Lab - Transferring FSMO Roles in Active Directory

Overview

In this lab, students will learn about the five Flexible Single Master Operations (FSMO) roles (also known as operations master roles) and their function in Active Directory.

Lab Requirements

- One Domain Controller (2012/2016) configured as the forest root.
- One Domain Controller (2012/2016) configured as a replica server

Multi-Master Model

The task of updating most Active Directory objects can be performed using any Domain Controller except for those designated as read-only. Updates such as computer object properties renamed organizational units, and user account password resets can be handled using any writable domain controller.

When an object has changed on one domain controller, those changes are propagated to the other domain controllers using replication. During replication, all Domain Controllers on the network share their changes. A domain user can use a Domain Controller located in one part of the domain to reset their password, and once all the Domain Controllers have replicated their changes, the new password will be stored on the Domain Controller the user uses to signs onto the network.

This model works very well for most objects. In the case of any conflicts, such as a password reset done by both the central helpdesk and the network administrator, those conflicts are resolved using the last timestamped change. However, some changes are too important and not well suited to this model.

Single-Master Model

There are five specific types of updates to Active Directory that are very important and to help avoid conflicts; these changes are performed only on Domain Controllers designated to have one of the five Flexible Single Master Operations roles (FSMO) assigned to it.

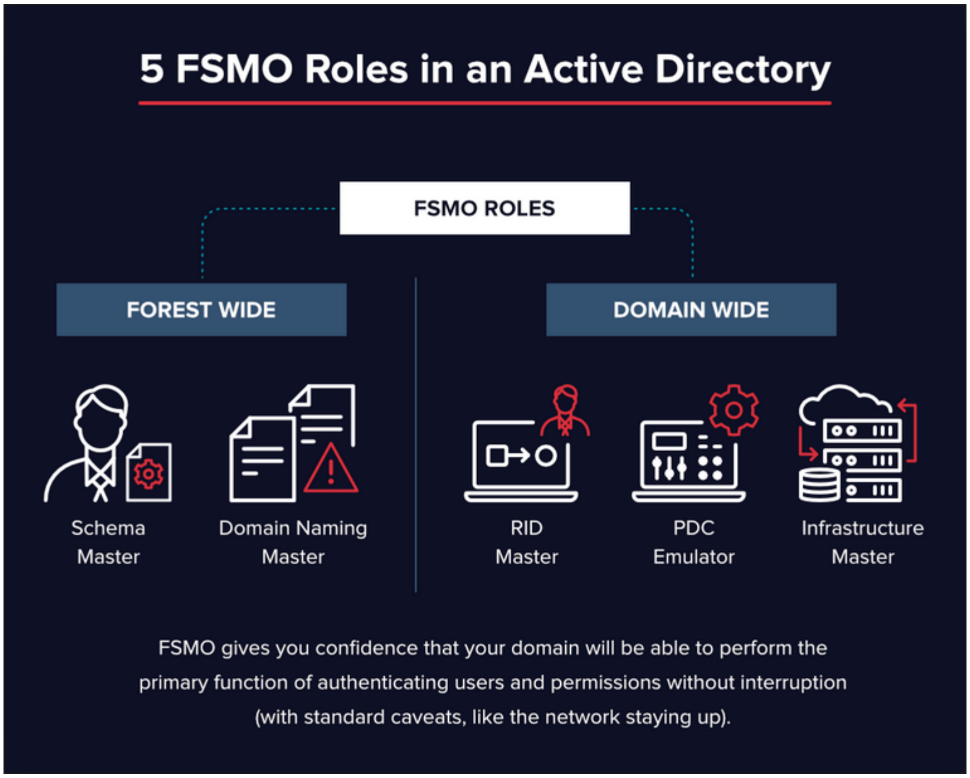
The following five FSMO roles are present in every forest.

- Schema Master
- Domain Naming Master
- Infrastructure Master

- Relative ID (RID) Master
- Primary Domain Controller (PDC) Emulator

Three of the five FSMO roles are also needed once in every domain in the forest:

- Infrastructure Master
- Relative ID (RID) Master
- Primary Domain Controller (PDC) Emulator


5 FSMO Roles in an Active Directory

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).

Schema Master: The Schema Master role manages the read-write copy of your Active Directory schema. The AD Schema defines all the attributes – things like employee ID, phone number, email address, and login name – that you can apply to an object in your AD database.

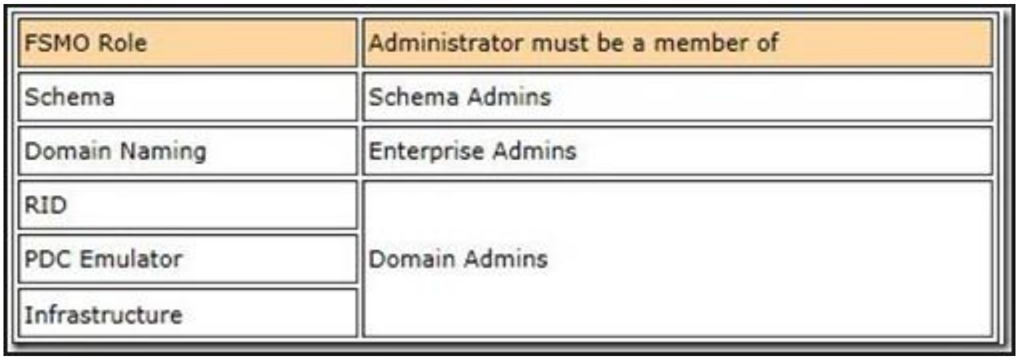
Domain Naming Master: The Domain Naming Master makes sure that you don't create a second domain in the same forest with the same name as another. It is the master of your domain names. Creating new domains isn't something that happens often, so of all the roles, this one is most likely to live on the same DC with another role.

RID Master: The Relative ID Master assigns blocks of Security Identifiers (SID) to different DCs they can use for newly created objects. Each object in AD has a SID, and the last few digits of the SID are the Relative portion. To keep multiple objects from having the same SID, the RID Master grants each DC the privilege of assigning certain SIDs.

PDC Emulator: The DC with the Primary Domain Controller Emulator role is the authoritative DC in the domain. The PDC Emulator responds to authentication requests, changes passwords, and manages Group Policy Objects. And the PDC Emulator tells everyone else what time it is!

Infrastructure Master: The Infrastructure Master role translates Globally Unique Identifiers (GUID), SIDs, and Distinguished Names (DN) between domains. If the Infrastructure Master doesn't do its job correctly, you will see SIDs in place of resolved names in your Access Control Lists (ACL).

Some FSMO's are more sensitive than other, and their access requires enrollment with specific administrator accounts.



FSMO Role	Administrator must be a member of
Schema	Schema Admins
Domain Naming	Enterprise Admins
RID	Domain Admins
PDC Emulator	
Infrastructure	

Transferring vs. Seizing the FSMO roles

There are three situations to distinguish whether to transfer or seize any FSMO role:

1. The downtime is scheduled, and the DC will come back online: Decide to temporarily transfer the roles to a different DC or be aware of the effects during the downtime.

2. **The DC is scheduled to be demoted.** Before you demote the Domain controller, transfer any FSMO roles to a different DC.

3. The DC is offline because of a problem: Identify which roles are affected and what it means for your forest. If there is no chance the Domain controller we come back again, seize the roles using the next available Domain Controller.

It at all possible the FSMO roles should be gracefully transferred using the GUI. Transferring requires that the DC which currently owns the role is still working and online. Transferring notifies the old DC that it does not own the FSMO role(s) anymore.

If the Domain controller with the FSMO role is unavailable and will be replaced, you will need to seize the role using the next available Domain Controller. It is very important the old DC never be connected to the network again. If the old Domain Controller is connected again, there will be conflicts that will lead to an inconsistent AD. The old Domain Controller will see it still has the FSMO master.

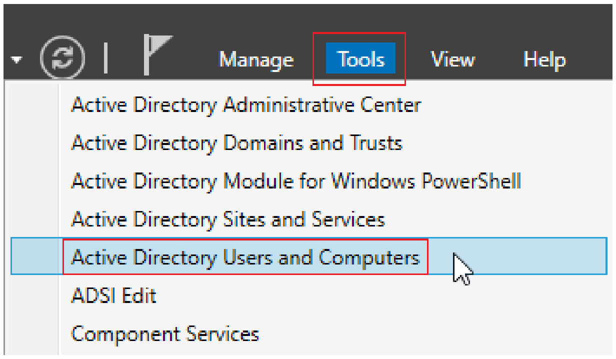
Identify Where FSMO Roles Are Presently

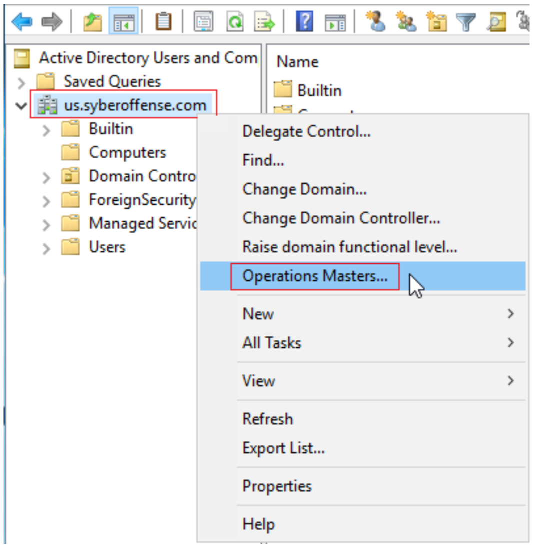
In this scenario, we have two domain controllers present. DC1 which is authoritative for the forest and has all 5 FSMO roles present. DC2 has the three domain-specific FSMO roles, i.e., RID Master, Infrastructure Master, and PDC Emulator.

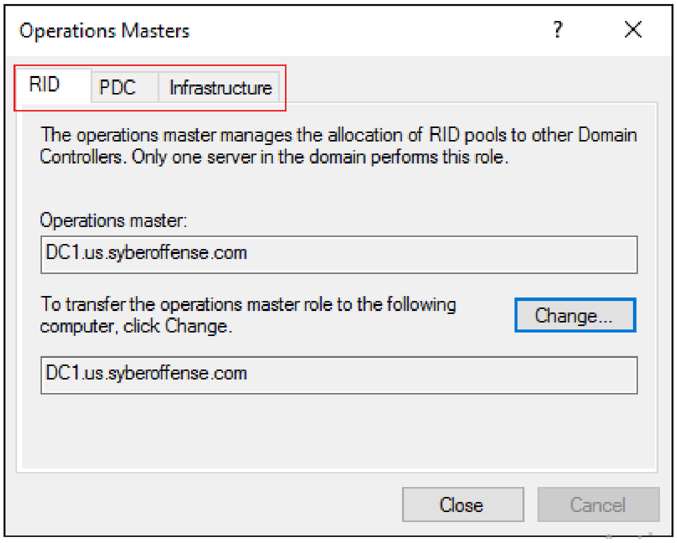
We need to demote DC1. Before we can demote the server, we need to transfer any exsiting FSMO roles onto DC2.

Log onto your forest root. Using Server Manager, Click on Tools and from the context menu, open the Active Directory Users and Computers console, right-click the name of your domain and select Operations Masters. Here we are shown the domain-specific FSMO roles:

- RID Master
- Infrastructure Master
- PDC Emulator.


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services





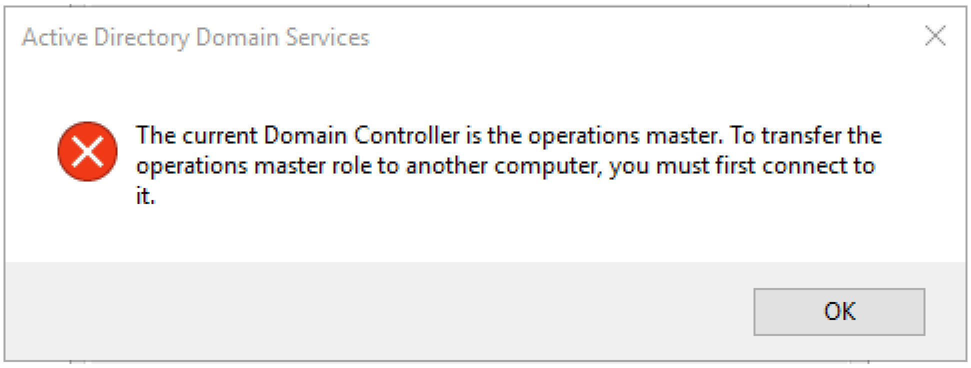
The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:
DC1.us.syberoffense.com

To transfer the operations master role to the following computer, click Change.

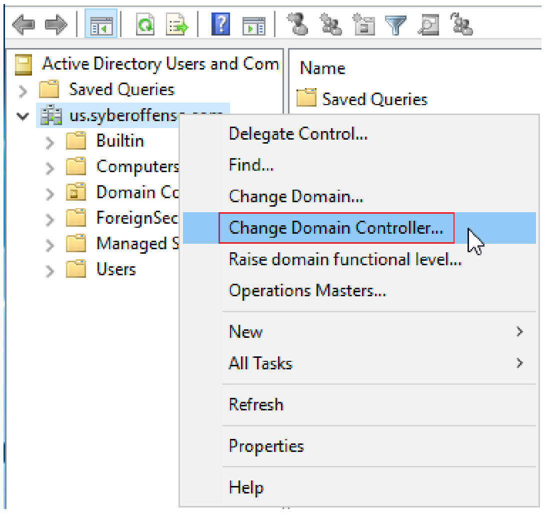
DC1.us.syberoffense.com

Since the machine is the operations master, I must connect to the receiving Domain Controller to initiate the transfer.

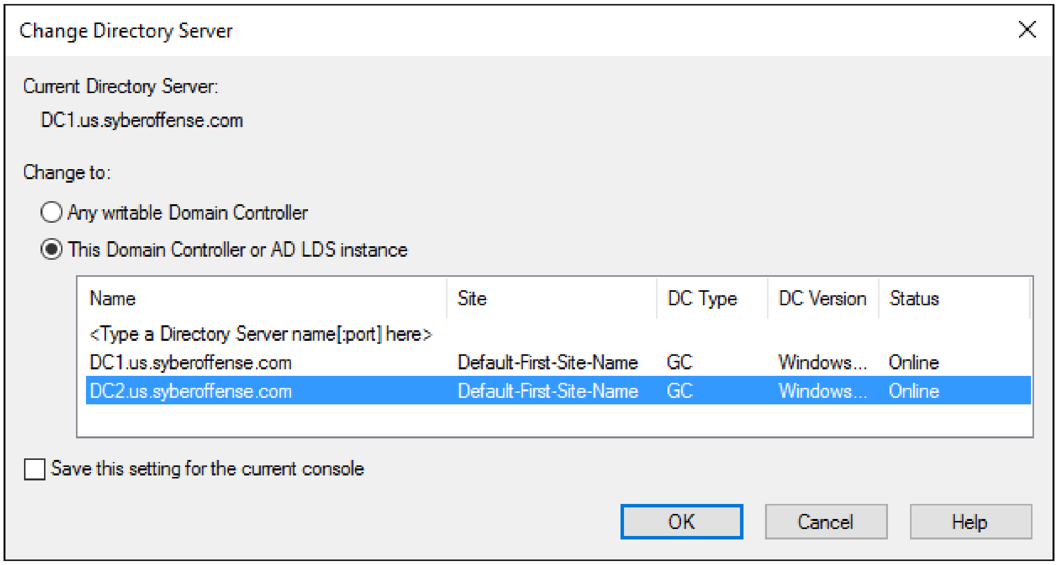


The current Domain Controller is the operations master. To transfer the operations master role to another computer, you must first connect to it.

Right click on the name if your domain and from the context menu. Select Change Domain Controller.



From the list of available Domain Controllers, choose the machine the role is being transferred to. Click Ok.



Change Directory Server

Current Directory Server:
DC1.us.syberoffense.com

Change to:

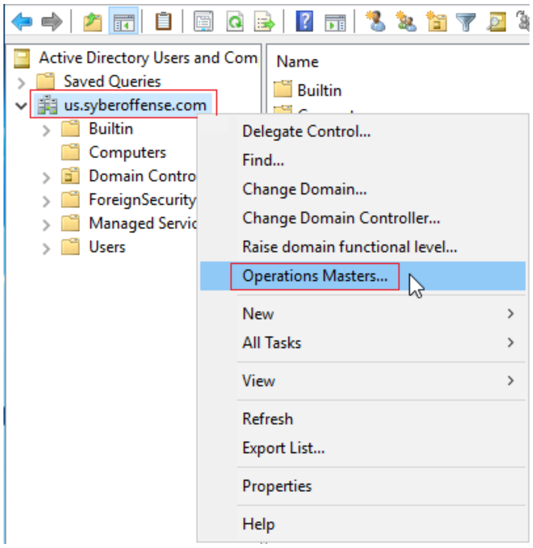
○ Any writable Domain Controller

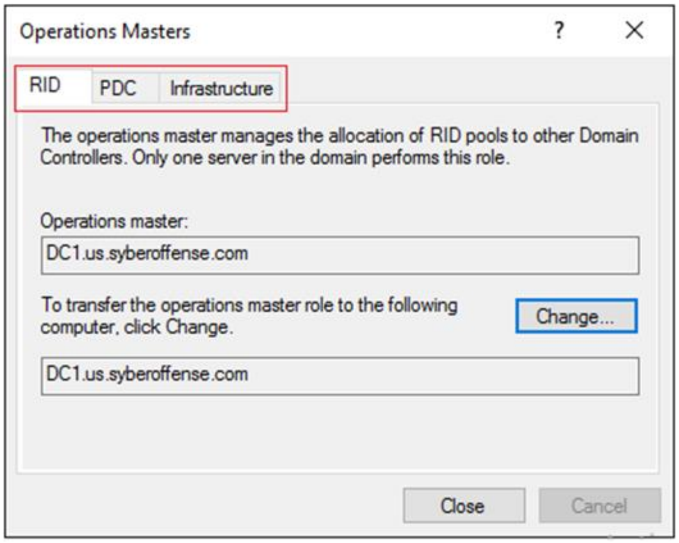
● This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
DC1.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online
DC2.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online

□ Save this setting for the current console

Your ADUC console is now connected to your receiving Domain Controller. Right click on the name of your domain and again select. Operations Masters.



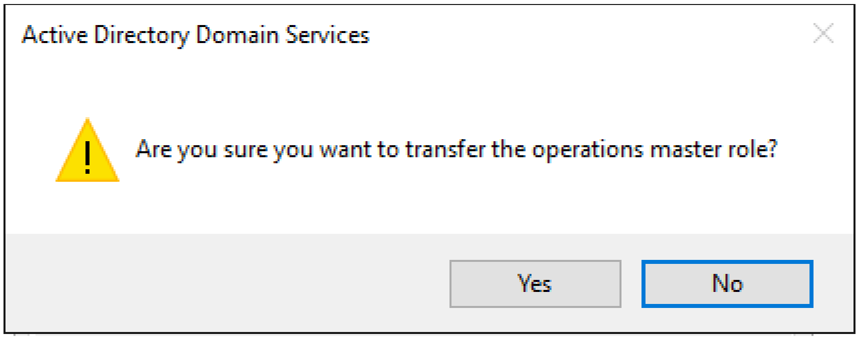


The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:
DC1.us.syberoffense.com

To transfer the operations master role to the following computer, click Change.
DC1.us.syberoffense.com

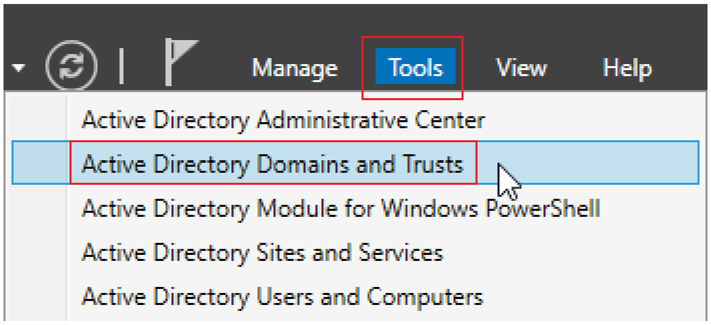
Choose any of the three roles for transfer, click the change button and complete the role transfer.



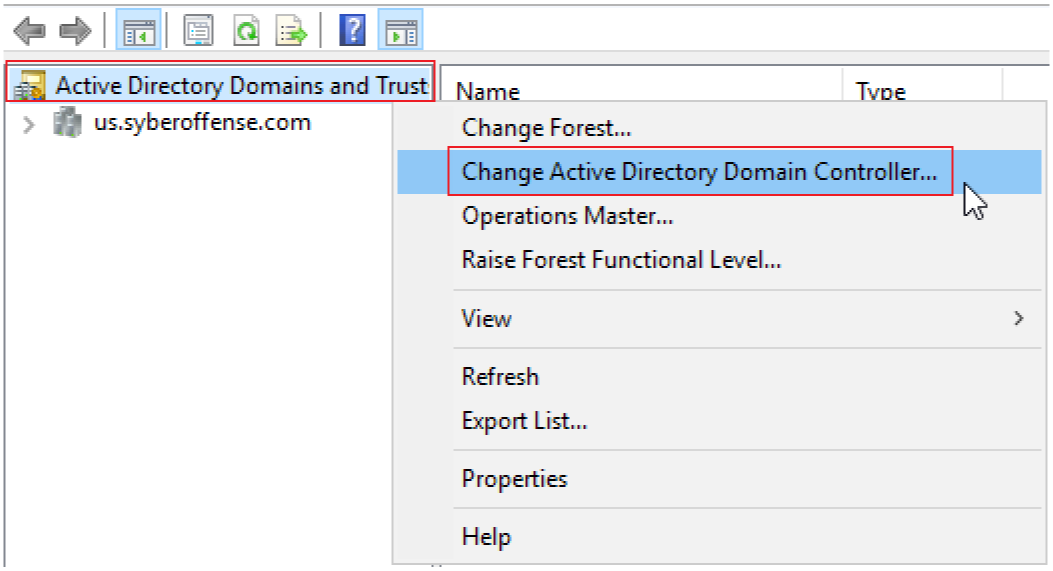
Are you sure you want to transfer the operations master role?

To transfer the forest-specific FSMO **Domain Naming Master** role, follow these steps.

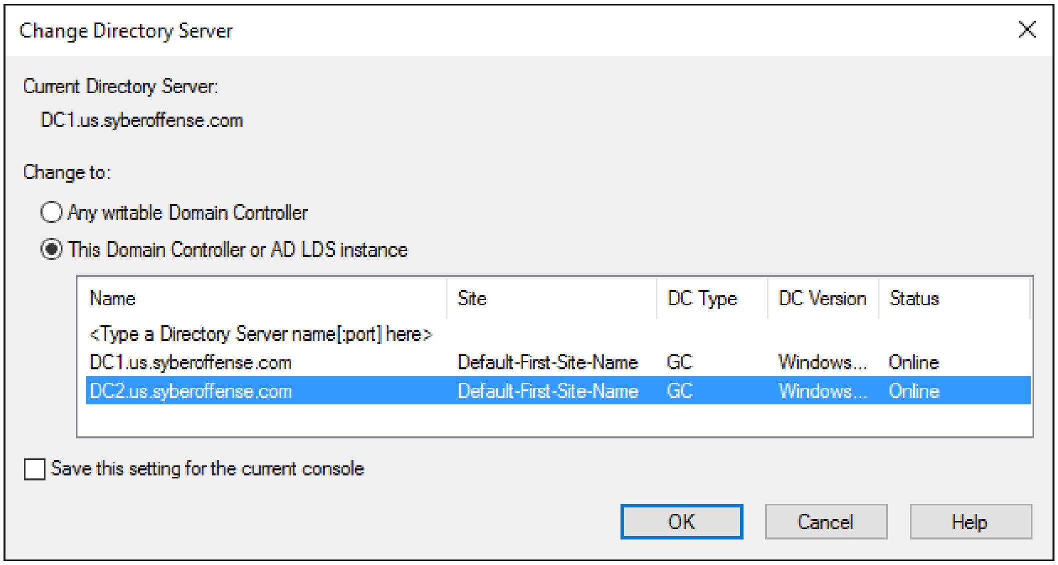
Close out the AUDC console and return to Server Manager. Go to Tools and from the menu select, Active Directory Domain and Trusts.


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers

We first need to connect to the receiving Domain Controller. Find the icon at the top of the left window pane and right click. From the menu, select, Change Active Directory Domain Controller.


Active Directory Domains and Trust
us.syberoffense.com
Name
Type
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help

Select the server that will receive the FSMO role. Click OK.


Change Directory Server

Current Directory Server:
DC1.us.syberoffense.com

Change to:

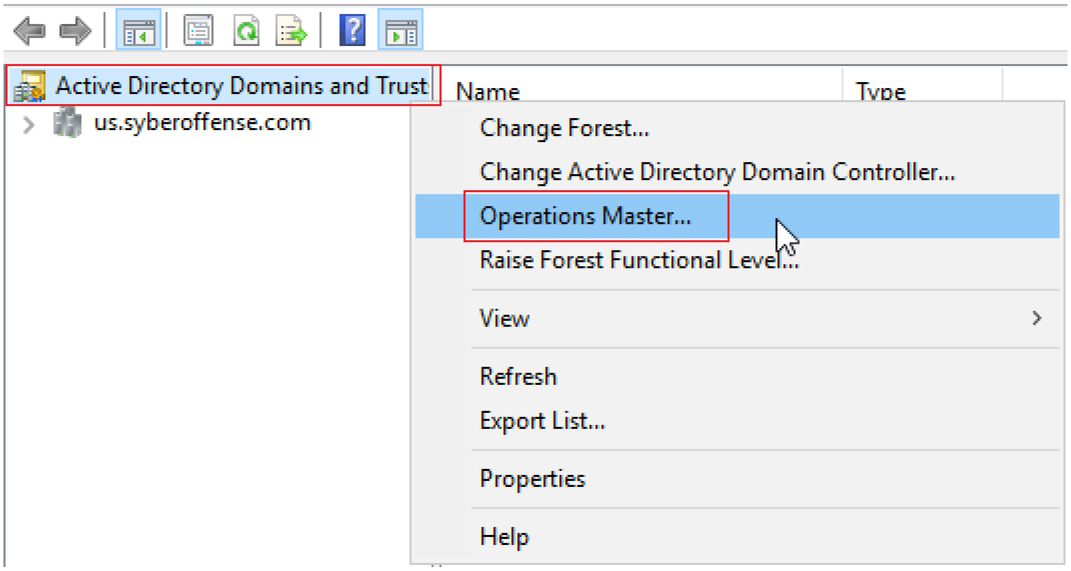
○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

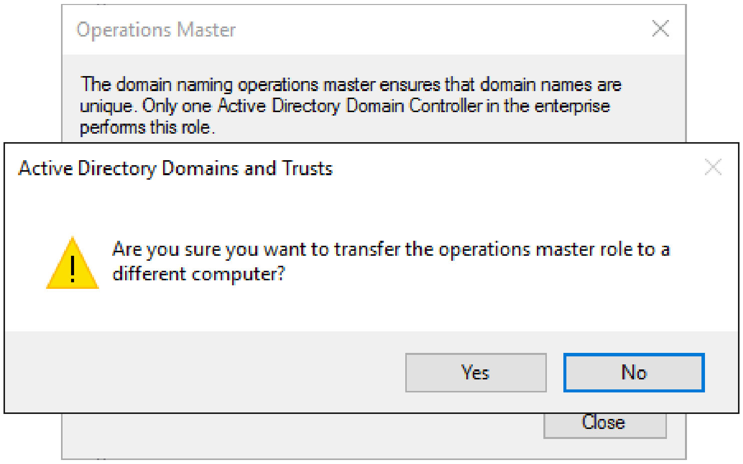
Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
DC1.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online
DC2.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online

□ Save this setting for the current console

Where you see the icon, right click and select Operations Master.


Active Directory Domains and Trust
us.syberoffense.com
Name
Type
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help

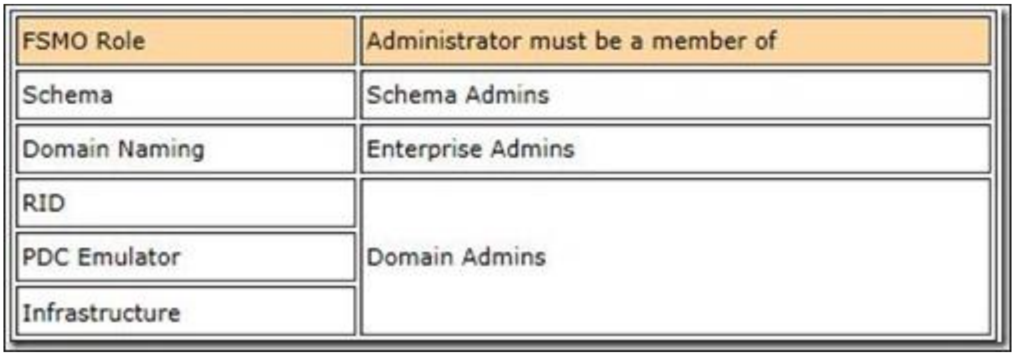
Complete the transfer.



The domain naming operations master ensures that domain names are unique. Only one Active Directory Domain Controller in the enterprise performs this role.

Are you sure you want to transfer the operations master role to a different computer?

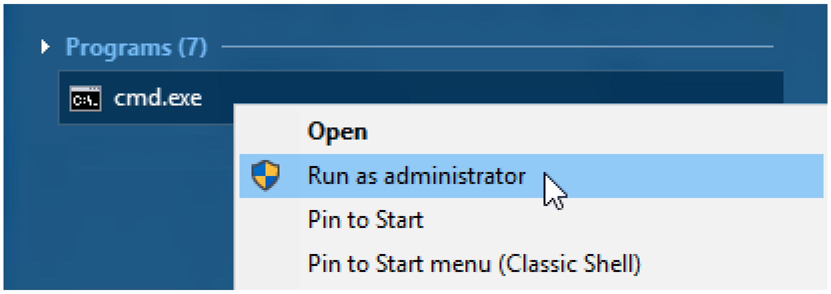
Individuals need to be a member of the following groups to manage FSMO roles.



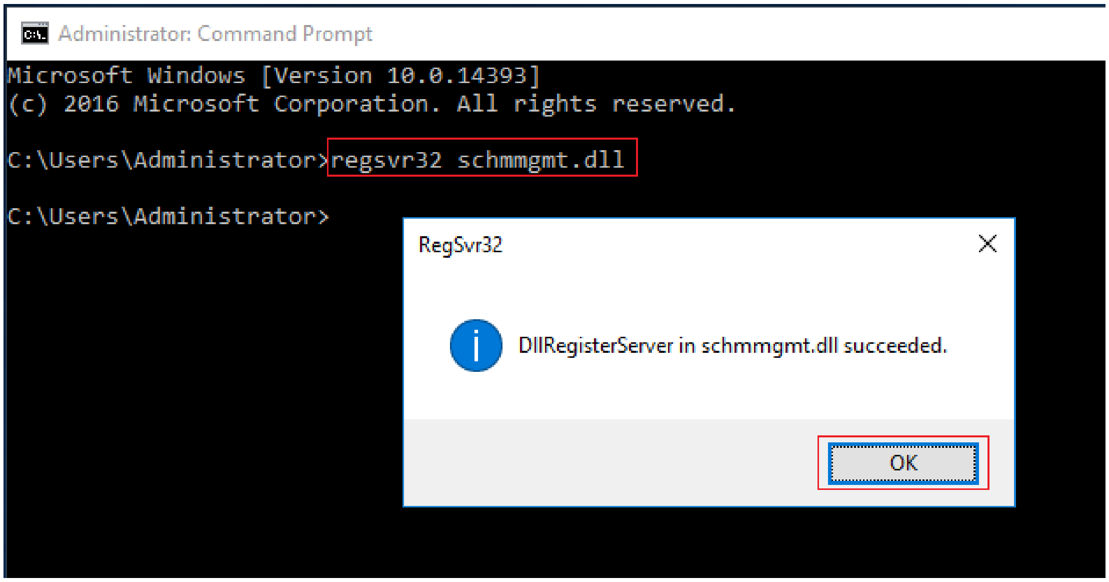
FSMO Role	Administrator must be a member of
Schema	Schema Admins
Domain Naming	Enterprise Admins
RID	Domain Admins
PDC Emulator	
Infrastructure	

On top of the special group membership requirements, the Schema Management Snap-in will not be readily accessible without first registering its DLL on the forest root.

On your root Domain controller, launch the command prompt using run as administrator



At the command prompt type: `regsvr32 schmmgmt.dll`

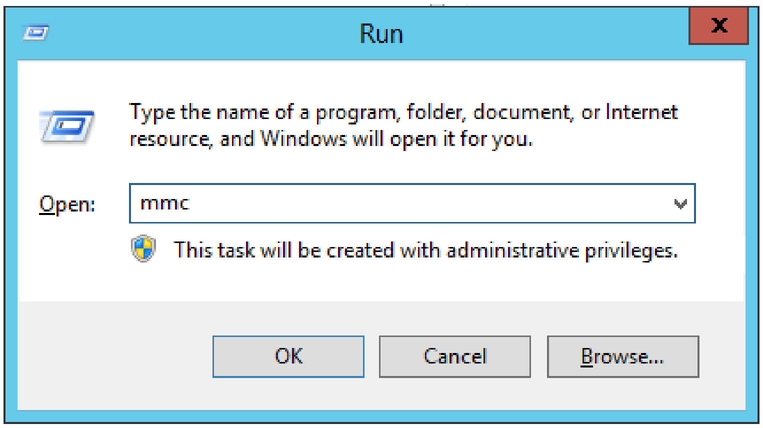


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>regsvr32 schmmgmt.dll

C:\Users\Administrator>
```

DllRegisterServer in schmmgmt.dll succeeded.

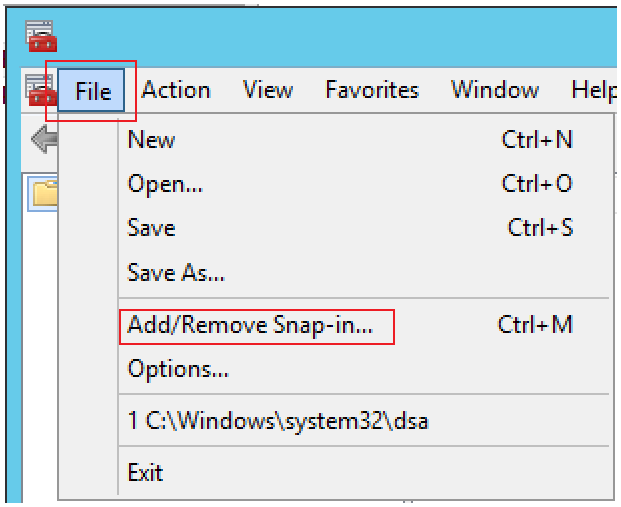
We next need to add the Schema Management Snap-in using the Microsoft Management Console. To do this, we can use the run line.

From your keyboard, press the Window+R key to open a run line. In the run line, type MMC, short for Microsoft Management Console. Click OK.

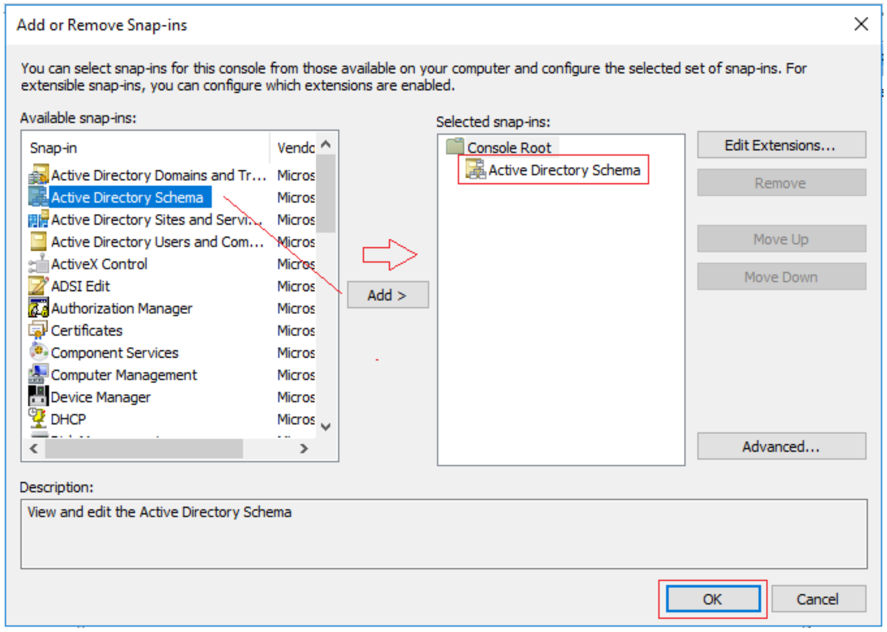


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
mmc
This task will be created with administrative privileges.
OK
Cancel
Browse...

Click on File>Add/Remove Snap-in



From the list of available snap-ins, click on Active Directory Schema and click the Add> button. Click OK.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendc
Active Directory Domains and Tr...	Micros
Active Directory Schema	Micros
Active Directory Sites and Servi...	Micros
Active Directory Users and Com...	Micros
ActiveX Control	Micros
ADSI Edit	Micros
Authorization Manager	Micros
Certificates	Micros
Component Services	Micros
Computer Management	Micros
Device Manager	Micros
DHCP	Micros

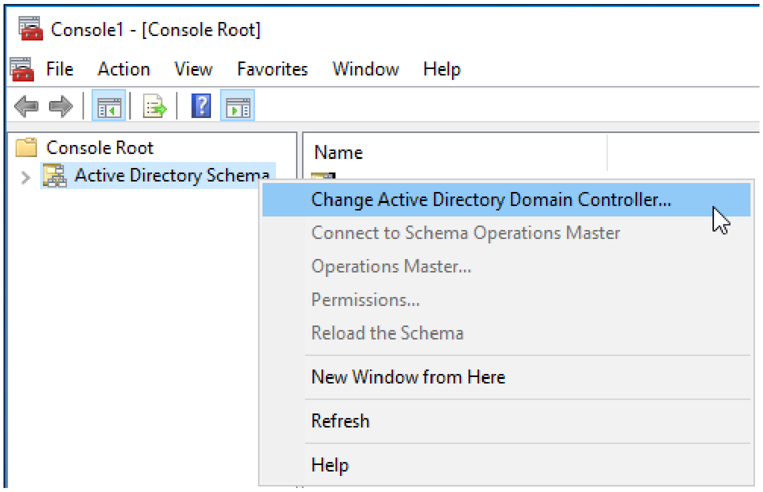
Selected snap-ins:

Console Root
Active Directory Schema

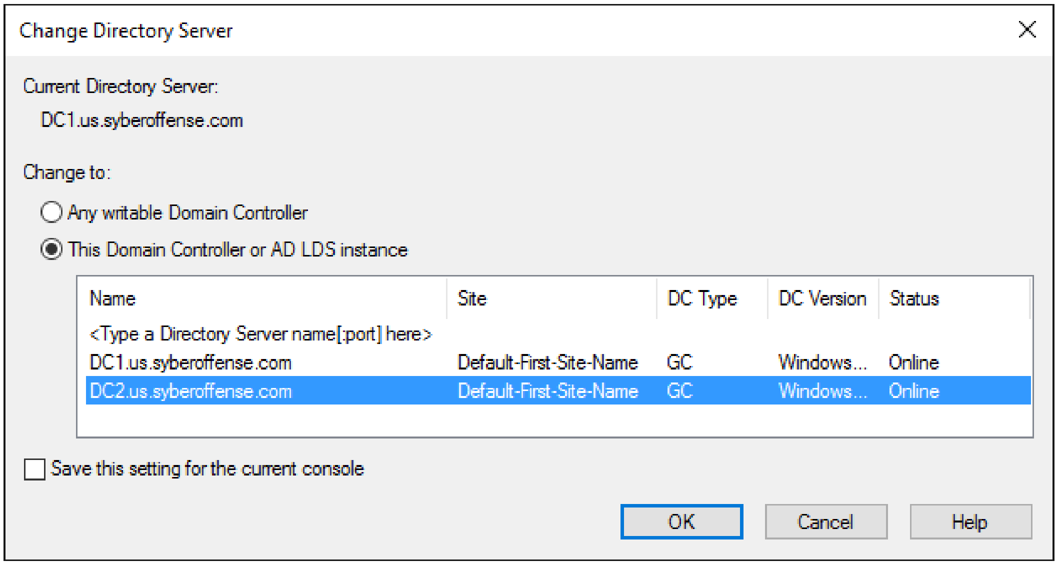
Description:

View and edit the Active Directory Schema

Inside the left window pane of the console window, find the Active Directory Schema snap-in. Right-click and from the context menu, select **Change Active Directory Domain Controller**.



Select the server that will receive the Schema Master role. Click OK.



Change Directory Server

Current Directory Server:

DC1.us.syberoffense.com

Change to:

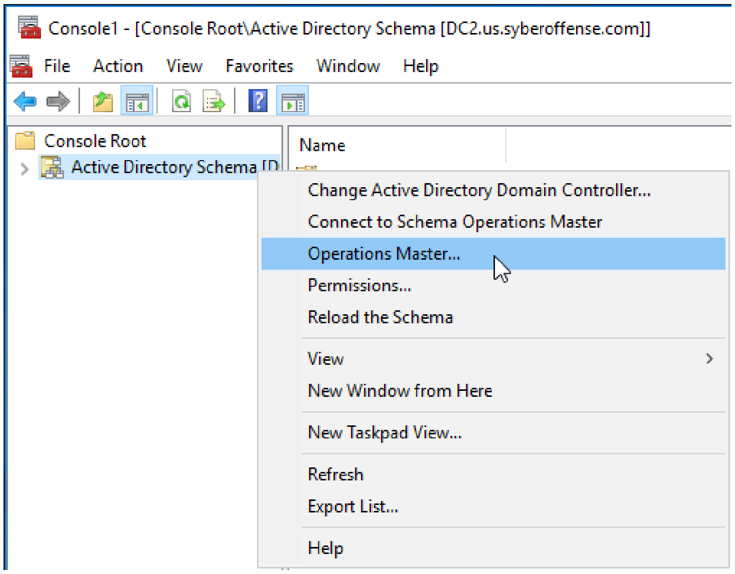
○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
DC1.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online
DC2.us.syberoffense.com	Default-First-Site-Name	GC	Windows...	Online

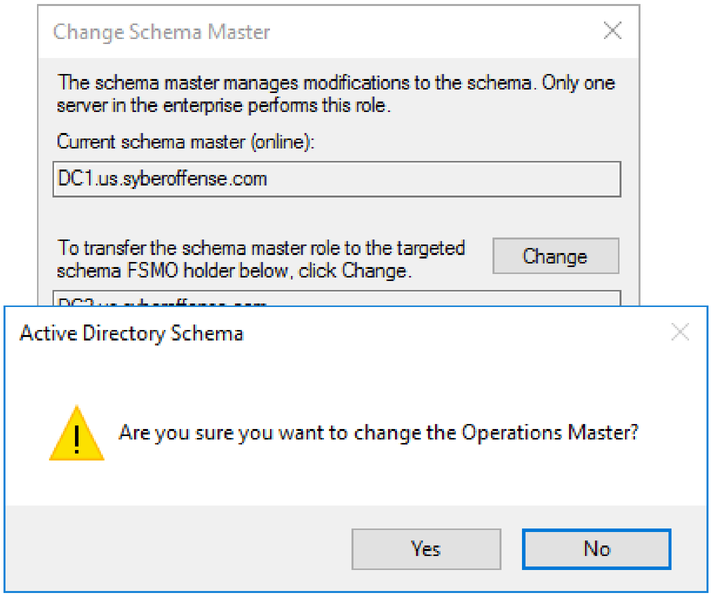
□ Save this setting for the current console

Back at the left window pane, again, right-click in the name of the Schema snap-in and from the context menu select, Operations Master.



Console1 - [Console Root\Active Directory Schema [DC2.us.syberoffense.com]]

Click on the change button to transfer the Schema Operations Master Role.



Change Schema Master

The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

DC1.us.syberoffense.com

To transfer the schema master role to the targeted schema FSMO holder below, click Change.

DC2.us.syberoffense.com

Active Directory Schema

Are you sure you want to change the Operations Master?

Summary –

In a perfect world, we would have the opportunity to gracefully transfer each FSMO role from one Domain Controller to the next, but this is hardly ever the case. The reality is we wouldn’t need to transfer any FSMO role unless there was a genuine need. There will be times when a Domain Controller has been recovered from a crash or a bad install of a Microsoft Update only to find that Active Directly is now badly damaged and generating numerous critical event logs. You hope the FSMO roles will transfer gracefully so you can take the machine offline for repair but when this won’t happen, your only option is to try and seize the FSMO roles using the ntdsutil.

End of the lab!