SYBEROFFENSE

Lab - Seizing the FSMO Roles Using the NTDSUTIL

Overview

In this lab, you will learn how to seize the Flexible Single Master Operation (FSMO) roles using the NTDSUTIL. In the event the domain controller which owns the FSMO (Flexible Single Master Operation) roles, has a catastrophic failure, the FSMO roles must be seized and transferred to a replica domain controller to ensure proper functioning of the Active Directory domain.

The steps shown in this lab apply to Server 2012 r2, Server 2016 and Server 2019.

Scenario

In our Active Directory domain there are 2 domain controllers, running Windows Server 2016.

- Forest Root - DC1 – dc1.us.syberoffense.com. (Powered off)
- Replica – DC3 - dc3.us.syberoffense.com. (Powered on)

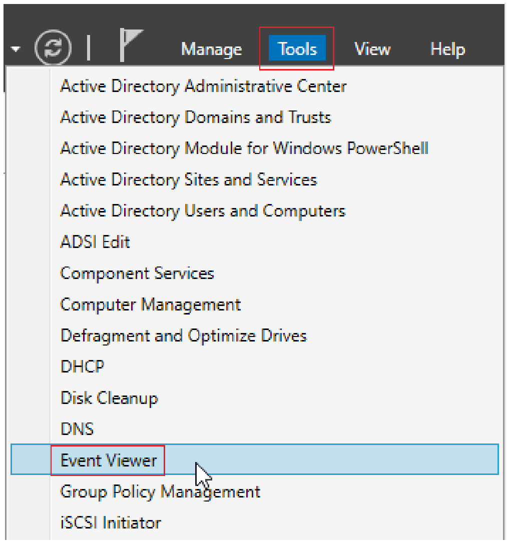
DC1 has had a catastrophic failure and will be down for an extended period. It has been decided that DC1 we need to be completely rebuilt. Since DC1 was the forest root, it will need to have all assigned FSMO roles seized and given to DC3, a replica server running in the domain.

Begin the lab!

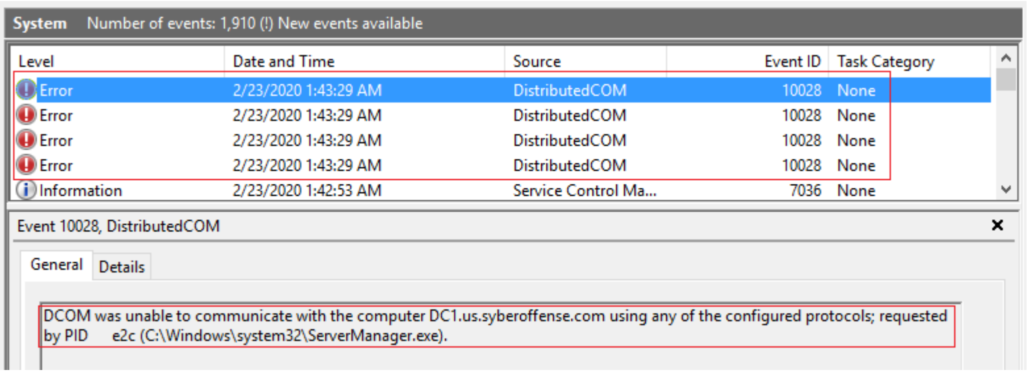
Ensure your forest root has been powered off. The only server needed for the lab is your replica and the name of your replica is not important. The name of my replica server is DC3, your server name may vary.

Ensure that your replica server is up and running and you have logged on to the domain.

Network users started reporting problem with logging in to the domain and not being able to access some resources. You log on to your replica domain controller. From the Server Manager of your replica domain controller, you go to Tools, Event Viewer.


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
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

As you look through the event logs looking for signs of trouble, you find numerous event logs related to DC1. Under the system logs, you find numerous DCOM errors related to DC1 unable to communicate with DC3.



System Number of events: 1,910 (!) New events available

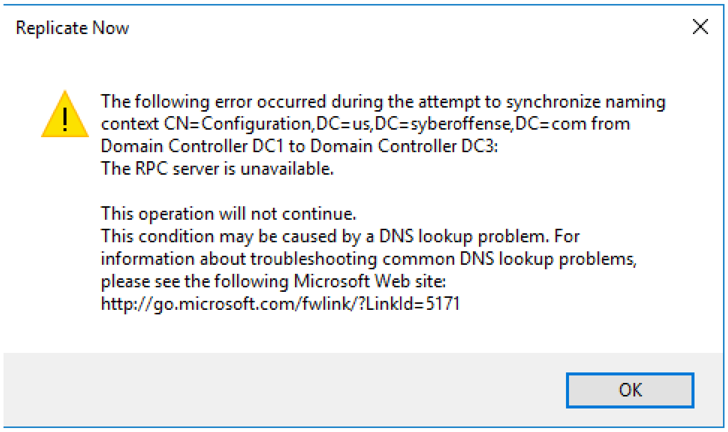
Level	Date and Time	Source	Event ID	Task Category
Error	2/23/2020 1:43:29 AM	DistributedCOM	10028	None
Error	2/23/2020 1:43:29 AM	DistributedCOM	10028	None
Error	2/23/2020 1:43:29 AM	DistributedCOM	10028	None
Error	2/23/2020 1:43:29 AM	DistributedCOM	10028	None
Information	2/23/2020 1:42:53 AM	Service Control Ma...	7036	None

Event 10028, DistributedCOM

DCOM was unable to communicate with the computer DC1.us.syberoffense.com using any of the configured protocols; requested by PID e2c (C:\Windows\system32\ServerManager.exe).

In the Application and Service logs, you find numerous DFS Replication log entries stating that the replication between DC1 and the replica domain controller has failed. DC1 is unreachable.

To confirm the replication between DC1 and your replica domain controller is not working, you open the management console for Active Directory Sites and Services located under the Tools menu. From the left windowpane, you expand the **Default-First-Site-Name** container. You next expand the Servers container. Under the Servers container, you expand DC1 and right click on the NTDS settings for DC1. From the content menu, you try and force DC1 to replicate with it's chosen server. After a short pause you receive the following error message.



Replicate Now

The following error occurred during the attempt to synchronize naming context CN=Configuration,DC=us,DC=syberoffense,DC=com from Domain Controller DC1 to Domain Controller DC3:
The RPC server is unavailable.

This operation will not continue.
This condition may be caused by a DNS lookup problem. For information about troubleshooting common DNS lookup problems, please see the following Microsoft Web site:
http://go.microsoft.com/fwlink/?LinkId=5171

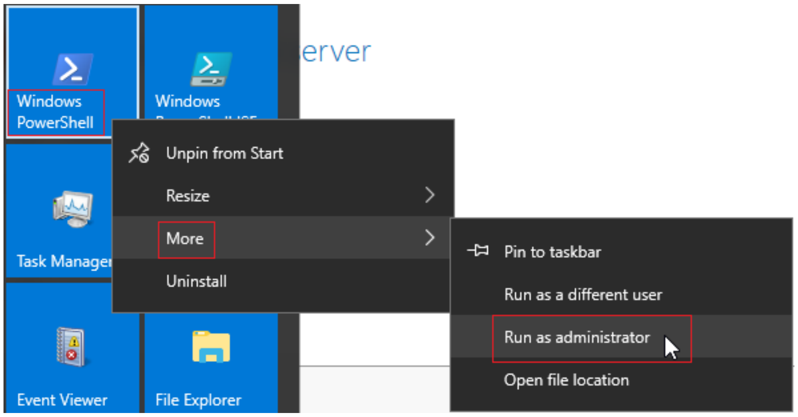
To confirm that DC1 is physically down on the network, you next attempt to start and then logon to DC1 without success (simulate). Your team determines that DC1 has suffered a catastrophic failure and will need to be replaced.

Your replica server is running DNS and you have configured your replica as a DHCP failover partner with DC1. You next need to seize the FSMO roles for the DC1 and clean up any metadata left over that points to DC1 as the forest root and as a domain controller.

Caveat

For this to work, your account must be a member Domain Admins and Schema Admins. It is recommended that you perform all action on the same machine in which you will transfer the FSMO roles. In my case, that would be my DC3. The name of your replica may differ.

Click on the start menu and from the tiles, right clock on Windows PowerShell click on More, and select Run as Administrator.

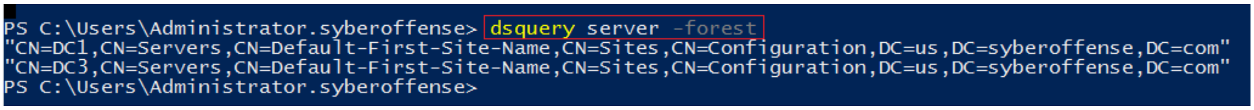


Using PowerShell, we query the domain for information about the forest roots.

Dsquery

Queries the directory by using search criteria that you specify. Each of the dsquery commands finds objects of a specific object type, except for dsquery *, which can query for any type of object.

At the prompt type the following command and press enter: `dsquery server -forest`



```
PS C:\Users\Administrator.syberoffense> dsquery server -forest
"CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com"
"CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com"
PS C:\Users\Administrator.syberoffense>
```

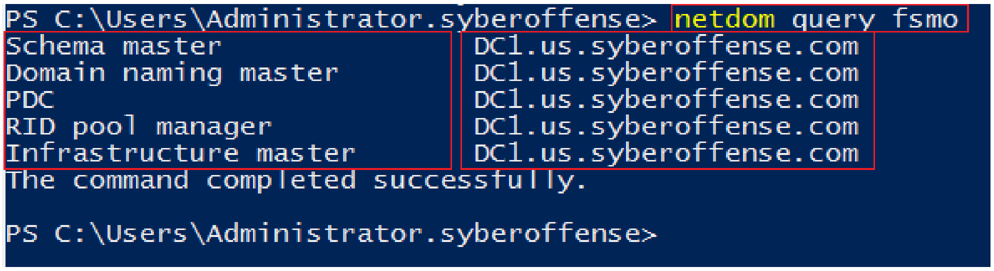
The results show we have two servers acting as the forest root.

We next need to check which server has ownership of all the FSMO roles.

Netdom

NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

At the prompt type the following command and press enter: `netdom query fsmo`

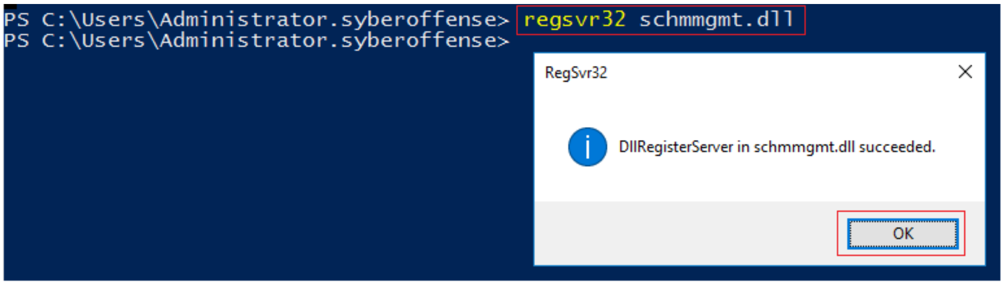


```
PS C:\Users\Administrator.syberoffense> netdom query fsmo
Schema master               DC1.us.syberoffense.com
Domain naming master        DC1.us.syberoffense.com
PDC                         DC1.us.syberoffense.com
RID pool manager            DC1.us.syberoffense.com
Infrastructure master       DC1.us.syberoffense.com
The command completed successfully.

PS C:\Users\Administrator.syberoffense>
```

The results show that DC1 is holding all five RSMO roles for the forest.

Before we transfer the FSMO roles on the additional domain controller, you must register the Active Directory schema management library. Without this crucial step, the transfer will fail.

At the prompt, type the following command and press enter: `regsvr32 schmmgmt.dll`



```
PS C:\Users\Administrator.syberoffense> regsvr32 schmmgmt.dll
PS C:\Users\Administrator.syberoffense>
```

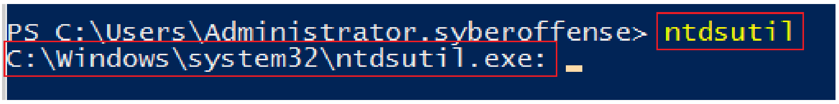
RegSvr32

DllRegisterServer in schmmgmt.dll succeeded.

Click OK to close out the message.

We are now ready to seize the 5 FSMO roles from DC1 and transfer the roles to DC3 using the console utility NTDSUTIL (ADDS service and management tool).

From the prompt, type the following command and press enter: `ntdsutil`

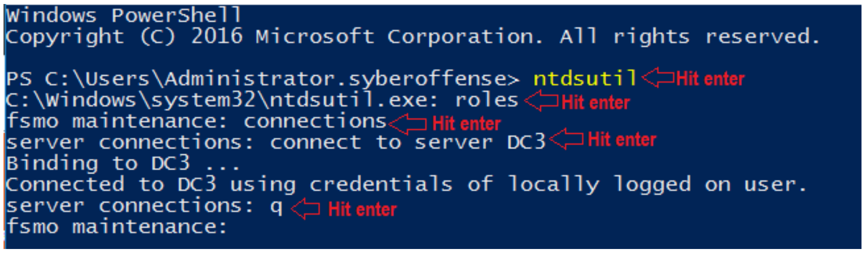


```
PS C:\Users\Administrator.syberoffense> ntdsutil
C:\Windows\system32\ntdsutil.exe: _
```

Notice your prompt changes to let you know that you are in the interfacing with the NTDSUTIL directory.

At the NTDSUTIL prompt, type each of the following commands one at a time and hitting enter after each.

```
roles
connections
connect to server DC3
q
```



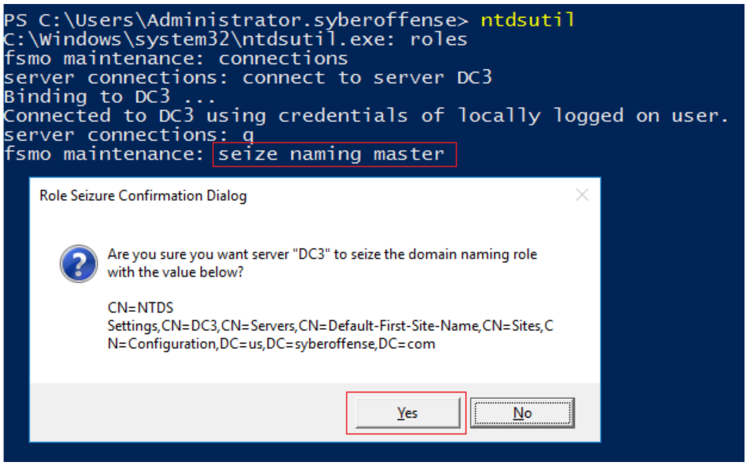
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.syberoffense> ntdsutil
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server DC3
Binding to DC3 ...
Connected to DC3 using credentials of locally logged on user.
server connections: q
fsmo maintenance:
```

We have connected to DC3 and we are ready to now ready seize all five FSMO roles.

To seize the naming master role, type the following and press enter.

```
seize naming master
```

When prompted to confirm, click yes.



```
PS C:\Users\Administrator.syberoffense> ntdsutil
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server DC3
Binding to DC3 ...
Connected to DC3 using credentials of locally logged on user.
server connections: q
fsmo maintenance: seize naming master
```

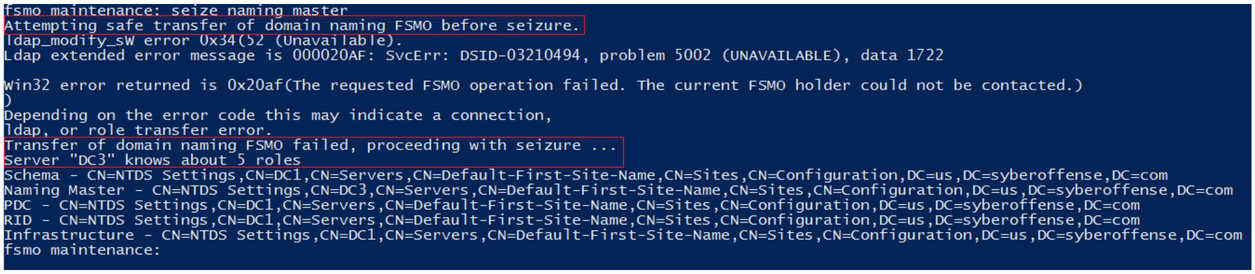
Role Seizure Confirmation Dialog

Are you sure you want server "DC3" to seize the domain naming role with the value below?

CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com

The NTDSUTL will attempt a safe transfer before seizing.

Read the results carefully!

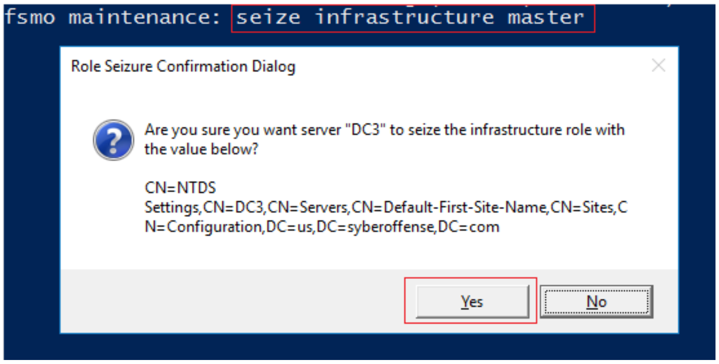


```
fsmo maintenance: seize naming master
Attempting safe transfer of domain naming FSMO before seizure.
ldap_modify_sW error 0x34(52 (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-03210494, problem 5002 (UNAVAILABLE), data 1722

Win32 error returned is 0x20af(The requested FSMO operation failed. The current FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of domain naming FSMO failed, proceeding with seizure ...
Server "DC3" knows about 5 roles
Schema - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
Naming Master - CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
PDC - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
RID - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
Infrastructure - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
fsmo maintenance:
```

At the prompt, type the following command and press enter.

```
seize infrastructure master
```

When prompted to confirm, click yes.



```
fsmo maintenance: seize infrastructure master
```

Role Seizure Confirmation Dialog

Are you sure you want server "DC3" to seize the infrastructure role with the value below?

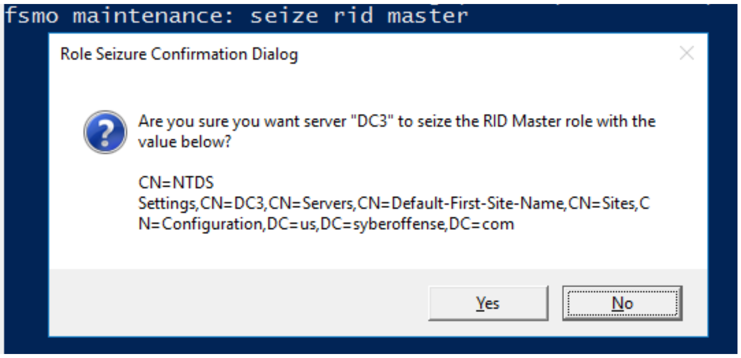
CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com

The same results with the first role seized. Be patient!

Once the role has been seized, seize the rid master, type the following command and press enter.

```
seize rid master
```

Confirm the seizure.



```
fsmo maintenance: seize rid master
```

Role Seizure Confirmation Dialog

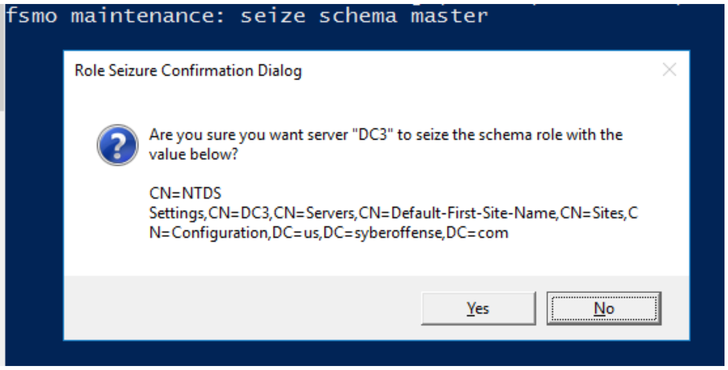
Are you sure you want server "DC3" to seize the RID Master role with the value below?

CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com

You receive the same confirmation as before. Move on to seizing the schema master role.

Type in the following command and press enter. Confirm your choice.

```
seize schema master
```



```
fsmo maintenance: seize schema master
```

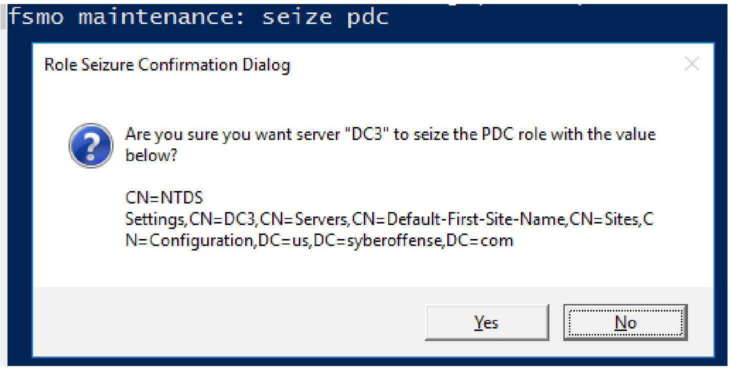
Role Seizure Confirmation Dialog

Are you sure you want server "DC3" to seize the schema role with the value below?

CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com

You receive the same confirmation as before. Move on to seizing the pdc role.

Type in the following command and press enter. Confirm your choice. `seize pdc`



```
fsmo maintenance: seize pdc
```

Role Seizure Confirmation Dialog

Are you sure you want server "DC3" to seize the PDC role with the value below?

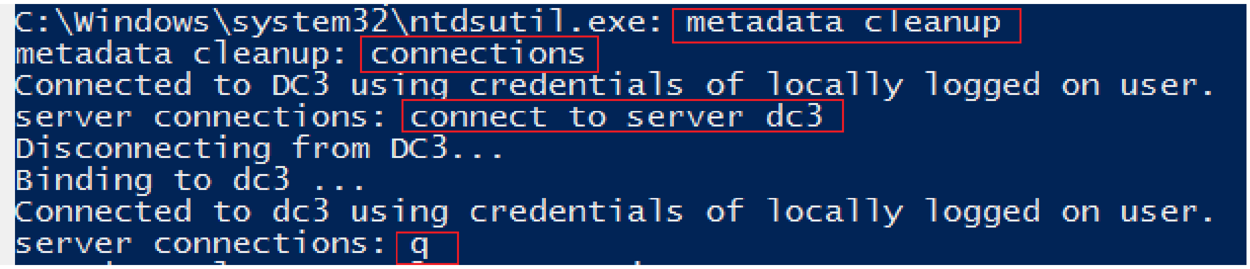
CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com

Once the confirmation come back, will have usefully seized all five roles. We are done with the seizures and we can move on to the metadata cleanup.

Once you have received the same confirmation as before. Type in the letter, q

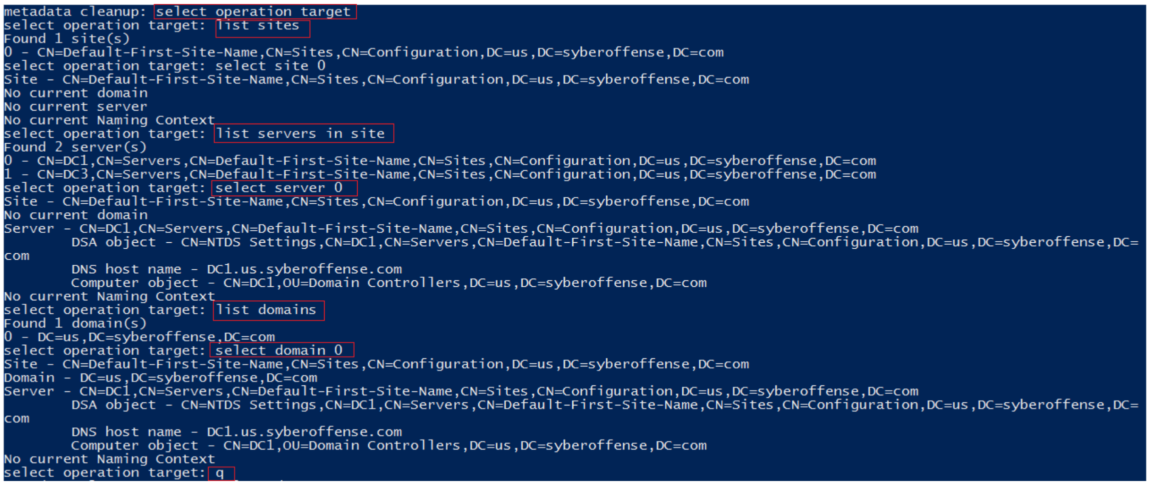
At the prompt type the following commands one at a time and press enter after each command.

```
metadata cleanup
connections
connect to server dc3
q
```



```
C:\Windows\system32\ntdsutil.exe: metadata cleanup
metadata cleanup: connections
Connected to DC3 using credentials of locally logged on user.
server connections: connect to server dc3
Disconnecting from DC3...
Binding to dc3 ...
Connected to dc3 using credentials of locally logged on user.
server connections: q
```

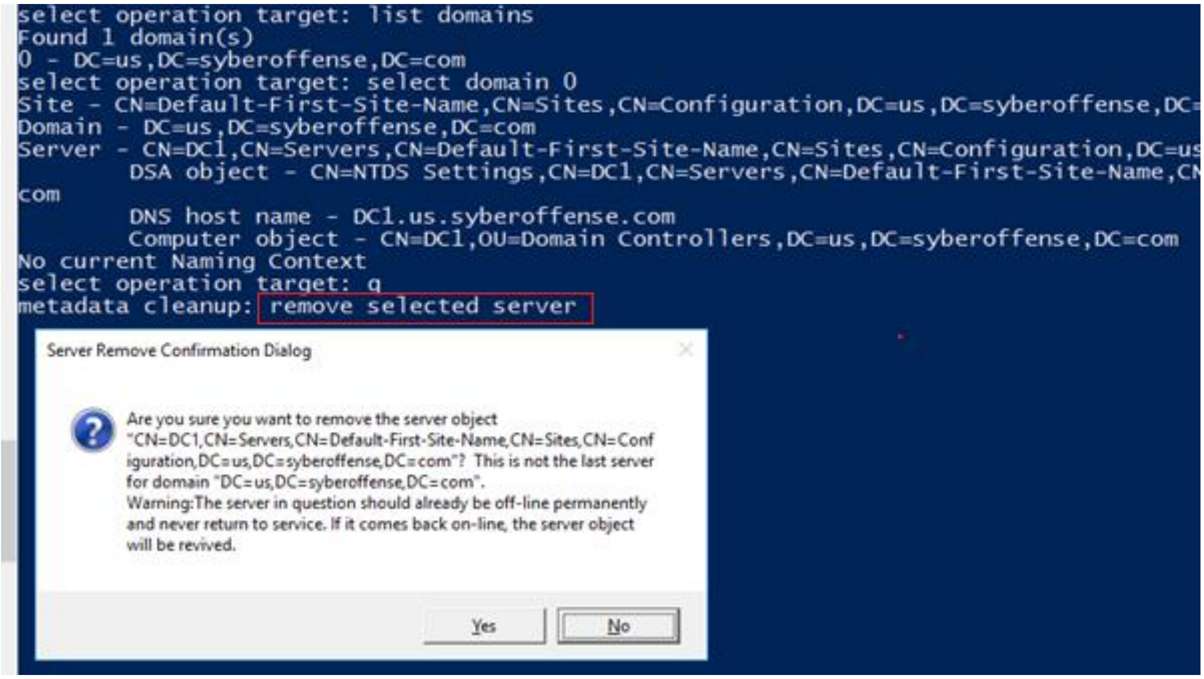
```
select operation target
list sites
select site 0
list servers in site
select server 0
list domains
select domain 0
q
```



```
metadata cleanup: select operation target
select operation target: list sites
Found 1 site(s)
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
select operation target: select site 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
No current domain
No current server
No current Naming Context
select operation target: list servers in site
Found 2 server(s)
0 - CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
1 - CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
select operation target: select server 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
No current domain
Server - CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
        DSA object - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=
com
        DNS host name - DC1.us.syberoffense.com
        Computer object - CN=DC1,OU=Domain Controllers,DC=us,DC=syberoffense,DC=com
No current Naming Context
select operation target: list domains
Found 1 domain(s)
0 - DC=us,DC=syberoffense,DC=com
select operation target: select domain 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
Domain - DC=us,DC=syberoffense,DC=com
Server - CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com
        DSA object - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=
com
        DNS host name - DC1.us.syberoffense.com
        Computer object - CN=DC1,OU=Domain Controllers,DC=us,DC=syberoffense,DC=com
No current Naming Context
select operation target: q
```

`remove selected server`

In the dialog box, are you sure you want to remove the server object … confirm the removal of a domain controller.

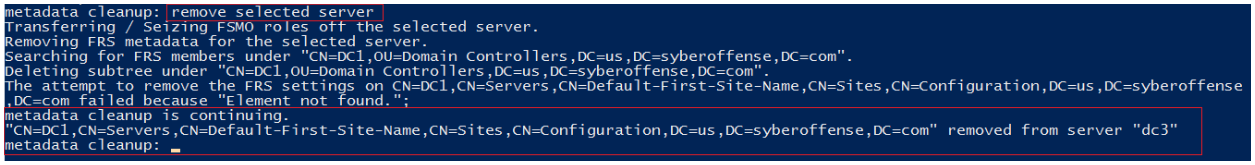


```
select operation target: list domains
Found 1 domain(s)
0 - DC=us,DC=syberoffense,DC=com
select operation target: select domain 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=
Domain - DC=us,DC=syberoffense,DC=com
Server - CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us
        DSA object - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN
com
        DNS host name - DC1.us.syberoffense.com
        Computer object - CN=DC1,OU=Domain Controllers,DC=us,DC=syberoffense,DC=com
No current Naming Context
select operation target: q
metadata cleanup: remove selected server
```

Server Remove Confirmation Dialog

Are you sure you want to remove the server object "CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com"? This is not the last server for domain "DC=us,DC=syberoffense,DC=com".
Warning:The server in question should already be off-line permanently and never return to service. If it comes back on-line, the server object will be revived.

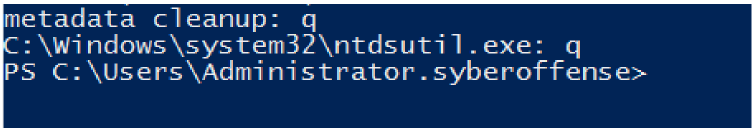
If everything was typed in correctly, you should receive confirmation that DC1 was removed from DC3. Be sure to read the confirmation message.



```
metadata cleanup: remove selected server
Transferring / Seizing FSMO roles off the selected server.
Removing FRS metadata for the selected server.
Searching for FRS members under "CN=DC1,OU=Domain Controllers,DC=us,DC=syberoffense,DC=com".
Deleting subtree under "CN=DC1,OU=Domain Controllers,DC=us,DC=syberoffense,DC=com".
The attempt to remove the FRS settings on CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense
,DC=com failed because "Element not found.";
metadata cleanup is continuing.
"CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=us,DC=syberoffense,DC=com" removed from server "dc3"
metadata cleanup: _
```

Type in, q to quit metadata cleanup.

At the prompt, type q one more timer to exit the NTDSUTIL.



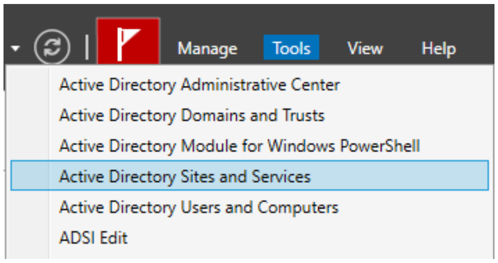
```
metadata cleanup: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Users\Administrator.syberoffense>
```

Close out Powershell.

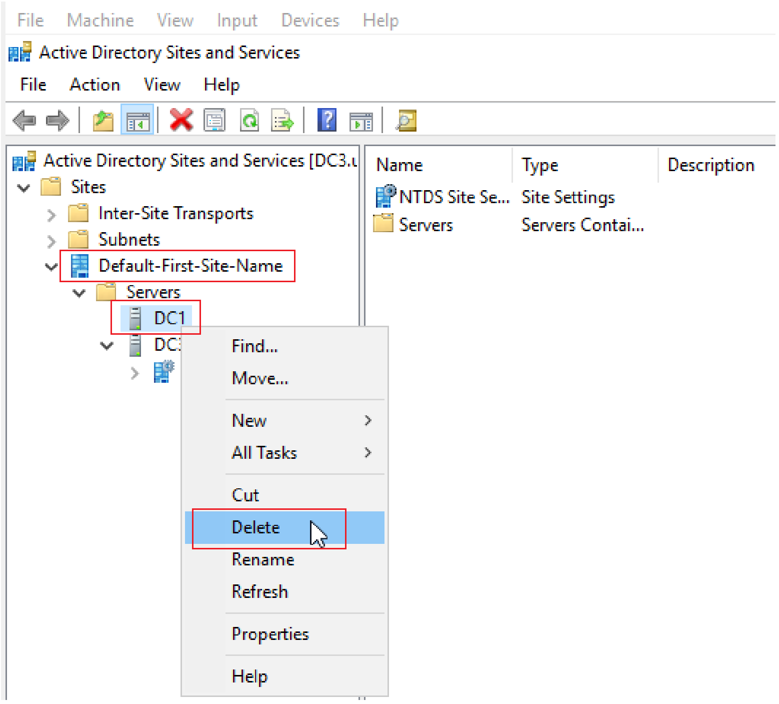
Manually Cleaning Any Reference to DC1

We still have more remnants of DC1 to clean up.

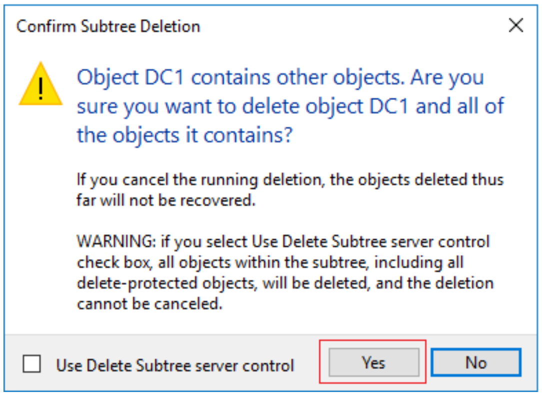
From your server Manager, go to Tools and from the context menu, Select Active directory Sites and Services.


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

Expand your site where DC1 is located, expand the server container, find any mention of DC1, right click and from the context menu, choose delete.



Confirm the deletion.

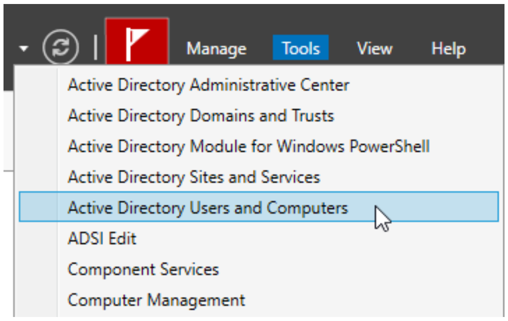

Confirm Subtree Deletion

Object DC1 contains other objects. Are you sure you want to delete object DC1 and all of the objects it contains?

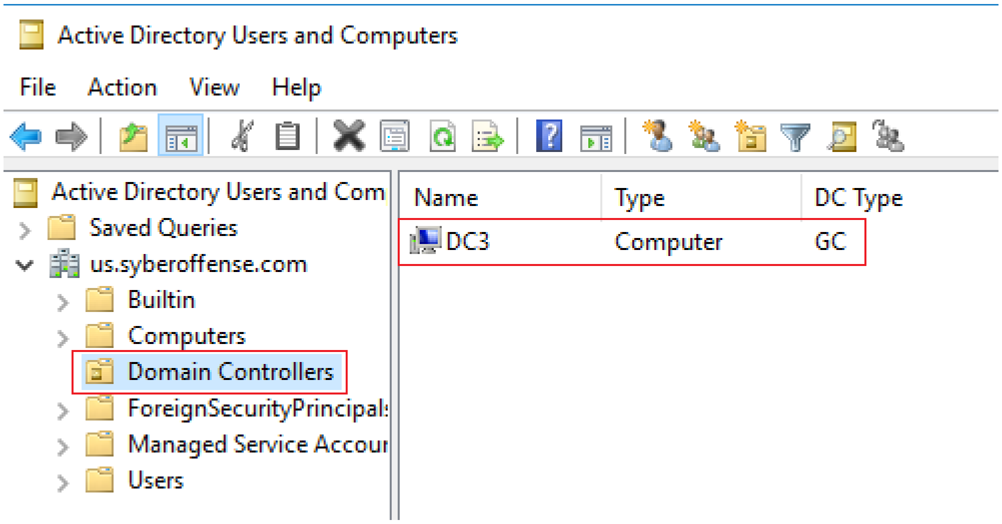
If you cancel the running deletion, the objects deleted thus far will not be recovered.

WARNING: if you select Use Delete Subtree server control check box, all objects within the subtree, including all delete-protected objects, will be deleted, and the deletion cannot be canceled.

Close out Sites and Services and from the Tools menu, open Active Directory Users and Computers.


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
Computer Management

Open your Domain Controllers container and confirm that DC1 is no longer present.



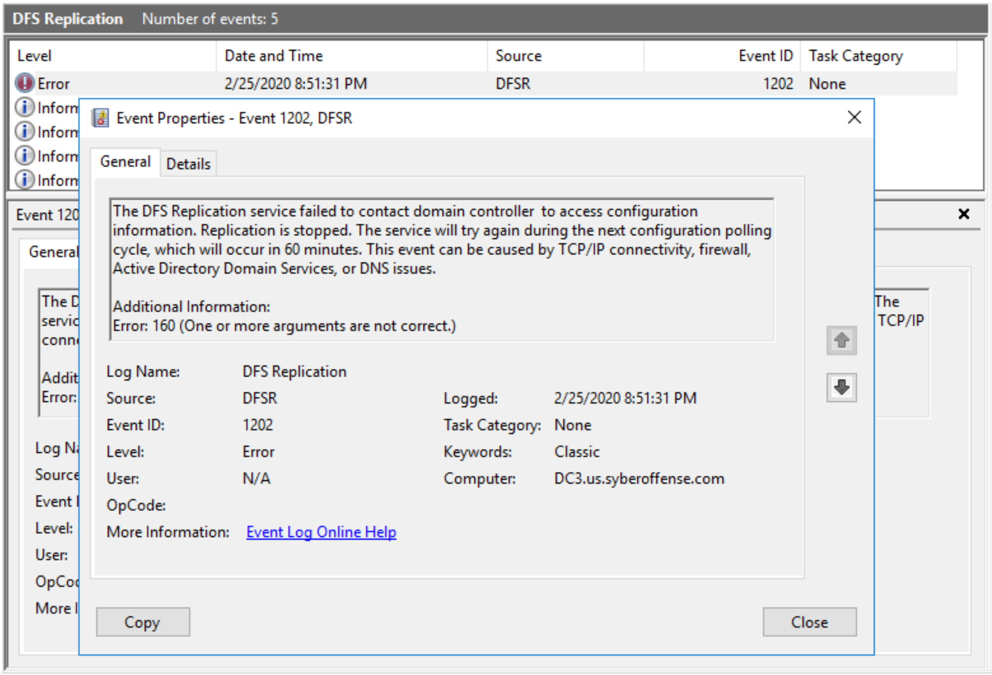
Name	Type	DC Type
DC3	Computer	GC

Summary

There's no way to remove every incident of metadata from any Active Directory database. Your event viewer will be blown up with countless critical errors that call on your failed forest root. You can spend months troubleshooting each of the critical events. Some you can fix, and some will stay with your AD forever.

In this example, I have cleared all the log files from my Event viewer and restarted DC3. When the server has restarted, we can see what fresh events are present inside the event logs for DFS Replication.

This is the event log for DFS replication after the metadata cleanup and the manual removal of DC1 from the Active directory Database.



DFS Replication Number of events: 5

Level	Date and Time	Source	Event ID	Task Category
Error	2/25/2020 8:51:31 PM	DFSR	1202	None
Inform				
Inform				
Inform				
Inform				

Event Properties - Event 1202, DFSR

The DFS Replication service failed to contact domain controller to access configuration information. Replication is stopped. The service will try again during the next configuration polling cycle, which will occur in 60 minutes. This event can be caused by TCP/IP connectivity, firewall, Active Directory Domain Services, or DNS issues.

Additional Information:
Error: 160 (One or more arguments are not correct.)

Log Name:	DFS Replication		
Source:	DFSR	Logged:	2/25/2020 8:51:31 PM
Event ID:	1202	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	DC3.us.syberoffense.com
OpCode:			
More Information:	Event Log Online Help		

Somewhere deep inside the Active Directory database, the replication service is calling on DC1. It’s not a showstopper but imagine that you have numerous remote sites that call on DC1 to replicate their Active directory database with.

End of the lab!