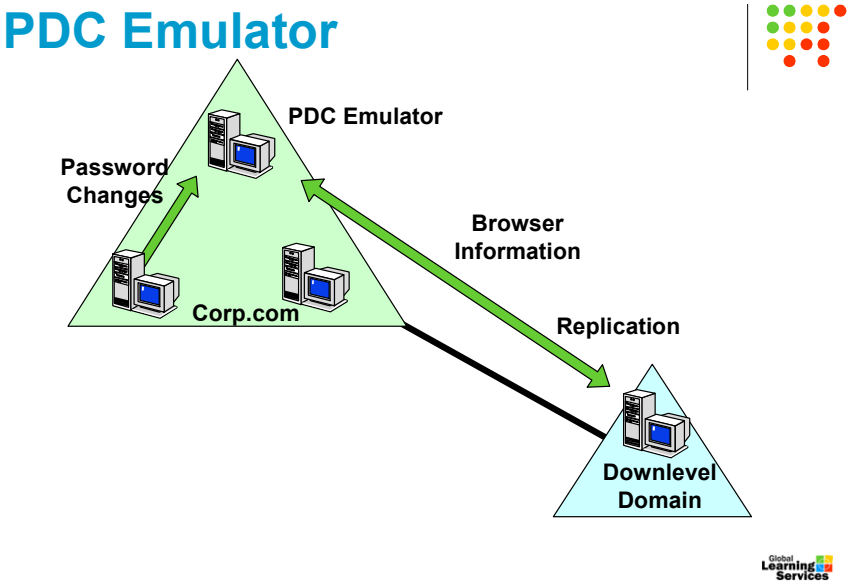
- Add new domains or application directory partitions to the forest.
- Remove existing domains or application directory partitions from the forest.
- Add or remove cross-reference objects to or from external directories.

There is one domain naming master per forest. Certain components of Active Directory, such as domain names, must be unique within the forest. The domain naming master achieves this by querying the Global Catalog server, which contains a partial replica of every object in the forest.

In Windows 2000, the domain naming master must be placed on the same server as a Global Catalog. When the domain naming master creates an object representing a new domain, it ensures that no other object—domain object or otherwise—has the same name.

If the domain naming master is placed on a Windows Server 2003 domain controller, there is no requirement for that domain controller to be a Global Catalog server. In Windows Server 2003, the domain naming master is capable of querying a remote Global Catalog server when needed.

PDC Emulator



The PDC emulator FSMO role holder is an Active Directory domain controller that advertises itself as the PDC to pre-Windows 2000 workstations, member servers, and domain controllers. For pre-Windows 2000 workstations requiring directory writes (such as password changes), only the PDC emulator can service such requests. Backup domain controllers (BDCs) running pre-Windows 2000 operating systems (such as Microsoft® Windows NT® 3.51 or Windows NT® 4.0) will synchronise changes from the PDC emulator. In networks running the Windows NT Browser service, the PDC emulator plays the role of domain master browser. In addition, any NetBIOS program that issues a NetGetDCName() API call must talk to the PDC emulator.

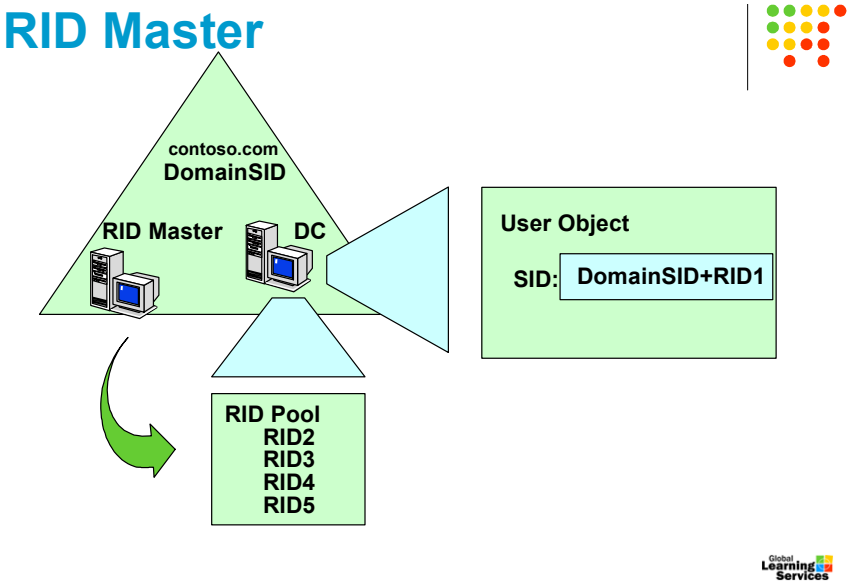
In an Active Directory domain, the PDC emulator role holder retains the following functions even when there are no pre-Windows 2000 clients:

- Password changes performed by domain controllers are replicated preferentially to the PDC emulator.
- Authentication failures that occur at a given domain controller in a domain because of an incorrect password are forwarded to the PDC emulator before a bad password failure message is reported to the user.
- Account lockouts are urgently replicated to the PDC emulator.
- Any changes to the domain-based Distributed File System must be made by connecting to the PDC emulator.
- Changes to the Group Policy will be directed to the PDC emulator in preference to other domain controllers.
- The time synchronisation service uses PDC emulators to synchronize clocks between members of the forest.
- The SD Propagator process (SDProp) runs on the PDC emulator to implement the protection of administrative groups.
- Active Directory administrative tools (Active Directory Domains and Trusts and Active Directory Users and Computers) automatically target the PDC emulator when raising the domain functional level.

Windows 2000 and later clients and pre-Windows 2000 clients that have the Active Directory client package can utilise any domain controller that hosts an appropriate naming context for directory writes. Other clients must use the PDC emulator for directory writes. Once all the domain controllers in a domain are running Active Directory and the domain has been upgraded to Windows 2000 functional level (previously native mode) the PDC can no longer receive replication requests from down-level domain controllers.

There is one PDC emulator per domain in the directory. So, in a directory containing three domains, there are three PDC emulators (one in each domain).

RID Master



RID

Every security principal object in the directory has an associated SID. This is a unique identifier that the system uses to recognize the object for authorization purposes. When a security principal (such as a user or group) is created and a SID is added as an attribute of it.

The SID is a single identifier that consists of two pieces of information. The first piece of information is the Domain SID (the SID that identifies the domain). This is combined with a Relative ID (RID) that is supplied by the domain controller that creates the object. Since all objects in the domain use the domain SID as part of their own identifier, the RID must be unique for each object. In a multi-master environment it is possible for any domain controller to create an object so some means of centrally managing the RID allocation is needed.

RID Master

The RID master performs two functions:

- The RID master maintains a domain wide “pool” of RIDs and allocates them on an “as needed” basis to each domain controller. Each domain controller in a domain has a pool of RIDs it assigns to objects it creates. When the number of unused RIDs in a domain controller’s RID pool falls below a threshold (80 percent), the domain controller will request an additional 500 RIDs from the domain's RID master. The domain's RID master then removes RIDs from the domain's RID pool and assigns them to the pool on the domain controller making the request.
- Objects can be moved from one domain to another with tools such as Movetree and ADMT. When an object moves between domains, its distinguished name (DN) changes and its security ID (SID) changes but its unique ID (Object-GUID) remains the same.
  Only the RID master of a domain will be able to move an object out of its domain. This prevents Active Directory from creating two objects in different domains having the same unique ID, as would happen if an object were moved to two places from two different domain controllers at about the same time.

There is one RID master per domain in a directory. So, in a forest containing three domains, there are three RID masters, one in each domain.

Note:

The RID master is not really maintaining a pool of numbers. It maintains the highest value of the last range it allocated. When a new request is received, it increments that value by one to establish the low value in the new RID pool and then adds 499 to establish the new maximum value. It sends these two values to the requesting domain controller to use as its next allocation of RIDs.

RID Attributes in Active Directory

Attribute Name	DN Path	Description
FsmoRoleOwner	CN=RID Manager$, CN=System, DC=<domain>, DC=com	Points to Domain Name path of the current RID masters NTDS Settings object according to domain controller that is being queried.
RidAvailablePool	CN=RID Manager$, CN=System, DC=<domain>, DC=com	Global RID space for an entire domain is defined in as a large integer with upper and lower parts. The upper part defines the number of security principals that can be allocated per domain (0x3FFFFFFF or just over 1 billion). The lower part is the represents the beginning of next RID pool to be allocated in the domain known as *RidMaster FreeSpace*. To view both parts, use the Large Integer Converter command in the Utilities menu in Ldp.exe.
RidAllocationPool	CN=Rid Set, Cn=<computername> ,ou=domain controllers, DC=<domain>, DC=COM	Each domain controller has two pools: the one that they are currently acting on, and the pool that they will use next. It is the next pool, which is allocated by the RID FSMO, which will be used for creation of security principals in the domain when the current pool is exhausted. This attribute stores the first and last RID in the current pool known as the *Starting RID* and *Ending RID* respectively. To view both parts, use the Large Integer Converter command in the Utilities menu in Ldp.exe.

Attribute Name	DN Path	Description
RidNextRid	CN=Rid Set, Cn=<computername>, ou=domain controllers, DC=<domain>, DC=COM	The RID that is assigned to next security principal that is created on the local domain controller. RidNextRid is a non-replicated value in Active Directory.
RidPreviousAllocationPool	CN=Rid Set, Cn=<computername>, ou=domain controllers, DC=<domain>, DC=COM	The pool from which RIDs are currently taken. The value for RidNextRid is implicitly a member of this pool. Use the Large Integer Converter command in the Utilities menu in Ldp.exe to view the beginning and ending RIDS in the current pool. RidPreviousAllocationPools is a non-replicated value in Active Directory.
RidUsedPool	CN=Rid Set, Cn=<computername>, ou=domain controllers, DC=<domain>, DC=COM	Unused attribute
NextRid	DC=<domain>, DC=COM	Unused attribute

RID Master

RID Master

- Duplicate RIDs
  - System State restore
  - RID Master seizure
- Safeguards
  - Initial “successful” replication
  - Urgent replication of RID Pool
  - Invalidation of overlapping RID Pool
  - Duplicate SID detection

If the domain has multiple RID pool role owners, there is a potential issue that objects with duplicate SIDs could be created. The most common contributor to duplicate SIDs is a System State restore on the RID Master FSMO. Replication problems between other domain controllers in the domain after the restore of the RID FSMO may also contribute to the problem.

An additional situation that has been identified as a possible cause of allocation of duplicate relative identifier pools is if the relative ID master role has been seized while the original relative ID master is still operational but has been temporarily disconnected from the network. In normal practice, after one replication cycle, the relative ID master role is assumed by one and only one domain controller, but it might be possible that before the role ownership is resolved, two different domain controllers each request a new relative ID pool and they may well be allocated the same RID pool.

The following symptoms may be encountered when duplicate RIDS exist in an Active Directory domain:

- User and computer accounts with duplicate SIDS cannot logon.
- Users, computers and groups are deleted from Active Directory when accessed by the user, computer or administrator.
- When viewing, modifying or deleting a user or computer account with a duplicate SID in the "Active Directory Users and Computers" snap-in, the following error message appears:

  ```
  The specified user does not exist.
  ```

- When accounts with duplicate SIDS are accessed by the operating system , "Event Viewer" reports the following error in the Directory Service node :

  ```
  Event 12293: There are two or more objects that
  have the same SID attribute in the SAM database
  ```

- Replication to Windows NT 4.0 domain controllers may stop.

To prevent problems and FSMO-related conflicts due to duplicate role holders or stale state, Windows 2000 DCs with post-SP2 versions of NTDSA.DLL and all Windows Server 2003 DCs perform an initial synchronization on the NC associated with that FSMO role before advertising that FSMO role in the Directory. (Initial synchronization is the attempt a domain controller makes to source its NCs when first booted.)

For example, the domain controller holding the RID FSMO role would have to replicate the Domain NC before advertising and issuing new RID pools. (An enterprise-wide FSMO whose DN path was located in the configuration NC would have to replicate that partition before advertising.)

This safeguard is an effort to detect if a conflicting FSMO has been restored or brought up while the current FSMO is down. In pre-SP3 Windows 2000 domain controllers, successful replication of the host NC was not a requirement. For this reason, conflicting operations could occur, such as duplicate RID pools being handed out or the RID FSMO being seized while the old RID FSMO was not able to replicate in the change of FSMO role. In Windows Server 2003, the requirement of at least one “successful” synchronization was added to prevent this scenario.

The following additional checks are done to minimize the possibility of having duplicate RID pool role owners.

- The global RID (available) pool state is replicated urgently to maximize chances that candidates for the new RID FSMO are up-to-date.
- If the RID master allocates a RID pool to a domain controller that overlaps with the RID pool of another domain controller, the domain controller whose pool overlaps with the new pool notices this when this information replicates to it, and then proceeds by invalidating its current pool and requesting a new RID pool. This prevents the domain controller from issuing further duplicates and quickly "moves" all domain controllers that have overlapping pools to acquire fresh pools that do not overlap.
- The operating system contains checks to detect and handle instances of duplicate RIDs.

If duplicate RIDS are suspected of existing on a domain, the following procedure can be used to help determine the cause of the problem.

Inventory all domain controllers in the restored domain and record the following values for each domain controller:

- RID FSMO
- FsmoRoleOwner Attribute
- RIDNextRID
- Rid AllocationPool
- Start RID
- End RID
- RidMaster FreeSpace is a derived value from the Rid Emulator that represents the beginning of next RID pool to be allocated in the domain. The value for "RidMaster FreeSpace" should be higher than the RID values for all other security principals in the domain.

Use the inventory list to verify the following:

- No RID pools overlap each other.
- No RID pools overlap the "RidMasterFreeSpace" of the RID FSMO owner.
- The value for "RidMasterFreeSpace" on the RID FSMO is greater than any SID allocated to users, computers or groups in the domain.

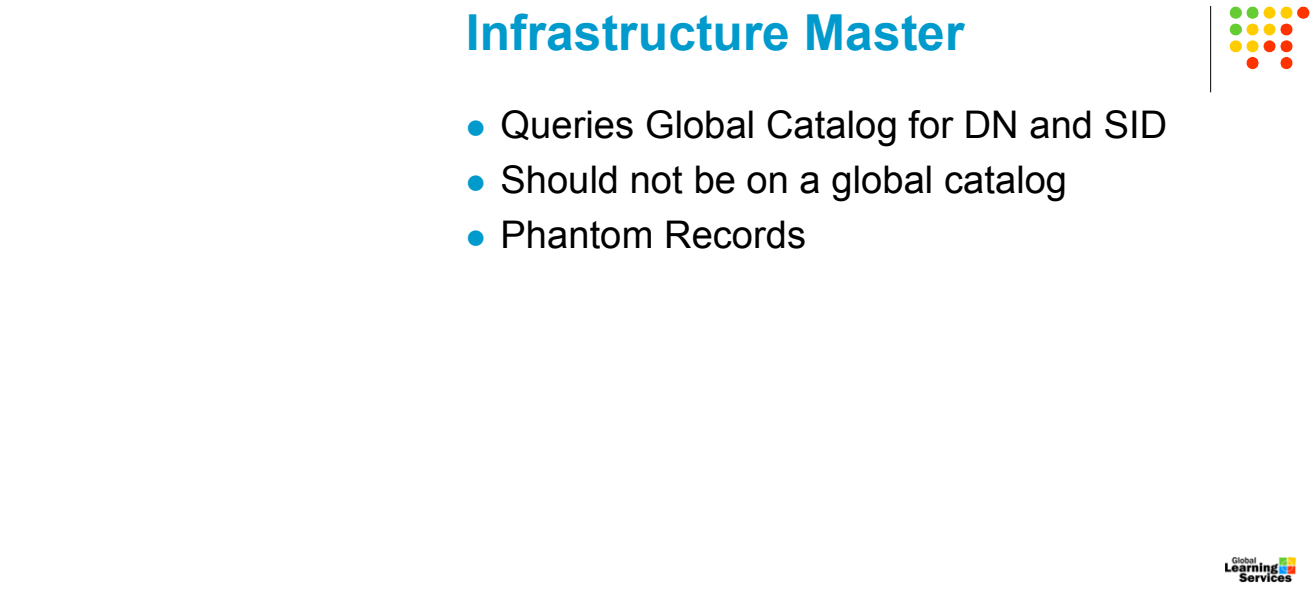
If the value for "RidMasterFreeSpace" value is found to be lower than any RID present in the domain, increase this value to one number higher than the highest RID in the domain. If one RID pool overlaps another RID pool or

“RidMasterFreeSpace," it must be invalidated. There is no background task to detect duplicate SIDS in Active Directory. However, once a search operation, such as logon authentication or an administrative task on an object with a duplicate SID occurs, event 12293 is recorded in the Directory Services event log and, clean up efforts are attempted. To resolve these issues, see the article referenced below.

For more information, see the following Knowledge Base article: 305477 “How to recognize and recover from duplicate SIDS on Windows 2000 and Server 2003 domain controllers.”

The Ntdsutil tool contains an option, Security account management, to detect and clean all instances of duplicate SIDs. Accounts with duplicate SIDs can be deleted.

Infrastructure Master



When an object on one domain controller references an object that is not on that domain controller, it represents that reference as a record containing the GUID, the SID (for references to security principals), and the distinguished name of the object being referenced. If the referenced object moves, its GUID does not change, its SID changes if the move is cross-domain, and its distinguished name always changes.

The infrastructure master for a domain periodically examines the references, within its replica of the directory data, to objects not held on that domain controller. It queries a Global Catalog server for current information about the distinguished name and SID of each referenced object. If this information has changed, the infrastructure master makes the change in its local replica and also replicates the new values to other domain controllers within the domain.

If the infrastructure master and Global Catalog are the same system, then the infrastructure master will not function (and it will post events in event viewer hourly stating so). If the infrastructure master and Global Catalog and are on the same computer, the computer will never update any references because it does not contain any references to objects that it does not hold. That is because a Global Catalog server holds a partial replica of every object in the forest. If all of the domain controllers in a domain are Global Catalog servers, it does not matter what domain controller holds the infrastructure master role.

There is one infrastructure master per domain in a directory. So, in a directory containing three domains, there are three infrastructure masters, one in each domain.

Phantom Records

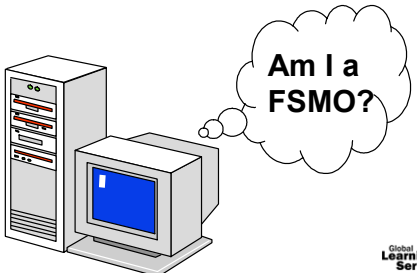
In Active Directory, all references from one object to another are stored as the database identifier of the referenced object. For example, a user object might have an attribute that defines that user's manager; the value for that attribute is the database identifier of the user object that represents the manager in the database. If the referenced object does not exist (for example, a user account in one domain has a manager in a different domain, and the contacted server is not a Global Catalog), a "phantom" is created as a record in the database, and the database identifier of that record is used. A phantom record contains the GUID, the SID (in the case of references to security principals), and the distinguished name of the object that is being referenced. If a copy of the object named in the attribute exists in the local database, no phantom is needed. If the object is located in an external directory partition, the local database uses a phantom

record. For example, if an object in the domain dc=c1,dc=contoso,dc=com holds a reference to an object in dc=c2,dc=contoso,dc=com, a phantom for that object and its parent exist in the domain dc=c1,dc=contoso,dc=com. The infrastructure master deletes phantom objects when the objects that they reference are renamed or deleted.

Default Roles

Default Roles

1. Check the directory for FSMO Role
2. Wait for one *successful* inbound replication cycle
3. Verify that FSMO data is correct
4. Assume Role



Default Roles

Setup

When the first domain controller in the forest is created it will assume all five roles. These defaults will be appropriate in a single domain environment only. The infrastructure master must not be on a global catalog if new domains are added to the forest, and the administrator must take steps to ensure that this is not the case. The first domain controller in subsequent domains will be assigned the three per domain roles for that domain.

After Boot

When a domain controller is booted it looks inside its own copy of the directory to see if it is the current holder of any of the FSMO roles. If the domain controller finds information indicating that it holds one of the FSMO roles, it will not act on that information immediately. The domain controller will first wait for one *successful* inbound replication of information on the configuration of domain naming contexts to make sure that its FSMO role information is the most up-to-date. If the replicated information indicates that the role is currently held by another domain controller, then it will not assume the role itself.

Operational Attributes

Operational attributes is an attribute that is used only for administering the directory database. It is an artefact attribute that is never defined in the schema and does not require any storage. When the attribute is read, generally the result is a calculated result from the server. When the attribute is written, a predefined action occurs on the domain controller.

The following operational attributes are used to transfer FSMO roles and are located on the RootDSE (or Root DSA Specific Entry, the root of the Active Directory tree for a given domain controller where specific information about the domain controller is kept). In the operation of writing to the appropriate operational attribute on the domain controller to receive the FSMO role, the old domain controller is demoted and the new domain controller is promoted automatically. No manual intervention is required. However, it is best practice to move the FSMO before demotion. The operational attributes that represent the FSMO roles are:

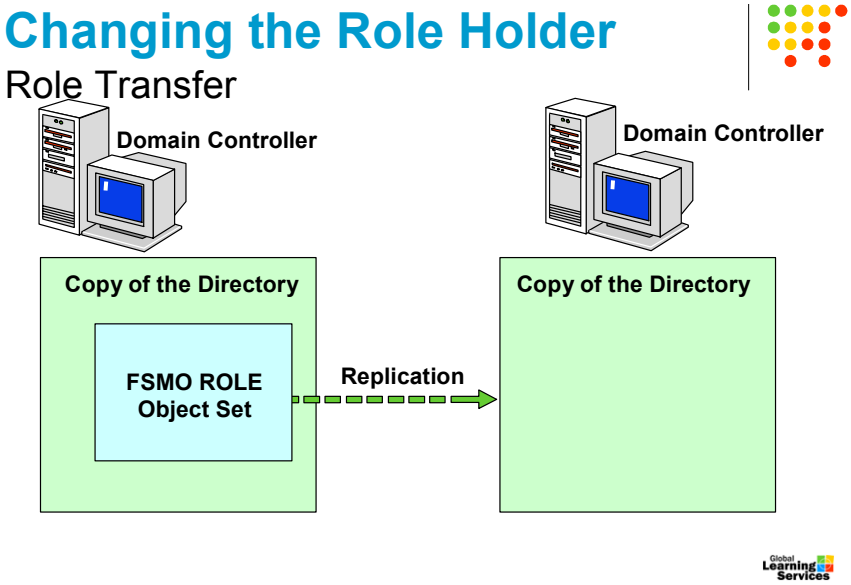
- becomeRidMaster
- becomeSchemaMaster

- becomeDomainMaster
- becomePDC
- becomeInfrastructureMaster

If the administrator specifies the server to receive the FSMO role using a tool such as Ntdsutil, the exchange of the FSMO role is defined between the current owner and the domain controller specified by the administrator.

In all transfers, if the role is a domain-specific role, the role can be moved only to another domain controller in the same domain. Otherwise, any domain controller in the enterprise is a candidate.

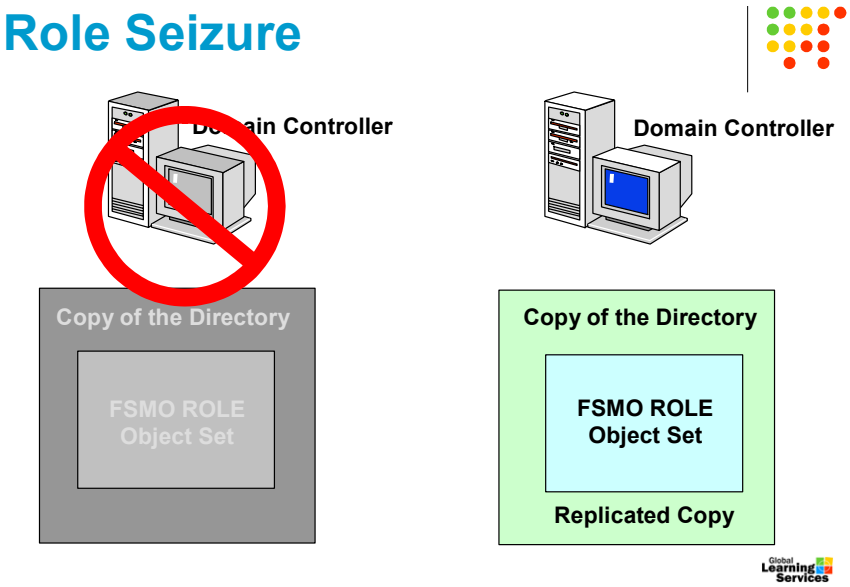
Changing the Role Holder



Role transfer is the controlled movement of the FSMO role from one domain controller to another. To complete a role transfer, both domain controllers must be connected to the network and functioning normally.

All the FSMO data is contained in the directory inside various role objects that make up the role object set. The process of role transfer involves the current FSMO replicating the role object set to the new domain controller. This ensures that the new FSMO will begin its operation with the most current information available. This process uses the normal directory replication mechanism. If there is no updated information to replicate (meaning the new domain controller already has updates received during previous replication cycles) then the replication will not take place. Even if the role transfer fails after the current FSMO has performed its update, normal replication will complete the transfer eventually. Generally, the process can be completed faster by retrying the role transfer than waiting for the replication cycle.

Role Seizure



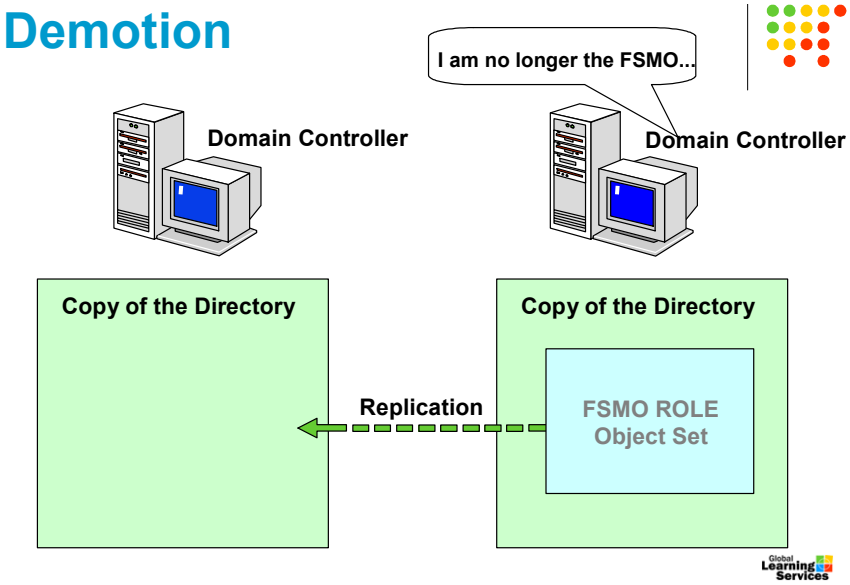
If for some reason a FSMO role holder becomes unavailable, it may become necessary to seize the FSMO role and reassign it to another system.

There can be some hidden problems involved in this process so it is best to be sure that the existing FSMO is unavailable for an extended amount of time. The impact of a missing FSMO will depend on a number of factors. If the system involved will only be down for a few hours, then it may not be necessary to reassign the FSMO duties to another domain controller.

The current FSMO role holder is not involved in role seizure. Therefore, a domain controller performing role seizure should ideally have an up-to-date replica of the role object set. This could be checked using a tool such as Replmon. If it assumes the FSMO role based on an older version of the role object set, then some data could be lost. An example of this would be attributes that have been added to the schema. If the object set that records the creation of the new attributes is lost before they have been replicated, then there will be no record of them in the directory, and the new schema FSMO will have no way of knowing that they are supposed to exist.

When attempting to seize a role with NTDSUTIL, it will always attempt to transfer the role before seizing it.

Demotion



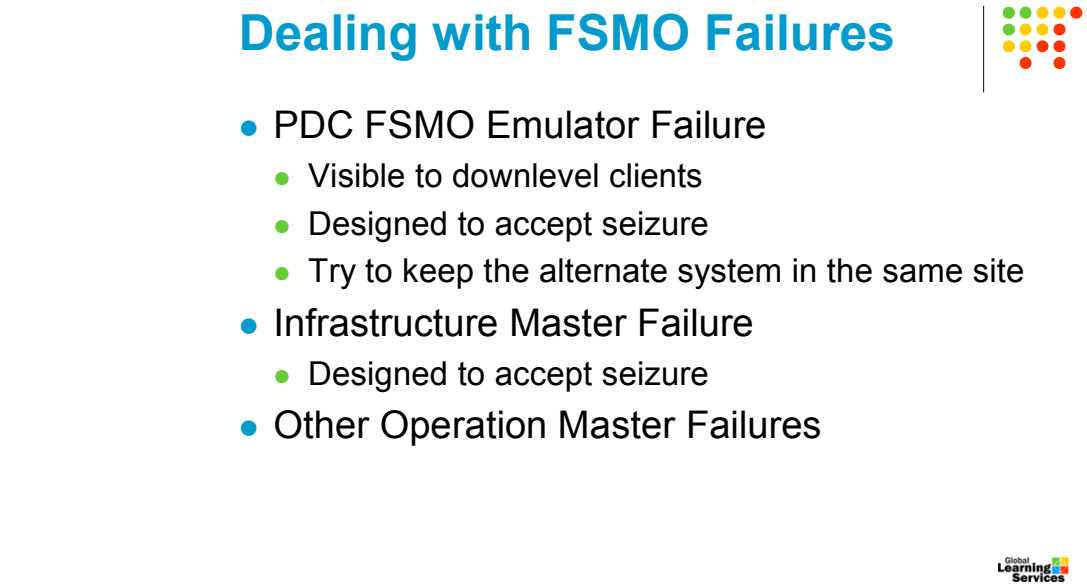
It is possible to instruct a FSMO role holder to voluntarily give up its role. This occurs when DCPROMO is run against a domain controller that holds a FSMO role. When a domain controller that is a FSMO goes through demotion, it will attempt to reassign its roles to other domain controllers in the domain. DCPROMO fails during demotion if it cannot successfully transfer the FSMO roles it holds to an appropriate domain controller.

When a domain controller is demoted, the operational attribute "GiveAwayAllFsmoRoles" is written, which triggers the domain controller to locate other domain controllers to offload any roles it currently owns. Active Directory determines which roles the domain controller being demoted currently owns and locates a suitable domain controller by following these rules:

1. Locate a server in the same site.
2. Locate a server to which there is RPC connectivity.
3. Use a server over an asynchronous transport (such as SMTP).

The preferred method to move roles from a domain controller that is to be demoted is to transfer them before running the Active Directory Installation Wizard so that the best domain controller for that role is chosen.

Dealing with FSMO Failures



Responding to PDC Emulator Failure

If the PDC emulator fails, it may require a fast response to keep the domain functioning at the client level. Down-level clients (computers that are not Windows 2000 or later or have not installed the Active Directory client package) will be affected by the failure of the PDC emulator. Problems will include the inability to change domain passwords and the loss of browser information pertaining to domain resources.

Because failure could have an immediate effect on the network, and this system may need to be brought back on line quickly, the PDC emulator role has been designed to facilitate seizure better than other roles without severe side effects. In case of a failure, use the alternate system (that was identified in planning) to seize the PDC emulator role. When the original PDC emulator domain controller comes back up, an administrator may decide to transfer the role back, although this is not mandatory or automatic.

In an environment that includes backup domain controllers in mixed-mode domains, it is recommended that the alternate PDC emulator (the system that will assume the role in case of failure) be located in the same site.

Responding to Infrastructure Master Failure

Like the PDC emulator, the infrastructure master has also been designed to handle role seizure gracefully. This means that in case of an extended failure, perform the role seizure. When the system is restored, transfer the role back again. Temporary loss of a domain's infrastructure master is not visible to end users, and is not visible to administrators unless a large number of accounts have recently been moved or renamed.

When administrators rename or move a member of a group (and that member resides in a different domain from the group), the group may temporarily appear not to contain that member (the SID will appear instead). The infrastructure master of the group's domain is responsible for updating the group so it knows the new name or location of the member.

There is no compromise to security during the time between the member rename and the group update. Only an administrator looking at that particular group membership would notice the temporary inconsistency.

Other Operations Master Failures

Temporary loss of the schema master, domain naming master, or RID master is ordinarily not visible to end users, but may inhibit the work of an administrator. Therefore, this problem needs to be addressed depending on differing factors.

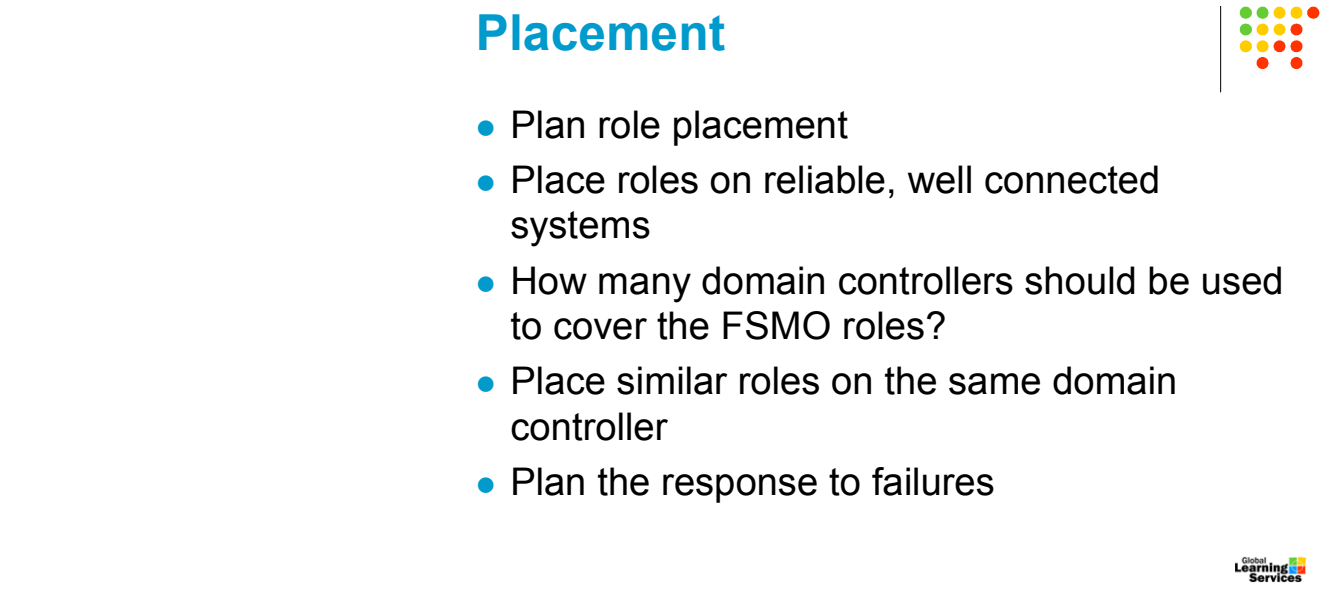
If an extremely long outage of the domain controller holding one of these roles is expected, that role could be seized to another domain controller. But, seizing any of these roles is a *drastic* step; one that should only be taken when the outage is permanent, as in the case when a domain controller is physically destroyed and cannot be restored from backup media.

A domain controller whose schema master, domain naming master, or RID master role is seized must *never* come back online. Before proceeding with the role seizure, ensure that the outage of this domain controller is permanent by physically disconnecting the domain controller from the network.

The domain controller that seizes the role should be fully up-to-date with respect to updates performed on the previous role owner. Because of replication latency, it is possible that the domain controller might not be up-to-date.

To check the status of updates for a domain controller, use the Repadmin command-line tool or Replmon.

Placement



Plan role placement – Active Directory performs an initial placement of roles on domain controllers during the setup of the domain. This placement generally works for domains with smaller numbers of domain controllers. However, the default configuration may not be optimal if the domains have large numbers of domain controllers.

Place all roles on Domain Controllers with reliable network connections – Poor network connectivity can cause problems with updates to the FSMO role objects, and interfere with administrative functions such as account creation.

How many domain controllers should be used to cover the FSMO roles? – One role-holding domain controller per domain is required although there may be reasons to have more than one:

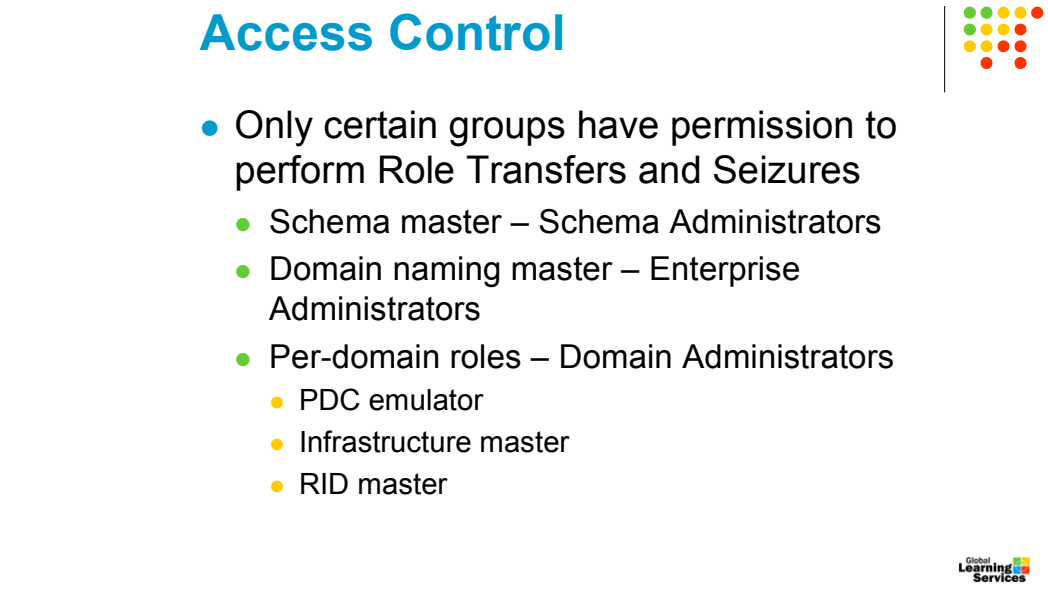
- If the preferred domain controller to hold the RID master and PDC emulator roles is also a Global Catalog server, it will not be able to host an infrastructure master (to prevent a conflict between the Global Catalog and infrastructure master).
- Large domains may require a dedicated domain controller to hold the PDC emulator role but no other roles (to prevent overworking the PDC).

Place similar roles on the same domain controller – Place the schema master and domain naming master roles on the same domain controller. The schema master and domain naming master roles have similar requirements:

- They are both directory-wide.
- They are both rarely used.
- They should both be tightly controlled by the organisation with overall responsibility for your directory implementation.

Plan the response to failures – Identify candidate role-holding domain controller in the same domain (and preferably the same site) for each role-holding DC to assume roles in case the role-holding domain controller suffers a lengthy failure. Create operational procedures for moving FSMOs in the event of failure. To keep data between the role holder and its potential failover partner, create manual connection objects between them as the KCC may remove automatically created ones. These operations procedures should include a disaster recovery plan containing the steps that operators need to take when a failure occurs. This plan might include—but is not limited to—details on how FSMOs will be monitored, backup procedures, and preset recovery scripts.

Access Control



During setup, the default configuration of the Active Directory sets default access permissions on the various role object sets. This governs who is allowed to perform role transfers and role seizures. The groups that have access by default are:

- Schema Administrators – Schema master
- Enterprise Administrators – Domain naming master
- Domain Administrators – Per-domain roles

Managing directory-wide functions such as role transfers and role seizures on schema and domain naming masters should be limited to a very small group. The default groups with permissions to perform these functions are the Schema Administrators and Enterprise Administrators respectively. Membership in these groups should be limited.

Managing domain-wide functions such as role transfers and role seizures on PDC emulators, infrastructure masters, and RID masters are other processes that should be monitored. By default, the Domain Administrators group has permissions to reassign these roles, so its membership should be limited.

FSMO Administration

FSMO Administration

- NTDSUTIL.EXE
  - Console application for FSMO administration
- Managed from MMC tools
  - Role Management
    - Users & Computers Manager
    - Schema Manager
    - Domains & Trusts
  - ADSI Edit
    - Set access permissions

Global Learning Services

NTDSUTIL.EXE allows administrators to perform role transfers, role seizures, list the current FSMO role holders, and a variety of other functions.

```
C:\>ntdsutil
ntdsutil: ?
 ?                              - Print this help information
 Authoritative Restore          - Authoritatively restore the DIT
Database
 Configurable Settings          - Manage configurable settings
 Domain Management              - Prepare for new domain creation
 Files                          - Manage NTDS database files
 Help                           - Print this help information
 LDAP policies                  - Manage LDAP protocol policies
 Metadata cleanup               - Clean up objects of decommissioned
servers
 Popups %s                      - (en/dis)able popups with "on" or "off"
 Quit                           - Quit the utility
 Roles                          - Manage NTDS role owner tokens
 Security account management    - Manage Security Account Database
 Semantic database analysis     - Semantic Checker
 Set DSRM Password              - Reset Directory Services Restore
administator account Password

ntdsutil: roles
fsmo maintenance: ?
 ?                              - Print this help information
 Connections                    - Connect to a specific domain controller
 Help                           - Print this help information
 Quit                           - Return to the prior menu
 Seize domain naming master     - Overwrite domain role on connected
server
 Seize infrastructure master    - Overwrite infrastructure role on
connected server
 Seize PDC                      - Overwrite PDC role on connected server
 Seize RID master               - Overwrite RID role on connected server
 Seize schema master            - Overwrite schema role on connected
server
 Select operation target        - Select sites, servers, domains, roles
and naming contexts
 Transfer domain naming master - Make connected server the domain
naming               master
 Transfer infrastructure master- Make connected server the
infrastructure master
 Transfer PDC                   - Make connected server the PDC
 Transfer RID master            - Make connected server the RID master
 Transfer schema master         - Make connected server the schema master
```

```
fsmo maintenance: connections
server connections: ?
 ?                              - Print this help information
 Clear creds                    - Clear prior connection credentials
 Connect to domain %s           - Connect to DNS domain name
 Connect to server %s           - Connect to server, DNS name or IP
address
 Help                           - Print this help information
 Info                           - Show connection information
 Quit                           - Return to the prior menu
 Set creds %s %s %s             - Set connection creds as domain, user,
pwd
                                Use "NULL" for null password

server connections: connect to server rootdns
Binding to rootdns ...
Connected to server01 using credentials of locally logged on user
server connections: quit
```

```
fsmo maintenance: transfer pdc
Server "rootdns" knows about 4 roles
Schema - CN=NTDS Settings,CN= rootdns,CN=Servers,
 CN=East,CN=Sites,CN=Configuration,
 ,DC=contoso,DC=com
Domain - CN=NTDS Settings,CN= rootdns,CN=Servers,
 CN=East,CN=Sites,CN=Configuration,
 DC=contoso,DC=com
PDC - CN=NTDS Settings,CN= rootdns,CN=Servers,
 CN=East,CN=Sites,CN=Configuration,
 DC=contoso,DC=com
RID - CN=NTDS Settings,CN=rootdns,CN=Servers,
 CN=East,CN=Sites,CN=Configuration,
 DC=contoso,DC=com
fsmo maintenance: quit
ntdsutil: quit
Disconnecting from rootdns ...
C:\>
```

Role Management

FSMO role transfers can be performed via the Microsoft Management Console (MMC)-based tools that are used for other directory administration by context clicking on the appropriate object within the interface and selecting the operations master choice from the available menu.

ADSI Edit

Using ADSI Edit, permissions can be set on any FSMO primary role object. These are the DNs of the FSMO primary role objects:

- Schema master
  CN=Schema, CN=Configuration, dc=<domain> (i.e., root of Schema NC)
- Domain naming master
  CN=Partitions, CN=Configuration, dc=<domain> (below root of Configuration NC)
- RID master
  CN=RID Manager$, CN=System, dc=<domain>
- PDC emulator
  dc=<domain> (i.e., root of domain NC)
- Infrastructure master
  CN=Infrastructure, dc=<domain>

Dumpfsmos

Dumpfmsos,cmd

This command-line tool dumps the FSMO roles for a domain. Using DumpFsmos, you can find the names of the domain controllers that are performing forest-wide operations master roles. The tool actually calls Ntdsutil to output the information, but saves time for the administrator by only outputting the relevant information. The user must be a member of the following groups to run Dump FSMO Roles:

Builtin\Administrator, to run the tool locally.

Domain\Administrator or Enterprise\Administrator, to run the tool remotely.

The syntax for DumpFsmos follows:

`dumpfsmos` *`DomainController`*

Parameters

`DomainController`

Is the name of a domain controller in any domain in the forest.

File Required

Dumpfsmos.cmd

Ntdsutil.exe

Source

Resource Kit