Windows Server 2016 – Project II

Download, create, and install Windows 10 VM.

A) Open this link and download the Windows 10 installation ISO file

https://ln2.sync.com/dl/f6ef7b730/kxad32z9-ifb8xftm-i4zac6eq-hgt3r449/view/default/9300482330007

B) In VirtualBox, create a new VM called: "Win10"

then apply the following specs:

- Attach the Windows ISO you downloaded.
- 4 GB of memory.
- 40 GB of Disk Space.
- 2 CPUs.

C) Run the VM and install Windows 10.

Install Guest Editions on your Windows 10 VM.

Download, extract, create VM, and import Kali Linux VM hard drive.

A) Open this link and download the latest 64-bit Kali Linux VM Image for Virtual Box.

https://www.kali.org/get-kali/#kali-virtual-machines

B) In VirtualBox, create a new VM called: "Kali".

Then apply the following specs:

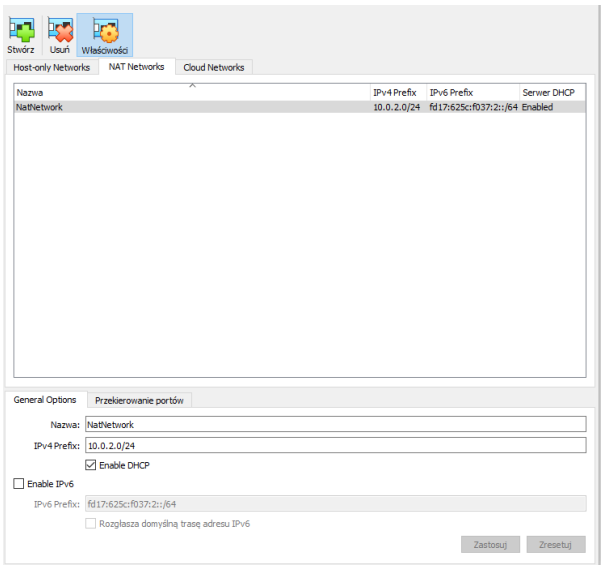
- 2 CPUs.
- 2 GB of memory.
- Extract the downloaded file and import the ".vdi" file as a hard drive

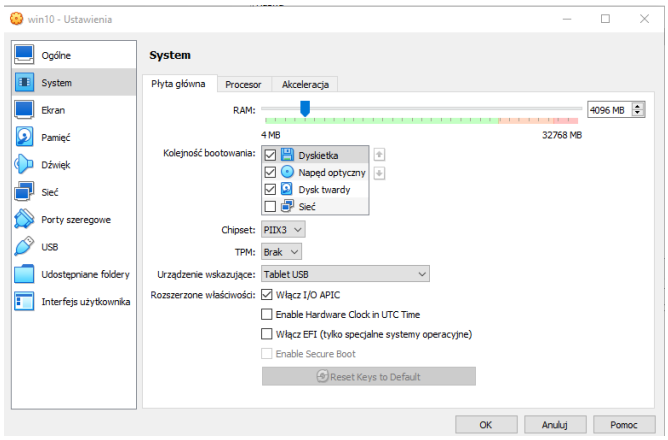
C) Run the VM and install Kali Linux.

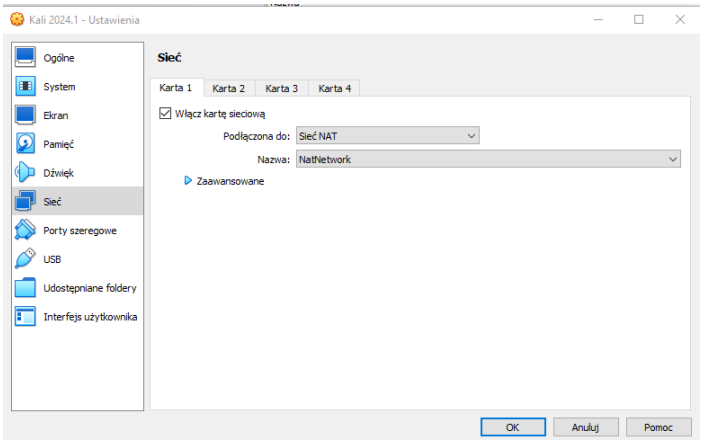
In VirtualBox, create a NAT-Network named: "Virtualization", use an IP address range of 10.0.2.0/24, and ensure the DHCP Server is set to Enabled.

Attach the newly created "Virtualization" NAT-Network to your Kali & Windows network adapters.

In both operating systems, utilize the ping command to assess connectivity between the virtual machines and Google's DNS server (8.8.8.8) to confirm a functioning Wide Area Network (WAN) connection.


Stwórz
Usuń
Właściwości
Host-only Networks
NAT Networks
Cloud Networks
Nazwa
IPv4 Prefix
IPv6 Prefix
Serwer DHCP
NatNetwork
10.0.2.0/24
fd17:625c:f037:2::/64
Enabled
General Options
Przekierowanie portów
Nazwa: NatNetwork
IPv4 Prefix: 10.0.2.0/24
Enable DHCP
Enable IPv6
IPv6 Prefix: fd17:625c:f037:2::/64
Rozgłasza domyślną trasę adresu IPv6
Zastosuj
Zresetuj


win10 - Ustawienia
Ogólne
System
Ekran
Pamięć
Dźwięk
Sieć
Porty szeregowe
USB
Udostępniane foldery
Interfejs użytkownika
System
Płyta główna
Procesor
Akceleracja
RAM:
4096 MB
4 MB
32768 MB
Kolejność bootowania:
Dyskietka
Napęd optyczny
Dysk twardy
Sieć
Chipset:
PIIX3
TPM:
Brak
Urządzenie wskazujące:
Tablet USB
Rozszerzone właściwości:
Włącz I/O APIC
Enable Hardware Clock in UTC Time
Włącz EFI (tylko specjalne systemy operacyjne)
Enable Secure Boot
Reset Keys to Default
OK
Anuluj
Pomoc


Kali 2024.1 - Ustawienia
Ogólne
System
Ekran
Pamięć
Dźwięk
Sieć
Porty szeregowe
USB
Udostępniane foldery
Interfejs użytkownika
Sieć
Karta 1
Karta 2
Karta 3
Karta 4
Włącz kartę sieciową
Podłączona do: Sieć NAT
Nazwa: NatNetwork
Zaawansowane
OK
Anuluj
Pomoc

Install a Windows Server 2016 operating system. A) Download Windows Server 2016 image: https://software-download.microsoft.com/download/pr/Windows_Server_2016_Datacenter_EVAL en-us_14393_refresh.ISO

B) In VirtualBox, create a new VM called: "WinServer"

Then apply the following specs:

Attach the Windows ISO you downloaded.

- 4 GB of memory.
- 2 CPUs.
- 50 GB of Disk Space.

Set the name of the Windows server as "Server20".

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe42:2da1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:2d:a1  txqueuelen 1000  (Ethernet)
        RX packets 32  bytes 5776 (5.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 5502 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::e4d9:bf1f:385a:42e4%3
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\Users\administrator>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=128 time=0.292 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=128 time=0.925 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=128 time=0.726 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=128 time=0.630 ms

── 10.0.2.15 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.292/0.643/0.925/0.229 ms
```

```
C:\Users\administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=57ms TTL=116
Reply from 8.8.8.8: bytes=32 time=97ms TTL=116
Reply from 8.8.8.8: bytes=32 time=74ms TTL=116
Reply from 8.8.8.8: bytes=32 time=64ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 97ms, Average = 73ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=62.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=47.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=58.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=46.8 ms

── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 46.784/53.636/62.570/6.904 ms
```

Install Active Directory services on the machine.

Install a Windows Server 2016 OS and Active Directory and perform the following operations: promote the machine to a domain controller, assign a client to the domain, create OUs, users and groups, configure different GPOs, and set a DNS and DHCP servers.

1.Install a Windows Server 2016 operating system or import an OVA.

Installing Windows Server 2016

1. **Prepare Installation Media**:

- Download the Windows Server 2016 ISO file from the official Microsoft website or obtain a physical installation disc.
- Create a bootable USB drive using tools like Rufus if using an ISO file.

2. **Boot from Installation Media**:

- Insert the installation media (USB or DVD) into the server or virtual machine.
- Restart the system and boot from the installation media. This may require changing the boot order in the BIOS/UEFI settings.

3. **Begin Installation**:

- Once the system boots from the installation media, you'll see the Windows Server 2016 installation screen.
- Select your language, time and currency format, and keyboard input method, then click **Next**.
- Click **Install now**.

4. **Enter Product Key**:

- Enter your product key and click **Next**.
- If you don't have a product key, you can select **I don't have a product key** to install a trial version.

5. **Select Installation Type**:

- Choose either **Windows Server 2016 Standard** or **Datacenter** edition.
- Select **Desktop Experience** if you want a GUI, or **Server Core** for a minimal, command-line interface installation.
- Click **Next**.

6. **Accept License Terms**:

- Read and accept the license terms, then click **Next**.

7. **Select Installation Type**:

- Choose **Custom: Install Windows only (advanced)** for a clean installation.

8. **Partition the Disk**:

- Select the disk where you want to install Windows Server 2016.
- Create a new partition if necessary and format it.
- Click **Next** to begin the installation.

9. **Installation Process**:

- The installation process will start and may take some time.
- The system will restart several times during the installation.

10. **Initial Configuration**:

- After the final restart, configure the initial settings like setting a password for the Administrator account.

11. **Finalize Setup**:

- Log in with the Administrator account and complete any remaining configuration steps.

Importing an OVA (Open Virtual Appliance)

1. **Obtain the OVA File**:

- Download the Windows Server 2016 OVA file from a trusted source.

2. **Install Virtualization Software**:

- Install a virtualization platform like VMware Workstation, VMware ESXi, VirtualBox, or Hyper-V if not already installed.

3. **Open the Virtualization Software**:

- Launch the virtualization software on your host machine.

4. **Import the OVA**:

- In VMware Workstation:
    - Go to **File** > **Open**.
    - Browse to the location of the OVA file and select it.
    - Follow the prompts to import the OVA.

5. In VirtualBox:
    - Go to **File** > **Import Appliance**.
    - Browse to the location of the OVA file and select it.
    - Click **Next** and follow the prompts to import the OVA.

6. In Hyper-V (if OVA is converted to VHD):
    - Go to **Action** > **Import Virtual Machine**.
    - Follow the prompts to import the converted VHD.

7. **Configure the Virtual Machine**:

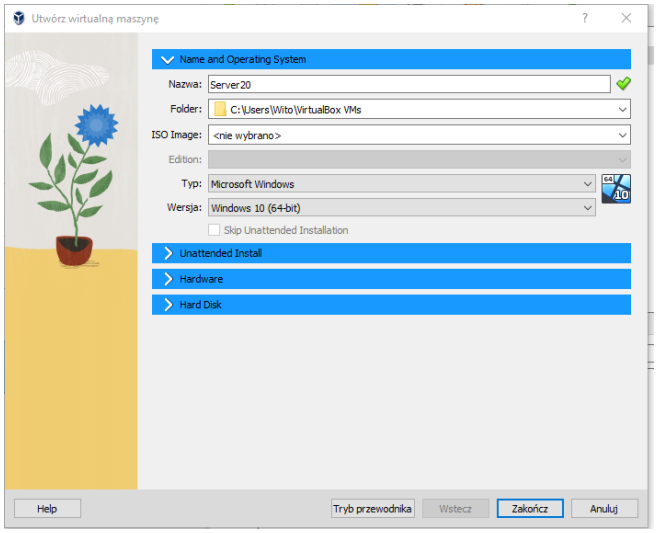
- Adjust the virtual machine settings as needed, such as allocating memory, CPUs, and configuring network settings.

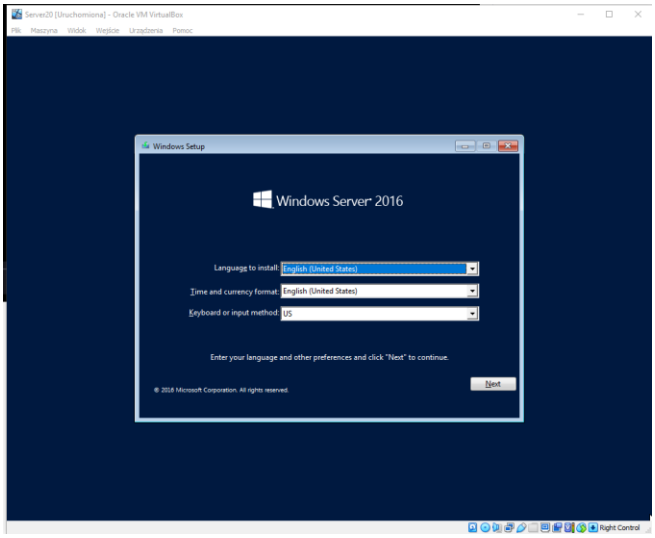
8. **Start the Virtual Machine**:

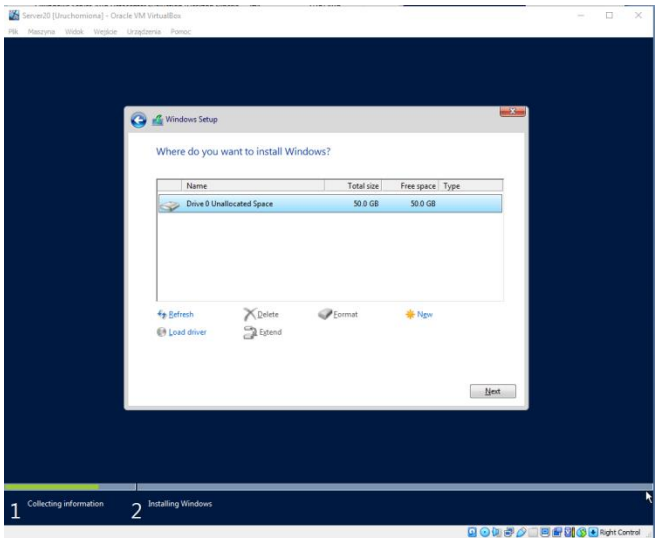
- Power on the virtual machine.
- Complete any initial setup prompts.

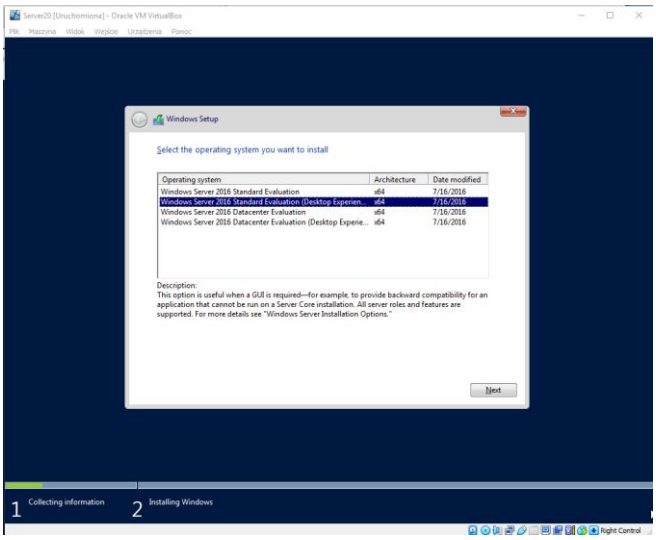
9. **Post-Import Configuration**:

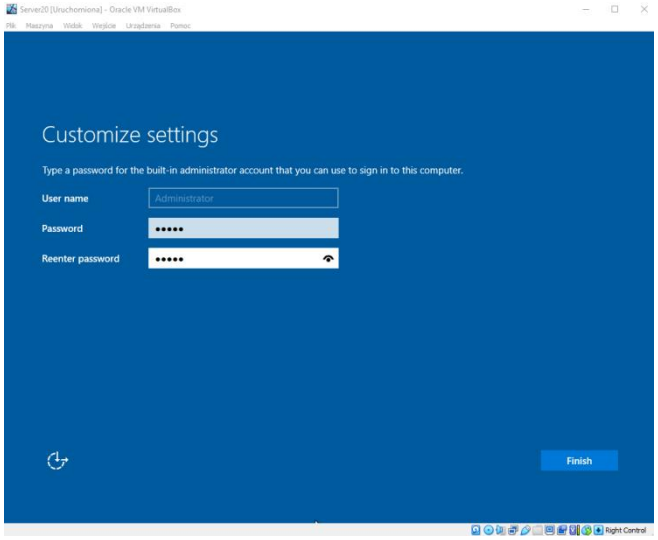
- Log in to the Windows Server 2016 virtual machine.
- Configure the network settings, install updates, and perform any additional setup tasks as needed.

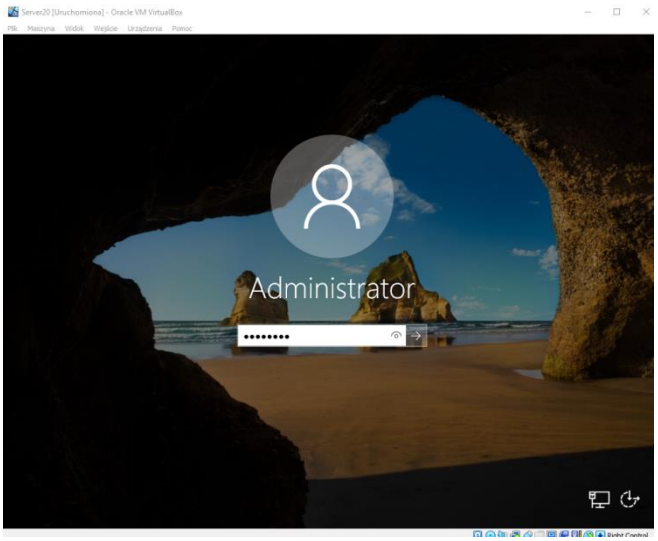






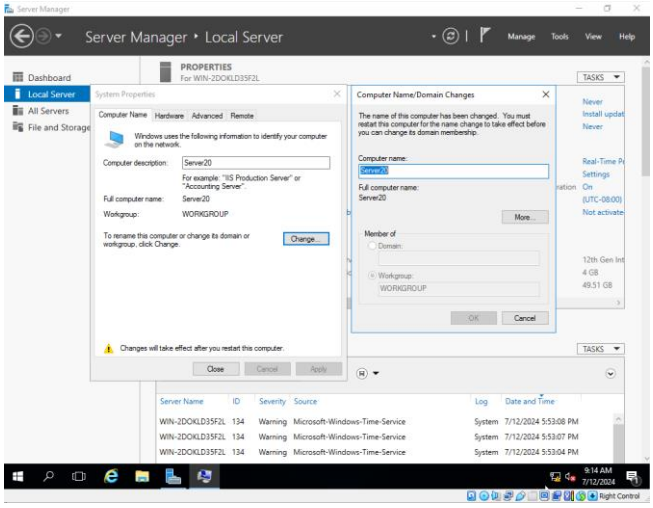


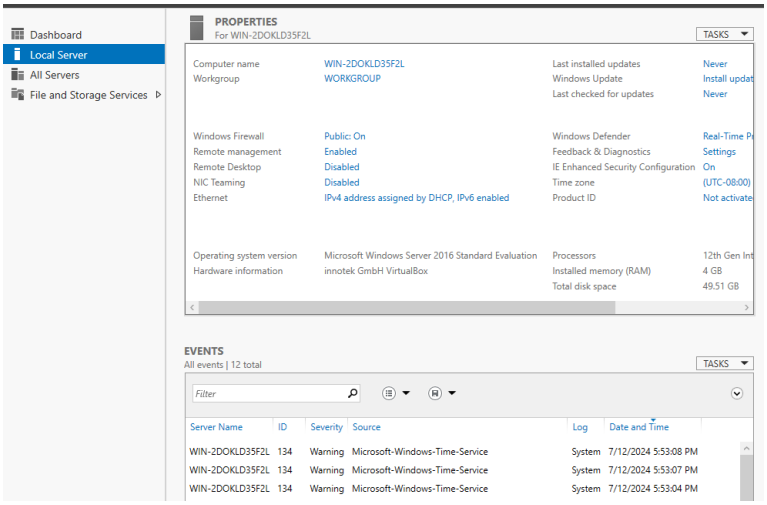

Server20 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish
Right Control

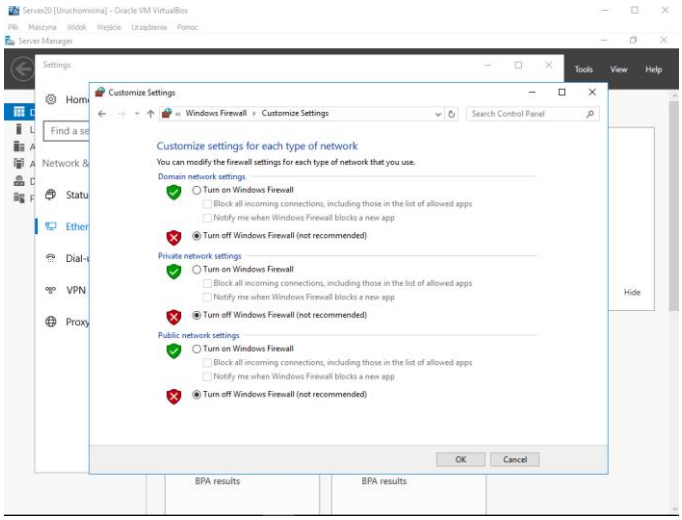

Server20 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Administrator

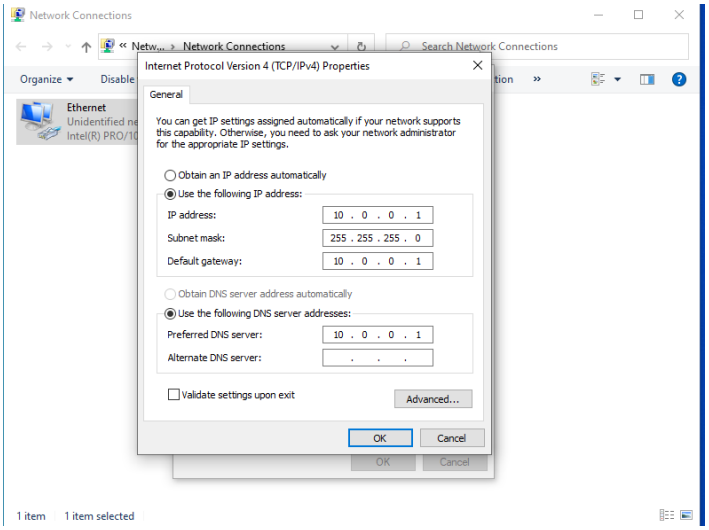
2.Set the name of the Windows server as "Server20".

- Open the **Server Manager**.
- Go to **Local Server**.
- Click on the current computer name.
- Click **Change** in the **System Properties** window.
- Enter "Server20" in the **Computer Name** field.
- Click **OK** and restart the server when prompted.
- Set the Network IP and turn off Windows defender (otherwise it will Block the connection between Server and client).









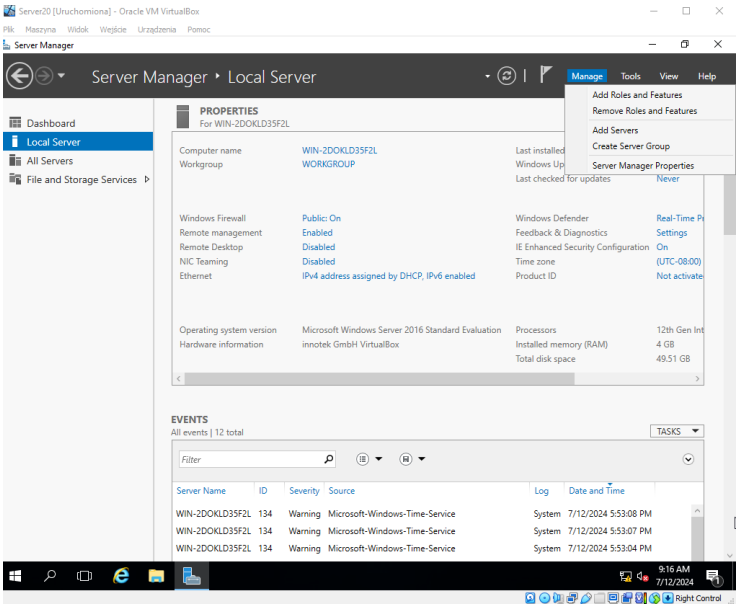
3.Install Active Directory services on the machine.

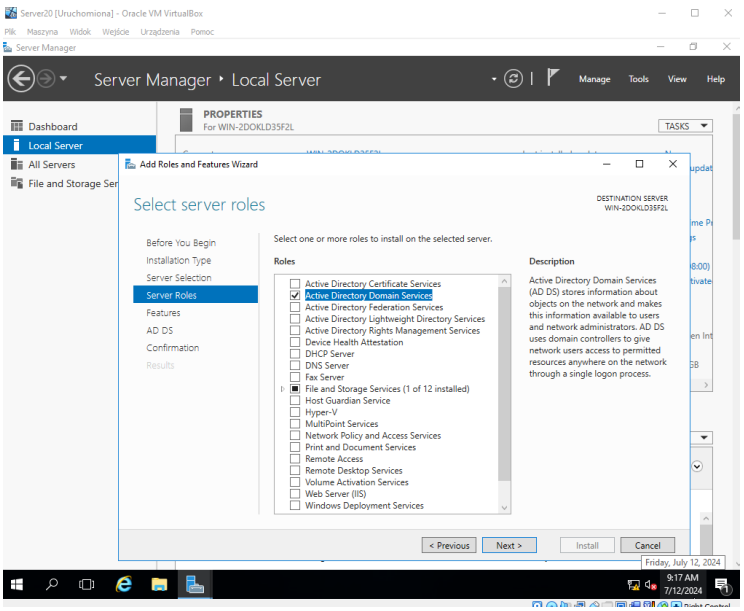
Open the **Server Manager**.

Click **Manage** and then **Add Roles and Features**.

Follow the wizard to install **Active Directory Domain Services (AD DS)**.

When the installation is complete, promote the server to a domain controller.





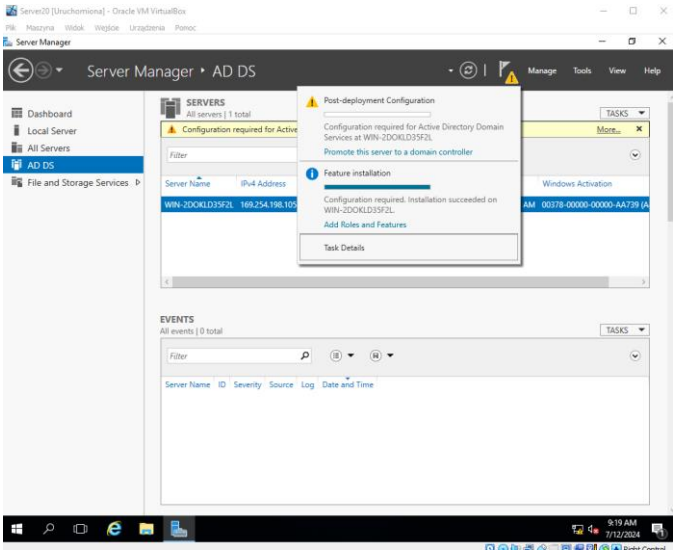
4.Promote the server to a domain controller.

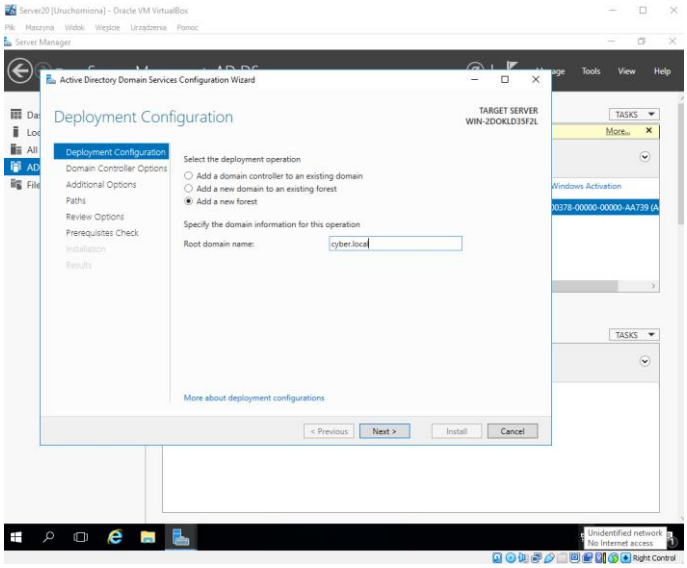
After installing AD DS, there will be a notification flag in the Server Manager. Click on it and select **Promote this server to a domain controller**.

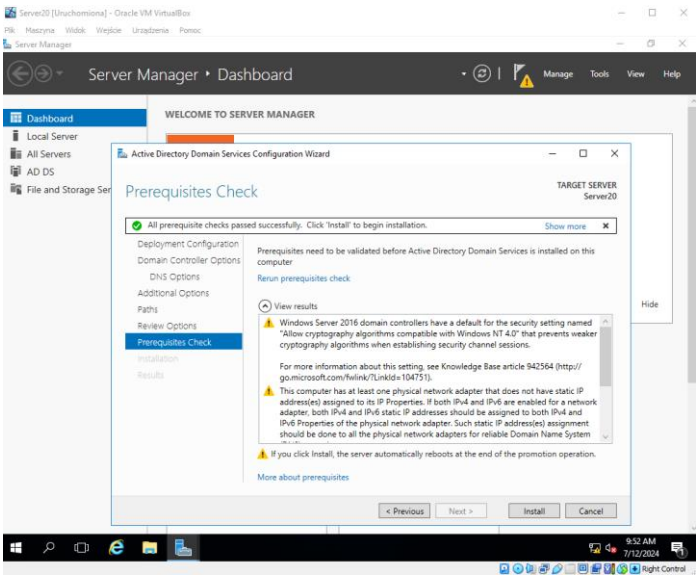
Select **Add a new forest** and provide the **Root domain name**.

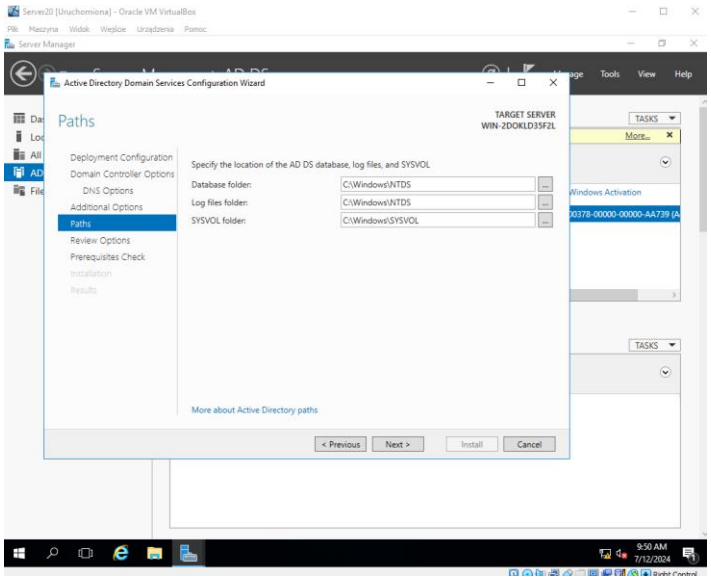
Follow the wizard to complete the promotion process, which includes specifying the **Domain Name System (DNS)** options, **NetBIOS** name, and **Directory Services Restore Mode (DSRM)** password.

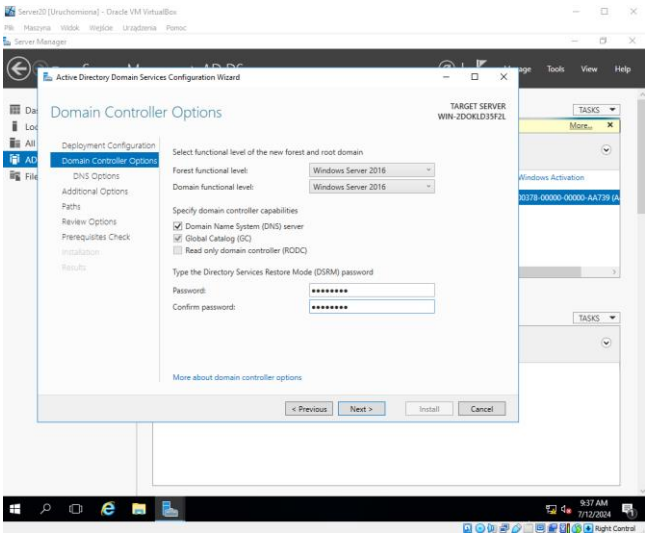
Once the server restarts, it will be a domain controller.

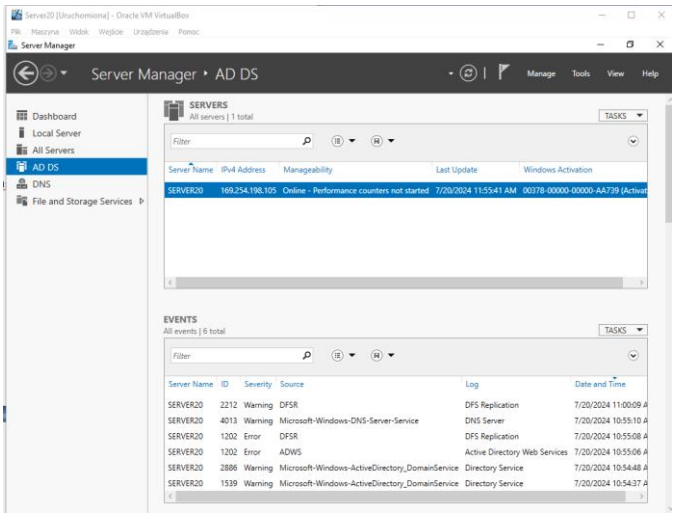









Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
WIN-2DOKLD35F2L
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel


Server Manager
Server Manager • AD DS
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
SERVERS
All servers | 1 total
TASKS
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
SERVER20
169.254.198.105
Online - Performance counters not started
7/20/2024 11:55:41 AM
00378-00000-00000-AA739 (Activat
EVENTS
All events | 6 total
Server Name
ID
Severity
Source
Log
Date and Time
SERVER20 2212 Warning DFSR DFS Replication 7/20/2024 11:00:09 A
SERVER20 4013 Warning Microsoft-Windows-DNS-Server-Service DNS Server 7/20/2024 10:55:10 A
SERVER20 1202 Error DFSR DFS Replication 7/20/2024 10:55:08 A
SERVER20 1202 Error ADWS Active Directory Web Services 7/20/2024 10:55:06 A
SERVER20 2886 Warning Microsoft-Windows-ActiveDirectory_DomainService Directory Service 7/20/2024 10:54:48 A
SERVER20 1539 Warning Microsoft-Windows-ActiveDirectory_DomainService Directory Service 7/20/2024 10:54:37 A

5.Rename the Windows 10 client machine as "PC1" and assign the domain to it.

On the Windows 10 machine, right-click **This PC** and select **Properties**.

Click **Change settings** next to the computer name.

Click **Change** in the **System Properties** window.

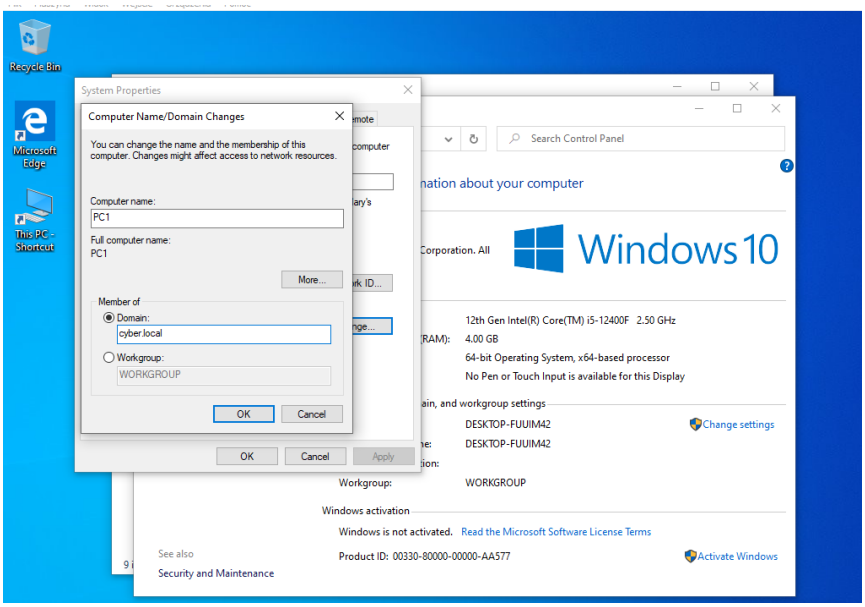
Enter "PC1" in the **Computer Name** field.

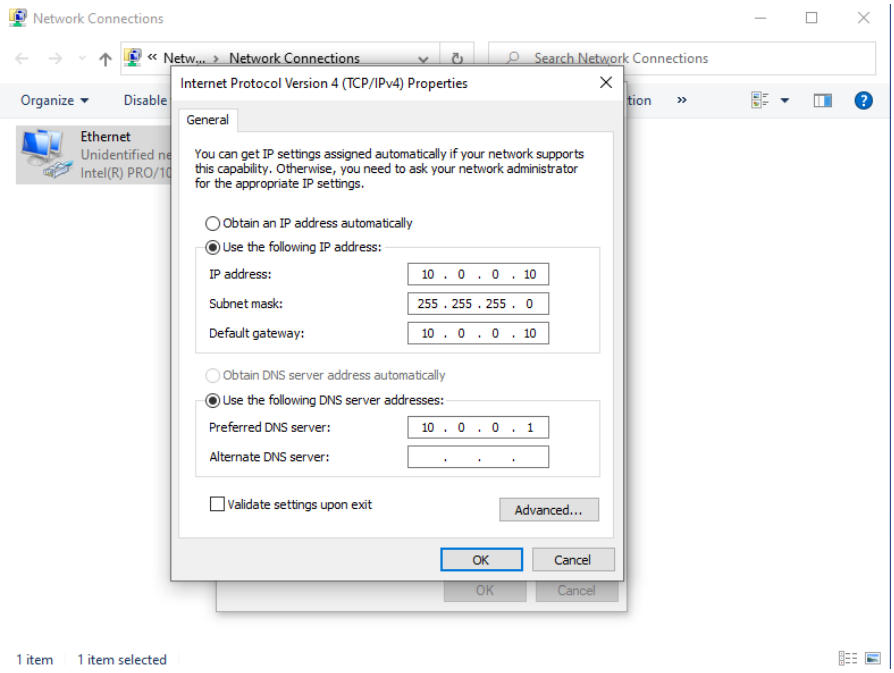
Select **Domain** under **Member of**, and enter the domain name created in the previous step.

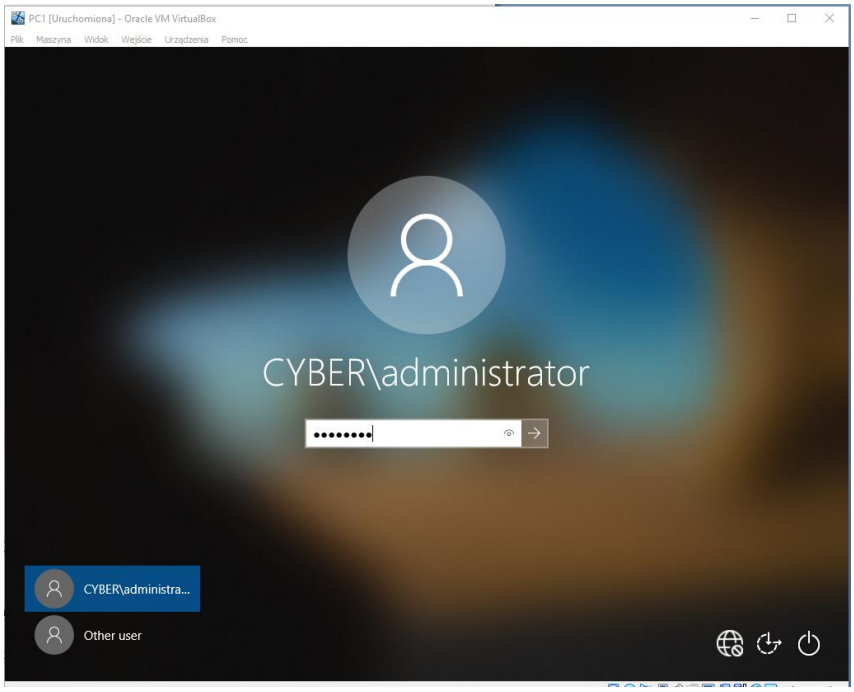
Click **OK**, provide domain admin credentials, and restart the machine.

Set the Network IP adress and check the firewall.

Login as Administrator on Client machine PC1.






PC1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
CYBER\administrator
CYBER\administra...
Other user

6.Create the following OUS on the DC machine:

Developers, IT, QA, HR, and Designers.
Add 5 users for each OU.
Create the appropriate groups and assign users to them.
Add one user from each department to the Domain Admins group.

1. Creating Organizational Units (OUs)

Open "Active Directory Users and Computers" on the DC machine.

Right-click on the domain (e.g., "yourdomain.local") and select "New" -> "Organizational Unit".

Create the following OUs: Developers, IT, QA, HR, Designers.

2. Adding Users to Each OU

Navigate to each created OU (e.g., Developers) in "Active Directory Users and Computers".

Right-click on the OU and select "New" -> "User".

Enter the required information for each user (e.g., devuser1, devuser2, etc.) and set a password.

Repeat this process to create 5 users in each OU.

3. Creating Appropriate Groups and Assigning Users to Them

Go to each OU.

Right-click on the OU and select "New" -> "Group".

Create groups for each organizational unit (e.g., Developers_Group, IT_Group, QA_Group, HR_Group, Designers_Group).

To add users to a group, right-click on the group, select "Properties" -> "Members" tab -> "Add", and then add the appropriate users.

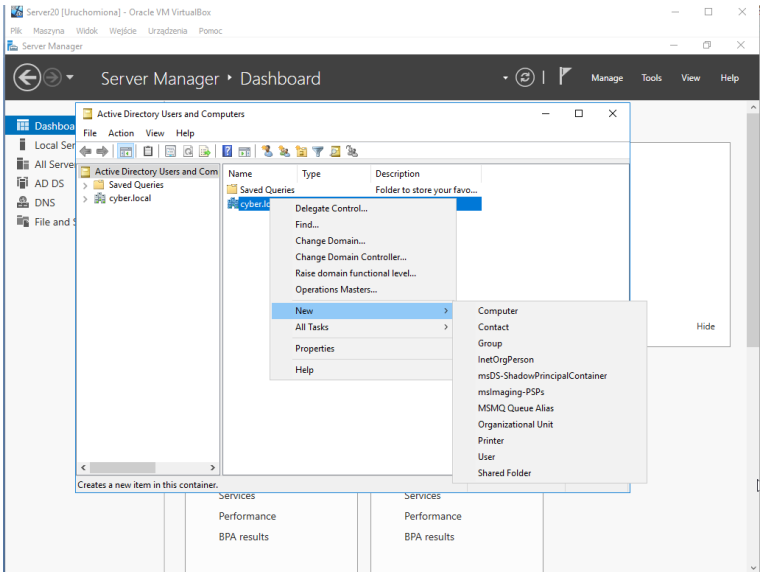
4. Adding One User from Each Organizational Unit to the "Domain Admins" Group

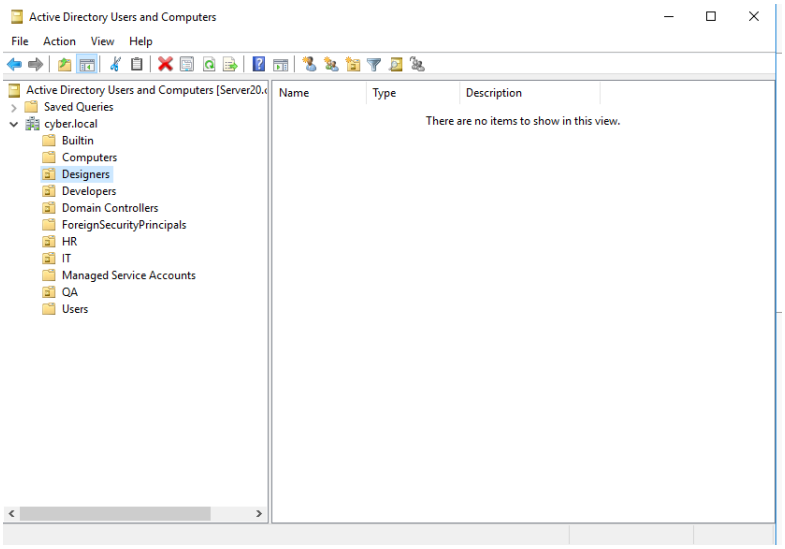
Open "Active Directory Users and Computers".

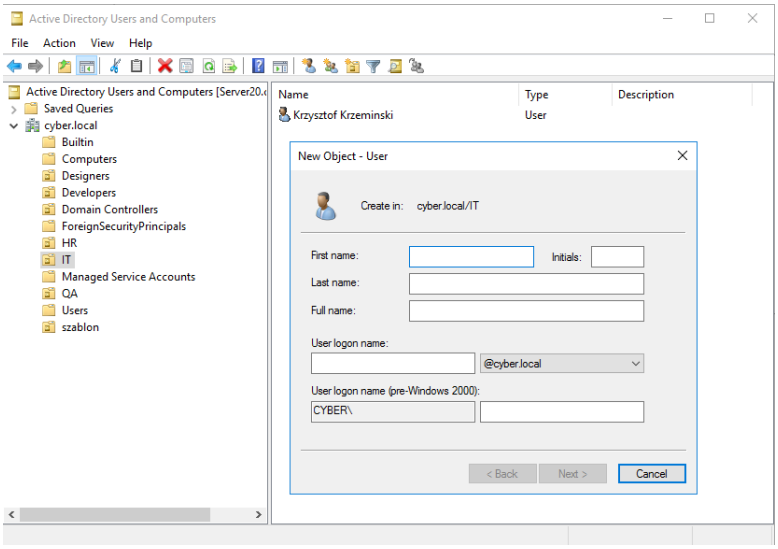
Go to the "Domain Admins" group (located in the "Users" OU).

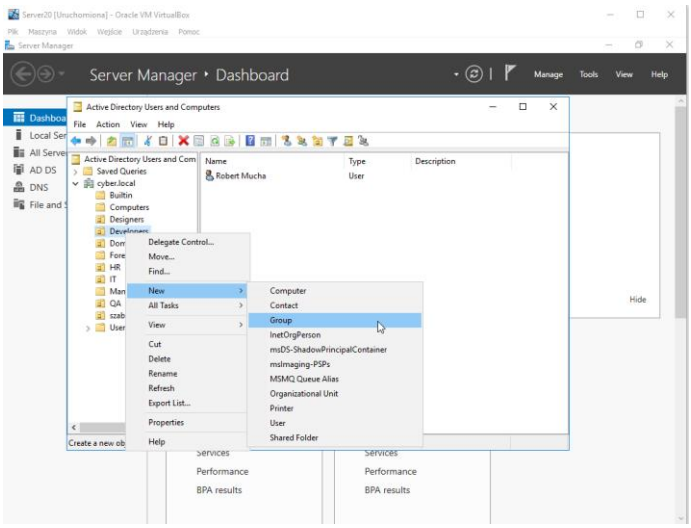
Right-click on "Domain Admins", select "Properties" -> "Members" tab -> "Add".

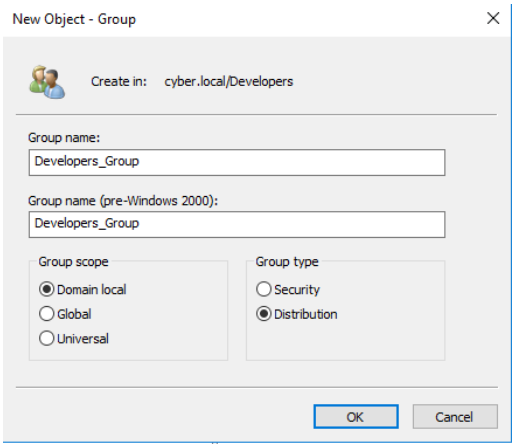
Add one user from each organizational unit to the "Domain Admins" group.

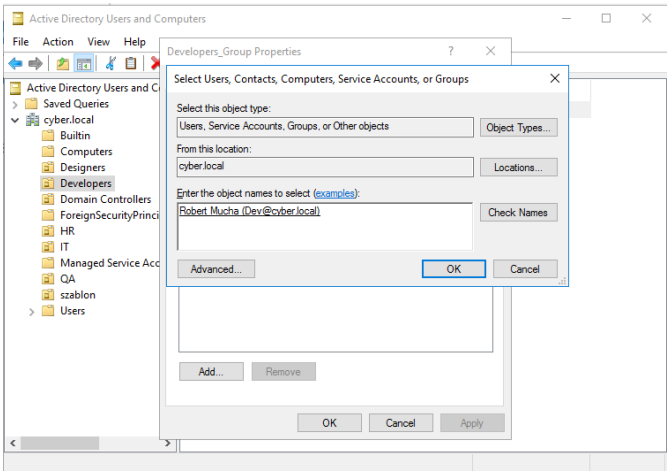

Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Name
Type
Description
Saved Queries
Folder to store your favo...
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Creates a new item in this container.
Services
Performance
BPA results

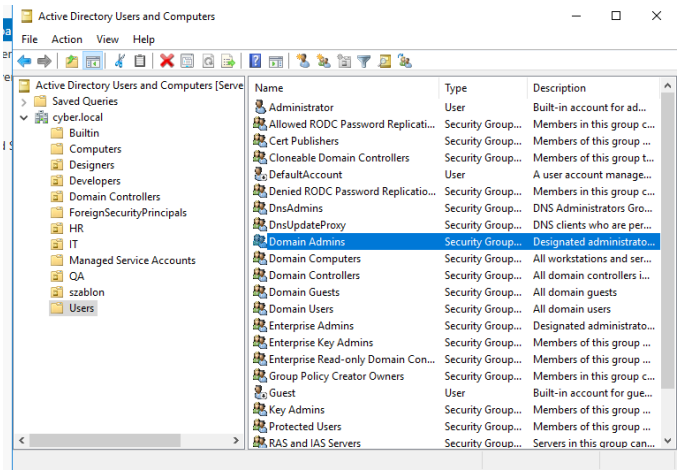

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [Server20.
Saved Queries
cyber.local
Builtin
Computers
Designers
Developers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Managed Service Accounts
QA
Users
Name
Type
Description
There are no items to show in this view.

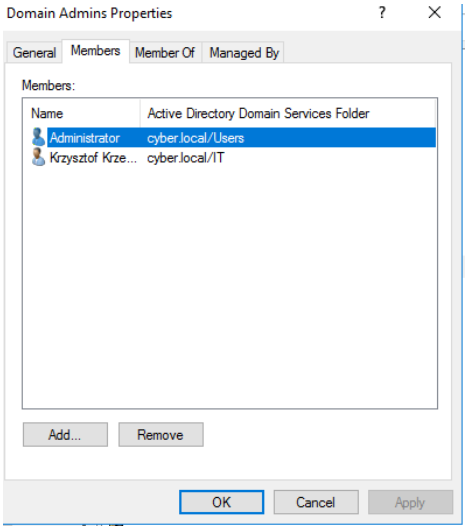

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [Server20.
Saved Queries
cyber.local
Builtin
Computers
Designers
Developers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Managed Service Accounts
QA
Users
szablon
Name
Type
Description
Krzysztof Krzeminski
User
New Object - User
Create in: cyber.local/IT
First name:
Initials:
Last name:
Full name:
User logon name:
@cyber.local
User logon name (pre-Windows 2000):
CYBER\
< Back
Next >
Cancel


Server Manager • Dashboard
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
cyber.local
Builtin
Computers
Designers
Developers
HR
IT
QA
szablon
Users
Name
Type
Description
Robert Mucha
User
Delegate Control...
Move...
Find...
New
All Tasks
View
Cut
Delete
Rename
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Hide
Services
Performance
BPA results


New Object - Group
Create in: cyber.local/Developers
Group name:
Developers_Group
Group name (pre-Windows 2000):
Developers_Group
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel


Active Directory Users and Computers
File Action View Help
Developers_Group Properties
Select Users, Contacts, Computers, Service Accounts, or Groups
Select this object type:
Users, Service Accounts, Groups, or Other objects
Object Types...
From this location:
cyber.local
Locations...
Enter the object names to select (examples):
Robert Mucha (Dev@cyber.local)
Check Names
Advanced...
OK
Cancel
Add...
Remove
OK
Cancel
Apply


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [Serve
Saved Queries
cyber.local
Builtin
Computers
Designers
Developers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Managed Service Accounts
QA
szablon
Users
Name Type Description
Administrator User Built-in account for ad...
Allowed RODC Password Replicati... Security Group... Members in this group c...
Cert Publishers Security Group... Members of this group ...
Cloneable Domain Controllers Security Group... Members of this group t...
DefaultAccount User A user account manage...
Denied RODC Password Replicatio... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateProxy Security Group... DNS clients who are per...
Domain Admins Security Group... Designated administrato...
Domain Computers Security Group... All workstations and ser...
Domain Controllers Security Group... All domain controllers i...
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise Admins Security Group... Designated administrato...
Enterprise Key Admins Security Group... Members of this group ...
Enterprise Read-only Domain Con... Security Group... Members of this group ...
Group Policy Creator Owners Security Group... Members in this group c...
Guest User Built-in account for gue...
Key Admins Security Group... Members of this group ...
Protected Users Security Group... Members of this group ...
RAS and IAS Servers Security Group... Servers in this group can...


Domain Admins Properties
General Members Member Of Managed By
Members:
Name Active Directory Domain Services Folder
Administrator cyber.local/Users
Krzysztof Krze... cyber.local/IT
Add... Remove
OK Cancel Apply

7.Create the following GPOs:

- Set a different wallpaper for each department.

- Prevent the QA department's users from accessing the Control Panel.

- Prevent the HR department's users from accessing the CMD.

1. Creating Different Wallpapers for Each Department

Open Group Policy Management:

-On the Domain Controller (DC), open “Group Policy Management”.

-Create a New GPO for Each Department:

-Right-click on "Group Policy Objects" and select "New".

-Create a new GPO for each department, for example, "Wallpaper_Developers", "Wallpaper_IT", "Wallpaper_QA", "Wallpaper_HR", "Wallpaper_Designers".

Configure the Wallpaper:

-Right-click the created GPO and select “Edit”.

-Navigate to “User Configuration” -> “Policies” -> “Administrative Templates” -> “Desktop” -> “Desktop”.

-Double-click “Desktop Wallpaper” and set the path to the wallpaper image for the specific department.

-Set “Wallpaper Style” to “Fill” (or another preferred option).

Link the GPO to the Appropriate OU:

-Right-click the appropriate Organizational Unit (OU) (e.g., “Developers”) and select “Link an existing GPO”.

-Select the appropriate GPO (e.g., “Wallpaper_Developers”) and click “OK”.

-Prevent QA Department Users from Accessing the Control Panel

Create a New GPO:

In “Group Policy Management”, right-click on "Group Policy Objects" and select "New".

Name the new GPO, for example, "Disable_ControlPanel_QA".

Configure the Control Panel Block:

-Right-click the created GPO and select “Edit”.

-Navigate to “User Configuration” -> “Policies” -> “Administrative Templates” -> “Control Panel”.

-Double-click “Prohibit access to Control Panel and PC settings” and set it to “Enabled”.

Link the GPO to the OU:

-Right-click the “QA” Organizational Unit (OU) and select “Link an existing GPO”.

-Select “Disable_ControlPanel_QA” and click “OK”.

Prevent HR Department Users from Accessing CMD

Create a New GPO:

-In “Group Policy Management”, right-click on "Group Policy Objects" and select "New".

-Name the new GPO, for example, "Disable_CMD_HR".

Configure the CMD Block:

Right-click the created GPO and select “Edit”.

Navigate to “User Configuration” -> “Policies” -> “Administrative Templates” -> “System”.

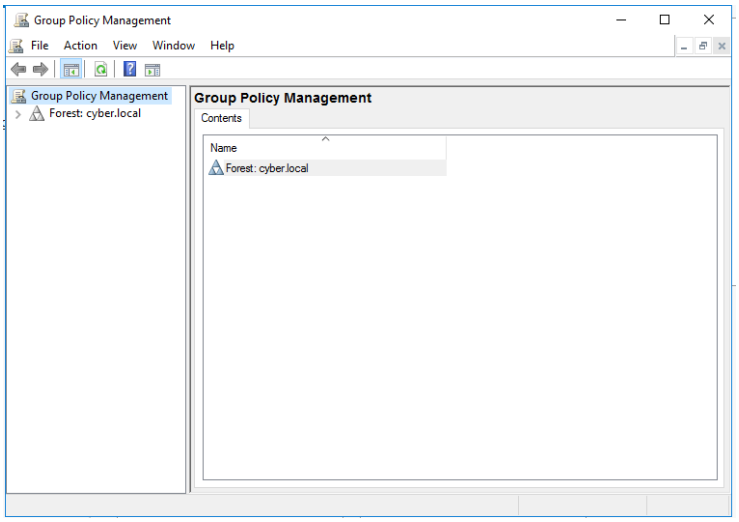
Double-click “Prevent access to the command prompt” and set it to “Enabled”.

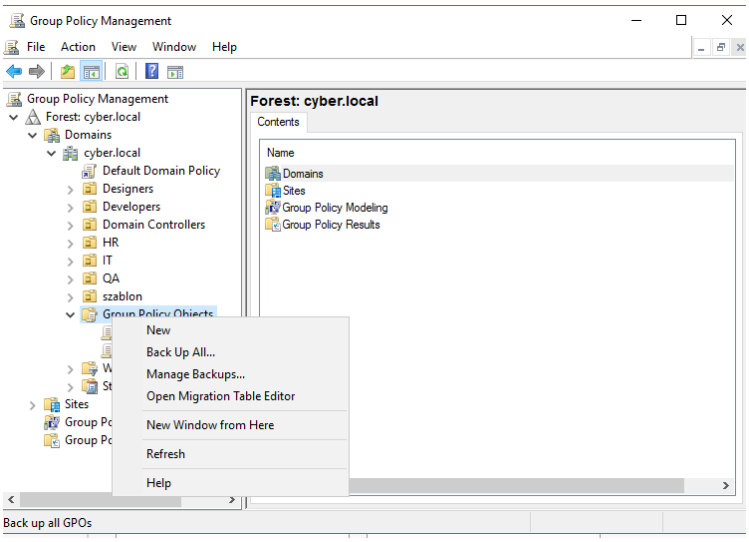
Optionally, you can set “Disable the command prompt script processing also?” to “Yes”.

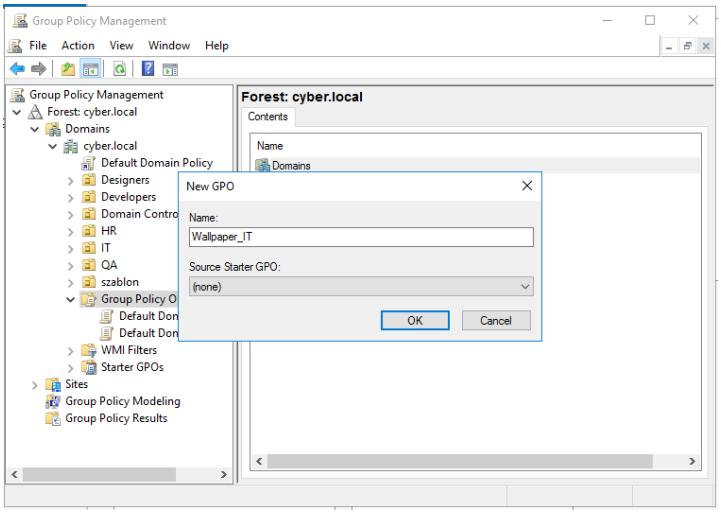
Link the GPO to the OU:

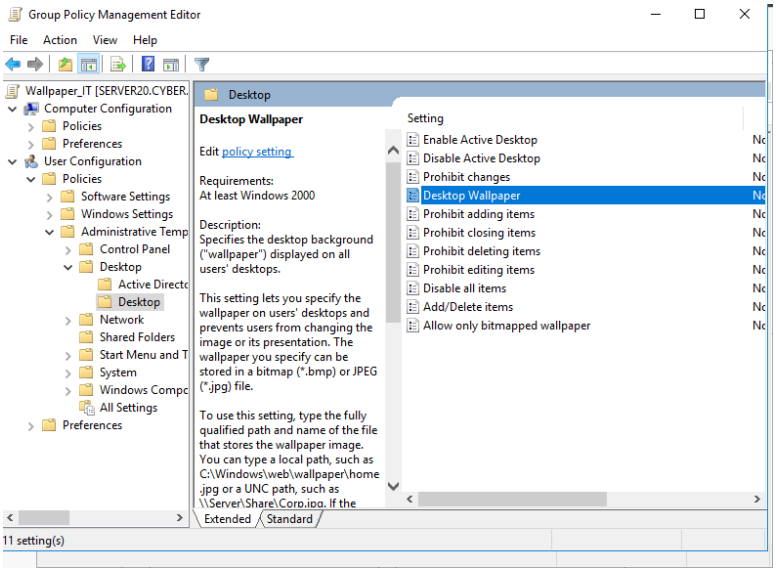
Right-click the “HR” Organizational Unit (OU) and select “Link an existing GPO”.

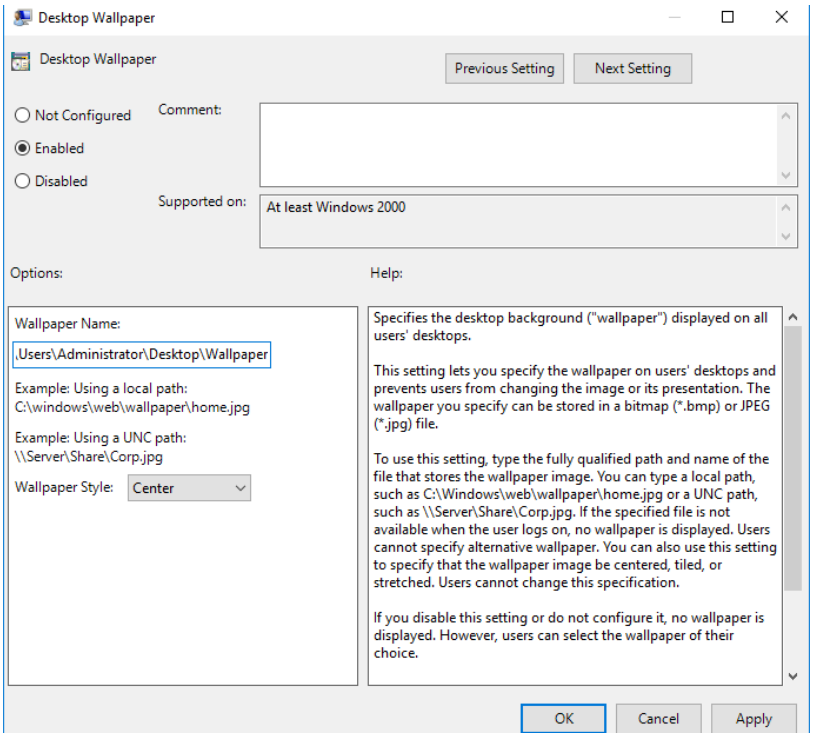
Select “Disable_CMD_HR” and click “OK”.

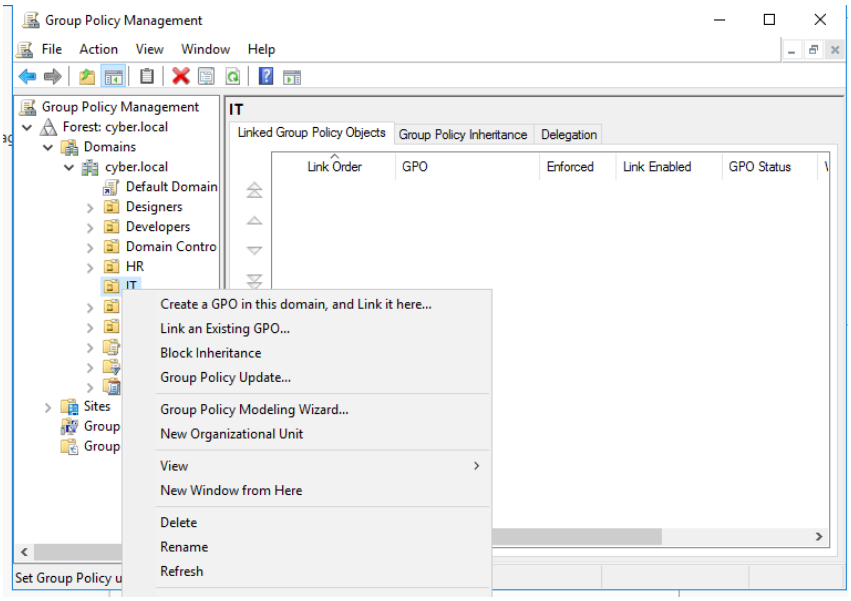


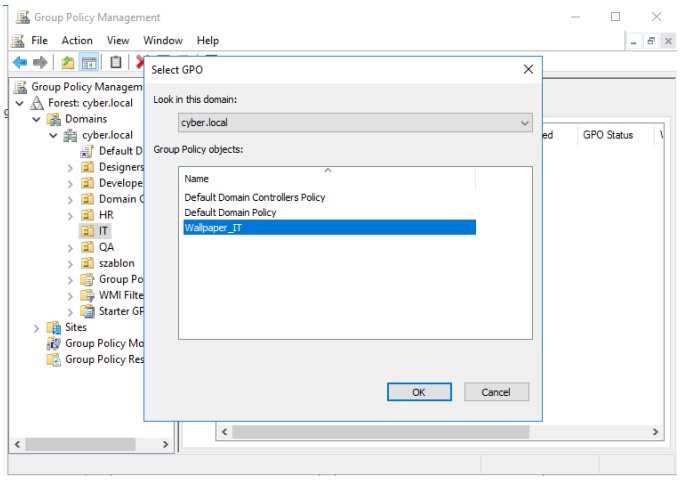

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Default Domain Policy
Designers
Developers
Domain Controllers
HR
IT
QA
szablon
Group Policy Objects
Sites
Group Policy Modeling
Group Policy Results
Forest: cyber.local
Contents
Name
Domains
Sites
Group Policy Modeling
Group Policy Results
New
Back Up All...
Manage Backups...
Open Migration Table Editor
New Window from Here
Refresh
Help
Back up all GPOs

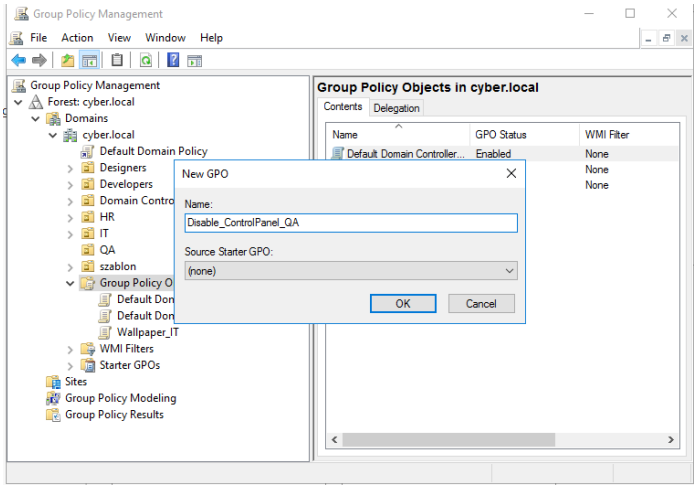

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Default Domain Policy
Designers
Developers
HR
IT
QA
szablon
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Forest: cyber.local
Contents
Name
Domains
New GPO
Name:
Wallpaper_IT
Source Starter GPO:
(none)
OK
Cancel

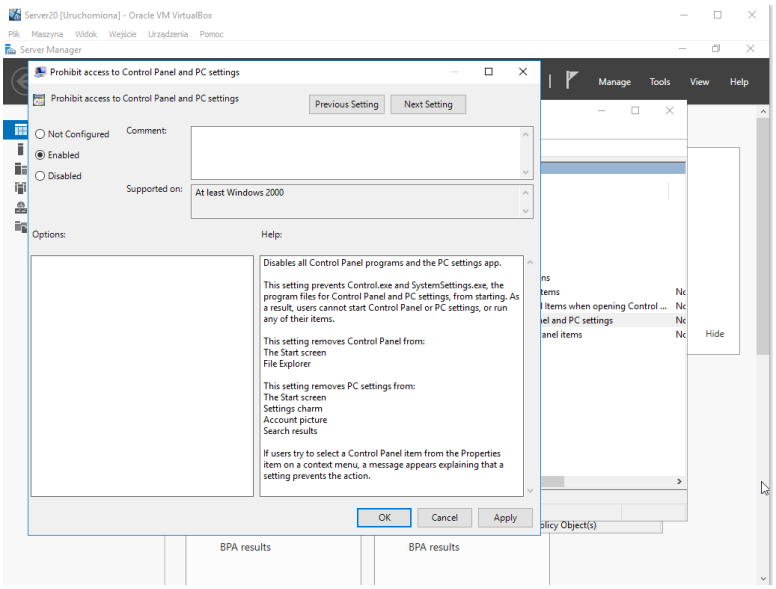

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Control Panel
Desktop
Network
Shared Folders
System
All Settings
Preferences
Desktop
Desktop Wallpaper
Edit policy setting
Requirements:
At least Windows 2000
Description:
Specifies the desktop background ("wallpaper") displayed on all users' desktops.
This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.
To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the
Setting
Enable Active Desktop
Disable Active Desktop
Prohibit changes
Desktop Wallpaper
Prohibit adding items
Prohibit closing items
Prohibit deleting items
Prohibit editing items
Disable all items
Add/Delete items
Allow only bitmapped wallpaper
Extended
Standard
11 setting(s)

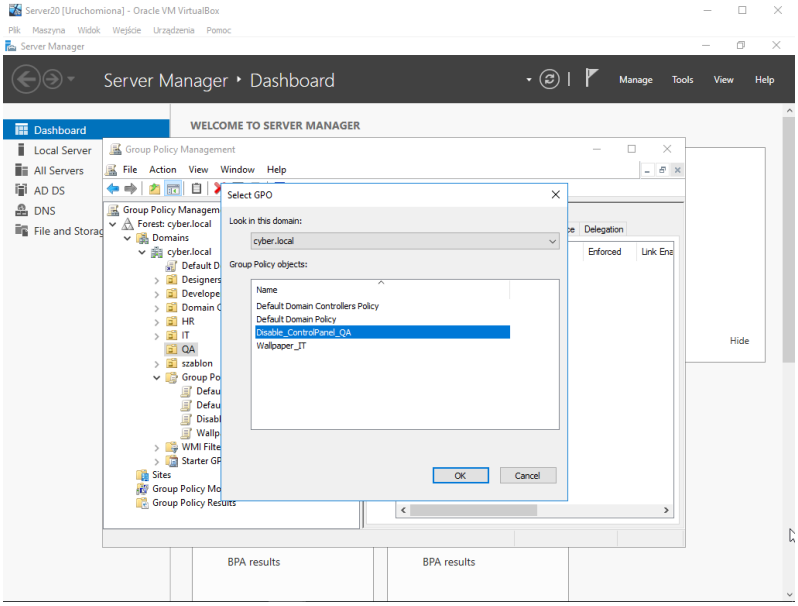

Desktop Wallpaper
Desktop Wallpaper
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Wallpaper Name:
,Users\Administrator\Desktop\Wallpaper
Example: Using a local path:
C:\windows\web\wallpaper\home.jpg
Example: Using a UNC path:
\\Server\Share\Corp.jpg
Wallpaper Style:
Center
Specifies the desktop background ("wallpaper") displayed on all users' desktops.
This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.
To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.
If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.
OK
Cancel
Apply

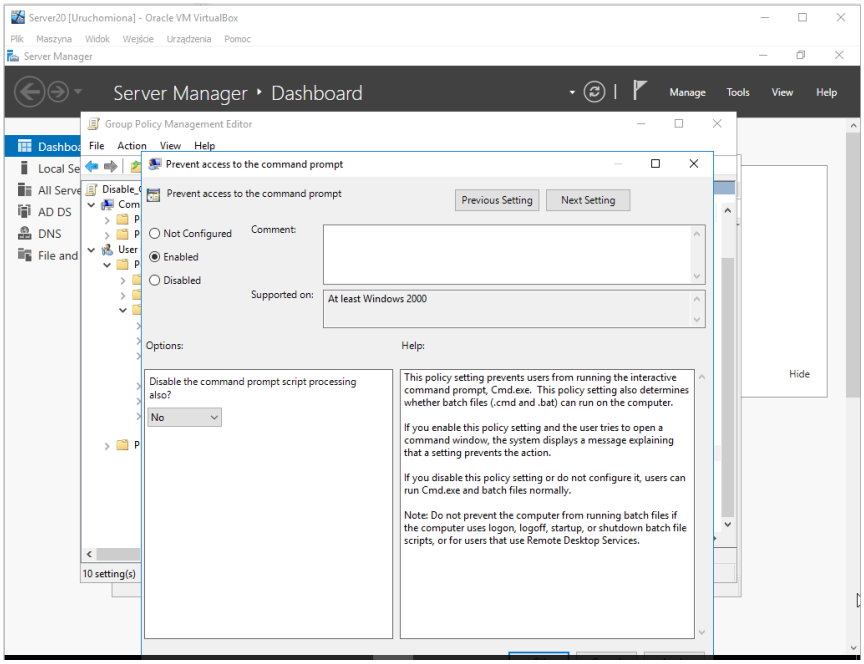

Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Default Domain
Designers
Developers
Domain Contro
HR
IT
Sites
Group
Group
IT
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
View
New Window from Here
Delete
Rename
Refresh
Set Group Policy u

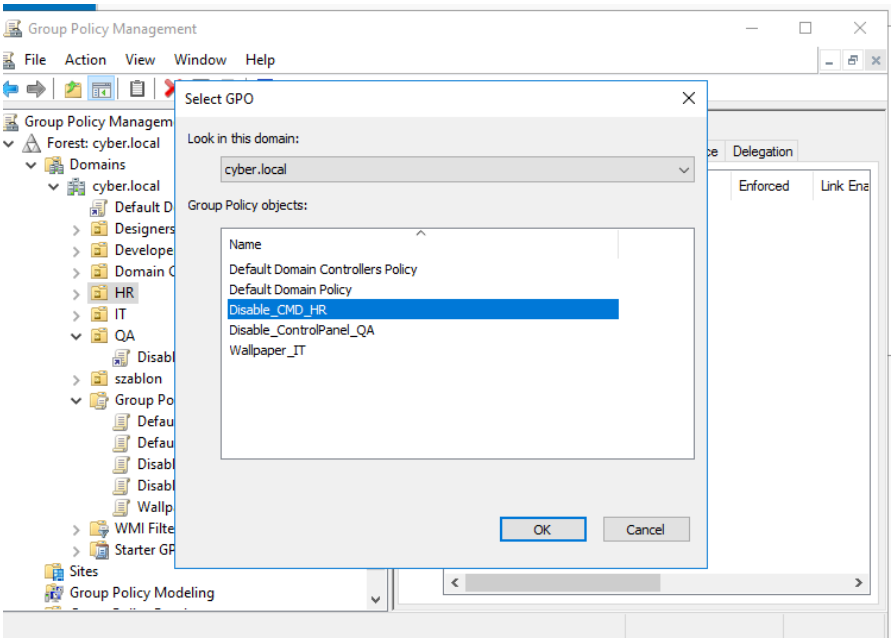

Group Policy Management
File Action View Window Help
Select GPO
Look in this domain:
cyber.local
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
Wallpaper_IT
OK
Cancel
GPO Status


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Default Domain Policy
Designers
Developers
HR
IT
QA
szablon
Wallpaper_IT
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in cyber.local
Contents
Delegation
Name
GPO Status
WMI Filter
Default Domain Controller...
Enabled
None
New GPO
Name:
Disable_ControlPanel_QA
Source Starter GPO:
(none)
OK
Cancel


Server20 [Uruchomiona] - Oracle VM VirtualBox
Server Manager
Prohibit access to Control Panel and PC settings
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results
If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.
OK
Cancel
Apply
Manage
Tools
View
Help
Hide
BPA results
BPA results


Server20 [Uruchomiona] - Oracle VM VirtualBox
Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
WELCOME TO SERVER MANAGER
Group Policy Management
File
Action
View
Window
Help
Select GPO
Look in this domain:
cyber.local
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
Disable_ControlPanel_QA
Wallpaper_IT
OK
Cancel
Forest: cyber.local
Domains
cyber.local
HR
IT
QA
szablon
WMI Filte
Starter GP
Sites
Group Policy Results
Delegation
Enforced
Hide
BPA results
BPA results


Server20 [Uruchomiona] - Oracle VM VirtualBox
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Group Policy Management Editor
File
Action
View
Help
Prevent access to the command prompt
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Disable the command prompt script processing also?
No
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.
If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.
10 setting(s)
Hide


Group Policy Management
File
Action
View
Window
Help
Select GPO
Look in this domain:
cyber.local
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
Disable_CMD_HR
Disable_ControlPanel_QA
Wallpaper_IT
OK
Cancel
Forest: cyber.local
Domains
cyber.local
HR
IT
QA
szablon
Sites
Group Policy Modeling
Delegation
Enforced

8.Configure the system to lock out users after 3 failed login attempts. Only the administrator will be able to unlock the user account.

Using Group Policy Management

Open Group Policy Management:

-On the Domain Controller (DC), open “Group Policy Management”.

Create a New GPO:

-Right-click on "Group Policy Objects" and select "New".

-Name the new GPO, for example, "Account_Lockout_Policy".

-Configure Account Lockout Policy:

-Right-click the created GPO and select “Edit”.

-Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Account Policies” -> “Account Lockout Policy”.

Set Account Lockout Policy:

-Account lockout threshold: Double-click and set to 3 failed login attempts.

-Account lockout duration: Double-click and set to 0, which means the account will remain locked until manually unlocked by an administrator.

-Reset account 25ock out counter after: Double-click and set to an appropriate time, e.g., 30 minutes.

Link the GPO to the Domain:

-Right-click the domain (e.g., “yourdomain.local”) and select “Link an existing GPO”.

-Select “Account_Lockout_Policy” and click “OK”.

-Verify Configuration

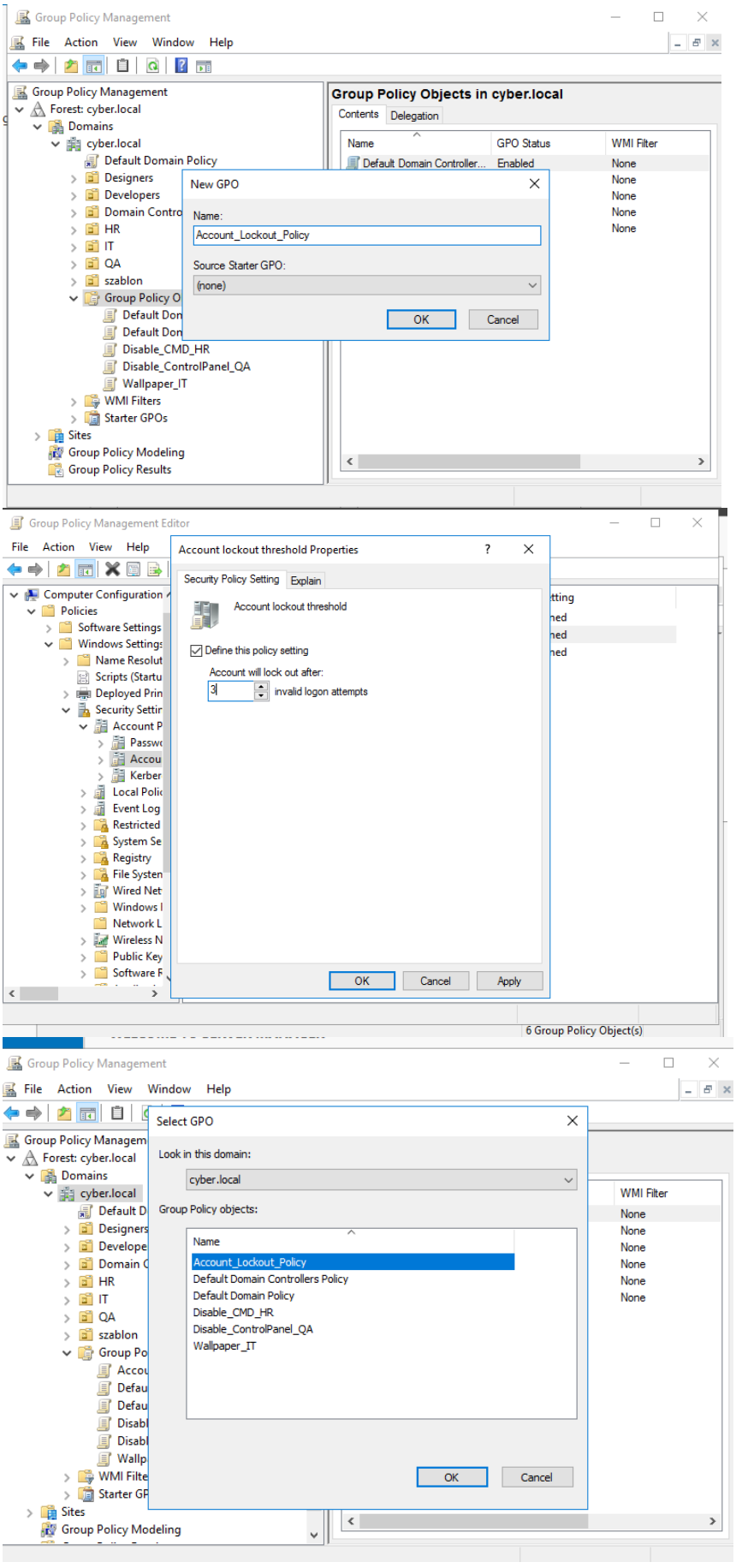
-After completing the above steps, it's important to verify that the policy has been applied correctly:

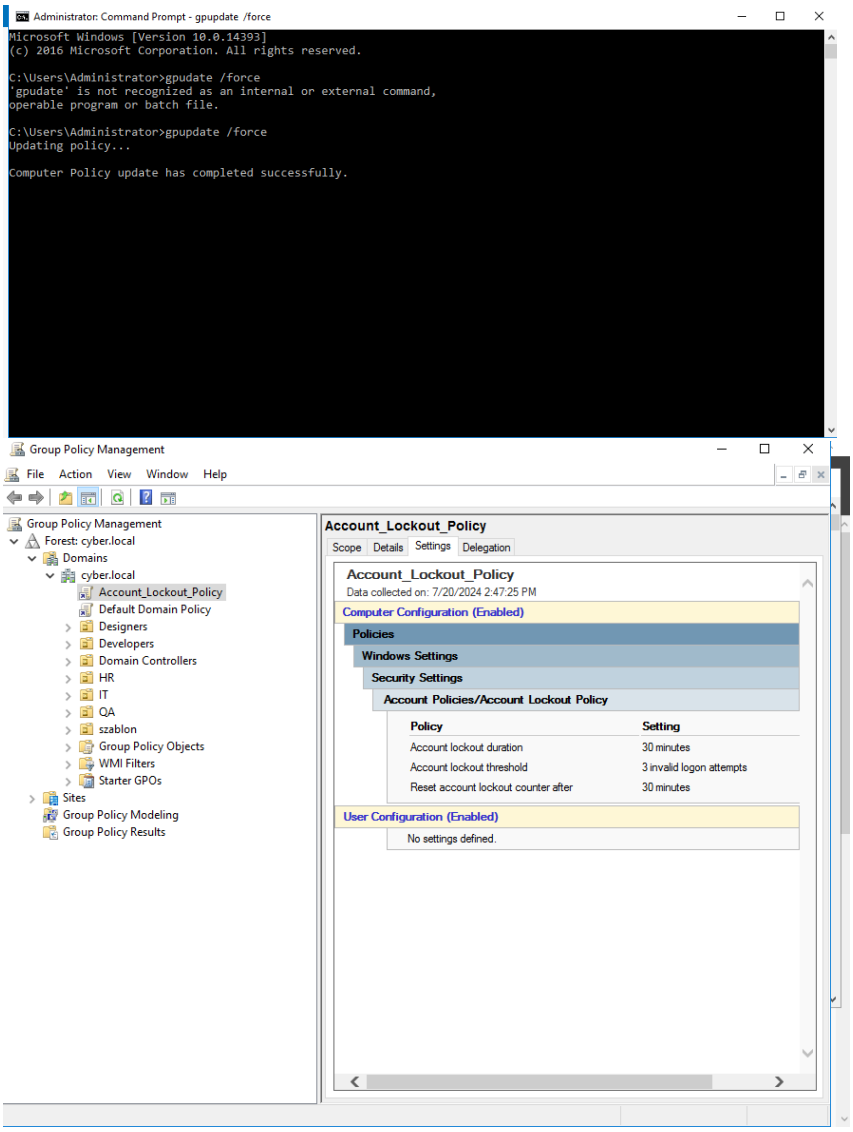
-Open Command Prompt as Administrator:

-On a Windows computer, open Command Prompt as an administrator.

Force Group Policy Update:

-Type the command gpupdate /force to force the update of group policies.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Default Domain Policy
Designers
Developers
HR
IT
QA
szablon
Group Policy Objects
Wallpaper_IT
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in cyber.local
Contents
Delegation
Name
GPO Status
WMI Filter
Default Domain Controller...
Enabled
None
New GPO
Name:
Account_Lockout_Policy
Source Starter GPO:
(none)
OK
Cancel
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Account Policies
Local Policies
Event Log
Restricted Groups
Registry
Wireless Network
Public Key Policies
Account lockout threshold Properties
Security Policy Setting
Explain
Account lockout threshold
Define this policy setting
Account will lock out after:
3
invalid logon attempts
OK
Cancel
Apply
6 Group Policy Object(s)
Group Policy Management
File Action View Window Help
Select GPO
Look in this domain:
cyber.local
Group Policy objects:
Name
Account_Lockout_Policy
Default Domain Controllers Policy
Default Domain Policy
Disable_CMD_HR
Disable_ControlPanel_QA
Wallpaper_IT
OK
Cancel


Administrator: Command Prompt - gpupdate /force
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>gpudate /force
'gpudate' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: cyber.local
Domains
cyber.local
Account_Lockout_Policy
Default Domain Policy
Designers
Developers
Domain Controllers
HR
IT
QA
szablon
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Account_Lockout_Policy
Scope Details Settings Delegation
Account_Lockout_Policy
Data collected on: 7/20/2024 2:47:25 PM
Computer Configuration (Enabled)
Policies
Windows Settings
Security Settings
Account Policies/Account Lockout Policy
Policy Setting
Account lockout duration 30 minutes
Account lockout threshold 3 invalid logon attempts
Reset account lockout counter after 30 minutes
User Configuration (Enabled)
No settings defined.

9.Create a shared drive named "Files" that will only be accessible to users of the Designers and Developers departments.
Create a Folder on the Disk:

-Log in to the Windows Server as an administrator.

-Open File Explorer and navigate to the location where you want to create a new folder.

-Right-click in an empty space, select "New," and then "Folder."

-Name the folder "Files."

Configure Folder Sharing:

-Right-click on the "Files" folder and select "Properties."

-Go to the "Sharing" tab and click "Share...".

-In the "Share" window, click "Add" to add groups or users you want to grant access to. Enter "Designers" and "Developers" (or the corresponding user groups).

-Click "Add," then set the appropriate permissions (e.g., "Full Control" or "Read") for these groups.

-Click "Share," then "Done."

Set NTFS Permissions:

-In the "Properties" window of the "Files" folder, go to the "Security" tab.

-Click "Edit" to adjust the permissions.

-Ensure that only the "Designers" and "Developers" groups have the appropriate permissions to the folder. You can do this by clicking "Add" and entering the group names.

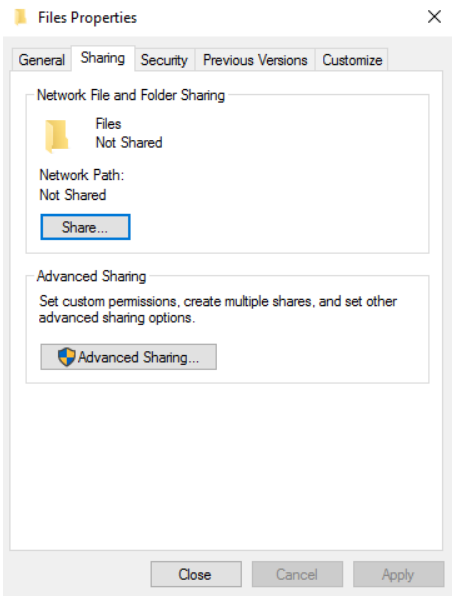
-Grant the appropriate permissions for these groups.

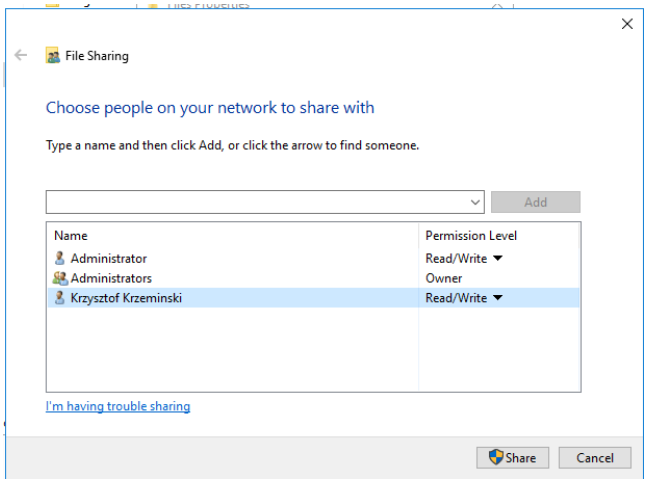
-Click "OK" to save the changes.

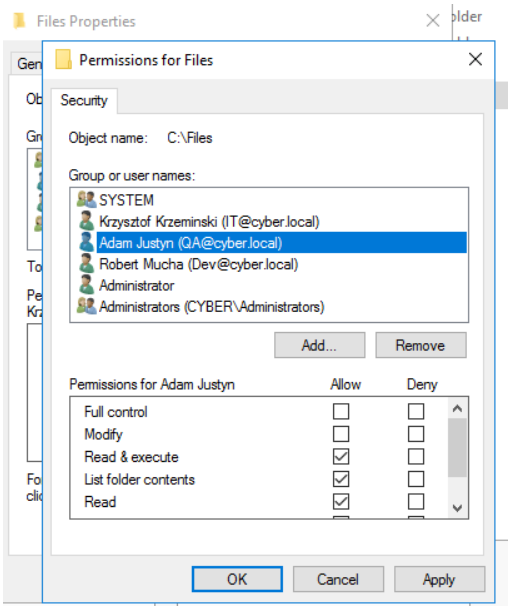
Test Access:

-Log in as a user from the "Designers" or "Developers" group and verify that you can access the "Files" folder and have the correct permissions.

-Ensure that users outside of these groups do not have access to the folder.


Files Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Files
Not Shared
Network Path:
Not Shared
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Close
Cancel
Apply


File Sharing
Choose people on your network to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Name
Permission Level
Administrator
Read/Write
Administrators
Owner
Krzysztof Krzeminski
Read/Write
I'm having trouble sharing
Share
Cancel


Files Properties
Permissions for Files
Security
Object name: C:\Files
Group or user names:
SYSTEM
Krzysztof Krzeminski (IT@cyber.local)
Adam Justyn (QA@cyber.local)
Robert Mucha (Dev@cyber.local)
Administrator
Administrators (CYBER\Administrators)
Add...
Remove
Permissions for Adam Justyn
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply

10.Configure a DHCP server that assigns IP addresses from the pool in the range of10.0.2.120-10.0.2.150.

-Install the DHCP Server Role

-Log in to the Windows Server as an administrator.

Open Server Manager:

-Press Win + R, type servermanager, and press Enter, or click the Server Manager icon on the taskbar.

-Add the DHCP Server Role:

-In Server Manager, click on Add roles and features.

-In the wizard, click Next until you reach the Server Roles section.

-Check the DHCP Server role and click Next.

-Follow the prompts to complete the installation of the role.

Configure the DHCP Server

-Open the DHCP Management Console:

-In Server Manager, click on Tools and select DHCP.

-Start the New Scope Wizard:

-In the DHCP Management Console, right-click on the server name in the left pane and select New Scope.

Go through the New Scope Wizard:

-Scope Name and Description: Provide a name and description for the new scope (e.g., "Client IP Range").

-IP Address Range: Enter the IP address range to be assigned, which is from 10.0.2.120 to 10.0.2.150.

-Subnet Mask: Typically for this range, it will be 255.255.255.0.

-Default Gateway: Enter the IP address of the default gateway if required.

-DNS Servers: Optionally, provide the IP addresses of DNS servers to be assigned to clients.

Configure Scope Options:

-Click Next and configure additional scope options such as lease duration if needed.

-Complete the Scope Configuration:

-Click Finish to complete the wizard.

Activate the Scope:

Ensure that the new scope is activated. Right-click on the scope name in the DHCP console and select Activate if it is not already active.

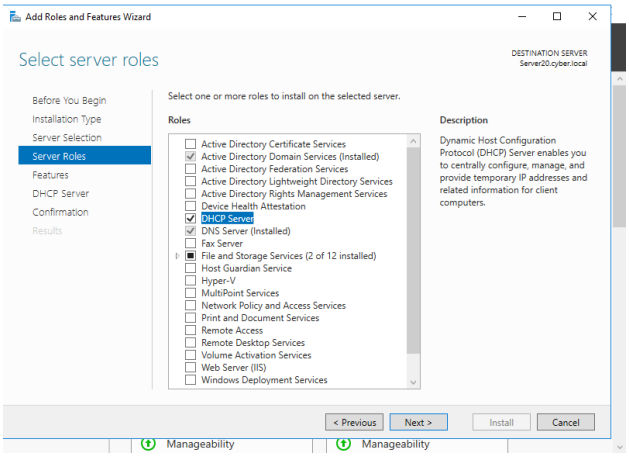
Test the Configuration

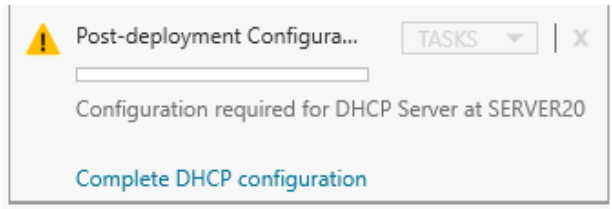
-Check if Clients Receive IP Addresses:

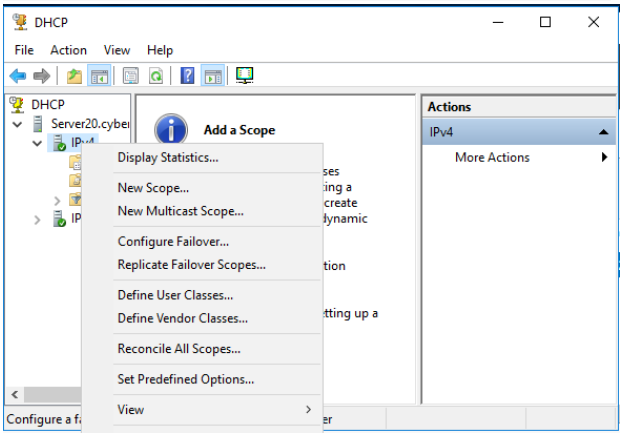
-Connect a computer or other device to the network and verify that it receives an IP address from the range 10.0.2.120 to 10.0.2.150.

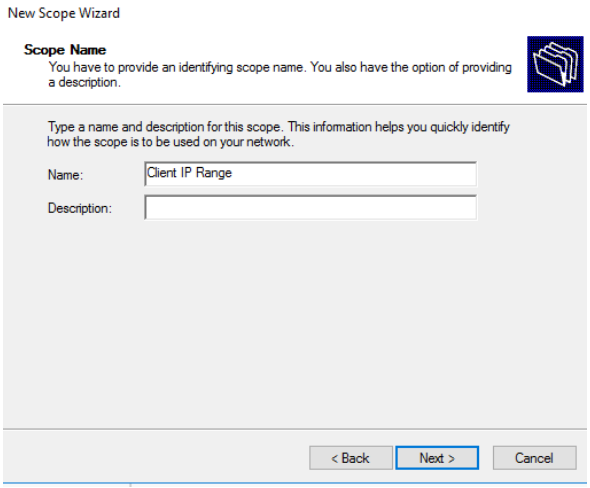
Monitor Logs and Events:

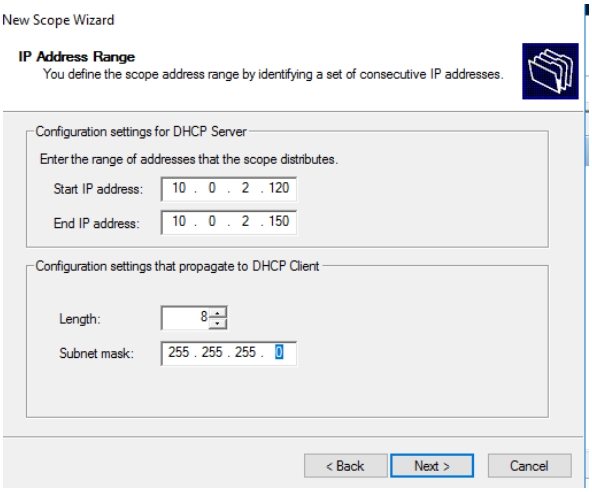
-You can monitor IP address assignments and any issues using the DHCP console and system logs.

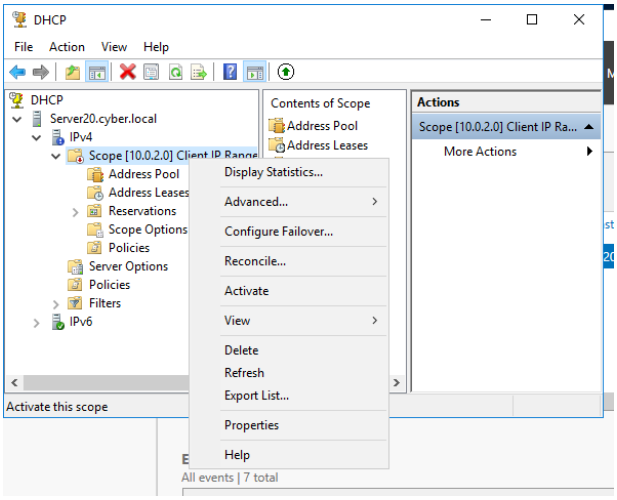


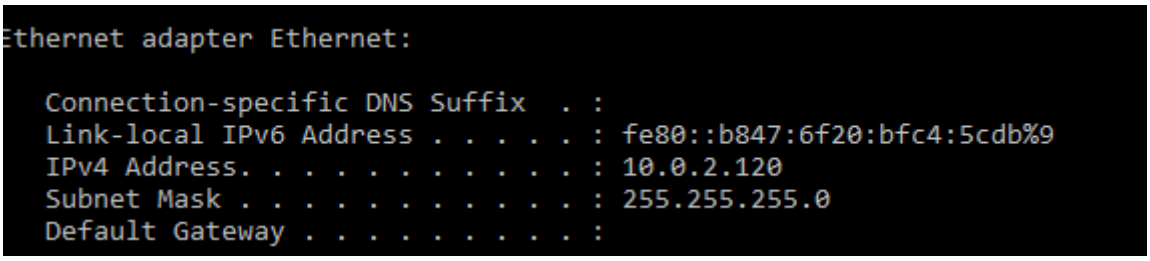





New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
Client IP Range
Description:
< Back
Next >
Cancel


New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address:
10 . 0 . 2 . 120
End IP address:
10 . 0 . 2 . 150
Configuration settings that propagate to DHCP Client
Length:
8
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel


DHCP
File Action View Help
DHCP
Server20.cyber.local
IPv4
Scope [10.0.2.0] Client IP Range
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Contents of Scope
Address Pool
Address Leases
Actions
Scope [10.0.2.0] Client IP Ra...
More Actions
Display Statistics...
Advanced...
Configure Failover...
Reconcile...
Activate
View
Delete
Refresh
Export List...
Properties
Help
Activate this scope
All events | 7 total



11.Create a DNS record that will identify the Windows 10 client machine by the name "Client-A."

Steps to Create a DNS Record

1. **Open DNS Manager**

- On your DNS server, open **DNS Manager**.
- Press Win + R, type dnsmgmt.msc, and press Enter, or

Open **Server Manager**, go to **Tools**, and select **DNS**.

2. **Navigate to the Appropriate Zone**

- In the DNS Manager console, expand the server node.
- Expand the **Forward Lookup Zones** to find the zone where you want to add the record. This will typically be the domain that your Windows 10 client is part of (e.g., example.com).

3. **Create a New A Record**

Right-click on the zone where you want to add the record and select **New Host (A or AAAA)**.

4. **Configure the New Host Record**

- **Name**: Enter the name for the DNS record. In this case, enter Client-A. This will create a record for Client-A.yourdomain.com.
- **IP Address**: Enter the IP address of the Windows 10 client machine that you want to associate with this name.
- **Optional**: Check the box **Create associated pointer (PTR) record** if you want to create a reverse DNS record as well. This will automatically create a PTR record in the reverse lookup zone if it's properly configured.

5. **Save the Record**

- Click **Add Host** to create the record.

You will see a confirmation message that the record was created successfully.

6. **Verify the DNS Record**

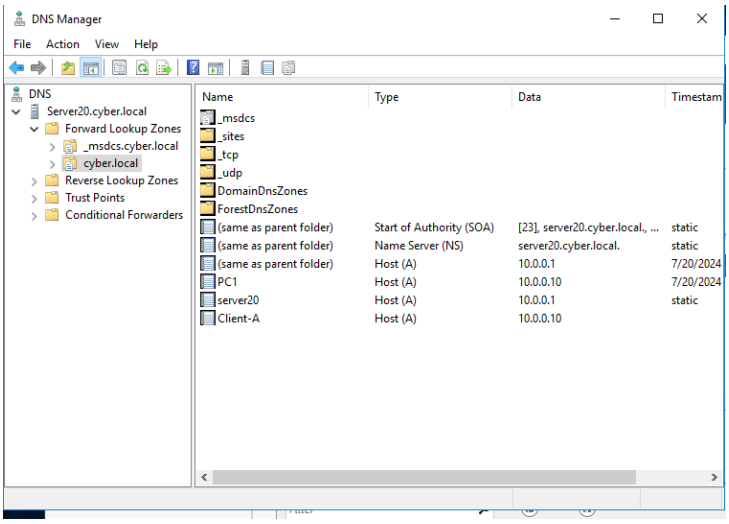
- After creating the record, you can verify it by using the **nslookup** command:

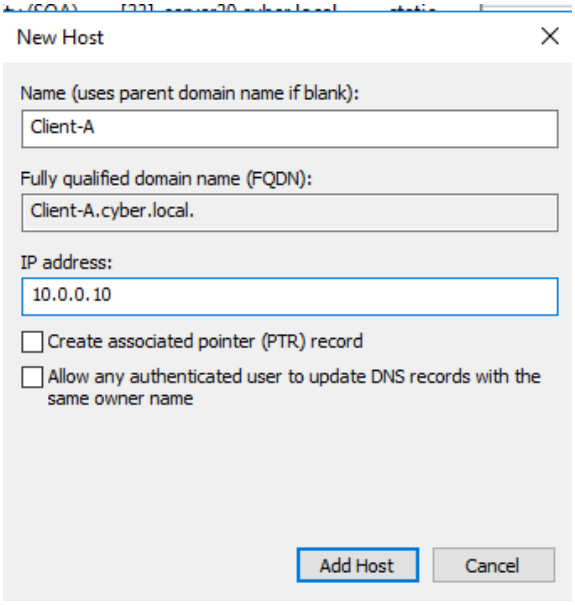
Open Command Prompt (cmd) on any computer.

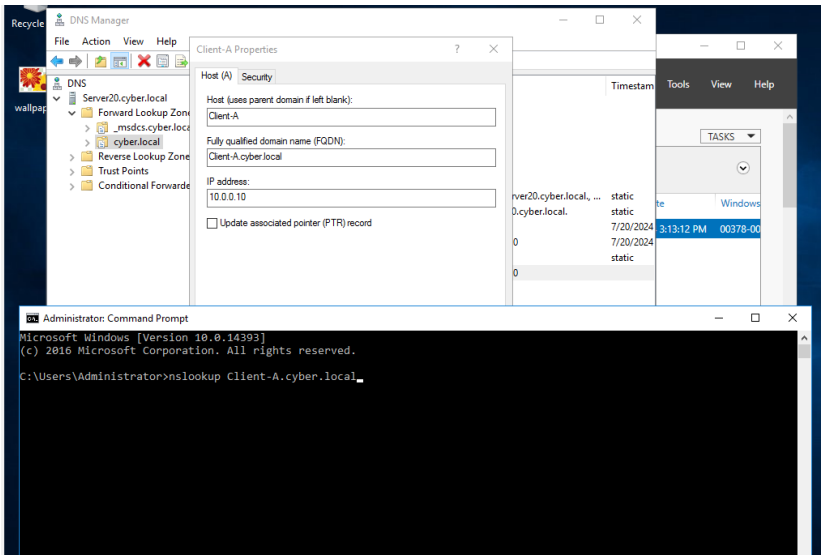
Type nslookup Client-A.yourdomain.com and press Enter.

Verify that the correct IP address is returned.

- You can also use **DNS Manager** to verify that the record appears in the DNS zone and is correctly configured.






Recycle
DNS Manager
File Action View Help
DNS
Server20.cyber.local
Forward Lookup Zone
_msdcs.cyber.local
cyber.local
Reverse Lookup Zone
Trust Points
Conditional Forwarde
Client-A Properties
Host (A)
Security
Host (uses parent domain if left blank):
Client-A
Fully qualified domain name (FQDN):
Client-A.cyber.local
IP address:
10.0.0.10
Update associated pointer (PTR) record
Timestam
Tools View Help
TASKS
rver20.cyber.local., ... static
0.cyber.local. static
7/20/2024
0 7/20/2024
static
0
te Windows
3:13:12 PM 00378-00
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup Client-A.cyber.local