Identification, Authentication, and Authorization

Exercise 1: Implementing Access Controls in Windows Machine

Lab Scenario

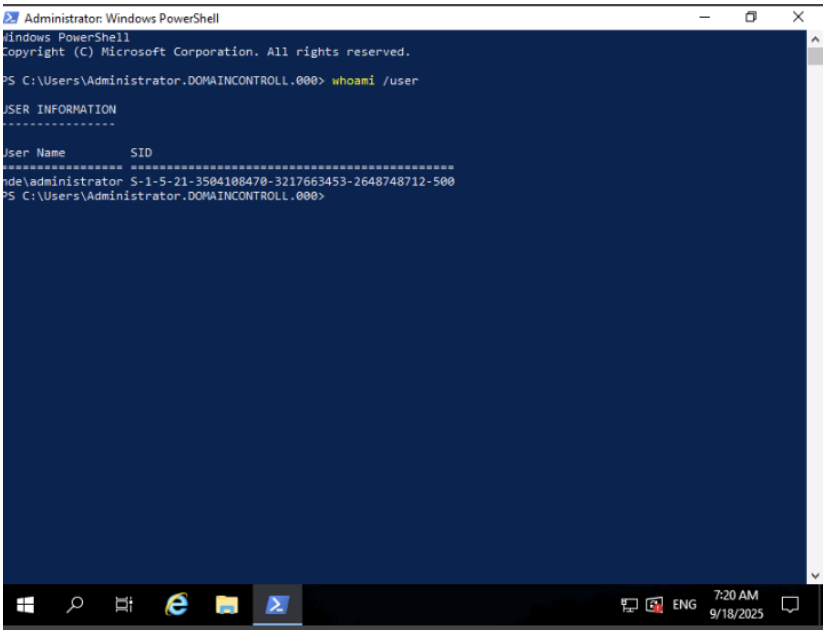
Access control is a method of limiting the access of users to an organization's resources.

Lab Objectives

This lab demonstrates how to manage objects in Active Directory using different types of accounts and how to apply account policies using GPO (Group Policy Object) in a Windows machine.

Overview of Access Control

An access control function uses identification, authentication, and mechanisms to identify, authenticate, and authorize a user requesting 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 access control is to maintain the integrity, confidentiality, and availability of the information.



Administrator: Windows PowerShell

```
----------------

User Name         SID
================= ==========================================
nde\administrator S-1-5-21-3504108470-3217663453-2648748712-500
PS C:\Users\Administrator.DOMAINCONTROLL.000> 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                        : NDE.com/Users/Administrator
Certificates                         : {}
City                                 :
CN                                   : Administrator
codePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 6/22/2021 1:34:58 AM
createTimeStamp                      : 6/22/2021 1:34:58 AM
Deleted                              :
Department                           :
Description                          : Built-in account for administering the computer/domain
DisplayName                          :
DistinguishedName                    : CN=Administrator,CN=Users,DC=NDE,DC=com
Division                             :
DoesNotRequirePreAuth                : False
```

ENG 7:21 AM 9/18/2025

New Object - Organizational Unit

Create in: NDE.com/

Name: Network Admin

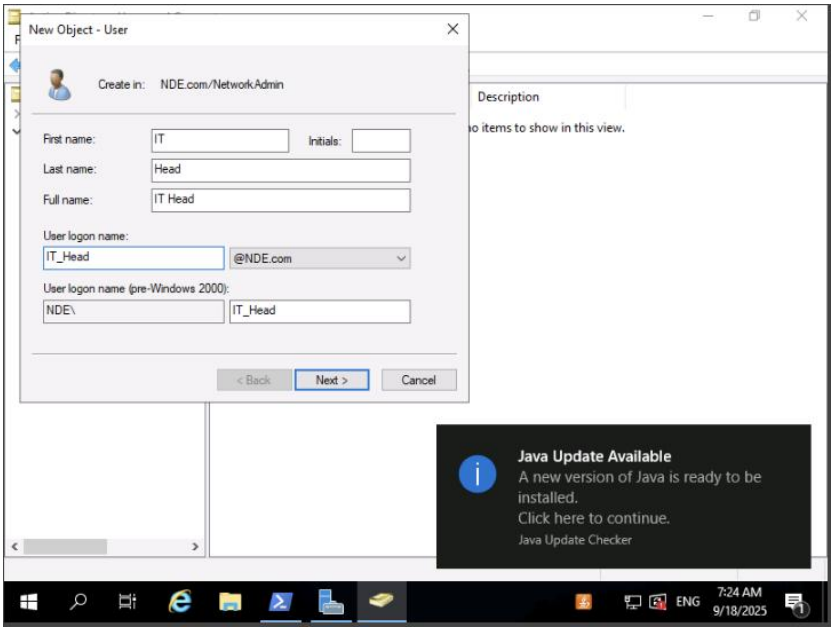
☑ Protect container from accidental deletion

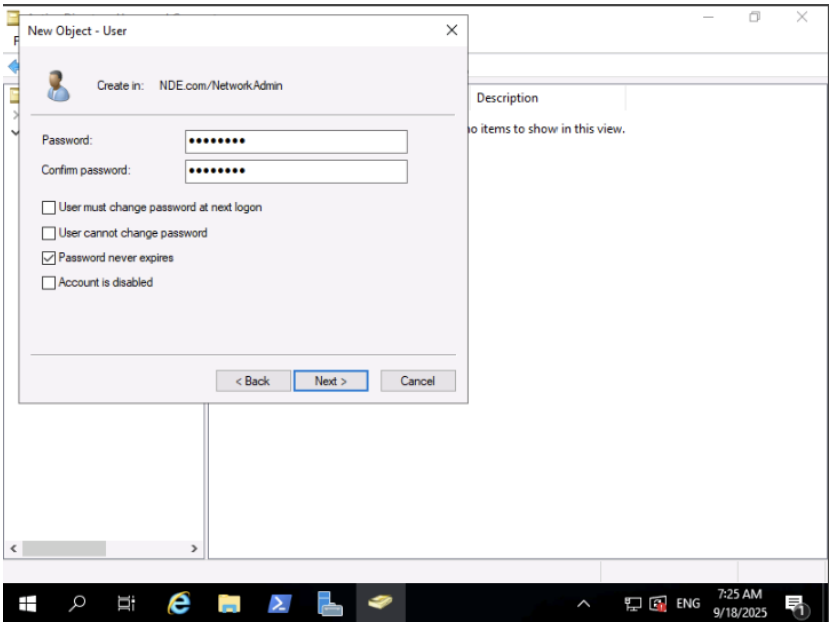
OK Cancel Help

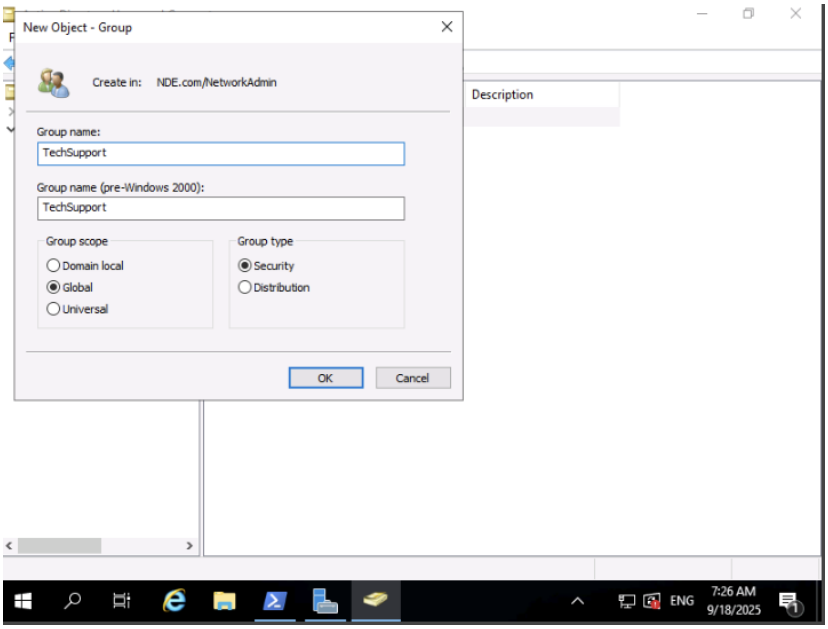
Enterprise Read-only D...	Security Group...	Members of this group ...
Group Policy Creator ...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
john j.	User	
Key Admins	Security Group...	Members of this group ...
martin S.	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...

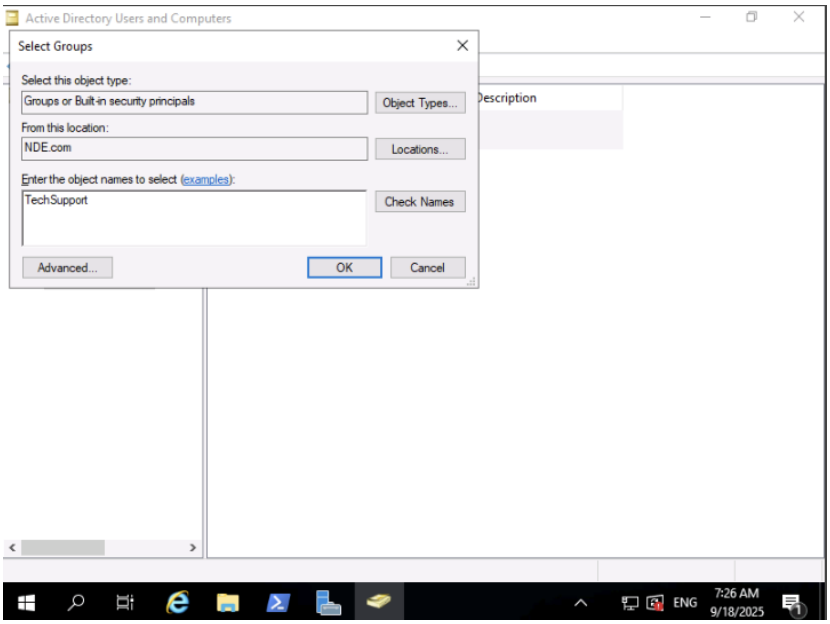
Description
Built-in account for ad...
Members in this group c...
Members of this group ...
Members of this group t...
Members in this group c...
DNS Administrators Gro...
DNS clients who are per...
Designated administrato...
All workstations and ser...
All domain controllers i...
All domain guests
All domain users
Designated administrato...
Members of this group ...
Members of this group ...
Members in this group c...
Members of this group ...
Members of this group ...

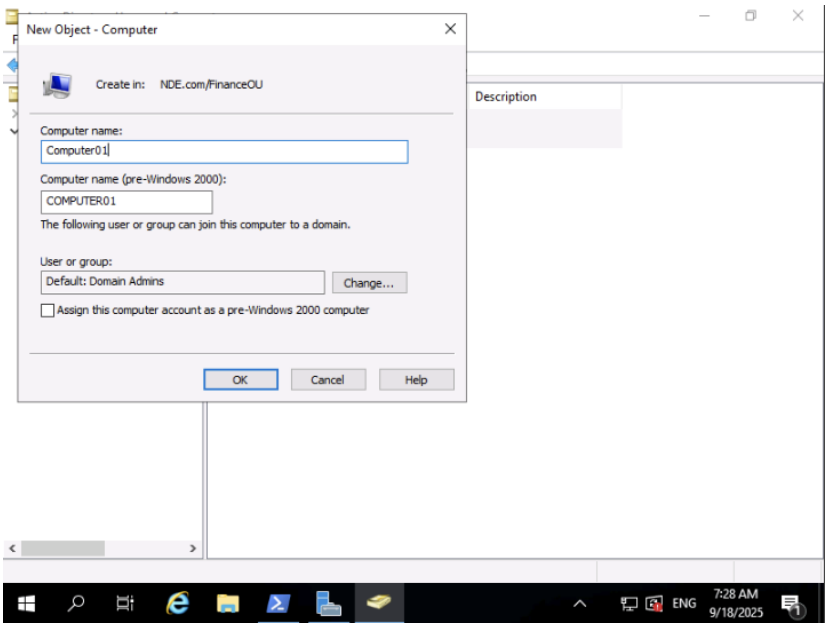
ENG 7:23 AM 9/18/2025

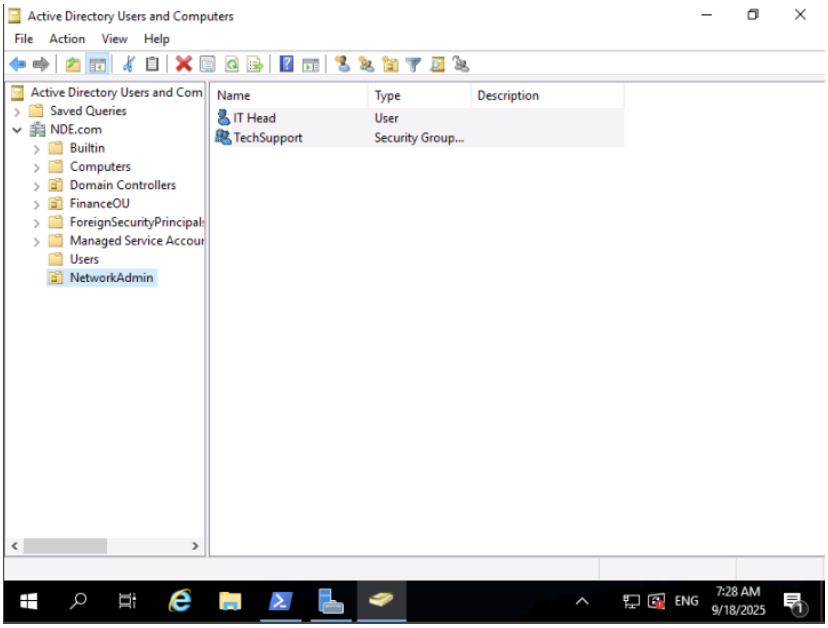

New Object - User
Create in: NDE.com/NetworkAdmin
First name: IT
Initials:
Last name: Head
Full name: IT Head
User logon name:
IT_Head
@NDE.com
User logon name (pre-Windows 2000):
NDE\
IT_Head
< Back
Next >
Cancel
Description
No items to show in this view.
Java Update Available
A new version of Java is ready to be installed.
Click here to continue.
Java Update Checker
ENG
7:24 AM
9/18/2025

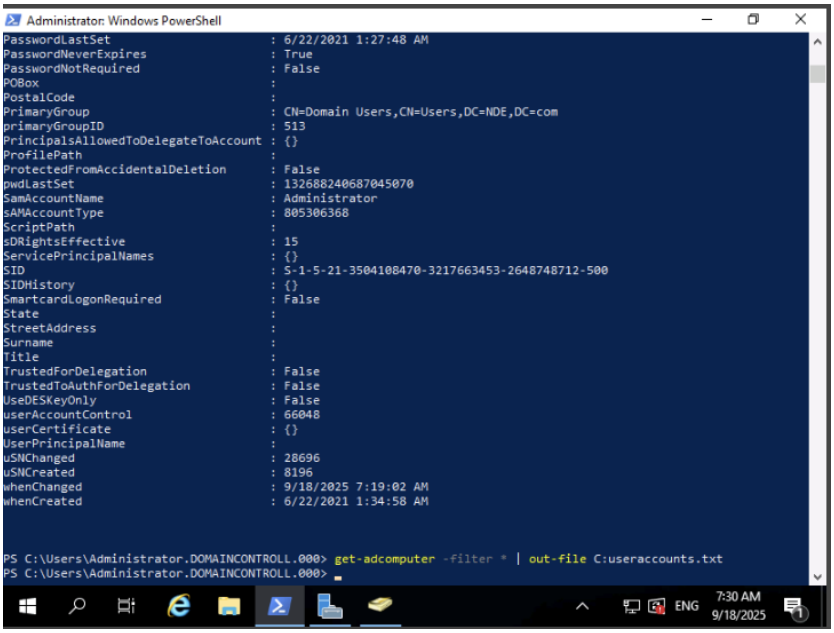

New Object - User
Create in: NDE.com/NetworkAdmin
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Description
No items to show in this view.
ENG
7:25 AM
9/18/2025

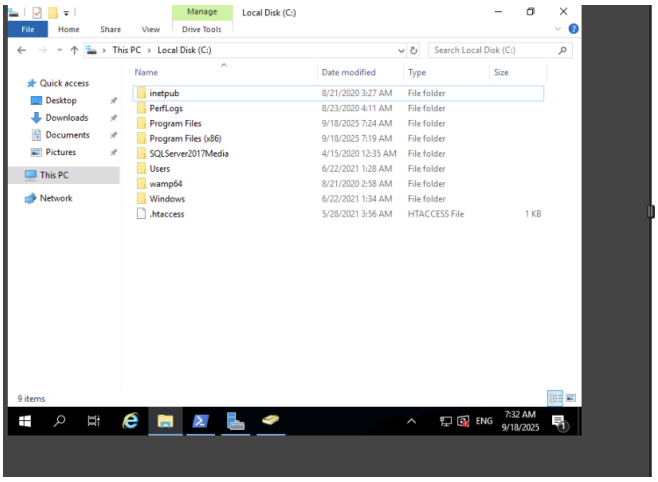

New Object - Group
Create in: NDE.com/NetworkAdmin
Group name:
TechSupport
Group name (pre-Windows 2000):
TechSupport
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel
Description
ENG
7:26 AM
9/18/2025

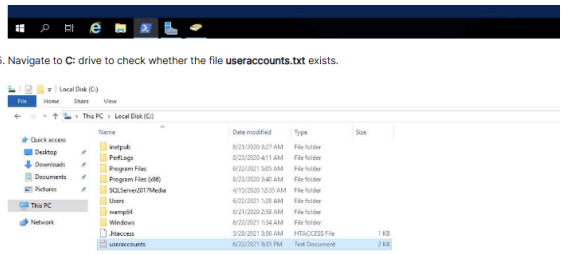

Active Directory Users and Computers
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
NDE.com
Locations...
Enter the object names to select (examples):
TechSupport
Check Names
Advanced...
OK
Cancel
Description
ENG
7:26 AM
9/18/2025


New Object - Computer
Create in: NDE.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
Change...
Assign this computer account as a pre-Windows 2000 computer
OK
Cancel
Help
Description
ENG
7:28 AM
9/18/2025


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
NDE.com
Builtin
Computers
Domain Controllers
FinanceOU
ForeignSecurityPrincipal
Managed Service Accour
Users
NetworkAdmin
Name
Type
Description
IT Head
User
TechSupport
Security Group...
ENG
7:28 AM
9/18/2025







25. Navigate to **C:** drive to check whether the file **useraccounts.txt** exists.

Administrator: Windows PowerShell

```
PasswordNeverExpires                : True
PasswordNotRequired                 : False
POBox                               :
PostalCode                          :
PrimaryGroup                        : CN=Domain Users,CN=Users,DC=NDE,DC=com
primaryGroupID                      : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                         :
ProtectedFromAccidentalDeletion     : False
pwdLastSet                          : 132688240687045070
SamAccountName                      : Administrator
sAMAccountType                      : 805306368
ScriptPath                          :
sDRightsEffective                   : 15
servicePrincipalNames               : {}
SID                                 : S-1-5-21-3504108470-3217663453-2648748712-500
SIDHistory                          : {}
SmartcardLogonRequired              : False
State                               :
StreetAddress                       :
Surname                             :
Title                               :
TrustedForDelegation                : False
TrustedToAuthForDelegation          : False
UseDESKeyOnly                       : False
userAccountControl                  : 66048
userCertificate                     : {}
UserPrincipalName                   :
uSNChanged                          : 28696
uSNCreated                          : 8196
whenChanged                         : 9/18/2025 7:19:02 AM
whenCreated                         : 6/22/2021 1:34:58 AM


PS C:\Users\Administrator.DOMAINCONTROLL.000> get-adcomputer -filter * | out-file C:useraccounts.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000> Get-ADUser -Filter * | Out-file C:\useraccount.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000>
```

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	9/18/2025 7:24 AM	File folder	
Program Files (x86)	9/18/2025 7:19 AM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
Users	6/22/2021 1:28 AM	File folder	
wamp64	8/21/2020 2:58 AM	File folder	
Windows	6/22/2021 1:34 AM	File folder	
.htaccess	5/28/2021 3:56 AM	HTACCESS File	1 KB
useraccount	9/18/2025 7:33 AM	Text Document	6 KB

Active Directory Users and Computers

10 items

useraccount - Notepad

File Edit Format View Help

```
DistinguishedName : CN=Administrator,CN=Users,DC=NDE,DC=com
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 4db6046e-131d-490e-9940-5bb5079c59fa
SamAccountName    : Administrator
SID               : S-1-5-21-3504108470-3217663453-2648748712-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=NDE,DC=com
Enabled           : False
GivenName         :
Name              : Guest
ObjectClass       : user
ObjectGUID        : 73fe7c54-c12f-4f9f-9c01-8a21fb92368d
SamAccountName    : Guest
SID               : S-1-5-21-3504108470-3217663453-2648748712-501
Surname           :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=NDE,DC=com
Enabled           : False
```

Windows (CRLF) | Ln 1, Col 1 | 100%

ENG 7:35 AM 9/18/2025

Administrator: Windows PowerShell

Group Policy Management

File Action View Window Help

- Group Policy Management
  - Forest: NDE.com
    - Domains
      - NDE.com
        - Default Domain Policy
        - Domain Controllers
        - FinanceOU
        - NetworkAdmin
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

Default Domain Policy

Scope | Details | Settings | Delegation

Links

Display links in this location: NDE.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
NDE.com	No	Yes	NDE.com

Security Filtering

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

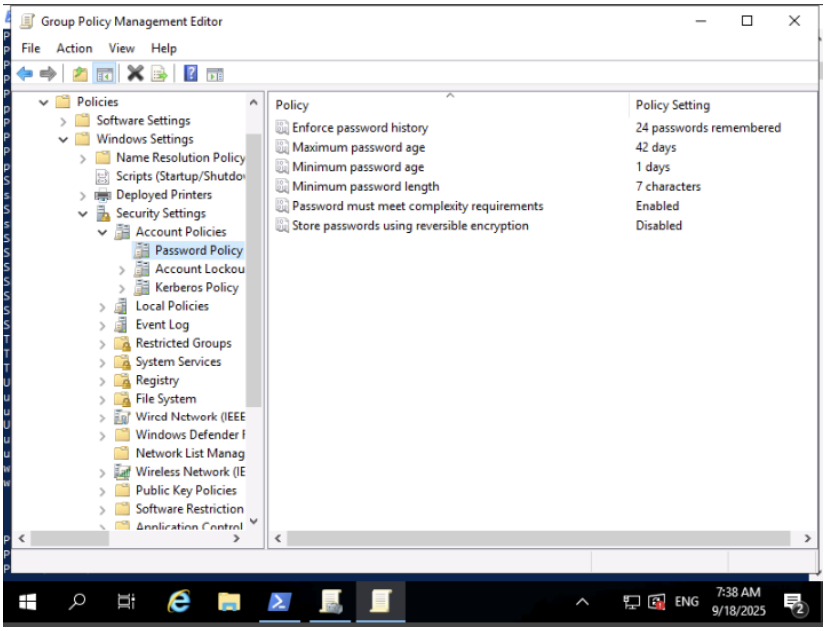
Name
Authenticated Users

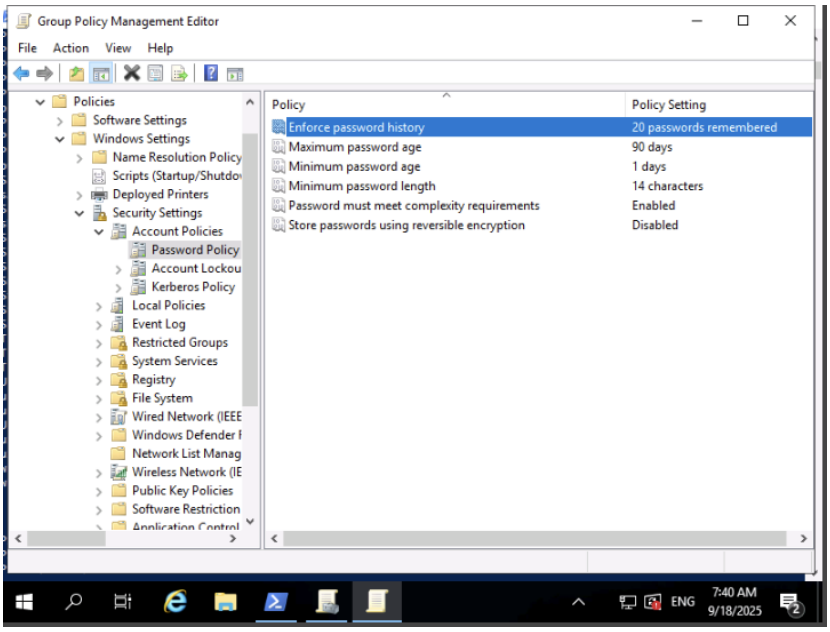
Add... Remove Properties

WMI Filtering

This GPO is linked to the following WMI filter:

ENG 7:37 AM 9/18/2025


Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdo
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockou
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Defender F
Network List Manag
Wireless Network (IE
Public Key Policies
Software Restriction
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
ENG
7:38 AM
9/18/2025


Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdo
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockou
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Defender F
Network List Manag
Wireless Network (IE
Public Key Policies
Software Restriction
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
ENG
7:40 AM
9/18/2025

Administrator: Windows PowerShell

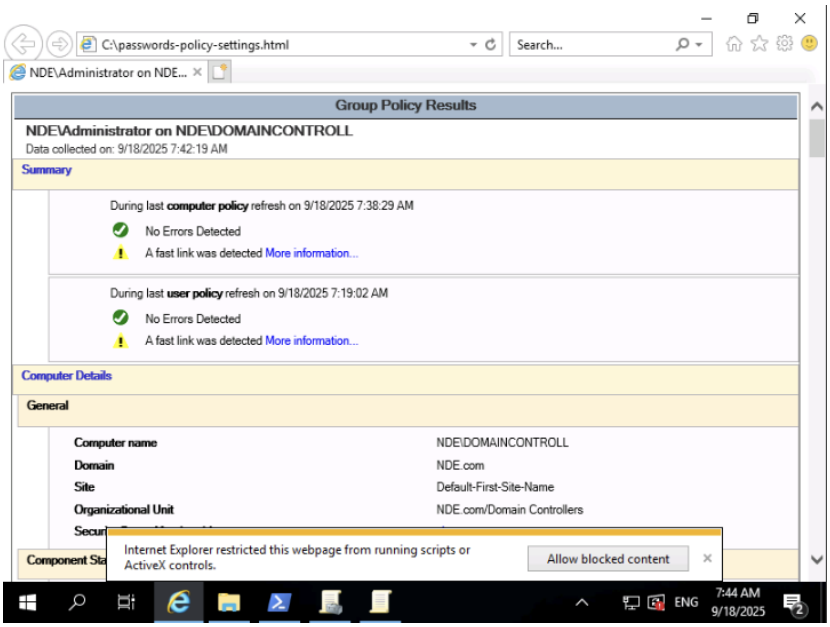
```
PasswordNotRequired                 : False
POBox                               :
PostalCode                          :
PrimaryGroup                        : CN=Domain Users,CN=Users,DC=NDE,DC=com
primaryGroupID                      : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                         :
ProtectedFromAccidentalDeletion     : False
pwdLastSet                          : 132688240687045070
SamAccountName                      : Administrator
sAMAccountType                      : 805306368
ScriptPath                          :
sDRightsEffective                   : 15
ServicePrincipalNames               : {}
SID                                 : S-1-5-21-3504108470-3217663453-2648748712-500
SIDHistory                          : {}
SmartcardLogonRequired              : False
State                               :
StreetAddress                       :
Surname                             :
Title                               :
TrustedForDelegation                : False
TrustedToAuthForDelegation          : False
UseDESKeyOnly                       : False
userAccountControl                  : 66048
userCertificate                     : {}
UserPrincipalName                   :
uSNChanged                          : 28696
uSNCreated                          : 8196
whenChanged                         : 9/18/2025 7:19:02 AM
whenCreated                         : 6/22/2021 1:34:58 AM


PS C:\Users\Administrator.DOMAINCONTROLL.000> get-adcomputer -filter * | out-file C:useraccounts.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000> Get-ADUser -Filter * | Out-file C:\useraccount.txt
PS C:\Users\Administrator.DOMAINCONTROLL.000> gpresult /H C:\passwords-policy-settings.html
PS C:\Users\Administrator.DOMAINCONTROLL.000>
```

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	9/18/2025 7:24 AM	File folder	
Program Files (x86)	9/18/2025 7:19 AM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
Users	6/22/2021 1:28 AM	File folder	
wamp64	8/21/2020 2:58 AM	File folder	
Windows	6/22/2021 1:34 AM	File folder	
.htaccess	5/28/2021 3:56 AM	HTACCESS File	1 KB
passwords-policy-settings	9/18/2025 7:42 AM	HTML Document	486 KB
useraccount	9/18/2025 7:33 AM	Text Document	6 KB

11 items



Exercise 2: Managing Access Controls in Linux Machine

Lab Scenario

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

Lab Objectives

This lab demonstrates how to manage access control policies in a Linux machine. First, we will create local user accounts and groups on the 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.

Overview of Access Control

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

```
root@bob-Virtual-Machine: /home/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 testuser01
useradd: user 'testuser01' already exists
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# team

Command 'team' not found, did you mean:

  command 'steam' from snap steam (1.0.0.81)
  command 'tea' from deb tea (47.1.0-1build1)
  command 'teamd' from deb libteam-utils (1.30-1)

See 'snap info <snapname>' for additional versions.

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

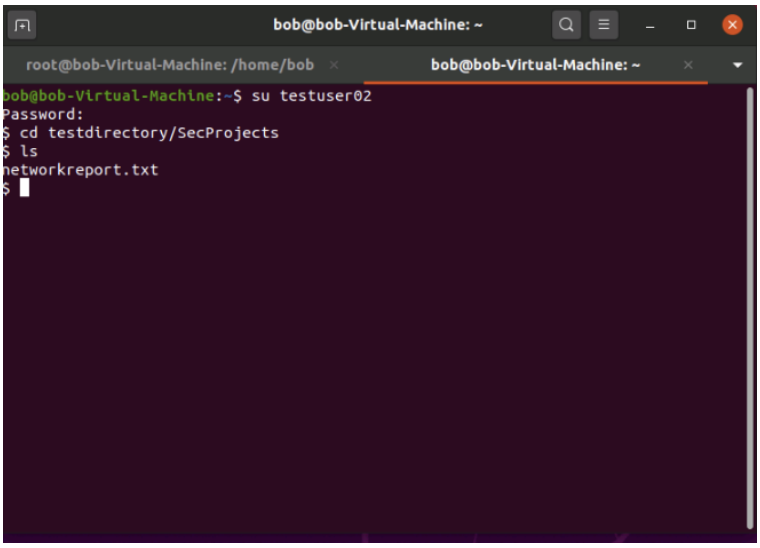
```
root@bob-Virtual-Machine: /home/bob
root@bob-Virtual-Machine:/home/bob# passwd testuser02
New password:
Retype new password:
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# team

Command 'team' not found, did you mean:

  command 'steam' from snap steam (1.0.0.81)
  command 'tea' from deb tea (47.1.0-1build1)
  command 'teamd' from deb libteam-utils (1.30-1)

See 'snap info <snapname>' for additional versions.

root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser02
root@bob-Virtual-Machine:/home/bob# iduser01
iduser01: command not found
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),1003(admin)
root@bob-Virtual-Machine:/home/bob#
```

```
root@bob-Virtual-Machine: /home/bob
passwd: password updated successfully
root@bob-Virtual-Machine:/home/bob# groupadd admin
root@bob-Virtual-Machine:/home/bob# team

Command 'team' not found, did you mean:

  command 'steam' from snap steam (1.0.0.81)
  command 'tea' from deb tea (47.1.0-1build1)
  command 'teamd' from deb libteam-utils (1.30-1)

See 'snap info <snapname>' for additional versions.

root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser02
root@bob-Virtual-Machine:/home/bob# iduser01
iduser01: command not found
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),1003(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#
```

```
root@bob-Virtual-Machine: /home/bob
Command 'team' not found, did you mean:

  command 'steam' from snap steam (1.0.0.81)
  command 'tea' from deb tea (47.1.0-1build1)
  command 'teamd' from deb libteam-utils (1.30-1)

See 'snap info <snapname>' for additional versions.

root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser02
root@bob-Virtual-Machine:/home/bob# iduser01
iduser01: command not found
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),1003(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/networkrepor
t.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.
txt
root@bob-Virtual-Machine:/home/bob#
```

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

root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser01
root@bob-Virtual-Machine:/home/bob# usermod -aG admin testuser02
root@bob-Virtual-Machine:/home/bob# iduser01
iduser01: command not found
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),1003(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/networkrepor
t.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.
txt
root@bob-Virtual-Machine:/home/bob# ls -id testdirectory
4327575 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecP
rojects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamP
rojects
chown: invalid group: ‘testuser02:team’
root@bob-Virtual-Machine:/home/bob#
```

```
root@bob-Virtual-Machine: /home/bob
uid=1002(testuser02) gid=1002(testuser02) groups=1002(testuser02),1003(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/networkrepor
t.txt
root@bob-Virtual-Machine:/home/bob# touch testdirectory/TeamProjects/workreport.
txt
root@bob-Virtual-Machine:/home/bob# ls -id testdirectory
4327575 testdirectory
root@bob-Virtual-Machine:/home/bob# chown -R testuser01:admin testdirectory/SecP
rojects
root@bob-Virtual-Machine:/home/bob# chown -R testuser02:team testdirectory/TeamP
rojects
chown: invalid group: ‘testuser02:team’
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/SecProjects
drwxr-xr-x 2 testuser01 admin 4096 Sep 19 07:54 testdirectory/SecProjects
root@bob-Virtual-Machine:/home/bob# ls -ld testdirectory/TeamProjects
drwxr-xr-x 2 root root 4096 Sep 19 07:55 testdirectory/TeamProjects
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o-r testdirectory/SecProje
cts
root@bob-Virtual-Machine:/home/bob# chmod u=rwx,g=rwx,o=rx testdirectory/TeamPro
jects
root@bob-Virtual-Machine:/home/bob#
```



Exercise 3: Implementing 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 the network.

Lab Scenario

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

Lab Objectives

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

Overview of WAC

The Windows Admin Center (WAC) is a web-based administration tool used to manage server and client operating systems, hyper-converged clusters, and failover clusters. Some of the features of WAC are listed below:

- Device management
- Windows event management

- File management
- Firewall management
- Local users and groups management
- Network management
- PowerShell tool
- Process tool
- Registry tool
- Remote desktop
- Role and features
- Services, storage, updates, etc.

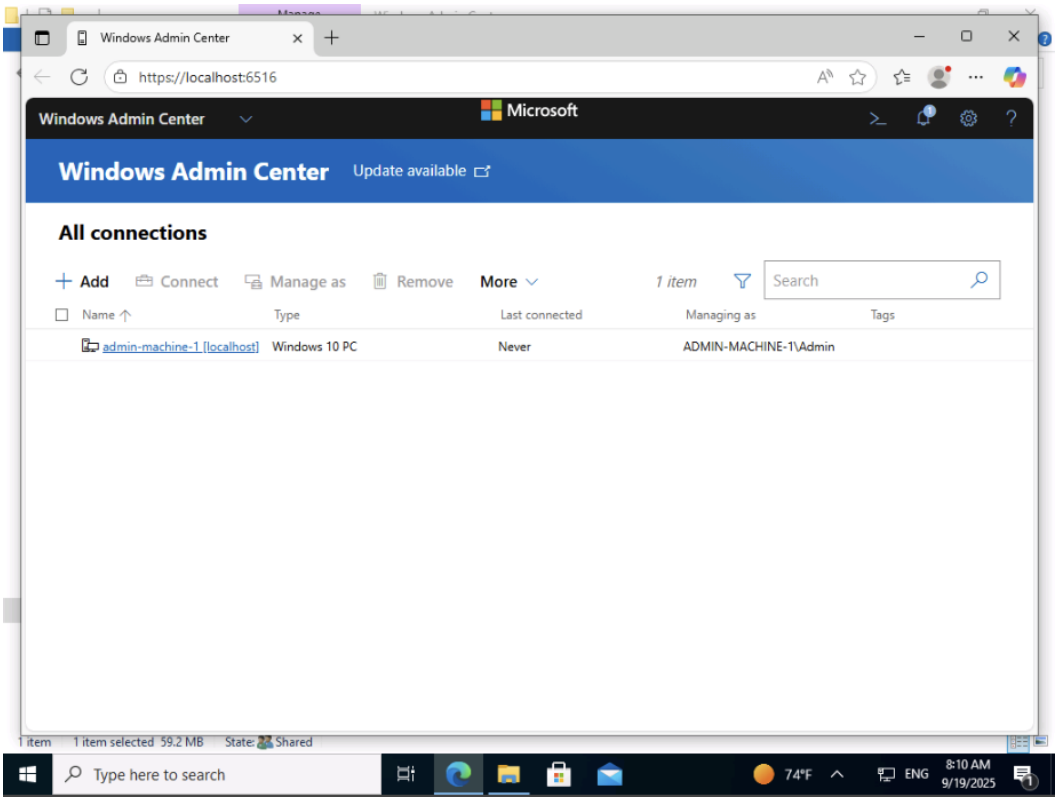
In WAC, RBAC provides limited access to users on the target computers. RBAC in WAC works by configuring every managed server with a PowerShell Just-Enough Administration endpoint. The roles are defined by the endpoint. After connecting to the restricted endpoint, a temporary local administrator account is created for managing the machine. If the user is not managing the machine utilizing WAC, then the temporary account will be automatically deleted. When the user connects to the system with the configured RBAC, the WAC will initially check whether or not the user is a local administrator. If the user is a local administrator, then the user can access WAC without restrictions; otherwise, WAC will check whether the user is assigned to any predefined roles. The user will get limited access to the system if the user belongs to a WAC role but is not a full administrator. If the user is not an administrator or a member of a role, then the user will not get access to the machine.

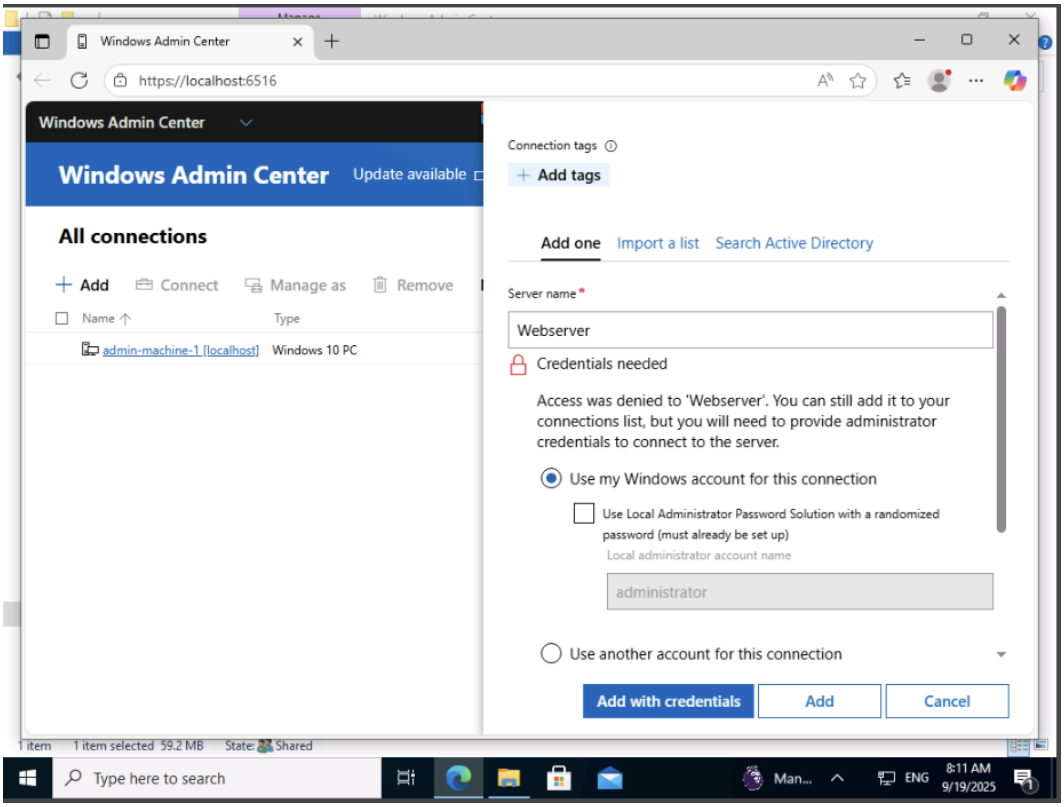
WAC supports the following built-in roles.

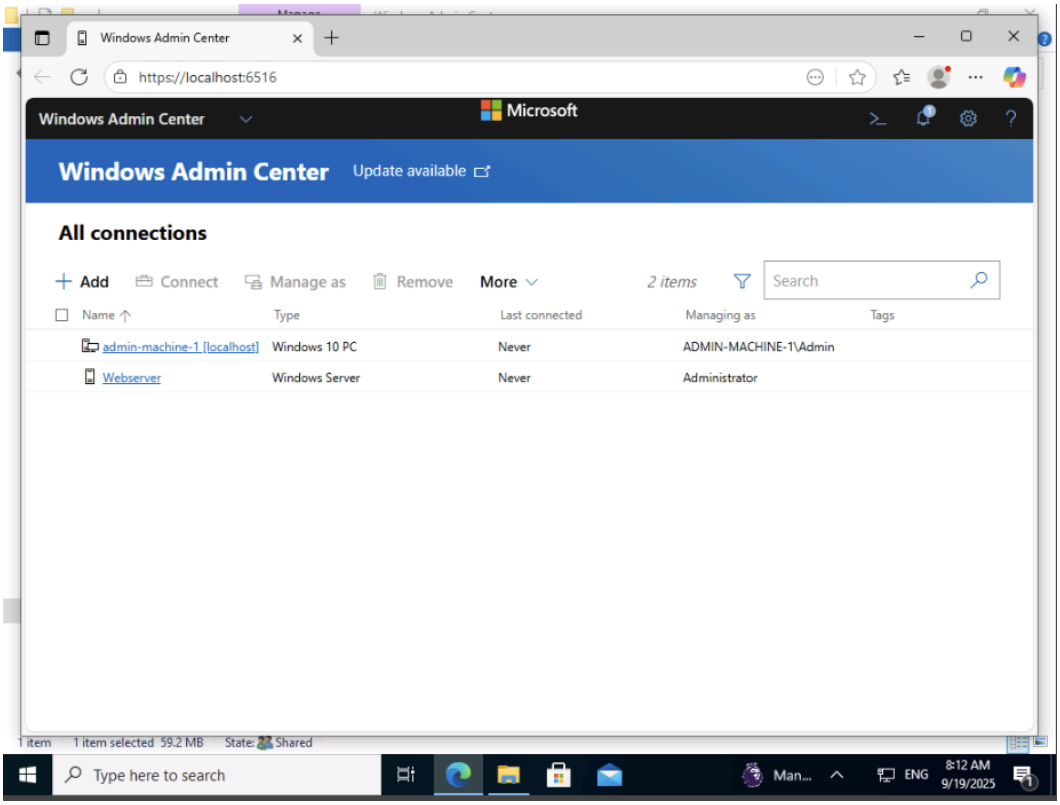
Administrators: Allows users to use most WAC features without granting them access to Remote Desktop or PowerShell.

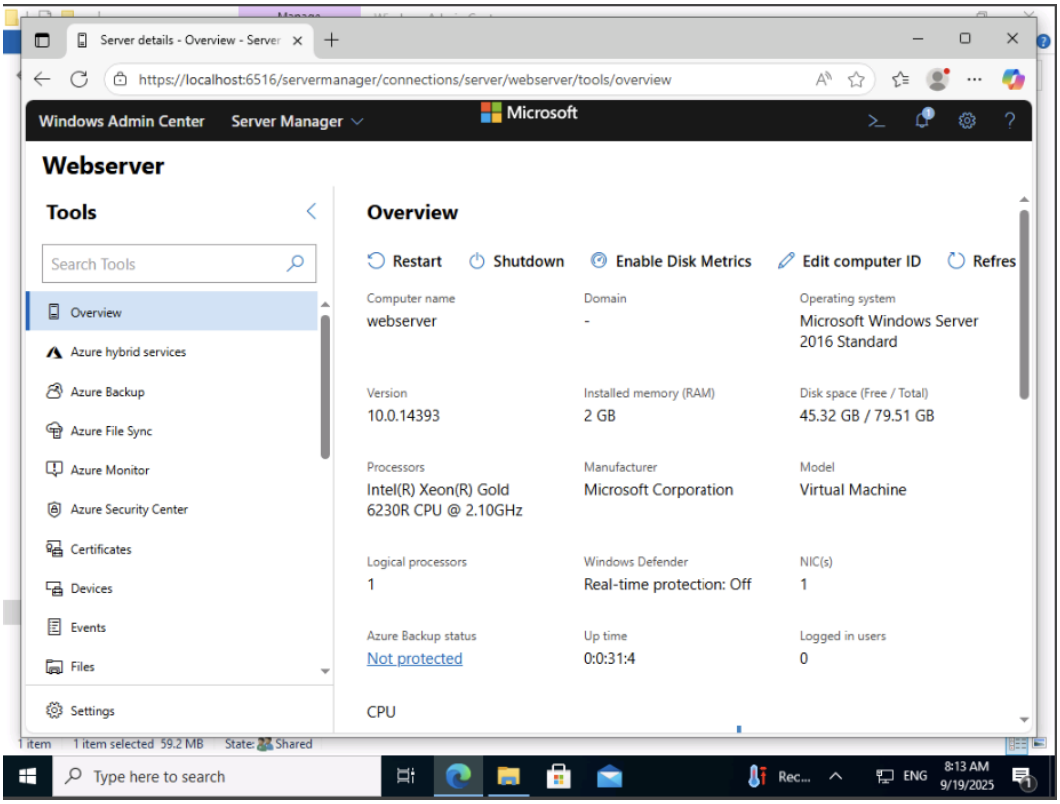
Readers: Allows users to view information and settings on the server, but not make changes.

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


Windows Admin Center
https://localhost:6516
Windows Admin Center
Microsoft
Windows Admin Center
Update available
All connections
Add
Connect
Manage as
Remove
More
1 item
Search
Name
Type
Last connected
Managing as
Tags
admin-machine-1 [localhost]
Windows 10 PC
Never
ADMIN-MACHINE-1\Admin
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
74°F
ENG
8:10 AM
9/19/2025


Windows Admin Center
https://localhost:6516
Windows Admin Center
Windows Admin Center
Update available
All connections
Add
Connect
Manage as
Remove
Name
Type
admin-machine-1 [localhost]
Windows 10 PC
Connection tags
Add tags
Add one
Import a list
Search Active Directory
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
Add with credentials
Add
Cancel
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
Man...
ENG
8:11 AM
9/19/2025


Windows Admin Center
https://localhost:6516
Windows Admin Center
Microsoft
Windows Admin Center
Update available
All connections
Add
Connect
Manage as
Remove
More
2 items
Search
Name
Type
Last connected
Managing as
Tags
admin-machine-1 [localhost]
Windows 10 PC
Never
ADMIN-MACHINE-1\Admin
Webserver
Windows Server
Never
Administrator
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
Man...
ENG
8:12 AM
9/19/2025


Server details - Overview - Server
https://localhost:6516/servermanager/connections/server/webserver/tools/overview
Windows Admin Center
Server Manager
Microsoft
Webserver
Tools
Search Tools
Overview
Azure hybrid services
Azure Backup
Azure File Sync
Azure Monitor
Azure Security Center
Certificates
Devices
Events
Files
Settings
Overview
Restart
Shutdown
Enable Disk Metrics
Edit computer ID
Refres
Computer name
webserver
Domain
-
Operating system
Microsoft Windows Server 2016 Standard
Version
10.0.14393
Installed memory (RAM)
2 GB
Disk space (Free / Total)
45.32 GB / 79.51 GB
Processors
Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
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
0:0:31:4
Logged in users
0
CPU
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
Rec...
ENG
8:13 AM
9/19/2025

Role-based Access Control - Setti

https://localhost:6516/servermanager/connections/server/webserver/tools/settings/rbacSettings

Windows Admin Center Server Manager Microsoft

Webserver

Tools

Search Tools

- Overview
- Azure hybrid services
- Azure Backup
- Azure File Sync
- Azure Monitor
- Azure Security Center
- Certificates
- Devices
- Events
- Files
- Settings

Settings

General

- Environment variables
- Azure Arc for Servers
- Power configuration
- Remote Desktop
- Role-based Access Control

Successfully scheduled the application of RBAC
Successfully scheduled the application of role-based access control. This can take up to 10 minutes to apply—check it...
webserver 8:16:16 AM

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.

Apply Remove

1 item 1 item selected 59.2 MB State: Shared

Type here to search Result ENG 8:16 AM 9/19/2025

Role-based Access Control - Setti

https://localhost:6516/servermanager/connections/server/webserver/tools/settings/rbacSettings

Windows Admin Center Server Manager Microsoft Notifications

Webserver

Tools

Search Tools

- Azure Security Center
- Certificates
- Devices
- Events
- Files
- Firewall
- Installed apps
- Local users & groups
- Networks
- Performance Monitor
- Settings

Settings

General

- Environment variables
- Azure Arc for Servers
- Power configuration
- Remote Desktop
- Role-based Access Control

Role-based access control

Role-based access control: **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.

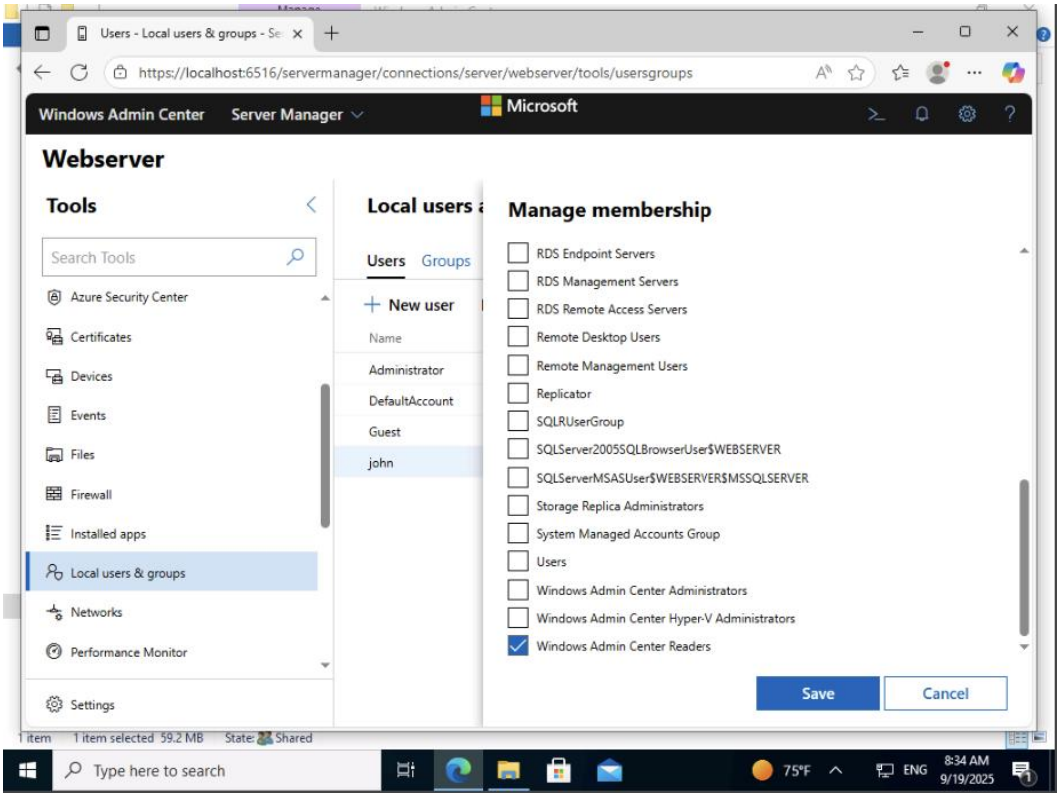
Windows Admin Center Hyper-V-Administrators
Allows users to manage Hyper-V virtual machines and switches. Other tools are available in read-only mode.

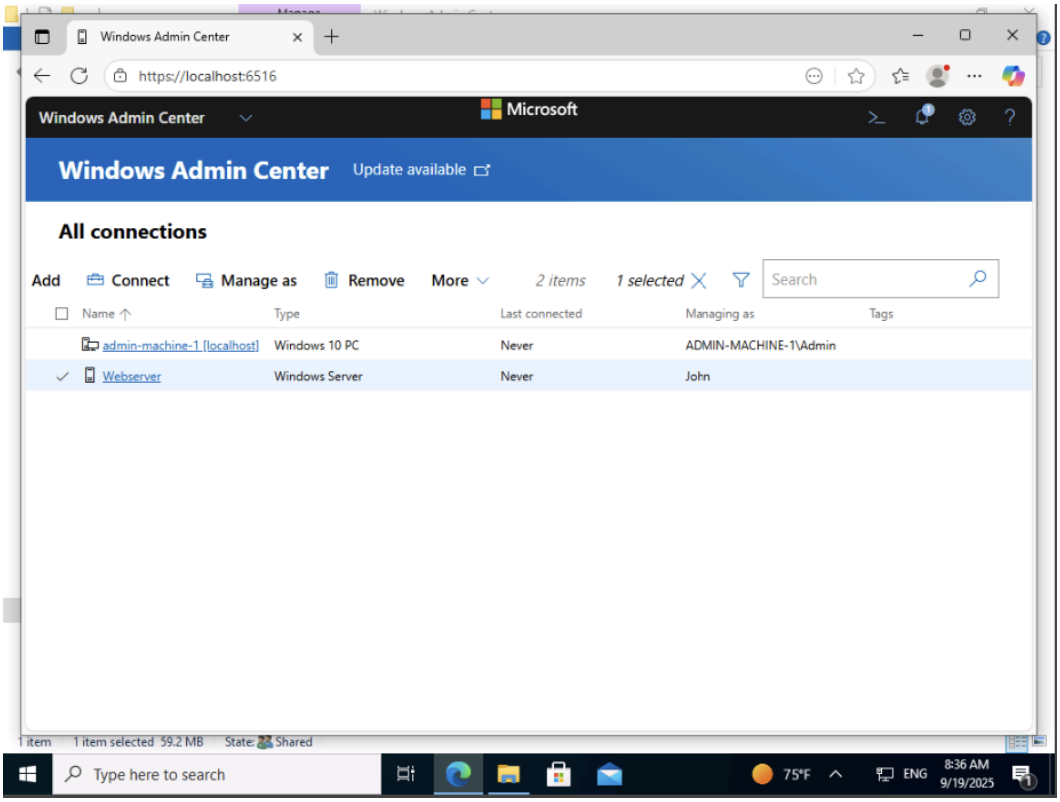
Windows Admin Center Readers
Allows users to view most tools, but doesn't allow them to make any changes.

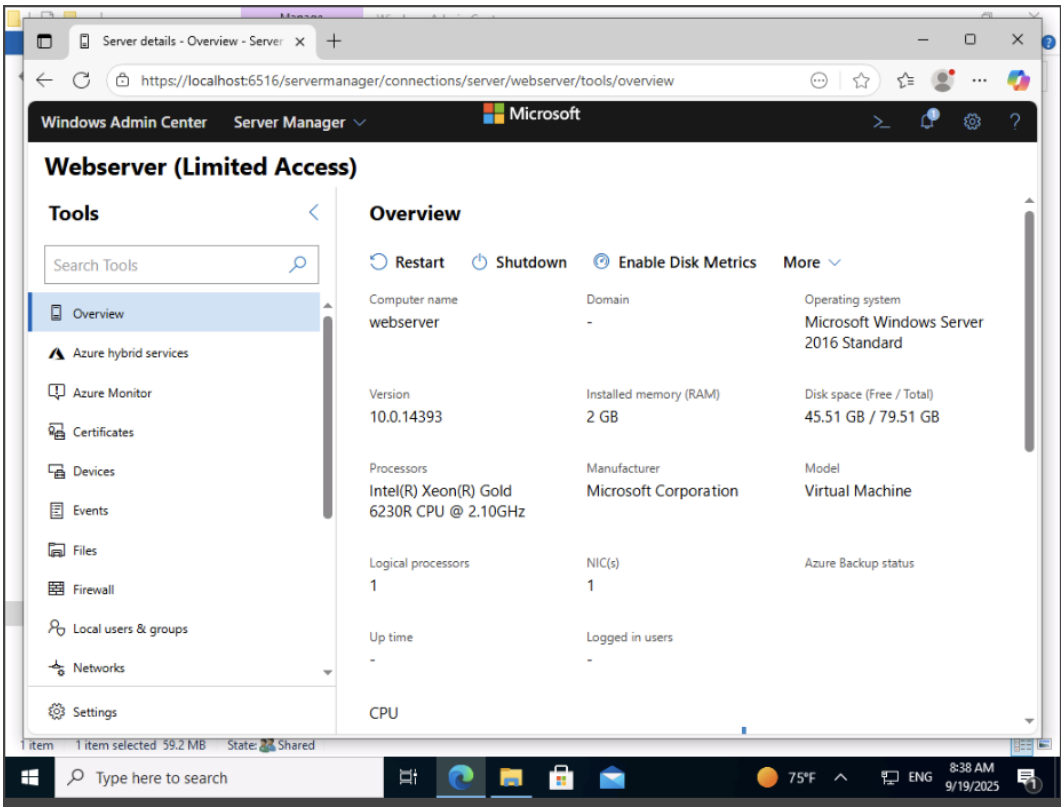
To assign users to roles, first select 'Apply' to enable the feature and create the appropriate groups (this can take up to 10 minutes – check here for updates). Then add the users to the corresponding group in

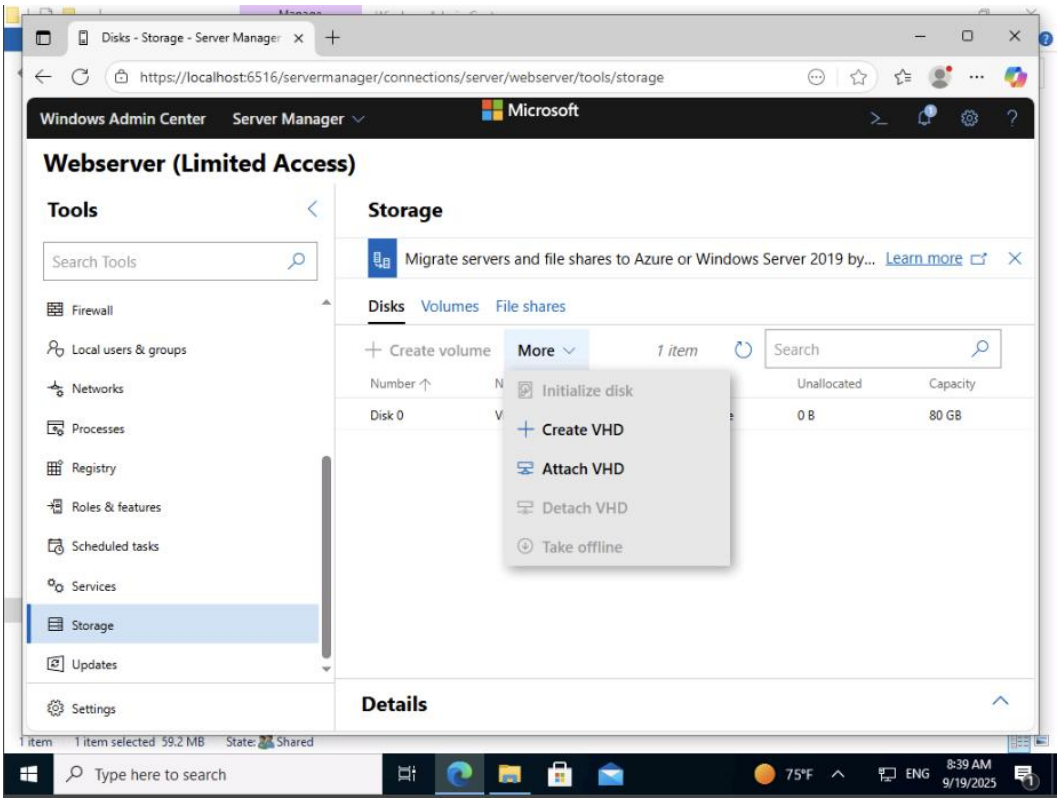
1 item 1 item selected 59.2 MB State: Shared

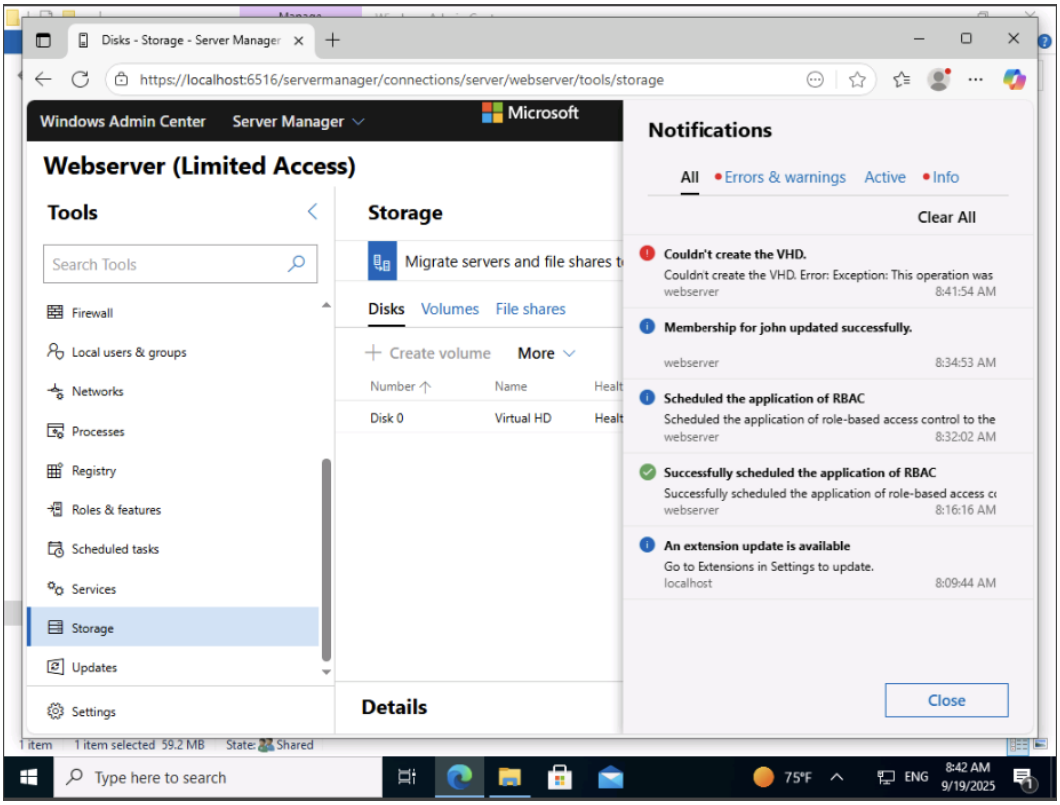
Type here to search 75°F ENG 8:32 AM 9/19/2025


Users - Local users & groups - Se
https://localhost:6516/servermanager/connections/server/webserver/tools/usersgroups
Windows Admin Center
Server Manager
Microsoft
Webserver
Tools
Search Tools
Azure Security Center
Certificates
Devices
Events
Files
Firewall
Installed apps
Local users & groups
Networks
Performance Monitor
Settings
Local users a
Users
Groups
New user
Name
Administrator
DefaultAccount
Guest
john
Manage membership
RDS Endpoint Servers
RDS Management Servers
RDS Remote Access Servers
Remote Desktop Users
Remote Management Users
Replicator
SQLRUserGroup
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
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
75°F
ENG
8:34 AM
9/19/2025


Windows Admin Center
https://localhost:6516
Windows Admin Center
Microsoft
Windows Admin Center
Update available
All connections
Add
Connect
Manage as
Remove
More
2 items
1 selected
Search
Name
Type
Last connected
Managing as
Tags
admin-machine-1 [localhost]
Windows 10 PC
Never
ADMIN-MACHINE-1\Admin
Webserver
Windows Server
Never
John
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
75°F
ENG
8:36 AM
9/19/2025


Server details - Overview - Server
https://localhost:6516/servermanager/connections/server/webserver/tools/overview
Windows Admin Center
Server Manager
Microsoft
Webserver (Limited Access)
Tools
Search Tools
Overview
Azure hybrid services
Azure Monitor
Certificates
Devices
Events
Files
Firewall
Local users & groups
Networks
Settings
Overview
Restart
Shutdown
Enable Disk Metrics
More
Computer name
webserver
Domain
-
Operating system
Microsoft Windows Server 2016 Standard
Version
10.0.14393
Installed memory (RAM)
2 GB
Disk space (Free / Total)
45.51 GB / 79.51 GB
Processors
Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
Manufacturer
Microsoft Corporation
Model
Virtual Machine
Logical processors
1
NIC(s)
1
Azure Backup status
Up time
-
Logged in users
-
CPU
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
75°F
ENG
8:38 AM
9/19/2025


Disks - Storage - Server Manager
https://localhost:6516/servermanager/connections/server/webserver/tools/storage
Windows Admin Center
Server Manager
Microsoft
Webserver (Limited Access)
Tools
Search Tools
Firewall
Local users & groups
Networks
Processes
Registry
Roles & features
Scheduled tasks
Services
Storage
Updates
Settings
Storage
Migrate servers and file shares to Azure or Windows Server 2019 by...
Learn more
Disks
Volumes
File shares
Create volume
More
1 item
Search
Number
Unallocated
Capacity
Disk 0
0 B
80 GB
Initialize disk
Create VHD
Attach VHD
Detach VHD
Take offline
Details
1 item
1 item selected 59.2 MB
State: Shared
Type here to search
75°F
ENG
8:39 AM
9/19/2025



Lab Summary: Identification, Authentication, and Authorization

Exercise 1: Implementing Access Controls in Windows Machine

This exercise demonstrated how to manage objects in Active Directory using different types of accounts and how to apply account policies through Group Policy Objects (GPO). Access control was implemented by configuring user properties and security identifiers within Active Directory. A PowerShell command was used to extract account data into a text file, but the file did not appear in the C:\ drive as expected, highlighting a potential command mismatch (Get-ADComputer instead of Get-ADUser). This step showed the importance of using correct filters and verifying output when applying access controls.

Exercise 2: Managing Access Controls in Linux Machine

This exercise focused on managing access control policies within a Linux environment. Local user accounts and groups were created, and ownership permissions were configured for directories and files. Access control lists (ACLs) were applied to enforce user-specific restrictions. This demonstrated how Linux uses user/group ownership and permission bits to enforce integrity, confidentiality, and availability of resources.

Exercise 3: Implementing Role-Based Access Control in Windows Admin Center (WAC)

In this exercise, the Windows Admin Center (WAC) was installed and configured to demonstrate role-based access control (RBAC). WAC's web-based interface allowed administrative tasks such as device management, firewall configuration, and user/group management. RBAC roles (Administrators, Readers, Hyper-V Administrators) were applied to limit access based on user privileges. The lab highlighted how RBAC in WAC uses PowerShell Just Enough Administration (JEA) endpoints to restrict non-administrator accounts, creating temporary local administrator accounts when necessary. This reinforced the principle of granting the least privilege required to perform specific tasks.