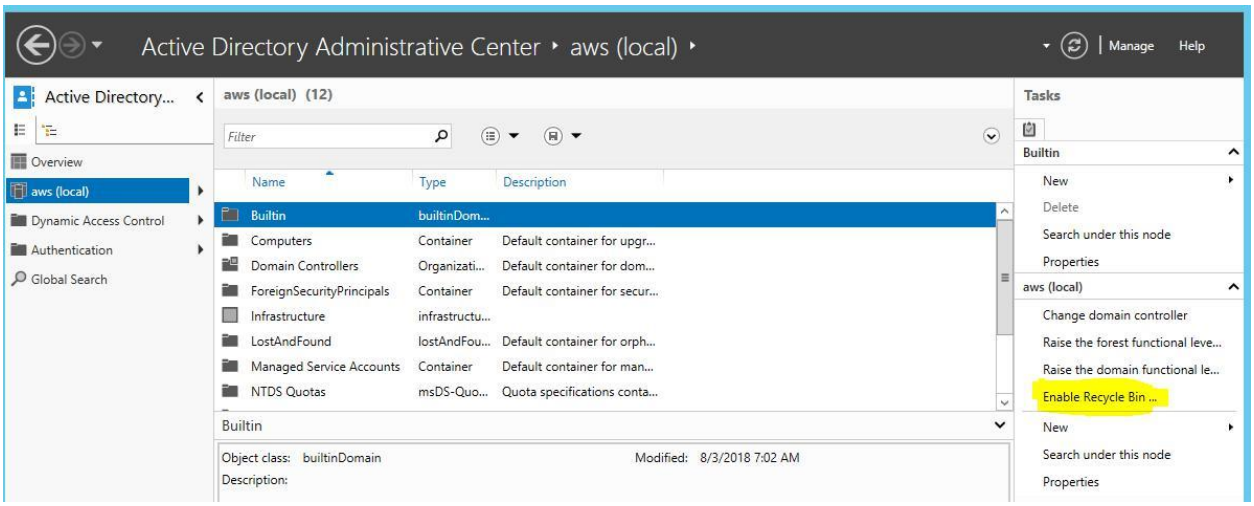
NUST Cyber Security Team (NCST) Windows Lab 3

1. Managing Active Directory Domain Services

Domain: cyber.local

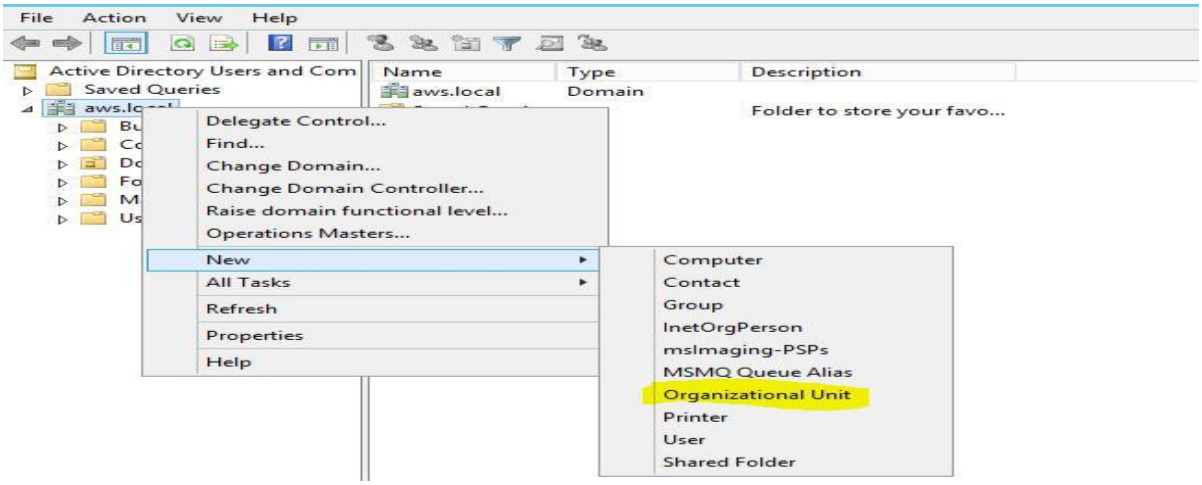
1.1 Enable Recycle bin

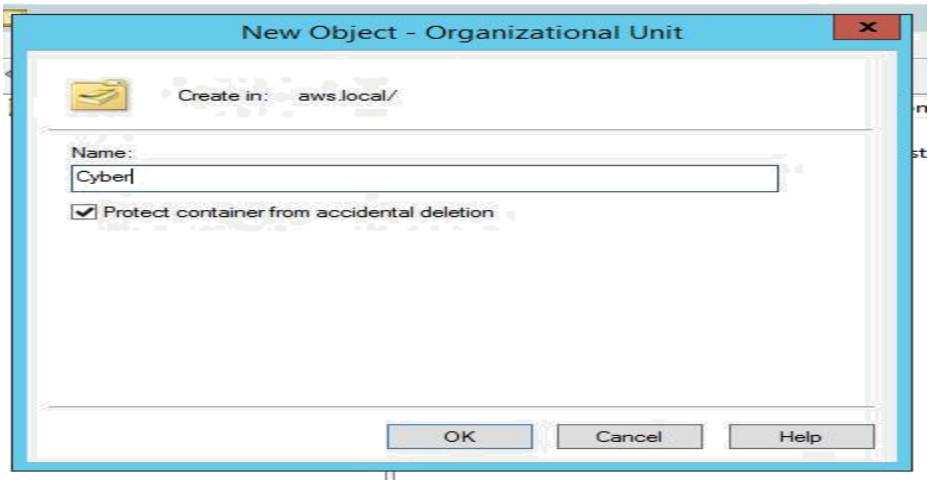
Tools → Active Directory administrative Center →cyber (local) Enable Recycle Bin



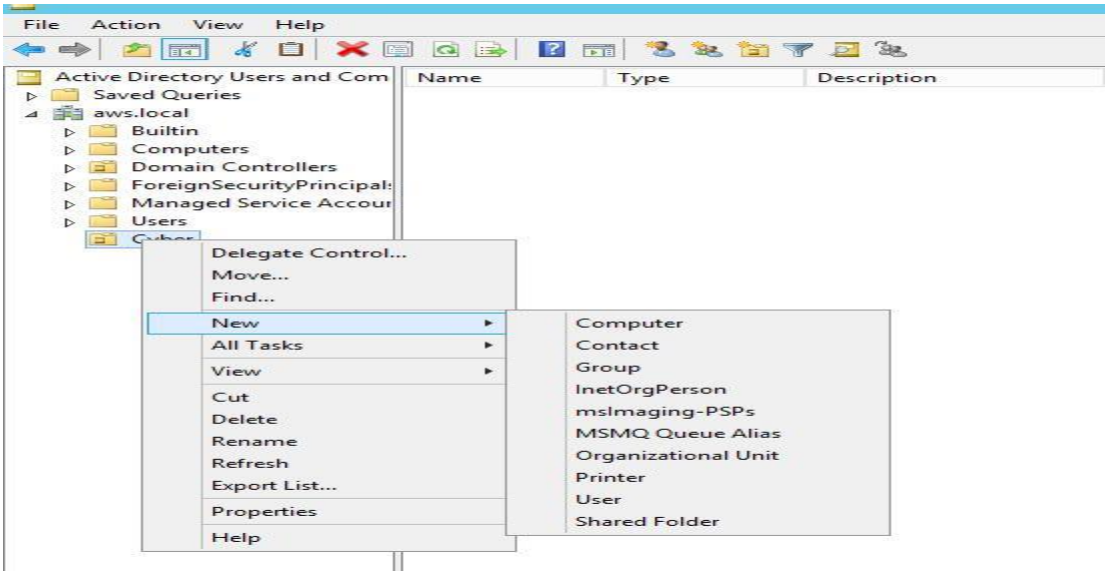
1.2 Create organisational unit (OU) namely *Cyber*

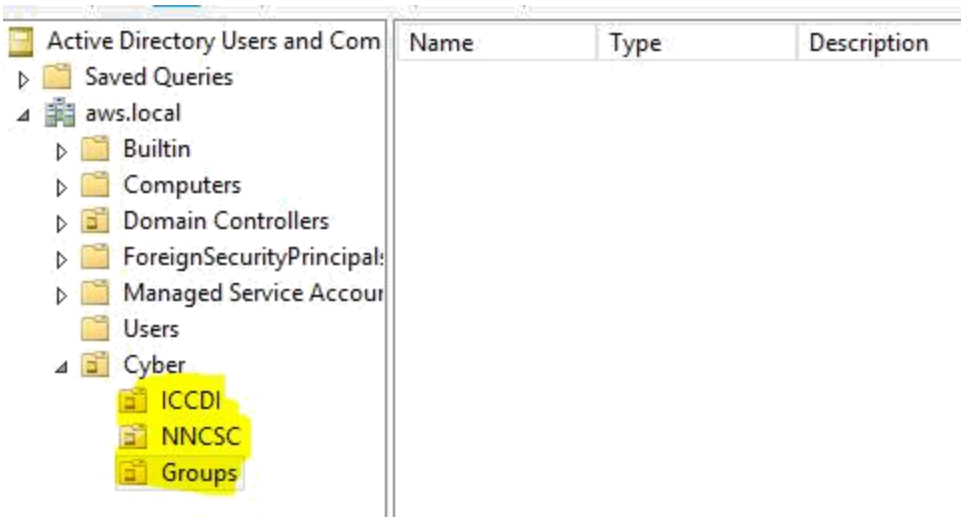
Active Directory Users and Computers cyber.local



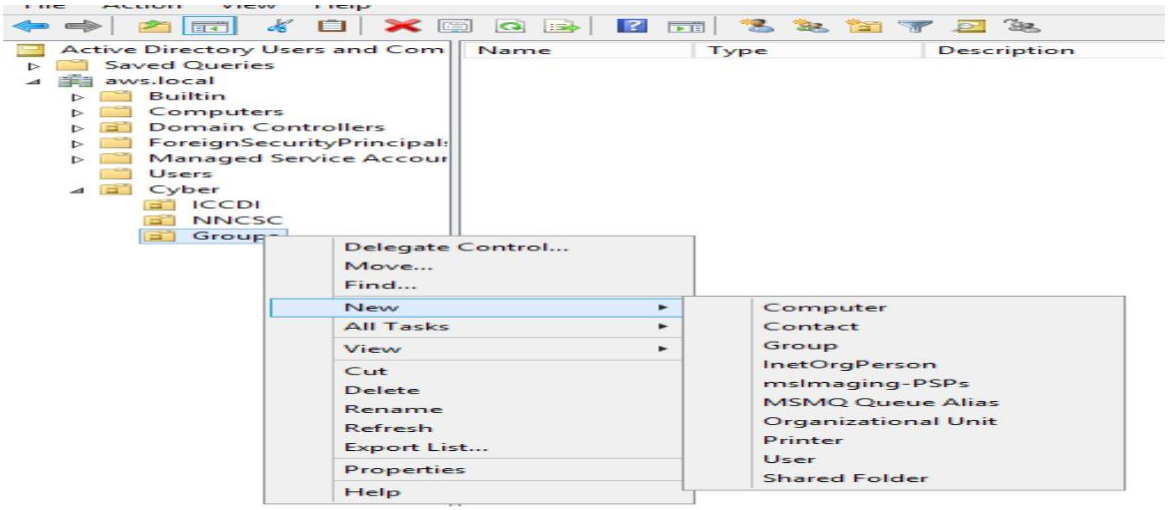


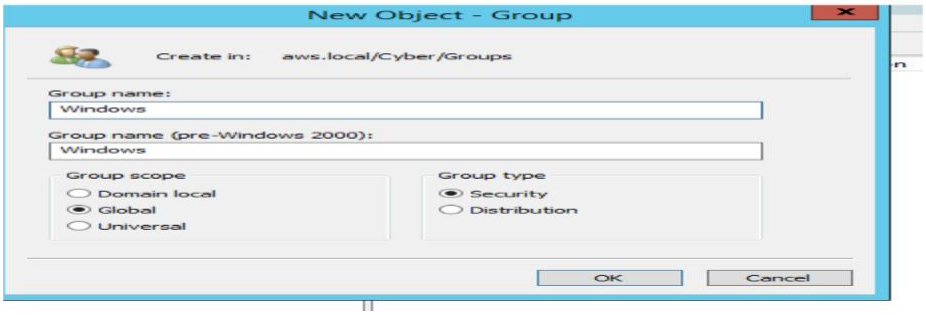
1.3 Create Sub OU'S *ICCDI and NNCSC*

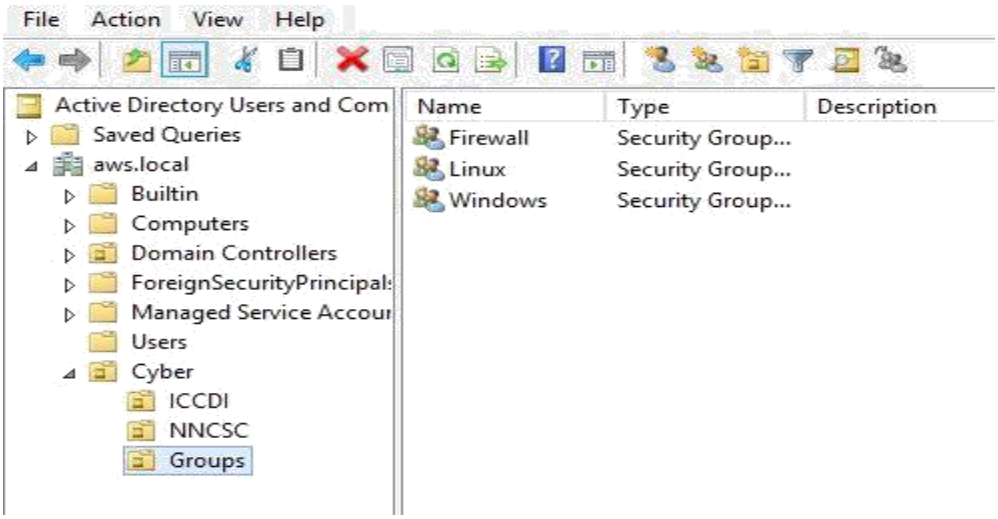




1.4 Create groups namely *Windows, Linux, Firewall under Groups OU*







1.5 Create the following users under ICCDI

Owen

Ulrigh

Maria

Tinashe

Amanda

Alves

Martha

Pius

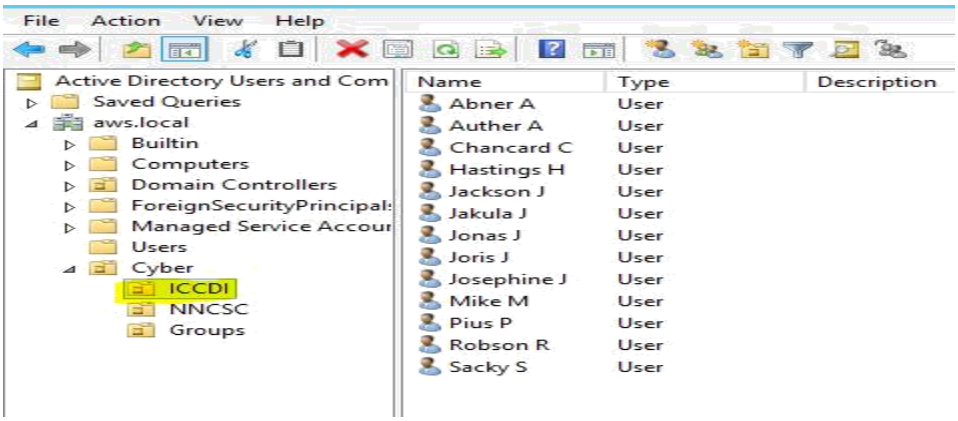
Anene

Robson

Thomas

Titus

Derick



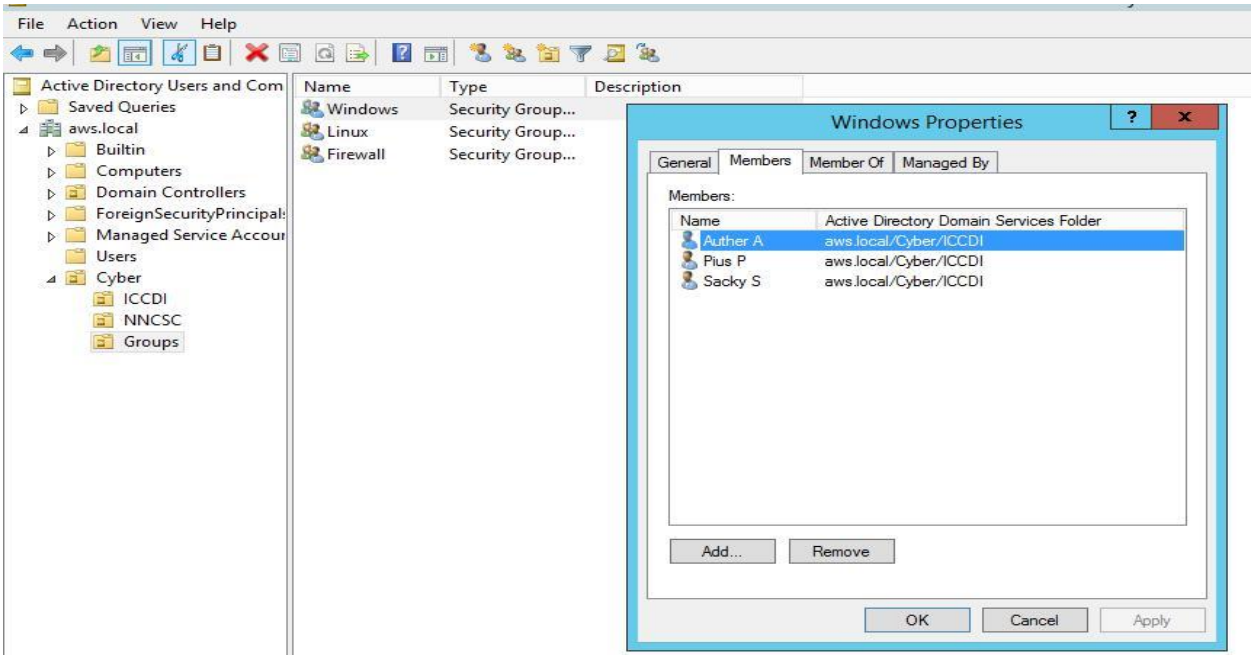
1.6 Add Pius, Tinashe and Alves to Windows group

1.7 Add Martha, Anene, Robson and Jakula to Linux group

1.8 Add Titus, Maria, Derick and Amanda Firewall group

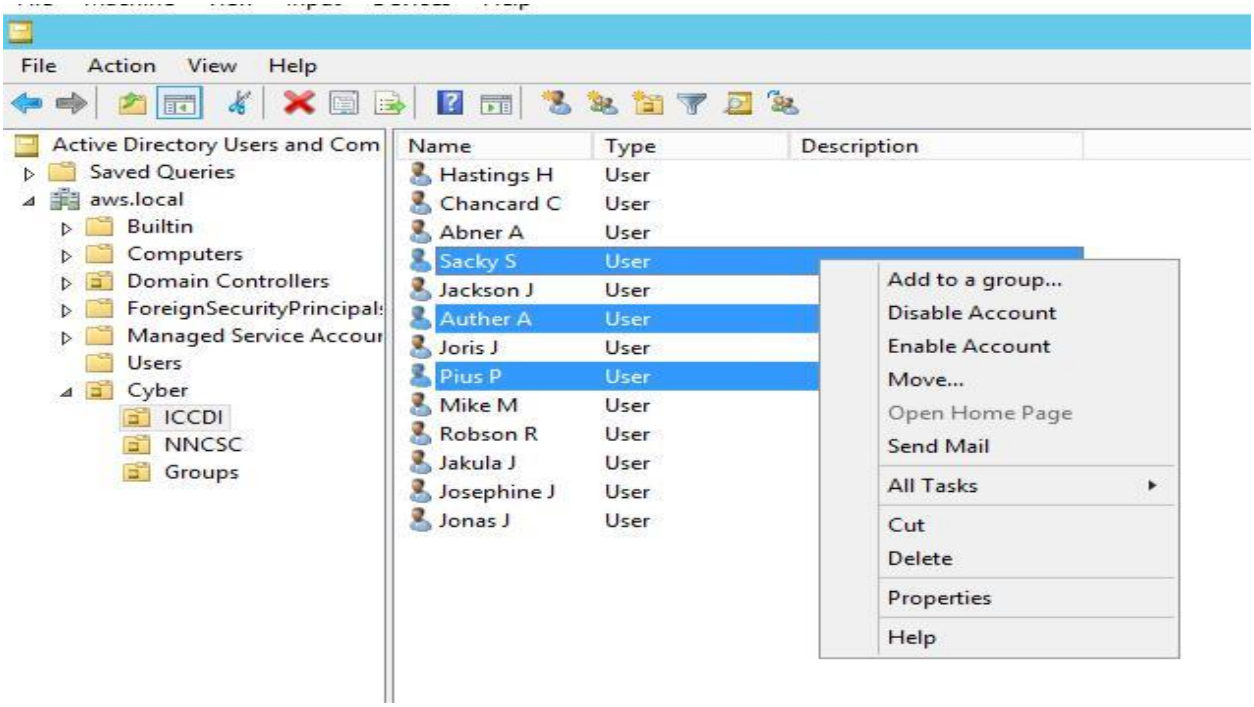
1.9 Add Owen, Ulrigh and Maria to all the Goup members *Groups*

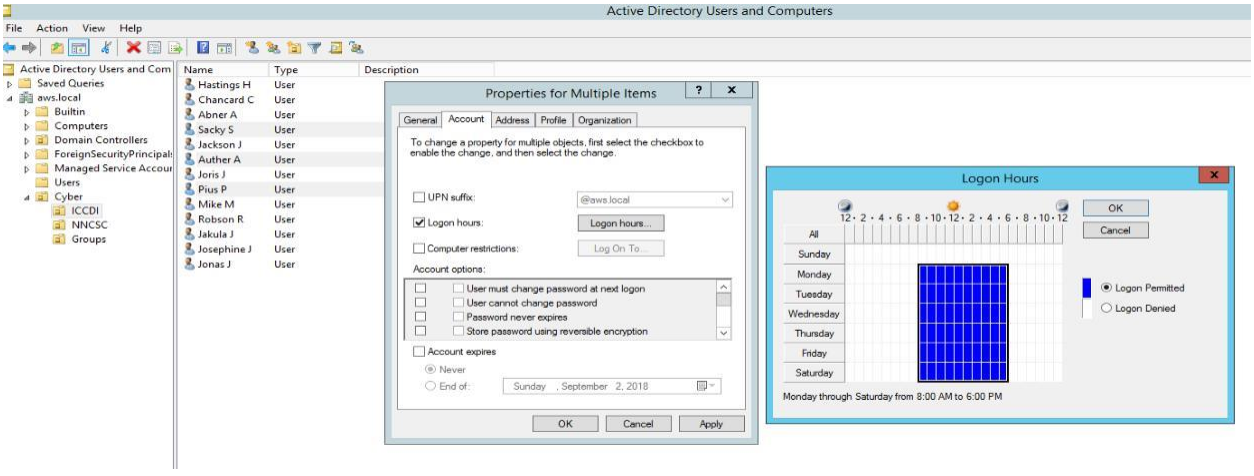
→ Windows →properties→ members→ add→name



1.10 Restrict members of windows to login only *between Mondays and Saturday from 08:00-18:00*

select all user for a specific group member→ Right click→ properties→ account→ logon hours → logon denied highlight days and time given → logon permitted → ok → apply





Challenge 1

Restrict members of firewall to deny login on *Saturday from 08:00-13:00*

Test & verify by login with one of firewall user on your client

Challenge 2

Reset all the users password using the following command

Dsquery user ou=Cyber,ou=iccdi,dc=cyber,dc=local | dsmod user –pwd Password5 -mustchpwd yes

Test and verify

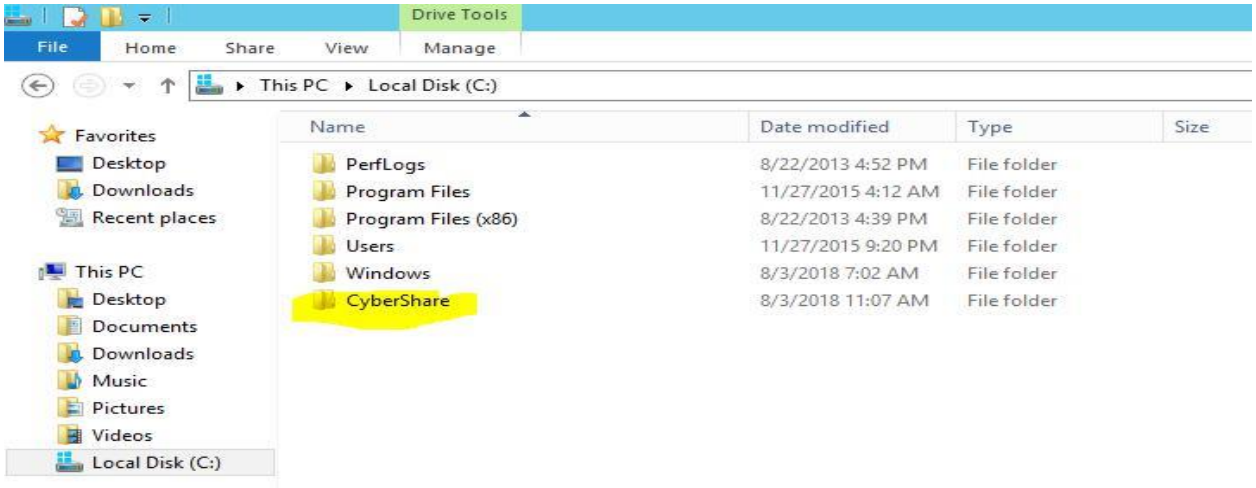
Login with four (4) different user accounts

Did you succeed?

2. Creating, securing and sharing a folders

2.1 Create a folder CyberShare under drive

C:\Cyber

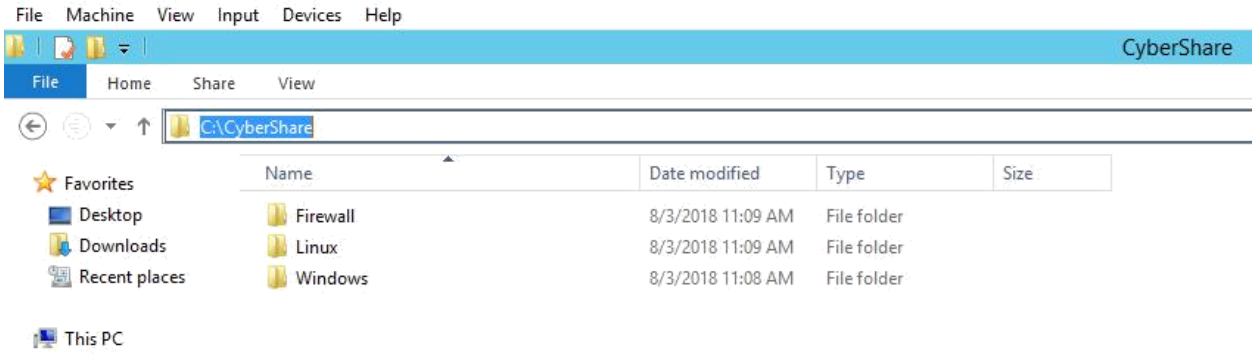


2.2 Create Windows, Linux and firewall folders

C:\ CyberShare \Windows C:\ CyberShare

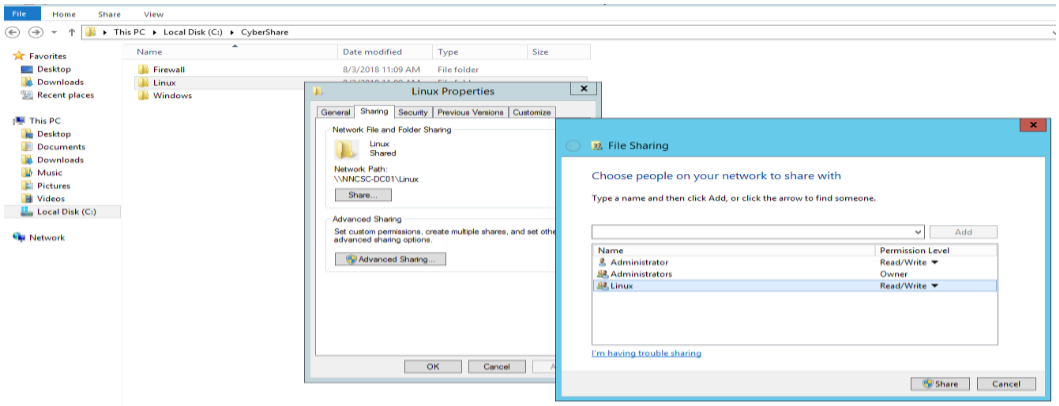
\Linux

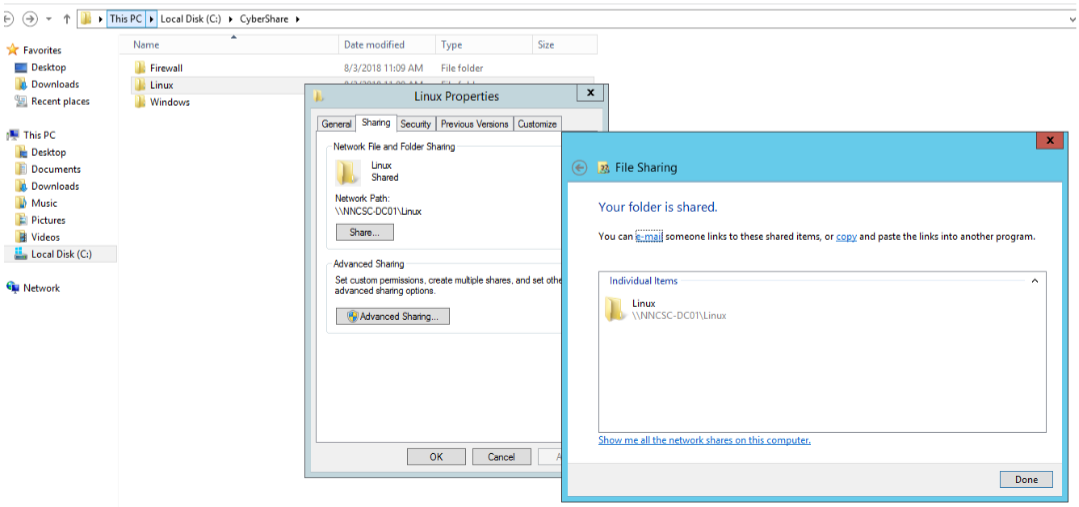
C:\ CyberShare \Firewall



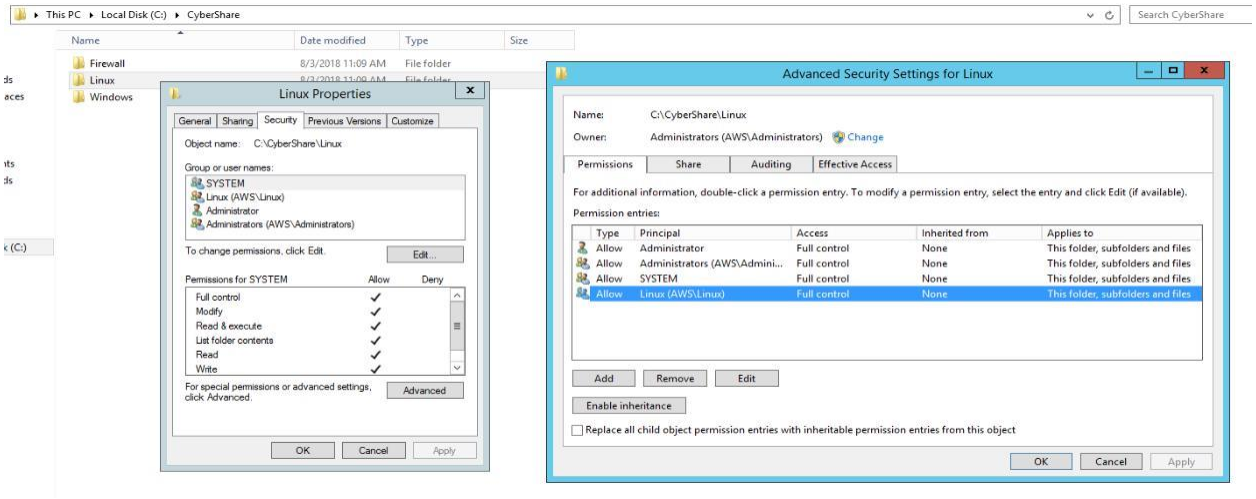
2.3 Configure permissions on all folders for each group with read and write

Linux→ properties →sharing network and folder→ sharing→ share→ find people→ firewall→ read/write→ share →done





Linux →properties →security → advanced → add →select principal "enter Linux → Ok" basic permissions "select" → ok →disable inheritance →"second option" apply → ok →close



Test and verify

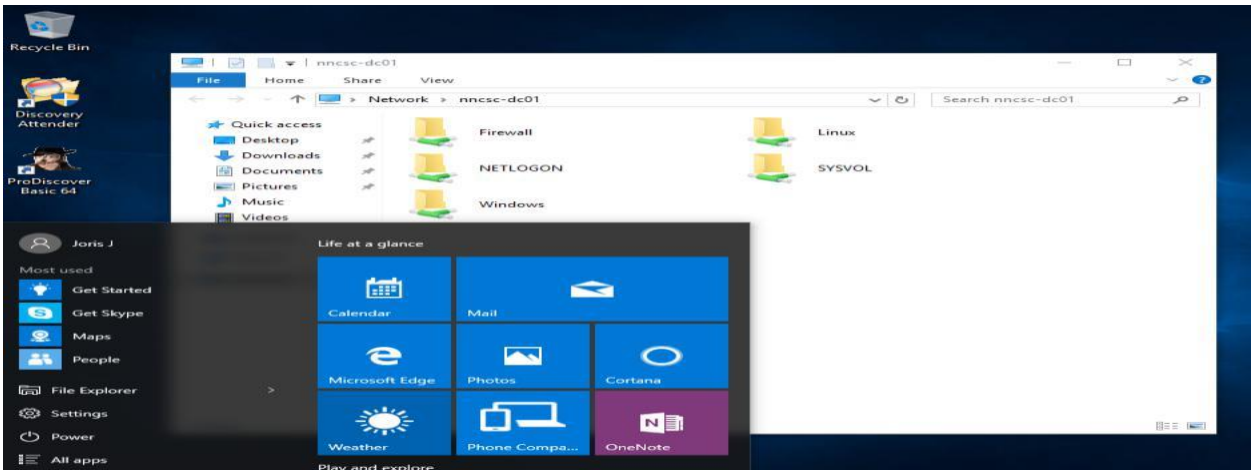
Login with Martha user account on your client

Type \\nncsc-dc01 on search bar

What can you see?

What can you access?

What can you not access?



2.3 NB: Repeat for Windows and firewall folders

2.4 Grant full access to Owen, Ulrigh and Maria to all the folders.

Test and verify

Test your permissions by login with one user of each group

Did you succeed?

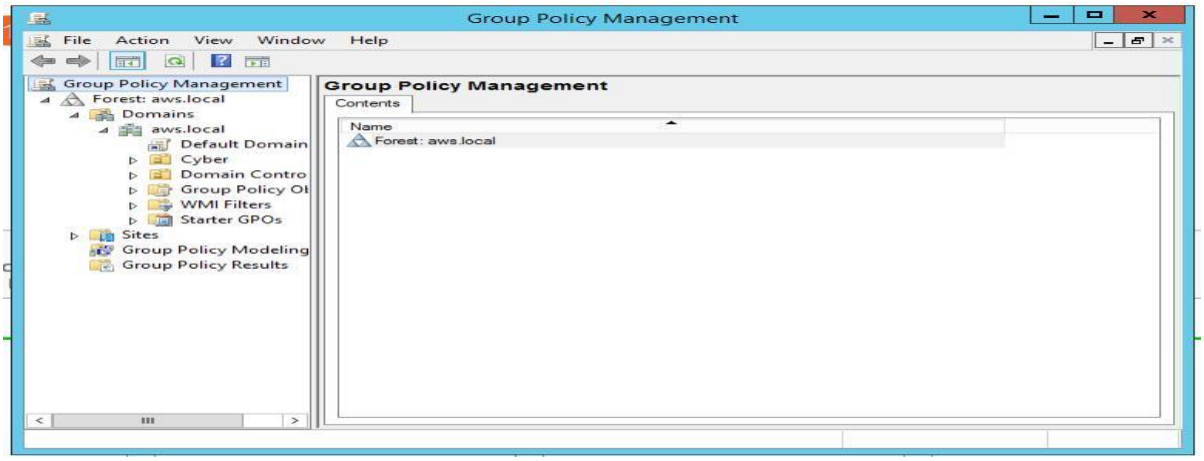
Are there any challenges?

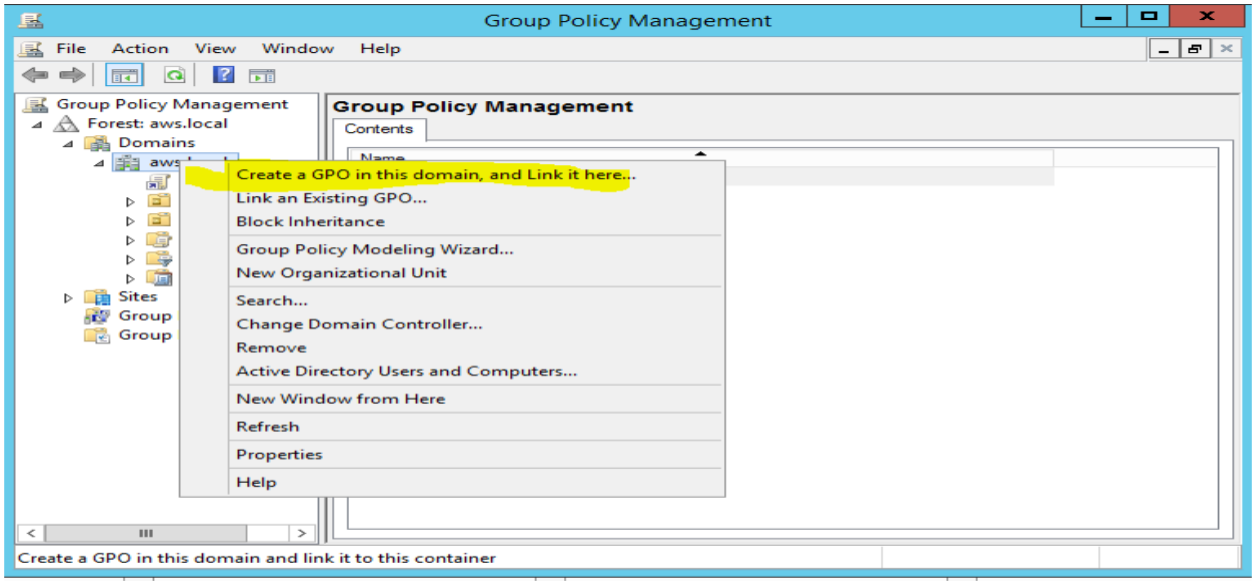
Challenge 3

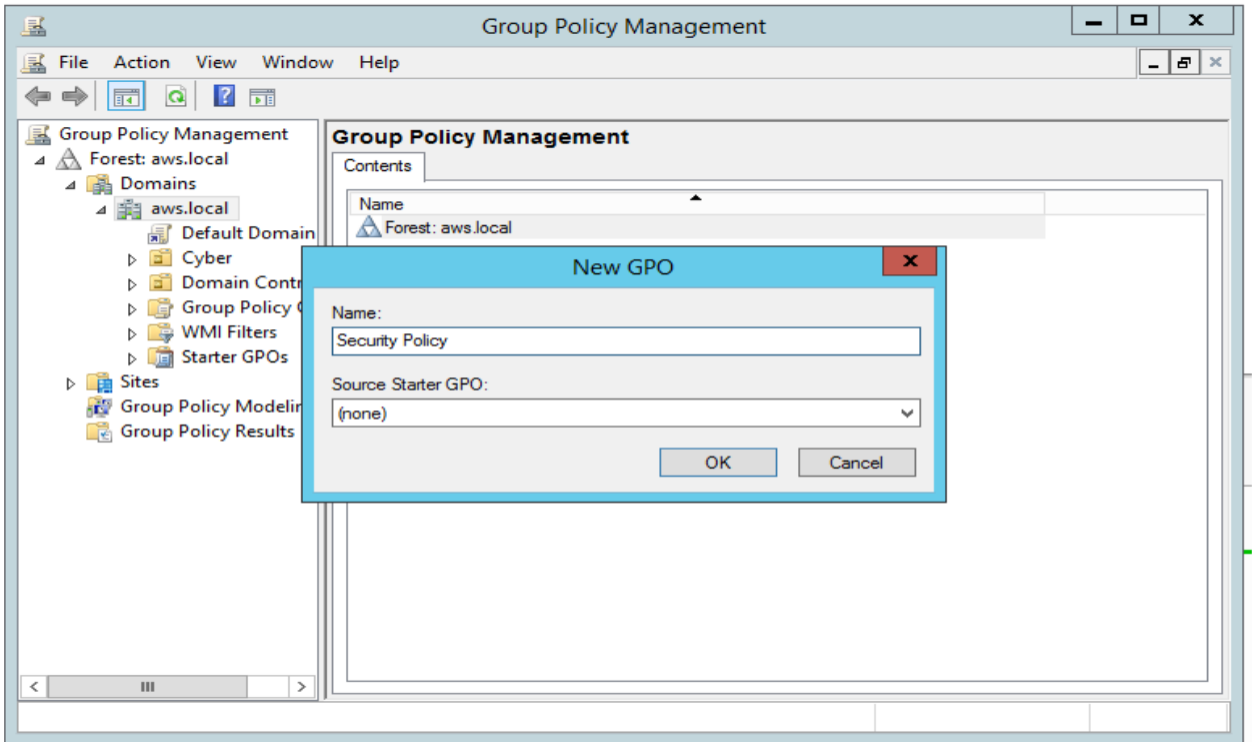
Create two folders on your local drive namely Homes and Profiles. Share these folders as hidden shares. Configure user home folders and profiles to use the folders you create to keep their information. Make sure users cannot have access to other people's personal home folders

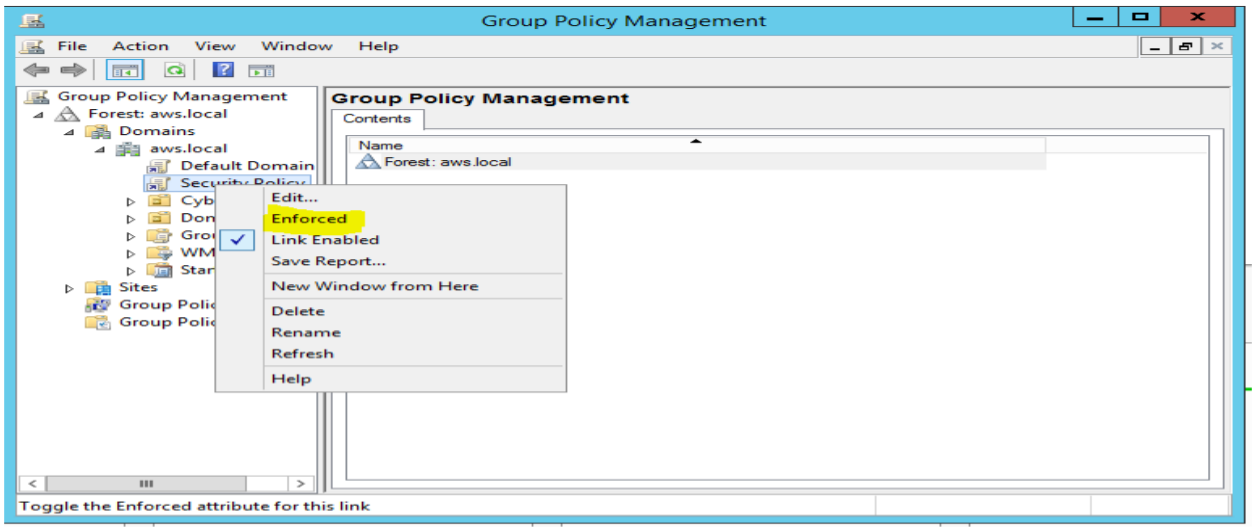
3. Group Policy Management

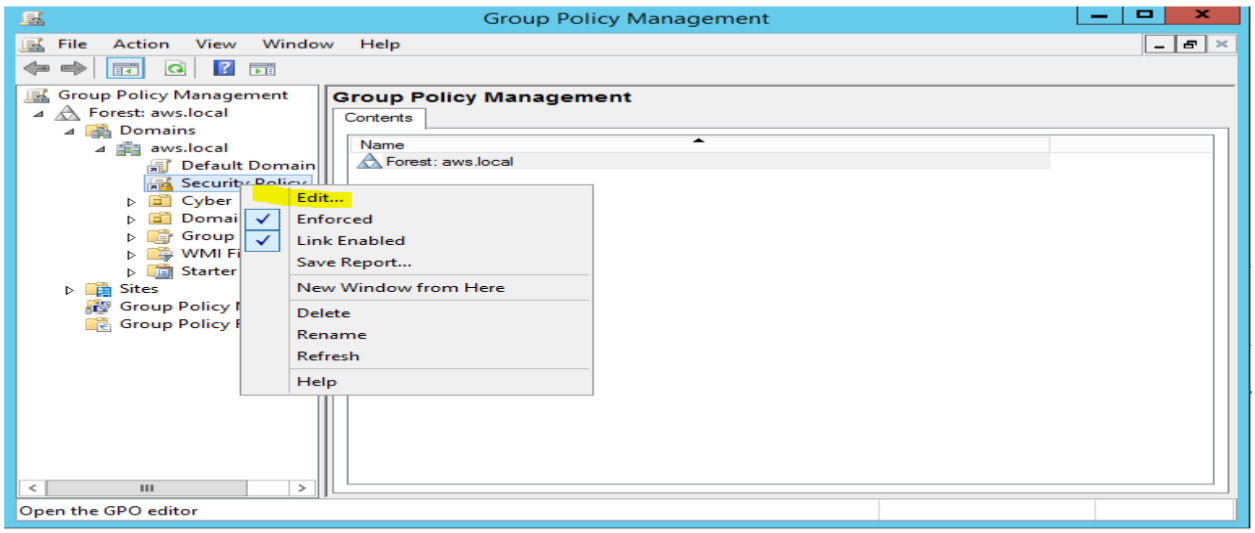
3.1 Create a security group policy with the settings at page 14, link and enforce them to ***cyber.local***

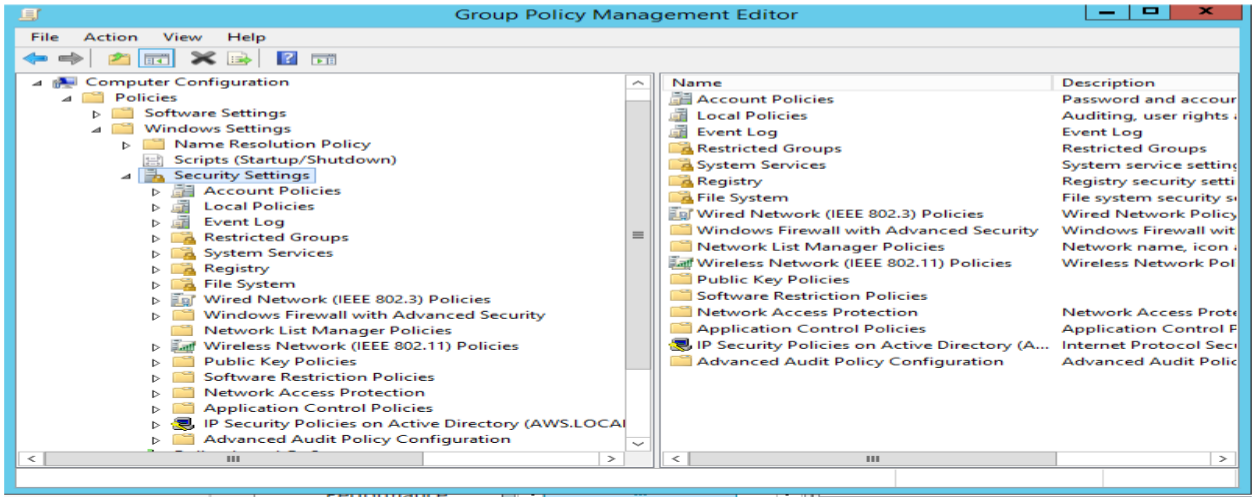


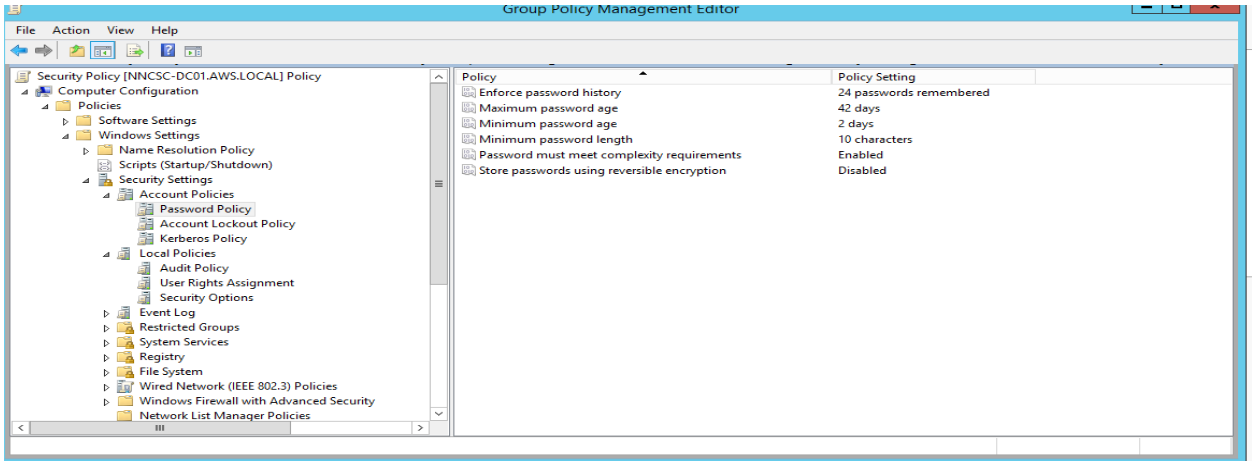

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: aws.local
Domains
Sites
Group
Group
Group Policy Management
Contents
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help
Create a GPO in this domain and link it to this container

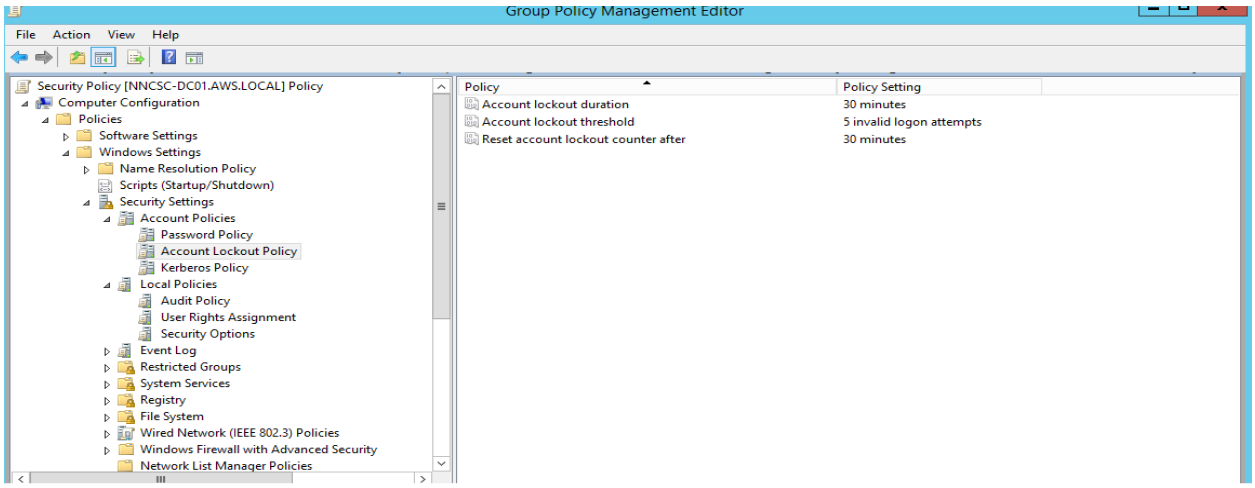

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: aws.local
Domains
aws.local
Default Domain
Cyber
Domain Contr
Group Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modelir
Group Policy Results
Group Policy Management
Contents
Name
Forest: aws.local
New GPO
Name:
Security Policy
Source Starter GPO:
(none)
OK
Cancel

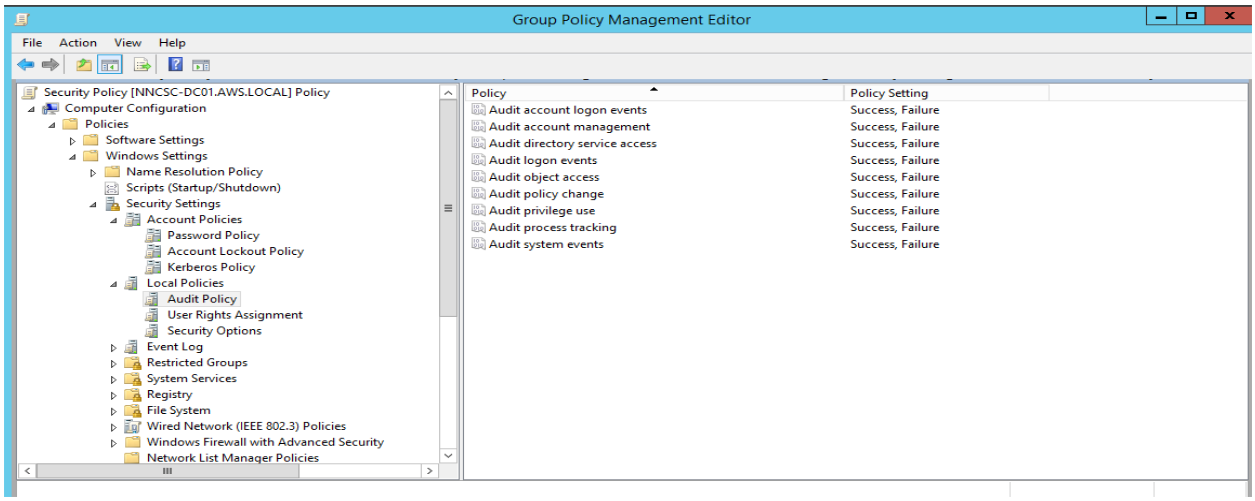

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: aws.local
Domains
aws.local
Default Domain
Sites
Group Policy Management
Forest: aws.local
Edit...
Enforced
Link Enabled
Save Report...
New Window from Here
Delete
Rename
Refresh
Help
Toggle the Enforced attribute for this link

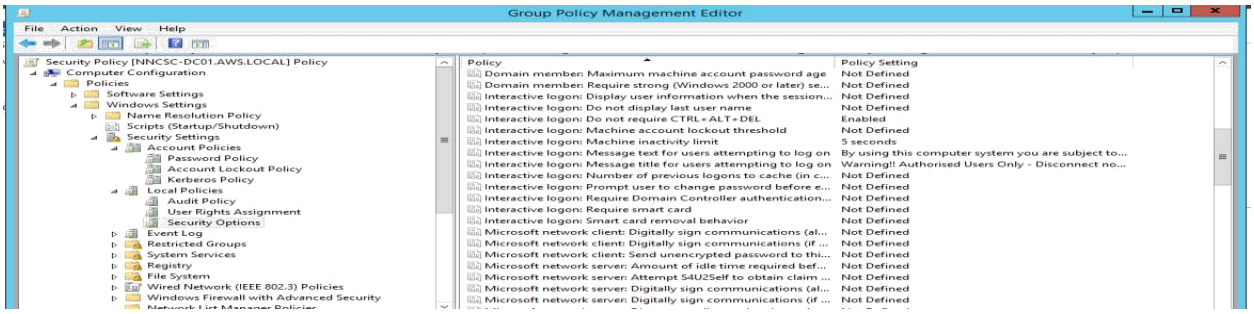

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: aws.local
Domains
aws.local
Default Domain
Sites
Group Policy Management
Forest: aws.local
Edit...
Enforced
Link Enabled
Save Report...
New Window from Here
Delete
Rename
Refresh
Help
Open the GPO editor


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (AWS.LOCAL
Advanced Audit Policy Configuration
Name
Description
Account Policies
Password and accour
Local Policies
Auditing, user rights
Event Log
Event Log
Restricted Groups
Restricted Groups
System Services
System service setting
Registry
Registry security setti
File System
File system security s
Wired Network (IEEE 802.3) Policies
Wired Network Policy
Windows Firewall with Advanced Security
Windows Firewall wit
Network List Manager Policies
Network name, icon
Wireless Network (IEEE 802.11) Policies
Wireless Network Pol
Public Key Policies
Software Restriction Policies
Network Access Protection
Network Access Prote
Application Control Policies
Application Control P
IP Security Policies on Active Directory (A...
Internet Protocol Secu
Advanced Audit Policy Configuration
Advanced Audit Polic


Group Policy Management Editor
File Action View Help
Security Policy [NNCSC-DC01.AWS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Policy
Policy Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
2 days
Minimum password length
10 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled


Group Policy Management Editor
File Action View Help
Security Policy [NNCSC-DC01.AWS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Policy
Policy Setting
Account lockout duration
30 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
30 minutes


Group Policy Management Editor
File Action View Help
Security Policy [NNCSC-DC01.AWS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Policy
Policy Setting
Audit account logon events
Success, Failure
Audit account management
Success, Failure
Audit directory service access
Success, Failure
Audit logon events
Success, Failure
Audit object access
Success, Failure
Audit policy change
Success, Failure
Audit privilege use
Success, Failure
Audit process tracking
Success, Failure
Audit system events
Success, Failure



3.2 NCST- Security Policy

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies

✓	**Enforce password history –** 24
✓	**Maximum Password Age -** 42 days
✓	**Minimum Password Age –**2 days
✓	**Minimum password length** - 10 characters
✓	**Password Complexity -** Enable
✓	**Store Password using Reversible Encryption for all Users in the Domain -** Disable
✓	**Account Lockout Duration** - 30 minutes
✓	~~**Account Lockout Threshold –** 5 attempts~~
✓	~~**Reset Account Lockout Counter** - 30 minutes~~
✓	~~**Enforce User Logon Restrictions** - Enable~~
✓	~~**Maximum Lifetime for Service Ticket** - 600 minutes~~
✓	**Maximum Lifetime for User Ticket** - 8 hours
✓	**Maximum Lifetime for User Ticket Renewal** - 7 days
✓	**Maximum Tolerance for Computer Clock Synchronization** - 5 minutes
✓	☐ **WINDOWS AUDIT POLICY AND ADVANCED SECURITY AUDIT POLICY (GROUP POLICY)**

- ✓ All Event Log files must be set to 2048KB and must be set to overwrite events as needed.
- ✓ **Audit account logon event** - Success, Failure
- ✓ **Audit account management** - Success, Failure
- ✓ **Audit directory service access** - Failure
- ✓ **Audit logon events** - Success, Failure
- ✓ **Audit object access** - Success, Failure
- ✓ **Audit policy change** - Success, Failure
- ✓ **Audit process tracking** - Not configured
- ✓ **Audit privilege use** - Success, Failure
- ✓ **Audit system events** - Success, Failure
- ✓ **Audit Authentication Policy Change** - Success
- ✓ **System: System Integrity** - Success, Failure
- ✓ **Security System Extension** - Success, Failure
- ✓ **Security State Change** - Success, Failure
- ✓ **Logoff** - Success, Failure
- ✓ **Logon** - Success, Failure
- ✓ **Special Logon** - Success, Failure
- ✓ **File System** - Success, Failure
- ✓ **Registry** - Success, Failure

Sensitive Privilege Use - Success, Failure

- ✓ **Interactive Logon: Display User Information when the Session is Locked -** Enabled
- ✓ **interactive logon: Do Not Display Last User Name -** Enabled
- ✓ **Interactive logon: Do Not Require CTRL+ALT+DEL -** Disabled
- ✓ **Interactive logon: Message Text for Users Attempting to Log On –** ***'By using this computer system you are subject to the 'Computer Systems Policy' of NUST CYBER SECURITY TEAM. The policy is available on the NCST Intranet and should be checked regularly for any updates'***
- ✓ **Interactive logon: Message Title for Users Attempting to Log on-** For example ***'Warning – Authorized Users Only – Disconnect now if you are not unauthorized to use this system'***

Test and verify

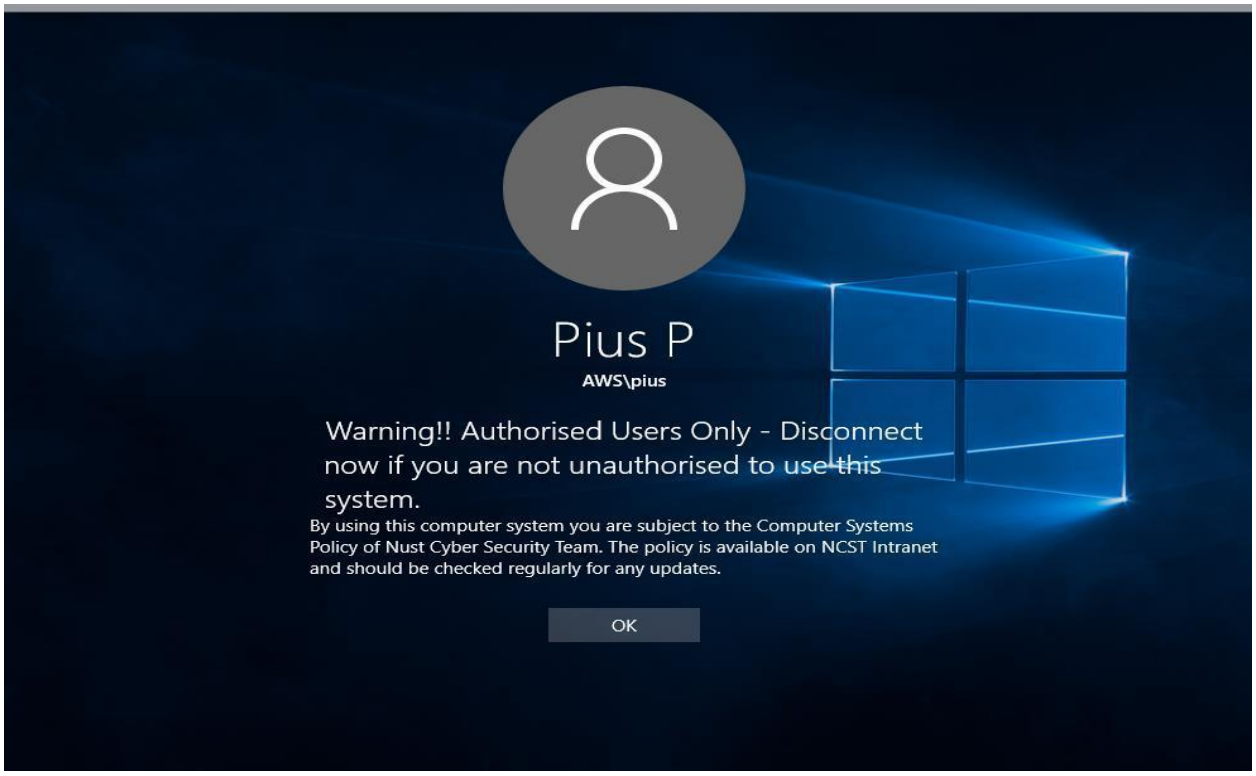
Run gpupdate /force on the server and login to your client with any of the account users.

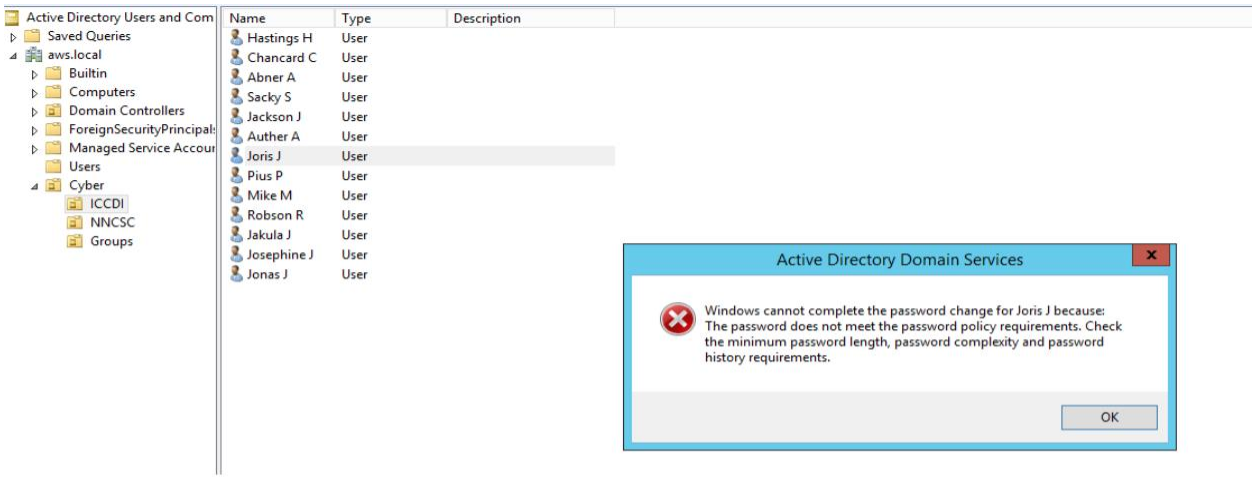
Generate a report for GPO and show your report to your captain

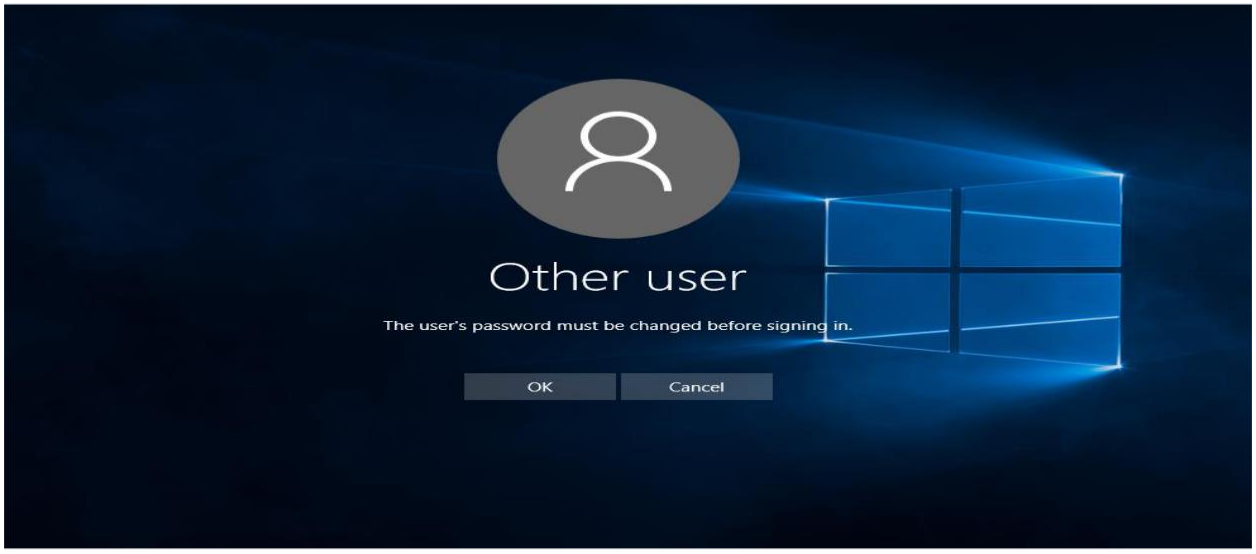
Did you succeed?

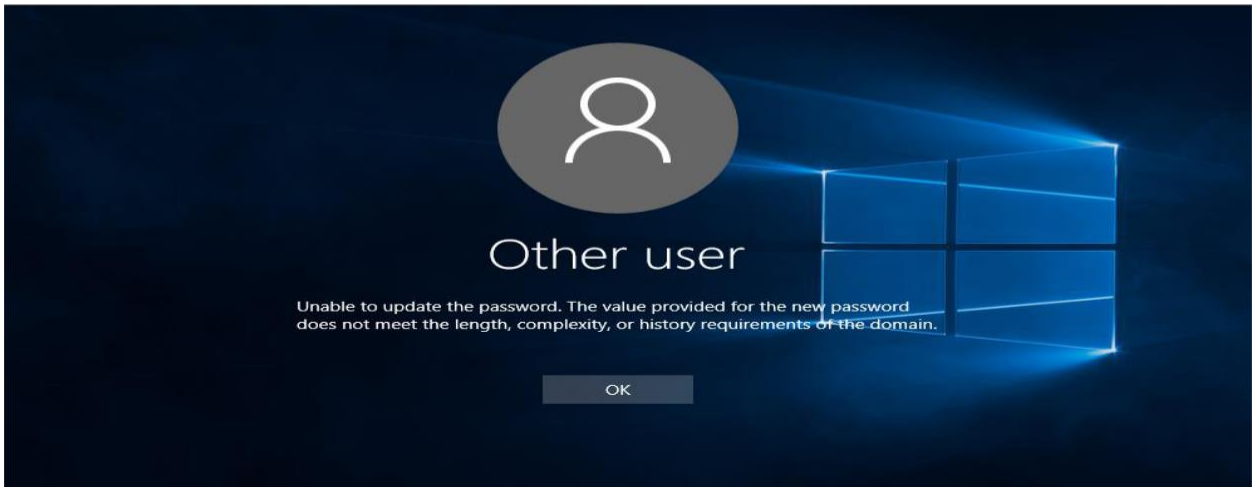
Are the GPO applying on the clients?

Are there some challenges?




Active Directory Users and Com
Saved Queries
aws.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Cyber
ICCDI
NNCSC
Groups
Name
Type
Description
Hastings H
Chancard C
Abner A
Sacky S
Jackson J
Auther A
Joris J
Pius P
Mike M
Robson R
Jakula J
Josephine J
Jonas J
User
Active Directory Domain Services
Windows cannot complete the password change for Joris J because:
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
OK


Other user
The user's password must be changed before signing in.
OK
Cancel


Other user
Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.
OK

Challenge 4

Generate an html GPO report both on the server and on client.

Configure firewall settings using group policy that only apply to ICCDI but should not apply to NNCSC.

4. Homework challenge

1. Find out how to add following users on NNCSC OU using command prompt or PowerShell.

   Comrade
   Jackson
   Gotty
   Alicia
   Ronny
   Van wyk
   James
2. Find out more other security settings that you can apply using Group Policy Management.
3. Find out on how to map a drive and only the member of that group must see it and have access to it.