Domain Controller, Types of Domain Controllers, FSMO roles, Organizational Units

Date: 08-08-2023

Domain Controller:

Domain is defined as **collection of users, groups, accounts, networks, applications, systems, database servers and resources controlled from a centralized location is known as domain.**

Domain Controller is a **server that manages network and identity requests,** domain controller works as primary mode for authenticating user identities to windows-based systems, networks, applications and so on. From one domain controller we can create n number of additional domain controllers. If we create an object in domain controller it will replicate in additional domain controller and vice-versa.

The main purpose of domain controller is to make sure that all bad actors stay out of the domain, only authorized users access the relevant resources in the domain.

Trust relationships allow domain controllers in different domains to share resources and authenticate users across domains. Trusts can be one-way or two-way and are configured in the Active Directory Domains and Trusts console.

Domain controllers serve several key roles, including:

- Authenticating users and computers when they log in.
- Storing and managing the Active Directory database.
- Replicating data to maintain consistency across the network.
- Enforcing security policies and access control.

- Domain controller is a server that is used to **store a copy of NTDS.DIT (New Technology Directory Services Directory Information Tree)database** is known as domain controller, along with NTDS.DIT, SYSVOL folder copy also saved.
- All domain controllers will store read/write copy of NTDS.DIT and SYSVOL except RODC.
- RODC is used in scenarios like we are having an office named with Contoso and it is having a branch across the different states, one is in Hyderabad which is known as main branch with a database of NTDS.DIT. And this database contains printers, scanners, groups etc. In Hyderabad branch we have 3000 employees. Each employee has credentials to login. User authentication is done by the database.
- Coming to Chennai branch we have only 300 employees. Here we have no database to check the user authentication every time we need to send the information to Hyderabad branch, if the connection between these two branches is good then we have fast results, otherwise it will be a problem.
- To prevent all this process, we use RODC, the database present in the Hyderabad will be replicated and updated as a copy in read only mode. The replicated database present in Chennai will help to cross check the user authentication and makes a fast progress.
- RODC is a domain controller with database, which has no write access.
- Due to **replication concept same data will be available across the domain.** Here user from Hyderabad will go to Australia branch even from Australia he can access the data of NTDS.DIT due to the replication of domain.
- NTDS.DIT is the database, **SYSVOL folder contains all the template settings for group policy organizations.**
- AD DS replication service to synchronize changes and updates to the AD DS database between the domain controllers in the domain.
- The SYSVOL folders are replicated either by File Replication Service (FRS)/Distributed File System (DFS).
- Domain Controller host several other Active Directory related services, including Kerberos services, which is used by user and computer account for logon authentication.

Global Catalog:

- A global catalog is a distributed database that contains index of every object from all the domains in multidomain forest.
- By default, global catalog server that is created is the first domain controller in the forest root domain.
- In a single domain, all domain controllers can be configured as holders of global catalog.
- In multidomain environment the infrastructure master should not be global catalog server.

Types of Domain Controllers:

- **Primary Domain Controller:**

  It maintains the **master copy of the database NTDS.DIT and validate the users.** Database contains users, computers, printers etc.

  If PDC fails, then BDC (Backup domain controller) can be promoted as the PDC.

  A PDC can be demoted to a BDC if one of the BDC is promoted as PDC.

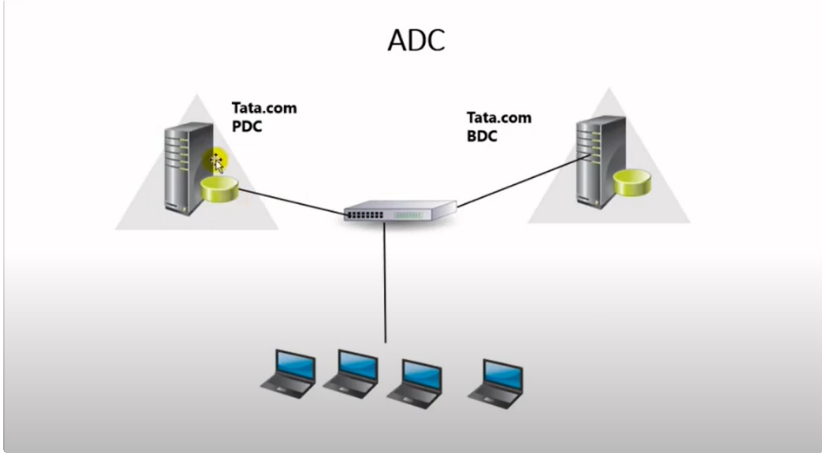
  PDC is also called as root domain controller, tree root domain controller, forest root domain controller.

- **Additional Domain Controller:**

  Additional Domain Controller is also known as backup domain controller. You can install ADC after the installation of PDC.

  A BDC contains **copy of directory database and can validate users.** Possible data loss is user changes that have not yet been replicated from PDC to BDC.

  We can create objects on ADC as same as PDC like users, groups, objects.



Additional Domain Controller

- **Read Only Domain Controller:**

  Read Only Domain Controller is a special type of domain controller, which stores the passwords of some users, not all the forest.

  If RODC stolen, we can change passwords from forest domain controller.

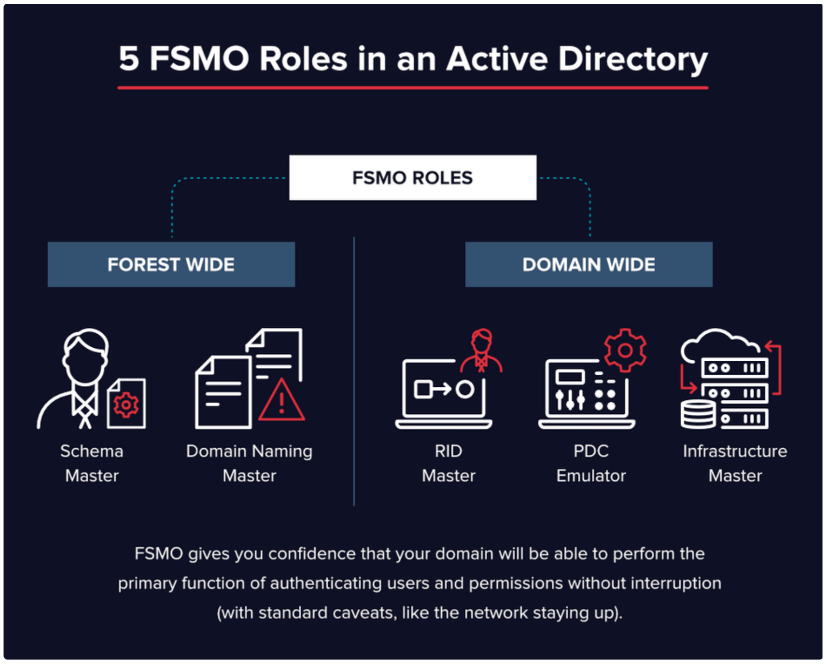
  We deploy RODC in branch office where 10-30 employees work and no special in it infrastructure.

- **Child Domain Controller:**

  CDC is known as the child domain controller, it is part of your main domain, if yahoo.com is your main domain then mail.yahoo.com will be your subdomain.

FSMO Roles:

FSMO roles are of five types which are categorized as following picture:



5 FSMO Roles in an Active Directory

FSMO ROLES

FOREST WIDE

DOMAIN WIDE

Schema Master

Domain Naming Master

RID Master

PDC Emulator

Infrastructure Master

FSMO gives you confidence that your domain will be able to perform the primary function of authenticating users and permissions without interruption (with standard caveats, like the network staying up).

Forest Wide:

- **Schema Master:**
  It is a collection of class (user accounts, computers, groups), objects and its attributes such as employee name, phone number, login name. Basically, schema master is hidden to unhide it we use a command in run which is regsvr32 schmmgmt. dll . After that type mmc to get the schema master open. Basically, in schema there will be no changes done, if any changes are done then it will replicate in the entire forest.

- **Domain Naming Master:**
  Domain naming master is responsible for **promote and demote domain controllers**. Domain naming master is used to **create, add, prevent duplicate name created in the forest.**

Domain Wide:

- **RID Master:**
  Relative Identification master is responsible to **assign unique identification to the objects (computers, groups, accounts), which is called SID (Security Identification).**
  For example, if we have an Aadhar card and that number cannot be assigned to another person. The same thing will apply in RID master. If we created a RID account, we would have a SID number so SID number cannot be duplicated to a different user account. All permission rights are associated to SID not username.
  RID master provides RID pool for every domain controller. If RID pool is finished, then the domain controller cannot create user accounts unless it again contacts the RID master to extend the pool limit.

- **PDC Emulator:**
  Primary Domain Controller is **responsible for synchronization of time across the forest, authentication, user password change update.**
  Passwords are replicated immediately if the password is changed.

- **Infrastructure Master:**
  It is responsible to **update user account information when it’s moved to different domain.**
  It is important if there is multiple forest/single large forest.
  Also, it should not be placed in domain controller which hold global catalog.

- FSMO (Flexible Single Master Operation) roles helps to **prevent the data conflicts and maintaining the data consistency**. If we have 2 different forests and, in their forests, different users. But with same name during the synchronization of two forests we will get a conflict of having duplicate users. To overcome this FSMO roles are introduced.
- FSMO roles are relevant in environments running Active Directory Domain Services (AD DS) with multiple domain controllers.

- FSMO roles are necessary to maintain the **integrity of a multi-master replication directory service. They ensure that only one domain controller is responsible for specific operations, preventing conflicts and ensuring data consistency.**
- The FSMO roles are specialized operations performed by specific domain controllers. These roles include the PDC Emulator, Infrastructure Master, RID Master, Schema Master, and Domain Naming Master. **They control specific functions in the Active Directory forest and domain.**
- You can **transfer FSMO roles using the Active Directory Users and Computers or the ntdsutil command.** Seizing roles, on the other hand, is performed in case of failure and involves using the ntdsutil command to forcibly take over roles.
- Transferring an FSMO role is the **recommended and controlled process of moving a role from one domain controller to another.** Seizing an FSMO role is an **emergency action taken when the current role holder is permanently unavailable, and there is no opportunity for a graceful transfer. Seizing should be used as a last resort.**
- Seizing an FSMO role should be done carefully, as it forces the role to move to a new domain controller without the cooperation of the current role holder. It can lead to conflicts and issues if not executed correctly. Seizing should only be done when the current role holder is permanently unavailable.
- Improper management or unavailability of FSMO roles can lead to various issues, including difficulties with schema changes, domain controller additions, replication, and time synchronization. It's crucial to monitor and maintain FSMO roles to ensure the smooth operation of Active Directory.

Organizational Unit:

- Everything in an active directory is an object.
- **An organizational unit is a container for these objects.**
- In addition to OU, there are also built-in containers.
- OU serves three main purposes:
- The main purposes are Keep objects organized.
- Delegate administrative privileges.
- Manage group policy.
- OUs are containers used for organizing objects within domains. Domains are distinct security boundaries, and forests consist of one or more domains. OUs help structure and manage objects within domains.
- OUs can be created by administrators or users with the necessary permissions in Active Directory. To create an OU, you typically use the Active Directory Users and Computers management console or PowerShell.
- Group Policies can be applied at the OU level. When policies are linked to an OU, they affect the objects (users and computers) within that OU and any child OUs. This allows administrators to customize settings for specific groups of users or computers.
- OUs can be renamed or moved within Active Directory. Renaming an OU does not affect the objects contained within it. Moving an OU to a different location can also be done to reorganize the directory structure.