EC-Council

codered
FROM EC-COUNCIL

CHAPTER 4

IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 4:
Identification, Authentication, and Authorization

SCENARIO

The most serious risk faced by organizations involves unauthorized access to sensitive data. To control data breach events, organizations require strong identification, authentication, and authorization mechanisms to effectively manage the access to critical assets and sensitive data. The labs in this module will provide real-time experience in using the various methods and techniques employed for the identification, authentication, and authorization of users who access critical assets and resources.

OBJECTIVE

The objective of this lab is to provide expert knowledge in identifying, authenticating, and authorizing users who access critical assets and resources. This lab includes the following tasks:

- Implementation of access control policies in Windows and Linux machines

- Implementation of role-based access control using tools such as Windows Admin Center (WAC)

- Implementation of centralized authentication using Windows utilities

OVERVIEW OF IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most commonly used technique for authenticating the users in the network and applications.

Authentication involves verifying the credentials provided by a user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network.

Authorization refers to the process of providing permission to access the resources or perform an action on the network. Admin can decide the user privileges and access permissions of users on a multiuser system.

LAB TASKS

Cyber security professionals or a security professionals use numerous tools and techniques to implement access control policies. The recommended labs that will assist you in learning various identification, authentication and authorization techniques include:

01 **Implement Access Controls in Windows Machine**

02 **Manage Access Controls in Linux Machine**

03 **Implement Role-Based Access Control in windows Admin Center (WAC)**

04 **Implement Centralized Authentication Mechanism**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

Access control is a method of limiting the access of an organization’s resources for the users.

LAB SCENARIO

A security professional must have the required knowledge to manage objects in the Active Directory using different types of accounts and know the application of account policies using GPO in Windows machine.

OBJECTIVE

This lab demonstrates the implementation of access control policies in Windows machine.

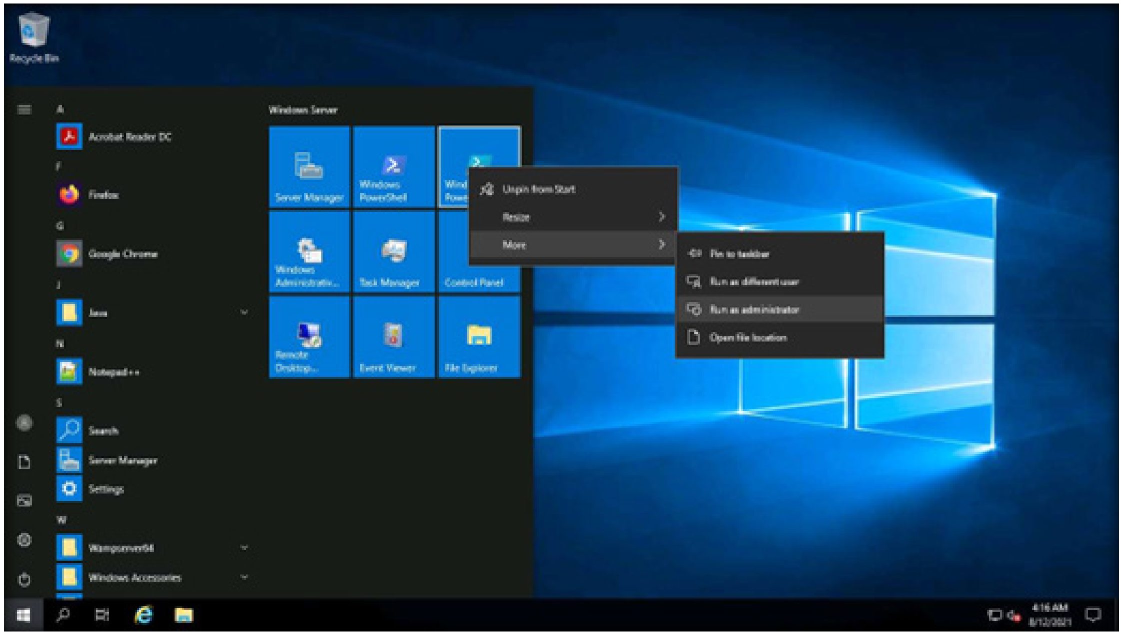
OVERVIEW OF ACCESS CONTROL

An access control function uses identification, authentication, and authorization mechanisms to identify, authenticate, and authorize the user who requests access to a specific resource. The access permissions determine the approvals or permissions provided to a user for accessing a system and other resources. A crucial aspect of implementing an access control is to maintain the integrity, confidentiality, and availability of information.

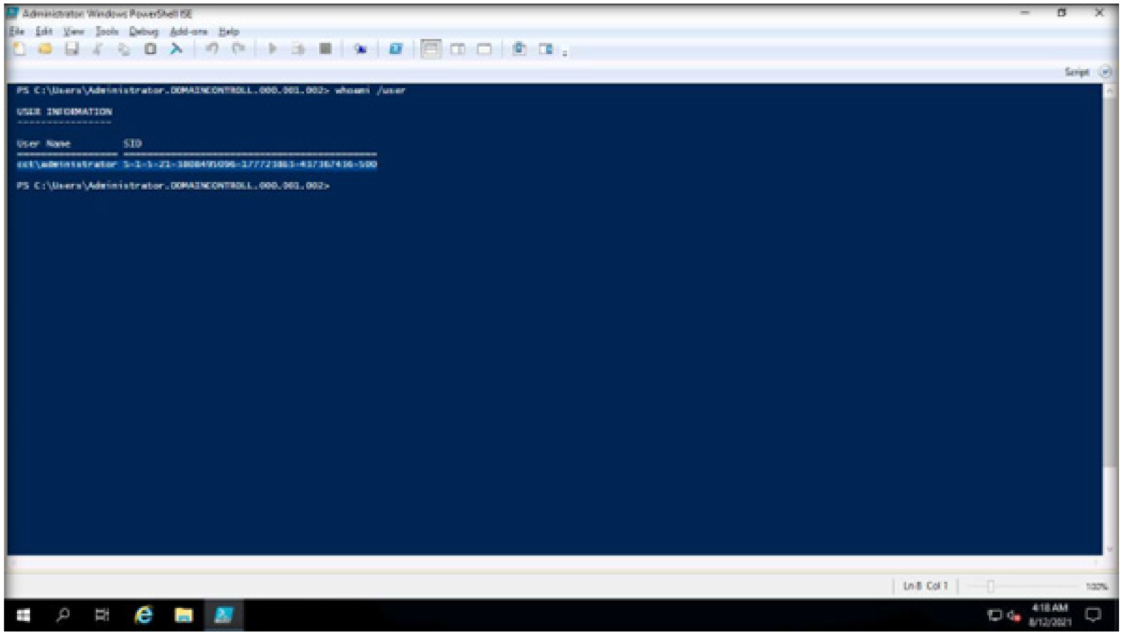
EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the AD Domain Controller virtual machine.
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.
Note: The networks screen appears, click Yes.
Note: If a Shutdown Event Tracker window appears, click Cancel.
3. Before implementing access control policies, we will first examine the properties of the current Administrator account.
4. Click Start icon on the Desktop, right-click Windows PowerShell and navigate to More Run as administrator.
Note: If User Account Control pop-up appears, click Yes to continue.

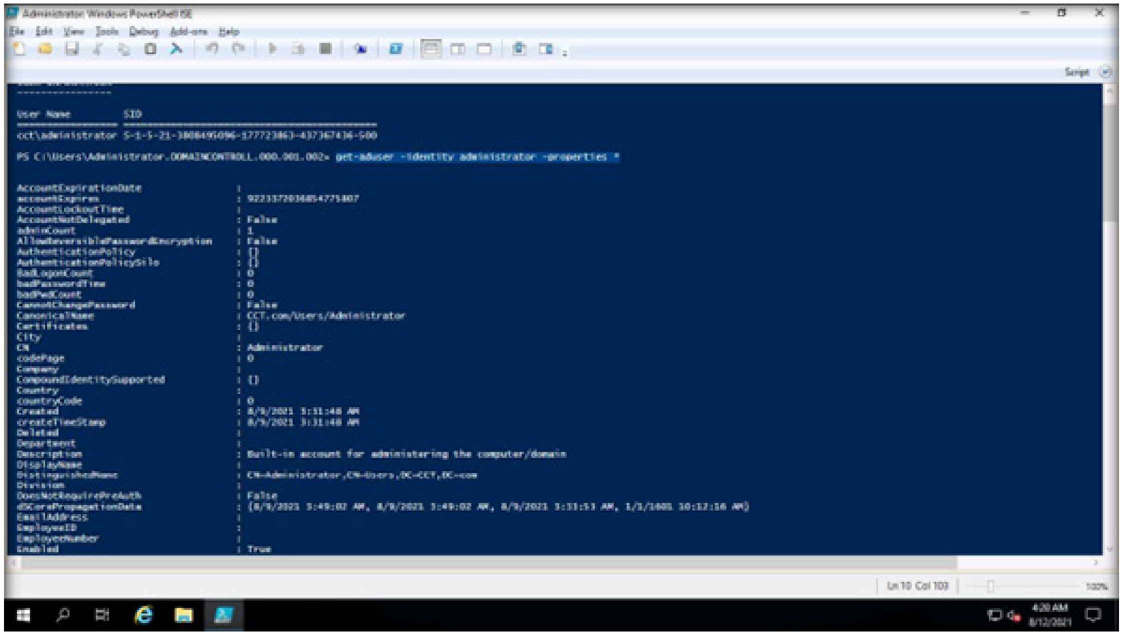


5. In the PowerShell, type whoami /user and press Enter to display the details regarding Security ID (SID) and other additional information of the current user.
Note: User accounts are identified in the system by their unique numbers. In Windows, this number is the Security Identifier (SID). In Linux, it is the User Identifier (UID).


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Ln 8 Col 1
100%
4:18 AM
8/12/2021

```
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> whoami /user

USER INFORMATION
----------------

User Name         SID
================= =============================================
cct\administrator S-1-5-21-1808495096-1777723863-4173167436-500

PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

6. Now, type get-aduser -identity administrator -properties * and press Enter to display user account information.



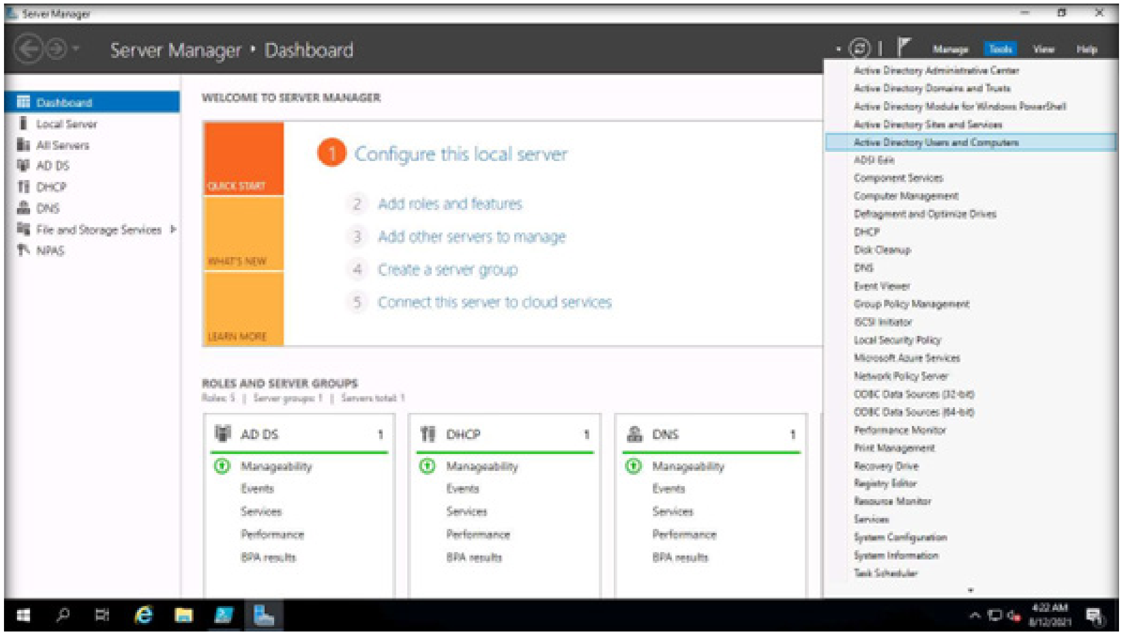
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Ln 10 Col 103
100%
4:20 AM
8/12/2021

```
User Name          SID
================== ==============================================
cct\administrator  S-1-5-21-3808495096-177723863-437367436-500

PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> get-aduser -identity administrator -properties *


AccountExpirationDate                : 
accountExpires                       : 9223372036854775807
AccountLockoutTime                   : 
AccountNotDelegated                  : False
adminCount                           : 1
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : CCT.com/Users/Administrator
Certificates                         : {}
City                                 : 
CN                                   : Administrator
codePage                             : 0
Company                              : 
CompoundIdentitySupported            : {}
Country                              : 
countryCode                          : 0
Created                              : 8/9/2021 3:31:48 AM
createTimeStamp                      : 8/9/2021 3:31:48 AM
Deleted                              : 
Department                           : 
Description                          : Built-in account for administering the computer/domain
DisplayName                          : 
DistinguishedName                    : CN=Administrator,CN=Users,DC=CCT,DC=com
Division                             : 
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {8/9/2021 3:49:02 AM, 8/9/2021 3:49:02 AM, 8/9/2021 3:33:53 AM, 1/1/1601 10:12:16 AM}
EmailAddress                         : 
EmployeeID                           : 
EmployeeNumber                       : 
Enabled                              : True
```

7. Minimize the Administrator: Windows PowerShell window.

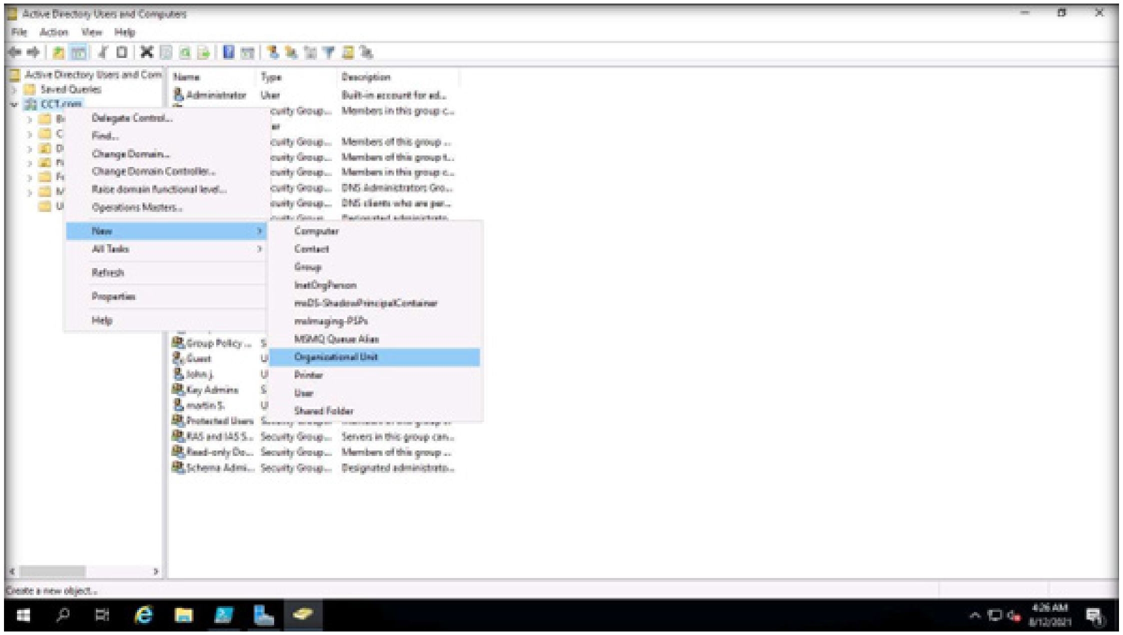
8. Click Start icon in the Desktop, click Server Manager.

9. The Server Manager window appears, click Tools option at the top right corner of the window and select Active Directory Users and Computers option.

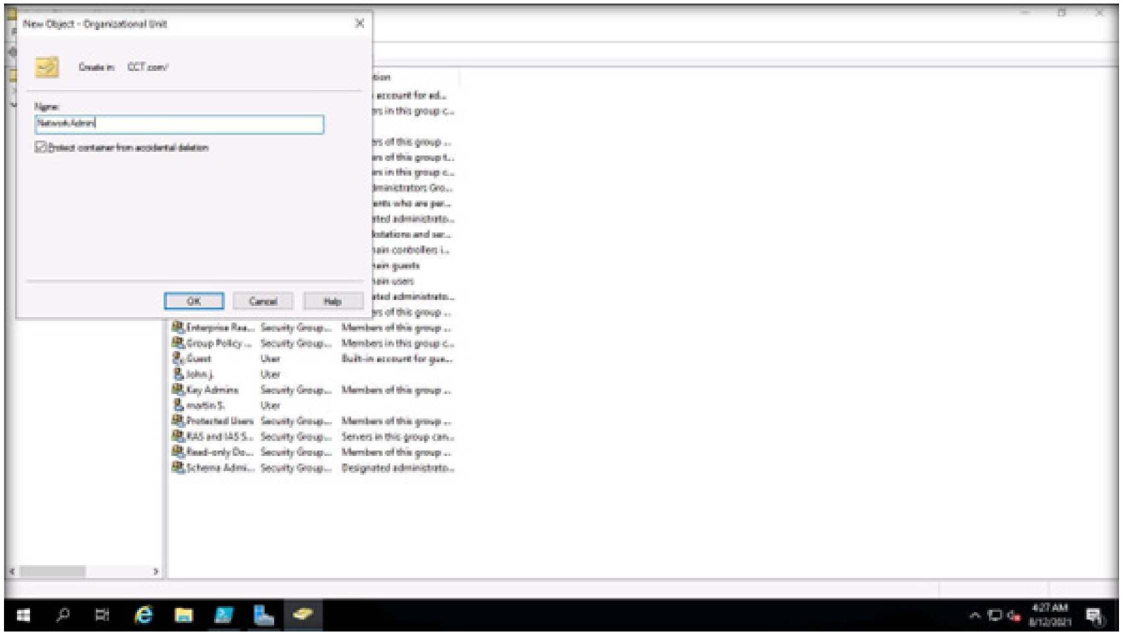


EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

10. Right-click CCT.com domain and navigate to New → Organizational Unit.



11. New Object - Organizational Unit pop-up appears, type NetworkAdmin in the Name field and click OK.



New Object - Organizational Unit

Create in: CCT.com/

Name:

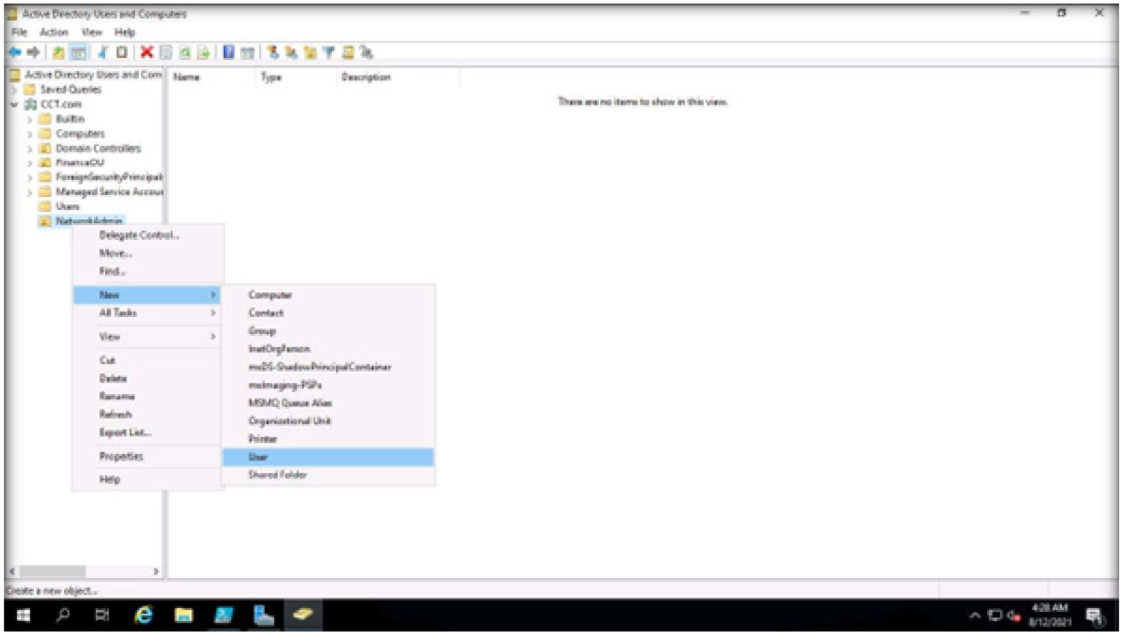
NetworkAdmin

☑ Protect container from accidental deletion

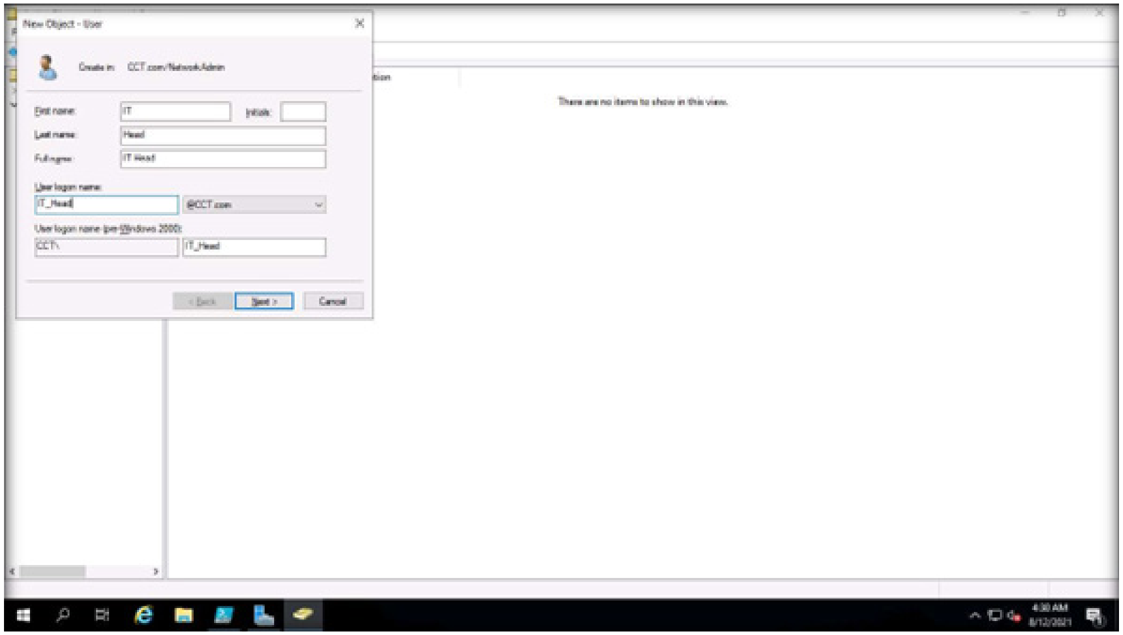
Enterprise Rea...	Security Group...	Members of this group ...
Group Policy ...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
John j.	User	
Key Admins	Security Group...	Members of this group ...
martin S.	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS S...	Security Group...	Servers in this group can...
Read-only Do...	Security Group...	Members of this group ...
Schema Admi...	Security Group...	Designated administrato...

EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

12. Right-click NetworkAdmin Organizational Unit, navigate to New → User.



13. The New Object - User window appears, enter the following details and click Next:
- First name: IT
- Last name: Head
- User logon name: IT_Head



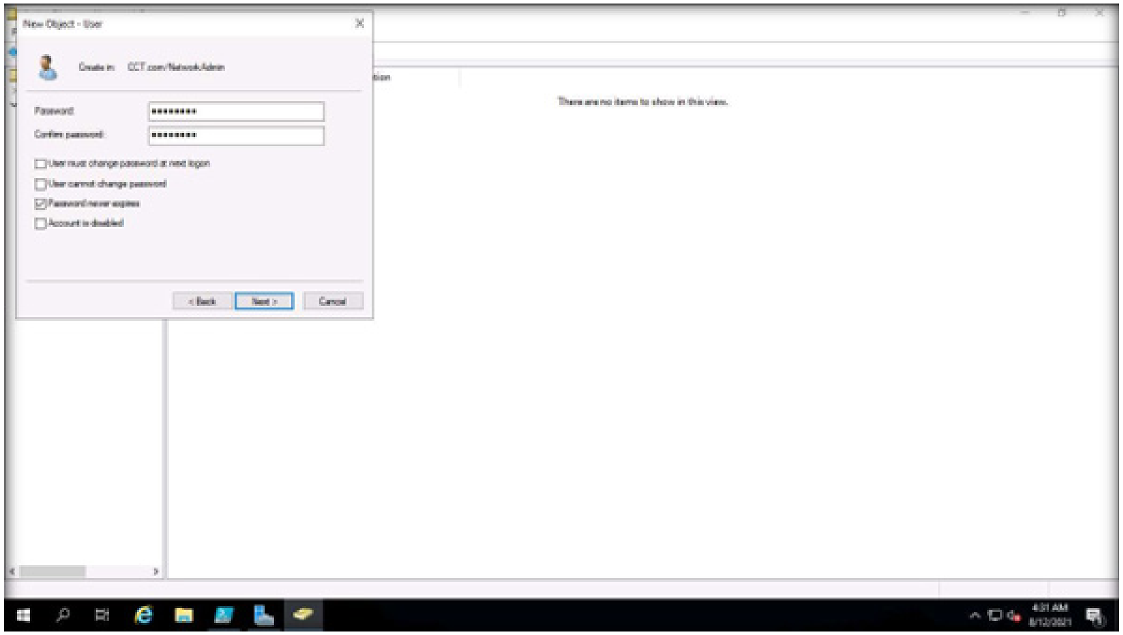
New Object - User

Create in: CCT.com/NetworkAdmin

First name: IT
Initials:
Last name: Head
Full name: IT Head
User logon name: IT_Head @CCT.com
User logon name (pre-Windows 2000): CCT\ IT_Head

There are no items to show in this view.

14. Enter test@123 in both Password and Confirm Password fields. Uncheck User must change password at next logon and check Password never expires option. Click Next.



New Object - User

Create in: CCT.com/NetworkAdmin

Password: •••••••••

Confirm password: •••••••••

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

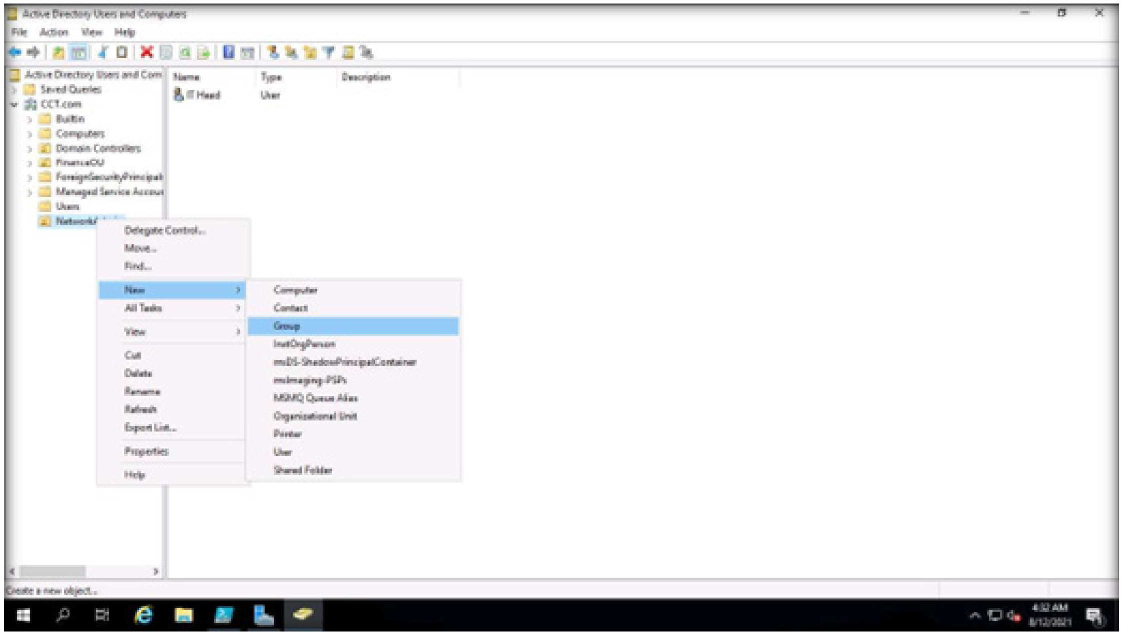
□ Account is disabled

There are no items to show in this view.

15. In the next window, click Finish.

16. Now, we must create a global security group within the NetworkAdmin Organizational Unit.

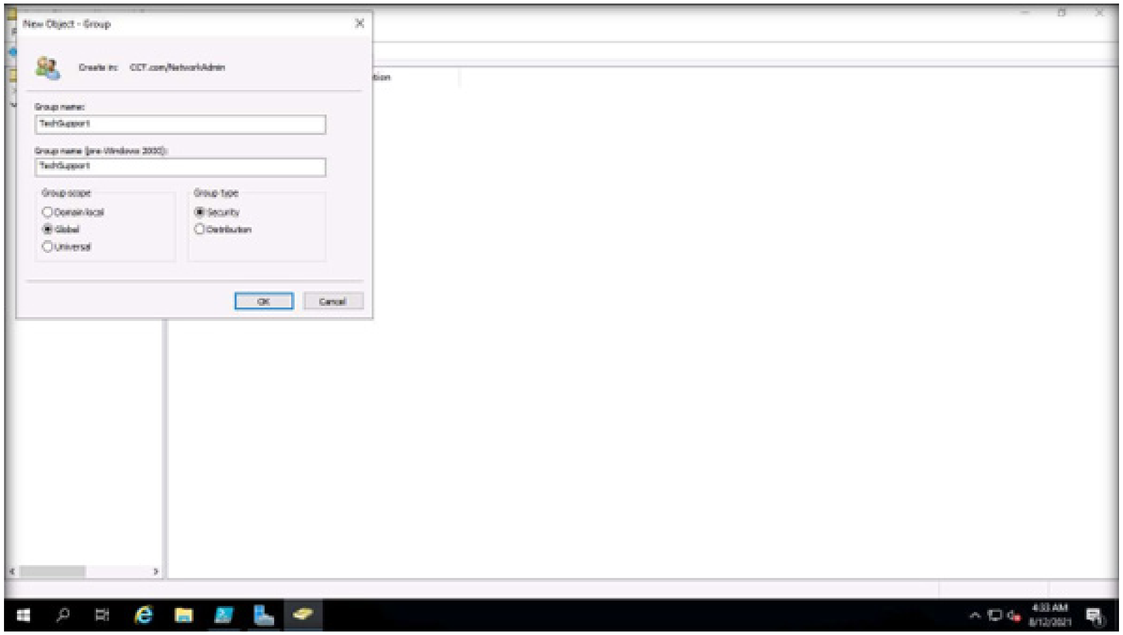
17. Right-click NetworkAdmin Organizational Unit and navigate to New → Group.



Name	Type	Description
IT Head	User	

Create a new object...

18. The New Object - Group window appears, type TechSupport in the Group name, leave all the other options set to default and click OK.



New Object - Group

Create in: CCT.com/NetworkAdmin

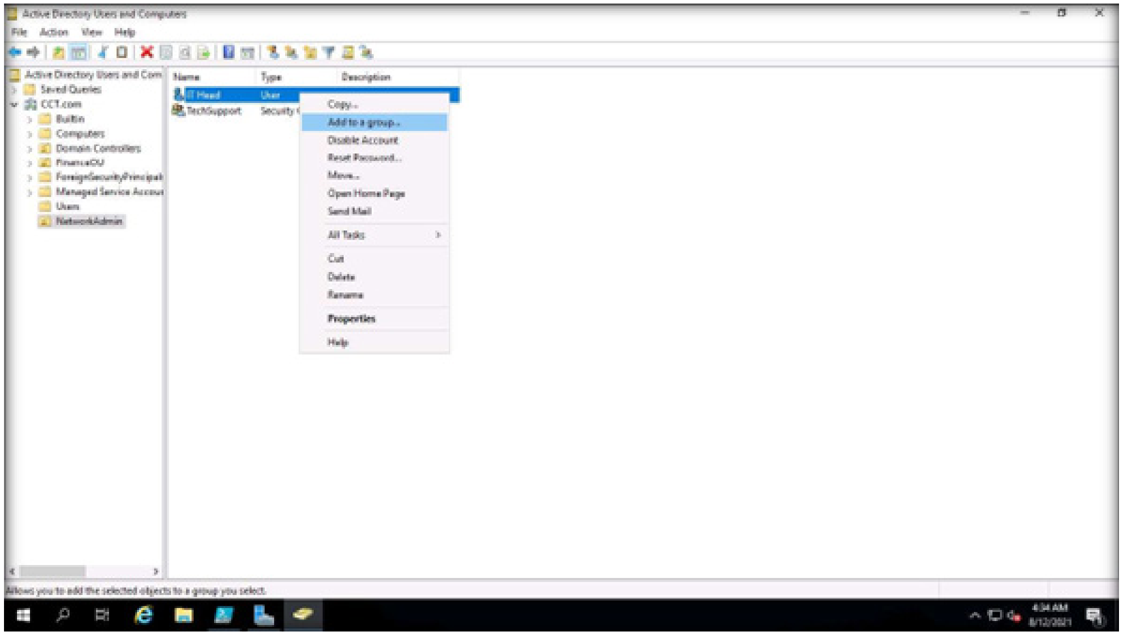
Group name: TechSupport

Group name (pre-Windows 2000): TechSupport

Group scope
○ Domain local
● Global
○ Universal

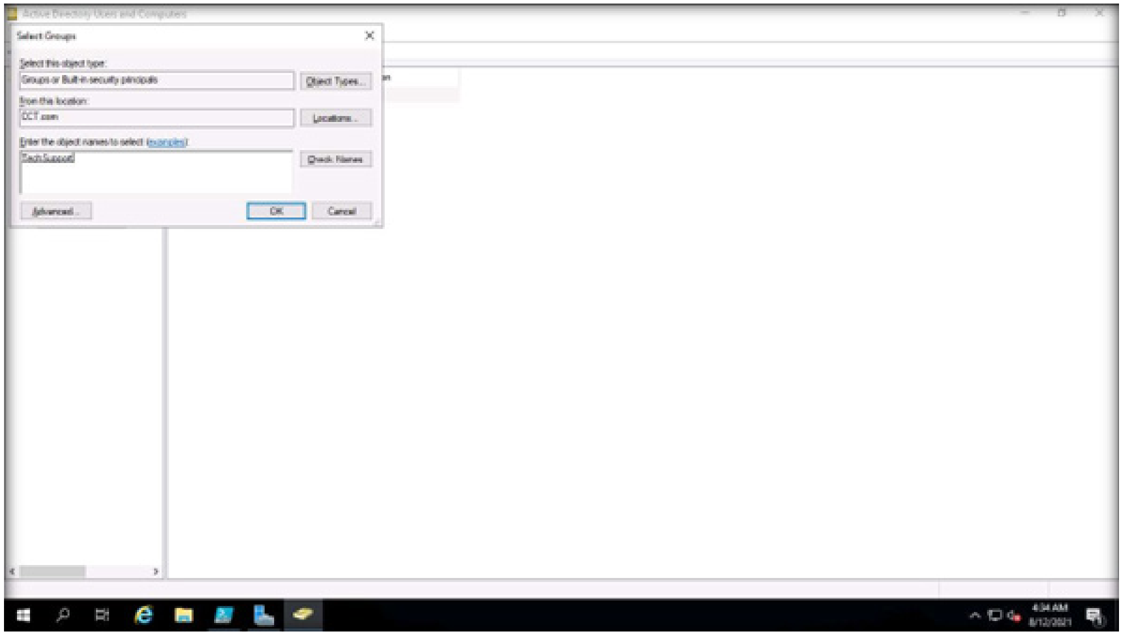
Group type
● Security
○ Distribution

19. Now, add the IT Head account to the TechSupport group. For this, right-click on IT Head and select Add to a group....



Allows you to add the selected objects to a group you select.

20. The Select Groups window appears, in the Enter the object names to select field, type Tech and click Check Names button. Then, the TechSupport name appears, click OK.

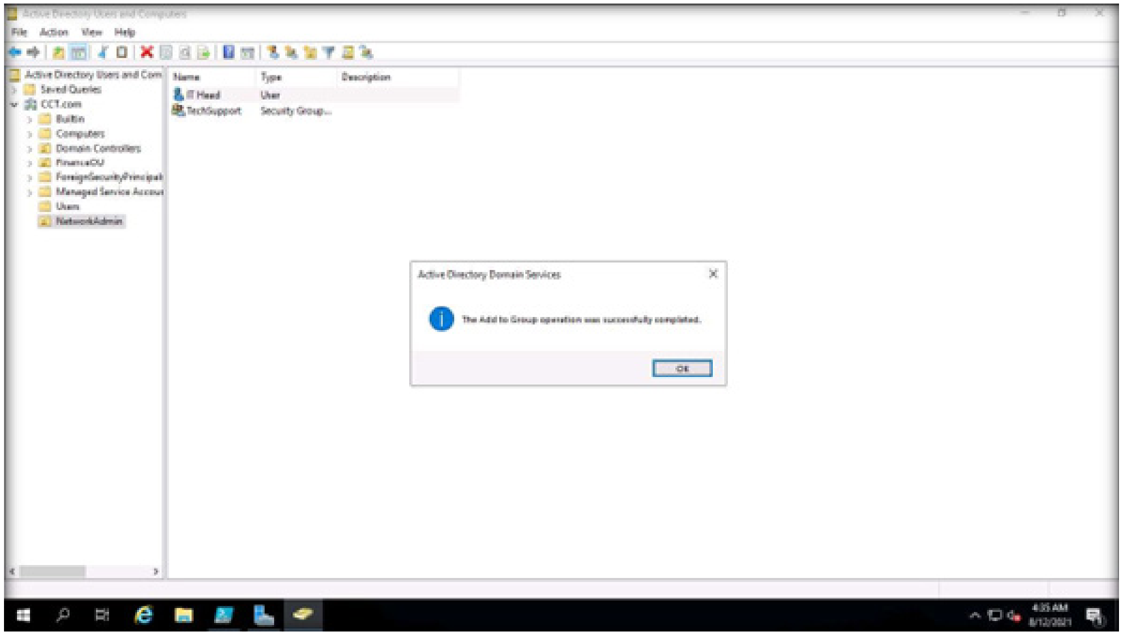


Select this object type:
Groups or Built-in security principals

From this location:
CCT.com

Enter the object names to select (examples):
TechSupport

21. A pop-up appears, indicating the successful addition of a user to the group. Click OK.



Name	Type	Description
IT Head	User	
TechSupport	Security Group...	

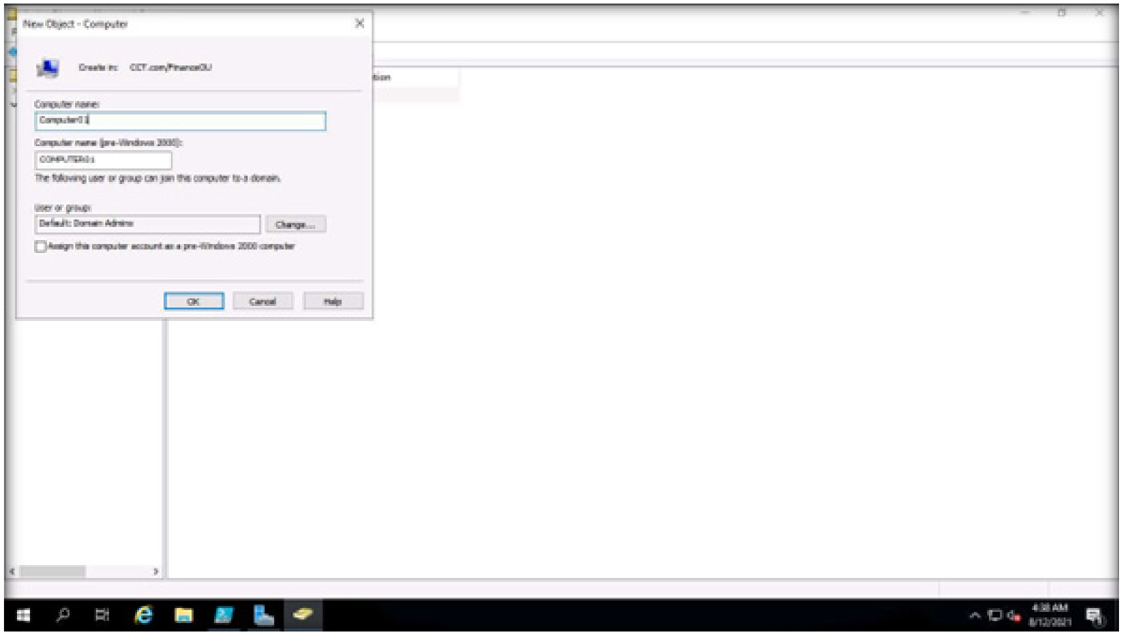
Active Directory Domain Services

The Add to Group operation was successfully completed.

EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

22. Now, right-click FinanceOU Organizational Unit and navigate to New → Computer.

23. The New Object - Computer window appears, type Computer01 in the Computer Name field and click OK



Create in: CCT.com/FinanceOU

Computer name:
Computer01

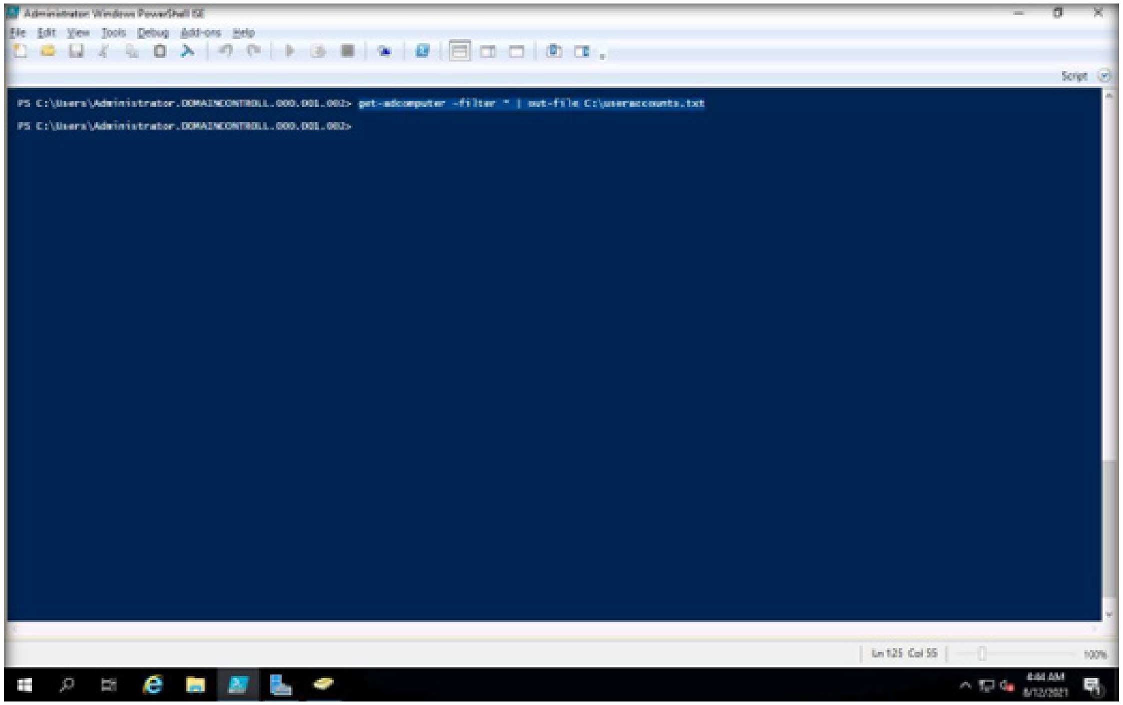
Computer name (pre-Windows 2000):
COMPUTER01

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins

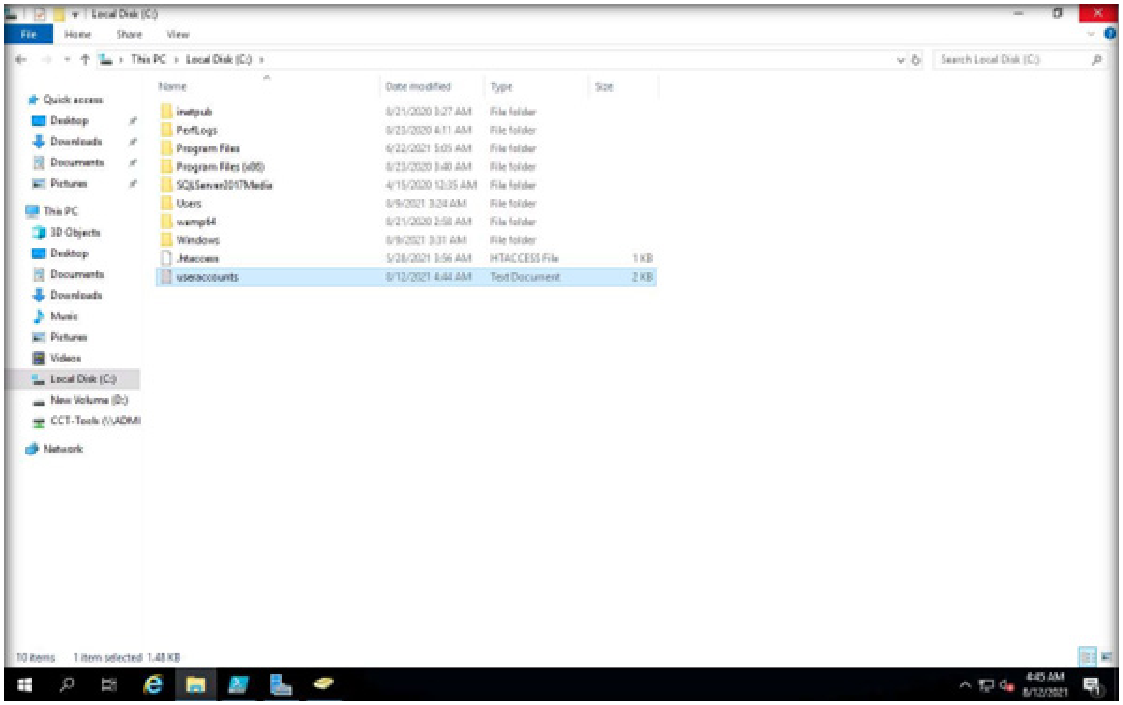
□ Assign this computer account as a pre-Windows 2000 computer

24. Switch to the Administrator: Windows PowerShell window, type get-adcomputer -filter * | out-file C:\useraccounts.txt and press Enter to create a detailed report of all computer objects in the domain.


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Ln 125 Col 55
100%
4:44 AM
8/12/2021

```
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> get-adcomputer -filter * | out-file C:\useraccounts.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

25. Now, navigate to C: drive to see if the useraccounts.txt file exists.



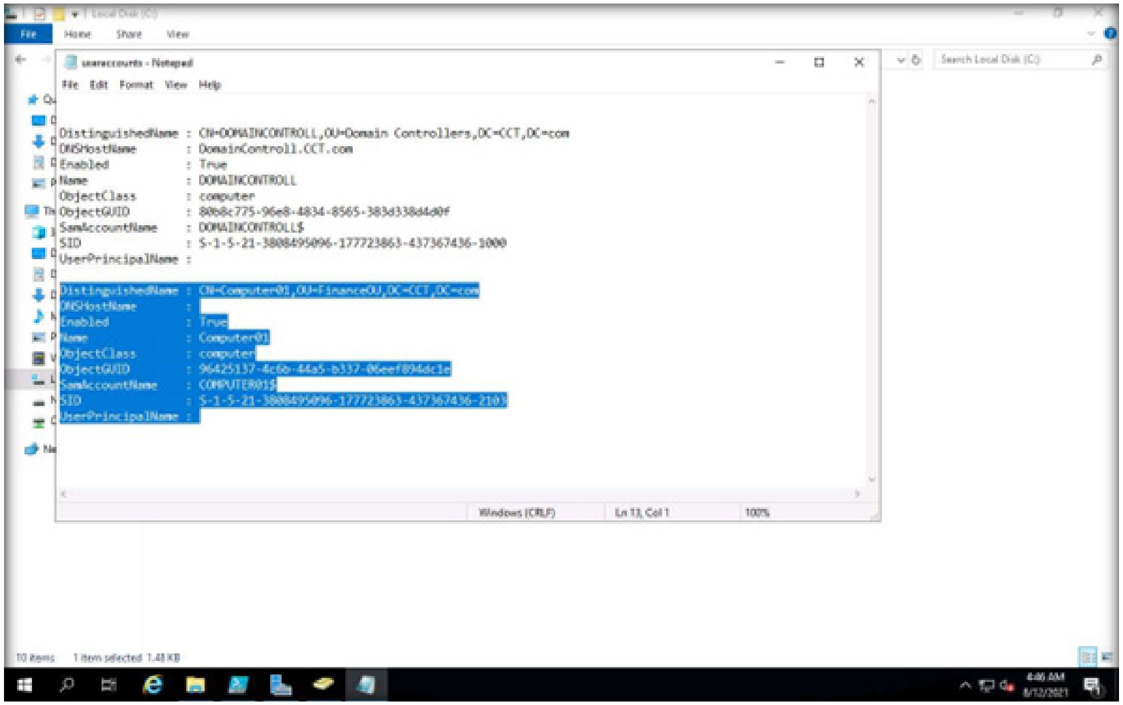
Local Disk (C:)

This PC › Local Disk (C:) ›

Name	Date modified	Type	Size
inetpub	8/21/2020 3:27 AM	File folder	
PerfLogs	8/23/2020 4:11 AM	File folder	
Program Files	6/22/2021 5:05 AM	File folder	
Program Files (x86)	8/23/2020 3:40 AM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
Users	8/9/2021 3:24 AM	File folder	
wamp64	8/21/2020 2:58 AM	File folder	
Windows	8/9/2021 3:31 AM	File folder	
.htaccess	5/28/2021 3:56 AM	HTACCESS File	1 KB
useraccounts	8/12/2021 4:44 AM	Text Document	2 KB

10 items 1 item selected 1.48 KB

26. Double-click useraccounts.txt file to see its content. You can view the newly created user account (Computer01), as shown in the screenshot.

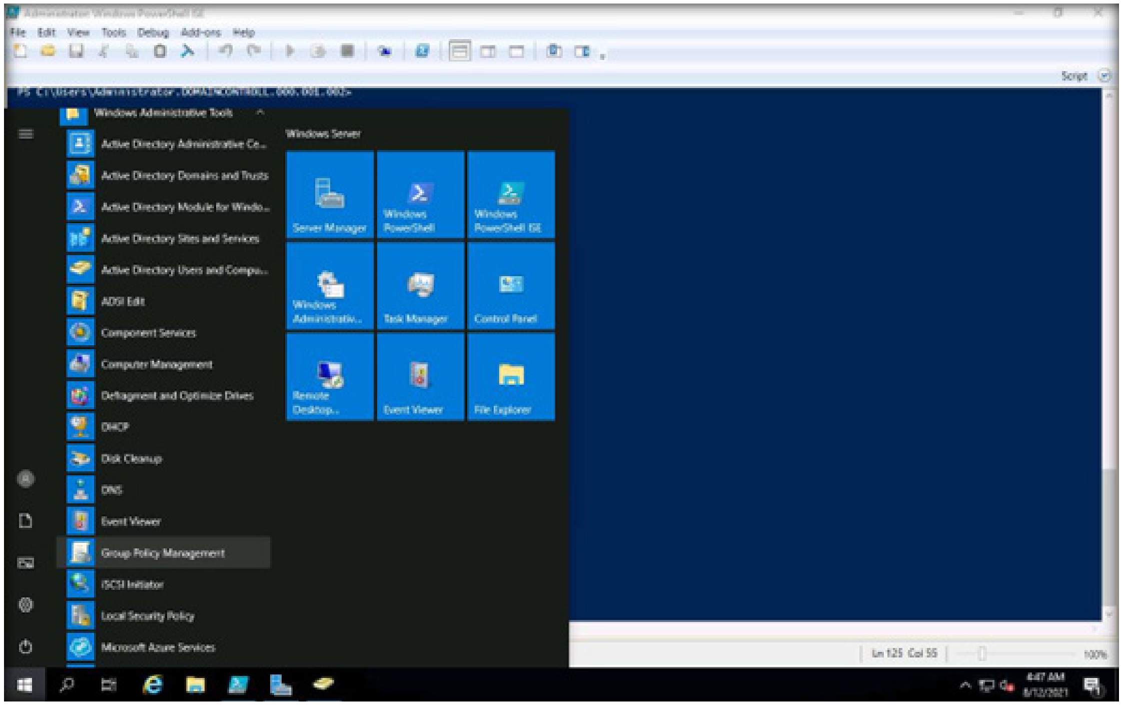


```
DistinguishedName : CN=DOMAINCONTROLL,OU=Domain Controllers,DC=CCT,DC=com
DNSHostName       : DomainControll.CCT.com
Enabled           : True
Name              : DOMAINCONTROLL
ObjectClass       : computer
ObjectGUID        : 80b8c775-96e8-4834-8565-383d338d4d0f
SamAccountName    : DOMAINCONTROLL$
SID               : S-1-5-21-3808495096-177723863-437367436-1000
UserPrincipalName :

DistinguishedName : CN=Computer01,OU=FinanceOU,DC=CCT,DC=com
DNSHostName       :
Enabled           : True
Name              : Computer01
ObjectClass       : computer
ObjectGUID        : 96425137-4c6b-44a5-b337-06eef894dc1e
SamAccountName    : COMPUTER01$
SID               : S-1-5-21-3808495096-177723863-437367436-2103
UserPrincipalName :
```

27. Close all the windows, except Windows PowerShell.

28. Now, we shall modify the existing GPO to set password requirements.

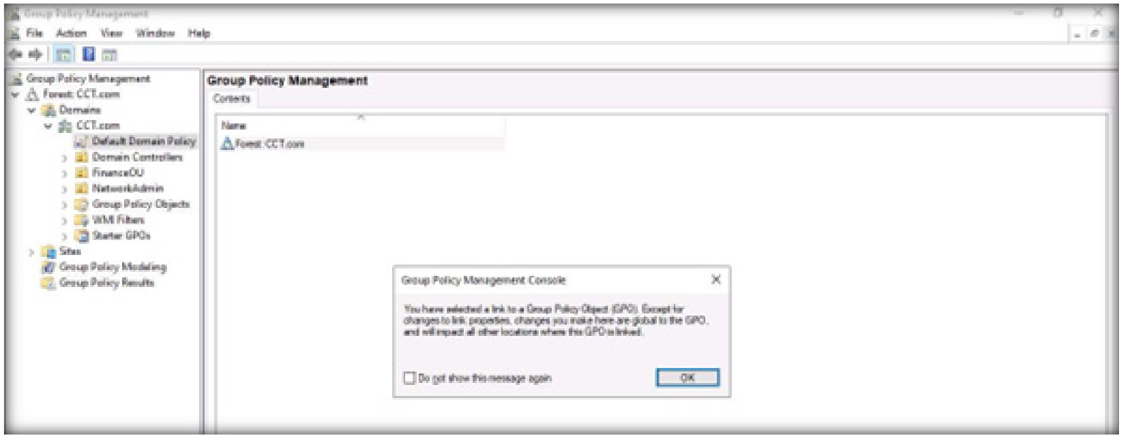
29. To launch Group Policy Management, click Windows Start icon and navigate to Windows Administrative Tools → Group Policy Management.
Note: Alternatively, you can launch Group Policy Management by typing gpmc.msc in Run. To open Run, right-click on Start and click Run.



```
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

30. The Group Policy Management main window appears. Expand the Forest: CCT.com → Domains → CCT.com and select Default Domain Policy, as shown in the screenshot.
Note: The Default Domain Policy is a single password policy that works for all members of a specific domain, it offers no flexibility to have different password polices for different types of users. It is recommended to only use it for password management.

31. In the Group Policy Management Console, click OK.



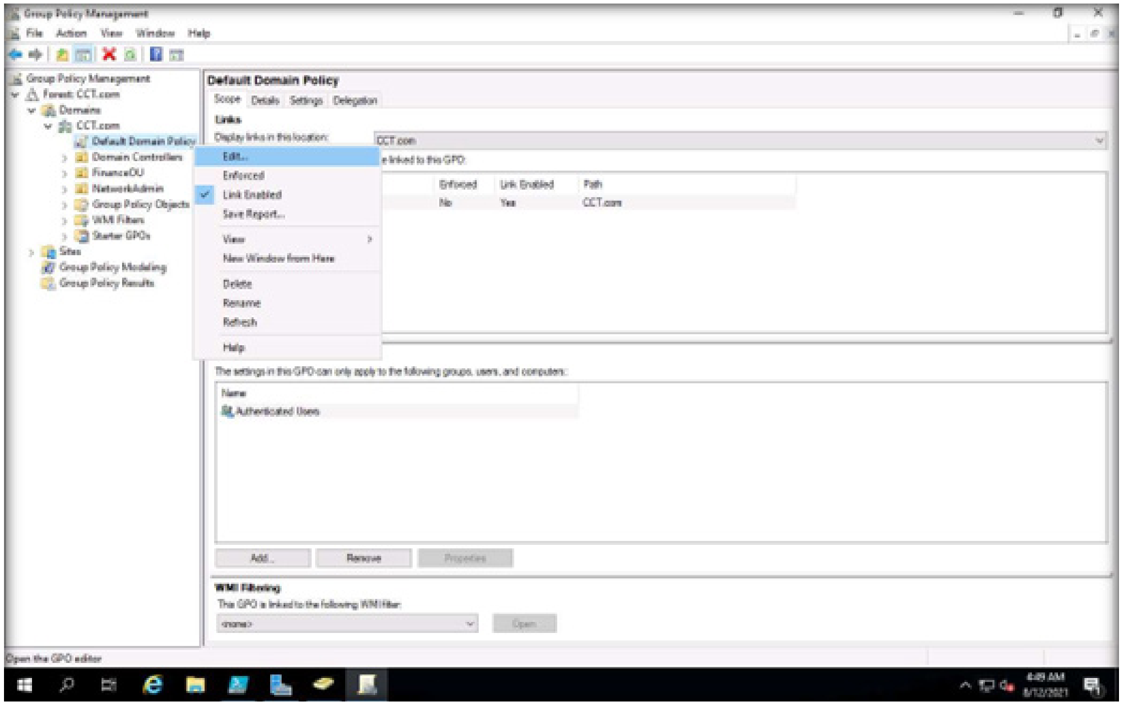
Group Policy Management Console

You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked.

☐ Do not show this message again

OK

32. Right-click Default Domain Policy node and select Edit....



Links

Display links in this location: CCT.com

...e linked to this GPO:

Enforced	Link Enabled	Path
No	Yes	CCT.com

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

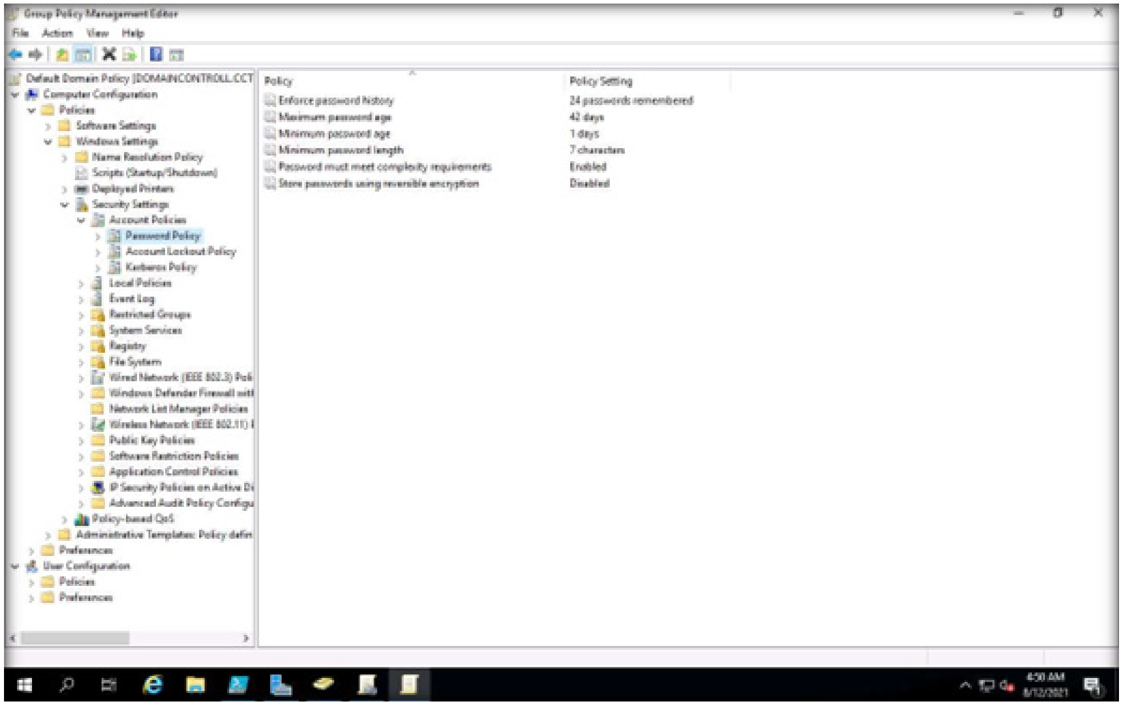
This GPO is linked to the following WMI filter:

<none>

Open the GPO editor

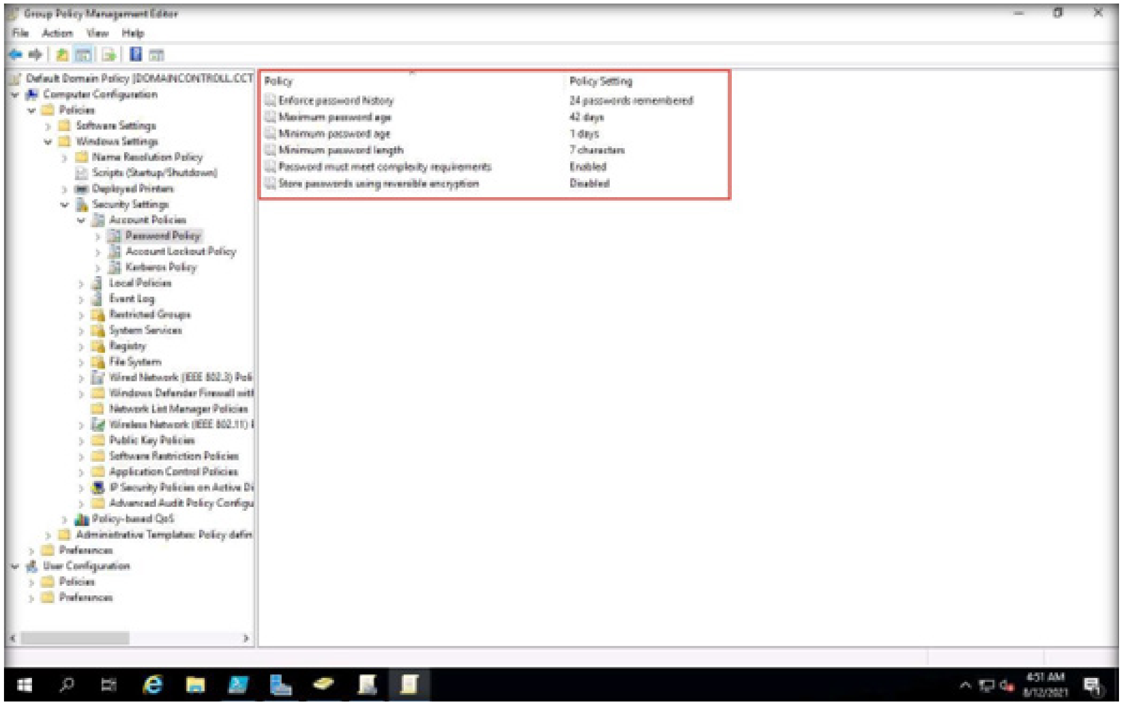
EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

33. In the Group Policy Management Editor window, expand Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies. Click on Password Policy; the password policies will be listed in the right pane.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

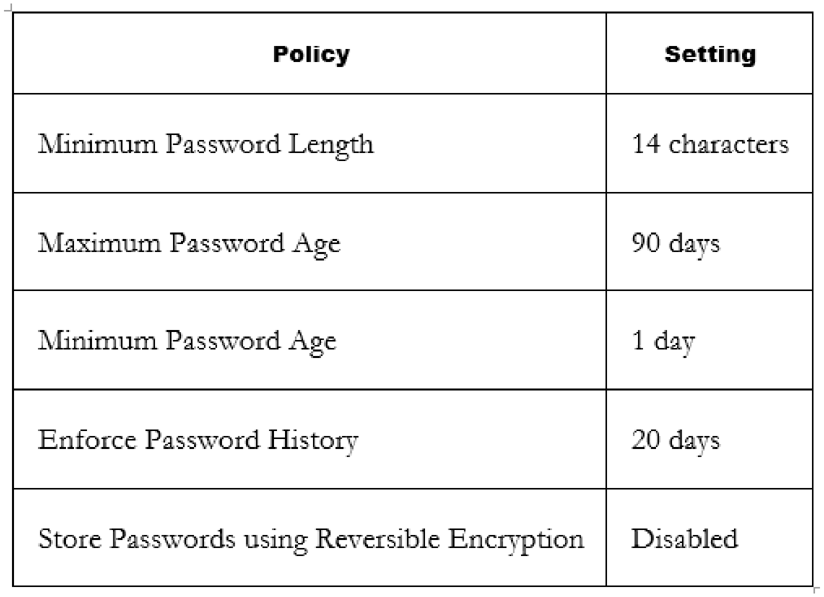
34. You can view the default password policies that are listed in the right-pane, as shown in the screenshot.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

35. We must configure the policies to match the requirements given below. To edit the policy, double-click each of them.

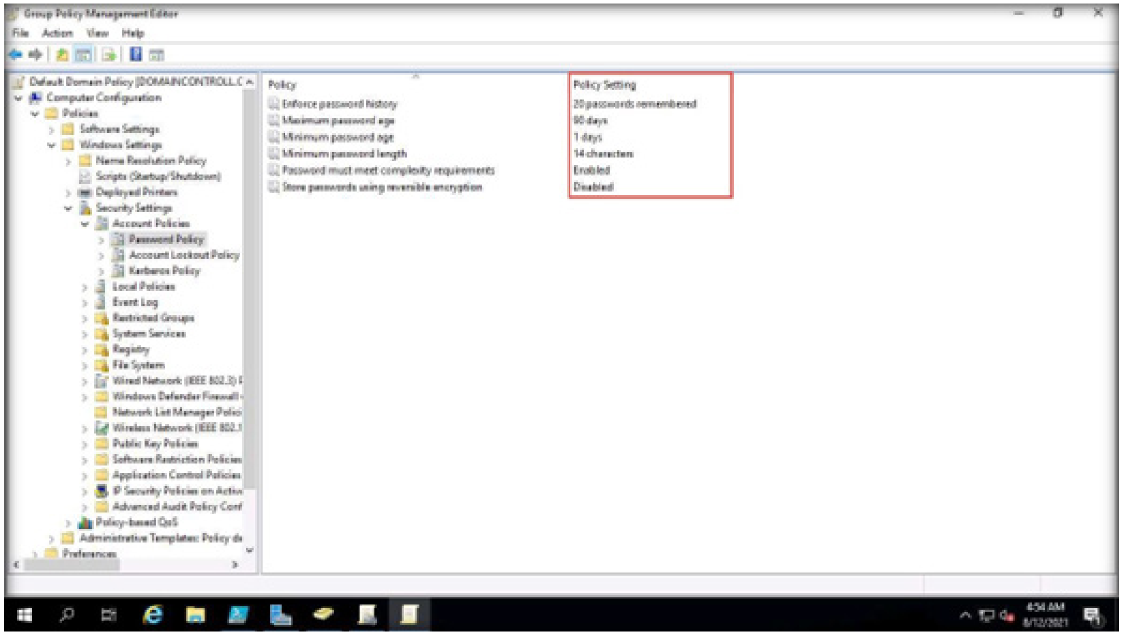
Note: To implement the changes in the Policy, make the desired modifications, then click Apply and click OK.



Policy	Setting
Minimum Password Length	14 characters
Maximum Password Age	90 days
Minimum Password Age	1 day
Enforce Password History	20 days
Store Passwords using Reversible Encryption	Disabled

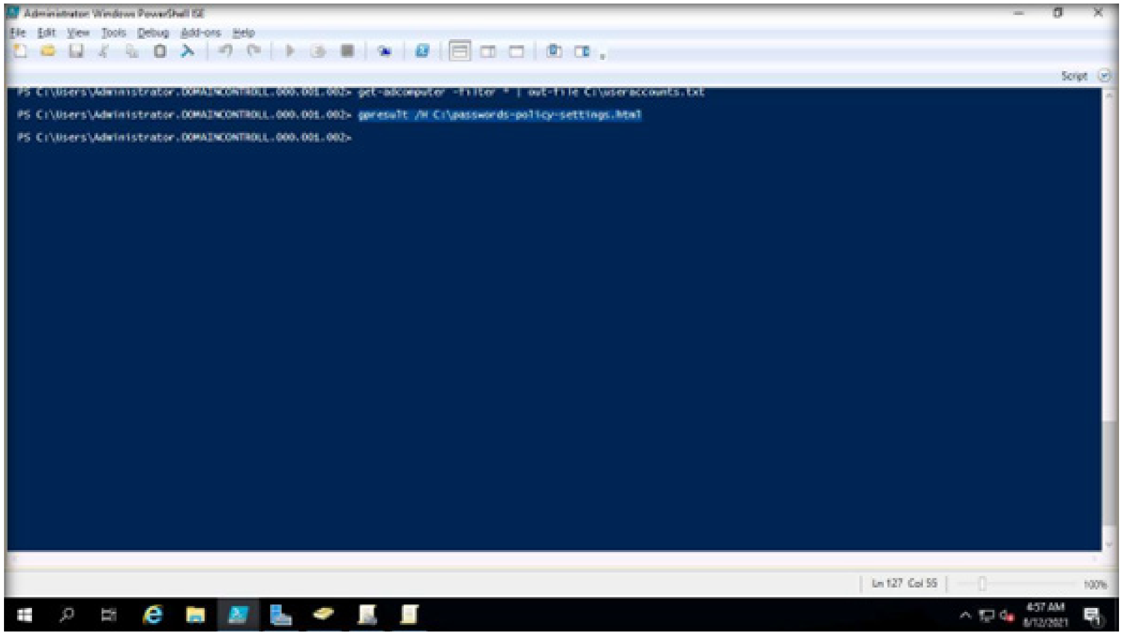
EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

36. The updated Password Policy settings, are shown in the below screenshot.


Group Policy Management Editor
File Action View Help
Default Domain Policy [DOMAINCONTROLL.C
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) P
Windows Defender Firewall
Network List Manager Polic
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Activ
Advanced Audit Policy Conf
Policy-based QoS
Administrative Templates: Policy de
Preferences
4:54 AM
8/12/2021

Policy	Policy Setting
Enforce password history	20 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

37. Switch to Administrator: Windows PowerShell, click to type gpresult /H C:\passwords-policy-settings.html and press Enter to generate the report of password policy settings to update the configuration documentation.

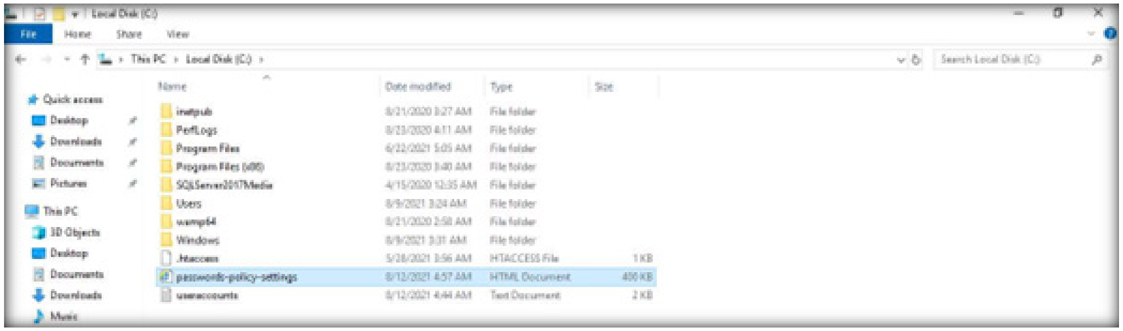


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Ln 127 Col 55
100%
4:57 AM
8/12/2021

```
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> get-adcomputer -filter * | out-file C:\useraccounts.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> gpresult /H C:\passwords-policy-settings.html
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

EXERCISE 1: IMPLEMENT ACCESS CONTROLS IN WINDOWS MACHINE

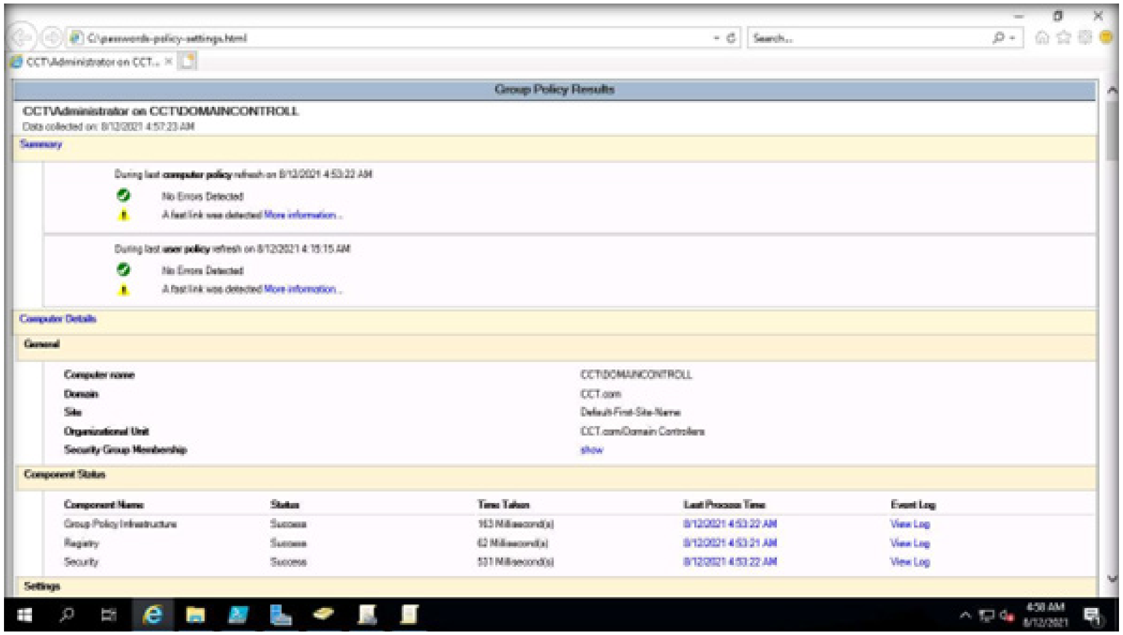
38. Navigate to C: drive to see if the passwords-policy-settings.html file exists.



Name	Date modified	Type	Size
inetpub	8/21/2020 3:27 AM	File folder	
PerfLogs	8/23/2020 4:11 AM	File folder	
Program Files	6/22/2021 5:05 AM	File folder	
Program Files (x86)	8/23/2020 3:40 AM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
Users	8/9/2021 3:24 AM	File folder	
wamp64	8/21/2020 2:58 AM	File folder	
Windows	8/9/2021 3:31 AM	File folder	
.htaccess	5/28/2021 3:56 AM	HTACCESS File	1 KB
passwords-policy-settings	8/12/2021 4:57 AM	HTML Document	400 KB
useraccounts	8/12/2021 4:44 AM	Text Document	2 KB

39. Now, double click the passwords-policy-settings.html file.

40. A browser window appears displaying the Group Policy Results file, as shown in the screenshot.
Note: If browser notification appears, click Ask me later.



C:\passwords-policy-settings.html
Search...
CCT\Administrator on CCT...

Group Policy Results

CCT\Administrator on CCT\DOMAINCONTROLL
Data collected on: 8/12/2021 4:57:23 AM

Summary

During last **computer policy** refresh on 8/12/2021 4:53:22 AM
✓ No Errors Detected
⚠ A fast link was detected More information...

During last **user policy** refresh on 8/12/2021 4:18:15 AM
✓ No Errors Detected
⚠ A fast link was detected More information...

Computer Details

General

Computer name	CCT\DOMAINCONTROLL
Domain	CCT.com
Site	Default-First-Site-Name
Organizational Unit	CCT.com/Domain Controllers
Security Group Membership	show

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	163 Millisecond(s)	8/12/2021 4:53:22 AM	View Log
Registry	Success	62 Millisecond(s)	8/12/2021 4:53:21 AM	View Log
Security	Success	531 Millisecond(s)	8/12/2021 4:53:22 AM	View Log

Settings

41. This file displays a detailed report on the implemented account policies. You can explore it further.

42. This concludes the demonstration of implementing access control policies in Windows machine.

43. Close all the opened windows.

44. Turn off the AD Domain Controller virtual machine.

EXERCISE 2: MANAGE ACCESS CONTROLS IN LINUX MACHINE

Access control assists in maintaining the integrity, confidentiality, and availability of the information and resources.

LAB SCENARIO

A security professional must have the required knowledge to manage access control policies on a Linux machine. First, we will create local user accounts and groups on a system. Then, we will create directories and files where access control policies will be implemented. Further, we will configure the ownership to these directories and files.

OBJECTIVE

This lab demonstrates implementation of access controls in Linux machine.

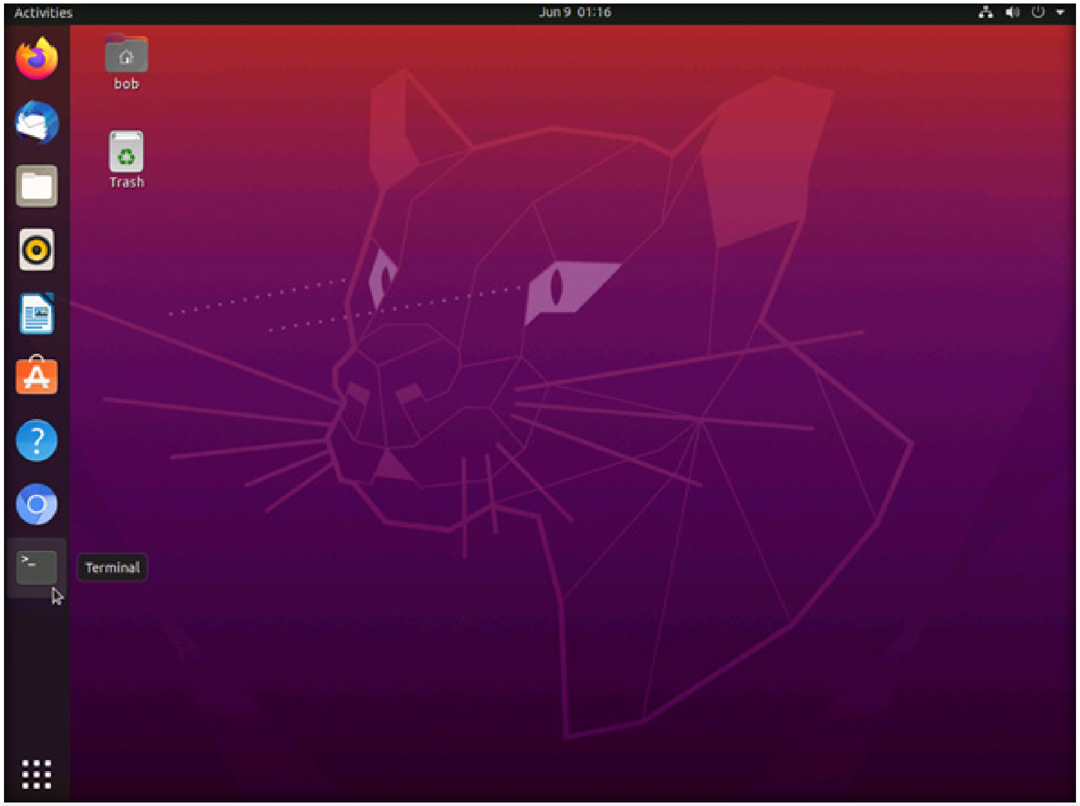
OVERVIEW OF ACCESS CONTROL

The principles of access control describe the access permission levels of users in detail. By enabling the access control process, the security of processes and resources can be ensured.

Note: Here, for demonstration purposes, we are using Attacker Machine-1 to show the implementation of access control policies in Linux machine.
Note: Ensure that PfSense Firewall virtual machine is running.

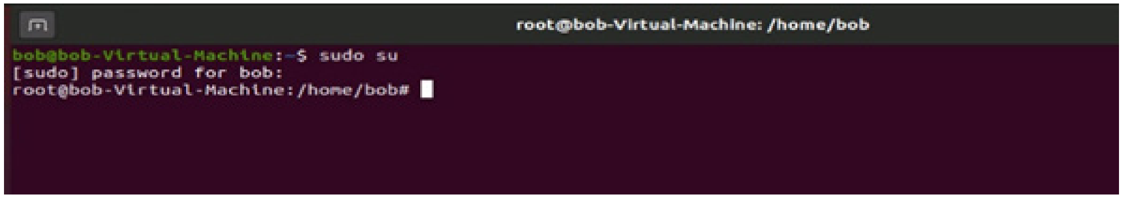
1. Turn on the Attacker Machine-1 virtual machine.
2. Click to select Bob account, in the Password field, type user@123 and press Enter to sign in.
3. First, we will create two sample users and two groups on this machine and configure the password of these the two users.
4. In the left pane, under the Activities list, click the Terminal icon to open the Terminal window
   Note: If the Software Updater pop-up appears, click Remind Me Later.

EXERCISE 2: MANAGE ACCESS CONTROLS IN LINUX MACHINE



5. In the Terminal window, type sudo su and press Enter to run programs as the root user.

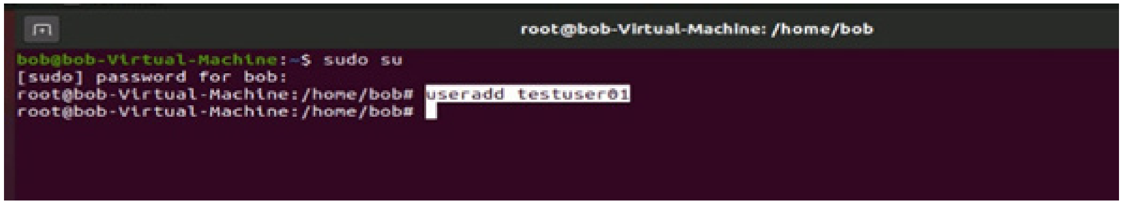
6. In the [sudo] password for bob field, type user@123 as a password and press Enter.
Note: The password typed by you will not be visible.



root@bob-Virtual-Machine: /home/bob

```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# 
```

7. Now, type useradd testuser01 and press Enter to create a new user.



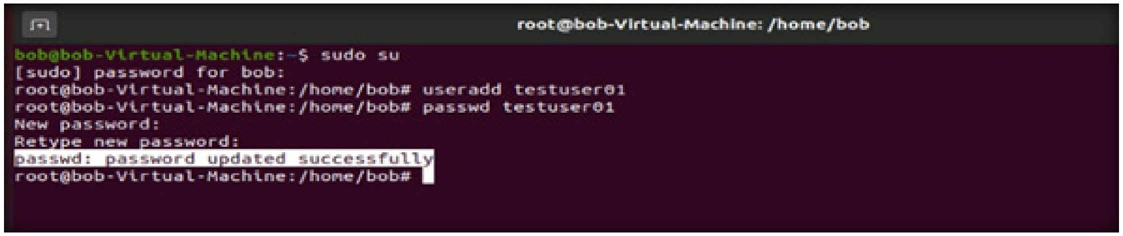
root@bob-Virtual-Machine: /home/bob

```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob#
```

EXERCISE 2: MANAGE ACCESS CONTROLS IN LINUX MACHINE

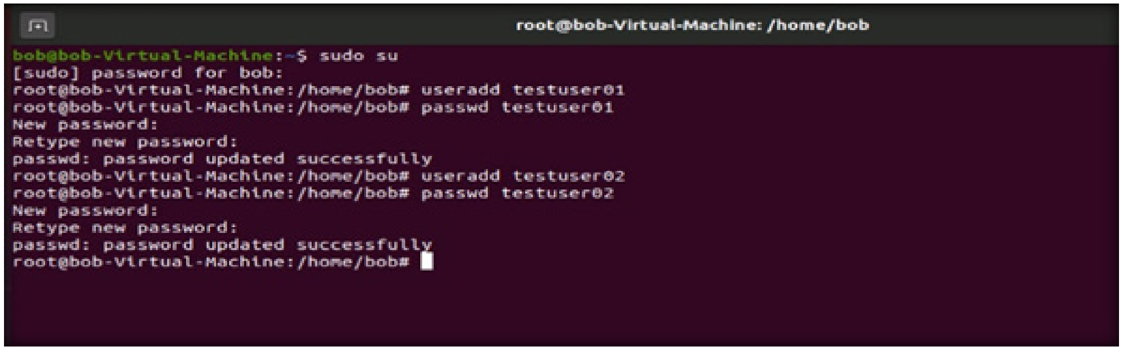
8. Type passwd testuser01 and press Enter to set password for the user (testuser01).

9. The New password field appears, type test@123 and Enter. In the Retype new password field, enter the same password (test@123) and press Enter to set the password. Subsequently, a password updated successfully message appears, as shown in the screenshot.
Note: You can set any user password of your choice.



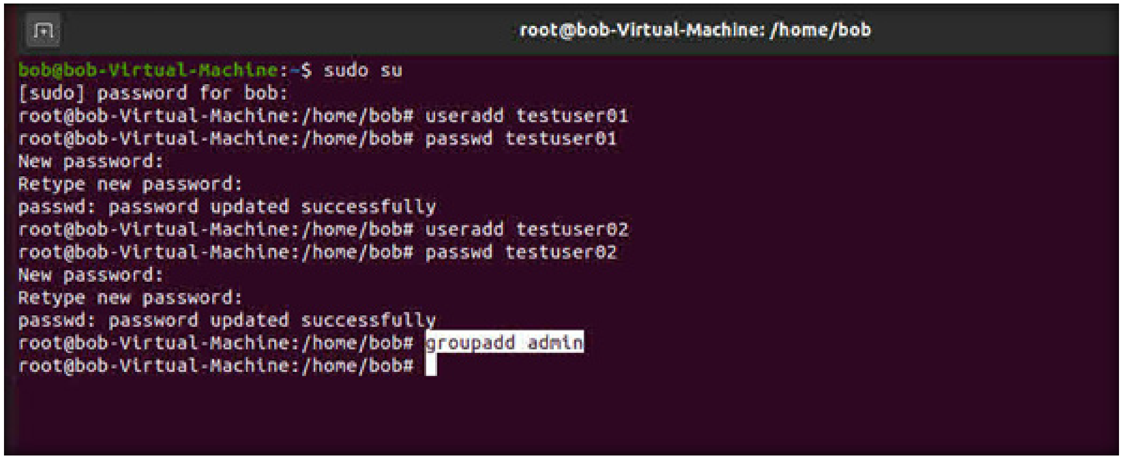
```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob#
```

10. Similarly, perform steps#7-9 to create another user account with username testuser02 and password test@123.



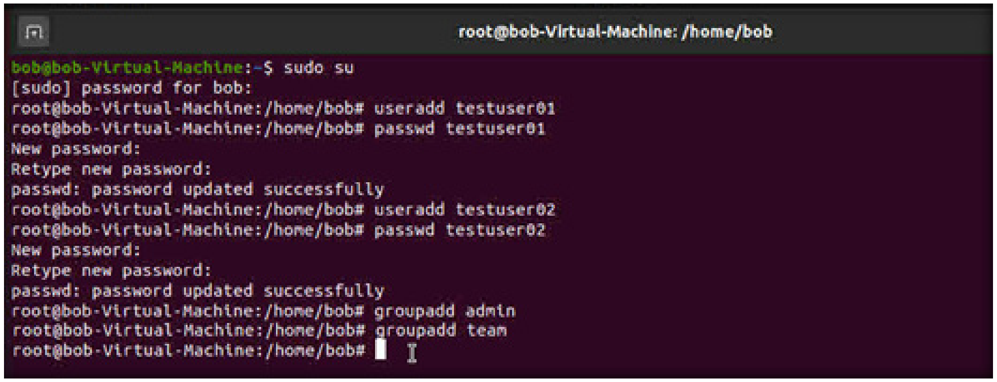
```
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# 
```

11. Now, we shall create a new group. For this, type groupadd admin and press Enter.



```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob#
```

12. Similarly, create another group named team by issuing the command groupadd team.

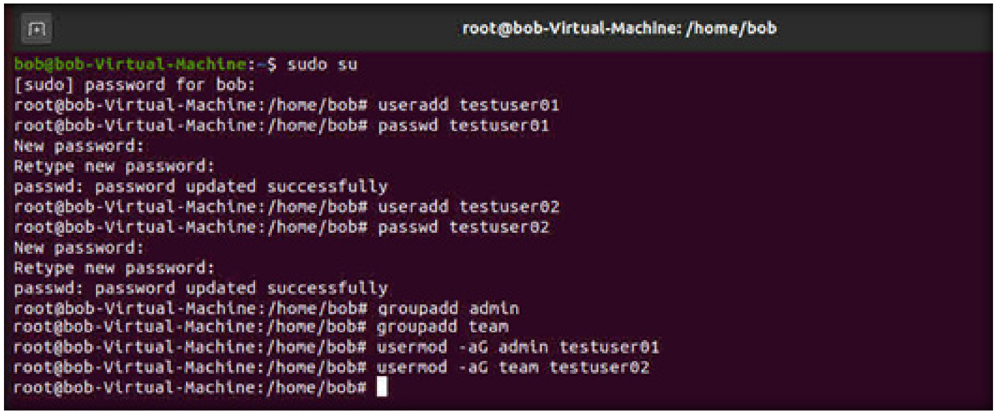


root@bob-Virtual-Machine: /home/bob

```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# groupadd team
root@bob-Virtual-Machine:/home/bob# 
```

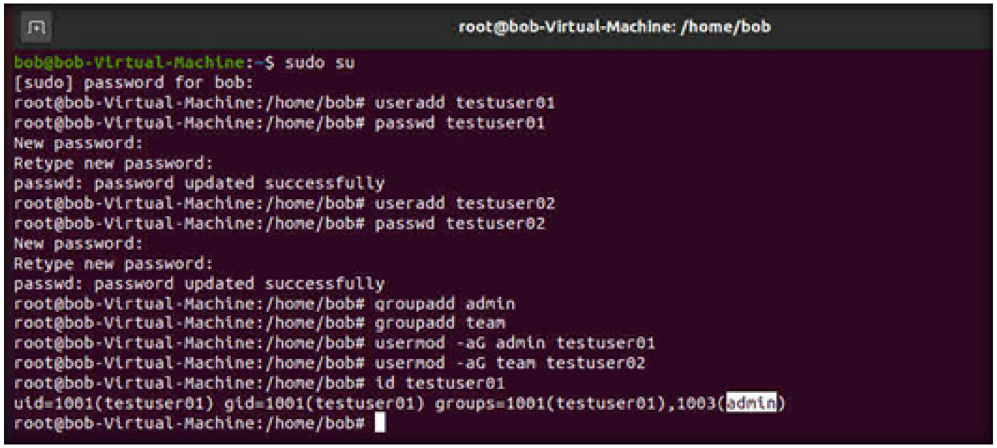
13. In the terminal window, type usermod -aG admin testuser01 and press Enter to add user testuser01 to the admin group.
Note: usermod command is used to modify the user object in order to add a user to the group.

14. Similarly, type usermod -aG team testuser02 and press Enter to add user testuser02 to the team group.



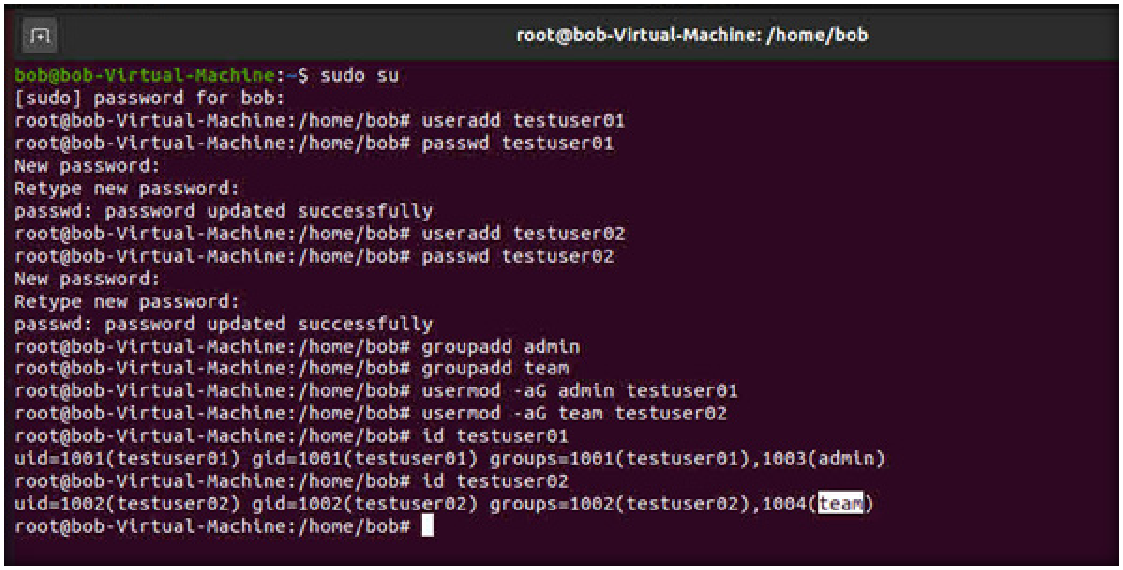
```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# groupadd team
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG team testuser02
root@bob-Virtual-Machine:/home/bob# 
```

15. Type id testuser01 and press Enter to verify that testuser01 has been added to the admin group.



```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# groupadd team
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG team testuser02
root@bob-Virtual-Machine:/home/bob# id testuser01
uid=1001(testuser01) gid=1001(testuser01) groups=1001(testuser01),1003(admin)
root@bob-Virtual-Machine:/home/bob# 
```

16. Similarly, type id testuser02 and press Enter to verify that testuser01 has been added to the team group.



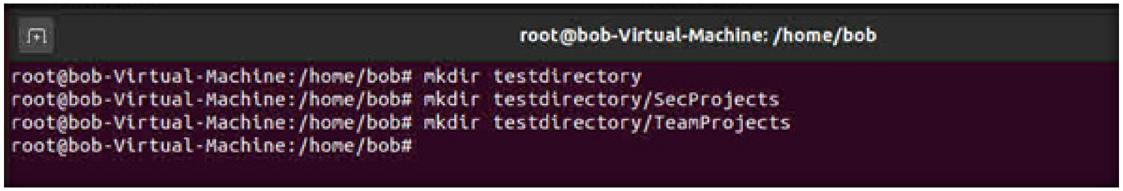
```
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# useradd testuser01
root@bob-Virtual-Machine:/home/bob# passwd testuser01
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# useradd testuser02
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# groupadd team
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG team testuser02
root@bob-Virtual-Machine:/home/bob# id testuser01
uid=1001(testuser01) gid=1001(testuser01) groups=1001(testuser01),1003(admin)
root@bob-Virtual-Machine:/home/bob# id testuser02
uid=1002(testuser02) gid=1002(testuser02) groups=1002(testuser02),1004(team)
root@bob-Virtual-Machine:/home/bob#
```

17. Now, we will create directories and files to demonstrate how the permissions are applied to them.
18. Execute the following commands to create three directories:

mkdir testdirectory

mkdir testdirectory/SecProjects

mkdir testdirectory/TeamProjects

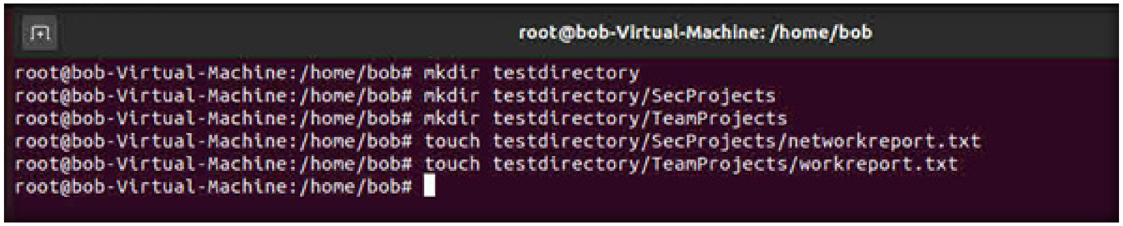


```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob#
```

19. Now, execute the following commands to create two files:

touch testdirectory/SecProjects/networkreport.txt

touch testdirectory/TeamProjects/workreport.txt

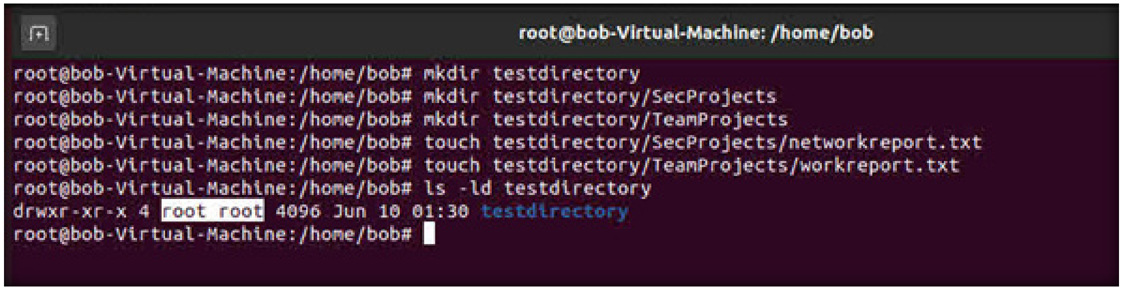


```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# 
```

20. By default, the creator of directories or resources controls the access to them. Therefore, users and groups must be permitted to own the directory content which allows them to configure permissions.

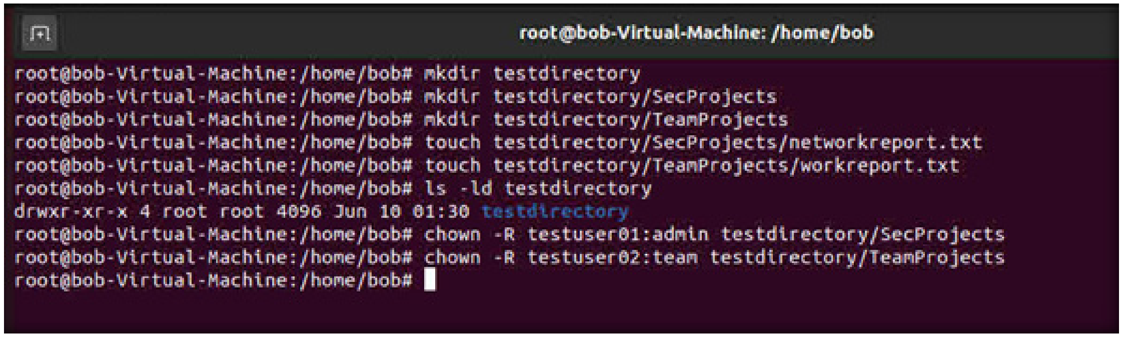
21. In the terminal window, type ls -ld testdirectory and press Enter to display the permissions of the testdirectory directory.

22. Here, root is the owner of the testdirectory, as shown in the screenshot.



```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# 
```

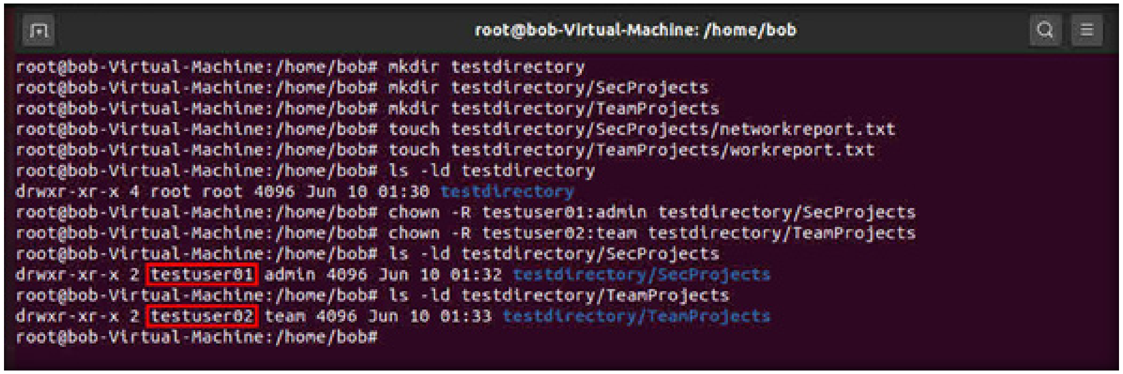
23. Now, we will execute the following commands to change the directory ownership to specific users and groups:
Note: The 'R' parameter allows you to change directory ownership recursively
chown -R testuser01:admin testdirectory/SecProjects
chown -R testuser02:team testdirectory/TeamProjects



```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# 
```

24. Type ls -ld testdirectory/SecProjects and press Enter to display the users and groups associated with testdirectory/SecProjects.

25. Type ls -ld testdirectory/TeamProjects and press Enter to display the users and groups associated with testdirectory/TeamProjects.

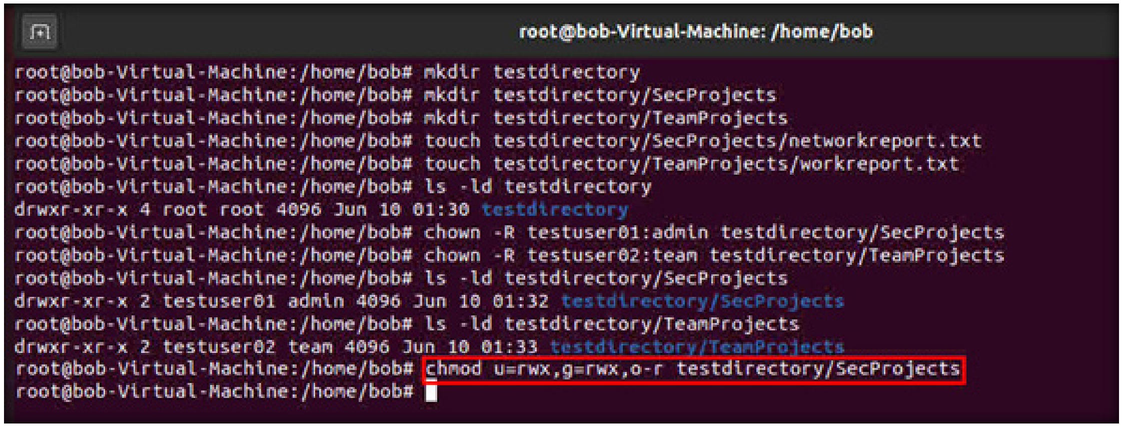


```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/SecProjects
drwxr-xr-x 2 testuser01 admin 4096 Jun 10 01:32 testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/TeamProjects
drwxr-xr-x 2 testuser02 team 4096 Jun 10 01:33 testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob#
```

26. Now, we will configure permissions for the directory owners.

27. In the terminal window, type chmod u=rwx,g=rwx,o-r testdirectory/SecProjects and press Enter to set the following permission for testuser01.

Access Level	Directory	User	Group
rwxrwxo-r	testdirectory/SecProjects	testuser01	admin



```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/SecProjects
drwxr-xr-x 2 testuser01 admin 4096 Jun 10 01:32 testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/TeamProjects
drwxr-xr-x 2 testuser02 team 4096 Jun 10 01:33 testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o-r testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# 
```

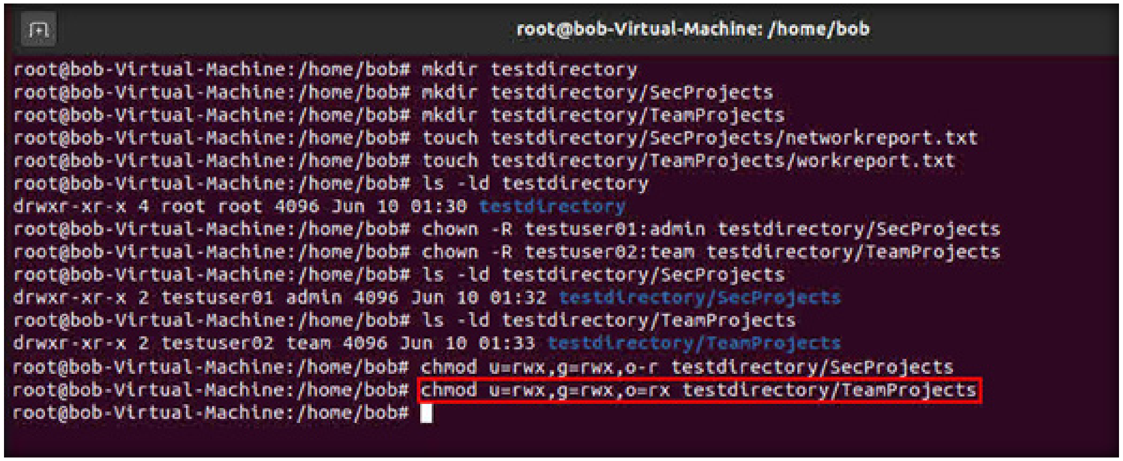
Note: Access Level Parameters: r: read a file or lit the content of a directory, w: write to a file or directory, x: execute a file or recurse a directory tree.

Note: Reference Parameters: u: user (file owner), g: group (members of the file's group), o: others (users who are neither the file's owner nor members of the file's group).

Note: Here, rwx: read, write and execute permissions are given to u(user) and g(group), o-r: read permission has been removed for o (others).

28. In the terminal window, type chmod u=rwx,g=rwx,o=rx testdirectory/TeamProjects and press Enter to set the following permission for user testuser02.

Access Level	Directory	User	Group
rwxrwxrx	testdirectory/TeamProjects	testuser02	team

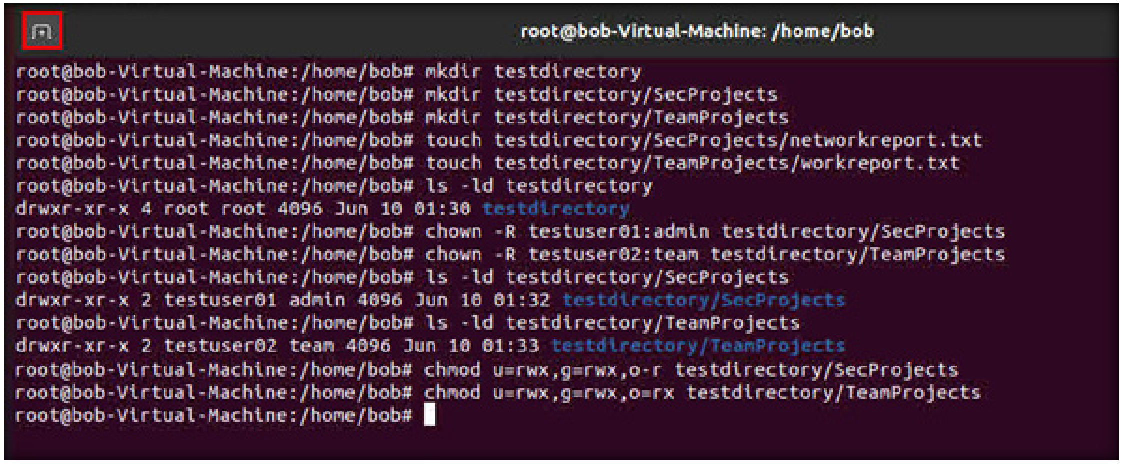


```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/SecProjects
drwxr-xr-x 2 testuser01 admin 4096 Jun 10 01:32 testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/TeamProjects
drwxr-xr-x 2 testuser02 team 4096 Jun 10 01:33 testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o-r testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o=rx testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# 
```

Note: Here, rwx: read, write and execute permissions are given to u(user) and g(group), rx: Read and execute permissions are given to o(others).

29. Thus, we have created the user accounts along with the specified resource access policies, we will test them.

30. Click on the Add icon (+) present on top-left corner of the Terminal window to open another terminal.

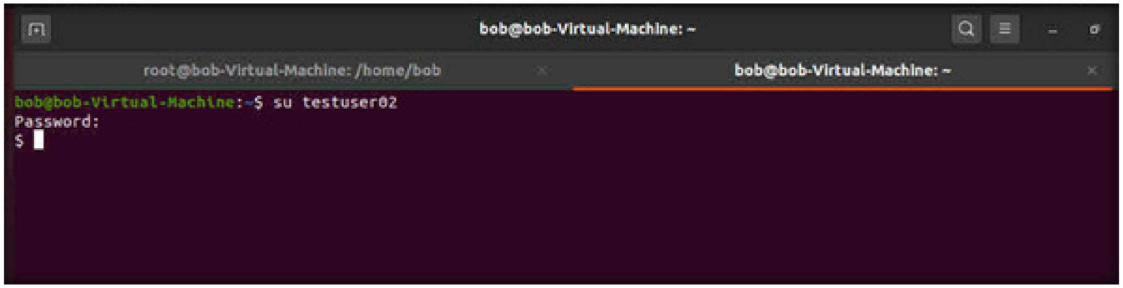


```
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# mkdir testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# touch testdirectory/SecProjects/networkreport.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.txt
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory
drwxr-xr-x 4 root root 4096 Jun 10 01:30 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/SecProjects
drwxr-xr-x 2 testuser01 admin 4096 Jun 10 01:32 testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/TeamProjects
drwxr-xr-x 2 testuser02 team 4096 Jun 10 01:33 testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o-r testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o=rx testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# 
```

31. A new Terminal window appears, in another tab.

32. In this new Terminal window, type su testuser02 and press Enter.
Note: su stands for substitute user, it is used to execute commands with the privileges of another user account.

33. A Password field appears, type test@123 and press Enter.
Note: The password types by you will not be visible.


bob@bob-Virtual-Machine: ~
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine: ~

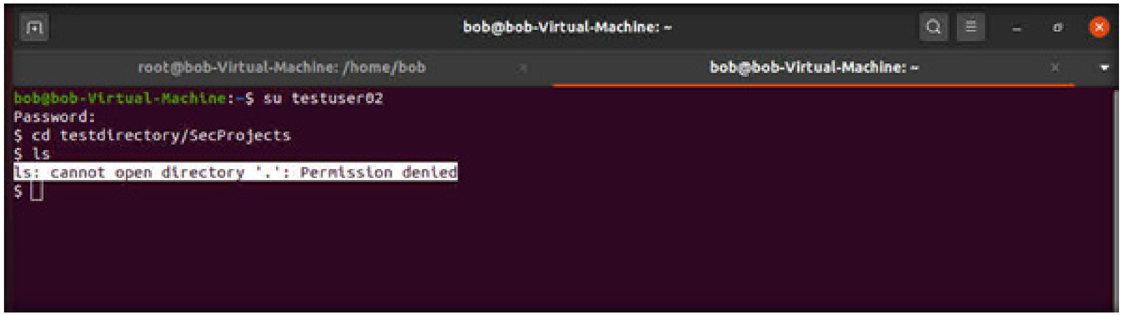
```
bob@bob-Virtual-Machine:~$ su testuser02
Password:
$ 
```

EXERCISE 2: MANAGE ACCESS CONTROLS IN LINUX MACHINE

34. In the terminal, type cd testdirectory/SecProjects and press Enter, to navigate to the SecProjects directory having with only Admin privileges.

35. Type ls and press Enter to list the files present in the directory.

36. According to the permissions specified in step#26, it can be observed that testuser02 does not have access to the directory content of testuser01. The testeruser02 is a normal user with limited access whereas testuser01 has admin level privileges.



bob@bob-Virtual-Machine: ~
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine: ~

```
bob@bob-Virtual-Machine:~$ su testuser02
Password:
$ cd testdirectory/SecProjects
$ ls
ls: cannot open directory '.': Permission denied
$ 
```

37. As described above, the root user can create multiple user accounts on the same machine with different level of access permissions, thereby, preventing the system and resources from unauthorized access.

38. This concludes the demonstration of implementing access control policies in Linux machine.

39. Close all open windows.

40. Turn off the Attacker Machine-1 virtual machine.

EXERCISE 2:
MANAGE ACCESS
CONTROLS IN
LINUX MACHINE

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)

Windows Admin Center (WAC) provides a web console to perform administrative tasks and manage different machines within a network.

LAB SCENARIO

A security professional should be aware of the various tools and tricks available to manage servers and clients. WAC enables you to perform administrative tasks on any client device (except mobile devices). It uses role-based access control (RBAC) to control the activity of users connected to the server. WAC allows the management of system activity such as starting various services, adding and removing resources, and controlling applications.

OBJECTIVE

This lab demonstrates how to install WAC and configure RBAC in WAC to restrict user activities.

OVERVIEW OF WAC

In WAC, RBAC provides limited access to users on the target computers. RBAC in WAC works by configuring every managed server with a PowerShell Just-Enough Administration endpoint. The roles are defined by the endpoint. After connecting a restricted endpoint, a temporary local administrator account is created for managing the machine. If the user is not managing the machine utilizing WAC, the temporary account is automatically deleted.

WAC supports the following built-in roles.

Administrators: They allow users to use most WAC features without granting them access to Remote Desktop or PowerShell.

Readers: They allow users to view information and settings on the server, but not make changes.

Hyper-V Administrators: They allow users to make changes to the Hyper-V VMs and switches but limits other features to read-only access.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)

Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the Admin Machine-1 virtual machine.

2. Log in with the credentials Admin and admin@123.
Note: If the network screen appears, click Yes.

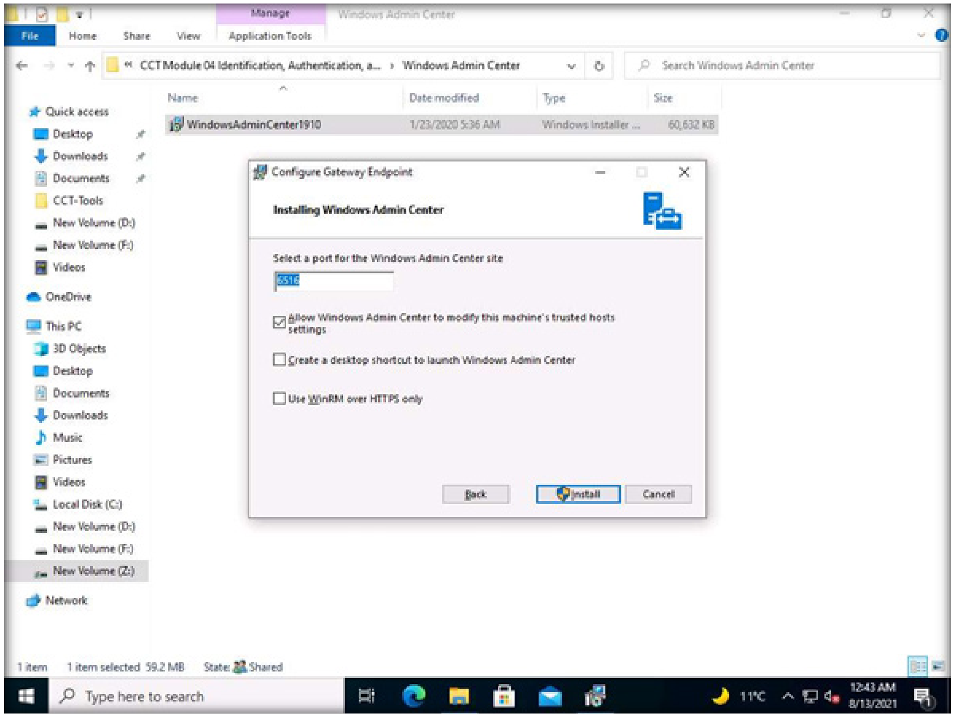
3. To install WAC, navigate to Z:\CCT-Tools\CCT Module 04 Identification, Authentication and Authorization\Windows Admin Center and double-click WindowsAdminCenter1910.msi.

4. The installation starts. Check I accept these terms. Click Next to continue.

5. The default option pertains to Microsoft updates. Click Next.

6. The Configure Gateway Endpoint window appears. Click Next to continue.

7. Leave the default settings for port and other options unchanged on the window. Click Install.



Configure Gateway Endpoint

Installing Windows Admin Center

Select a port for the Windows Admin Center site

6516

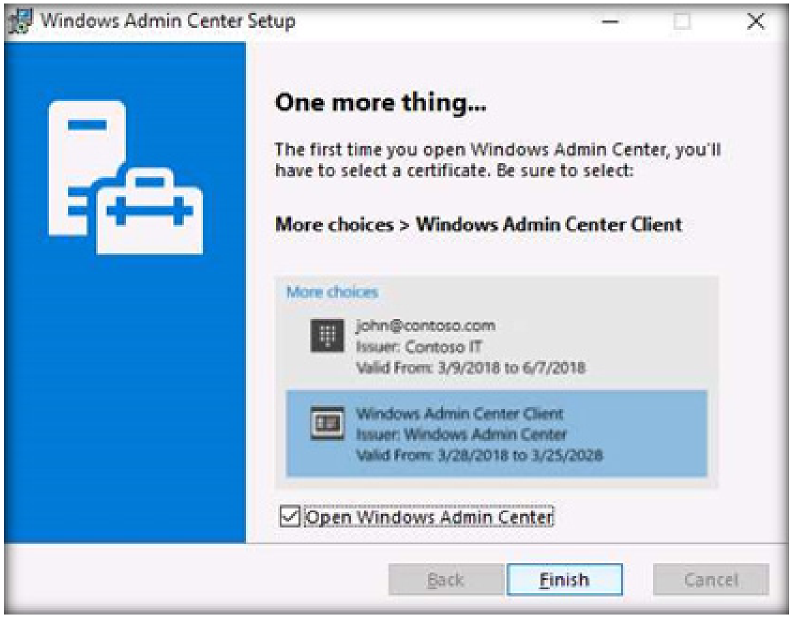
☑ Allow Windows Admin Center to modify this machine's trusted hosts settings

□ Create a desktop shortcut to launch Windows Admin Center

□ Use WinRM over HTTPS only

8. WAC installation starts. If the User Account Control window appears, click yes.

9. Installation continues. Check Open Windows Admin Center. Click Finish to complete the installation.



Windows Admin Center Setup

One more thing...

The first time you open Windows Admin Center, you'll have to select a certificate. Be sure to select:

More choices > Windows Admin Center Client

More choices

john@contoso.com
Issuer: Contoso IT
Valid From: 3/9/2018 to 6/7/2018

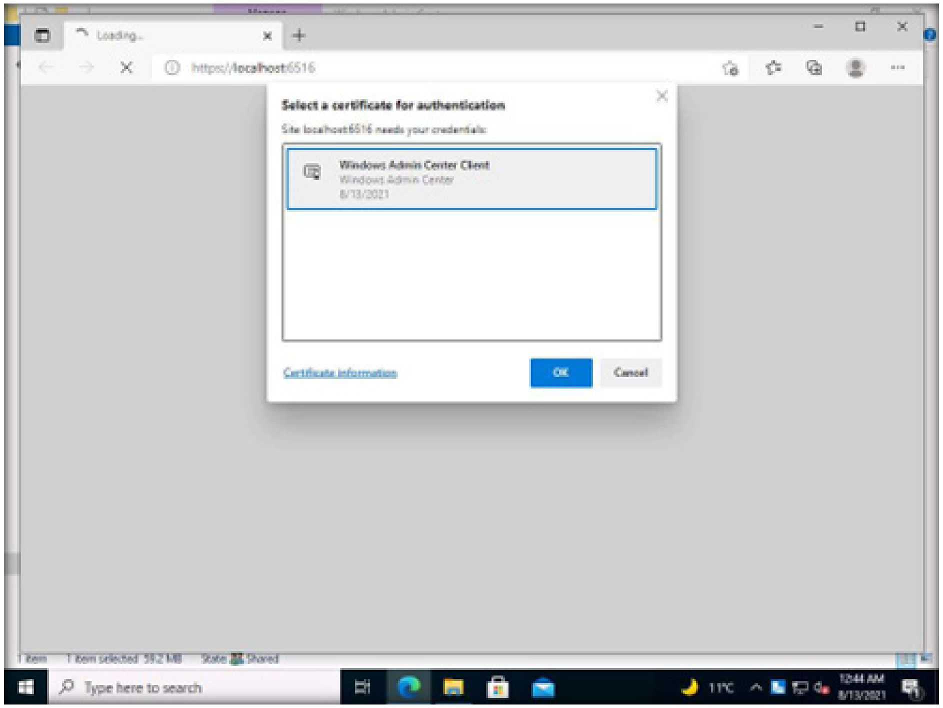
Windows Admin Center Client
Issuer: Windows Admin Center
Valid From: 3/28/2018 to 3/25/2028

☑ Open Windows Admin Center

10. If a list of browser applications pops-up, select Microsoft Edge and click OK.

11. Wait for a few seconds. The Edge browser loads Windows Admin Center.

12. If a Select a certificate for authentication pop-up appears, select the certificate and click OK.

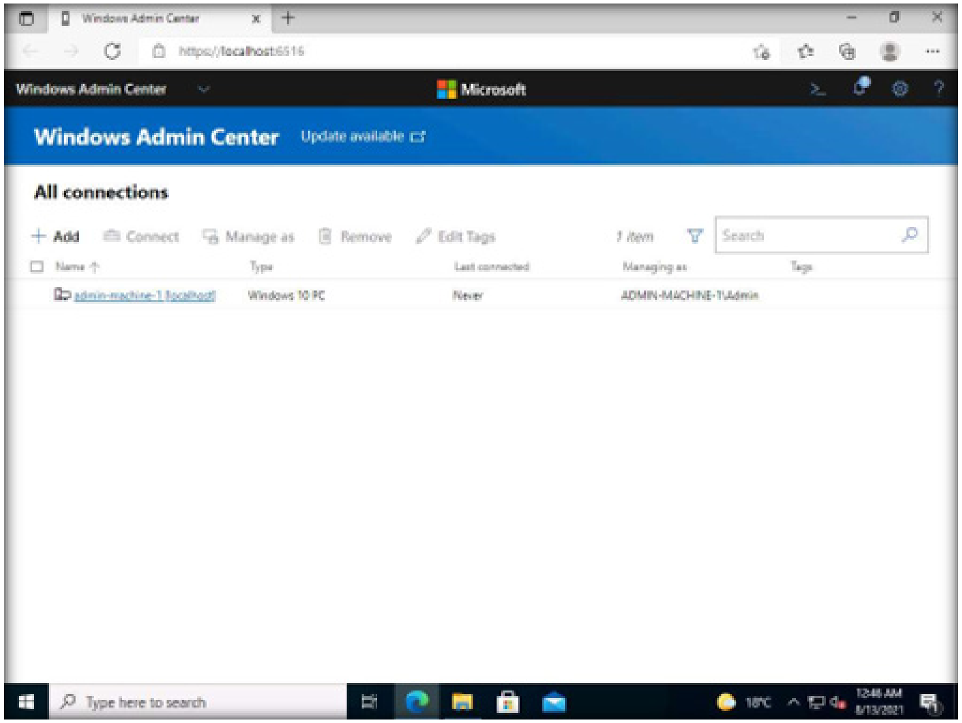


Select a certificate for authentication

Site localhost:6516 needs your credentials:

Windows Admin Center Client
Windows Admin Center
8/13/2021

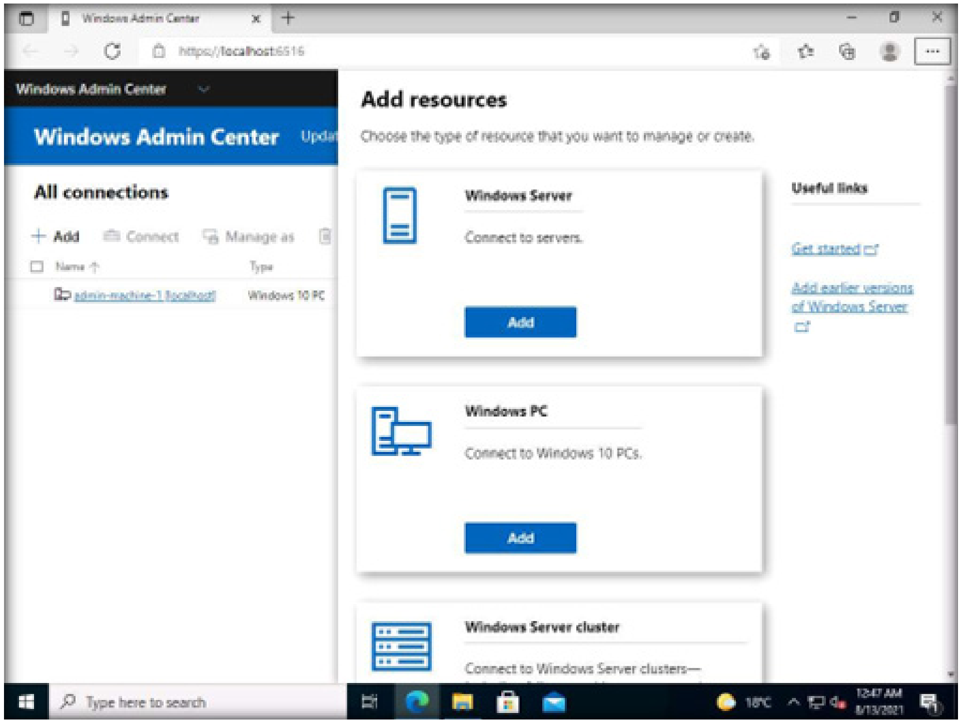
13. The Windows Admin Center appears. By default, you can see that Admin Machine-1 is connected and listed under All Connections.



All connections

Name ↑	Type	Last connected	Managing as	Tags
admin-machine-1 [localhost]	Windows 10 PC	Never	ADMIN-MACHINE-1\Admin	

14. Click on the +Add button to add the Webserver.



Add resources

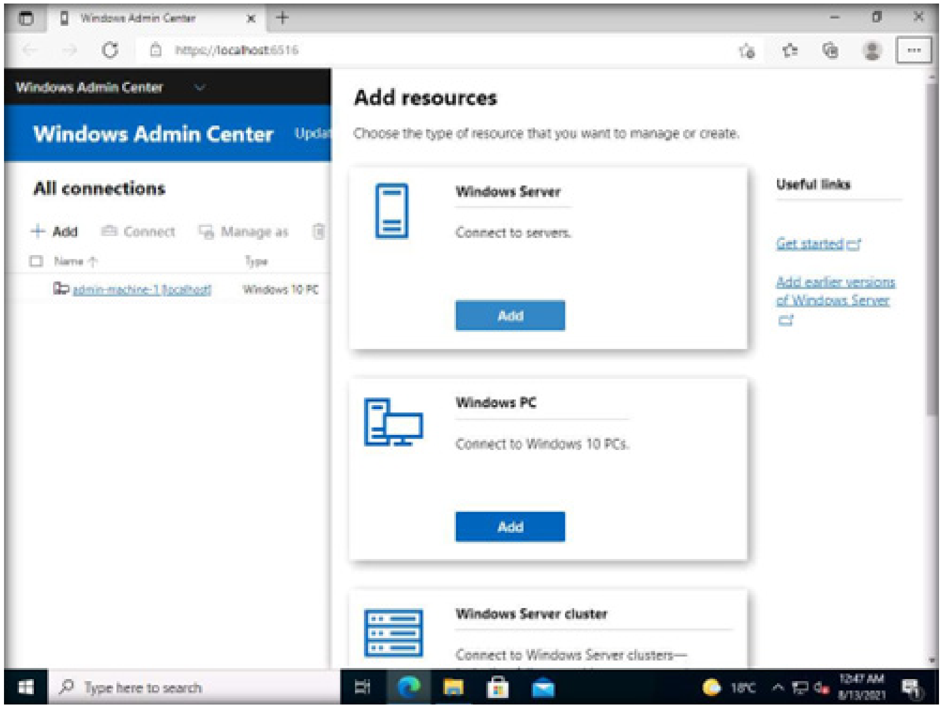
Choose the type of resource that you want to manage or create.

Windows Server — Connect to servers.

Windows PC — Connect to Windows 10 PCs.

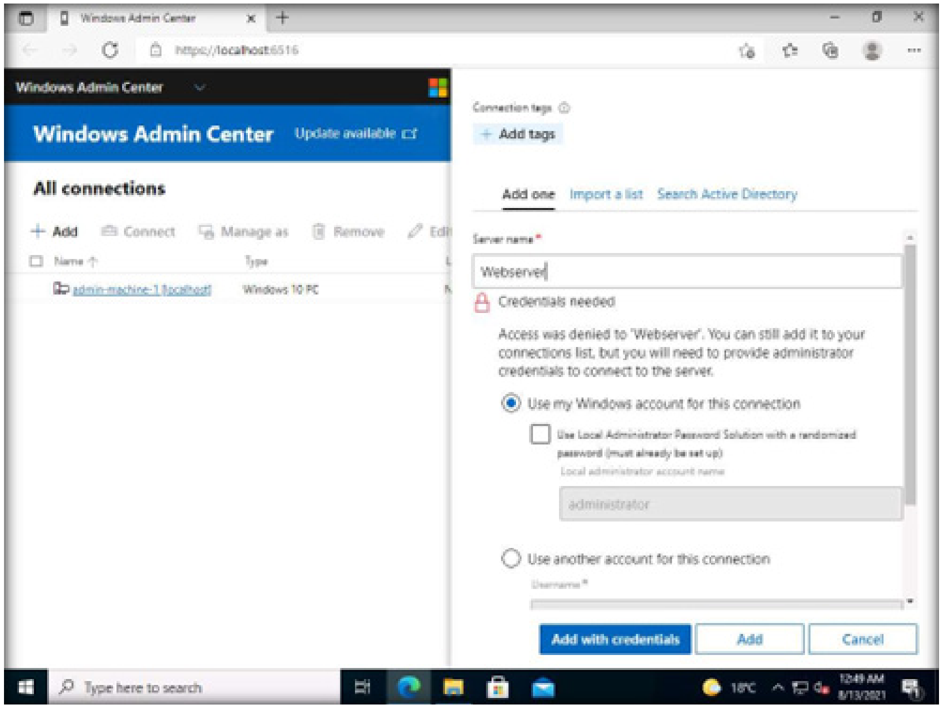
Windows Server cluster — Connect to Windows Server clusters—

15. The Add resources pane opens. Click Add under Windows Server.



16. The Connection tags pane appears. Type Webserver in the Server name field. Wait for few seconds.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



Server name *

Webserver

Credentials needed

Access was denied to 'Webserver'. You can still add it to your connections list, but you will need to provide administrator credentials to connect to the server.

● Use my Windows account for this connection

□ Use Local Administrator Password Solution with a randomized password (must already be set up)

Local administrator account name

administrator

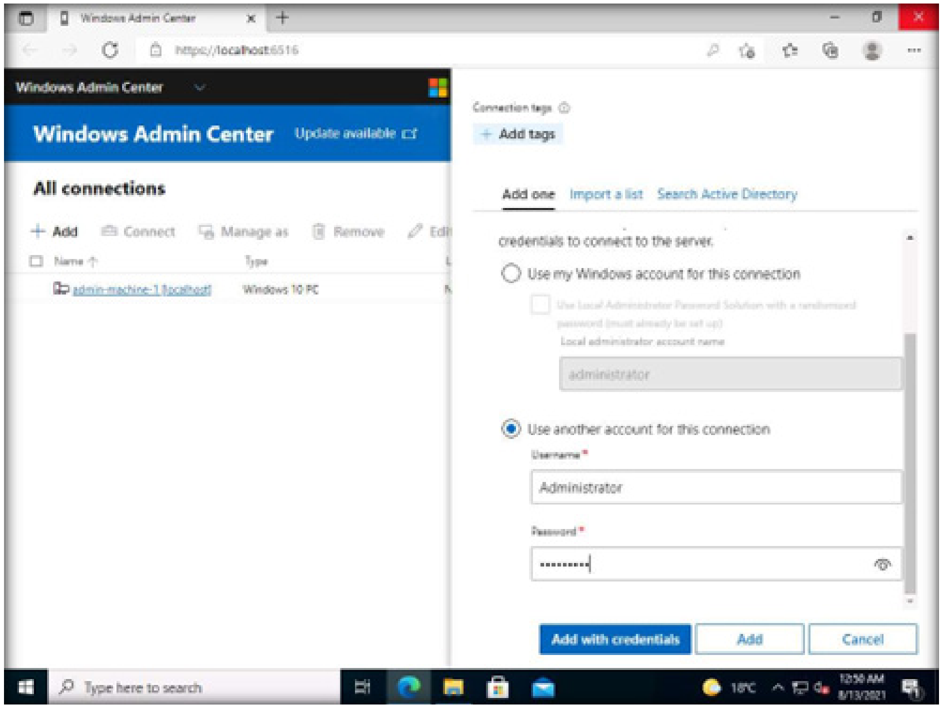
○ Use another account for this connection

Username *

Add with credentials | Add | Cancel

17. Select the Use another account for this connection radio button and type the username Administrator and password admin@123. Click Add with credentials.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



credentials to connect to the server.

○ Use my Windows account for this connection

□ Use Local Administrator Password Solution with a randomized password (must already be set up)

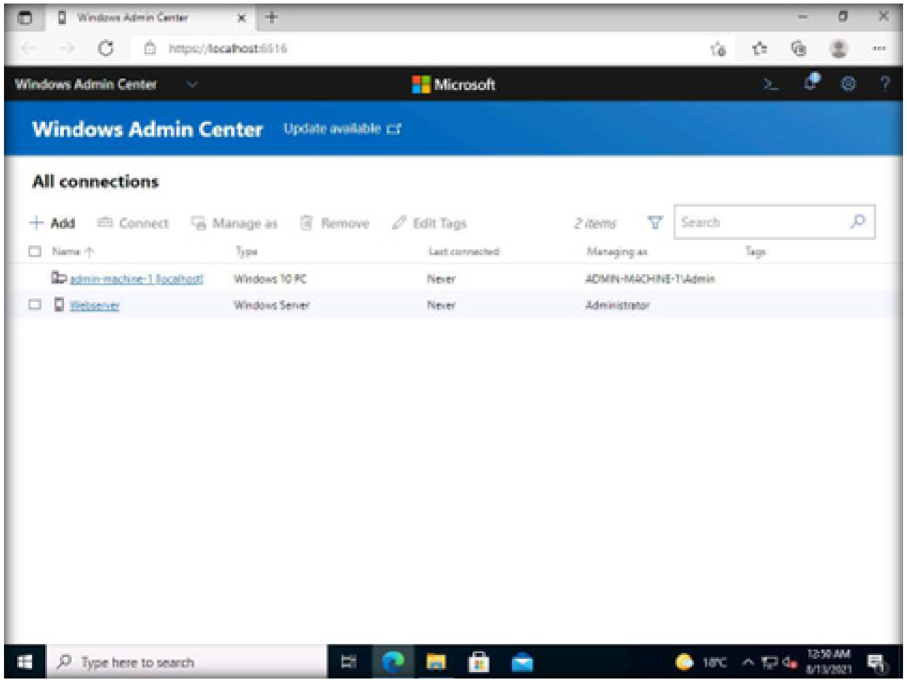
Local administrator account name: administrator

● Use another account for this connection

Username *: Administrator

Password *: •••••••••

18. The Webserver is added to the Windows Admin Center.
Note: if a Save password pop-up appears, click Never.

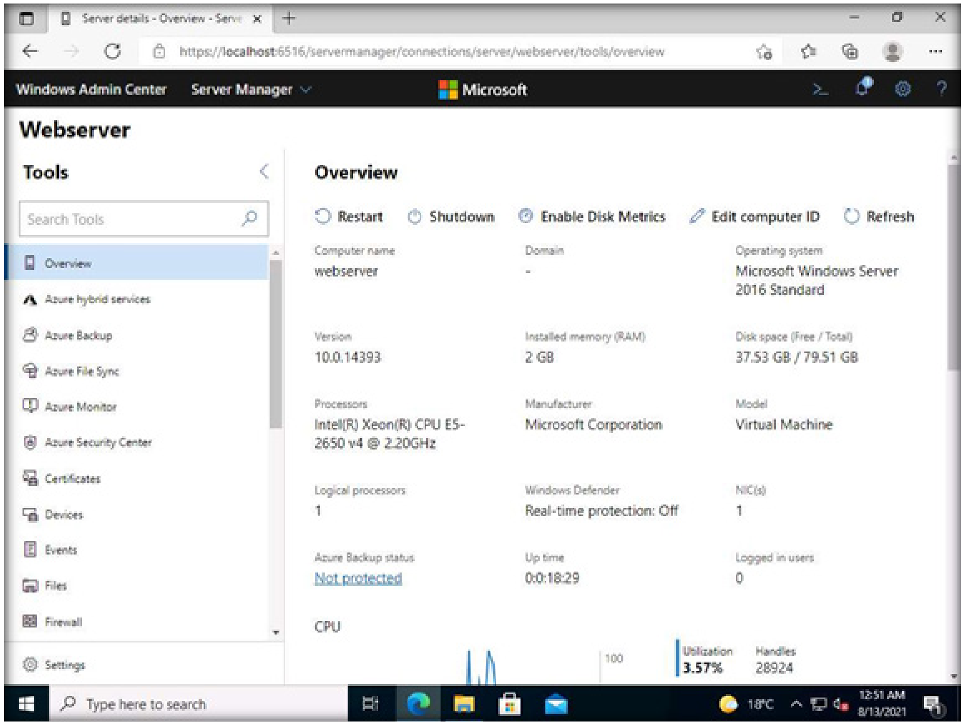


Name ↑	Type	Last connected	Managing as	Tags
admin-machine-1 [localhost]	Windows 10 PC	Never	ADMIN-MACHINE-1\Admin	
Webserver	Windows Server	Never	Administrator	

19. Click Webserver to connect the server.

20. The Windows Admin Center connects to Webserver and displays all tools under Server Manager.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



Computer name webserver	Domain -	Operating system Microsoft Windows Server 2016 Standard
Version 10.0.14393	Installed memory (RAM) 2 GB	Disk space (Free / Total) 37.53 GB / 79.51 GB
Processors Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz	Manufacturer Microsoft Corporation	Model Virtual Machine
Logical processors 1	Windows Defender Real-time protection: Off	NIC(s) 1
Azure Backup status Not protected	Up time 0:0:18:29	Logged in users 0

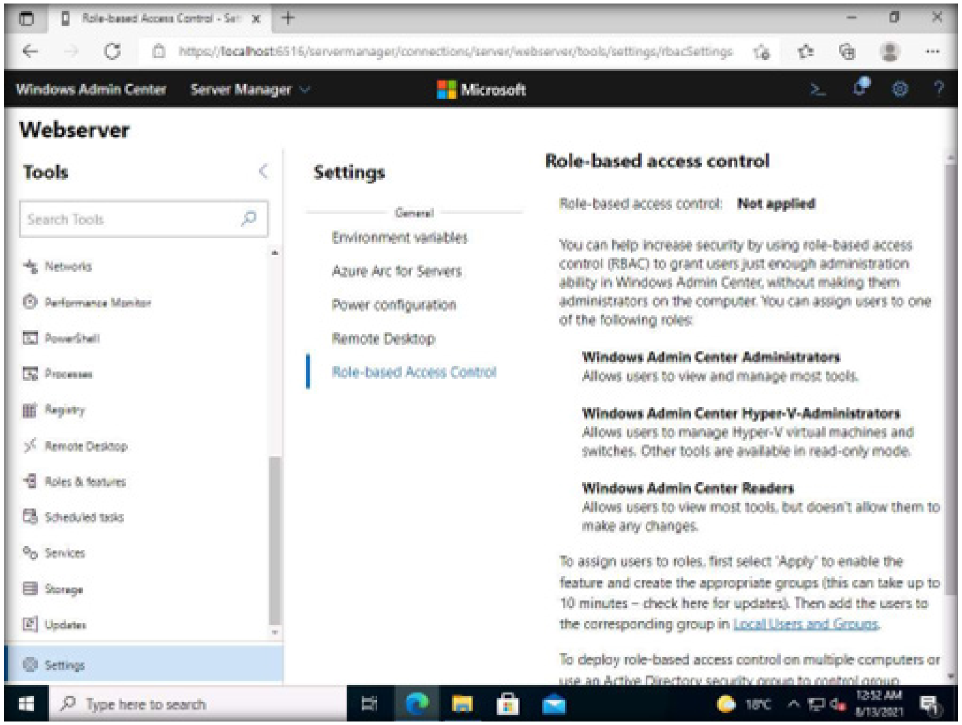
Utilization 3.57% Handles 28924

21. We have added Webserver to the Windows Admin Center. A security professional can now manage the Webserver through WAC.

22. Using RBAC option in WAC, a security professional can provide only limited access to a user of Web server machine. Here, we will assign limited access to the already created user (john) in Web Server machine. To configure RBAC for user john, click Settings at the bottom of the Tools pane on the left.

23. The Settings pane appears. Click Role-based Access Control.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



Role-based access control

Role-based access control: **Not applied**

You can help increase security by using role-based access control (RBAC) to grant users just enough administration ability in Windows Admin Center, without making them administrators on the computer. You can assign users to one of the following roles:

Windows Admin Center Administrators
Allows users to view and manage most tools.

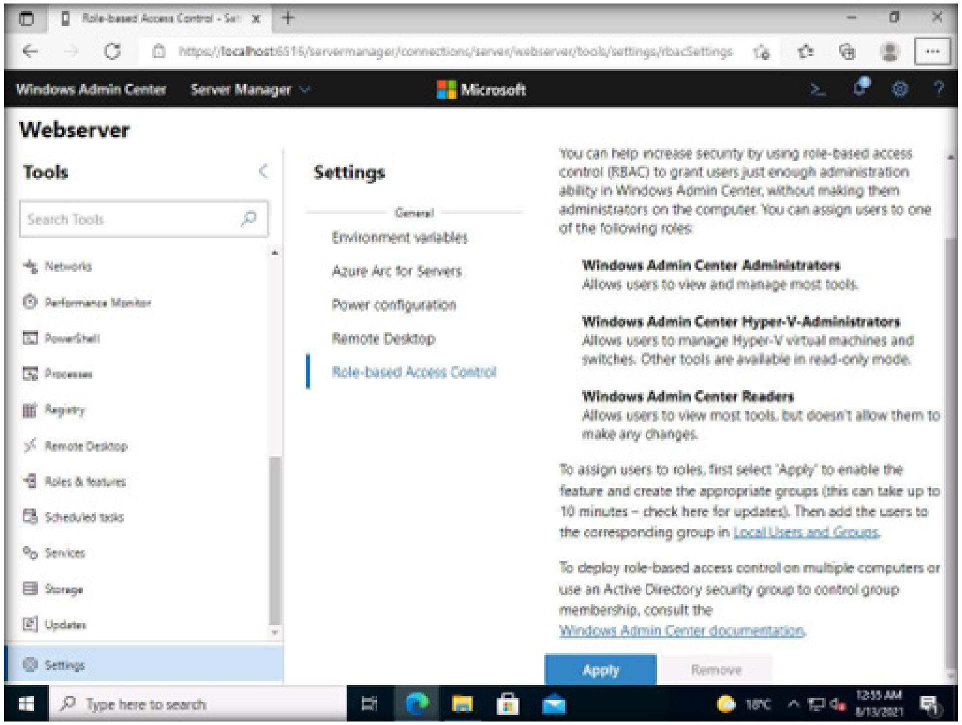
Windows Admin Center Hyper-V-Administrators
Allows users to manage Hyper-V virtual machines and switches. Other tools are available in read-only mode.

Windows Admin Center Readers
Allows users to view most tools, but doesn't allow them to make any changes.

To assign users to roles, first select 'Apply' to enable the feature and create the appropriate groups (this can take up to 10 minutes – check here for updates). Then add the users to the corresponding group in Local Users and Groups.

To deploy role-based access control on multiple computers or use an Active Directory security group to control group

24. The Role-based access control page appears. Click the Apply button at the bottom of the page.



You can help increase security by using role-based access control (RBAC) to grant users just enough administration ability in Windows Admin Center, without making them administrators on the computer. You can assign users to one of the following roles:

Windows Admin Center Administrators
Allows users to view and manage most tools.

Windows Admin Center Hyper-V-Administrators
Allows users to manage Hyper-V virtual machines and switches. Other tools are available in read-only mode.

Windows Admin Center Readers
Allows users to view most tools, but doesn't allow them to make any changes.

To assign users to roles, first select 'Apply' to enable the feature and create the appropriate groups (this can take up to 10 minutes – check here for updates). Then add the users to the corresponding group in Local Users and Groups.

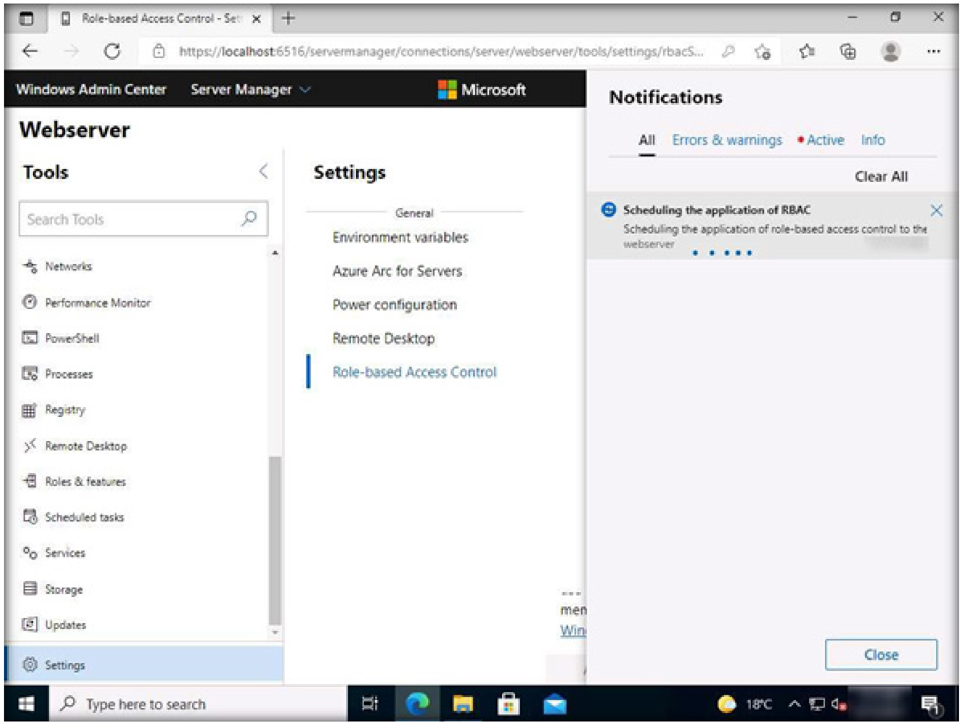
To deploy role-based access control on multiple computers or use an Active Directory security group to control group membership, consult the Windows Admin Center documentation.

25. The Restart the WinRM service? dialog appears. Click Yes to continue.

26. A notification (see the Notifications icon at the upper right corner) about scheduling the application of RBAC appears. It takes a maximum of 10 minutes to start the RBAC service. Wait for 10 minutes, refresh the Webserver connection.

Note: If logged out, log in with the credentials for Webserver as given in Step#17.

Thus, we reconnected to the Webserver. Navigate to Tools → Settings. Click the Role-based Access Control option. You can see that the Role-based access control status is Applied. Tonya-this



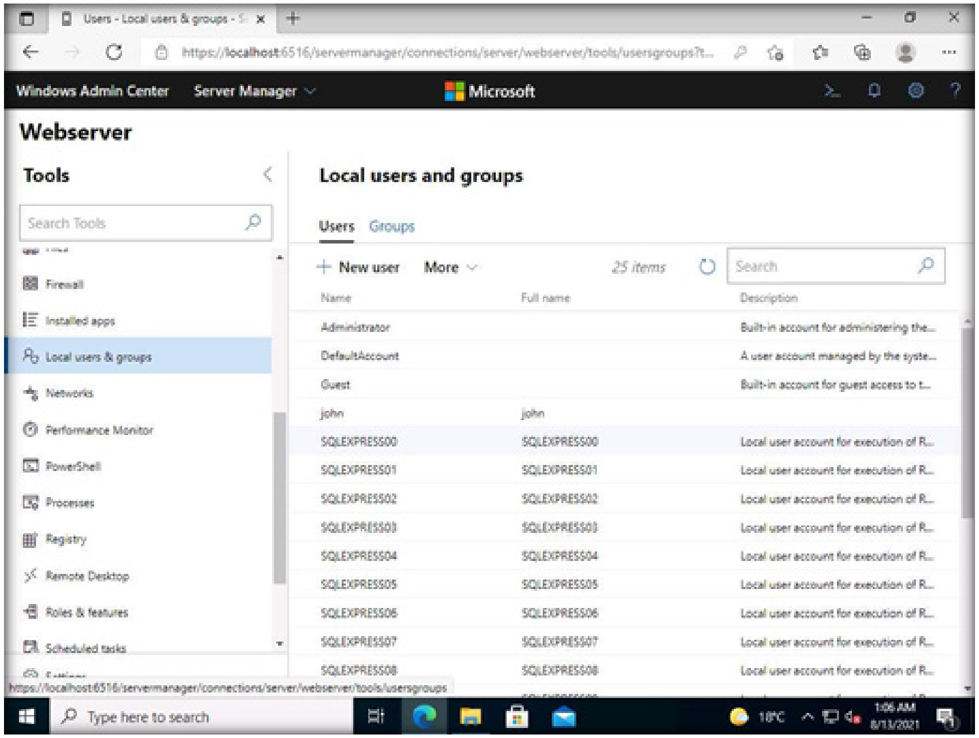
https://localhost:6516/servermanager/connections/server/webserver/tools/settings/rbacS...

Scheduling the application of RBAC

Scheduling the application of role-based access control to the webserver

27. RBAC is now added to Webserver.

28. Next, assign a user to the role. Click Local users & groups in the Tools pane on the left.

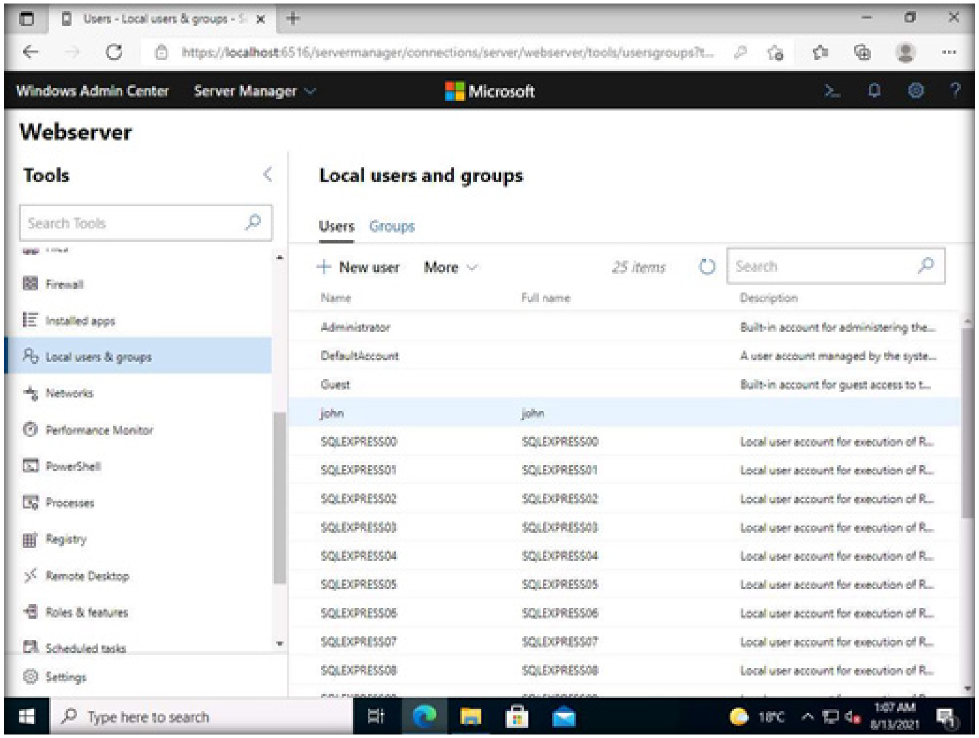


Name	Full name	Description
Administrator		Built-in account for administering the...
DefaultAccount		A user account managed by the syste...
Guest		Built-in account for guest access to t...
john	john	
SQLEXPRESS00	SQLEXPRESS00	Local user account for execution of R...
SQLEXPRESS01	SQLEXPRESS01	Local user account for execution of R...
SQLEXPRESS02	SQLEXPRESS02	Local user account for execution of R...
SQLEXPRESS03	SQLEXPRESS03	Local user account for execution of R...
SQLEXPRESS04	SQLEXPRESS04	Local user account for execution of R...
SQLEXPRESS05	SQLEXPRESS05	Local user account for execution of R...
SQLEXPRESS06	SQLEXPRESS06	Local user account for execution of R...
SQLEXPRESS07	SQLEXPRESS07	Local user account for execution of R...
SQLEXPRESS08	SQLEXPRESS08	Local user account for execution of R...

https://localhost:6516/servermanager/connections/server/webserver/tools/usersgroups

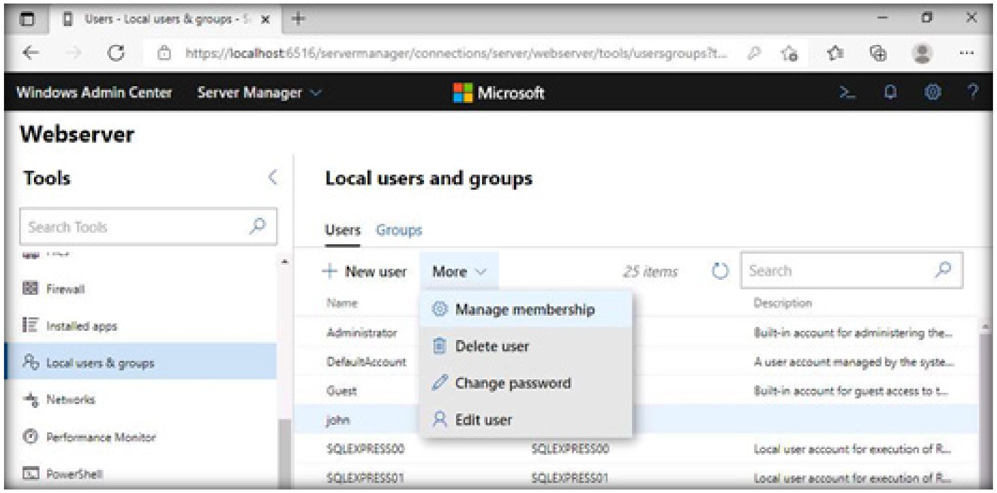
29. The Local users & groups pane appears. Select the user john under the Users tab.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



Name	Full name	Description
Administrator		Built-in account for administering the...
DefaultAccount		A user account managed by the syste...
Guest		Built-in account for guest access to t...
john	john	
SQLEXPRESS00	SQLEXPRESS00	Local user account for execution of R...
SQLEXPRESS01	SQLEXPRESS01	Local user account for execution of R...
SQLEXPRESS02	SQLEXPRESS02	Local user account for execution of R...
SQLEXPRESS03	SQLEXPRESS03	Local user account for execution of R...
SQLEXPRESS04	SQLEXPRESS04	Local user account for execution of R...
SQLEXPRESS05	SQLEXPRESS05	Local user account for execution of R...
SQLEXPRESS06	SQLEXPRESS06	Local user account for execution of R...
SQLEXPRESS07	SQLEXPRESS07	Local user account for execution of R...
SQLEXPRESS08	SQLEXPRESS08	Local user account for execution of R...

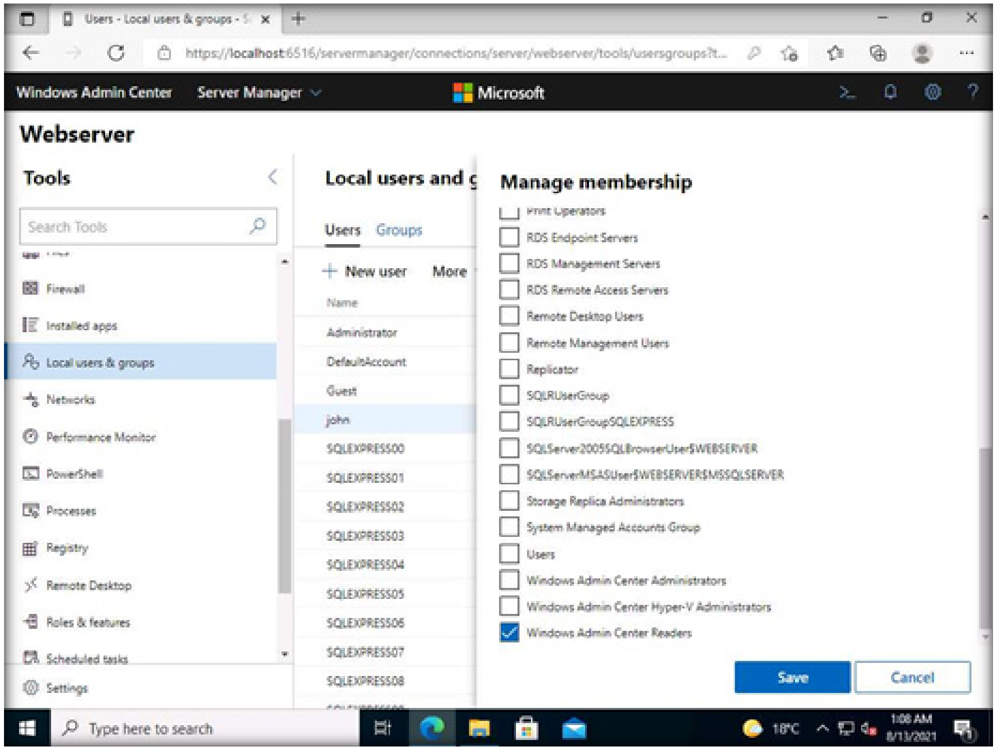
30. The Manage membership option is now visible. If it is not visible, click on More and select the Manage membership option.



Name		Description
Administrator		Built-in account for administering the...
DefaultAccount		A user account managed by the syste...
Guest		Built-in account for guest access to t...
john		
SQLEXPRESS00	SQLEXPRESS00	Local user account for execution of R...
SQLEXPRESS01	SQLEXPRESS01	Local user account for execution of R...

31. Click Manage membership to add membership for the user. The Manage membership pane now opens.

32. Scroll down the list that appears in the Manage Membership pane. In the list, uncheck Users, and check Windows Admin Center Readers. These changes will allow John to view information and settings on the server, but not make changes by assigning the windows admin center readers role. Click Save.



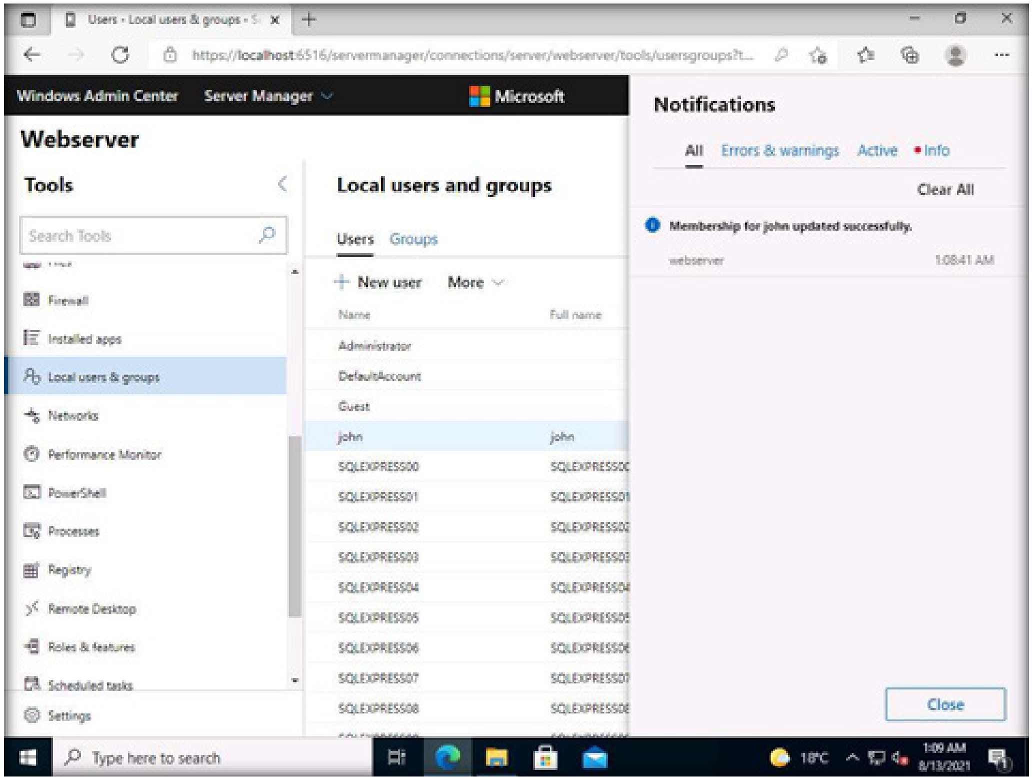
Manage membership

- □ Print Operators
- □ RDS Endpoint Servers
- □ RDS Management Servers
- □ RDS Remote Access Servers
- □ Remote Desktop Users
- □ Remote Management Users
- □ Replicator
- □ SQLRUserGroup
- □ SQLRUserGroupSQLEXPRESS
- □ SQLServer2005SQLBrowserUser$WEBSERVER
- □ SQLServerMSASUser$WEBSERVER$MSSQLSERVER
- □ Storage Replica Administrators
- □ System Managed Accounts Group
- □ Users
- □ Windows Admin Center Administrators
- □ Windows Admin Center Hyper-V Administrators
- ☑ Windows Admin Center Readers

Save Cancel

33. A notification (see the Notifications icon) appears indicating that the membership for the user john has been updated successfully.

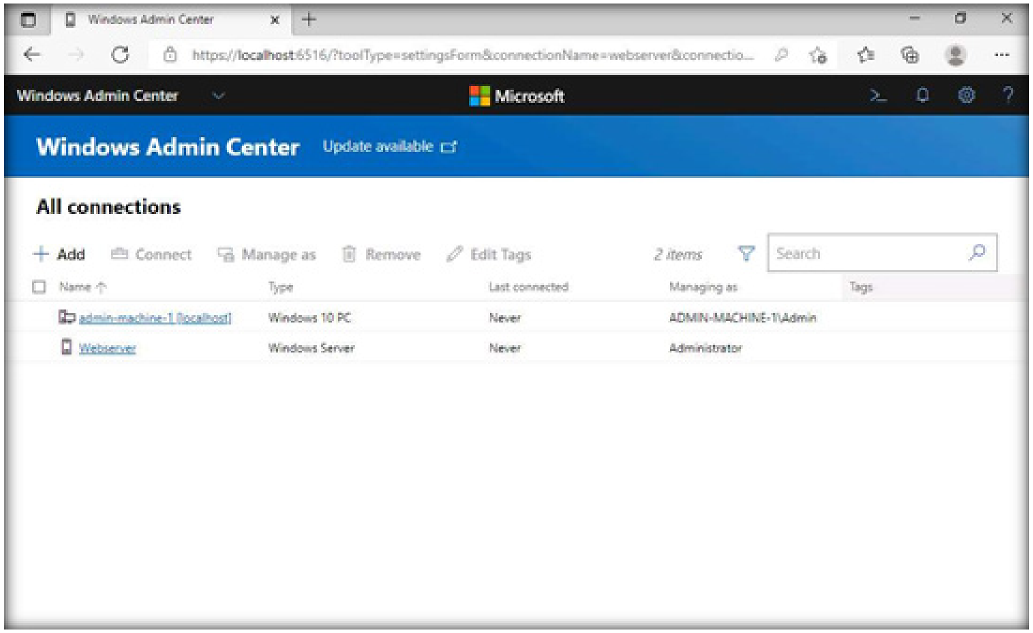
EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)



Name	Full name
Administrator	
DefaultAccount	
Guest	
john	john
SQLEXPRESS00	SQLEXPRESS0
SQLEXPRESS01	SQLEXPRESS01
SQLEXPRESS02	SQLEXPRESS02
SQLEXPRESS03	SQLEXPRESS03
SQLEXPRESS04	SQLEXPRESS04
SQLEXPRESS05	SQLEXPRESS05
SQLEXPRESS06	SQLEXPRESS06
SQLEXPRESS07	SQLEXPRESS07
SQLEXPRESS08	SQLEXPRESS08

Membership for john updated successfully.
webserver 1:08:41 AM

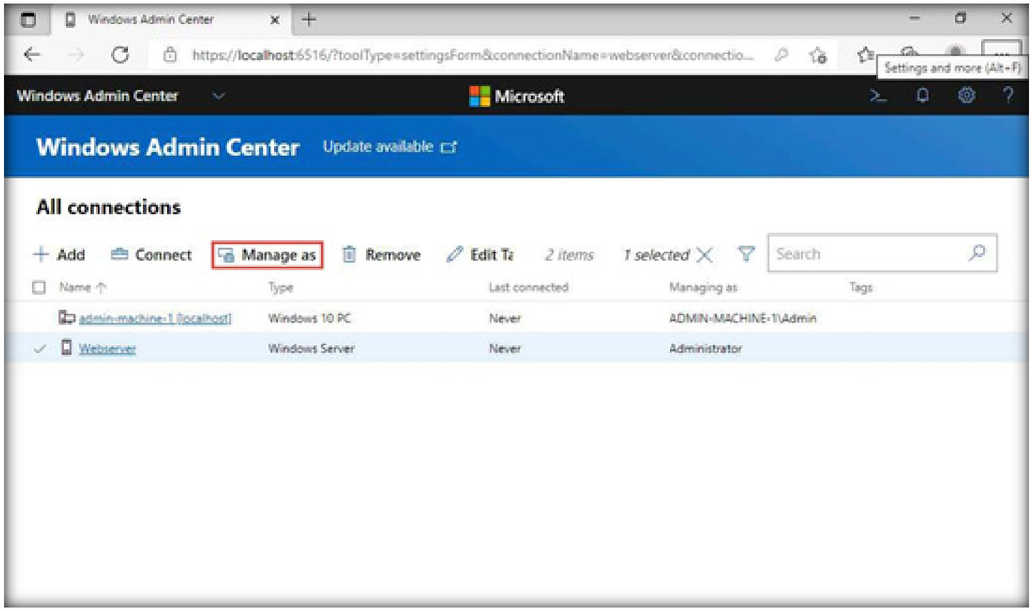
34. Click Windows Admin Center from the top-left corner of the dashboard, to navigate to the Home page.



Name ↑	Type	Last connected	Managing as	Tags
admin-machine-1 [localhost]	Windows 10 PC	Never	ADMIN-MACHINE-1\Admin	
Webserver	Windows Server	Never	Administrator	

35. Select Webserver and click the Manage as tab. If Manage as tab is not visible, click on More tab and select Manage as option.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)

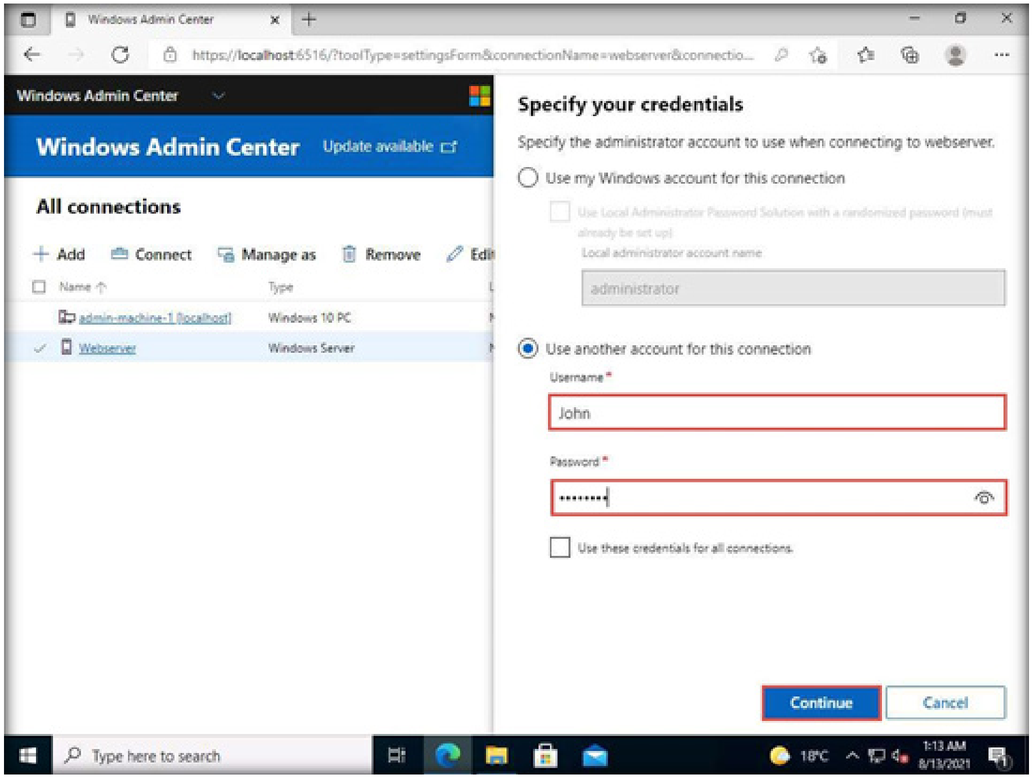


https://localhost:6516/?toolType=settingsForm&connectionName=webserver&connectio...

All connections

Name ↑	Type	Last connected	Managing as	Tags
admin-machine-1 [localhost]	Windows 10 PC	Never	ADMIN-MACHINE-1\Admin	
✓ Webserver	Windows Server	Never	Administrator	

36. Specify your credentials once the pane opens. Change username to John and password to user@123. We will now log in as a user to Webserver. In Windows Admin Center, click Continue.



Specify your credentials

Specify the administrator account to use when connecting to webserver.

○ Use my Windows account for this connection

□ Use Local Administrator Password Solution with a randomized password (must already be set up)

Local administrator account name: administrator

● Use another account for this connection

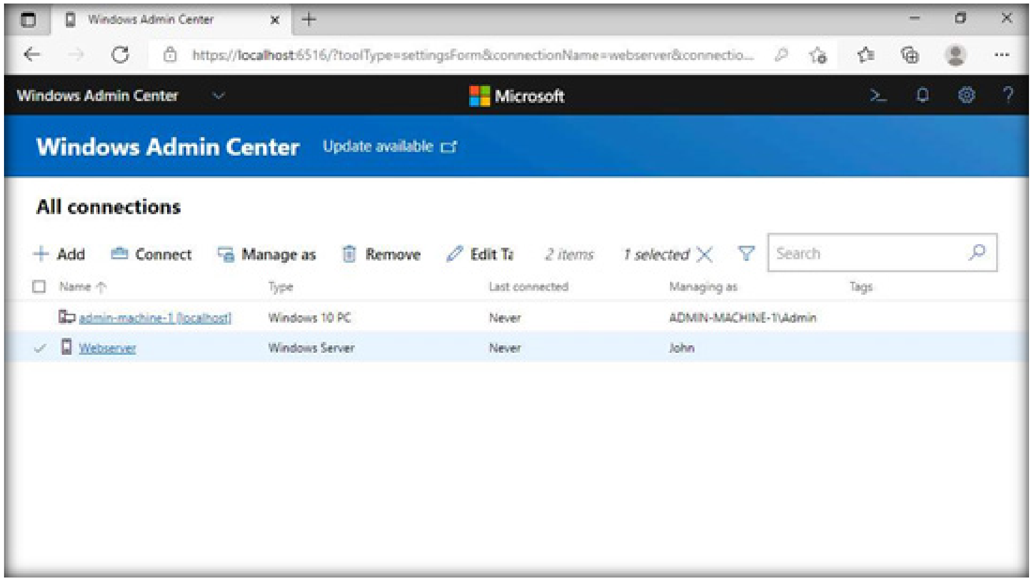
Username *: John

Password *: ••••••••

□ Use these credentials for all connections.

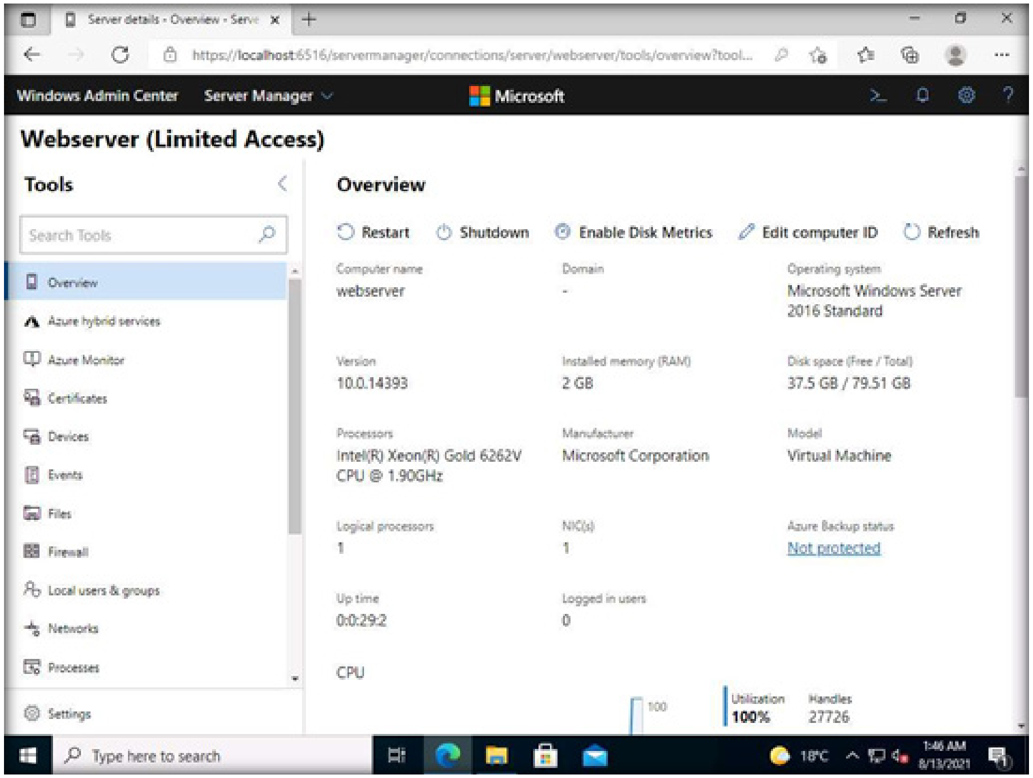
Continue Cancel

37. Wait for a few seconds; Webserver is loaded in WAC for the user john. It can be seen that the user john is selected under Managing as. Click the Webserver link to connect.



Name ↑	Type	Last connected	Managing as	Tags
admin-machine-1 [localhost]	Windows 10 PC	Never	ADMIN-MACHINE-1\Admin	
✓ Webserver	Windows Server	Never	John	

38. Because we have logged in as John in Windows Admin Center, Webserver is connected with limited access (shown at the upper left corner as Webserver (Limited Access)).
Note: If you receive any error pop-up, ignore it.



Server details - Overview - Serve
https://localhost:6516/servermanager/connections/server/webserver/tools/overview?tool...
Windows Admin Center
Server Manager
Microsoft

Webserver (Limited Access)

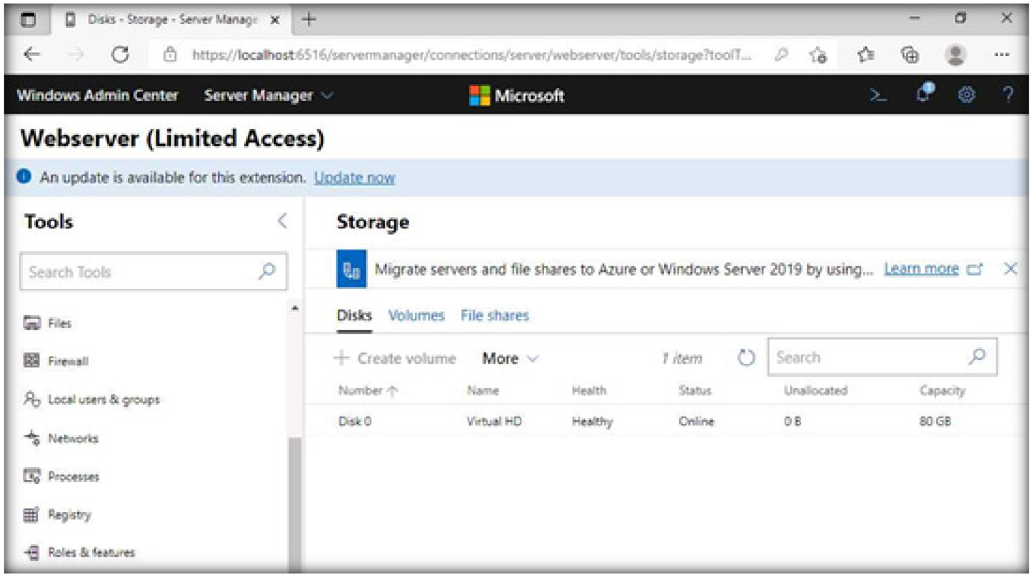
Overview

Computer name: webserver
Domain: -
Operating system: Microsoft Windows Server 2016 Standard
Version: 10.0.14393
Installed memory (RAM): 2 GB
Disk space (Free / Total): 37.5 GB / 79.51 GB
Processors: Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz
Manufacturer: Microsoft Corporation
Model: Virtual Machine
Logical processors: 1
NIC(s): 1
Azure Backup status: Not protected
Up time: 0:0:29:2
Logged in users: 0

CPU
Utilization: 100%
Handles: 27726

39. As a user of Webserver, you can try to add new storage to it. However, because we added the user john in RBAC and allowed limited access permission only, the system will not allow user John to add new storage.

40. Click Storage in the Tools pane. Wait for a few seconds; the Storage pane appears on the right side of the window.



Disks - Storage - Server Manage
https://localhost:6516/servermanager/connections/server/webserver/tools/storage?toolT...
Windows Admin Center
Server Manager
Microsoft

Webserver (Limited Access)

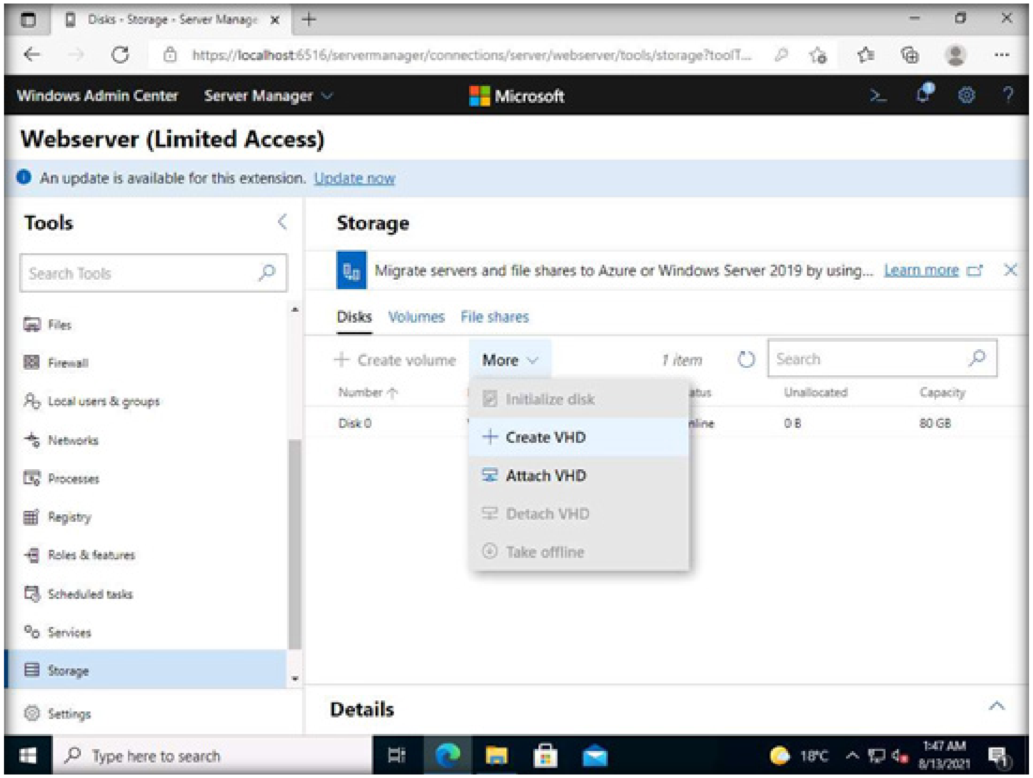
An update is available for this extension. Update now

Storage

Migrate servers and file shares to Azure or Windows Server 2019 by using... Learn more

Number	Name	Health	Status	Unallocated	Capacity
Disk 0	Virtual HD	Healthy	Online	0 B	80 GB

41. Under the Disks menu on the Storage pane, click More and select the Create VHD option.

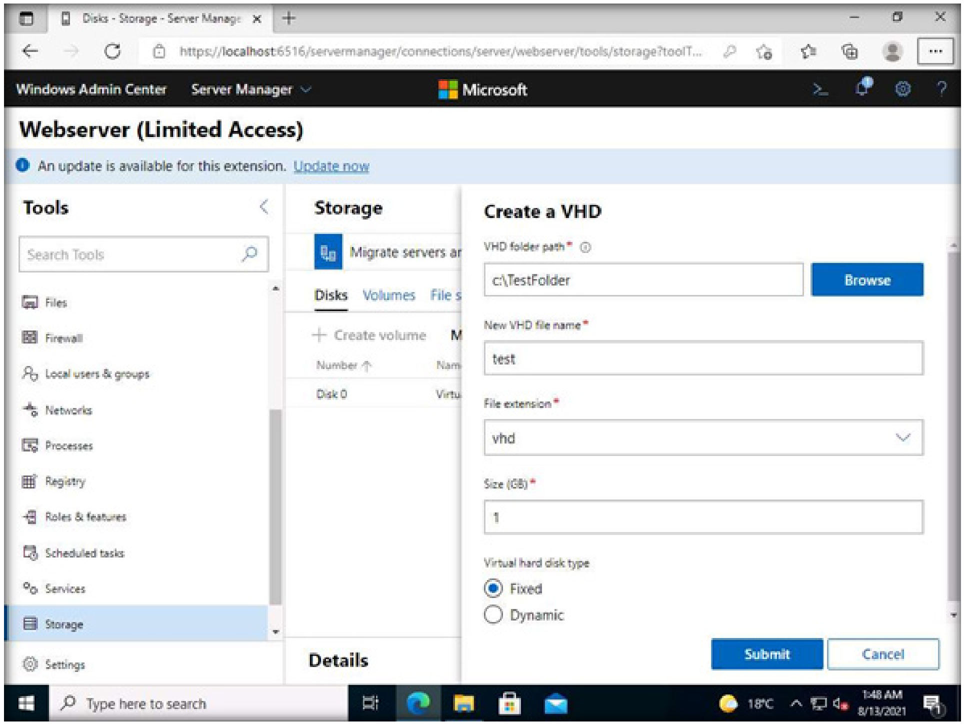


An update is available for this extension. Update now

Migrate servers and file shares to Azure or Windows Server 2019 by using... Learn more

42. The Create VHD pane opens. Type the following in the respective fields and click Submit.

- VHD folder path: c:\TestFolder
- New VHD file name: test
- File extension: vhd
- Size (GB): 1
- Virtual hard disk type: Fixed



Create a VHD

VHD folder path*: c:\TestFolder [Browse]

New VHD file name*: test

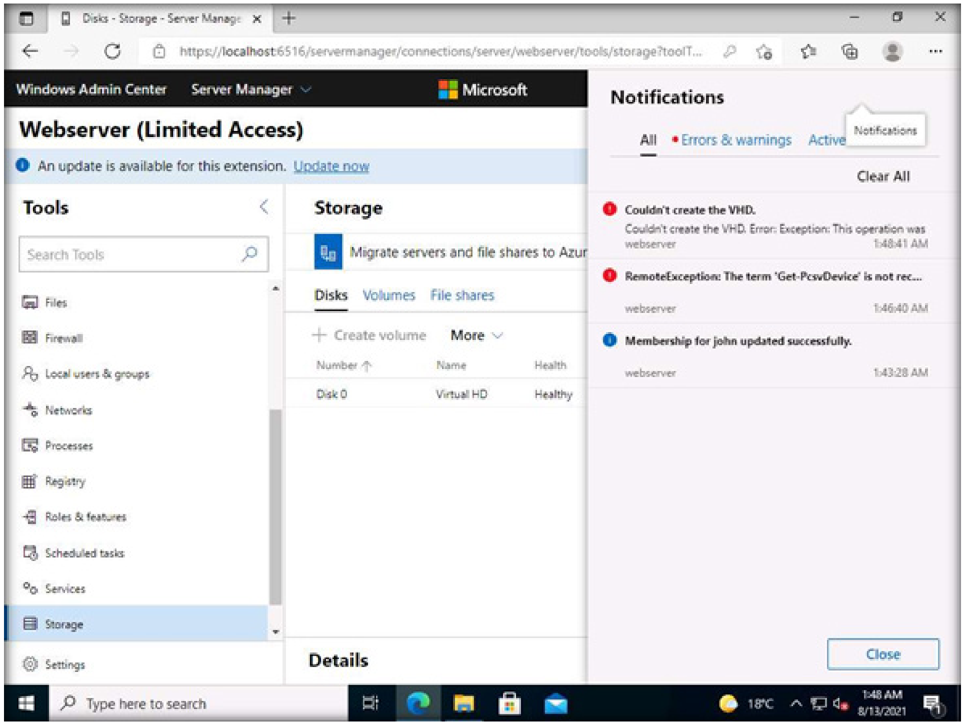
File extension*: vhd

Size (GB)*: 1

Virtual hard disk type
● Fixed
○ Dynamic

[Submit] [Cancel]

43. The following error notification appears (See the Notifications icon): Couldn't create the VHD. Error Exception: This operation was blocked by role-based access control settings.



An update is available for this extension. Update now

Number	Name	Health
Disk 0	Virtual HD	Healthy

Couldn't create the VHD.
Couldn't create the VHD. Error: Exception: This operation was
webserver 1:48:41 AM

RemoteException: The term 'Get-PcsvDevice' is not rec...
webserver 1:46:40 AM

Membership for john updated successfully.
webserver 1:43:28 AM

44. As demonstrated, a security professional can use the WAC tool to manage system resources and permissions.

45. Close all open windows.

46. Turn off the Admin Machine-1 virtual machine.

EXERCISE 3: IMPLEMENT ROLE-BASED ACCESS CONTROL IN WINDOWS ADMIN CENTER (WAC)

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

In centralized authentication, authorization for network access is ensured using a single centralized authorization unit.

LAB SCENARIO

A security professional should be aware of the various tools and tricks available to implement the centralized authentication mechanism. In this exercise, we will convert the AD Domain Controller machine to an authentication server. All authentication attempts will be forwarded to this machine. The machine PfSense will be converted to a client which will pass authentication attempts to the authentication server (AD Domain Controller machine). Here, the RADIUS protocol is used which acts as an authentication protocol between server and client.

OBJECTIVE

This lab will demonstrate the implementation of centralized authentication.

OVERVIEW OF CENTRALIZED AUTHENTICATION

The need for centralized authentication arose when it became difficult to implement the authorization process individually for each resource. It uses a central authorization database that allows or denies access to users and the access decision depends on the policies created by centralized units. This enables an easy authorization process for users who access different platforms. Centralized authorization units are easy to handle and have low costs. A single database provides access to all applications, thereby enabling effective security. A centralized database also provides an easy and inexpensive method of adding, modifying, and deleting applications from the centralized unit.

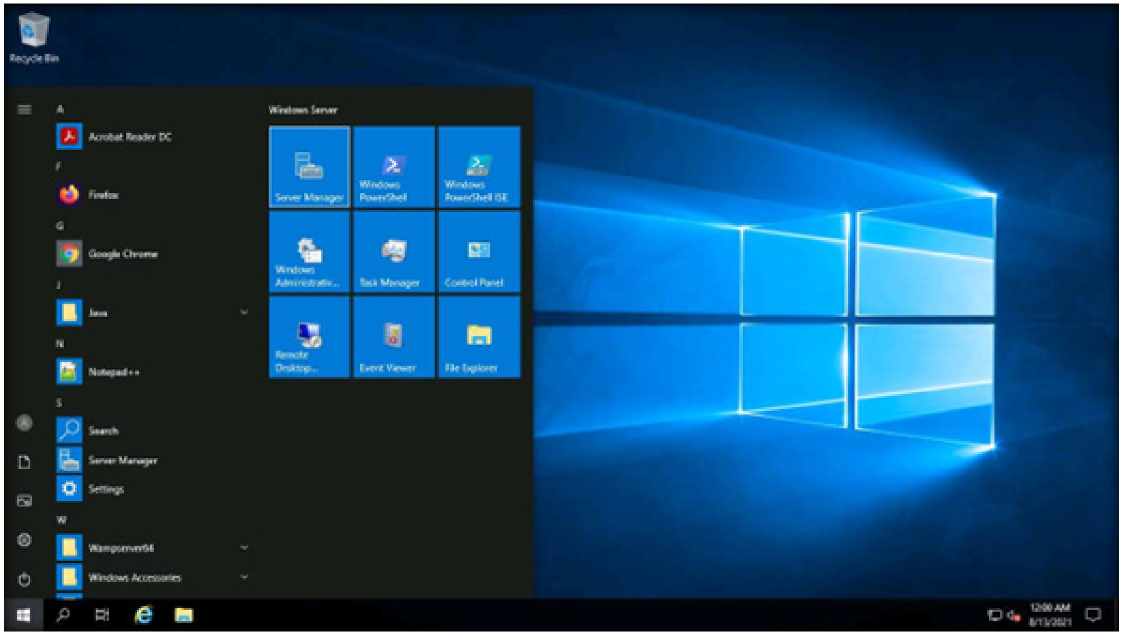
Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the AD Domain Controller virtual machine.

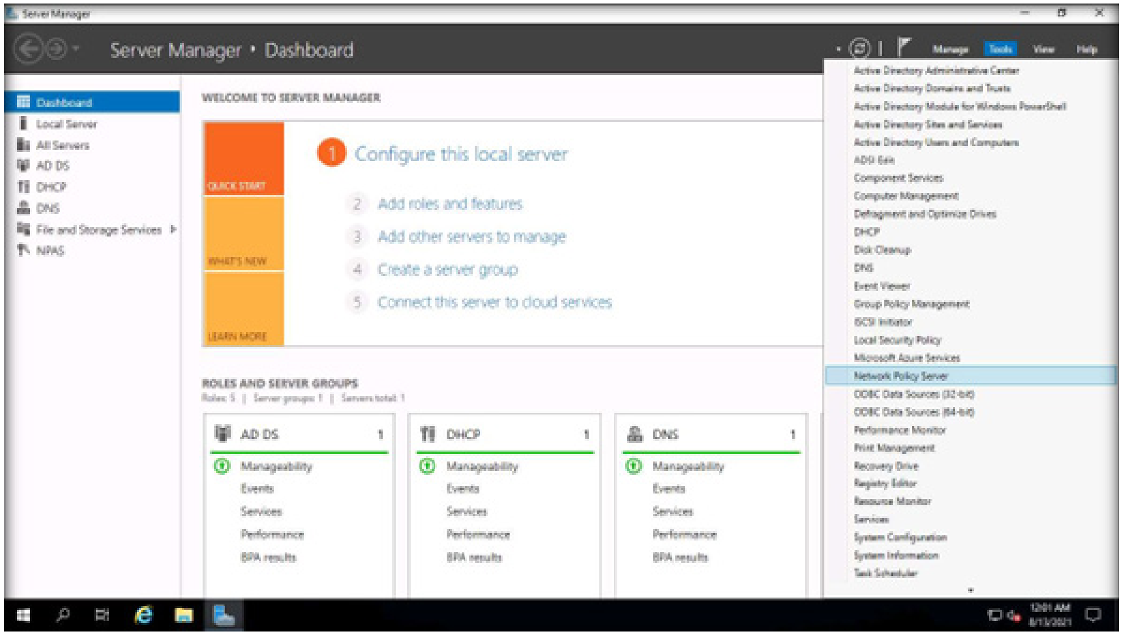
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.
Note: If the network screen appears, click Yes.

3. Click Start icon at the left bottom corner of the Desktop and click Server Manager.

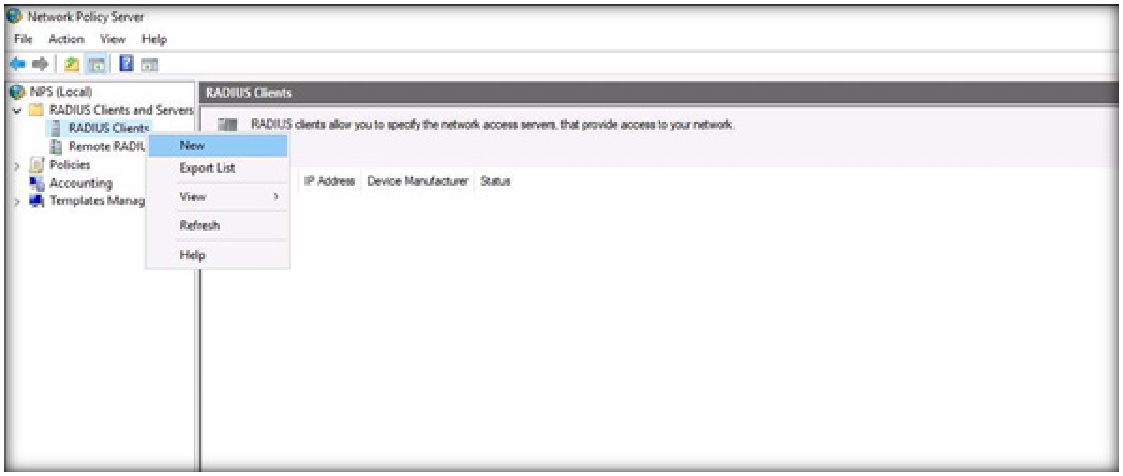
EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM



4. The Server Manager window appears, click Tools and select Network Policy Server from the drop-down list.



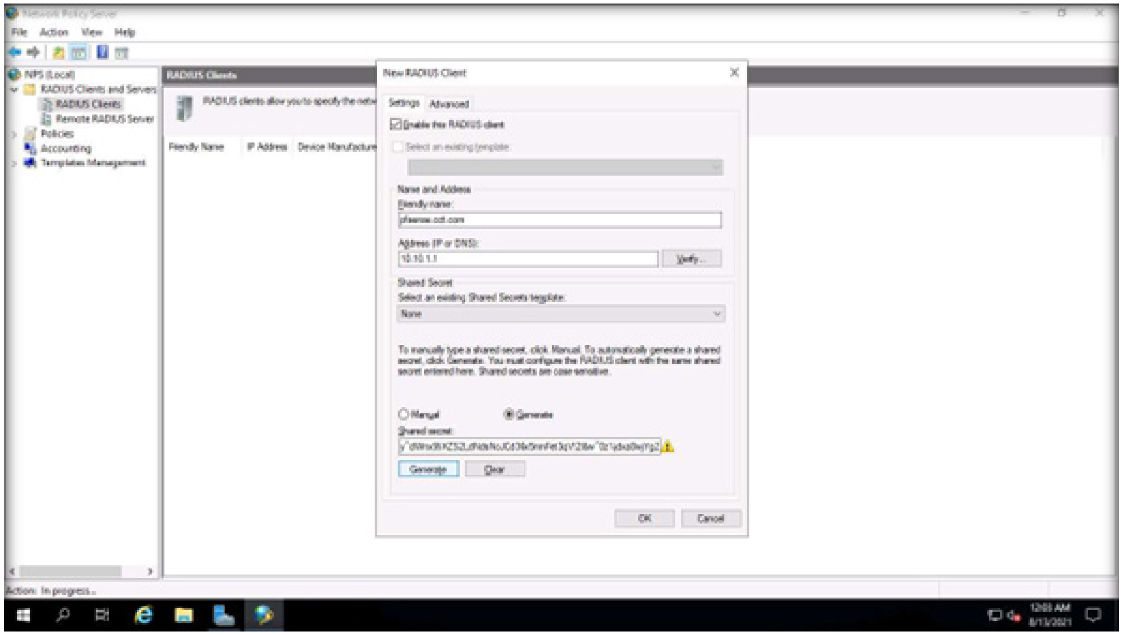
5. The Network Policy Server window appears. In the left pane, expand the RADIUS Clients and Servers node and select the RADIUS Clients node. Now, right-click RADIUS Clients node and click New.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

6. The New RADIUS Client wizard appears, ensure that the Enable this RADIUS Client checkbox is selected. In the Friendly name field, type pfsense.cct.com and in the Address (IP or DNS) field, type 10.10.1.1.

7. Now, select the Generate radio-button and click Generate to generate the Shared secret key.
Note: The shared secret key is a type of password key which is set on the RADIUS server (here, AD Domain Controller machine). This key value must be configured on each RADIUS client (here, we will be using the pfSense Firewall machine). If a secret key presented by a RADIUS client does not match with that of RADIUS server, then the request from the client is not accepted.



New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template

Name and Address

Friendly name: pfsense.cct.com

Address (IP or DNS): 10.10.1.1

Shared Secret

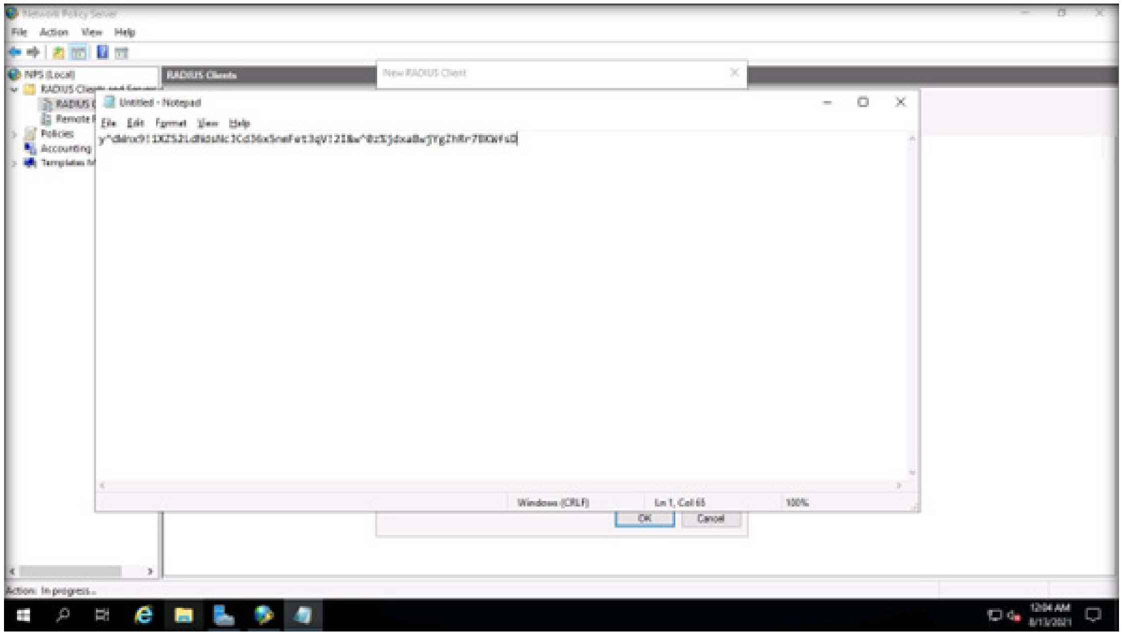
Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

○ Manual ● Generate

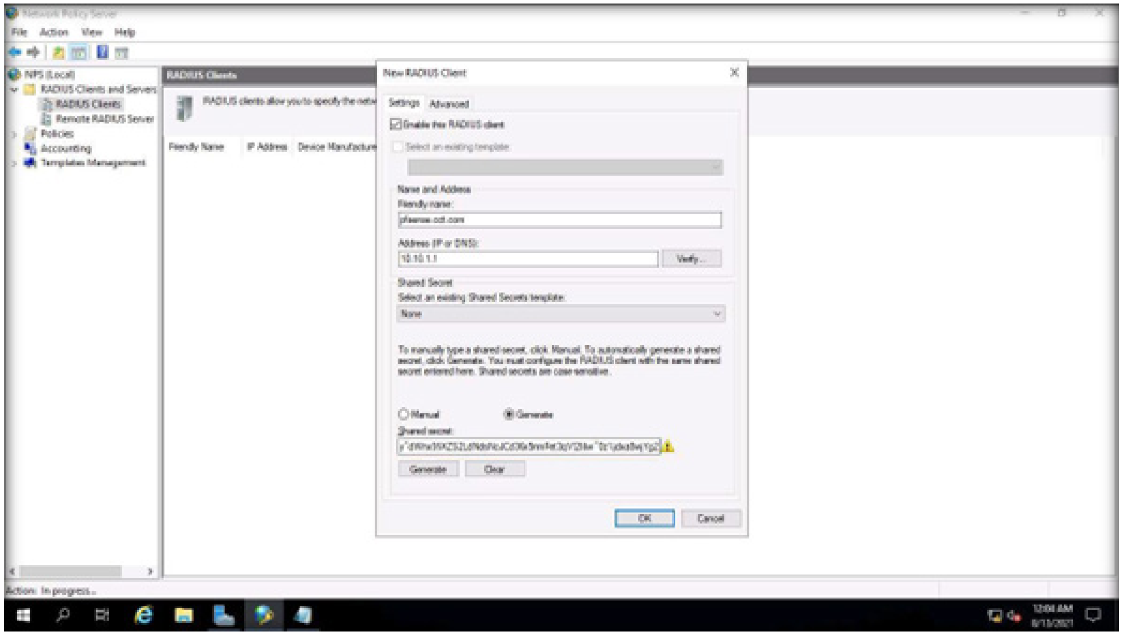
Shared secret: [illegible]

8. Copy the Shared secret value and paste it in the notepad file.



```
y^dWnx9!1XZ%2LdNdsNc3Cd36x5neFet3qV12IBw^@z%jdxaBwjYgZhRr7BKWfsD
```

9. Minimize the Notepad file and in the New RADIUS Client wizard, click OK.



New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: pfsense.cct.com

Address (IP or DNS): 10.10.1.1

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

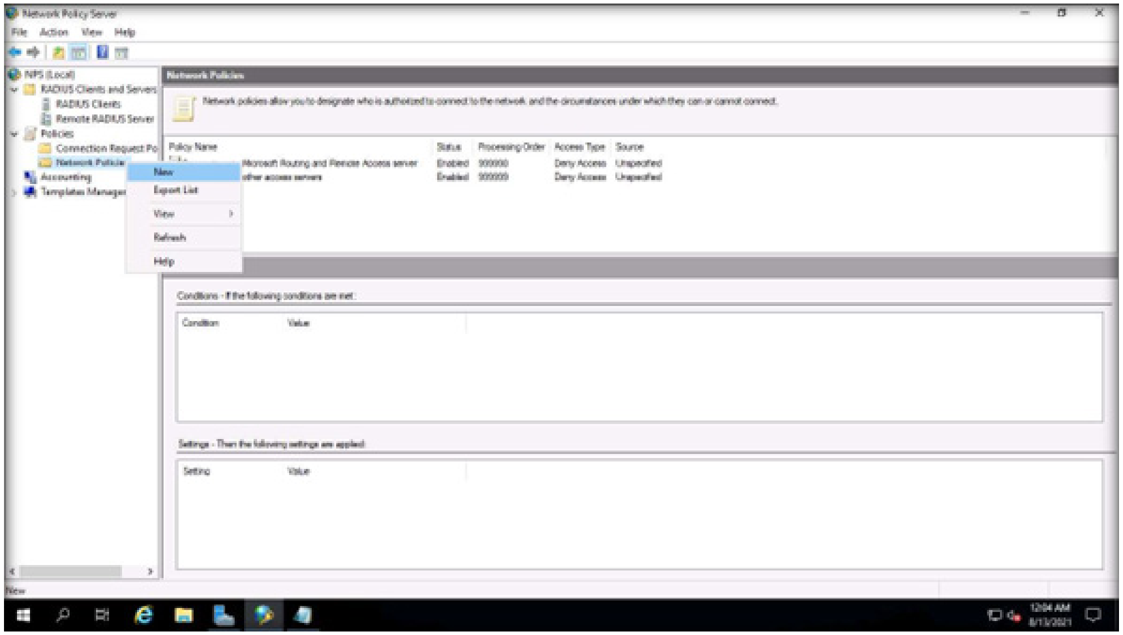
○ Manual ● Generate

Shared secret: [illegible]

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

10. Now, we will configure a network policy that allows users in the Admin-Support to authenticate themselves in the pfSense by using unencrypted authentication.

11. In the Network Policy Server window, expand the Policies node and select Network Policies node. Right-click Network Policies and click New.



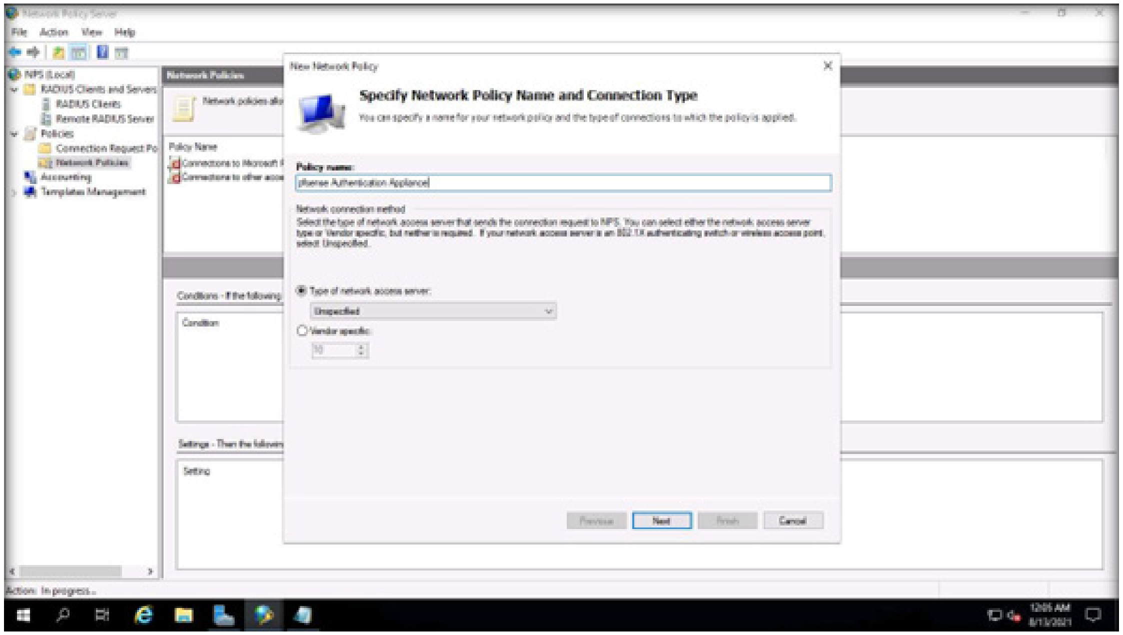
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
other access servers	Enabled	999999	Deny Access	Unspecified

Condition	Value

Setting	Value

12. The New Network Policy window appears. In the Policy name field, type pfsense Authentication Appliance. Click Next.



New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

pfsense Authentication Appliance

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

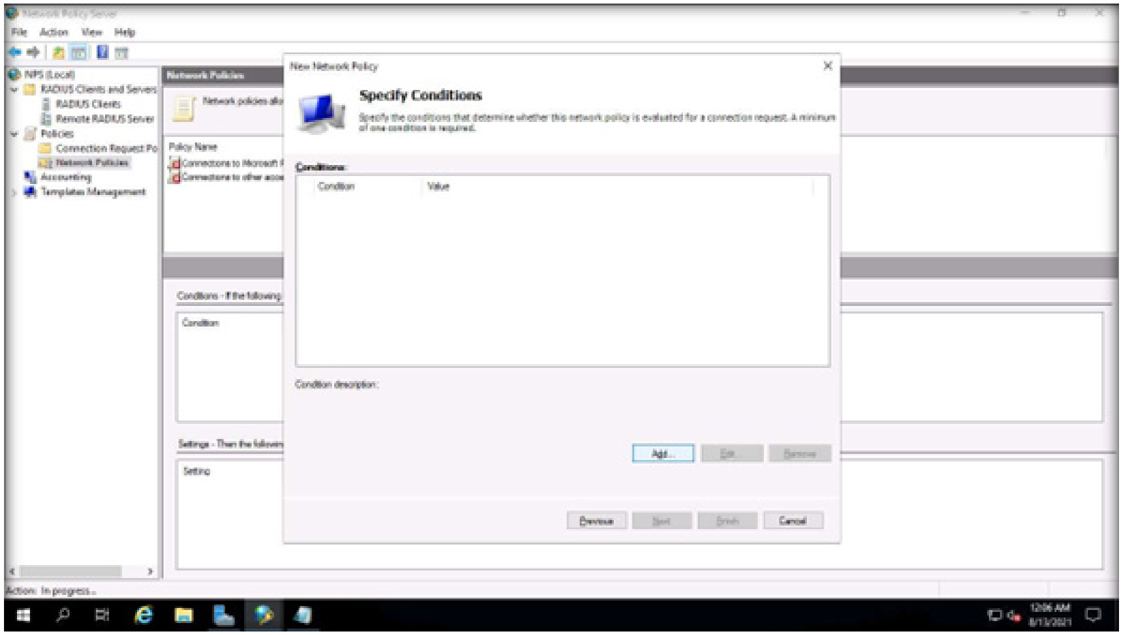
● Type of network access server:

Unspecified

○ Vendor specific:

10

13. Next, the Specify Conditions wizard appears, click Add....



New Network Policy

Specify Conditions

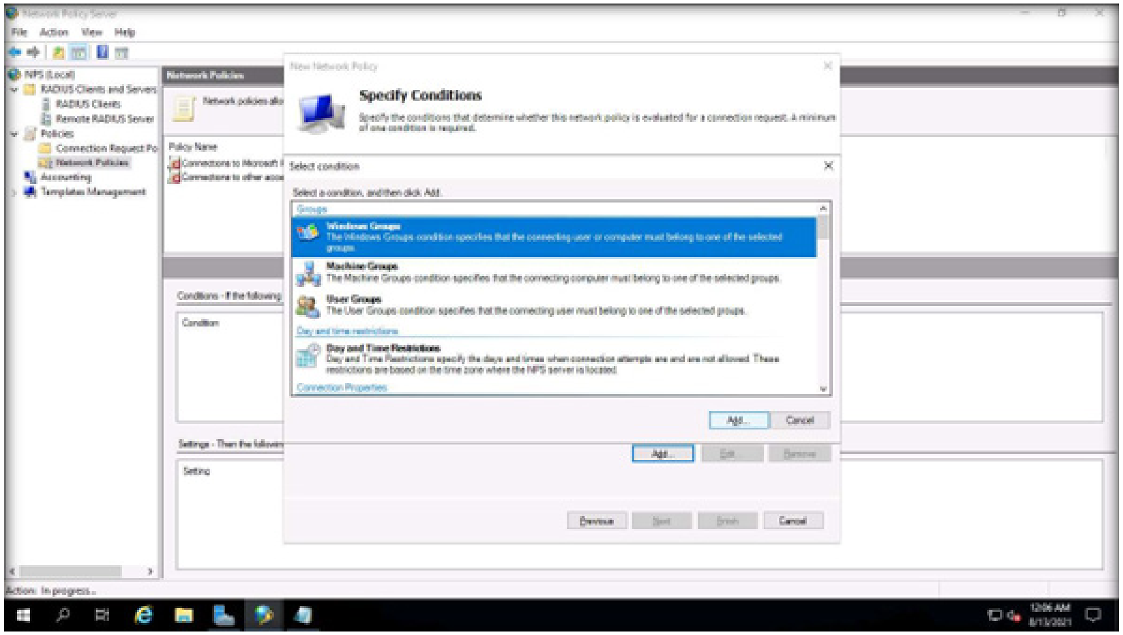
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

Condition description:

14. Under the Select condition section, select Windows Groups from the list of available options and click Add....



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

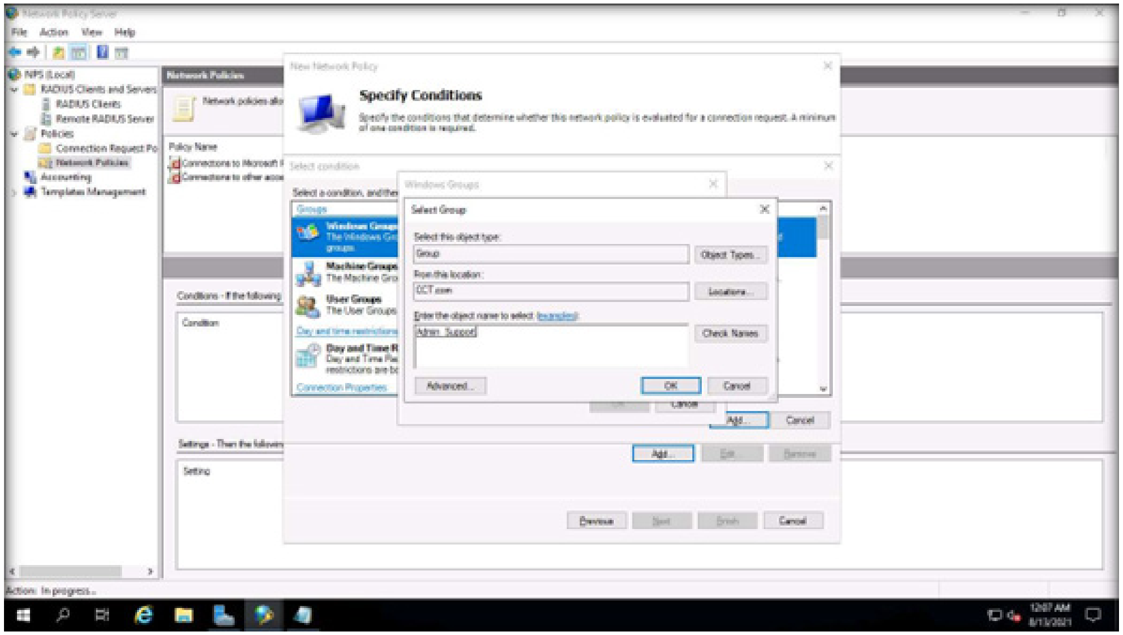
Connection Properties

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

15. The Windows Groups wizard appears, click the Add Groups... button.

16. In the Select Group dialog box, type Admin in the Enter the object name to select field and click Check Names button.

17. The Admin_Support group appears, click OK.


New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select Group

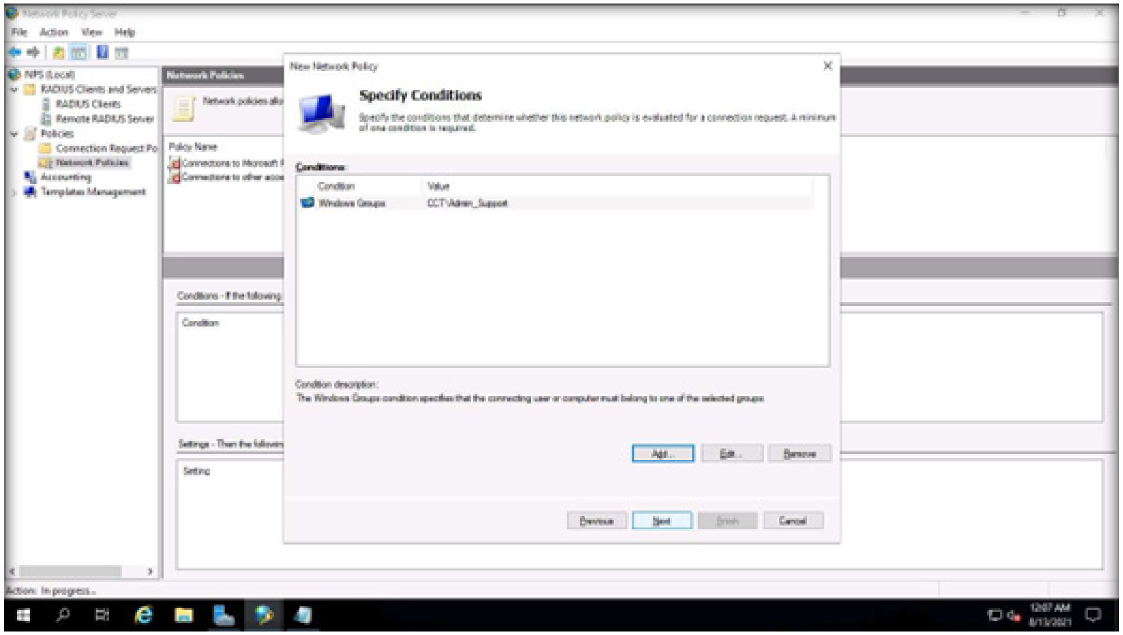
Select this object type:
Group

From this location:
CCT.com

Enter the object name to select (examples):
Admin_Support

18. In the Windows Groups wizard, click OK.

19. In the Specify Conditions wizard, click Next.



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

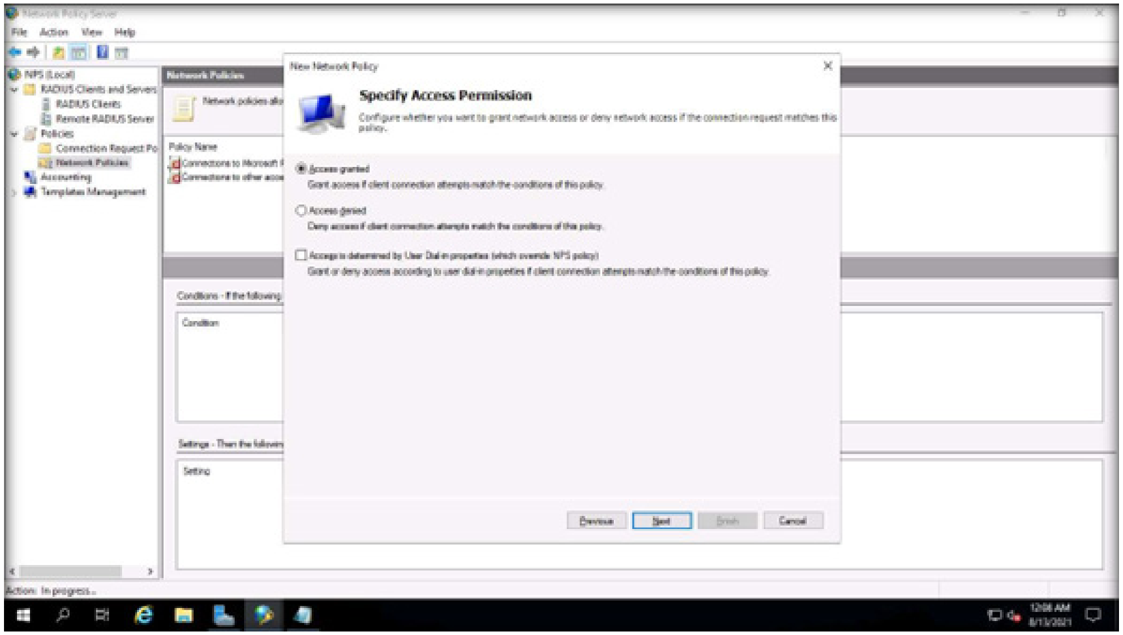
Condition	Value
Windows Groups	CCT\Admin_Support

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

20. In the Specify Access Permission window, ensure that Access granted radio-button is selected, click Next.


New Network Policy

Specify Access Permission

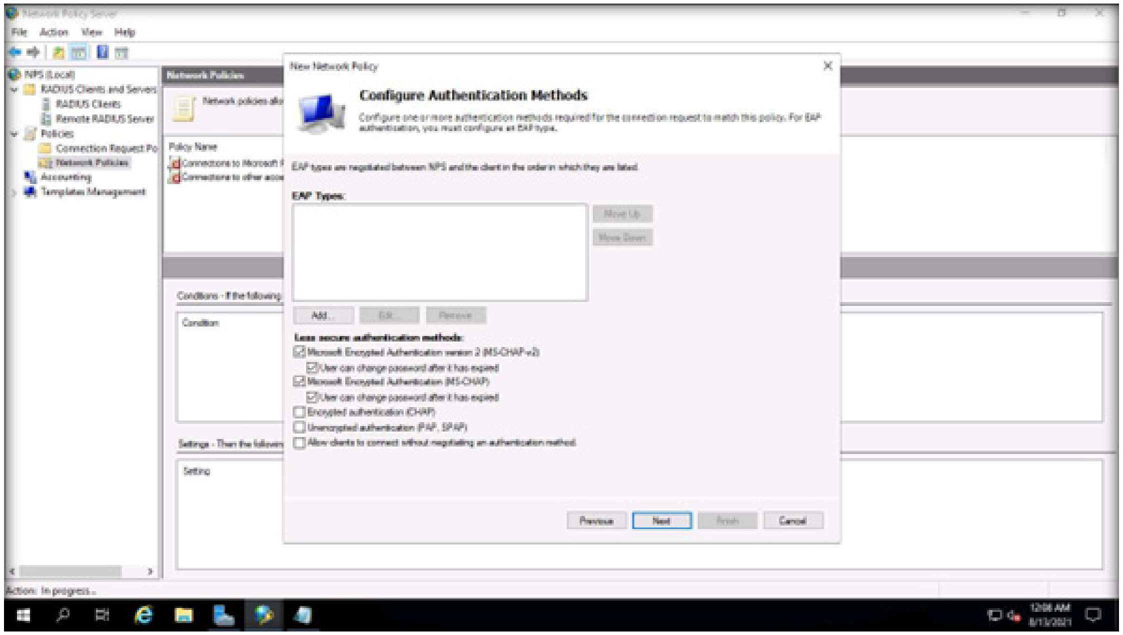
Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

21. In the Configure Authentication Methods wizard, do not change default settings and click Next.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

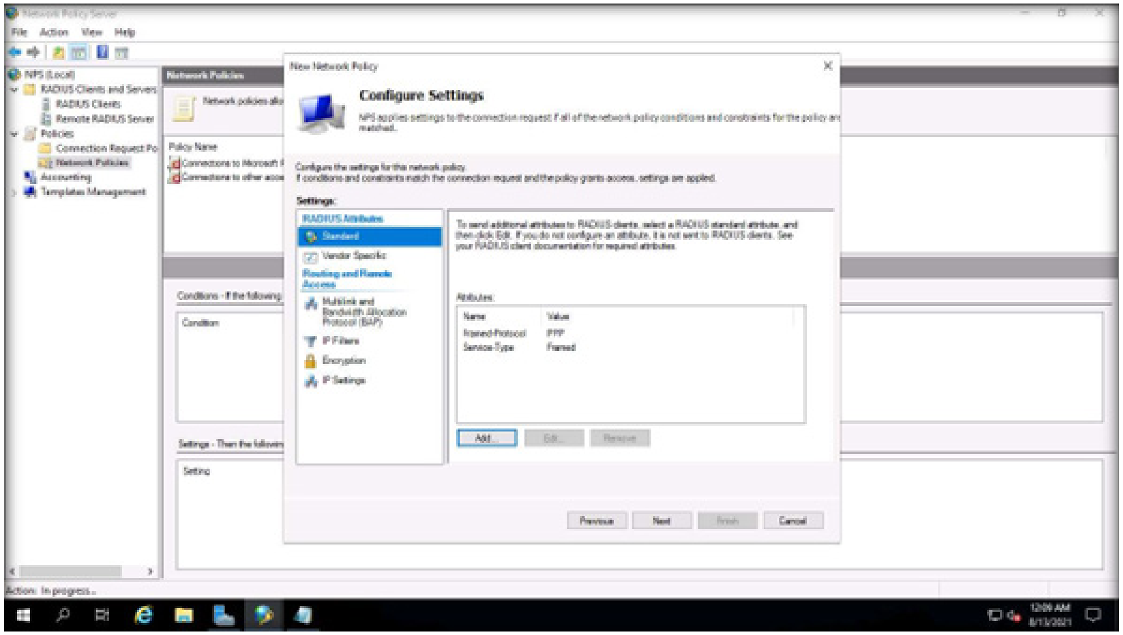
Less secure authentication methods:

- ☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☑ User can change password after it has expired
- ☑ Microsoft Encrypted Authentication (MS-CHAP)
  - ☑ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

22. In the Configure Constraints wizard, click Next.

23. In the Configure Settings wizard, click Add... button present under Attributes field.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

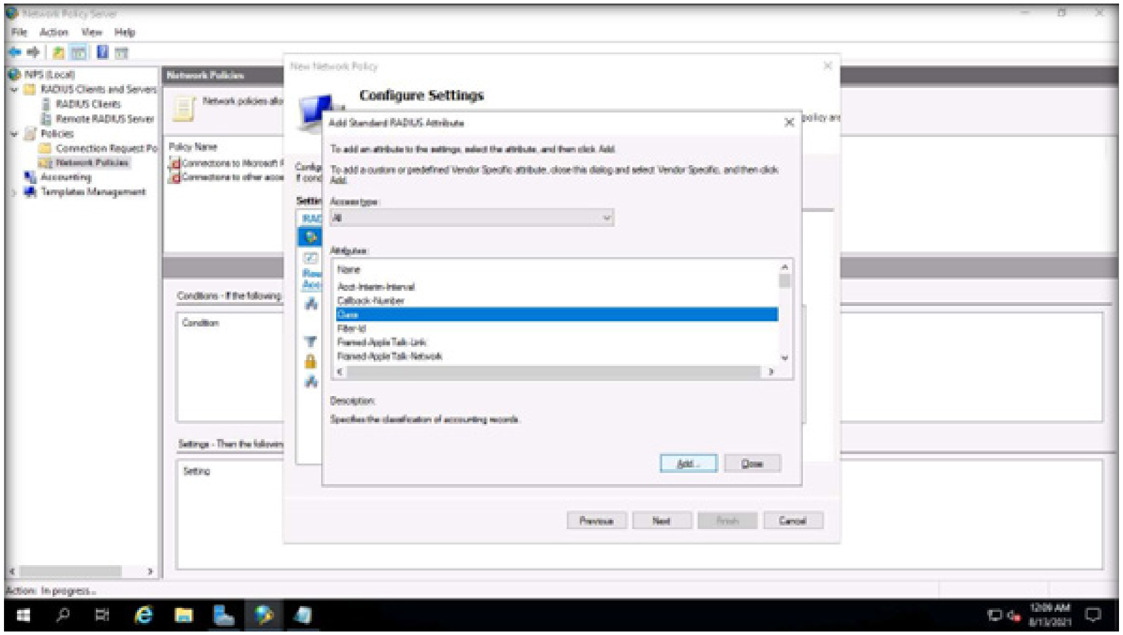
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

24. The Add Standard RADIUS Attribute window appears, select Class from the Attributes box and click Add....



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

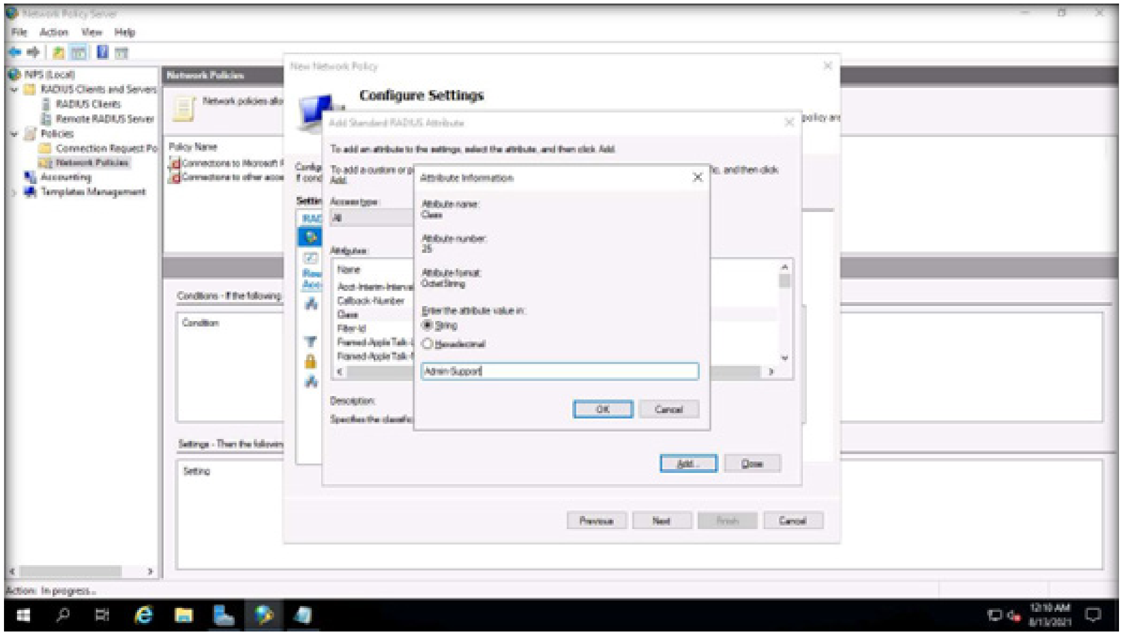
Attributes:

Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network

Description:

Specifies the classification of accounting records.

25. The Attribute Information pop-up appears, type Admin-Support in the field and click OK.



Attribute Information

Attribute name:
Class

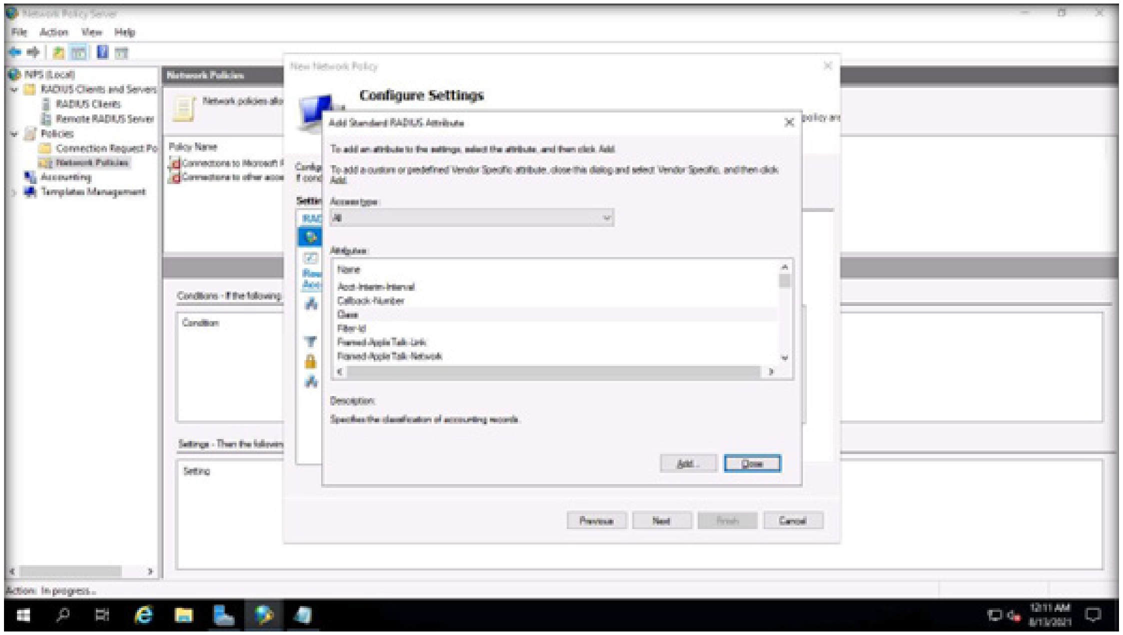
Attribute number:
25

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

Admin-Support

26. In the Add Standard RADIUS Attribute window, click Close.



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

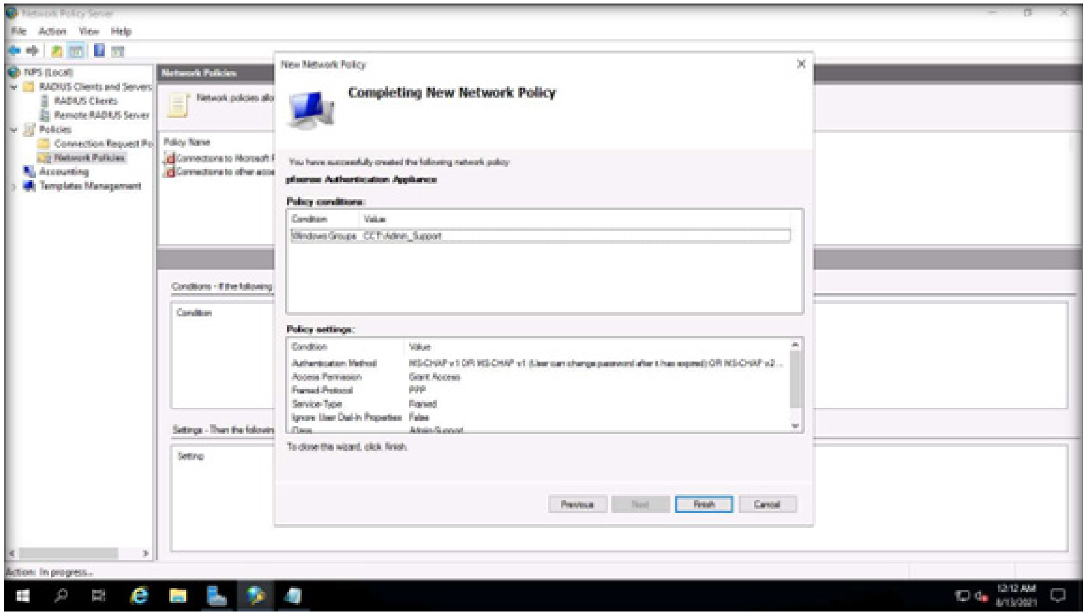
Attributes:
Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network

Description:
Specifies the classification of accounting records.

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

27. In the Configure Settings wizard, click Next.

28. In the Completing New Network Policy window, click Finish.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

pfsense Authentication Appliance

Policy conditions:

Condition	Value
Windows Groups	CCT\Admin_Support

Policy settings:

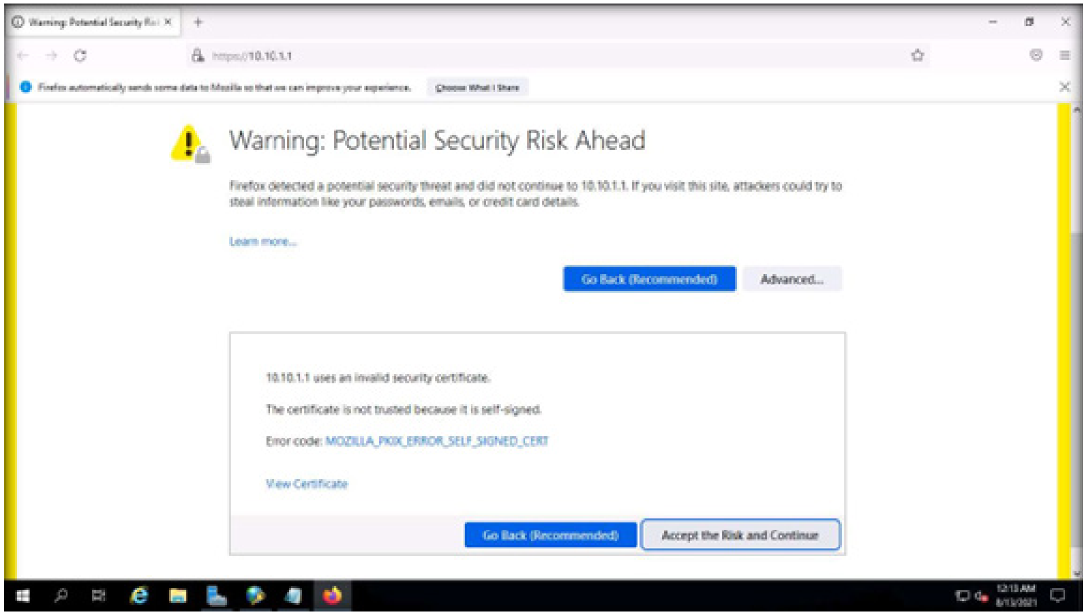
Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Class	Admin-Support

To close this wizard, click Finish.

29. Now, we will enter details regarding the RADIUS server in the PfSense Firewall machine to configure it as a RADIUS client. This allows the AD Domain Controller machine to receive all authentication requests from the PfSense Firewall machine.

30. Open any web browser (here, Mozilla Firefox), enter the URL as http://10.10.1.1 and press Enter.
Note: If an Update available pop-up appears click Dismiss.

31. A Warning: Potential Security Risk Ahead alert appears, click Advanced... button and click Accept the Risk and Continue.



Firefox automatically sends some data to Mozilla so that we can improve your experience.

Warning: Potential Security Risk Ahead

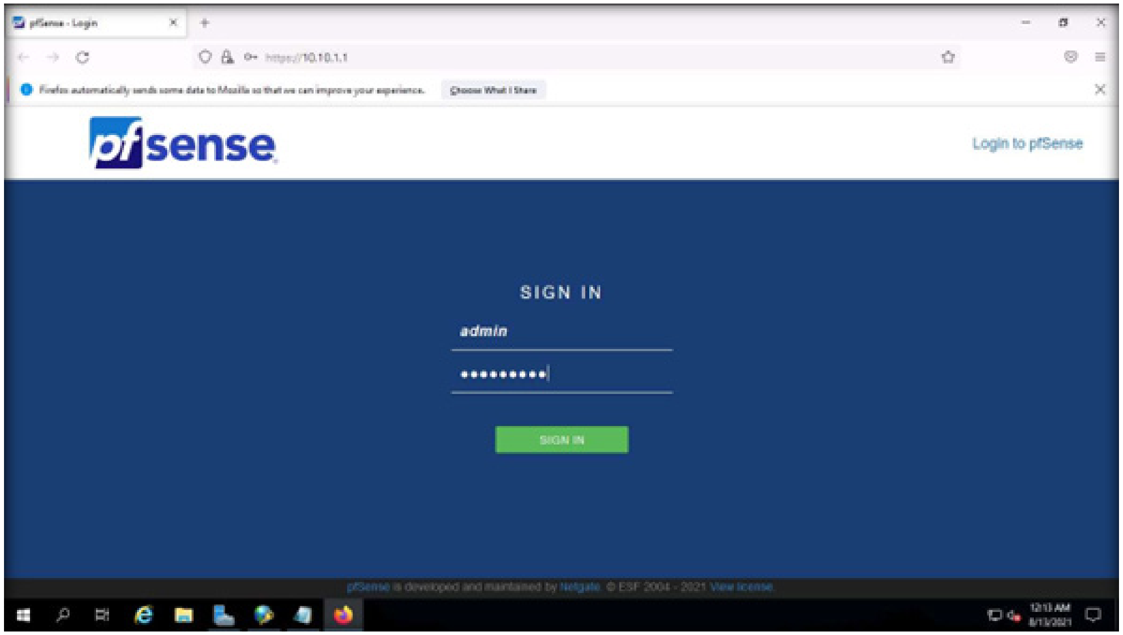
Firefox detected a potential security threat and did not continue to 10.10.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

10.10.1.1 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

32. The login page appears, enter Username and Password as admin and admin@123 respectively and click SIGN IN button.
Note: If the Save login credentials pop-up appears, click Don’t Save.



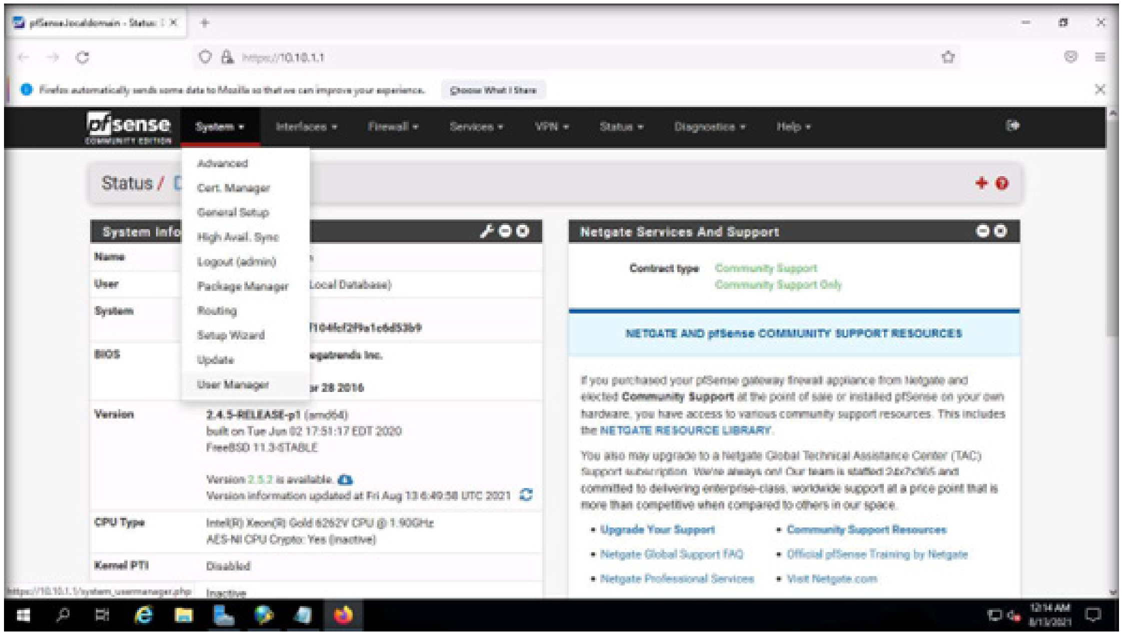
Firefox automatically sends some data to Mozilla so that we can improve your experience.

admin

••••••••••

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

33. The pfSense dashboard appears, navigate to System   User Manager.
Note: If you receive any error, then reload the page and perform step 33 again.



Name	
User	Local Database)
System	f104fcf2f9a1c6d53b9
BIOS	egatrends Inc. r 28 2016
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.5.2 is available. Version information updated at Fri Aug 13 6:49:58 UTC 2021
CPU Type	Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
	Inactive

Contract type Community Support
Community Support Only

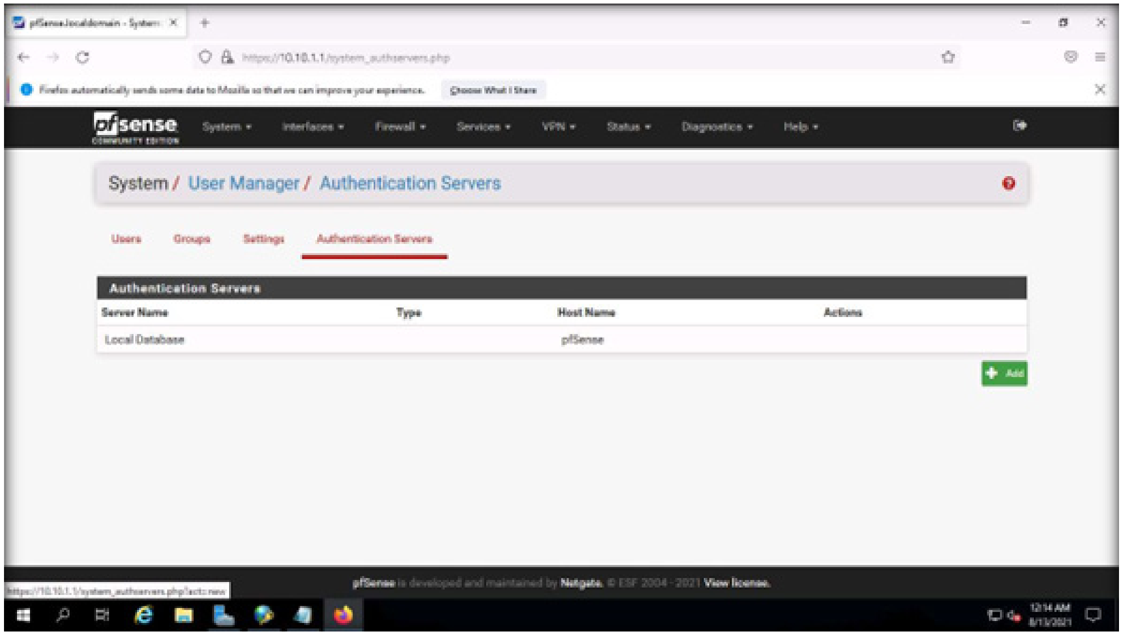
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

34. Navigate to the Authentication Servers tab and click + Add button.



pfSense.localdomain - System
https://10.10.1.1/system_authservers.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

System / User Manager / Authentication Servers

Users
Groups
Settings
Authentication Servers

Authentication Servers

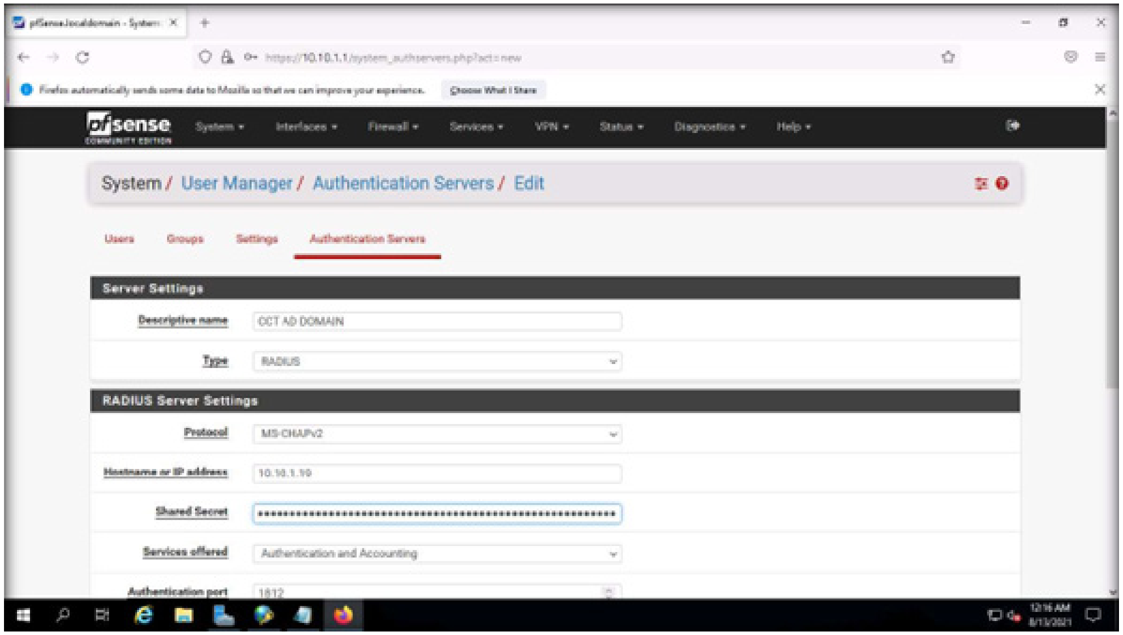
Server Name	Type	Host Name	Actions
Local Database		pfSense	

Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
https://10.10.1.1/system_authservers.php?act=new
12:14 AM
8/13/2021

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

35. In the Descriptive name, enter CCT AD DOMAIN. From the Type list, select RADIUS.
Note: By default, the MS-CHAPv2 protocol is selected under RADIUS Server Settings. MS-CHAPv2 is a password-based authentication protocol that is used to authenticate servers and clients.

36. In the Hostname or IP address field, enter 10.10.1.19. In the Shared Secret field, paste the key value from the Notepad filed.



System / User Manager / Authentication Servers / Edit

Server Settings

Descriptive name: CCT AD DOMAIN

Type: RADIUS

RADIUS Server Settings

Protocol: MS-CHAPv2

Hostname or IP address: 10.10.1.19

Shared Secret: ••

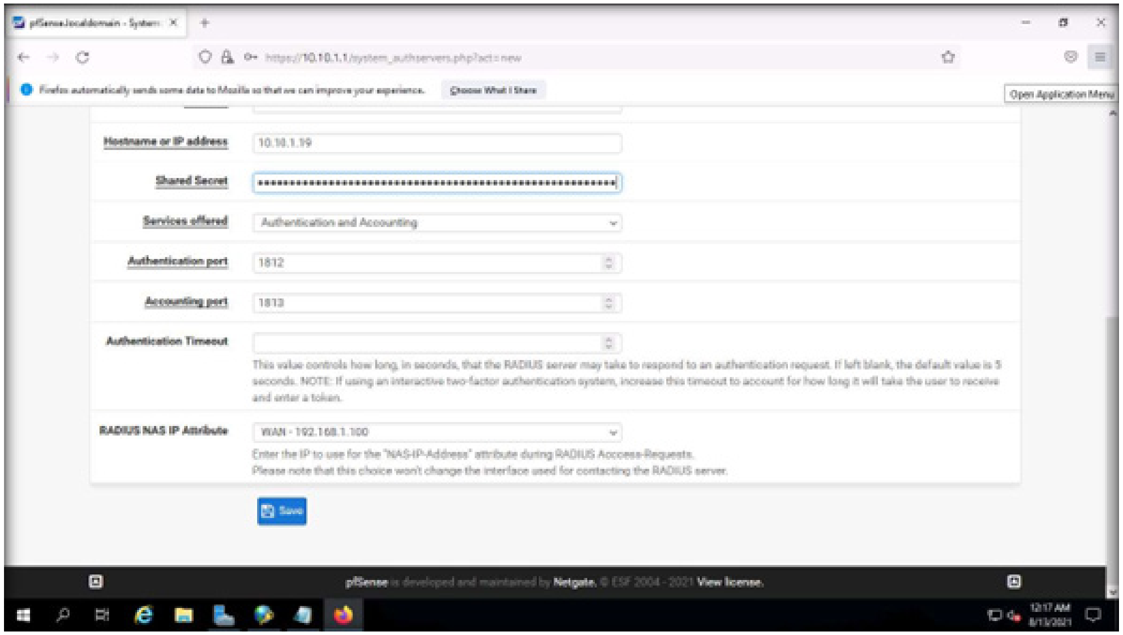
Services offered: Authentication and Accounting

Authentication port: 1812

pfSense.localdomain - System
https://10.10.1.1/system_authservers.php?act=new
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Users
Groups
Settings
Authentication Servers
12:16 AM
8/13/2021

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

37. Scroll-down and click Save button.
Note: If Save login credentials pop-up appears, click Don’t Save.



pfSense.localdomain - System
https://10.10.1.1/system_authservers.php?act=new
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Open Application Menu

Hostname or IP address: 10.10.1.19

Shared Secret: ••

Services offered: Authentication and Accounting

Authentication port: 1812

Accounting port: 1813

Authentication Timeout:

This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute: WAN - 192.168.1.100

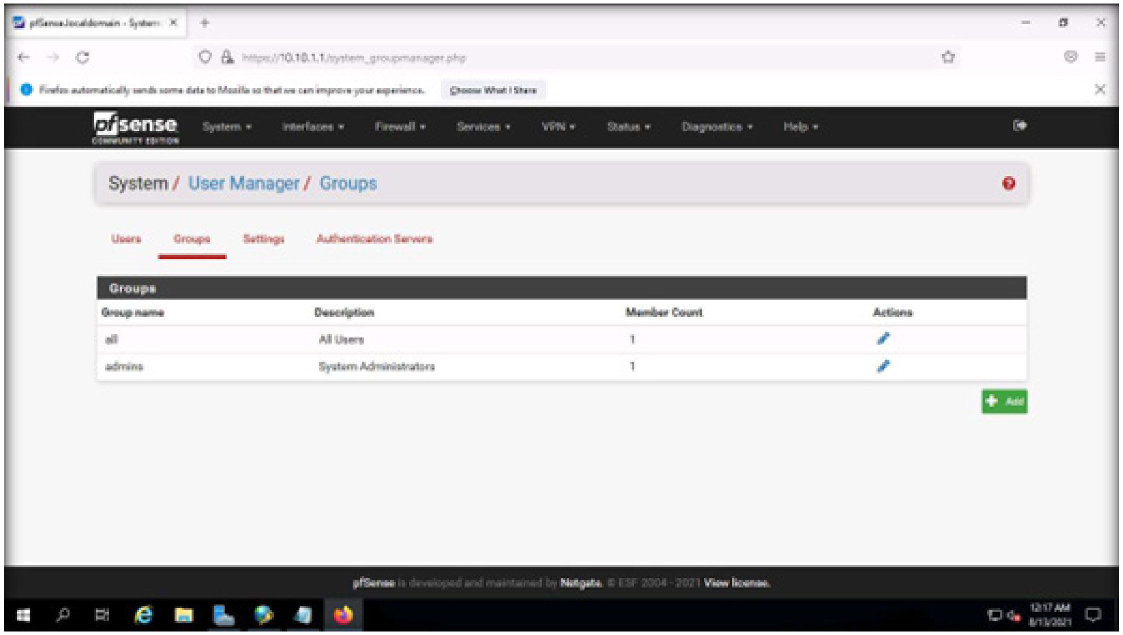
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
Please note that this choice won't change the interface used for contacting the RADIUS server.

Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:17 AM
8/13/2021

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

38. Now, we shall configure role-based access permission to the Admin-Support group. As per the role of users only basic permissions will be provided to ensure that they do not have access to advance system resources.

39. Navigate to the Groups tab, select the + Add button.



pfSense.localdomain - System
https://10.10.1.1/system_groupmanager.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

System / User Manager / Groups

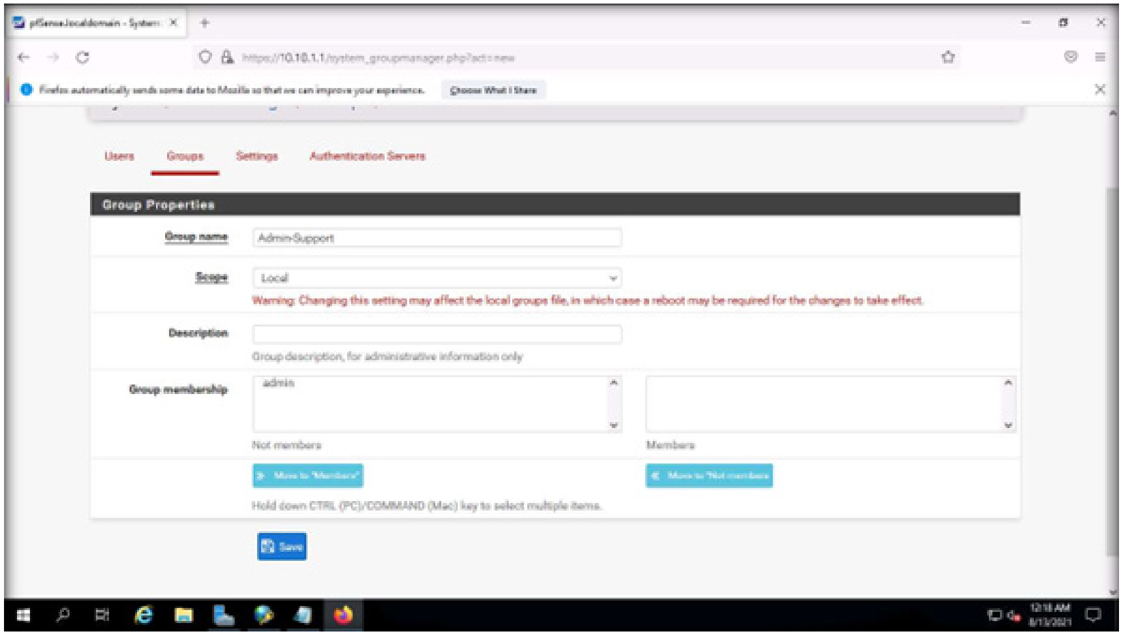
Users | Groups | Settings | Authentication Servers

Groups

Group name	Description	Member Count	Actions
all	All Users	1	✎
admins	System Administrators	1	✎

+ Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:17 AM
8/13/2021

40. In the Group name field, type Admin-Support, scroll-down and click Save.



pfSense.localdomain - System
https://10.10.1.1/system_groupmanager.php?act=new
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Users
Groups
Settings
Authentication Servers

Group Properties

Group name: Admin-Support

Scope: Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description:

Group description, for administrative information only

Group membership: admin

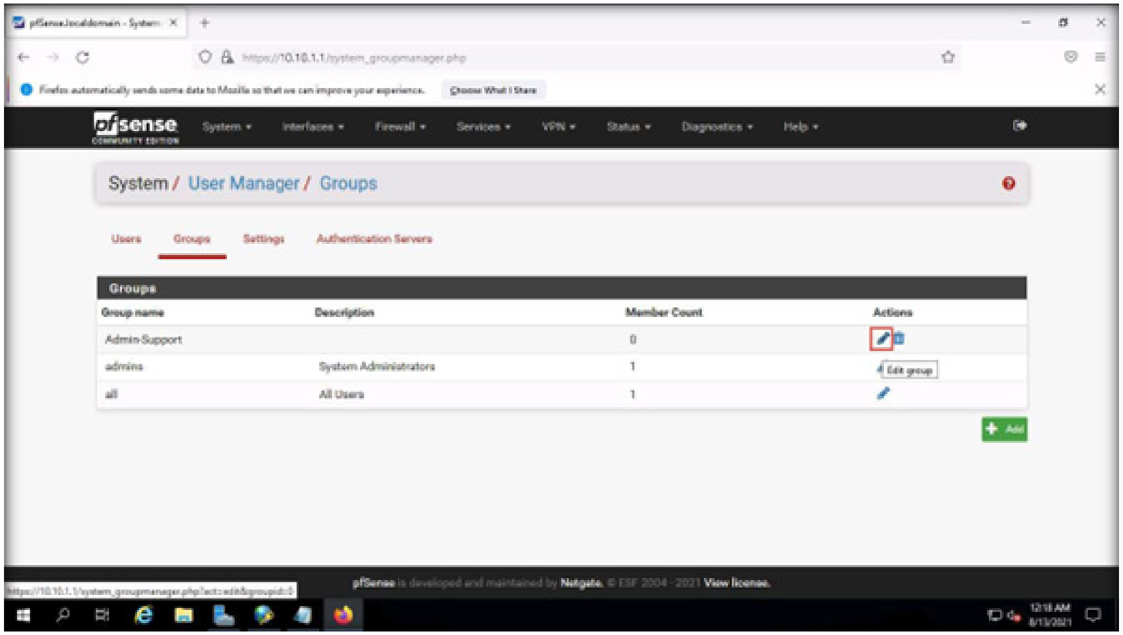
Not members

Members

Move to "Members"
Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

41. It can be viewed that Admin-Support group has been created, under the Actions column, click Edit group icon (pen icon).


pfSense.localdomain - System
https://10.10.1.1/system_groupmanager.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Users
Groups
Settings
Authentication Servers
Edit group
Add
https://10.10.1.1/system_groupmanager.php?act=edit&groupid=0
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:18 AM
8/13/2021

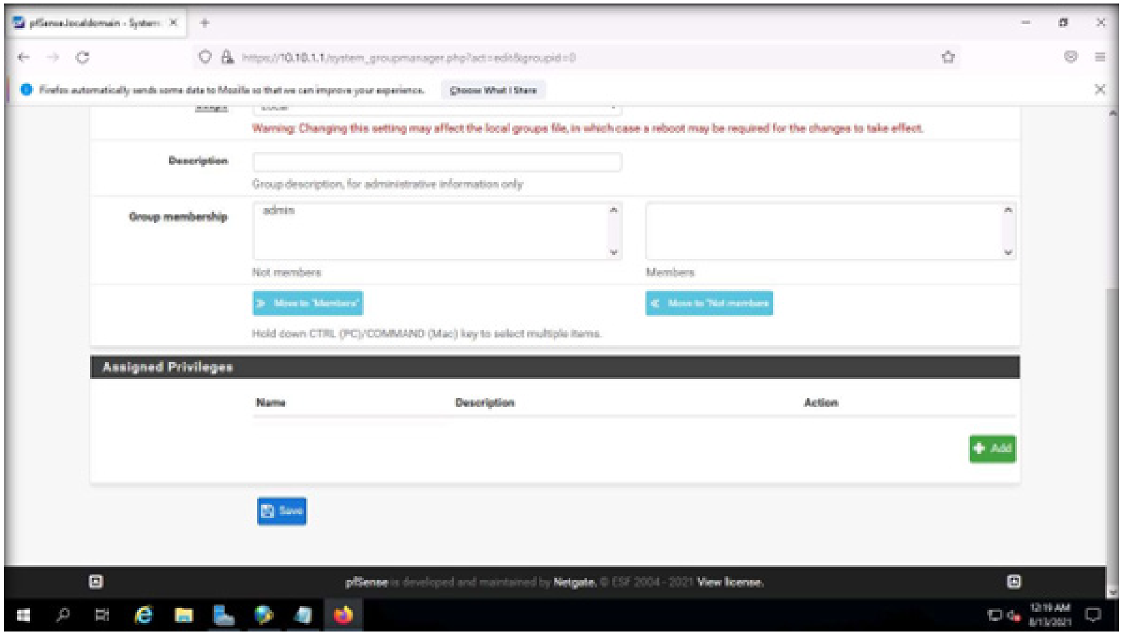
System / User Manager / Groups

Groups

Group name	Description	Member Count	Actions
Admin-Support		0	
admins	System Administrators	1	
all	All Users	1	

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

42. Under Assigned Privileges section, click + Add button.



https://10.10.1.1/system_groupmanager.php?act=edit&groupid=0

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description:

Group description, for administrative information only

Group membership: admin

Not members

Members

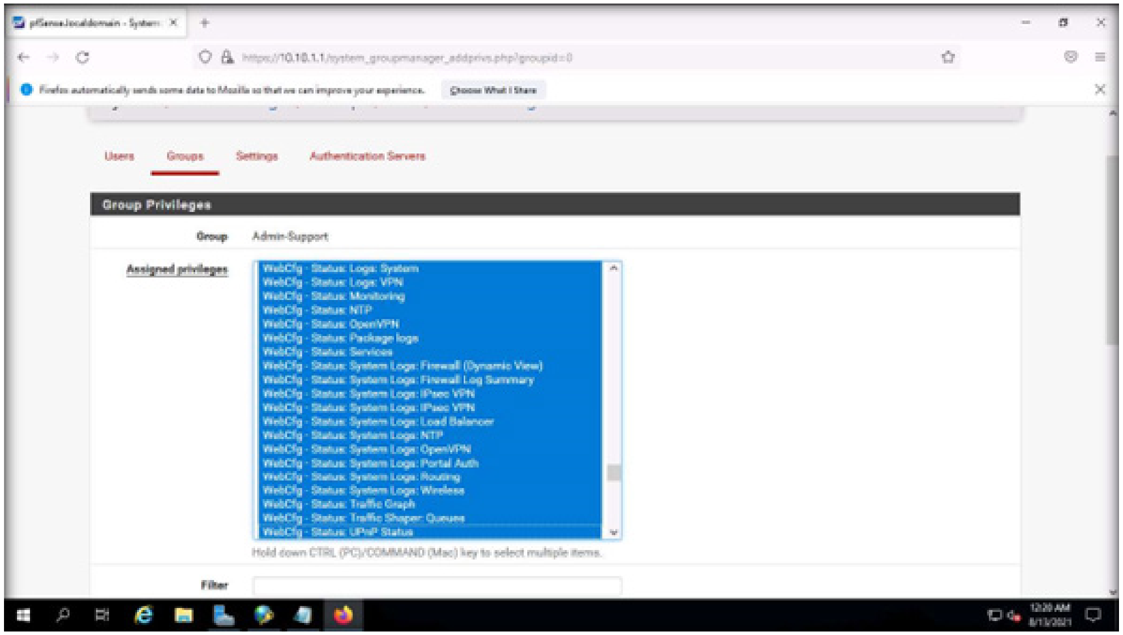
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description	Action

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

43. Under Assigned Privileges, click to select WebCfg - Dashboard (all) scroll down, press Shift key from the keyboard and click WebCfg - Status: UPnP Status. All the privileges from WebCfg - Dashboard (all) to WebCfg - Status: UPnP Status will be selected, as shown in the screenshot.



pfSense.localdomain - System

https://10.10.1.1/system_groupmanager_addprivs.php?groupid=0

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

Group Privileges

Group: Admin-Support

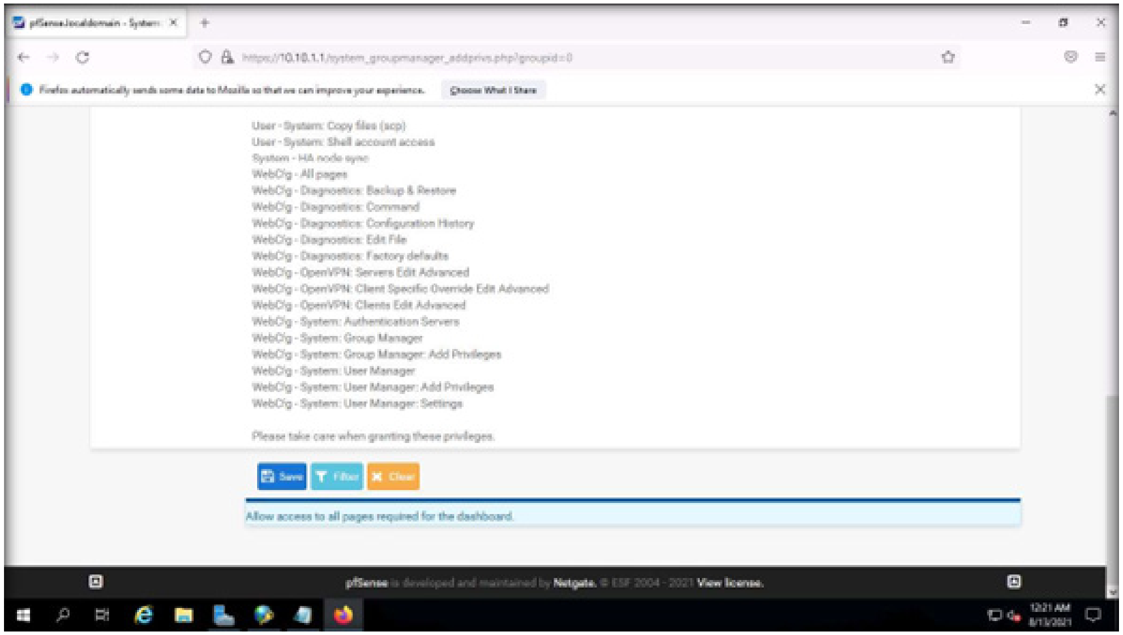
Assigned privileges:

- WebCfg - Status: Logs: System
- WebCfg - Status: Logs: VPN
- WebCfg - Status: Monitoring
- WebCfg - Status: NTP
- WebCfg - Status: OpenVPN
- WebCfg - Status: Package logs
- WebCfg - Status: Services
- WebCfg - Status: System Logs: Firewall (Dynamic View)
- WebCfg - Status: System Logs: Firewall Log Summary
- WebCfg - Status: System Logs: IPsec VPN
- WebCfg - Status: System Logs: IPsec VPN
- WebCfg - Status: System Logs: Load Balancer
- WebCfg - Status: System Logs: NTP
- WebCfg - Status: System Logs: OpenVPN
- WebCfg - Status: System Logs: Portal Auth
- WebCfg - Status: System Logs: Routing
- WebCfg - Status: System Logs: Wireless
- WebCfg - Status: Traffic Graph
- WebCfg - Status: Traffic Shaper: Queues
- WebCfg - Status: UPnP Status

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

44. Scroll down and click Save.



User - System: Copy files (scp)
User - System: Shell account access
System - HA node sync
WebCfg - All pages
WebCfg - Diagnostics: Backup & Restore
WebCfg - Diagnostics: Command
WebCfg - Diagnostics: Configuration History
WebCfg - Diagnostics: Edit File
WebCfg - Diagnostics: Factory defaults
WebCfg - OpenVPN: Servers Edit Advanced
WebCfg - OpenVPN: Client Specific Override Edit Advanced
WebCfg - OpenVPN: Clients Edit Advanced
WebCfg - System: Authentication Servers
WebCfg - System: Group Manager
WebCfg - System: Group Manager: Add Privileges
WebCfg - System: User Manager
WebCfg - System: User Manager: Add Privileges
WebCfg - System: User Manager: Settings

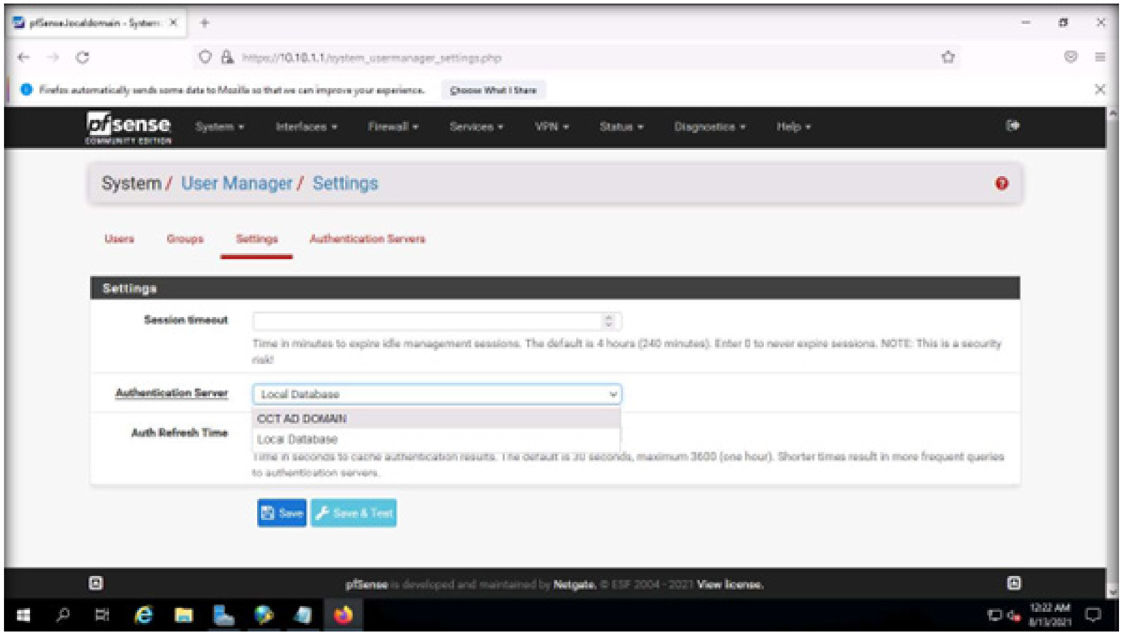
Please take care when granting these privileges.

Allow access to all pages required for the dashboard.

pfSense.localdomain - System
https://10.10.1.1/system_groupmanager_addprivs.php?groupid=0
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Save
Filter
Clear
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:21 AM
8/13/2021

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

45. Navigate to the Settings tab, select CCT AD DOMAIN as an Authentication Server and click Save.


pfSense.localdomain - System
https://10.10.1.1/system_usermanager_settings.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Users
Groups
Settings
Authentication Servers
Save
Save & Test
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:22 AM
8/13/2021

System / User Manager / Settings

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server: Local Database

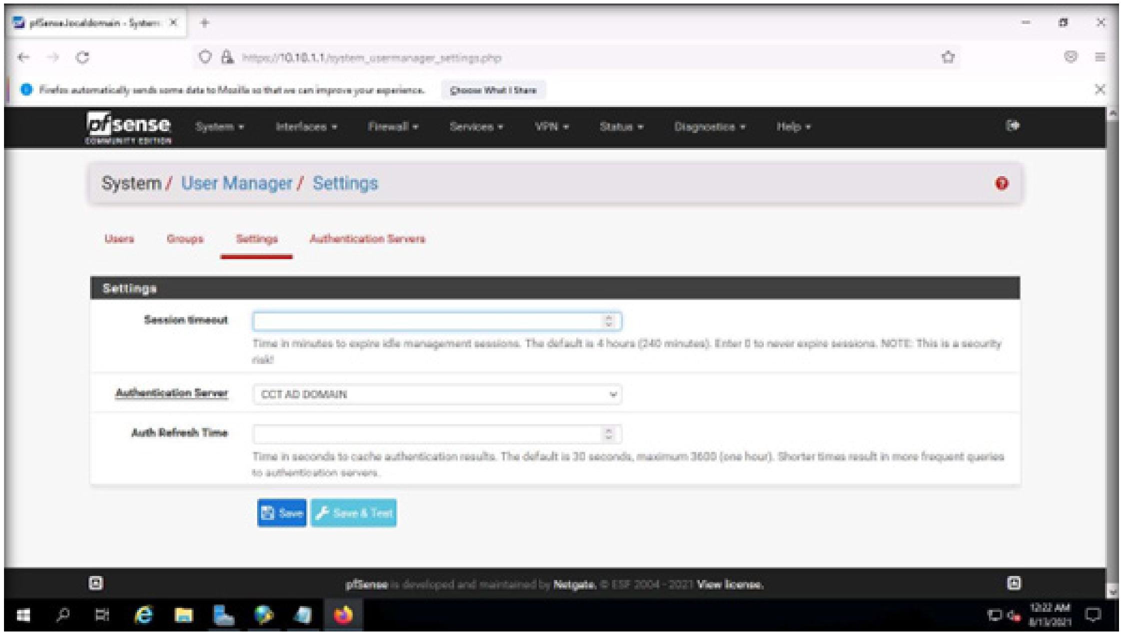
CCT AD DOMAIN
Local Database

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

EXERCISE 4: IMPLEMENT CENTRALIZED AUTHENTICATION MECHANISM

46. Next, click (⎋) icon from the top-right corner of the dashboard to logout from the account.


pfSense.localdomain - System
https://10.10.1.1/system_usermanager_settings.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System ▾
Interfaces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Help ▾
Users
Groups
Settings
Authentication Servers
Save
Save & Test
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:22 AM
8/13/2021

System / User Manager / Settings

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

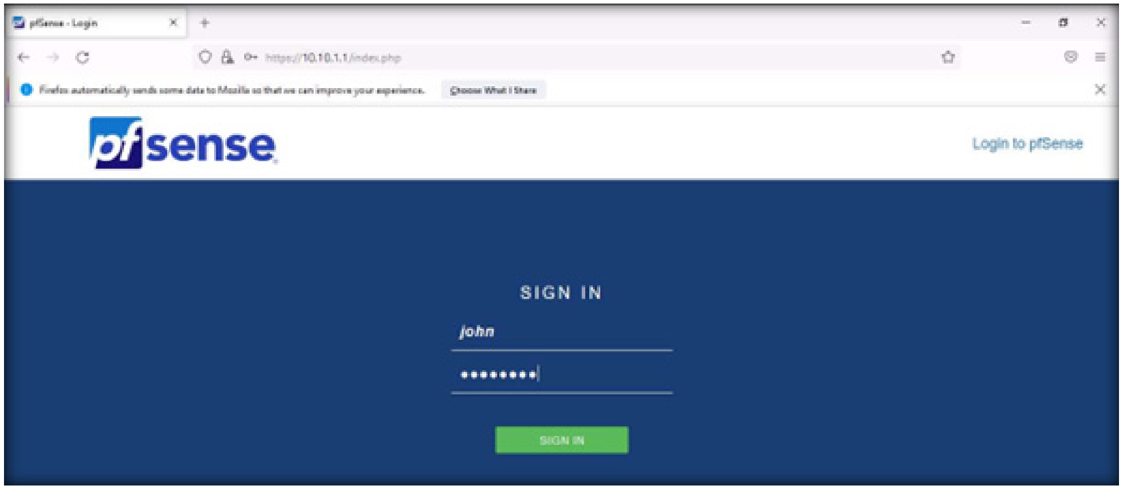
Authentication Server: CCT AD DOMAIN

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

47. Now, we will use non-administrative user account to sign into pfSense, the entered credentials will pass through the AD Domain Controller machine and if the user account is present in the group, it will be granted access.

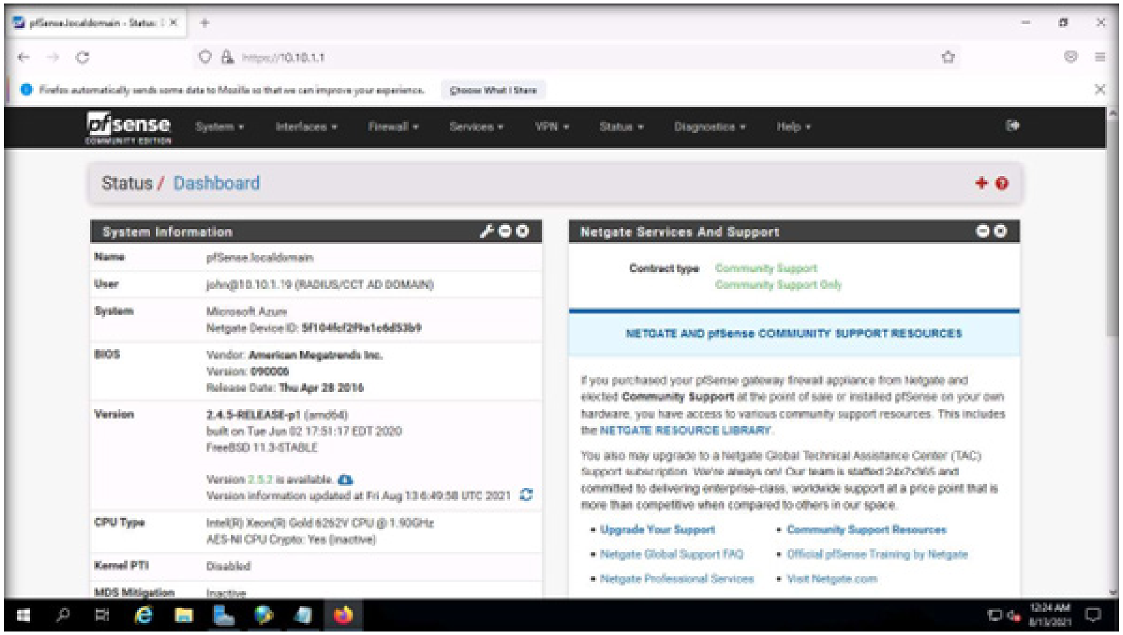
48. In the login page, enter Username and Password as john and user@123 respectively and click SIGN IN button.
Note: When, you login to the pfSense platform as a RADIUS client, the user credentials are passed to the RADIUS server (here, the AD Domain Controller machine) for verification and if the credentials match and user account is present in the Admin-Support group, then the user will be granted access to the platform.
Note: If a Save login credentials pop-up appears, click Don't Save.


pfSense - Login
https://10.10.1.1/index.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense
Login to pfSense
SIGN IN
SIGN IN

john

•••••••••

49. You will be logged into the pfsense platform with basic privileges.


pfSense.localdomain - Status: ×
https://10.10.1.1
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense COMMUNITY EDITION
System ▾
Interfaces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Help ▾
12:24 AM
8/13/2021

Status / Dashboard

System Information

Name	pfSense.localdomain
User	john@10.10.1.19 (RADIUS/CCT AD DOMAIN)
System	Microsoft Azure Netgate Device ID: **5f104fcf2f9a1c6d53b9**
BIOS	Vendor: **American Megatrends Inc.** Version: **090006** Release Date: **Thu Apr 28 2016**
Version	**2.4.5-RELEASE-p1** (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.5.2 is available. Version information updated at Fri Aug 13 6:49:58 UTC 2021
CPU Type	Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

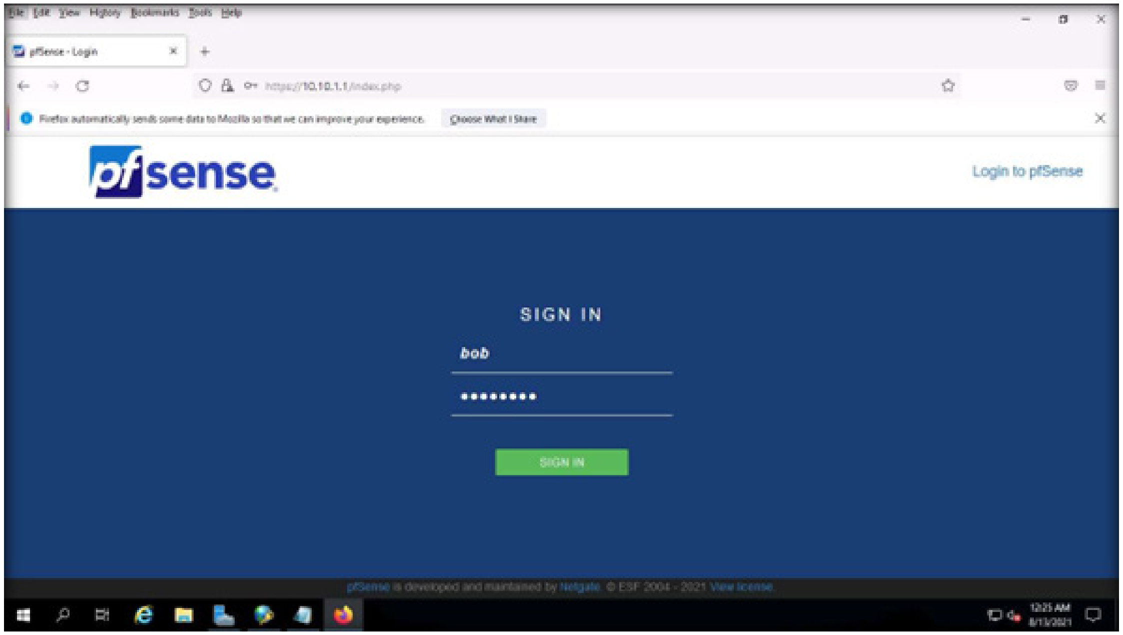
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

50. Now, we will try to login into the pfsense platform, using a user account that is not a member of Admin-Support group.

51. Click (➜) icon from the top-right corner of the dashboard to logout from the account.

52. In the login page, enter Username and Password as bob/user@123 respectively and click SIGN IN button.


File Edit View History Bookmarks Tools Help
pfSense - Login
https://10.10.1.1/index.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense
Login to pfSense
SIGN IN

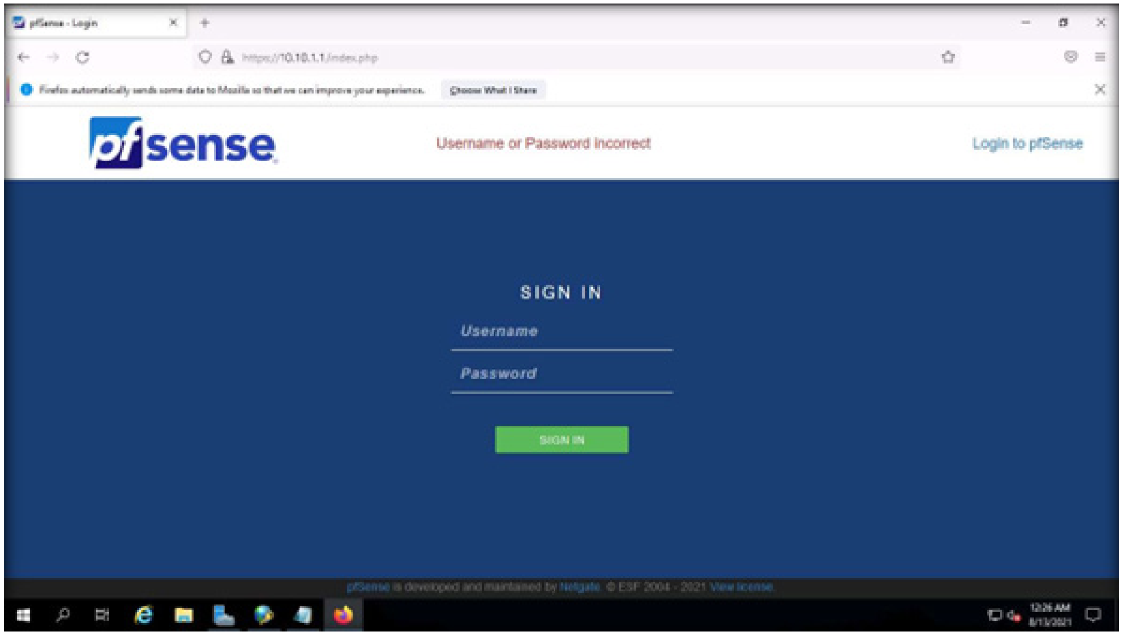
SIGN IN

bob

•••••••••

SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.
12:25 AM
8/13/2021

53. This user will not be able to login subsequently, a Username or Password incorrect notification appears, as shown in the screenshot.


pfSense - Login
https://10.10.1.1/index.php
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
pfsense
Login to pfSense
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license
12:26 AM
8/13/2021

Username or Password incorrect

54. This concludes the demonstration of implementing the centralized authentication mechanism using the AD Domain Controller as a RADIUS server and pfSense device as a RADIUS client.

55. Close all open windows.

56. Turn off AD Domain Controller and PfSense Firewall virtual machines.

EC-Council