**Assignment 4:** Creating and managing users, Active Directory and Group Policy and system maintenance.

**Required Resources**

* 3 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.**

**NOTE: Some research WILL be required for the completion of this assignment. You may use previous assignments and the internet as a resource but make sure to record all resources in the correct format in your documentation.**

**NOTICE:**

You may use the script **your** wrote for the NETW1500 - Final Project but you may not use the script I wrote, even if modified.

Just as a reminder, if you used my script with some modifications and it worked for you. You will receive a marks for successful execution of the script **BUT** you will not receive a grade for the script as you did not write it and the grade actually belongs to me.

As we discussed in class, you are to write your own script. There are plenty of resources on line to assist you with creating your own script for importing and creating multiple users with PowerShell.

Below are some examples of helpful sites.

<https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/>

<https://www.tutorialspoint.com/how-to-create-bulk-users-in-the-active-directory-using-powershell>

**Task 1 - Create a new OU and use a PowerShell script to create users**

Part 1

* If required, log into your Member Server as the domain administrator
* Create a PowerShell session with the Primary Domain Controller (PDC)
* **Stop**. Start a transcript called TranscriptA4.txt to capture your commands.
* Use the PowerShell command to create an OU called **Staff** that is protected from deletion in your Root Domain in Active Directory
* Run the PowerShell command to confirm your OU was created successfully in the correct location.
* **Stop**. Include a copy of your TranscriptA4 in your documentation.
* Create a CSV call file called **NETWUserList.csv** on yourMember Server in **c:\scripts** that follows the convention

FirstName | MiddleInitial | LastName | FirstInitial | Department | Office | Title

* Populate the csv file to include the data supplied below:
  + Department = **Exec**
    - Office = Executive offices
      * Charlotte H Anichka (title = VP)
      * Clare L Cade (title = VP)
      * Add your name here following the same format (title = CIO)
  + Department = general
    - Title = **Admin**
    - Office = General cubical space
      * Myra Y Dante
      * Jaymz A Dinara
      * Brock R Finn
      * Troy R Macey
      * Zia I Oleg
      * Francis R Uta
  + Department = **Sales**
    - Title = Rep
    - Office = Sales offices
      * Carlos A Yen
      * Bruce R Orca
      * Nina I Yuli
* **Stop.** Include a copy of your **NETWUserList.csv** call file converted to text in your documentation.
* Create a PowerShell script called **NETWaddusers\_YourInitials.ps1** script in your **c:\scripts**
* Using your **NETWaddusers\_YourInitials.ps1** script to:
* Sets the Execution Policy to “allow the script to run unrestricted during the current PowerShell session **ONLY**.”
* Create your users in the Staff OU
* Call on your NETWuserList.csv file for a datasource
* Set Common **Name** to be FirstName <space>MiddleInitial<space> LastName
* Set **SAMAccount Name** to match your naming convention
* Set **Display Name** to display as Last Name,<space> First Name
* Set **department** as identified in csv file
* Set **Office** information as identified in csv file
* Set **Title** information as identified in csv file
* Sets first time password for all users to **Netw2500@2024**
* Any other settings that may be required
* **Make sure** script includes required headings/commented lines that such as author, creation date, reason for script.
* Comment every line of script with **detailed** description of what you are doing at that line. \*\*Make sure to include descriptions for arguments and parameters.
* Create a new **PowerShell Session** with your PDC
* **MOVE** your **NETWaddusers\_YourInitials.ps1** script to c:\dcscripts on your PDC. \* Do **NOT** copy your csv file (call file), it MUST be called from your Member Server but you must ensure you are able to access it through script.
  + Remember to check your permissions, only the Domain Admins group and administrators should have access.
* **Stop.** Record the successful command with a screenshot to copy the scripts to your dcscripts directory.
* Run your script in a PowerShell console in your PowerShell Session
* Troubleshoot any issues with your script and user creation until your entire script executes correctly. **Note**: You may need to delete incomplete users accounts in order to troubleshoot your script, you can do this easily by creating a script to remove the accounts based on the call file.
* **Stop.** Record your successful script run used to complete this task with screenshots and add to your professional document.
* Confirm your new users have been created in Active Directory in your staff OU and have the correct information set.
* **Stop.** Include a copy of your **NETWaddusers\_YourInitials.ps1** script converted to text with all required and correct commands and comments in your documentation.

Part 2

Let us go further and add our new employees to the correct group.

* Now we will create a PowerShell script that will:
  + Automatically create three new groups (**General\_group, Sales\_group, Exec\_group** )
  + Add our users to the groups based on their department membership.
  + Set the execution policy to“allow the script to run unrestricted during the current PowerShell session **ONLY**.”
  + Comment the starting line of the script to add an Author and Creation Date
  + Comment EVERY line of script to identify what is happing at that line, remember to include arguments/parameters.
* Create a new **PowerShell Session** with your PDC
* **Move** the script as **NETWgroupadd.ps1** in your **c:\dcscripts (PDC)**
* Set the Execution Policy to “allow the script to run during the current PowerShell session **ONLY**.”
* Run your script in a PowerShell console in your PowerShell Session
* Troubleshoot any issues with your script and user group assignments until your entire script executes correctly. **Note**: You may need to delete incomplete groups in order to troubleshoot your script, you can do this easily by creating a script to remove the accounts based on the call file.
* Confirm your new employees have been added to the correct group in Active Directory Users and Computers.
* **Stop.** Include a copy of your **NETWgroupadd.ps1** script converted to text with the correct commands and comments in your documentation.
* **Stop.** Be prepared to Demo your scripts (user creation and groups) and call file with a new user supplied in class.

We should now have our Staff OU created and populated with our new uses and each user should be added to the correct group. **If all user information is correct, then we will move on to Task 2.**

**Task 2 - Managing User Environments**

Part 1

We would like to enforce a password policy for our new users

* Modify your “Your Initials Default Domain Policy” Group Policy created in Assignment 2 to create a password policy with these settings:
* History = 4
* Max age = 120 days
* Min age = 1 day
* Min length = 8 characters
* Complexity = disabled
* Store passwords = disabled

This is great for our new users, but it is not secure enough for our Sales group as they will have access to financial information. We do not want them to keep their passwords for 120 days. For security, reasons let us change their password to require more changes.

To do this we will need to create a Password Settings Object.

* In your Server Manager / Active Directory Administrative Center
* Select your System container (Builtin system settings) / Password Settings Container

Currently, this container is blank as there are not password objects by default as our current password policy applies to all users, but we will create a new Password Setting Object

* Create a Password Settings object with these settings:
* Name = SalesPassObj
* Precedence = 5
  + History = 10
  + Max age = 40 days
  + Min age = 1 day
  + Min length = 12 characters
  + Complexity = enabled
  + Store passwords = disabled
  + Protect from accidental deletion = unchecked
  + Enforce account lockout policy:
    - Number of failed logons is 3
    - Reset after 4 minutes
    - Lock account for 5 minutes
  + Description = Password policy for Sales Group. Created By: YourName Created On: Date
  + In Directly Applies To
    - Add the Sales\_group group
* Refresh your server in Server Manager to apply all your new changes
* Test your new Password Settings Object by changing the password for the users listed below:
  + User = **Carlos A Yen**
    - New password = Passw0rd@2500
    - Uncheck “User must change password at next log on”
  + User = **Bruce R Orca**
    - New password = Pass2
    - Uncheck “User must change password at next log on”
    - NOTE: If the Password Settings Object is applied, you will not meet password requirements for B Orca.
  + **Stop**. Take a screenshot to demonstrate successful execution of your Sales Password Policy.
    - Now set Bruce R Orcas Password to Passw0rd@2500

lPart 2

Let us create some Home Directories for our new users

* On your Secondary DC Server (**SDC**)
* Add the File Server Resource Manager role
* Run the PowerShell cmdlet **Get-WindowsFeature File\*** to confirm you have successfully installed the File and Storage Services feature
* If required add a new hard disk to your VM and create a new 60g NTFS Volume Drive with the drive letter E:
* Create the Folder E:\Home
* Share your E:\Home folder to meet the following criteria:
  + Share Name = Home$
  + Permission =
    - Everyone has Change and Read
    - Domain Administrators have Full Control
  + Run the cmdlet **Get-SmbShareAccess Home$** to view your permissions
* **If required log into your Member Server**
* Use your File and Storage Services to complete the following for your Home$ share:
  + If required, install File Resource Manager on your member server
  + Set Quota to:
    - Automatically apply Quotas to all user
    - 100MB limit Quota Template

While we are still on our Member Server we will complete a few more management and setup tasks.

* Use the environmental variable for usernames to create a home drive that uses the drive letter H: for all your new users at once to your new Home$ share.
  + **Stop.** Record the steps to set up ALL user’s home directories at once using the correct environmental variable
  + **Note**: You may use either *Active Directory Users and Computers* or a PowerShell command. The option is yours.
* **Stop.** Be prepared to demonstrate the creation of a home directory for your new user assigned in class.

**Task 3 – Securing Active Directory**

In order to better manage our Domain we would like to be able to hire some casual staff. We would like our new staff to be able to *image* and add computers to our Domain but we do not want them to make any other changes in our Domain.

*Additional Learning: When managing dozens or even hundreds of computers, Imaging is an important tool for most System Management Professionals. Imaging allows for consistency in computer design and management as well as a backup for key systems.*

*Additional Reading:*

[*https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11)*](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11))

[*https://www.smartdeploy.com/blog/what-is-computer-imaging/*](https://www.smartdeploy.com/blog/what-is-computer-imaging/)

* In your System Operators OU
* Create a new Global Security group called **CasualTechs\_gp** with a description *Reduced Privilege*
* Create a new user:
  + First Name = Bruce
  + Middle Name = Banner
  + Last Name = Brown
  + Full Name = Bruce B. Brown
  + User logon name = Sysop.BBB
  + Password never expires
  + Password = Passw0rd@2500
  + Groups = CasualTechs\_gp, Domain Users

Now we will give our Casual Techs group permission to add computers to our Domain

* Right click on your Computer OU
* Select Delegate Control…
* Add your Casual Techs Group
* Choose Create a custom task to delegate
* Delegate control of: Only the following object in the folder
  + Computer Objects
  + Create selected objects in this folder
  + Delete selected objects in this folder
  + **Stop**. Capture these settings in a screenshot before proceeding.
* Under Permissions/General, select the following:
  + Reset password
  + Read and write account restrictions
  + Validate write to DNS host name
  + Validate write to service principal name
  + **Stop**. Capture these settings in a series of screenshots before proceeding.

Now we will test your new Casual Techs abilities by adding our Windows 10 workstation to the domain

* Log into your workstation and
  + **Remove your workstation from the domain, clean out the old account from AD and rename with a A4 at the end of the client name**
  + Use your new **Sysop.BBB** account to add your workstation to the domain.
  + Confirm your client workstation is now a member of your domain by logging into your new client as **Bruce R Orca**
* **Stop**. Be prepared to demo your Sysop.BBB account by reconnecting your client back to your domain.

**Task 4 - Managing with Group Policies**

We do not want our clients to have multiple working copies of documents and to allow for reliable backups we will redirect our client Documents to our users Home directories.

* Modify your “Your Initials Default Domain Policy” Group Policy to redirect your staff users Documents to their home directories (Some research may be required for this step.)
  + Target = Under the root path
  + Root Path = User home drive
  + *Hint*: don’t forget to uncheck Grant the user exclusive rights to Documents and Move contents to the new location.
* Log into your workstation as Bruce R Orca to test your new Home drive and folder redirection
  + Open File Explorer.
  + Right-click a redirected folder (for example, the My Documents folder in the Documents library), and then select **Properties**.
  + Select the **Location** tab and confirm that the path displays the correct location of the share you specified instead of a local path.

With newer OSes, computer hard drives can quickly fill with unnecessary files, we will create a script called **NETWcleantemp.ps1** that will clear the C:\temp folders on our workstation when our users log on.

* If required log on to your Member Server
* Use the following Command to create a new variable for each of your temp files locations.

$tempfiles = @("c:\Users\\*\Appdata\Local\Temp\\*", "$env:windir\temp\\*")

* Now add the command to remove the $tempfiles, you must include the following arguments:
  + All files including subfolders
  + Force the removal
  + Have the script ignore any error messages that may occur
* Now add the command to create a new file item that:
  + Creates a new file in both temp locations
  + File name is cleanlog.txt
  + File content includes current date and time
* Comment the starting line of the script to add an Author and Creation Date
* Comment EVERY line of script to identify what is happing at that line, make sure to include detailed descriptions for variables and arguments.
* Save your script to your C:\scripts as **NETWcleantemp.ps1** on your general server
* **Stop.** Include a copy of your script converted to text with correct commands and comments to your documentation.
* Place a copy of your script in your sysvol startup scripts location

***Reminder****: The easiest way to find the correct location is through your Group Policy Manager.*

* **Stop.** Record the full path location of your script file in your SYSVOL and add to your professional document

***Example*.**

\\Dcd31101\SYSVOL\mad.it.net172.ca\Policies\{FBBFA0B9-ACB6-474C-8FEE-BFEEE3929DE8}\Machine\Scripts\Startup

Modify your “Your Initials Default Domain Policy” Group Policy to create a:

* + Computer Startup PowerShell script
  + Add your new NETWcleantemp.ps1 from your Sysvol location
  + Script Parameters = -executionpolicy bypass
  + GPO run order = Run Windows PowerShell scripts first
* To ensure our new policy runs and deploys our software **Enforce** your policy
* Set your **Security Filtering** to apply this GPO to
  + Authenticated Users
  + Domain Computers
* **Stop.** We want to make sure we have a copy of our policy for reference and troubleshooting. Selected your Link your new “Your Initials Default Domain Policy” Group Policy and save a report to C:\GPReports\”NameOfPolicy.vMM.DD.YY”.html. and upload a copy to your BrightSpace.
* ***ATTENTION:*** *Please upload this report separately as it must remain an* ***HTML*** *document. \*\* Please confirm the report is a live document and readable after upload.*

Now we will test your new startup script

* Log on to your workstation as BOrca and force your Group Policy to update
* Restart your computer (remember this is a startup script)
* Confirm your temp files have been deleted in both locations and your new files where added with the correct content. Note: some files are in use or required and will not be removed. This is an acceptable result.
* **Stop.** Be prepared to demonstrate your Group Policy and script settings with your new user.

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 snapshot of ALL your server in the OFF state.
* Capture a Gold copy of your PDC and SDC.
* Include the properties for your PDC and SDC gold copy in your documentation, make sure to include, location, creation date and size.
* Modify the correct Change Management logs for your servers and **upload ALL** your change logs to BrightSpace. (Note: user names are not required for change logs).
* Add all screenshots, documentation and scripts to your professional documentation.
* **Upload all your professional documentation to D2L.**

**Marking rubric**

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **Tasks** |
| 2 | TranscriptA4.txt with correct entries. |
| 5 | Copy of NETWUserList.csv with correct entries and format. |
| 2 | Record the successful command with a screenshot to copy the scripts to your dcscripts directory. |
| 4 | Record your successful script run used to complete this task with screenshots and add to your professional document. |
| 12 | Copy of your **NETWaddusers\_YourInitials.ps1** script converted to text with all required and correct commands and comments in your documentation. |
| 4 | Copy of your **NETWgroupadd.ps1** script converted to text with the correct commands and comments in your documentation. |
| 20 | Demo your scripts (user creation and groups) and call file with a new user supplied in class. |
| 2 | Screenshot to demonstrate successful execution of your Sales Password Policy. |
| 5 | Record the steps to set up ALL user’s home directories at once using the correct environmental variable.   * **Note**: You may use either *Active Directory Users and Computers* or a PowerShell command. The option is yours. |
| 4 | Demonstrate the creation of a home directory for your new user assigned in class. |
| 3 | **Stop**. Capture these settings in a screenshot before proceeding.  Delegate control of: Only the following object in the folder   * Computer Objects * Create selected objects in this folder * Delete selected objects in this folder |
| 4 | **Stop**. Capture these settings in a series of screenshots before proceeding.  Under Permissions/General, select the following:   * Reset password * Read and write account restrictions * Validate write to DNS host name * Validate write to service principal name |
| 4 | Demo your Sysop.BBB account by reconnecting your client back to your domain. |
| 4 | Copy of your **NETWcleantemp.ps1** script converted to text with correct commands and comments to your documentation. |
| 2 | Record the full path location of your script file in your SYSVOL and add to your professional document. |
| 6 | “Your Initials Default Domain Policy” Group Policy and save a report to C:\GPReports\”NameOfPolicy.vMM.DD.YY”.html. and upload a copy to your BrightSpace with all required settings and configurations.   * Password Settings * Folder redirection * Startup scripts |
| 5 | Demonstrate your Group Policy and script settings with your new user. |
| 3 | Snapshot of all your server in of state taken at the same time. |
| 2 | Gold copy properties for PDC and SDC |
| 5 | Change Management Log |
| 2 | Document Professionalism |
| **100** | **Total Marks possible** |
|  |  |