Lab -Transfer FSMO roles using PowerShell

Overview

In this short lab, students will see how quick and easy it is to transfer any FSMO role using PowerShell. With a domain controller is never a matter of if you will need to transfer roles, it's only a matter of when. Anyone who does domain administration long enough will eventually have to either transfer or seize the Operation Master roles for the forest and the domain.

Lab Requirements

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

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 existing FSMO roles onto DC2.

Transfer FSMO Roles using PowerShell

Moving FSMO roles using PowerShell has the following benefits:

You do not need to use any snap-ins to transfer the role to the future receiving server.
Transferring or seizing FSMO roles do not require a connection to the current or future role owner.
You can run the needed PowerShell cmdlets from a Windows 10 client or Microsoft Server with the Remote Server Administration Tools (RSAT) package installed.

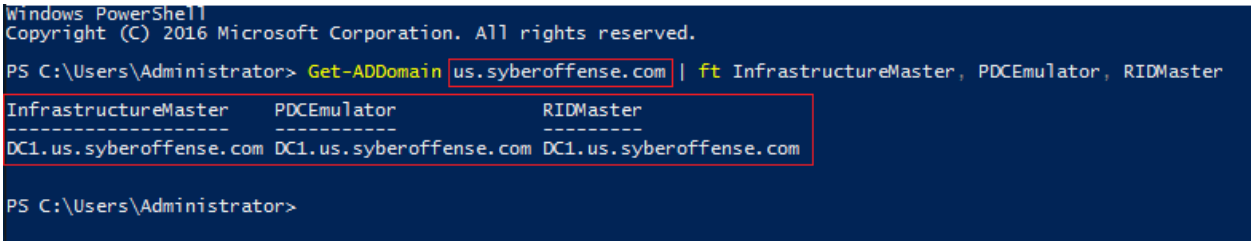
Determine Role Owners

To get the current forest level FSMO role owners (Domain Naming Master and Schema Master roles) you can use the following PowerShell command:

```
Get-ADForest us.syberoffense.com| ft DomainNamingMaster, SchemaMaster
```

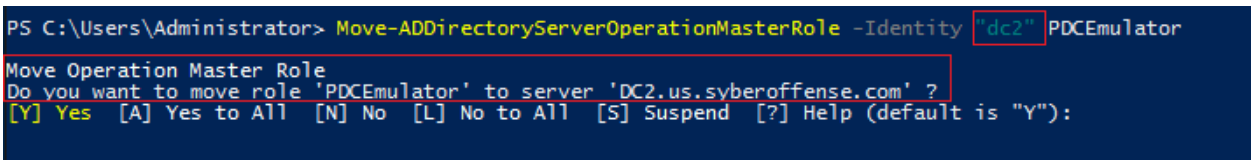
To view domain-wide FSMO roles (Infrastructure Master, PDC Emulator, and Relative Identifier Master roles) type:

```
Get-ADDomain us.syberoffense.com | ft InfrastructureMaster, PDCEmulator, RIDMaster
```



To transfer the PDC Emulator role to a domain controller named dc2, use the command:

```
Move-ADDirectoryServerOperationMasterRole -Identity "dc2" PDCEmulator
```



It is possible to transfer several roles at once:

```
Move-ADDirectoryServerOperationMasterRole -Identity “dc2” -
OperationMasterRole
DomainNamingMaster,PDCEmulator,RIDMaster,SchemaMaster,InfrastructureMaster
```

After entering the transfer command for all or several roles, a window appears asking whether you want to confirm your actions or cancel them.

```
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole -Identity "dc2" -OperationMasterRole DomainNamingMa
ster,PDCEmulator,RIDMaster,SchemaMaster,InfrastructureMaster

Move Operation Master Role
Do you want to move role 'DomainNamingMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'PDCEmulator' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'RIDMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'InfrastructureMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

To simplify the command, you can replace the names of roles with numbers from 0 to 4. The corresponding number assigned to each FSMO can be found in the following table.

PDCEmulator	0
RIDMaster	1
InfrastructureMaster	2
SchemaMaster	3
DomainNamingMaster	4

By using numbers to represent any Operations Master, our last command can be shortened significantly.

```
Move-ADDirectoryServerOperationMasterRole "dc2" -OperationMasterRole 0,1,2,3,4
```

```
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole "dc2" -OperationMasterRole 0,1,2,3,4

Move Operation Master Role
Do you want to move role 'PDCEmulator' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'RIDMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'InfrastructureMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N

Move Operation Master Role
Do you want to move role 'DomainNamingMaster' to server 'DC2.us.syberoffense.com' ?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): N
PS C:\Users\Administrator>
```

Summary –

Once again, PowerShell proves to be a more efficient way of getting something done. A lot less clicks using this method, and this could be done using PowerShell inside a minimal install of Server Core for either Server 2012 or 2016. In the event the current Operations Master is down hard or offline, by adding **-force** switch to the end of any of any transfer commands, you can seize the role(s).

The likely hood of having to seize the Operations Master roles as network administrator or consultant is very real. Domain controllers crashing or blue screening after a hard shutdown or a bad Microsoft update is a common occurrence, especially with off-the-shelf white boxes.

Seizing any Operations Master should be a last resort. The metadata left behind in Active Directory from a failed demotion of a domain controller can break replication and wreak havoc with your Active Directory Database.

In our next lab, **Seizing FSMO Roles in Active Directory Using the NTDSUIL**, we will see how much of the old metadata left behind after a failed demotion can be cleaned up using the NTDSUTIL.