

ITAS 241: Lab 6 Domain Controller & AD Management

By Ethan Holmes

Table of Contents

Activity 6-1:	3
Activity 6-2: Installing an RODC with Staging	3
Activity 6-3:	5
Activity 6-4:	6
Activity 6-5: Viewing Site Properties	6
Activity 6-6:	7
Activity 6-7: Transferring FSMO Roles	8
Activity 6-8: Creating a System State Backup	8
Activity 6-9: Restoring Active Directory from a System State Backup	9
Activity 6-10: Restoring Deleted Objects from the Active Directory Recycle Bin	12
Activity 6-11: Compacting the Active Directory Database	14
Conclusion:	16

Introduction:

In this lab, I will be learning how to backup and restore an active directory database within windows using the Windows Server Backup, as well as how to enable the recycling bin and creating a Read-Only Domain Controller using Powershell

Activity 6-1:

All Virtual Machines were reset

Activity 6-2: Installing an RODC with Staging

To start, I created a new OU called BranchOffice, and then made a new group and user called BranchOff-G and BranchUser1 and made the user a member of the group

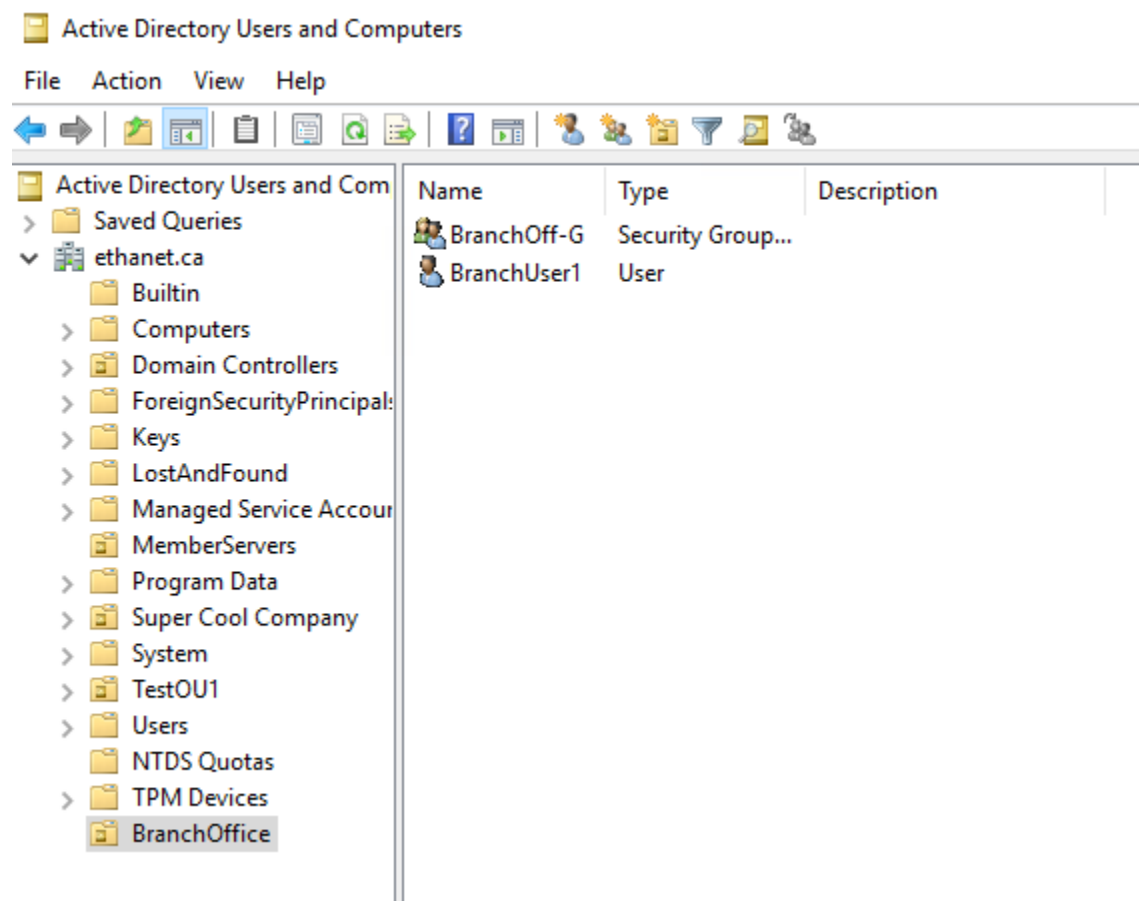


Figure 1: Created group and user

After running the command in the figure below, we can now make our SA server a Read-Only domain controller

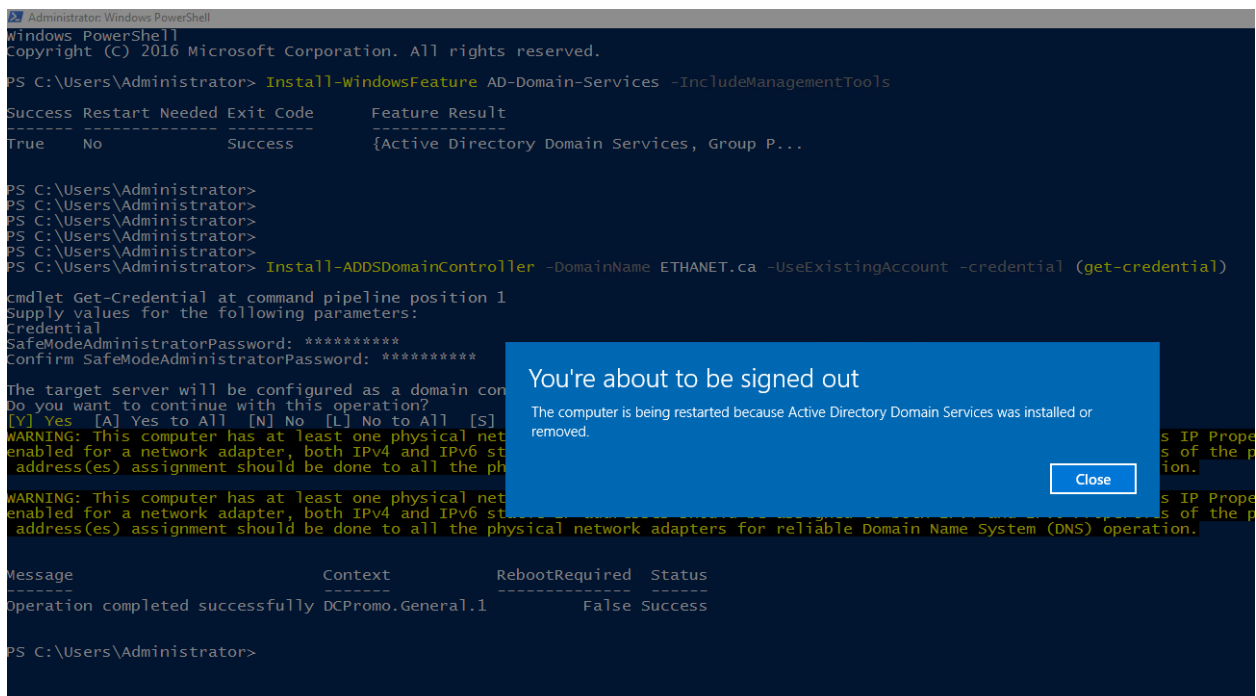
```
PS C:\Users\Administrator> Add-ADSRReadonlyDomainControllerAccount -DomainControllerAccountName EH-ServerSA1 -DomainName ETHANET.CA -SiteName Default-First-Site-Name -DelegatedAdministratorAccountName BranchOff-6
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

Message Context RebootRequired Status
-----
Operation completed successfully DCPromo.General.1 False Success

PS C:\Users\Administrator>
```

Figure 2: Read-Only domain creation

Below after doing the following commands, we can input the password of the BranchUser1 and finish the completion of the read-only domain controller.



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

PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code Feature Result
-----
True No Success {Active Directory Domain Services, Group P...

PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Install-ADDSDomainController -DomainName ETHANET.ca -UseExistingAccount -credential (get-credential)

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Skip
WARNING: This computer has at least one physical network adapter enabled for a network adapter, both IPv4 and IPv6 static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: This computer has at least one physical network adapter enabled for a network adapter, both IPv4 and IPv6 static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

Message Context RebootRequired Status
-----
Operation completed successfully DCPromo.General.1 False Success

PS C:\Users\Administrator>
```

Figure 3: Adding the users and group to be used

After a restart, we can see on DC1 that SA1 has become a read-only domain controller

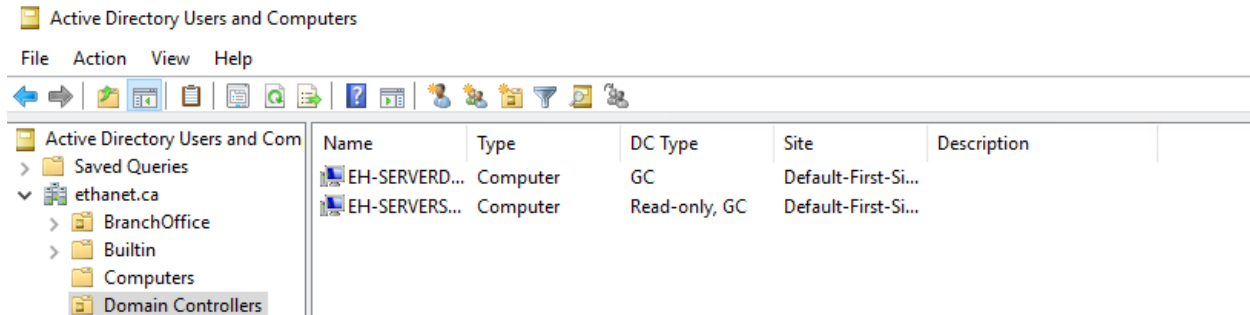


Figure 4: Creation of the Read-only domain in AD Users and Computers

Activity 6-3: Configuring the Password Replication Policy

Using the following command, we can add the BranchOff-G group to the RODC password replication group

```
PS C:\Users\Administrator> Add-ADGroupMember "Allowed RODC Password Replication Group" BranchOff-G
PS C:\Users\Administrator>
```

Figure 5: Adding the Branch group to the password replication group for the RODC

We can now see the BranchUser as well as the Group have been added to the stored accounts

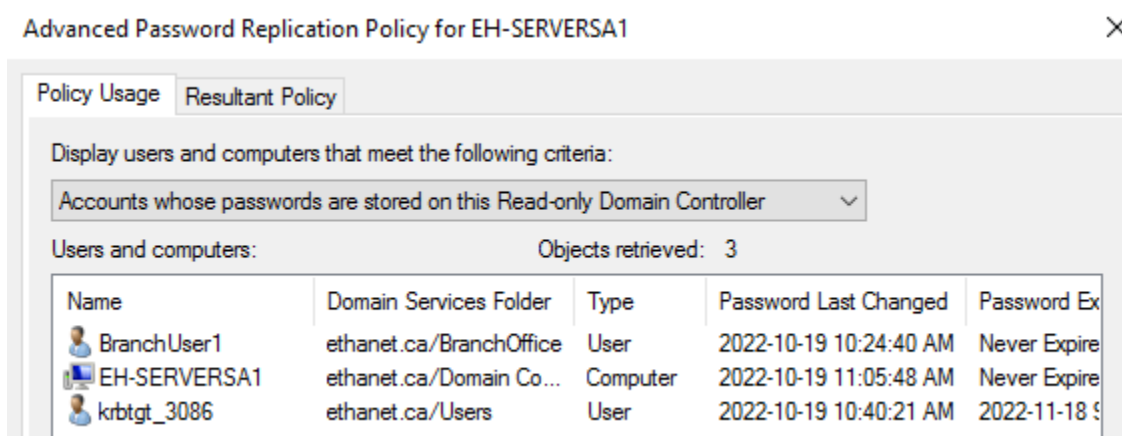


Figure 6: Users and Computers on RODC

Activity 6-4: Creating a Subnet in Active Directory Sites and Services

In this activity, we used our assigned subnet to create a site for our subnet, as well as renaming our current site to the 3rd octet of our subnet

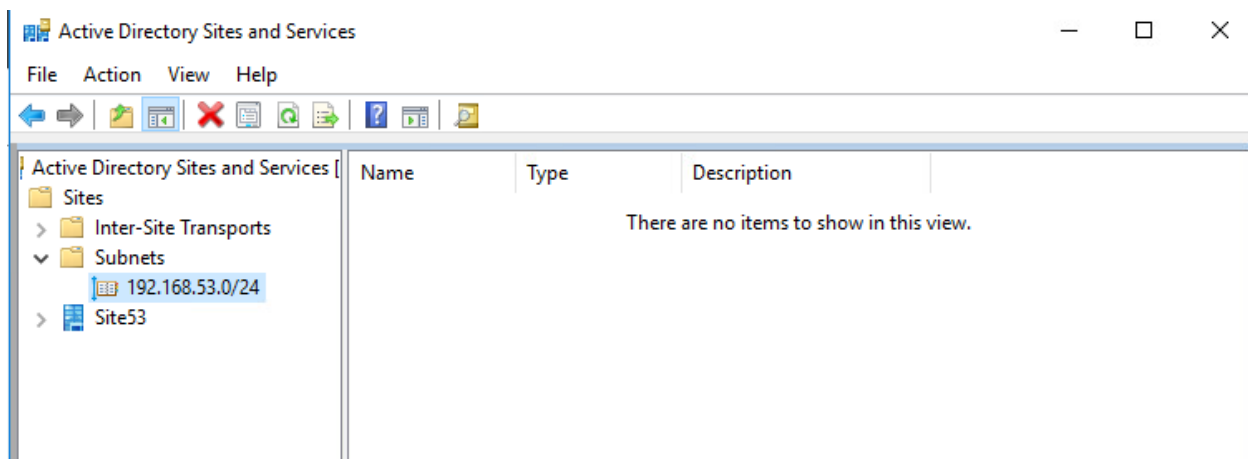


Figure 7: Subnet created

Activity 6-5: Viewing Site Properties

In this activity, we are just viewing the NTDS Site settings and view the intersite replication settings

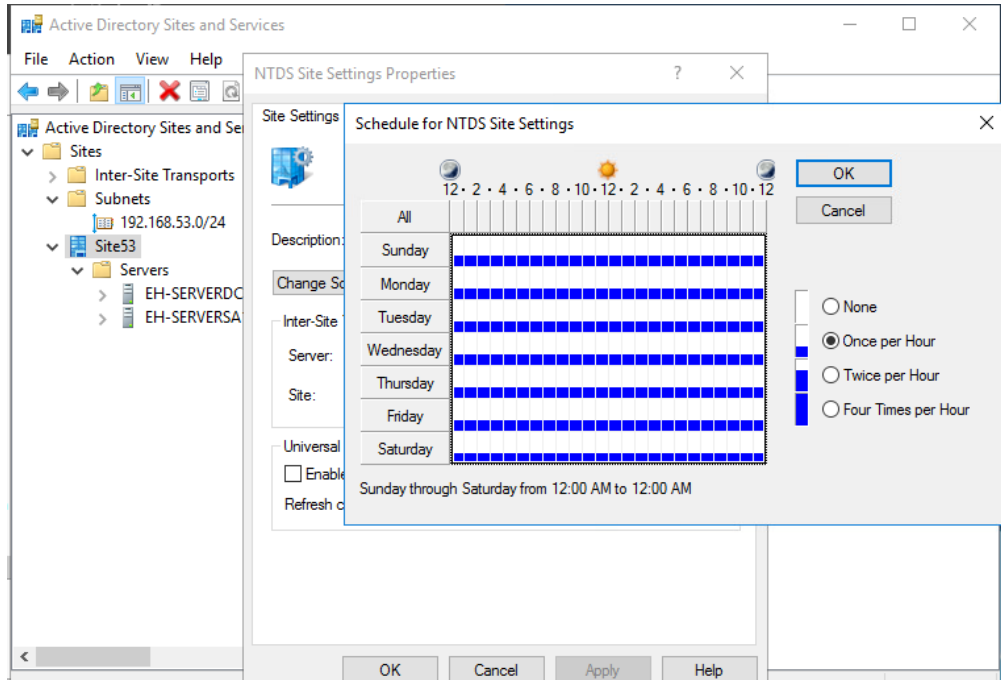


Figure 8: Intersite replication schedule

Activity 6-6:

Changing an RODC to a Standard DC

In this activity we will change the RODC to a standard domain controller

To start, we will first remove the DNS role from the RODC with the following powershell command

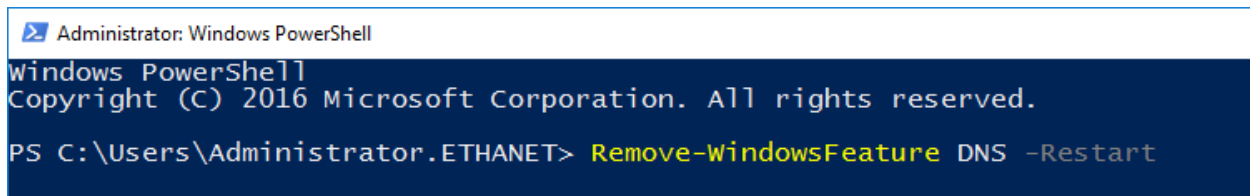


Figure 9: removing the DNS feature

After this we will then remove the Domain Controller function, which will just demote the machine from being a member server

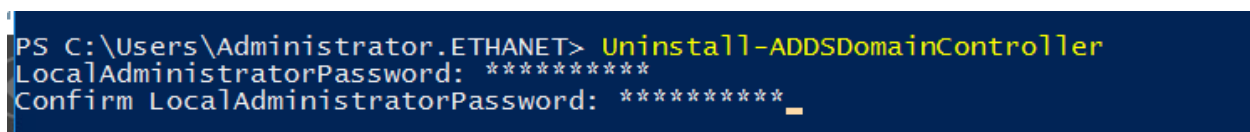


Figure 10: Removing the Read-Only domain controller

Activity 6-7: Transferring FSMO Roles

Once removed, the machine will again restart as to confirm the removing from the domain. Upon the restart, we will add the Active Directory Service back, but this time installing it without the ReadOnly parameter. After, we will transfer the Schema master role to SA1.

```
PS C:\Users\Administrator> Move-ADDirectoryServerOperationMasterRole -Identity EH-ServerSA1 -OperationMasterRole 3
Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'EH-ServerSA1.ethanet.ca' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
PS C:\Users\Administrator> Get-ADForest

ApplicationPartitions : {DC=DomainDnsZones,DC=ethanet,DC=ca, DC=ForestDnsZones,DC=ethanet,DC=ca}
CrossForestReferences : {}
DomainNamingMaster    : EH-ServerDC1.ethanet.ca
Domains               : {ethanet.ca}
ForestMode            : Windows2016Forest
GlobalCatalogs       : {EH-ServerDC1.ethanet.ca, EH-ServerSA1.ethanet.ca}
Name                  : ethanet.ca
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=ethanet,DC=ca
RootDomain            : ethanet.ca
SchemaMaster          : EH-ServerSA1.ethanet.ca
Sites                 : {Site53}
SPNSuffixes           : {}
UPNSuffixes           : {}

PS C:\Users\Administrator>
```

Figure 11: Transferring the Schema Master

We can now transfer this back to DC1 as this machine needs the schema role.

Activity 6-8: Creating a System State Backup

Here, we will install the Windows Server Backup role onto SA1, once this is done, we can then create the backup

```
PS C:\Users\Administrator.ETHANET> wbadmin start systemstatebackup -backuptarget:B:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Starting to back up the system state [2022-10-19 12:18 PM]...
Retrieving volume information...
This will back up the system state from volume(s) System Reserved (500.00 MB),(C:) to B:.
Do you want to start the backup operation?
[Y] Yes [N] No y
```

Figure 12: Backing up the domain config files for SA1

Once the backup is done, we can view the backup in the SA and see the folder that it has saved for us

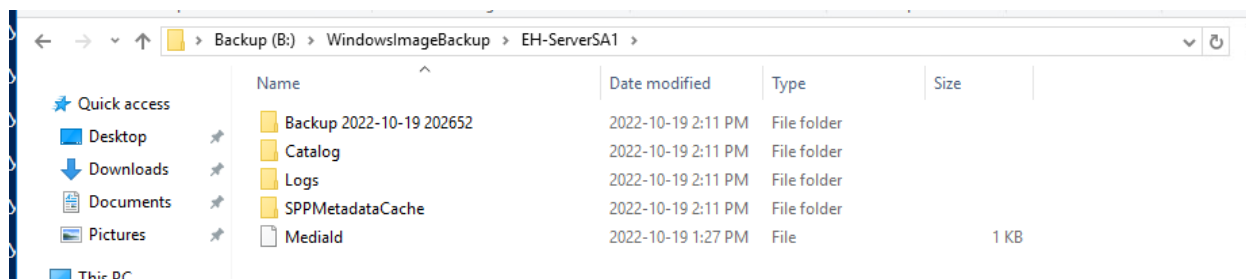


Figure 13: Completed backup

Activity 6-9: Restoring Active Directory from a System State Backup

In this activity, we will restore our deleted TestOU, and bring it back using our backup from the previous step.

To start, I first deleted the TestOU1 from the Users and Computers group

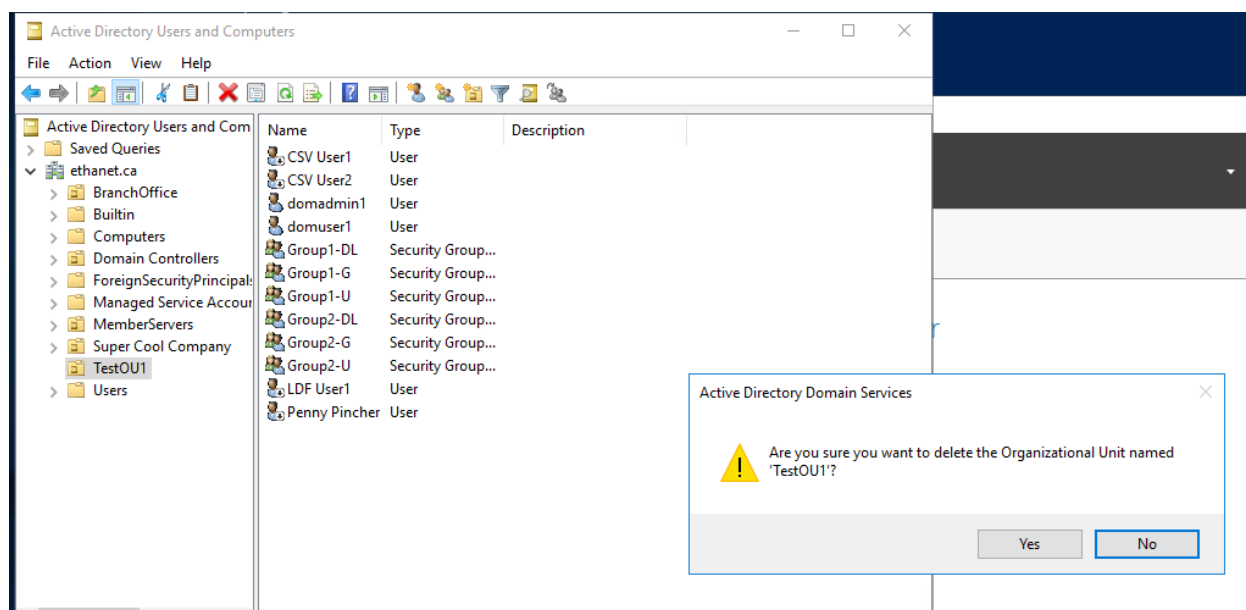


Figure 14: Deleting the TestOU1

We will then use msconfig to boot into safe mode with Active Directory repair

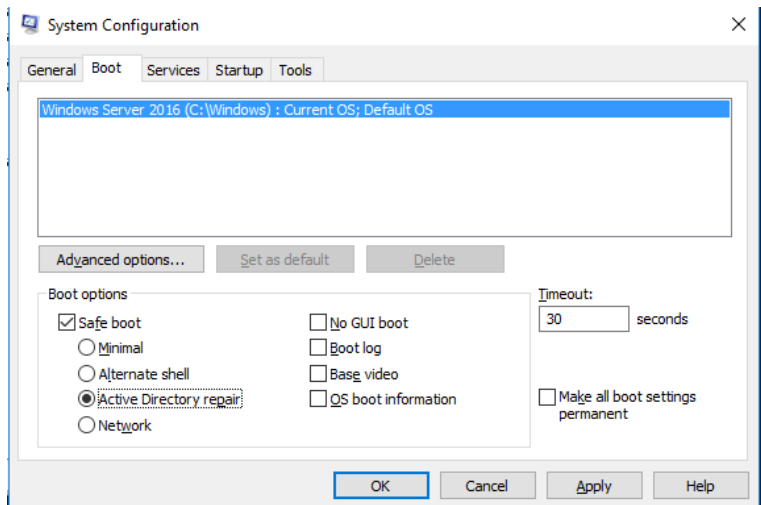


Figure 15: Booting into safe mode

Once we boot into the Safe Mode, we can then start the repair process of our Active Directory and bring back the TestOU

```
Administrator: Command Prompt - wbadmin start systemstaterecovery -version:10/19/2022-20:26 -backuptarget:B:
C:\Windows\system32>wbadmin get versions -backuptarget:B:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Backup time: 2022-10-19 1:26 PM
Backup target: 1394/USB Disk labeled B:
Version identifier: 10/19/2022-20:26
Can recover: Volume(s), File(s), Application(s), System State
Snapshot ID: {feb0b698-529d-40b3-94c1-597f10f9b985}

C:\Windows\system32>wbadmin start systemstaterecovery -version:10/19/2022-20:26 -backuptarget:B:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Do you want to start the system state recovery operation?
[Y] Yes [N] No y

Note: The recovery operation will cause all replicated content (replicated
using DFSR or FRS) on the local computer to resynchronize after recovery.
The rise in network traffic due to resynchronization may cause potential
latency or outage issues.
System state recovery cannot be paused or cancelled once it has started.
It will need a restart of the server to complete the recovery operation.

Do you want to continue ?
[Y] Yes [N] No y
```

Figure 16: System Recovery of the domain

We can then do then use ntdsutil and do an authoritative restore to bring back our OU

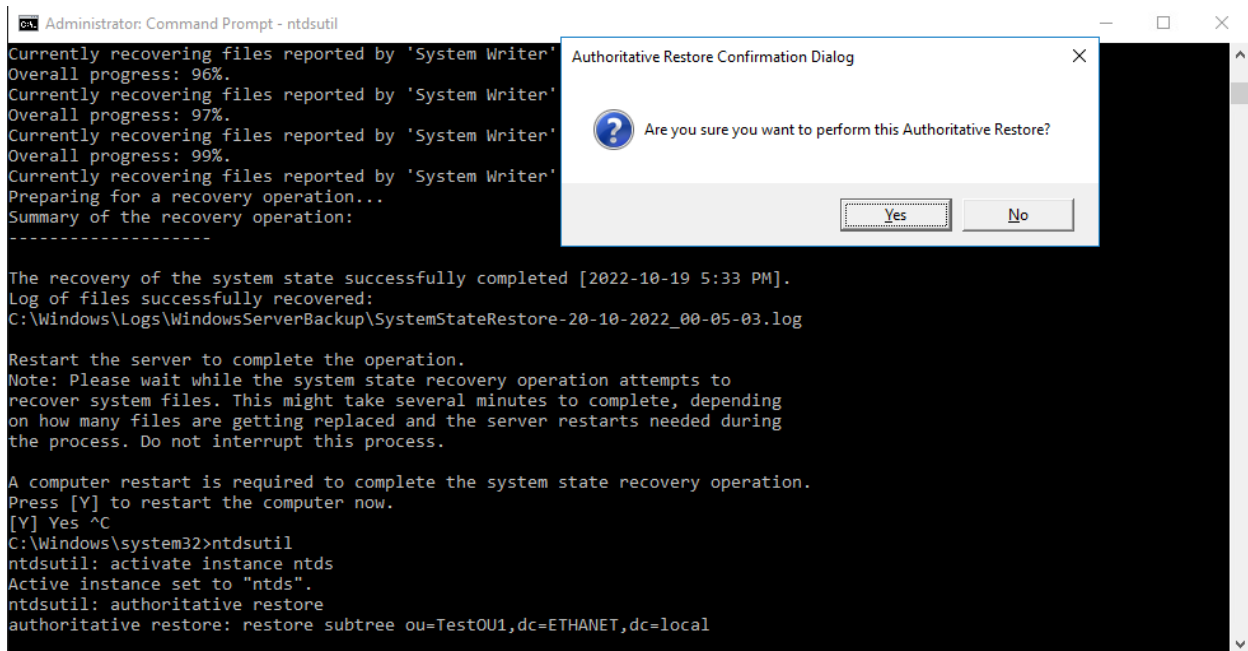


Figure 17: Doing an authoritative restore of TestOU1

Once this is completed, we can again use msconfig to remove safeboot and restart the machine. Once rebooted, we can sign into the server again.

Once we sign in, we see a message saying our restore was completed.

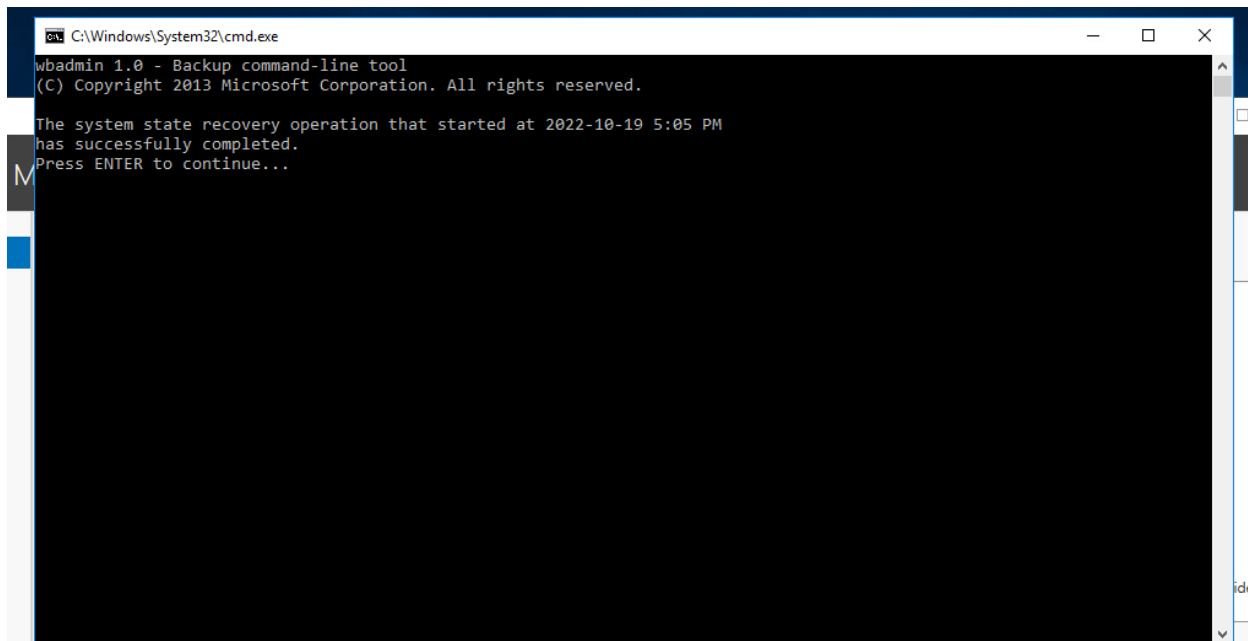


Figure 18: Login message after safe boot

And we can see from the figure below, it worked and TestOU1 was restored along with the users and groups inside of it.

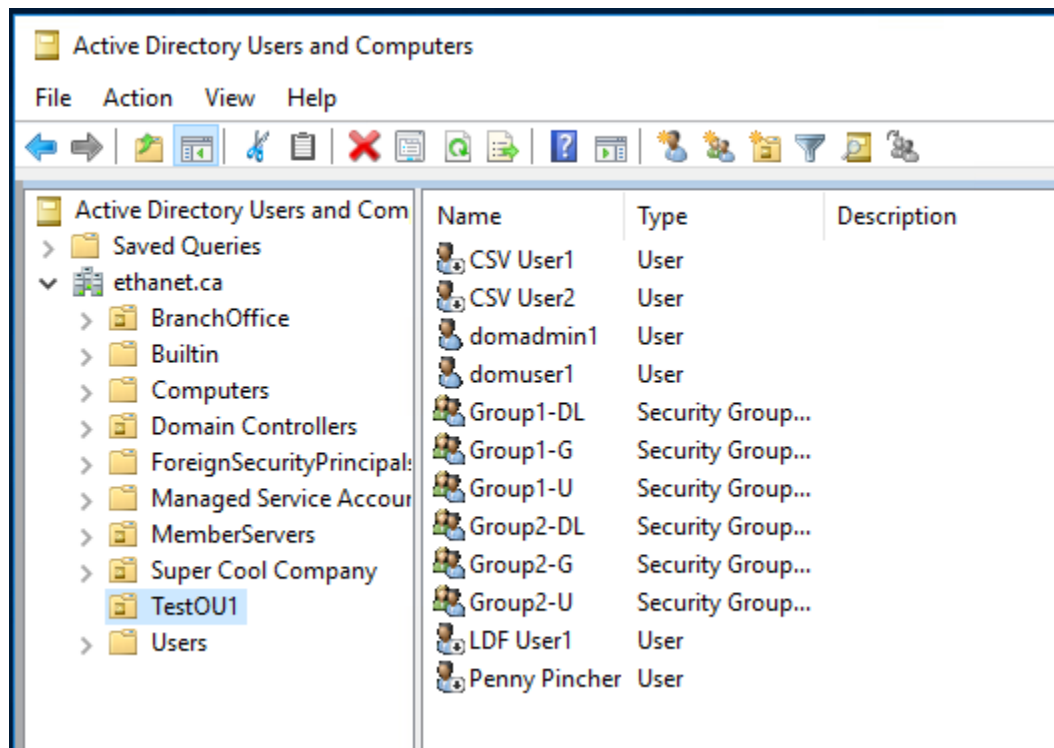


Figure 19: Restoration of the TestOU1 OU

Activity 6-10: Restoring Deleted Objects from the Active Directory Recycle Bin

In this activity, we will enable the recycling bin and restore items from the bin.

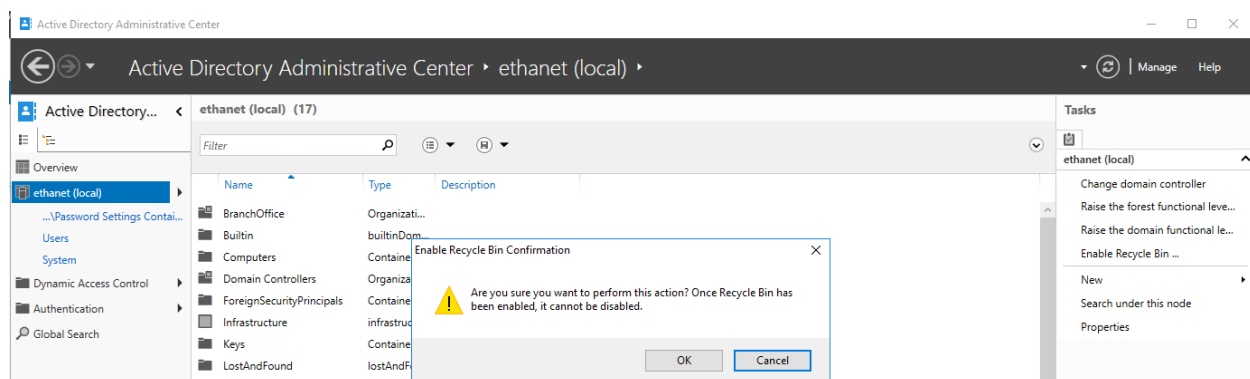


Figure 20: Enabling the recycling bin

After enabling the Recycling Bin from the ADDC, we can then delete things and start to test. I deleted a user account to test, and we can see in the deleted objects folder we can see the user there, we can then restore it with the “Restore” object on the right.

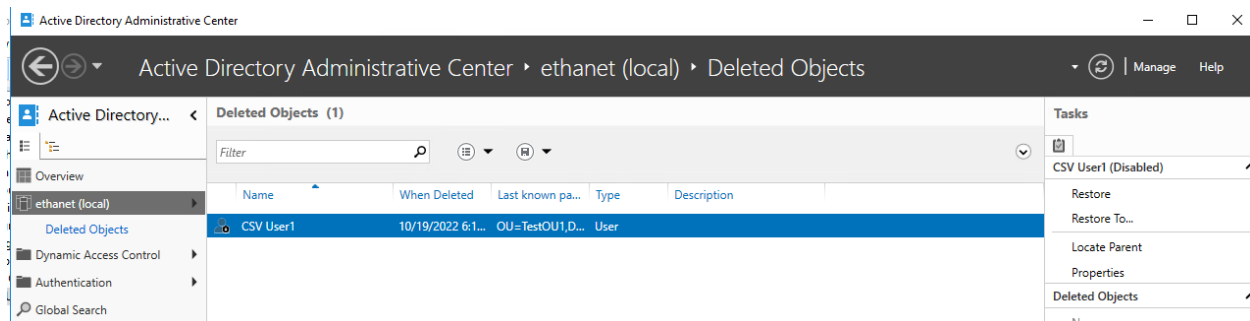


Figure 21: User in the Recycling Bin

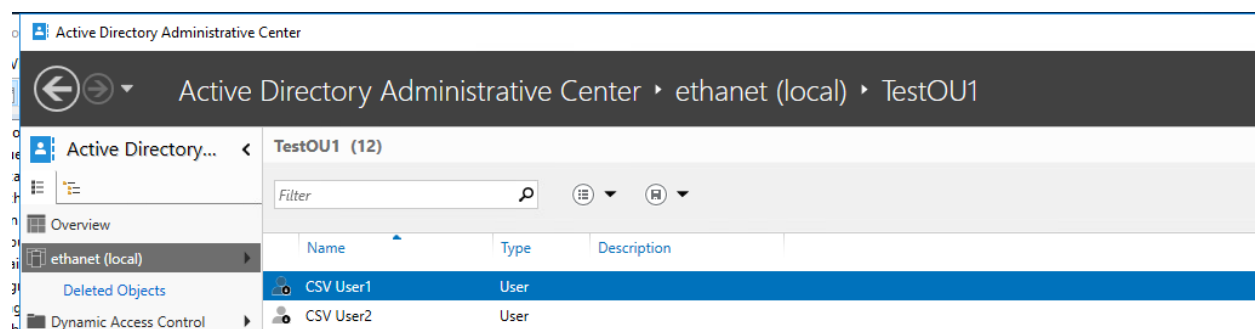


Figure 22: Restoring the user

We can then user Powershell to restore the Domuser1 account that we have deleted

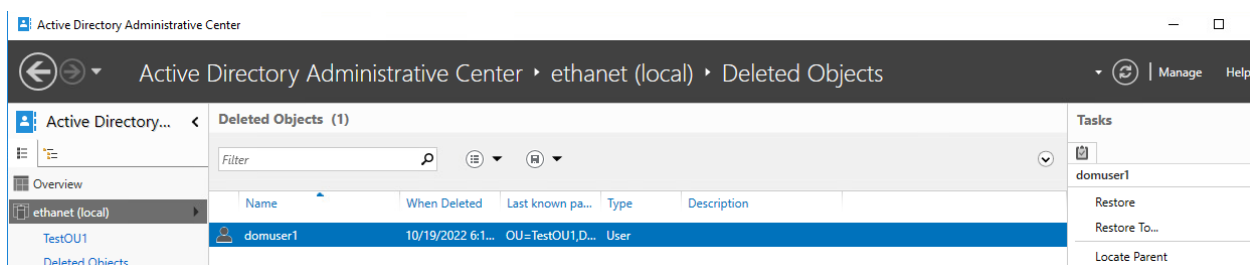


Figure 23: Deleting the user again

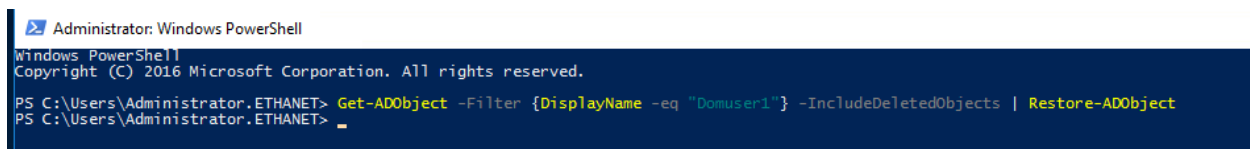


Figure 24: Restoring using Powershell

A refresh of the ADDC will show us that domuser1 was restored to the TestOU1

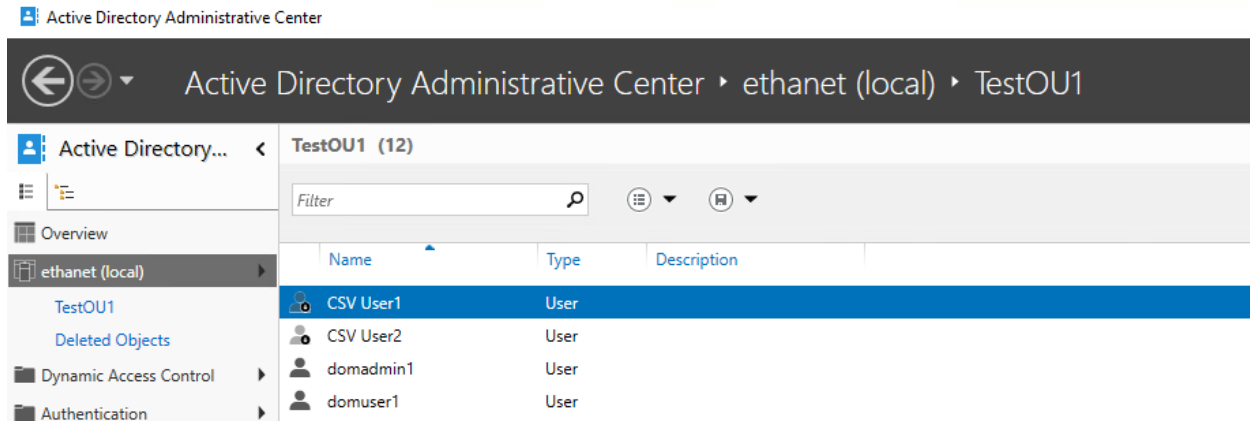


Figure 25: User is added back after a refresh

Activity 6-11: Compacting the Active Directory Database

After adding an alternative DNS entry that points to SA1 and making a tempAD and a backupAD folder in the C: drive, I will once again use ntds to compact the folders.

```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: compact to c:\tempAD
Initiating DEFRAGMENTATION mode...
Source Database: C:\Windows\NTDS\ntds.dit
Target Database: c:\tempAD\ntds.dit

Defragmentation Status (% complete)

0   10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
copy "c:\tempAD\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
del C:\Windows\NTDS\*.log
```

Figure 26: Compacting a file in the tempAD group

We can then copy our database to our backupAD file with the command below

```
C:\Users\Administrator>copy c:\windows\ntds\ntds.dit c:\backupAD
1 file(s) copied.

C:\Users\Administrator>_
```

Figure 27: Creating a backup of the database

We can copy the compacted database over the original with

```
C:\Users\Administrator>copy c:\tempAD\ntds.dit c:\windows\ntds\ntds.dit
Overwrite c:\windows\ntds\ntds.dit? (Yes/No/All): _
```

Figure 28: Overwriting the original with the compacted database file

And to run an integrity check we can use the following command

```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: integrity
Doing Integrity Check for db: C:\Windows\NTDS\ntds.dit.

Checking database integrity.

                Scanning  Status (% complete)

    0    10    20    30    40    50    60    70    80    90   100
    |----|----|----|----|----|----|----|----|----|----|
    .....

Integrity check successful.

It is recommended you run semantic database analysis
to ensure semantic database consistency as well.
```

Figure 29: Doing a database scan

After checking the databases, we can then start the Active Directory Service again with a “net start ntds”

```
ntdsutil: semantic database analysis
semantic checker: go fixup
Fixup mode is turned on

Opening DIT database... Done.

Done.

.....Done.

Writing summary into log file dsdit.dmp.0
SDs scanned:          128
Records scanned:      4064
Processing records..Done. Elapsed time 2 seconds.

semantic checker: quit
ntdsutil: quit

C:\Users\Administrator>net start ntds
The Active Directory Domain Services service is starting....
The Active Directory Domain Services service was started successfully.

C:\Users\Administrator>
```

Figure 30: Final database scan

Conclusion:

After this lab, I learned lots about the makeup of AD and how to create a RODC for an active directory, as well as how to authoritatively restore a machine, which are all helpful things to know in case I need them in the future.