**Assignment:** Domain Controller roles, backups and recovery.

**Required Resources**

* 2 x Windows Server (created in previous assignment)
* Windows 10 pro Workstation (created in previous assignment)
* Course Resources documentation as found on BrightSpace

**Professional Documentation**

All documentation must be done in a **professional style**. It must include:

* Title page
* **Updateable** Table of Contents
* Document introduction
* Section introductions or description, each section must be clearly identified
* Graphics or screenshots MUST include a title with a short description
* Any direct or copied quotes or graphics MUST be properly credited in a footnote
* ALL sources MUST be properly cited (APA format) and placed at the end of your document in a bibliography.
* **NO** embedded, zipped or compressed files. \*\* All scripts must be converted to text before including them in your documentation. \*\*
* **1 Professional Word Document ONLY.**

**Research and documentation sections** -Please complete all research and question responses in your own words. Research sections not completed in your own words may result in a mark of 0 for the section.

**NOTE:** Please do NOT copy and paste responses from internet, **even with a citation**. I expect each section or response to be in your own words. Be prepared to explain your responses and demonstrate your comprehension.

**No marks** will be given for cited or credited information included in document.

***\*\* I recommend completing any research section before completing any required task listed below as you will have a much better understanding of the material and data.***

**Evaluation:** This assignment is markedas per the attached Rubric (marks will be deducted for deviating from Requirements). \*\*You may be asked to demonstrate some of your assignment to show your comprehension of the material.

**Marking and Assignment Notes:**

* ScreenshotsMUST include user or device identifying information.
* Screenshots MUST be added to your document in the order of creation.
* Documentation must meet Professionalism requirements.
* **Automatic mark of 0 - Assignment not submitted or work not original.**

<http://www.nscc.ca/docs/about-nscc/policies-procedures/policy-studentcodeofconduct.pdf>

<https://www.nscc.ca/docs/about-nscc/policies-procedures/policy-academicintegrity.pdf>

**NOTE: This assignment may require some adaption, research and troubleshooting.**

**Task 1 – Create a Staged Read Only Domain Controller (RODC)**

\*\* You do NOT require an install log, change log or testing log for your RODC.

A Read Only Domain Controller is an option to allow you to create a Domain Controller in a secondary location where physical security or access may be an issue. It allows you the speed of authenticating locally but the security of housing your Domain Controller in your main data centre.

Staged RODC installations allows the Domain Administrator who has access to the Primary Domain Controller to preset the RODC and allow a local user to complete the setup.

We will use PowerShell for a large part of this assignment including our RODC staging and setup.

We may use some commands we are familiar with, but we will also be using some new commands. So, we will take this opportunity to create a **PowerShell reference document**.

* Record each line of code used or identified in this assignment
* Add a short definition to each line to explain what the code is doing
  + If the code contains arguments or switches make sure to explain each
* Add your reference document as an **Appendix** to your professional document.

Now we must create a new Server

* Create a new Read Only Domain Controller (RODC)
* As this is a third server we will be adding to our environment we will use the following minimum specifications:
* Windows Server 2019 Standard (**CORE**)
* Memory = 4G
* Default processors and cores
* 2 NICs set to NAT
* Drive partition information (1x 80g)
* Time and currency = English Canada
* Use **KMS** key for Server 2019 Standard
* Administrator password = **ROPassw0rd**
  + Password does not expire
* Set correct Time Zone
* **Do NOT add your new server to your domain at this time**
* Assume your new server will be on Rack 1 in U 30
* Server name (Hostname) as per Naming Convention
* Perform all critical and/or recommended Windows Updates
* Server IP Info
  + NIC 1
    - IP = 192.168.208.15 /24
    - Gateway = 192.168.208.2
    - DNS:
      * Primary = DNS Server
      * Secondary = DNS Server
  + Nic 2 = DHCP
* Update your VM description to capture Create information and login information.
* Confirm/install VMWare Tools
* Create a VMWare snapshot
* Reminder: We will NOT create an Install/Change Management Log for this server as this is for testing purposes ONLY.

Now we will need to switch servers to setup our remote office information and account

* Log into your Member Server as your System Operator
* In AD (Active Directory) create a new Organizational Unit (OU) in the root of your domain called RemoteOffice and protect it from accidental deletion.
  + Example: Distinguished Name = *OU=RemoteOffice,DC=mad,DC= netw2500,DC=ca*
* In your RemoteOffice OU create a new user with these settings
  + First Name, Initials and Last name = blank
  + Full name = Remote Administrator
  + User Logon name = remoteadmin
  + Do not make any other changes and select “Next”
  + Password = Radmin@2024
  + Password never expires
  + Modify your new user account as noted:
    - Description = Remote Office Administrator
    - Office = Branch Office
* In your RemoteOffice OU create a new Global Security Group called **RemoteOff\_gp** with the description Remote Administration Group.
* Add our RemoteOff\_gp group to our Domain Admins group.
* Modify your Remote office Administrator and add them as a member of RemoteOff\_gp .

Currently our Primary Domain Controller is running Server 2022 Core and all functions levels are set for support during the install. Let’s review and confirm our function levels for our DC server.

First let’s view our current function levels for confirmation

* On your **Primary Domain Controller** open a PowerShell Console
* In order to assist us with troubleshooting we will keep a Transcript of all our PowerShell cmdlets and command.
* Use the following command to Start your Transcript. Note: If for any reason you stop this assignment before you get to the end of your transcript requirement you MUST start it again and append the original transcript to capture your entire PowerShell history.

Start-Transcript -Path "C:\PDCtranscriptA3.txt" -NoClobber

* Now we must confirm we have the required PowerShell module to complete this task.
* Run the cmdlet

Import-Module ActiveDirectory

* Now run the cmdlets below to view the current function levels and out put the results to a text file called **C:\Reports\FLReport.txt** and add a copy to your documentation. \*\*Make sure to append your file so you capture all required results. **NOTE**: You may need to create the Reports directory on root of C first.
  + Function Levels:
    - Forest Mode = Get-ADForest
    - Domain Mode = Get-ADDomain
* **Question 1**. Review your FLReport File and answer the following questions. What is your Forest and Domain function levels identified in your commands. What are function levels and why are they set as recorded in your report?
* Make sure to keep your transcript running as you complete the next section or create a NEW transcript called C:\PDCtranscriptA3\_2.txt

Now that we have determined our function levels we are ready to setup our prestaging for our Read Only Domain Controller (RODC)

* On your Domain Controller open a PowerShell Console

**NOTE:** All one line of code.

Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName "yourRODCServerHostName" -DomainName "yourDomainName" -SiteName Default-First-Site-Name -DelegatedAdministratorAccountName “RemoteOff\_gp”

**NOTE**: You may see a warning message about security channel sessions, but you can ignore, it is just a warning. Your script should complete with the Message **Operation completed successfully.**

* Stop your Transcript before continuing forward. **Add** a copy of your Transcript to your documentation.
* If required, log onto your **Member Server**
* In your Active Directory Users and Computers, right click on your Domain Controllers OU

You should now see two Domain Controllers. Note that the new Domain Controller has a DC Type of Unoccupied DC Account (Read-only…).

* **Stop.** Take a screenshot of the contents of your Domain Controllers OU and make sure to include your Name, Type, and DC Type (make sure to capture the entire column) but not your Site or Description and add it to your documentation. **Note**: You may need to expand your DC Type column to view the full content.

Now will complete our setup of your Read Only Domain Controller (RODC).

* If required, log back on to your RODC as the **local** Administrator

We will need to install the Active Directory server role

* Open an elevated PowerShell console and **start a Transcript** called C:\RODCtranscriptA3.txt don’t forget to use the no clobber argument.
* Let’s start the install with the following code.

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

* Press Enter (this install may take some time) but you should receive verification of success.
* Now complete the install with the remaining code.

**NOTE:** All one line of code.

Install-ADDSDomainController -DomainName “yourDomainName” -UseExistingAccount -Credential (Get-Credential) -NoRebootOnCompletion:$True

* Press Enter
* In the credentials dialog complete with **domain\remoteadmin** and password created earlier
* You will also be prompted for a SafeModeAdministratorPassword. (This is the DSRM password), use “Passw0rd” for your DSRM password. **Stop**. Make sure to record this information in your VMWare Console View as you may need it later.
* You will then be notified that “The target server will be configured as a domain controller and restart……” the default option is Yes so hit Enter to continue
* After your role is installed your server will not restart automatically
* **Stop** your transcript and reboot your server.
* **Add** your transcripts and reports from both server that contain all the correct commands and data to your documentation as a text. Do **NOT** take screenshots.
* Log back into your RODC as the **Domain** Administrator

While your RODC is restarting let’s confirm it updated correctly

* Move back to your Member Server
* Select your Domain Controllers OU and refresh
* Your RODC should now have a DC Type of Read-Only, GC
* **Stop**: Take a screenshot of your DC type showing **Read-Only, GC** and add it to your professional Documentation.

\*\**Troubleshooting hint:* if your server fails to create your RODC uninstall your Domain Controller role from your RODC. Then review the error message and logs regarding why you failed. Error messages are the best way to determine where an error is arising from. Troubleshoot and correct all errors. Once corrected reinstall your role.

*Additional Learning: Read Only Domain Controllers do not contain passwords by default but process passwords and request to change passwords by passing them to a writable domain controller. You can allow some passwords to be cached on the RODC for certain groups to allow easier or quicker access.*

*Additional Reading:*

<https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/understanding-8220-read-only-domain-controller-8221/ba-p/395031>

<https://www.rebeladmin.com/2014/10/password-replication-in-rodc/>

<https://petri.com/controlling-password-replication-read-domain-controllers/>

<https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adod/84f88bd0-ba4d-4d27-83ec-5d6149e3390b>

We will now allow password replication by modifying our Password replication policy

* Log into your Member Server as your **Domain Administrator**
* Open Active Directory Users and Computers
* Open the properties of your new RODC
* View your current Password Replication Policy
* Click Advanced

Note that there are only two accounts stored on the RODC. One is the RODC computer account and the other is a special account used by the Kerberos authentication process.

Follow the instructions below to add our existing RemoteOff\_gp to the member of the Password Replication Policy.

* Close both your properties windows and open an elevated PowerShell Console
* Create a new session between your Member Server and your DC
* Run the following on your DC using your PowerShell session

**NOTE:** All one line of code.

Add-ADGroupMember "Allowed RODC Password Replication Group" RemoteOff\_gp

Let’s confirm our group was made a member of the correct permissions group.

* If required, open Active Directory Users and Computers
* Open the properties of your new RODC
* View your current Password Replication Policy
* Select the Allowed RODC Password Replication Group and double click to open the group
* View the group members
* If you your RemoteOff\_gp was not added then repeat the steps above.

Let’s test our replication

* Log into your RODC with your RemoteAdmin account
* Return to your Member Server
* Follow the previous steps to update your Domain Controllers OU and view the **Advanced properties** of your RODC Password Replication Policy. You should now see your Remote Administrator account has been added.
* **Stop**: Take a screenshot of your RODC Password Replication Policy with correct settings and all logged in users and add it to your professional Documentation.
* We have made a lot of changes by adding a new server. This would be a great time to shut all your servers down and **take a snapshot of each one in the Off state**.
* **Remember**. **When starting your server your Primary Domain Controller MUST be fully loaded and all services started before starting your other servers.**

**Task 2 - Create an Active Directory (AD) Sites and Services subnet and change your RODC to a Secondary Domain Controller**

* Log on to your Member Server as your **Domain Administrator**
* Open your Active Directory Sites and Services
  + **Note**: Don’t forget your RSAT tools for AD Administration
* Expand your Sites
* Add a new Subnet
  + Prefix = 192.168.208.0/24
  + Site Object = Default-First-Site-Name
* Modify the properties of your new subnet by adding a description:
  + Created by: “YourNameHere”
* Select your Default-First-Site-Name and rename it to NETWSite
* Open the properties for NETWSite
* Edit your description to “Site for 192.168.208.0/24”

Now let’s confirm our new Site subnet

* In your Active Directory Sites and Services console, expand your NETWSite /Servers/ you should now see both of your domain controllers
* Expand your DC
* Select your NTDS Settings\Properties
* Select the Connection Tab
* Confirm your RODC shows in your Replicate To:
* Repeat the steps to view the RODC connection information
* **Stop**: Take a screenshot of your NTDS Connections setting that shows your To: and From: for both servers and add it to your professional Documentation.
* **Notice which servers replicate to and from which server.**
* If everything is confirmed cancel out of this window

Now that we have confirmed our replication is setup correcting for our new Subnet and Site we will modify our replication schedule.

* Select your NETWSite in the left pane
* Select on your NTDS **Site** Settings properties from the right pane
* Select Change Schedule
* Notice that your schedule is set to once per hour by default, since a lot of changes can happen in an hour lets increase our replications
* Change your schedule to twice per hour
* **Stop**: Take a screenshot of your new replication settings and add it to your Documentation.

\*\* We will not be using our ReadOnly Domain Controller for the remainder of this assignment so we can take a Final Snapshot and create a Final Gold Copy.

**Task 3 – Roll back RODC and remove from Domain. NOTE**: As noted earlier, some additional troubleshooting may be required for this section.

* We are about to make a major change to one of our servers. This would be a great time to shut all your servers down and **take a snapshot of each one in the Off state**.
* **Remember**. **When starting your server your Primary Domain Controller MUST be fully loaded and all services started before starting your other servers.**
* Log on to your **RODC** as your Domain Administrator (if required log off your Remote Admin account first)
* Open a PowerShell Console execute the following command to demote your RODC back to a member server

Remove-WindowsFeature DNS -Restart

* This may take a few minutes to remove the feature
* Your server should now restart automatically

Now let’s remove any unrequired rolls or features so we can start fresh.

* Log on to your RODC as your **Domain** Administrator
* Open a PowerShell Console and execute the follow command

Uninstall-ADDSDomainController

* When prompted use the **local** administrator password.
* Hit enter to select yes as the default
* Once complete the server will restart automatically

Now we will check to confirm our server has been removed from our list of DCs and is shown as a member server only.

* Log into your Member Server and open Users and Computers
* Confirm your Domain Controllers only list your Primary DC and your RODC is now listed under computers along with your Member Server. Do NOT delete your RODC from your computer list.

Looks like the RODC has gone back to being a member server but we need to remove it from the domain so we can make some changes to it.

* Log back on to your RODC as **local** administrator
* Modify your RODC hostname to reflect it’s usage as a Secondary Domain Controller.

Some of your IP settings may have been modified when we installed the Read Only Domain Controller role and removed DNS on your RODC

* Confirm your NIC 1 IPv4 settings are as identified previously (\*confirm correct DNS settings)
* Confirm your second NIC is set **DHCP for IP and DNS** (remove loopback if required)
* Check your IP settings in an elevated PowerShell Console and use the command:

Get-NetIPConfiguration

We will now need to remove our RODC from the domain temporarily to clear out all the residual settings from our RODC role.

* Remove your RODC from the domain and place in a workgroup called “temp” restart when prompted.
* After your RODC is restarted
* Our RODC will now show as “Disabled” in our Active Directory Users and Computers\Computers, (*notice the arrow at the bottom of the icon*) **delete the server from the list**
* Since we will be creating a new Secondary Domain Controller modify your server host name to follow the naming convention.

**\*\* NOTE:** the changes made recently may affect your local Recycle bin and you may receive an error when logging into your Secondary Domain Controller with an established domain account. Please ignore the error.

* **\*\*This would be a great time to make snapshots of your all of your servers in the off state before we complete the next task.**

**NOTE**: Now that we will have 2 domain controllers it is important, we pay attention to connections and replication information. Particularly with our snapshots. In order to keep our replication in order we will make sure to always take a snapshot of ALL domain controllers at the same stage and if we require a rollback, we will rollback ALL domain controllers to the same stage.

**Task 4 – Create a new Secondary Domain Controller (SDC)**

Once your Secondary Domain Controller Server (SDC) has restarted let’s add it back to the domain as an additional domain controller

* Since we have setup a NEW Secondary Domain Controller it is important to capture all our settings and modifications in an **Install/Change Management Log**. (Remember, you require one for each NODE, excluding clients).
* Log in as the local administrator
* Add the Domain Controller Role to Secondary Domain Controller (SDC) and add your new SDC server to your domain. \*Notice we do not need to install DNS as it already exists on our PDC.

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Import-module ADDSDeployment

* Complete the process by editing and applying the following script. \*\* make sure to edit the **required** information.

**NOTE:** All one line of code.

Install-ADDSDomainController -NoGlobalCatalog:$false -CreateDnsDelegation:$false -CriticalReplicationOnly:$false -DatabasePath “C:\Windows\NTDS” -DomainName “DomainNameHere” -InstallDns:$False -LogPath “C:\Windows\NTDS” -NoRebootOnCompletion:$false -SiteName “OurNewSiteNameHere” -SysvolPath “C:\Windows\SYSVOL” -Force:$true -credential (Get-Credential)

* Set your DRSM password to the same DSRM password as your PDC.
* You may receive a selection of warning but no errors. You will receive a confirmation of success once complete.

Once you have installed your Domain Controller role and your server has restarted we will need to confirm our SDC was added correctly to our domain and confirm it is a secondary domain controller and not a primary domain controller.

* Restart your SDC server if it did not already done so at the end of the install.
* Login in to your SDC at least once as the **Domain Administrator** to complete the install.
* If required, log into your Member server as your systems operator
* Take a minute to add the new SDC to your managed servers (All Servers) on your member server
* Open your Active Directory Users and Computers on your Member Server
* Confirm your new SDC in the Domain Controllers OU \*Notice it now shows as a Global Catalog Server

Let’s confirm which server is our Primary Domain Controller and contains the required Master Role.

* In your Active Directory Users and Computers right click on your domain
  + Select Operations Masters
  + Select PDC
  + Note the Operations master in your list
  + If it is NOT your original DC you must remove your SDC and move your SDC back to a work group and repeat the previous steps.

Now we will confirm replication is supported between our two domain controllers

* Open your Active Directory Sites and Services on your Member Server
* Navigate to your NETWSite and expand to view the entire list of servers
* Attention: You may see your RODC still listed, this is because all your modifications have not yet replicated. Your may delete the RODC from your list in order to remove any confusion.
* Select the NTDS Settings for your PDC in the **left hand window**
* In your right hand pane **right** click on your <automatically generated> and select Replicate Now
* Repeat the process for your SDC
* If replication fails for either domain controller you must troubleshoot the issue and repeat.
* **REMINDER**: Make sure to update your VMWare Console view details for your SDC if you have not already done so.
* Check your NTDS Settings Properties/connections. Notice the settings for the SDC and PDC.
* **Stop.** Be Prepared to demo replication between domain controllers.

***Reminder****. Remember to always* ***start*** *your servers in the correct order:*

* + ***Primary Domain Controller*** *and all services*
  + ***Secondary Domain Controller*** *and all services*
  + *Any additional member servers or clients*
  + ***Note: Shutdown*** *of server should be in the reverse order.*
* **Stop**. This would be a great time to make snapshots of your PDC, SDC and Member Server. \*Remember, from now on we must keep our snapshots for each server in line with the other due to AD replication.
* **Stop**. This would be a great time to update our Install/Change Management Logs.

**Task 5 - Backing up and recovering Domain Controllers and Active Directory**

Before we can create any backups we will need to setup your backup directory and install the Windows Server Backup Tool

* Log onto your Primary Domain Controller as the Domain Administrator
* If you have not already done so we will need to put our second drive online, initialize it and create a new volume using the drive letter E
* In PowerShell execute the following commands (in blue) to create your E drive

Get-Disk (*confirms our disk exists and identify our disk number*)

Set-Disk -Number "DiskNumberIdentified" -IsOffline $False (*puts disk online*)

Initialize-Disk -Number "DiskNumberIdentified" (*initializes disk*)

**NOTE:** All one line of code.

New-Partition -DiskNumber "DiskNumberIdentified" -UseMaximumSize -DriveLetter E (*creates a new volume and assigns drive letter E*)

Format-Volume -DriveLetter E (*formats volume*)

Get-Volume (*confirms volume configuration*)

* Now we will open your Active Directory Users and Computers on your Member Server to create some objects we will use to test with.
* Create a new Organizational Unit in the root of your domain called TestBK (Do **NOT** select “Protect container from accidental deletion”
* Create a Test User inside your TestBK1 OU
  + Full Name = Test User 1
  + Logon name = TestUser1
  + Password = Passw0rd123
  + Password set to never expire

Now we will need to install our Server Backup feature

* In order to speed up our backup process we will shutdown all server except our PDC **\*Remember to follow your shutdown order.**
* Open a PowerShell Console on your PDC and execute the following command

Install-WindowsFeature Windows-Server-Backup

* Your result should show **Success=True** if this is not the result troubleshoot the issue before continuing.

Now we will need to start our system backup state

* In your PowerShell Console type

wbadmin start systemstatebackup -backuptarget:E: *(note the 2 colons)*

* Select yes to start your backup of your system state

***\*This can take some time to complete your system state backup on your new drive.***

***“The key to everything is patience. You get the chicken by hatching the egg, not by smashing it.”***

***– Arnold H. Glasow***

Since we have some time while our backup process runs, let’s do some research and research the following questions.

**Question 2.**

What is a System State Backup and what is included in a System State Backup?

What is a Bare Metal Backup?

**Question 3**. Notice your system is creating Shadow Copies of your volumes.

What are Volume Shadow Copies (VSS)? In your professional document write a short description of Volume Shadow Copies (VSS), make sure to include a description of:

* + Volume Shadow Copy Service (VSS)
  + Shadow Copies and Shadow Copy Sets
  + Providers
  + Requesters
  + Writers

So we have created a successful backup of our Active Directory and PDC. Let’s test it.

* Navigate to your PDC **E:\windowsimagebackup\”servername”\**
* Use the PowerShell command to view the contents of your E:\windowsimagebackup\”servername”\ directory
* Now that we are confident our System State backup was successful, we will start our remaining servers. **\* Remember your start up order.**
* Open your Active Directory User and Computer on your Member Server
* Delete your TestBK OU and contents we created earlier
* In the Confirm Subtree Deletion box select the “Use Delete Subtree server control” checkbox. (allows protected objects to be deleted)
* Refresh your domain OU and confirm you no longer see your TestBK OU

**STOP: This a great time to take another snapshot of your PDC and SDC and create a NEW Gold Copy as we going to Restore our Active Directory from our backup we created.**

**\*\* Remember** the shutdown and startup order for servers and clients.

**STOP: This a great time to update your Install/Change Management Logs.**

Ok, now we are ready to restore from our backup.

* Shutdown all your servers with the exception of the PDC
* Execute the following command to boot into Directory Service Repair Mode

bcdedit /set safeboot dsrepair

shutdown /r /t 0

* Sign in with **local** administrator (you will need to change your login user (esc)) and DSRM Password if required
* Completed repair by executing the following command in PowerShell

wbadmin get versions -backuptarget:E:

* **Stop.** Take a screenshot of the “version identifier” of your most recent backup, you will need this shortly.

**Example.**



Now we will do a recovery of our system state.

**\*This can take some time to complete your system state recovery from your drive.**

***“Patience is not the ability to wait but the ability to keep a good attitude while waiting.” - Joyce Meyer***

* Begin your recovery by executing the following PowerShell command

**NOTE:** All one line of code.

wbadmin start systemstaterecovery -version:VersionIdentifierRecordedAbove -backuptarget:E: -quiet

* If prompted to start the recovery hit enter to select yes
* \*\*\*\*When the recovery is complete **do NOT restart the server**, first we need to authorize the restoration.

\*\***User Ctrl+C to break out of the current session and quit wbadmin**

* While still in your console, type

ntdsutil

* Then type

activate instance ntds

* Then type

authoritative restore

* Then type

**NOTE:** All one line of code.

restore subtree ou=TestBK1,dc=yourinitials,dc=netw2500,dc=ca

* When the authoritative restore confirmation box opens click yes to confirm.
* Then type quit and press enter
* Then type quit and press enter **AGAIN**
* Then run the follow command to exit repair mode and reboot into your Windows server

bcdedit /deletevalue safeboot

shutdown /r /t 0

**NOTE:** Your server may ask to restart several times to complete the recovery

***Notice that we were not required to restore the entire server system state but able to select only the portion we required restored.***

* When your server has completed the recovery, log onto your Primary Domain Controller as your domain administrator.
* The system state recovery might need to complete some final tasks then display a message “Completed Successfully”
* Press enter when prompted
* Restart your PDC one more time to confirm our restoration has completed
* Ok, let’s confirm our restore was successful
* Restart your other server in the correct startup order
* Open your Active Directory Users and Computers on your Member Server
* Select your TestBK OU and confirm your objects have been restored

Restore from System State is great for large issues but there must be an easier way to restore for a few small accidental deletions.

* If required, Log on to your Member Server
* In your Server Manager / Active Directory Administrative Services select your domain
* In the right pane Enable Recycle Bin
* You will see a message saying we cannot reverse this decision, click OK
* If you receive an error that your directory partition has not replicated successuly at least once you may need to manually force replication from your Active Directory Sites and Services
  + Open Active Directory Sites and Services
  + Expand your NETWSite/Servers/”SDC Server”
  + Select NTDS Settings for your SDC Server
  + From the right hand pane right click on your server
  + Select Replicate Now
  + Repeat your step to Enable Recycle Bin
* You should now see a message telling you to refresh the Active Directory Administrative Center click OK
* Refresh the Active Directory Administrative Center
* You should now see a directory called Deleted Objects

Now let’s test our Recycle Bin

* Create a new Organizational Unit in the root of your domain called TestBK2 (Do **NOT** select “Protect container from accidental deletion”
* Create a Test User inside your TestBK2 OU
  + Full Name = Test User 2
  + Logon name = TestUser2
  + Password = Passw0rd456
  + Password set to never expire
* From your Active Directory Administrative Center **delete** your TestBK2 OU
* If required, in the Confirm Subtree Deletion box select the “Use Delete Subtree server control” checkbox. (allows protected objects to be deleted)
* Refresh your Active Directory Administrative Center
* Force replication between your Domain Controllers
* Log back onto your Member Server
* If required open your Active Directory Administrative Center
* Refresh your Active Directory Administrative Center if already open
* Confirm your TestBK2 is no longer in your list
* Double click your Deleted Objects directory
* You should now see your TestBK2 OU and TestUser2
* Select both (hold ctrl key) and then select Restore from the right hand pane
* Update your Active Directory Administrative Center
* Confirm your OU has been restored
* OK, one more time with PowerShell. Let’s delete just our TestUser2 this time
* Open a PowerShell console on your PDC
* Run the following command to delete your TestUser2 account (do NOT delete the Test OU)

Remove-ADUser -Identity “User’s Distinguished Name”

* \*\* Note, your deleted object will not show in your deleted items immediately, you may force replication to speed the process if you like.

Now let’s restore the user

* Open a PowerShell console on your PDC
* Run the following command to restore your TestUser2 account

**NOTE:** All one line of code.

Get-ADObject -Filter {DisplayName -eq “User’s Display Name”} -IncludeDeletedObjects | Restore-ADObject

* Refresh your Active Directory Administrative Center if already open
* Confirm that your User has been restored successfully. \*\* Note, your deleted object will not show as restored immediately, you may force replication to speed the process if you like.
* **Stop.** Be prepared to demo successful deletion and recreation of test user with command and from Recycle bin.

It is important to keep an up-to-date record of all changes and modifications made to your servers and have a reliable copy available as backup.

* Take a final snapshot of **ALL** your servers in the **OFF** state.
* Make sure to update your Gold copies of **ALL** your servers.
* Update your Install/Change management logs.
* Capture a screenshot of your Gold Copy properties for **EACH** server and add to your documentation.
* **Upload all your change logs to BrightSpace.** You may upload each one separately or include them in your formal documentation.
* **Upload your professional documentation to BrightSpace.**

**Marking Rubric**

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **In class marking** |
| 4 | Virtual Machine has correct system settings for **Server**. |
| 2 | VM Description contains all required information including RODC details. |
| 1 | Open FLReport on domain controller in correct location. |
| 2 | Open PDCTranscript and show you captured the required commands and results: |
| 3 | Disabled RODC server in AD with original correct hostname. |
| 4 | AD lists PDC and SDC in domain controller as a Global Catalog (GC) servers with the correct site. |
| 2 | AD \ Domain \ Operations Masters are listed in your PDC. |
| 2 | SDC has been added to All Servers on Member Server |
| 3 | Sites and Services New Subnet Properties |
| 5 | Demo NETWSite servers have correct NTDS Settings connections  Replication is successful between both servers. |
| 4 | Confirm successful image backup with correct content |
| 4 | Demo successful deletion and restoration test user with commands. |
| 4 | Demo successful deletion and restoration of from Recycle Bin |
| 6 | Snapshot of all 3 servers with correct time details |
| **46** | **SUB TOTAL** |
|  | **Documentation Submitted to Brightspace** |
| 2 | Copy of **FLReport** with correct contents |
| 2 | Copy of **PDCtranscript** with correct content |
| 3 | Screenshot of the contents of your Domain Controllers OU and make sure to include your Name, Type, and DC Type (make sure to capture the entire column) but not your Site or Description and add it to your documentation. **Note**: You may need to expand your DC Type column to view the full content. |
| 5 | Copy of **RODCTRanscript** with correct content |
| 2 | Screenshot of your Domain Controller OU with correct details for RODC |
| 2 | Screenshot of Remote Admin in RODC Password Replication Policy with correct settings and users. |
| 2 | Screenshot of NTDS Connection for both DC and RODC servers (TO and From) with correct results. |
| 2 | Screenshot of your new replication settings for NTDS |
| 2 | Question 1 |
| 2 | Question 2 |
| 1 | Screenshot of the “version identifier” of your most recent backup |
| 4 | Question 3 |
| 3 | Screenshot of each of your Gold Copy properties with correct details. |
| 5 | Install/Change Management logs contains all required changes, configurations and notes but is NOT a copy paste from assignment. |
| 5 | **PowerShell Reference Document** includes Code Log kept throughout assignment and posted in Appendix of document. |
| 2 | Document meets professionalism requirements as per page 1 of assignment. |
| **44** | **SUB TOTAL** |
| **90** | **Total Marks possible** |