TNE10005 Journal Lab (#1)

Khalid Yaseen Baig / 102763240

What I learned in this week's Lecture.

- Bus Topology refers to a connection, where all devices are connected through a single line, The connection can be easily broken if a computers breaks down in the line.

- Star Topology refers to a connection, where all devices are connected to a central hub/switch/router, This is generally used in our homes, wifi network uses this topology.

- Ring Topology refers to a connection, where the computer is connected to a central device, similar to star topology, the difference is, the routing network is in shape of rings.

- Fully Meshed Topology, where all devices are interconnected together. Its very expensive method but very reliable, quite difficult to administer and expensive to maintain.

- The OSI Layer 1 only sees 1's and 0's. The OSI Layer 2 breaks the 1's and 0's into bytes, and it will assign the meaning based on the location called FRAME.

- The Physical Address operates at Layer2, its burned into device when manufactured (MAC Address). The Logical Address operates at Layer 3, its used by router, its configured by the Network Administrator (IP Address). The Layer 2 and Layer 3 is linked through Address Resolution Protocol(ARP).

- IP Addresses(IPv4) have 32 bits, this gives 4million different possibilities. IP Addresses are hierarchical. Subnetting enables the hierarchy, Administrators use Subnet Masks to Configure Masks to configure devices to place in the hierarchy. A Subnet Mask is all 1's on the left and 0's (in binary) on the right, this mask is used to determine the network, sub-network and host portions of the IP Address.

- Addresses in the Subnet must be connected to the same LAN to Communicate. Communication with other Subnets/Network must be sent to a router.

- An effective Project Manager needs effective soft skills. There are nine areas of Project Management Knowledge:
  1. Integration Management
  2. Scope Management
  3. Time Management
  4. Cost Management
  5. Quality Management
  6. Human Resource Management
  7. Communications Management
  8. Risk Management
  9. Procurement Management

This week’s lab activities.

Hyper-v Minimum Hardware Requirements:

CPU Processor that supports Virtualization technology such as VT-x on Intel CPU or AMD-V on AMD CPU

RAM for installing a Virtual Machine: 4GB

Disk Space 32 GB

Besides hardware what else will be needed before you can both start and complete the installation?

Hyper-V works only on Windows 10 Enterprise, Windows 10 Pro and Windows 10 Education, It does not work on Windows 10 Home Edition. Virtualization needs to be enabled from the bios.

Where can you get these?

If Virtualization is disabled, it can be enabled from the bios. Intel system usually called it Intel Virtual Technology/Intel Virtualization Technology / VT-x / VT-d, AMD usually called it AMD-V, SVM Mode. Windows can be bought or upgraded thru Microsoft store.

- Observe how much RAM has been allocated to this virtual machine: 2048MB
- Which controller has the hard disk attached? SCSI Controller
- What network is the virtual machine attached to: Default Switch

The output for the Ethernet Adapter:

Connection-specific DNS Suffix … : mshome.net

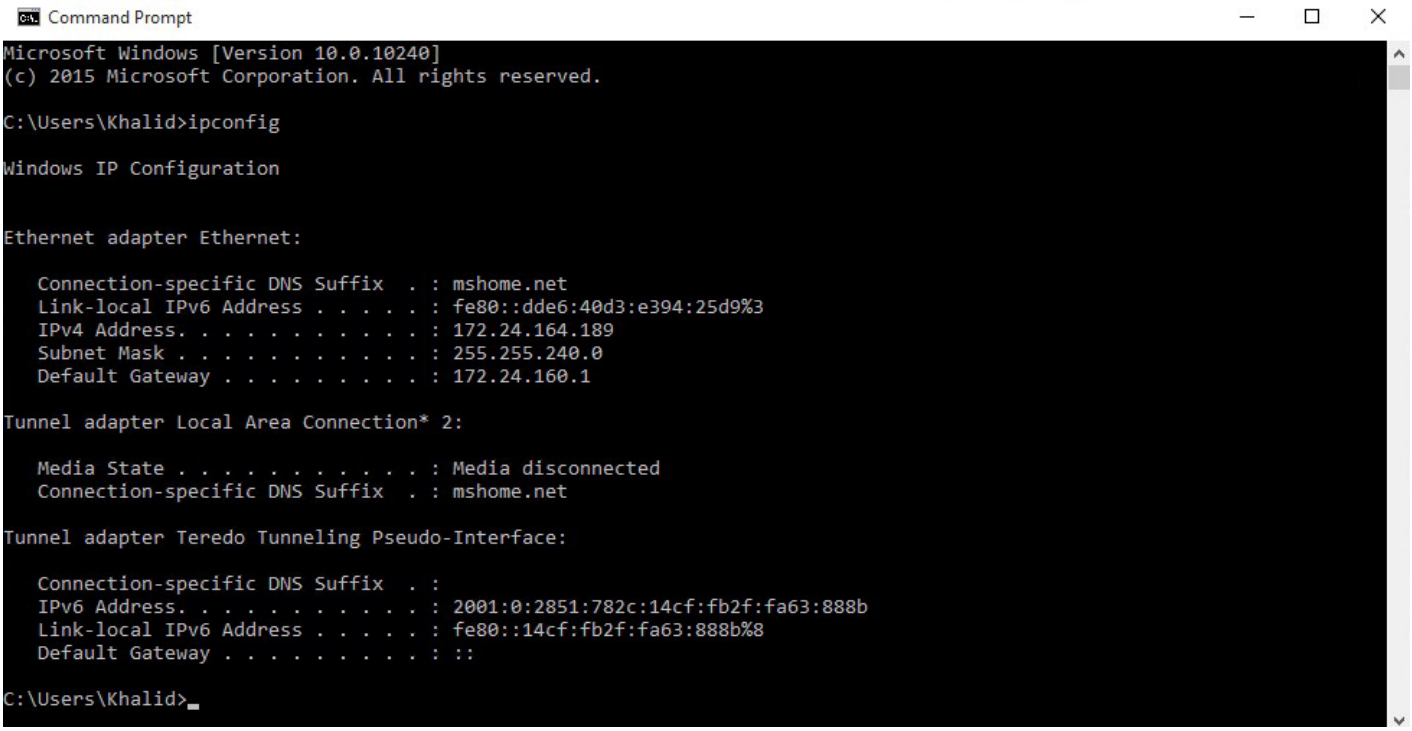
Link-local IPv6 Address ..... : fe80::dde6:40d3:e394:25d9%3

IPv4 Address .....: 172.24.264.189

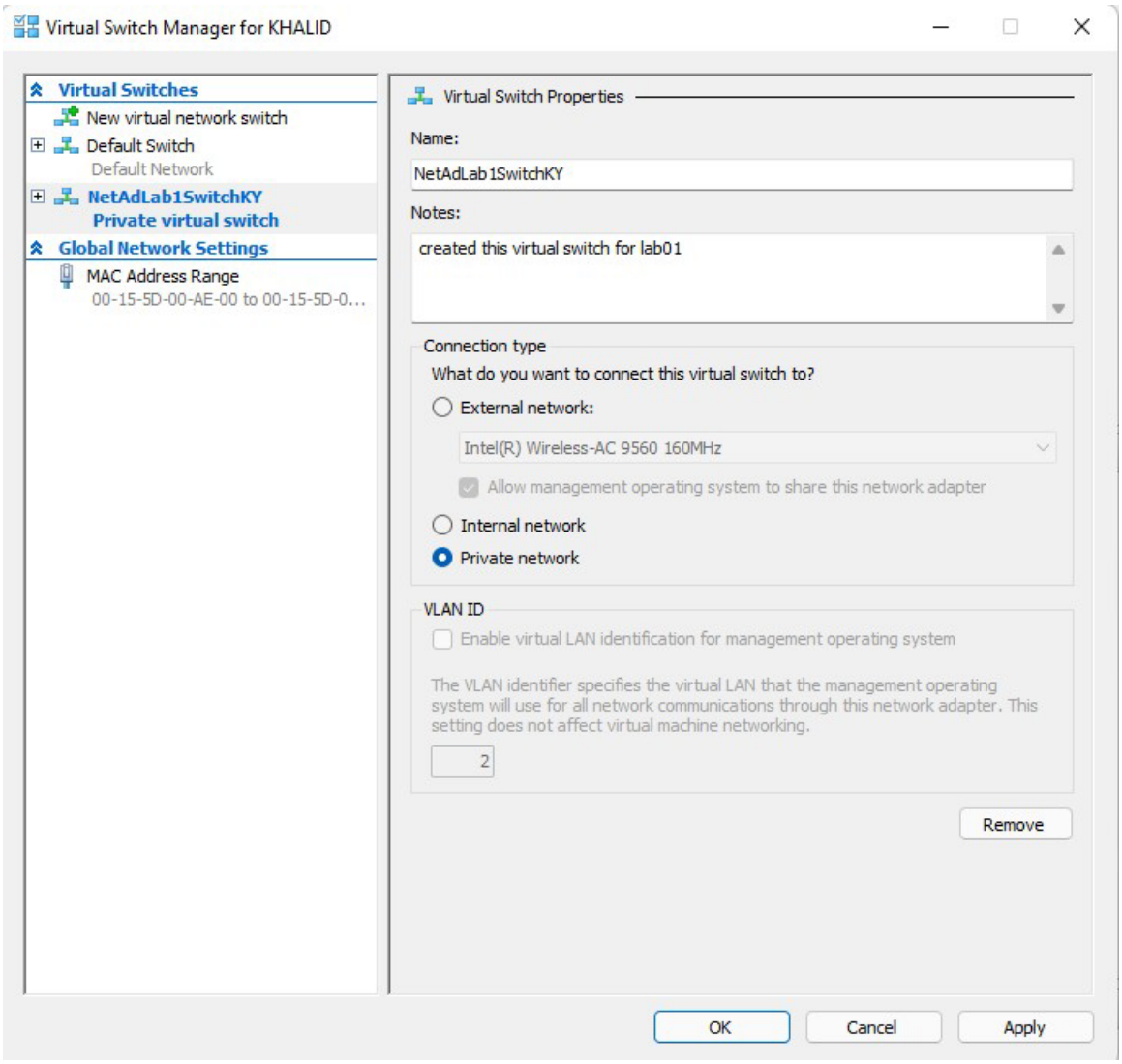
Subnet Mask .....: 255.255.240.0

Default Gateway .....: 172.24.160.1

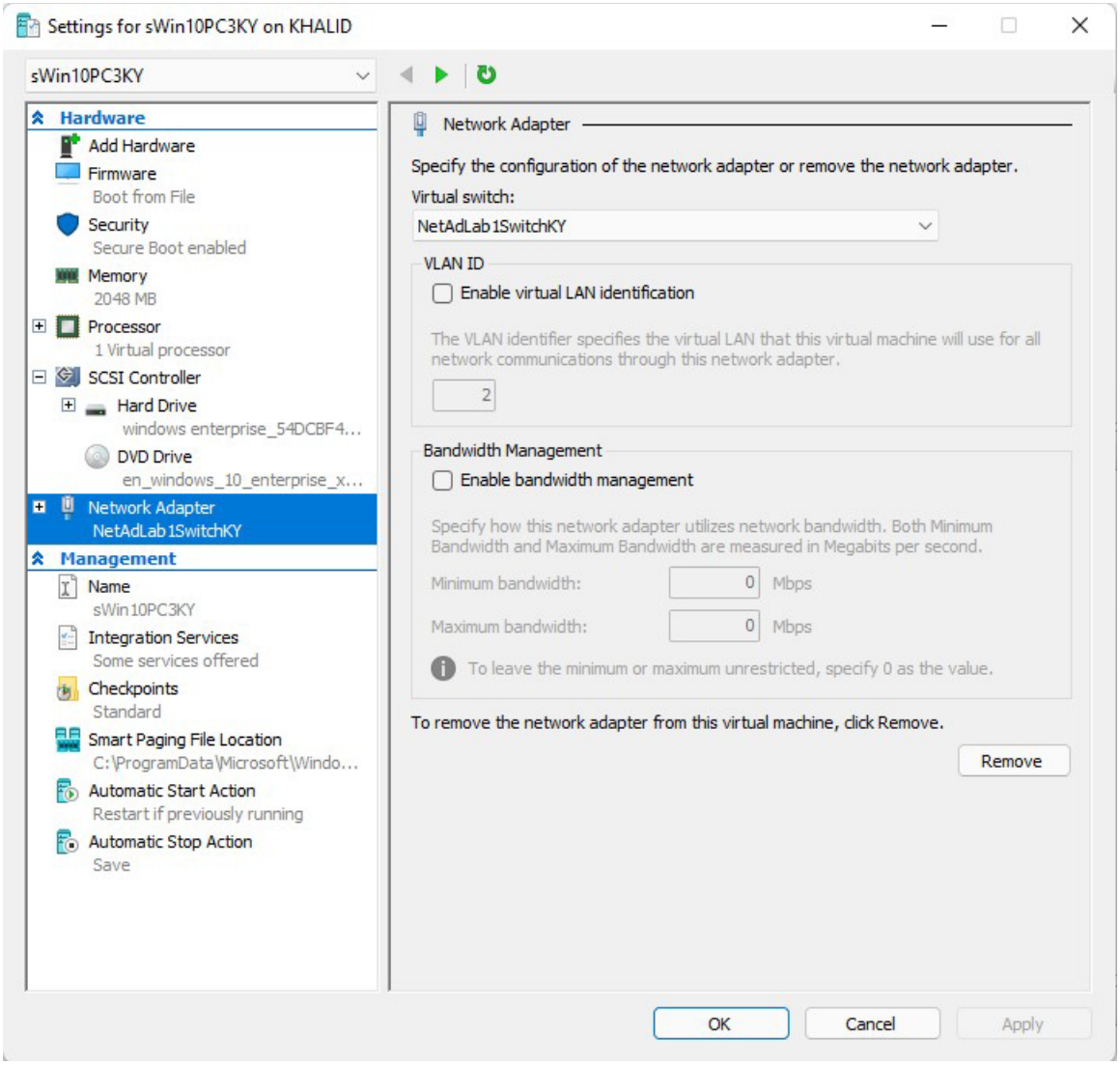
Screenshots of Important Steps Required for Lab.



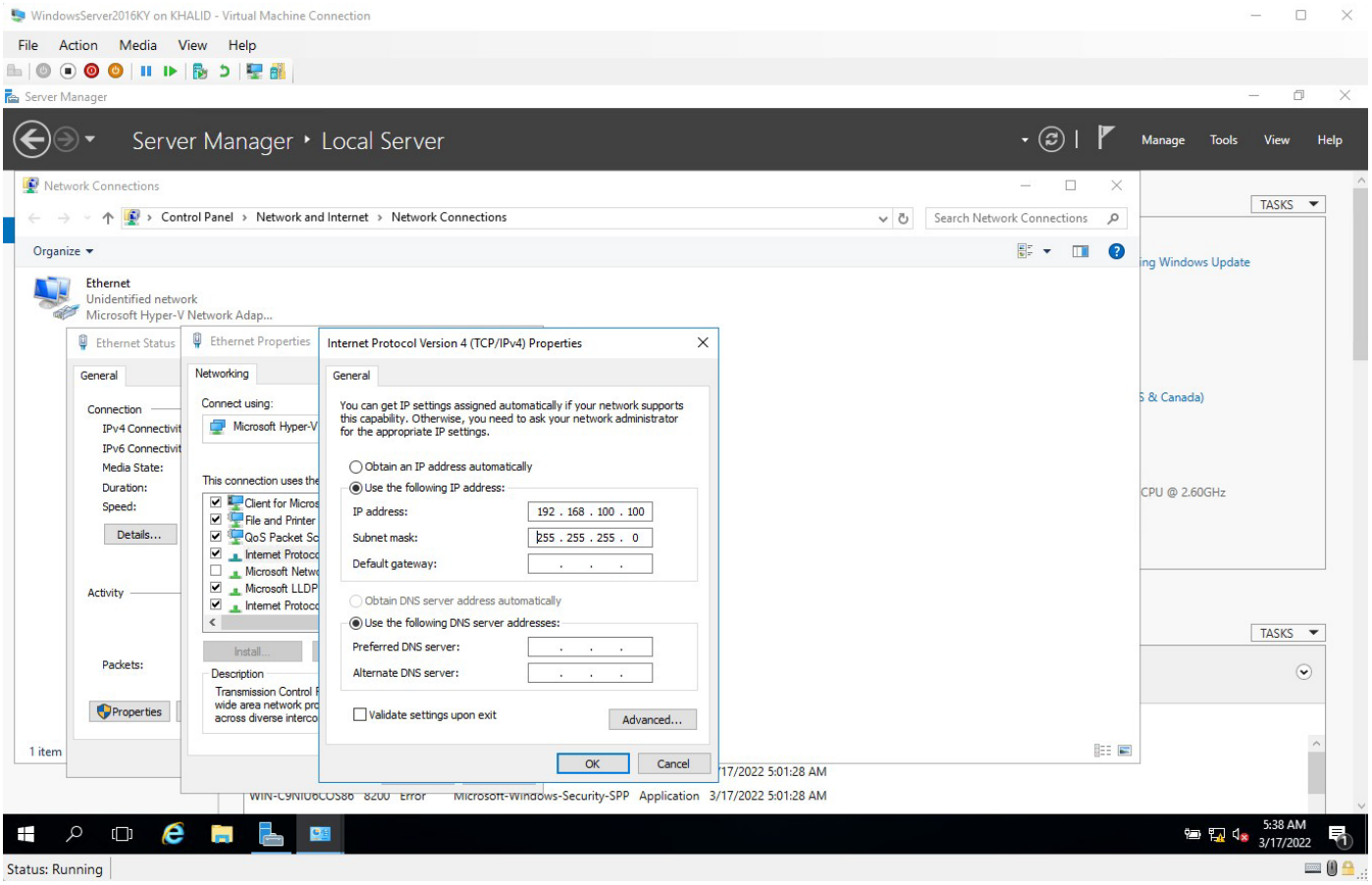
Step # 28 required us to **input Ipconfig in cmd** and **record the Output** from the **sWin10PC3KY** virtual machine, thus this is a screenshot of the Output. The virtual Machine's **Network Adapter** was connected to the **Default Switch** during the Session.



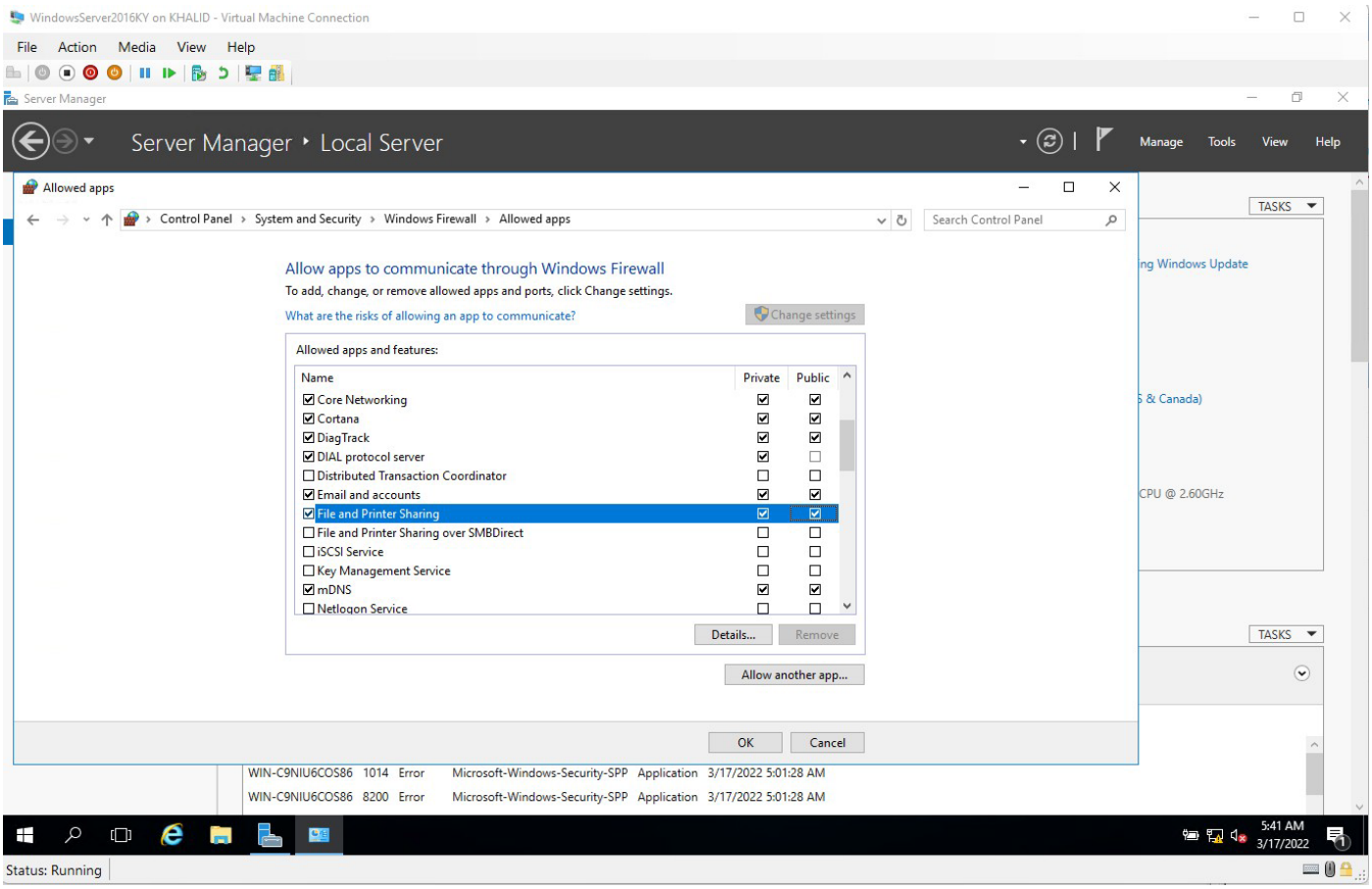
Steps **#31 to #33** required us to Create a Virtual Switch in Hyper-V. Firstly we had to select Virtual Switch Manager from the actions pane of Hyper-V Manager. Then we had to click the button Create Virtual Switch from the Create Virtual Switch Window. Then In the Name Field, **NetAdLab1SwitchKY** had to be entered and we had to configure the connection type to be private.



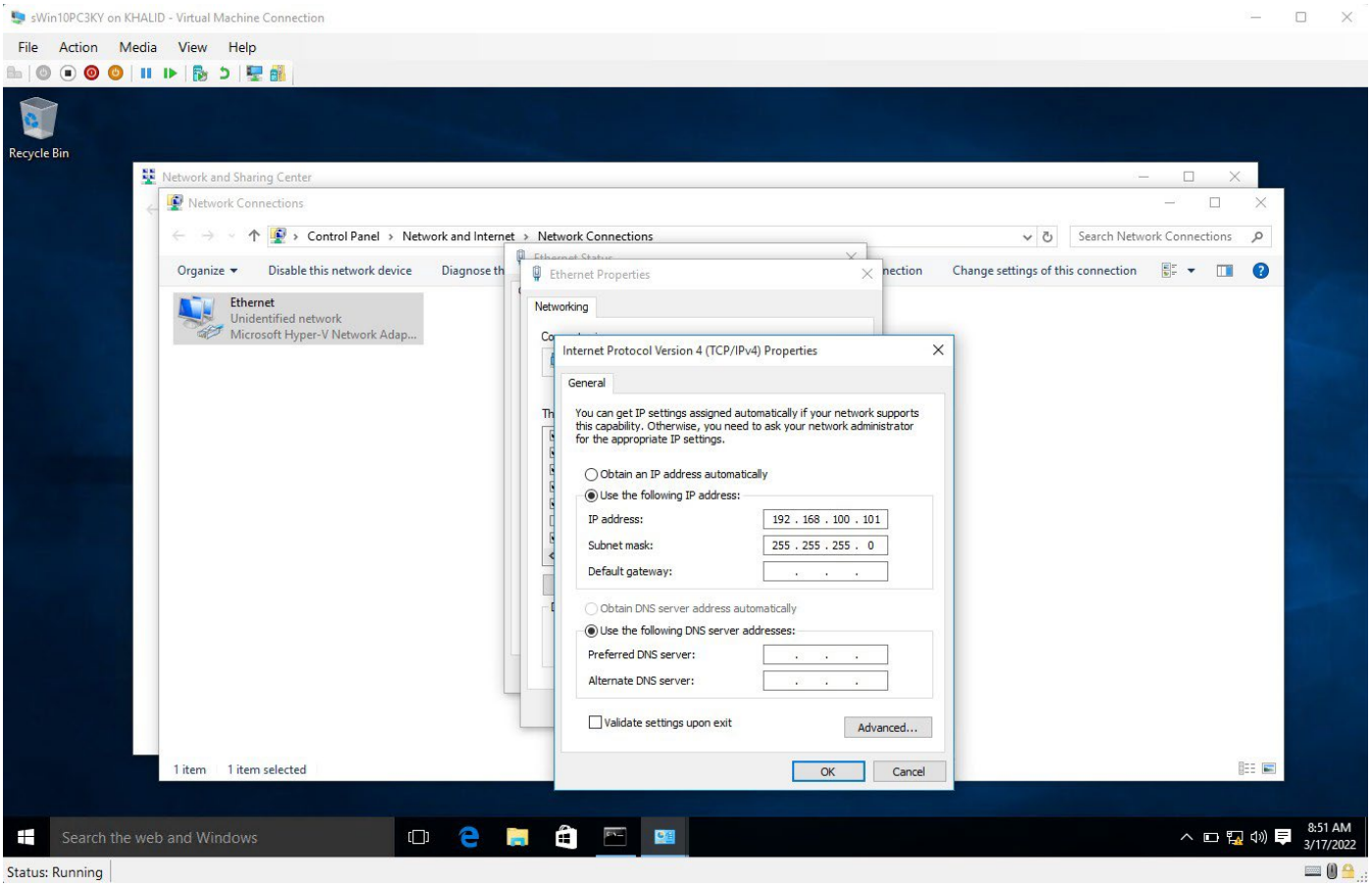
Step **#34** required us to Change the **Network Adapter Configuration** of **sWin10PC3KY** to **NetAdLab1SwitchKY** from the Default Switch.



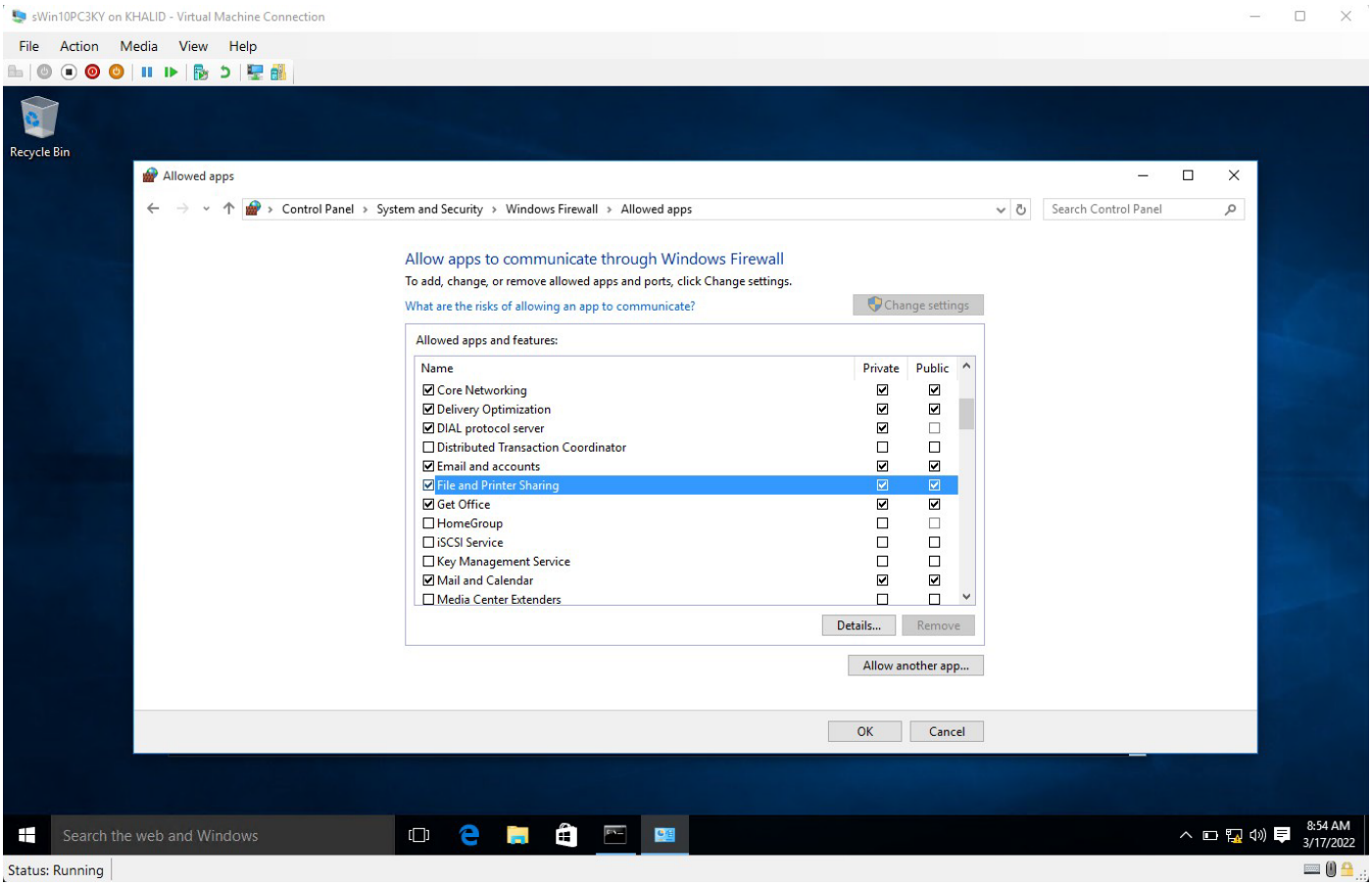
Steps **#57** to **#59** required us to **configure the IP Address** to **192.168.100** and the **Subnet Mask** to **255.255.255.0 .** It was done on **the WindowsServer2016KY** Virtual Machine. we had to Click Locqal Server, Below the properties section Click the Link next to Ethernet and Select Properties. Then Click on Internet Protocol Version 4(TCP/IPv4), and select the properties button. And then Configure the IP Address and the Subnet Mask.



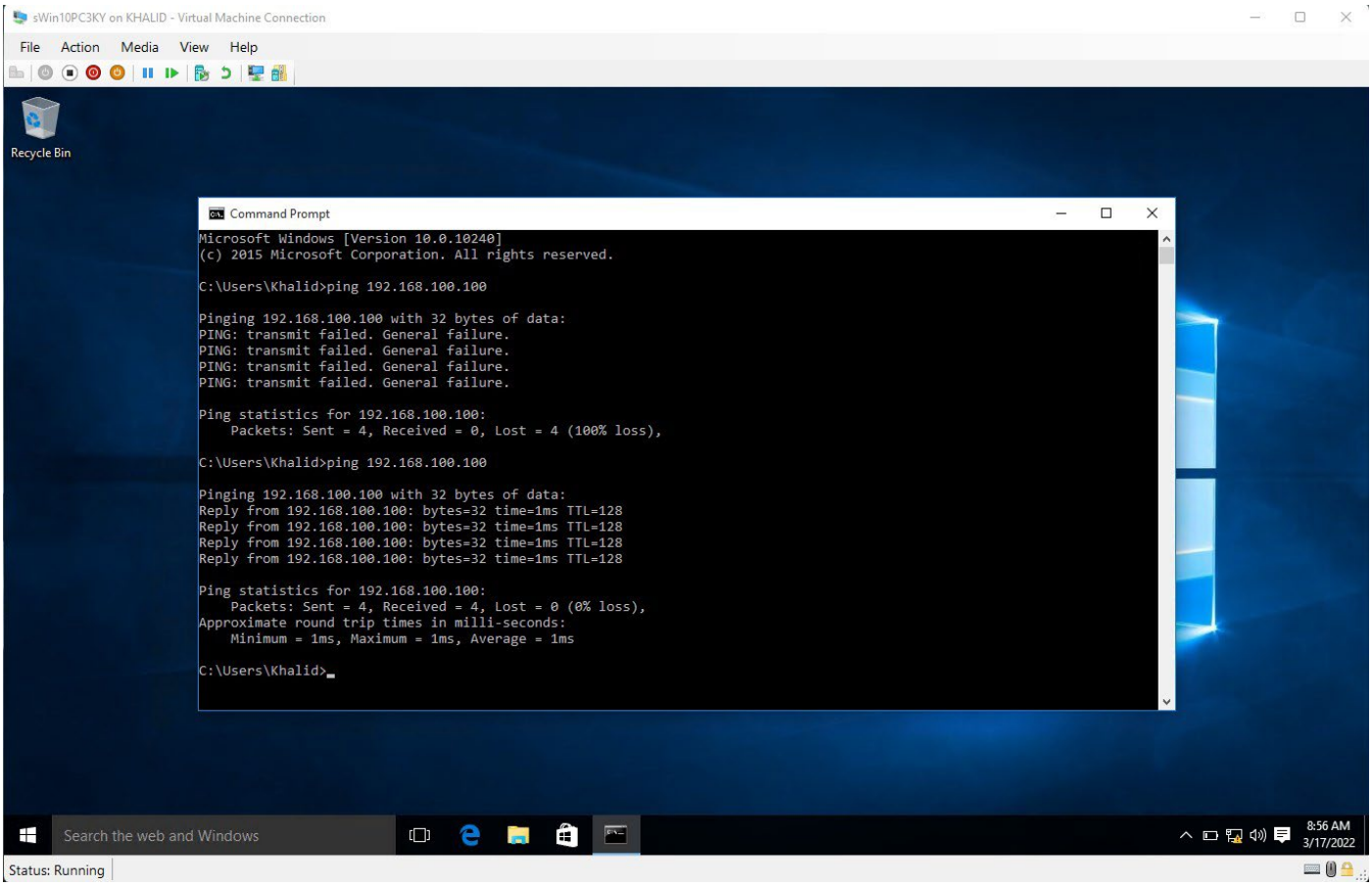
Step **#60** required us to **prepare for testing** after configuring IP Address. It was done on **the WindowsServer2016KY** Virtual Machine. We had to go to Systems and Security from the Control Panel, then Windows Firewall. Then Click Allow and App or Feature thru Windows Firewall. Then Click the check boxes next **to File and Printer Sharing** under the Private and Public Columns.



We had to repeat **Steps #58 and #59** for **sWIn10PC3KY Virtual Machine** and **Configure the IP Address** to **192.168.100.101** and **the Subnet Mask** to **255.255.255.0** like we did above on the **WindowsServer2016KY** Virtual Machine, so both of the Virtual Machines can **communicate with each other**.



We had to **repeat Step #60** for **sWin10PC3KY Virtual Machine** as we did with **WindowsServer2016KY Virtual Machine**. In order to **Prepare for testing** after configuring the IP Address, so that both the Virtual Machines can **Communicate with each other**.



Step **#48** Required us to verify if there is a **successful Connection between the Two Virtual Machines**. It was done by launching cmd from **sWin10PC3KY** Virtual Machine and typing **ping 192.168.100.100**, which is the **IP Address of the WindowsServer2016KY** virtual Machine, and there was a **successful reply from 192.168.100.100** which **verifies** that there is a **successful connection between the two virtual Machines**.

TNE10005 Journal Lab (#2)

Khalid Yaseen Baig / ID #102763240

What I learned in this week's Lecture.

- There are ten areas of Product Management, i. Integration Management, ii. Scope Management, iii. Time Management, iv. Cost Management, v. Quality Management, vi. Human Resource Management, vii. Communications Management, viii. Risk Management, ix. Procurement Management, x. Stakeholder Management.

- There are different styles of projects, ie. Agile, Iterative and Hybrid Projects. The 10 PMBOK knowledge areas are useful for larger predictive projects, where the aspects of project such as goals etc are predetermined. Agile Project changes overtime with situation and requirements of the project. The most common method used is Hybrid project management with predictive strategies used for the overall project and agile strategies for the sub-projects.

- Project Integration Management involves coordinating the other eight PMBOK areas throughout the project's lifetime, It especially involves identifying and communicating with the project's Key Stakeholders. Key stakeholders have a role in making decisions in the project. They tend to be specialised in areas of feasibility related to the project

- Project Quality Management system, makes sure the profuct is upto set standard by having certifications like iso 9001 etc.

- Project Human Resource Managemnt implies that personals with appropriate skills required for the Project should be hired after careful consideration and after procurement, appropriate tasks should be alloted and the individual should be accordingly motivated to do the tasks.

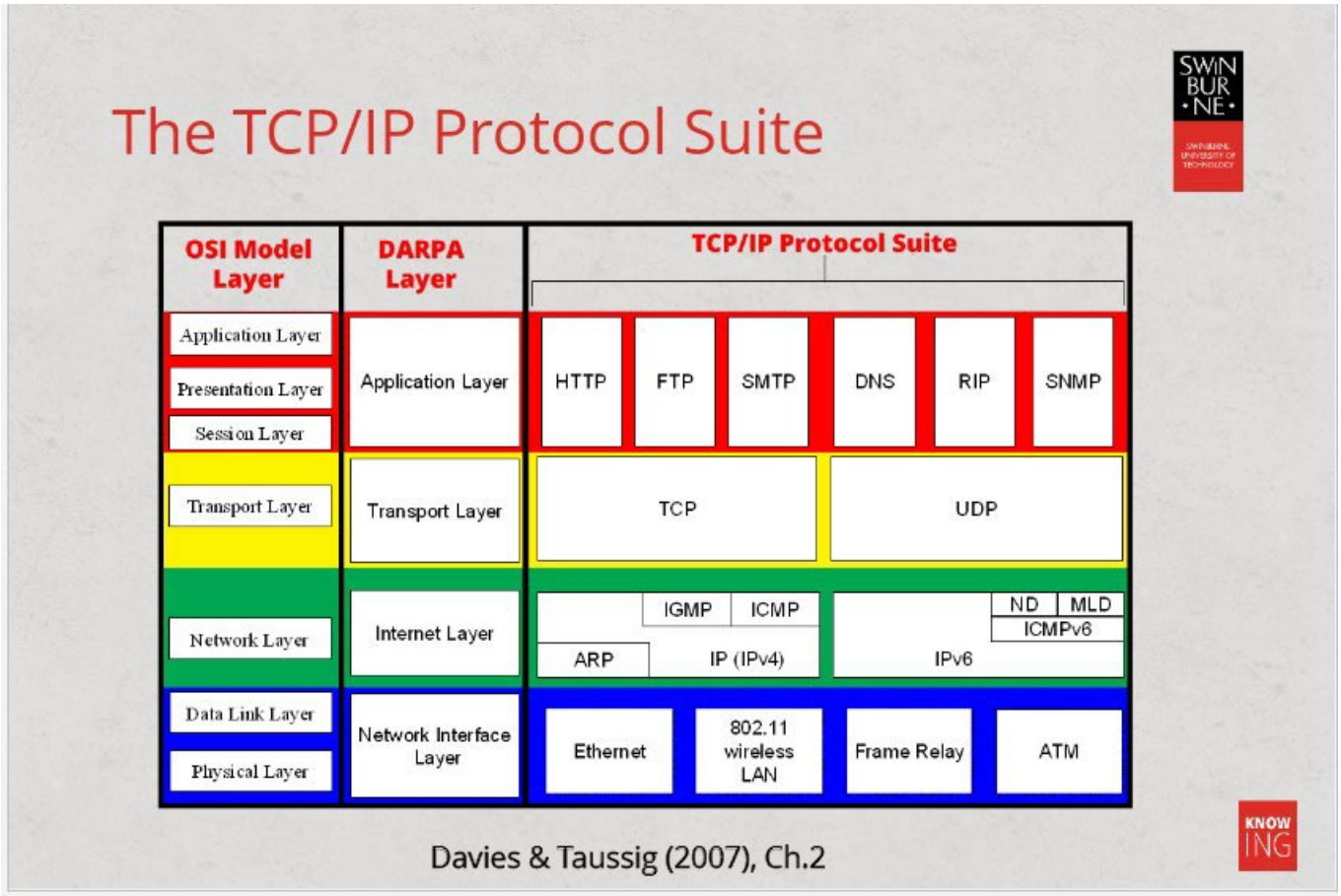
- Project Communications Management implies that proper communication should be maintained following the hierachy for efficient and effective completion of the project,

- Project risk management include thorough assessment of the IMPACT that the occurrence of a certain risk would have on the project, as well as the LIKELIHOOD or chance that a certain risk would occur over the project's lifetime. Using a combination of these criteria, we

prioritize the risks and then implement ways to REDUCE the likelihood of the risks occurring and the resulting harm.

- Project Procurement Management guarantees that your procurement processes are ali gned with those of your clients, and that procurement decisions are made in the proper se quence. Procurement management also deals with contracts.

- You limit hardware purchases to pre-approved models and limit the number of models permitted to a number of categories in a standard operating environment. These are usually from the same manufacturer, which improves computer compatibility and allows for disk image cloning. Vendors promise to keep certain models in production for a set amount of time.

- 

- A socket is a combination of an IP address, a transport protocol, and a port number. Devices must be in the same subnet to communicate in the same LAN, Thus an IP address and a Subnet Mask must be configured at a minimum. In order to communicate with other subnets a router must be used, Thus a default gateway address must be configured in order to communicate outside the local LAN.

Logical Address Constraints

- **224.0.0.0 – 239.255.255.255** are reserved for **multicast** purposes
- **240.0.0.0 – 255.255.255.254** are reserved for IETF **research** purposes
- **127.0.0.1 – 127.255.255.255** is reserved for **this device** (loopback address)
- **255.255.255.255** is reserved for **all devices** (universal broadcast address)
- **First address and last address of each subnet**
  e.g. for the subnet 136.186.0.0, 255.255.0.0
  136.186.0.0 is the network ID for this subnet
  136.186.255.255 is the broadcast address for this subnet
- **Private IP addresses** – are addresses reserved for private networks, and cannot be used for internet traffic (*note: NAT provides a work around)*
  - 10.0.0.0 – 10.255.255.255 – Class A
  - 172.16.0.0 – 172.31.255.255 – Class B
  - 192.168.0.0 – 192.168.255.255 – Class C
- **Automatic private IP addresses** (APIPA) 169.254.0.0 – 169.254.255.255
- If you want a server to host a resource (e.g. web page) from anywhere on the internet you must allocate the server a **PUBLIC IP address.**

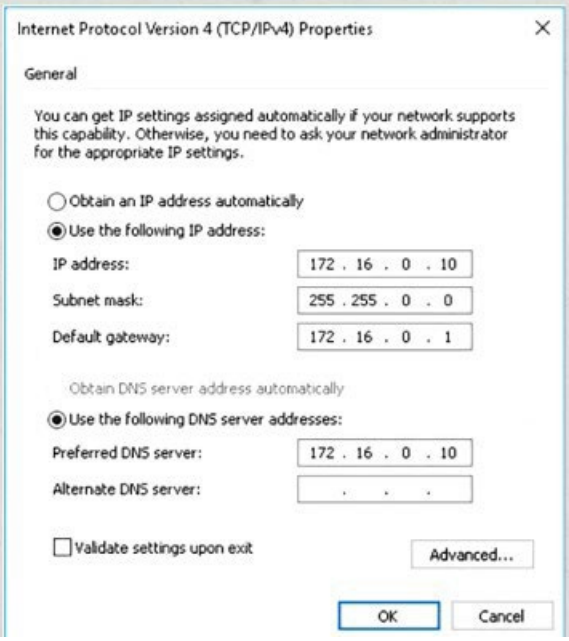
Generally speaking a Public IP address is an address that is not constrained by the other rules on this slide.

- Benefits of Using Subnetting include Using a single network address across multiple locations, Reduce network congestion by segmenting traffic, ncrease security by using firewalls to separate subnets.

Calculating Subnet ID and Subnet Broadcast Address

Address	172	.	16	.	255	.	1
Mask	255	.	255	.	0	.	0
Add.Bin	10101100	.	00010000	.	11111111	.	00000001
Msk.Bin	11111111	.	11111111	.	00000000	.	00000000
And	10101100	.	00010000	.	00000000	.	00000000
Result	172	.	16	.	0	.	0
Host portion all 0's	10101100	.	00010000	.			
Subnet ID	172	.	16	.			
Host portion all 1's	10101100	.	00010000	.			
Broadcast	172	.	16	.			

Configuring IPv4 Manually



Using PowerShell:

```
New-NetIPAddress –InterfaceAlias
“Ethernet” –IPAddress
172.16.16.10 –PrefixLength 20
–DefaultGateway 172.16.16.1
```

IPv4 Troubleshooting Tools

Tool	Description
Arp	Allows you to view and edit the Address Resolution Protocol (ARP) cache. The ARP cache maps IPv4 addresses to media access control (MAC) addresses. Windows uses these mappings to send data on the local network.
Hostname	Displays the host name of the computer.
Ipconfig	Displays current TCP/IP configuration values for both IPv4 and IPv6. Also used to manage DHCP configuration and the DNS client resolver cache.
Netsh	Displays and allows you to administer settings for IPv4 or IPv6 on either the local computer or a remote computer.
Netstat	Displays statistics and other information about current IPv4 and IPv6 connections.
Nslookup	Queries a DNS server.
Ping	Tests IPv4 or IPv6 connectivity to other IP nodes.
Route	Allows you to view the local IPv4 and IPv6 routing tables and to modify the local IPv4 routing table.
Tracert	Traces the route that an IPv4 or IPv6 packet takes to a destination.
Pathping	Traces the route that an IPv4 or IPv6 packet takes to a destination and displays information on packet losses for each router and subnet in the path.

- Tracert' is like a sequence of increasing pings that helps to map out the path our data travels in. It helps us to identify where along that path the connection may be down.

Troubleshooting Utilities

No.	Layer	Purpose	Datagram/PDU	Device	Protocol	Troubleshooting
7	Application	Network services to user				telnet
6	Presentation	Translates data formats				
5	Session	Establishes, manages, and terminates sessions between end hosts				
4	Transport	Reliable transit of data between end hosts	Segment			
3	Network	Path selection between end hosts	Packet	Router		ing, traceroute, ipconfig, print route
2	Data-link	Reliable transit over physical link	Frame	Bridge/Switch	Ethernet, MAC	arp*, ipconfig* (not a L2 utility, but provides L2 information)
1	Physical	Specifications of cables, voltages, etc	Bit	Repeater/Hub		Lights/Indicators

Work from the bottom up

This week's lab activities.

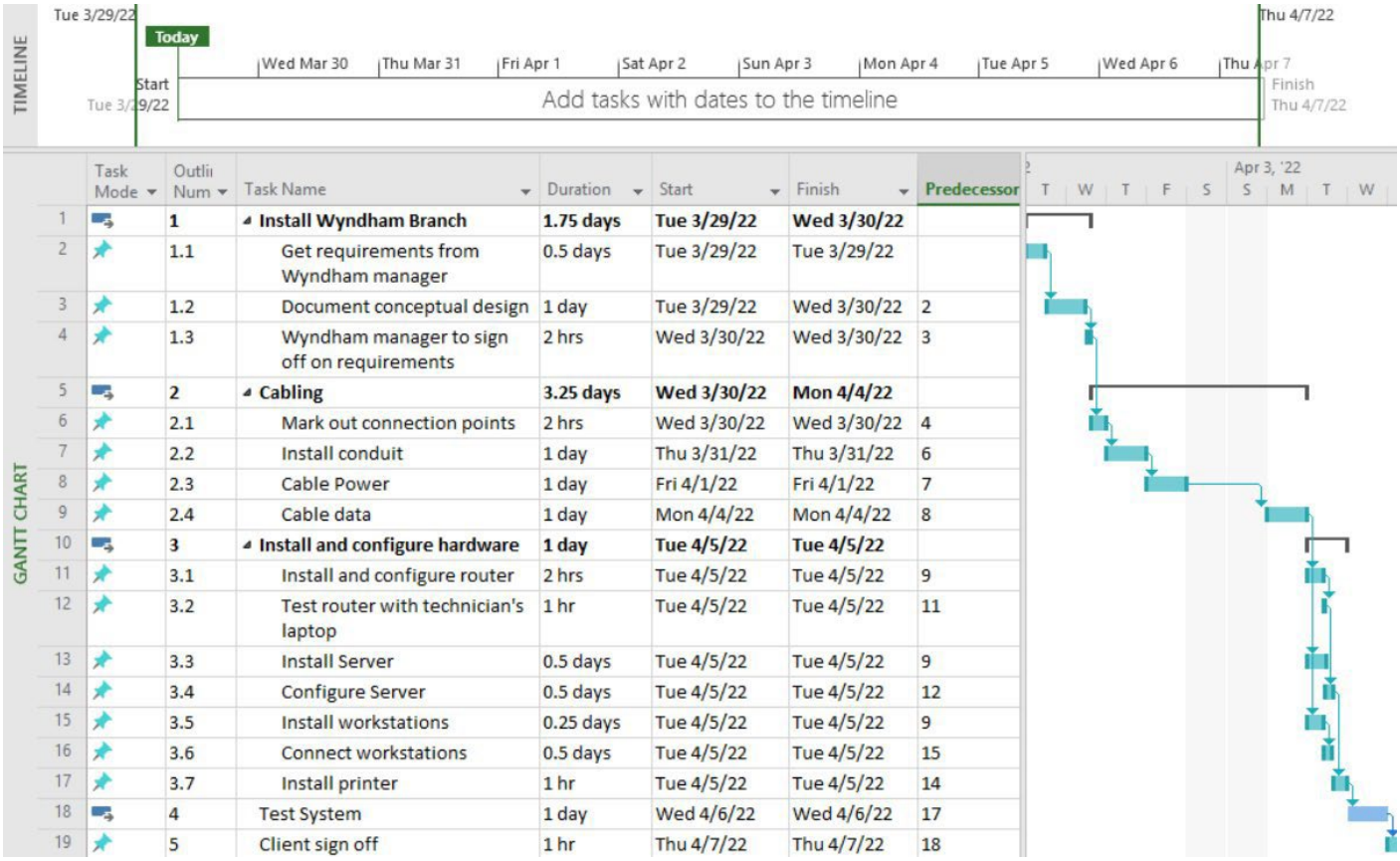
- **Creating a work Breakdown Structure**

GANTT CHART

	Task Mode	Outline Number	Task Name	Duration	Start	Finish	Predecessors
1		1	**Install Wyndham Branch**	**1 day**	**Tue 3/29/22**	**Tue 3/29/22**	
2		1.1	Get requirements from Wyndham manager	0.5 days			
3		1.2	Document conceptual design	1 day			
4		1.3	Wyndham manager to sign off on requirements	2 hrs			
5		2	**Cabling**	**1 day**	**Tue 3/29/22**	**Tue 3/29/22**	
6		2.1	Mark out connection points	2 hrs			
7		2.2	Install conduit	1 day			
8		2.3	Cable Power	1 day			
9		2.4	Cable data	1 day			
10		3	**Install and configure hardware**	**0.5 days**	**Tue 3/29/22**	**Tue 3/29/22**	
11		3.1	Install and configure router	2 hrs			
12		3.2	Test router with technician's laptop	1 hr			
13		3.3	Install Server	0.5 days			
14		3.4	Configure Server	0.5 days			
15		3.5	Install workstations	0.25 days			
16		3.6	Connect workstations	0.5 days			
17		3.7	Install printer	1 hr			
18		4	**Test System**	**0.13 days**	**Tue 3/29/22**	**Tue 3/29/22**	
19		4.1	Client sign off	1 hr			

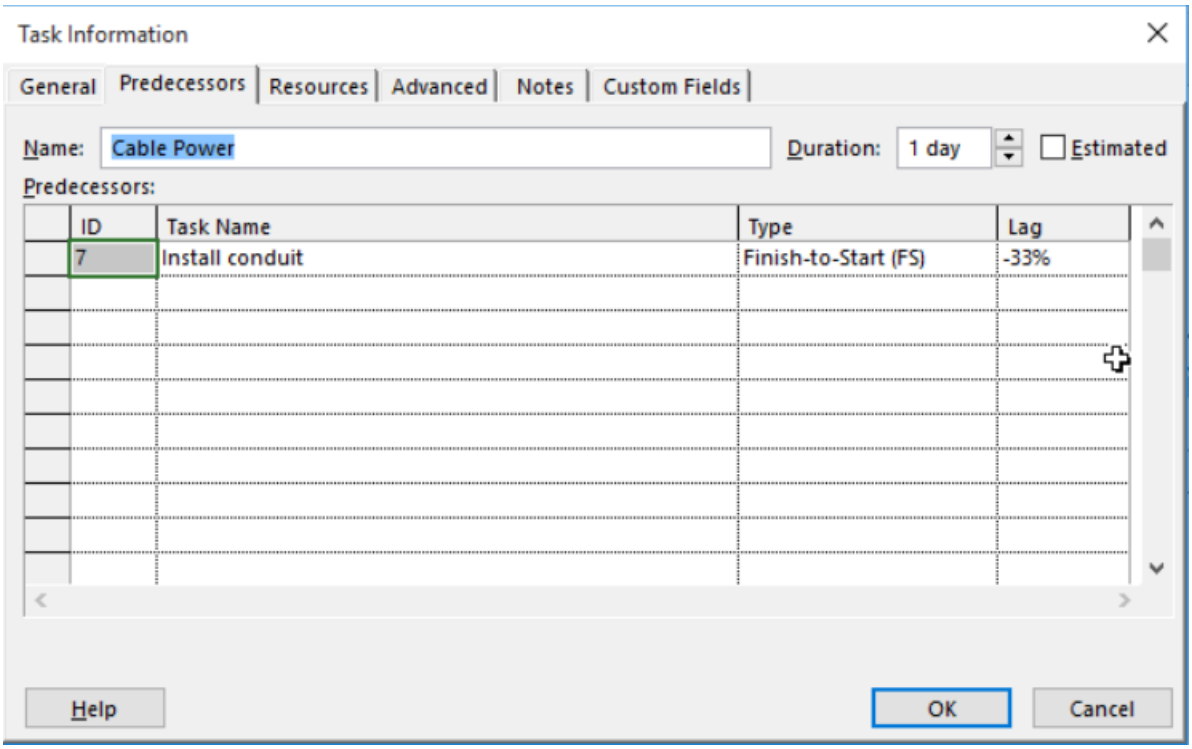
Steps #6 to #18 guided us in filling out the **Task Names column** in **MS PROJECT**, and then further organize the tasks into **sub-tasks** by highlighting the sub-tasks and clicking the right arrow button from the Task Tab. Then Numbering system was applied for Tasks and Sub-tasks as it would be more effective for communication purposes, it was enabled by selecting Insert column after right clicking the Task Name column header, then searching for **Outline Number**. Then **Tasks #15 - #17** further guided us in including **estimated duration for each task**, it was achieved by entering the duration in the **'Duration' column.** Finally, the above figure was achieved.

- **Creating a Gantt Chart**

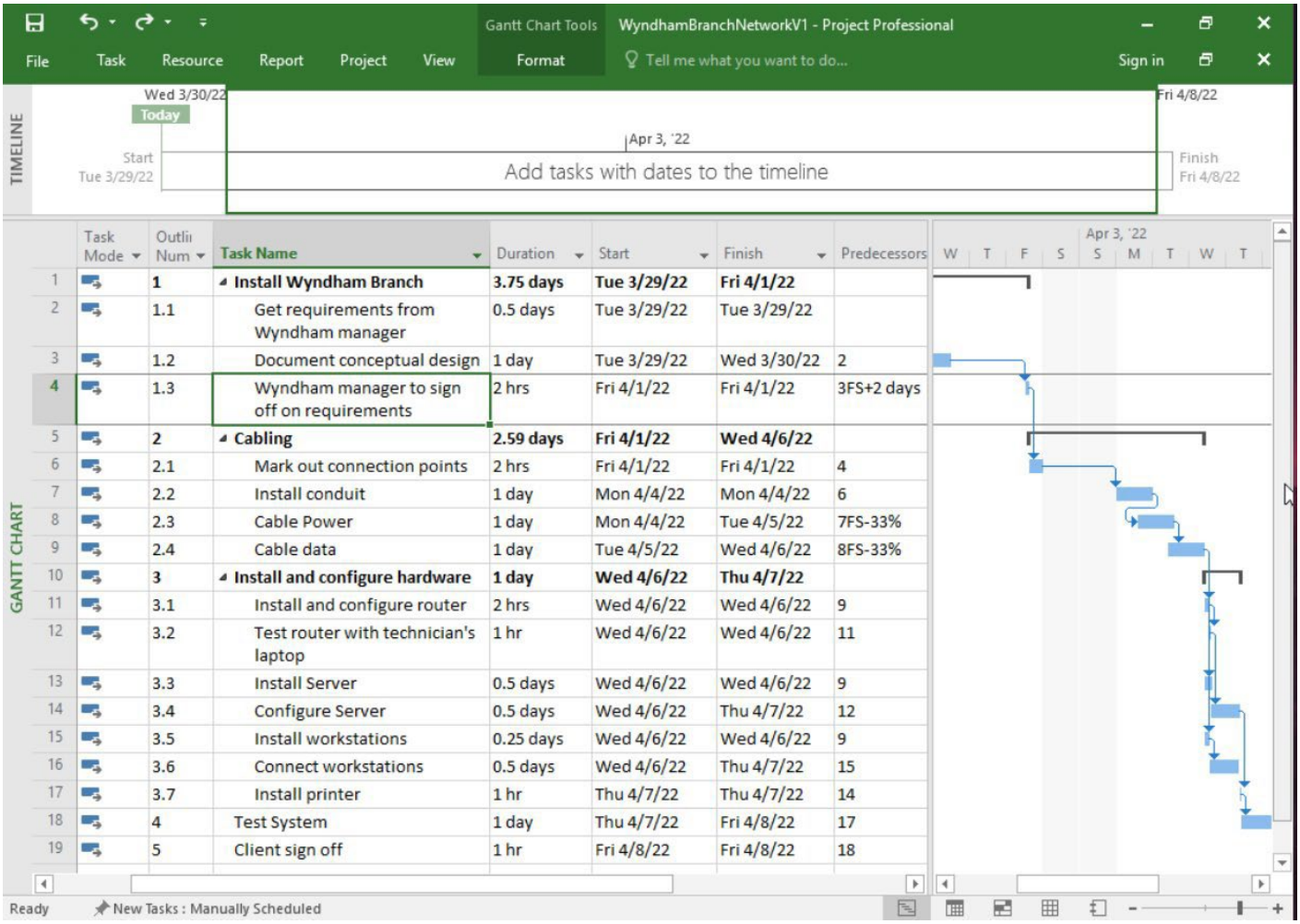


	Task Mode	Outli Num	Task Name	Duration	Start	Finish	Predecessor
1		**1**	**Install Wyndham Branch**	**1.75 days**	**Tue 3/29/22**	**Wed 3/30/22**	
2		1.1	Get requirements from Wyndham manager	0.5 days	Tue 3/29/22	Tue 3/29/22	
3		1.2	Document conceptual design	1 day	Tue 3/29/22	Wed 3/30/22	2
4		1.3	Wyndham manager to sign off on requirements	2 hrs	Wed 3/30/22	Wed 3/30/22	3
5		**2**	**Cabling**	**3.25 days**	**Wed 3/30/22**	**Mon 4/4/22**	
6		2.1	Mark out connection points	2 hrs	Wed 3/30/22	Wed 3/30/22	4
7		2.2	Install conduit	1 day	Thu 3/31/22	Thu 3/31/22	6
8		2.3	Cable Power	1 day	Fri 4/1/22	Fri 4/1/22	7
9		2.4	Cable data	1 day	Mon 4/4/22	Mon 4/4/22	8
10		**3**	**Install and configure hardware**	**1 day**	**Tue 4/5/22**	**Tue 4/5/22**	
11		3.1	Install and configure router	2 hrs	Tue 4/5/22	Tue 4/5/22	9
12		3.2	Test router with technician's laptop	1 hr	Tue 4/5/22	Tue 4/5/22	11
13		3.3	Install Server	0.5 days	Tue 4/5/22	Tue 4/5/22	9
14		3.4	Configure Server	0.5 days	Tue 4/5/22	Tue 4/5/22	12
15		3.5	Install workstations	0.25 days	Tue 4/5/22	Tue 4/5/22	9
16		3.6	Connect workstations	0.5 days	Tue 4/5/22	Tue 4/5/22	15
17		3.7	Install printer	1 hr	Tue 4/5/22	Tue 4/5/22	14
18		4	Test System	1 day	Wed 4/6/22	Wed 4/6/22	17
19		5	Client sign off	1 hr	Thu 4/7/22	Thu 4/7/22	18

Steps #19 to #23 familiarized us to the **Gantt chart**, the **bars in the Gantt chart** indicated when each **task is going to occur**. Initially all the bars were aligned in a single column as Tasks were not sequenced yet. The Task were **sequenced by entering a Predecessor for each task** in the Predecessor column. After entering the prescribed Predecessor for each task, the bars were **appropriately aligned in the Gantt chart** as shown in the above figure.

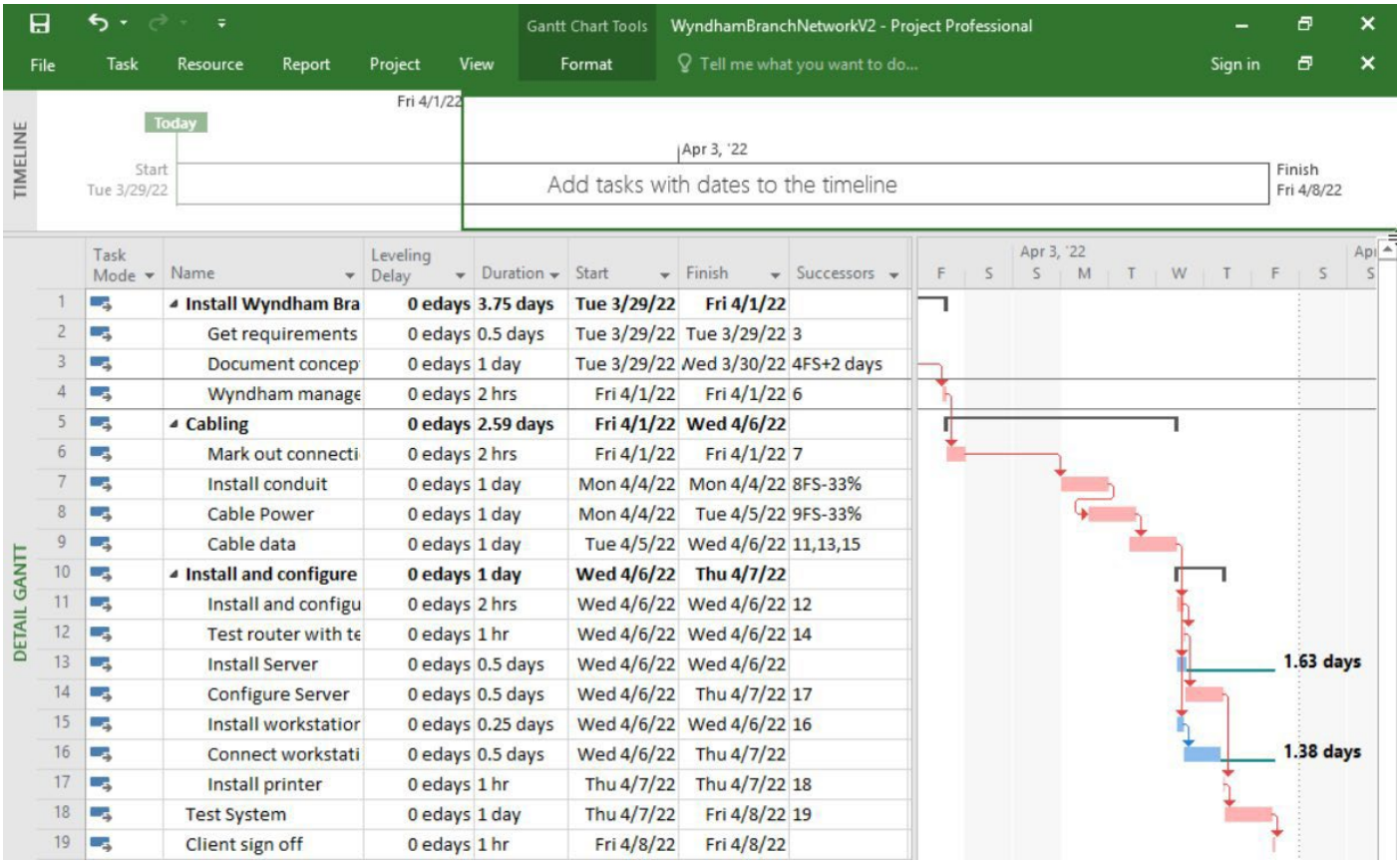


Steps #24 to #27 introduced us to concept of **Lead time**, as sometimes a **predecessor** doesn't necessarily have to be completely finished before a subsequent task can begin, thus there will overlap in the tasks, then we can start and finish subsequent tasks earlier, to achieve this we need to **configure a Lead time for Predecessor**, which can be done by double-clicking on the required task and accessing Task Information, then in the predecessor tab, changing the lag time to desired amount. Then **appropriate changes will be shown in Gantt Chart** as well.



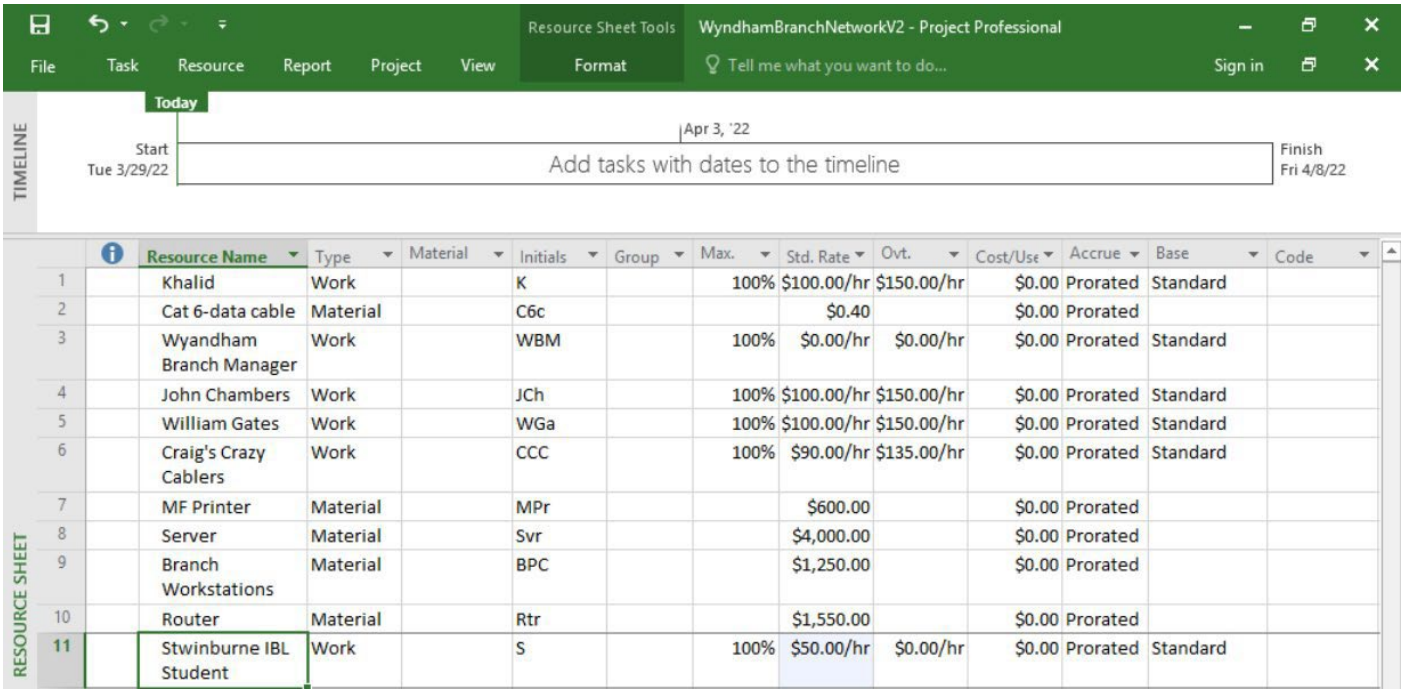
Steps #28 to #31 further guided us in implementing the **Lead time** for other Tasks. Then Auto Schedule feature can be used in order to solve complications occurred after adding lead time etc., it can be accessed by clicking the head of the Task Mode, then choosing the Task tab and clicking Auto Schedule. Finally the above figure was achieved.

- **Determining the Critical Path**



Step #33 introduced us to **Critical Path Analysis**, Critical path analysis finds the **sequence of activities that ultimately determine the length of the project**. If any of these activities fall behind schedule the whole project falls behind schedule, some like to think of it as the shortest path through **the Gantt chart**. It can be accessed from the View tab, clicking down on the Gantt Chart button, select more views Then Detail Gantt. Some of the **Gantt bars** have become **red**, these tasks are the tasks that determine the earliest the Project can finish, this is a very powerful tool in more complex projects. The **blue tasks** are the tasks that have some scheduling flexibility, hence we would in a considered manner give resource priority to the red tasks.

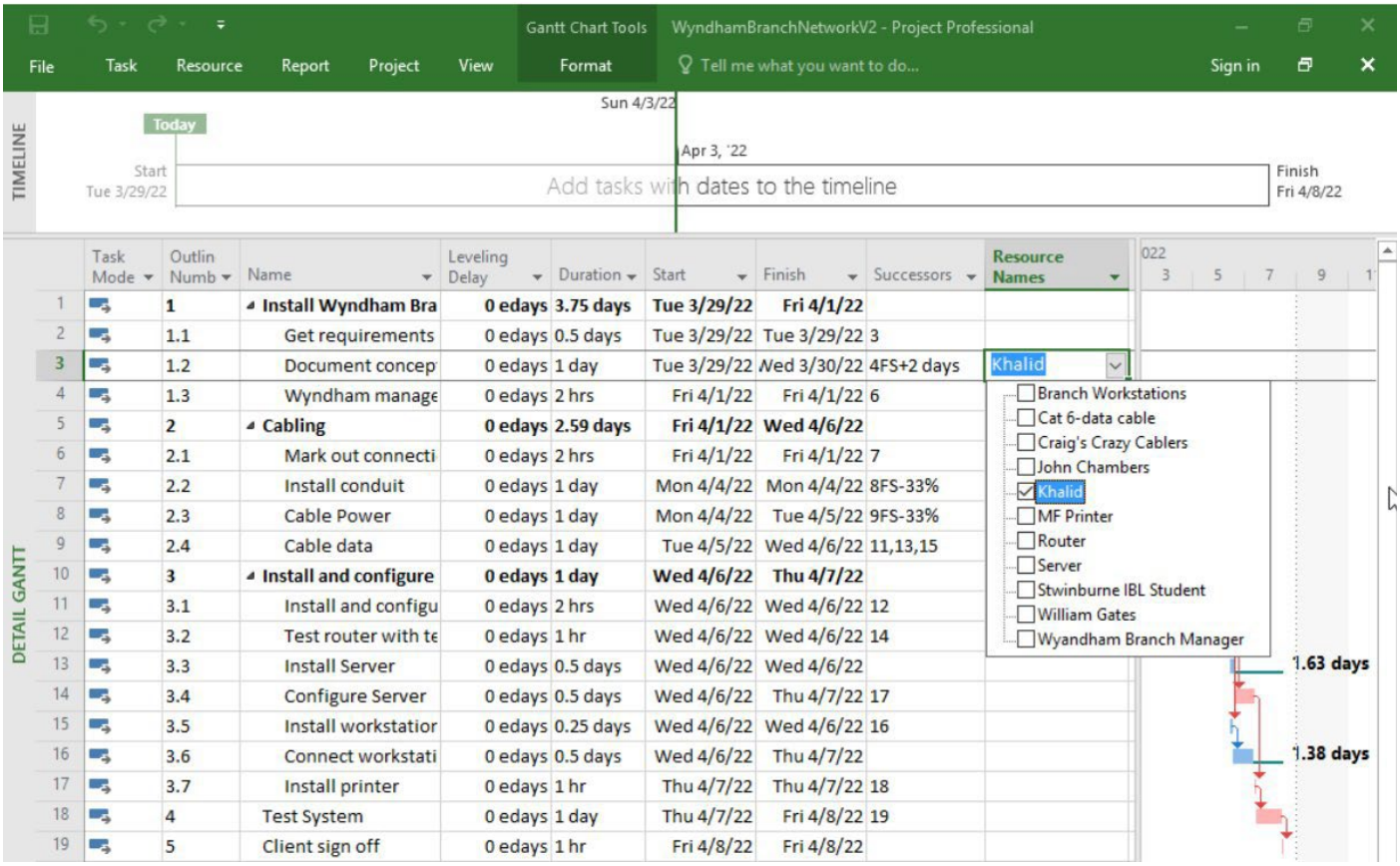
- **Managing Resources and Costs**



	Resource Name	Type	Material	Initials	Group	Max.	Std. Rate	Ovt.	Cost/Use	Accrue	Base	Code
1	Khalid	Work		K		100%	$100.00/hr	$150.00/hr	$0.00	Prorated	Standard	
2	Cat 6-data cable	Material		C6c			$0.40		$0.00	Prorated		
3	Wyandham Branch Manager	Work		WBM		100%	$0.00/hr	$0.00/hr	$0.00	Prorated	Standard	
4	John Chambers	Work		JCh		100%	$100.00/hr	$150.00/hr	$0.00	Prorated	Standard	
5	William Gates	Work		WGa		100%	$100.00/hr	$150.00/hr	$0.00	Prorated	Standard	
6	Craig's Crazy Cablers	Work		CCC		100%	$90.00/hr	$135.00/hr	$0.00	Prorated	Standard	
7	MF Printer	Material		MPr			$600.00		$0.00	Prorated		
8	Server	Material		Svr			$4,000.00		$0.00	Prorated		
9	Branch Workstations	Material		BPC			$1,250.00		$0.00	Prorated		
10	Router	Material		Rtr			$1,550.00		$0.00	Prorated		
11	Stwinburne IBL Student	Work		S		100%	$50.00/hr	$0.00/hr	$0.00	Prorated	Standard	

Steps #34 to #39 introduces us to **Resource Sheet**. It guides us thru basics of it like there are two type of resources which are **Human Resources and Material Resources**. Then we are asked to fill it out with the required information and then you end up with the above table.

- **Assigning Resources**

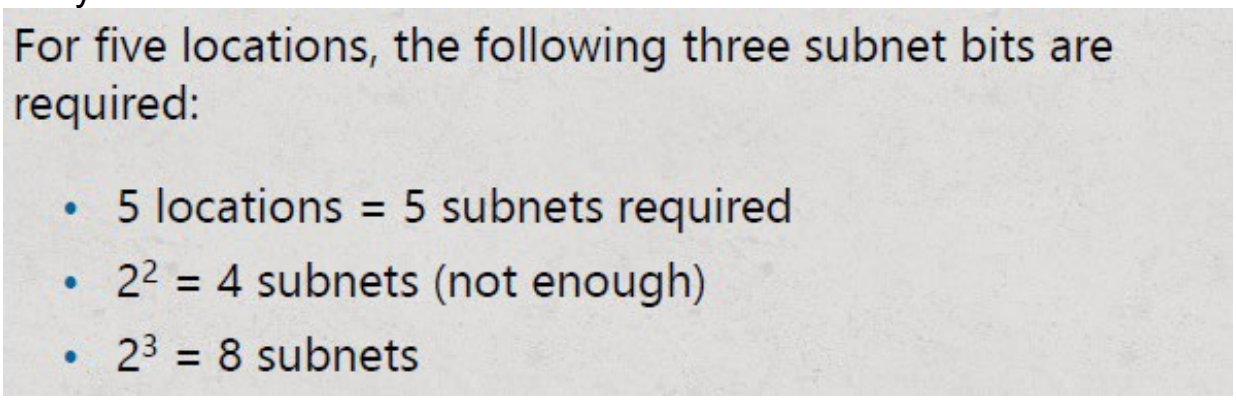


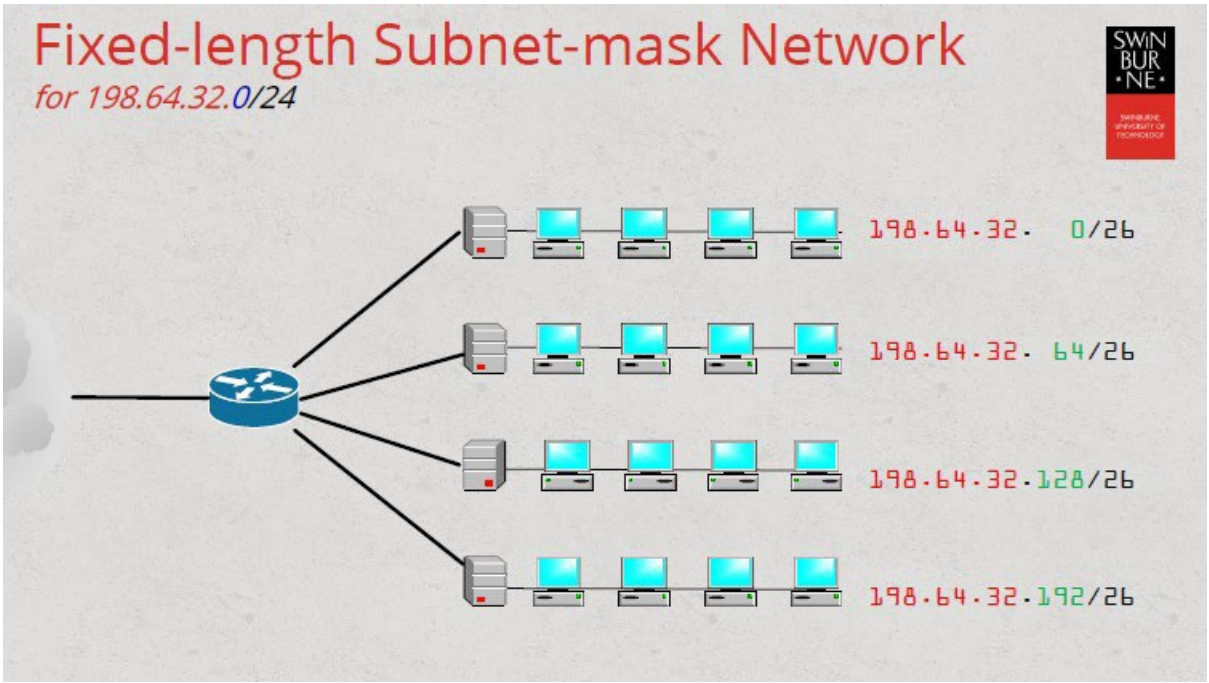
Steps #40 to #44 guides us on how we can use the **resource sheet** and **assign it to Tasks** in our main table. It can be done by clicking the Resource column of the task you want to assign the resource and just select from the list you just entered in the resource sheet, you can select more than one, the above figure shows how to do it exactly. Remember that, if materials are assigned repeatedly then they would be counted twice in our project.

TNE10005 Journal Lab (#3)

Khalid Yaseen Baig / ID #102763240

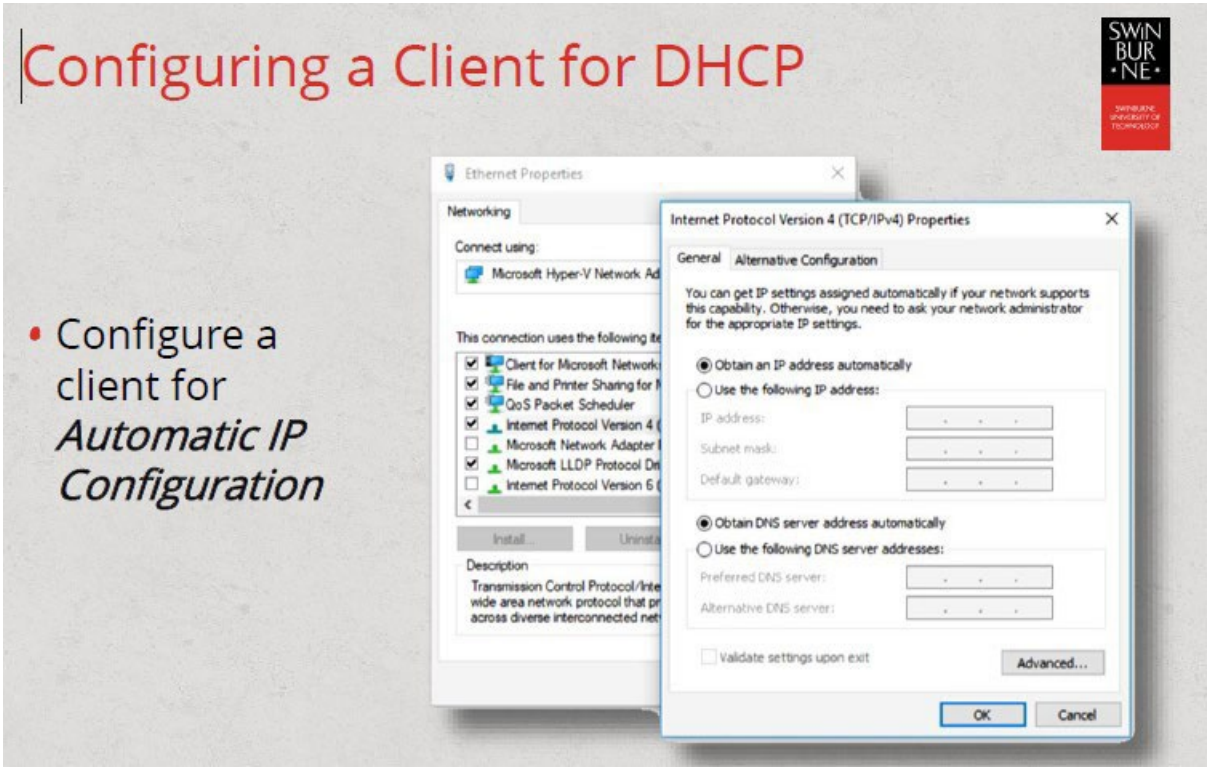
What I learned in this week's Lecture.

- When calculating subnet addresses, we should choose the number of subnet bits based on the number of subnets required, then use 2n to figure out how many subnets are accessible from n bits.
- 

- We should choose the number of host bits depending on the number of hosts required on each subnet and use 2n-2 to calculate the number of hosts accessible on each subnet when determining host addresses.
- 

- Class C addresses were the most affordable. The networks that you combine must be continuous. This is known as super netting.

- DHCP has the advantage of catering to 'nomadic' users who need to work at many branches. Allow for flexibility in IP address management by centralizing IP setup parameters.



- A DHCP Scope is a container for managing an address pool and IP settings. A Pool's addresses must all be from the same subnet. A Server can have several Scopes. A scope can have many address pools (rare).

- When some devices require manual configuration of their IP values, this is referred to as a DHCP Exclusion. These addresses are not available to other devices. These addresses are not offered by the DHCP server due to exclusions.

- DHCP reservations ensure that a device receives the same IP address. The device's MAC address is used to determine allocation.

This week's lab activities.

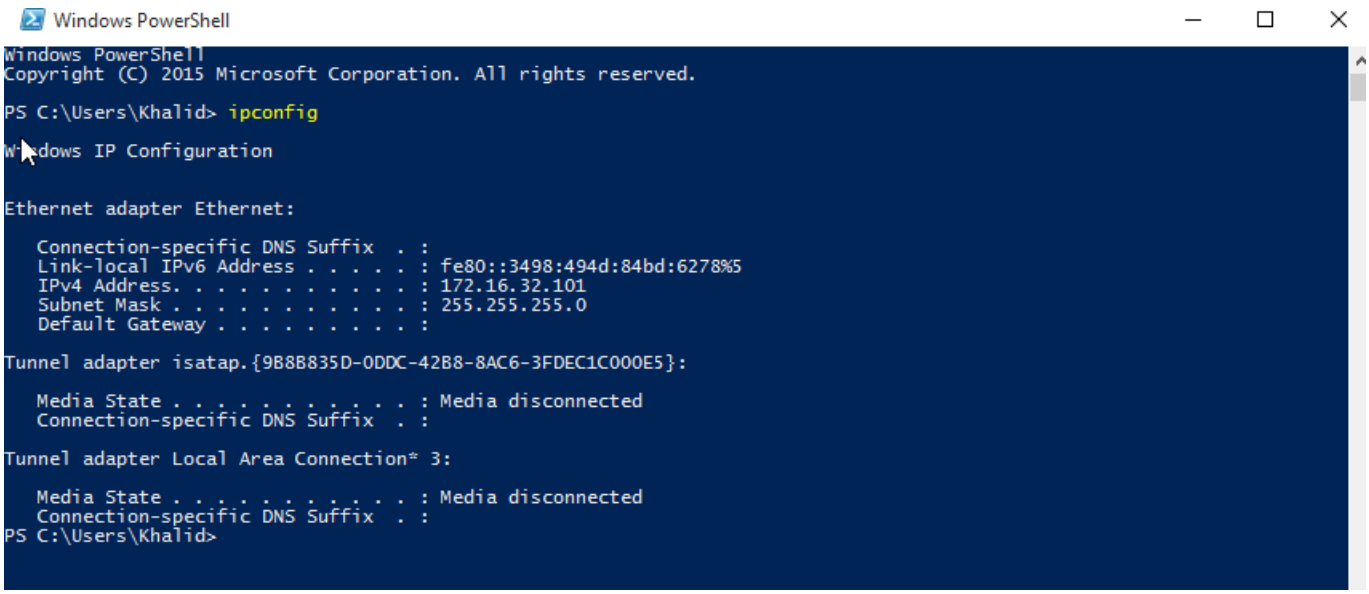
- Record the output here:

  Connection-Specific DNS Suffix: NIL

  IPv4 Address: 172.16.32.101

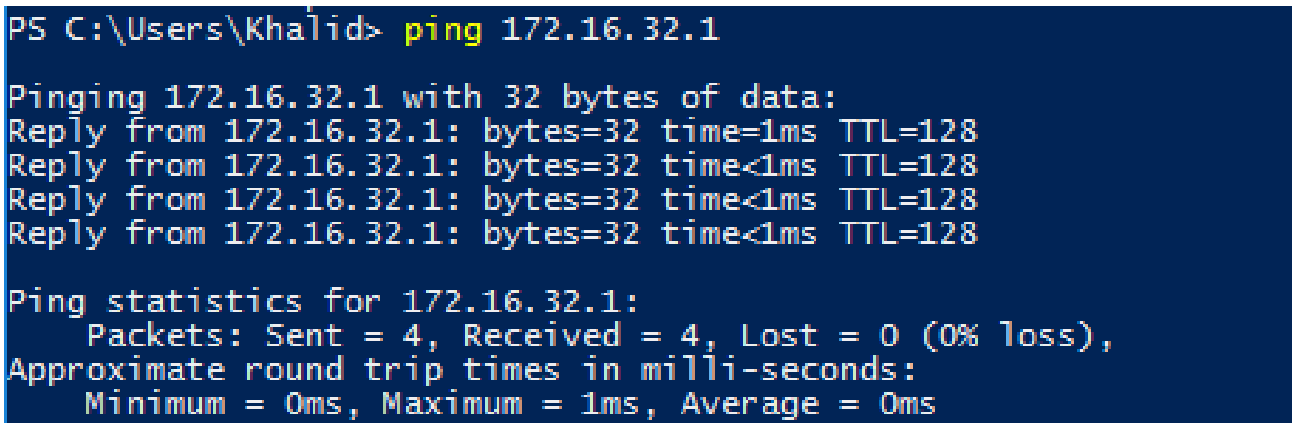
  Subnet Mask: 255.255.255.0

  Default Gateway: NIL



- Ping 172.16.32.1

  Was the ping successful? Yes



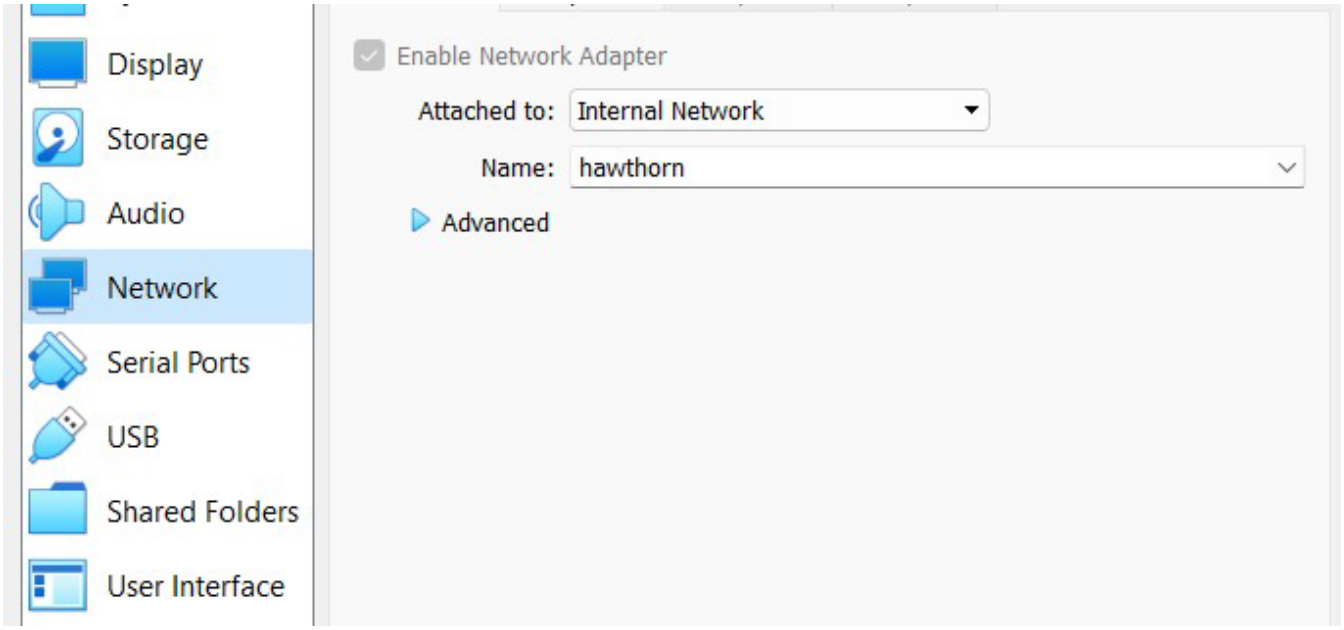
- Now ping the IP address of our **sWin10PC2**. At the PowerShell prompt type:

  `Ping 10.10.10.102`

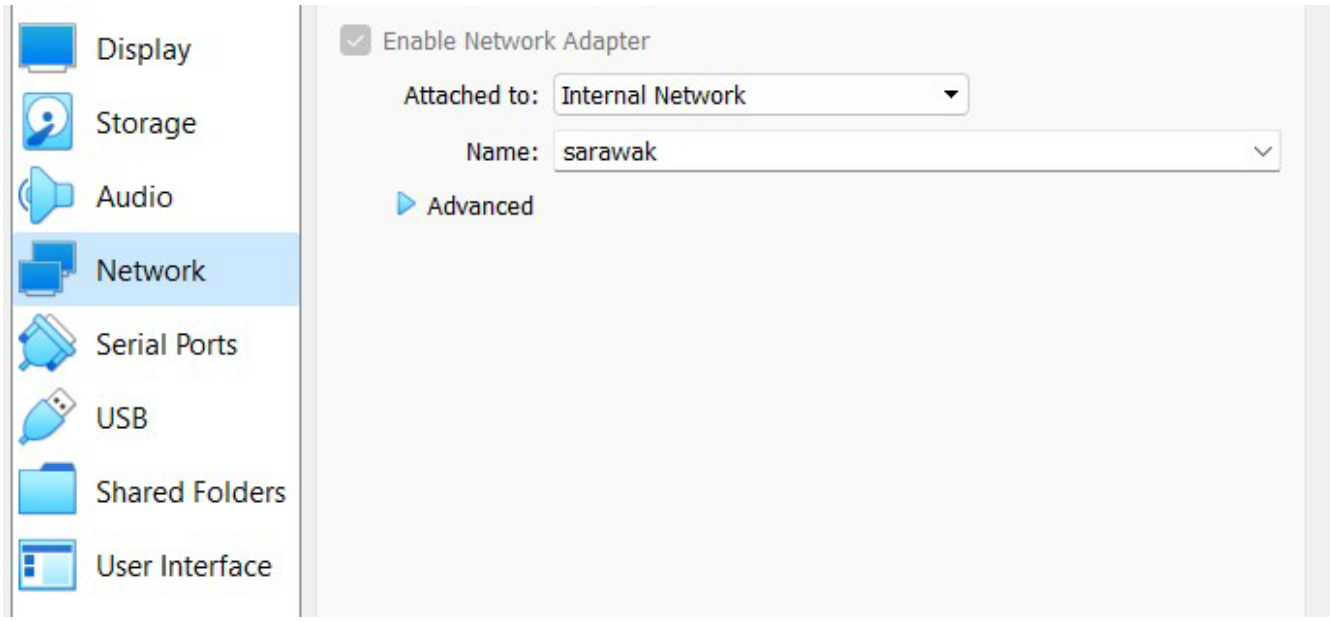
  Was this successful? NO

```
PS C:\Users\Khalid> ping 10.10.10.102

Pinging 10.10.10.102 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 10.10.10.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Khalid>
```

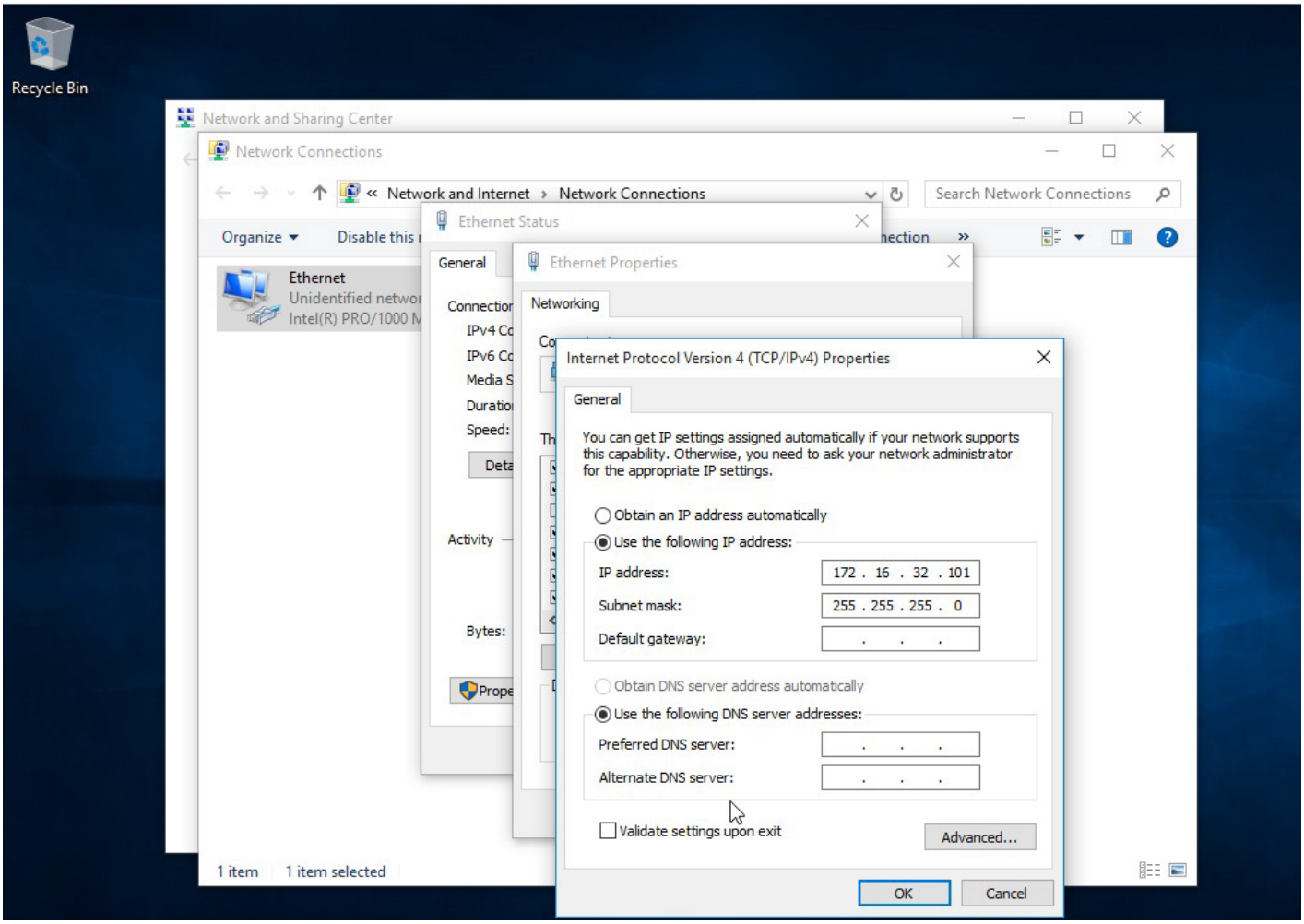
Screenshots of Important Steps Required for Lab.



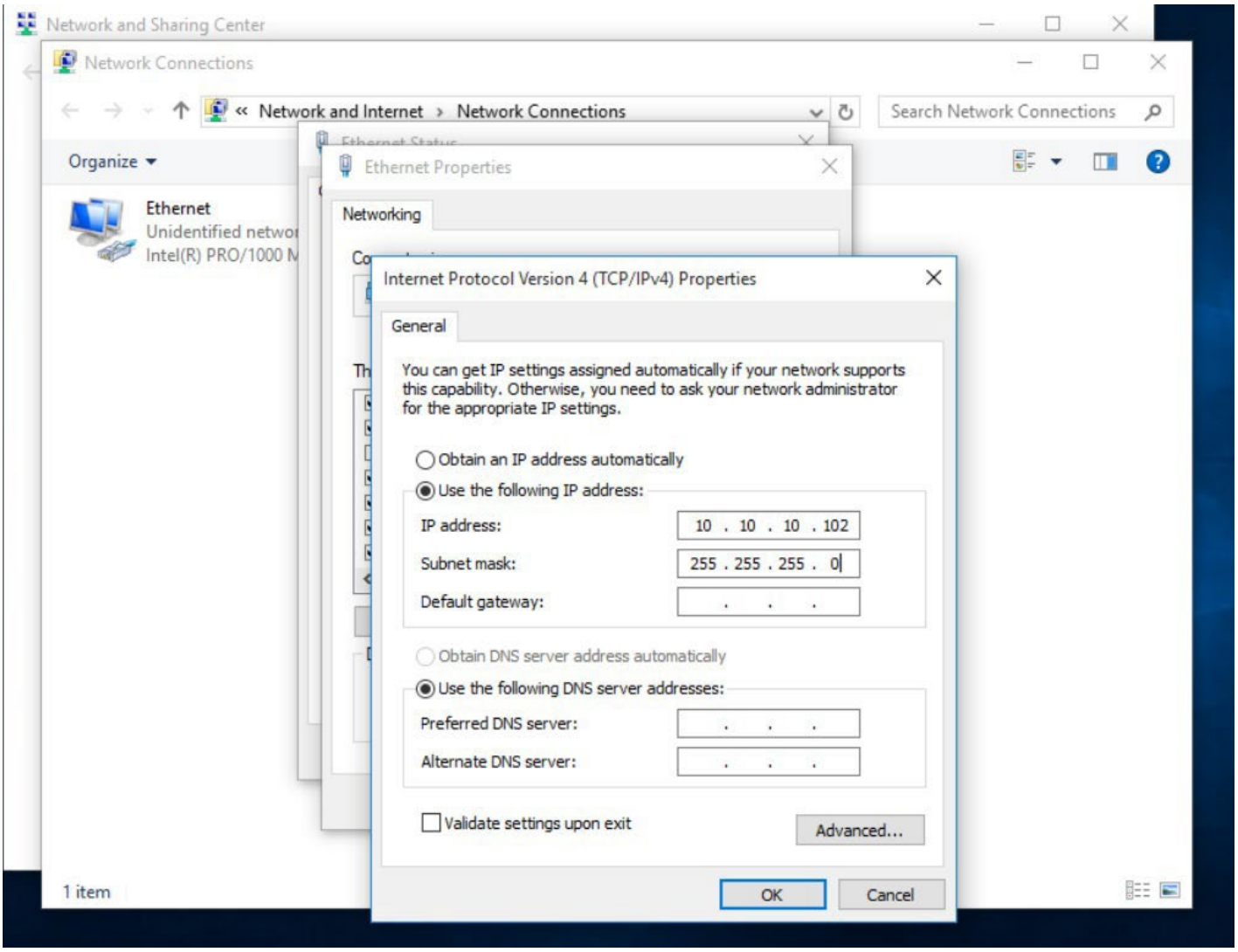
Step #2 instructed us to Change the network to Internal Network and name it hawthorn for sWin10PC1 and for Adapter 1 of sWin16RTR



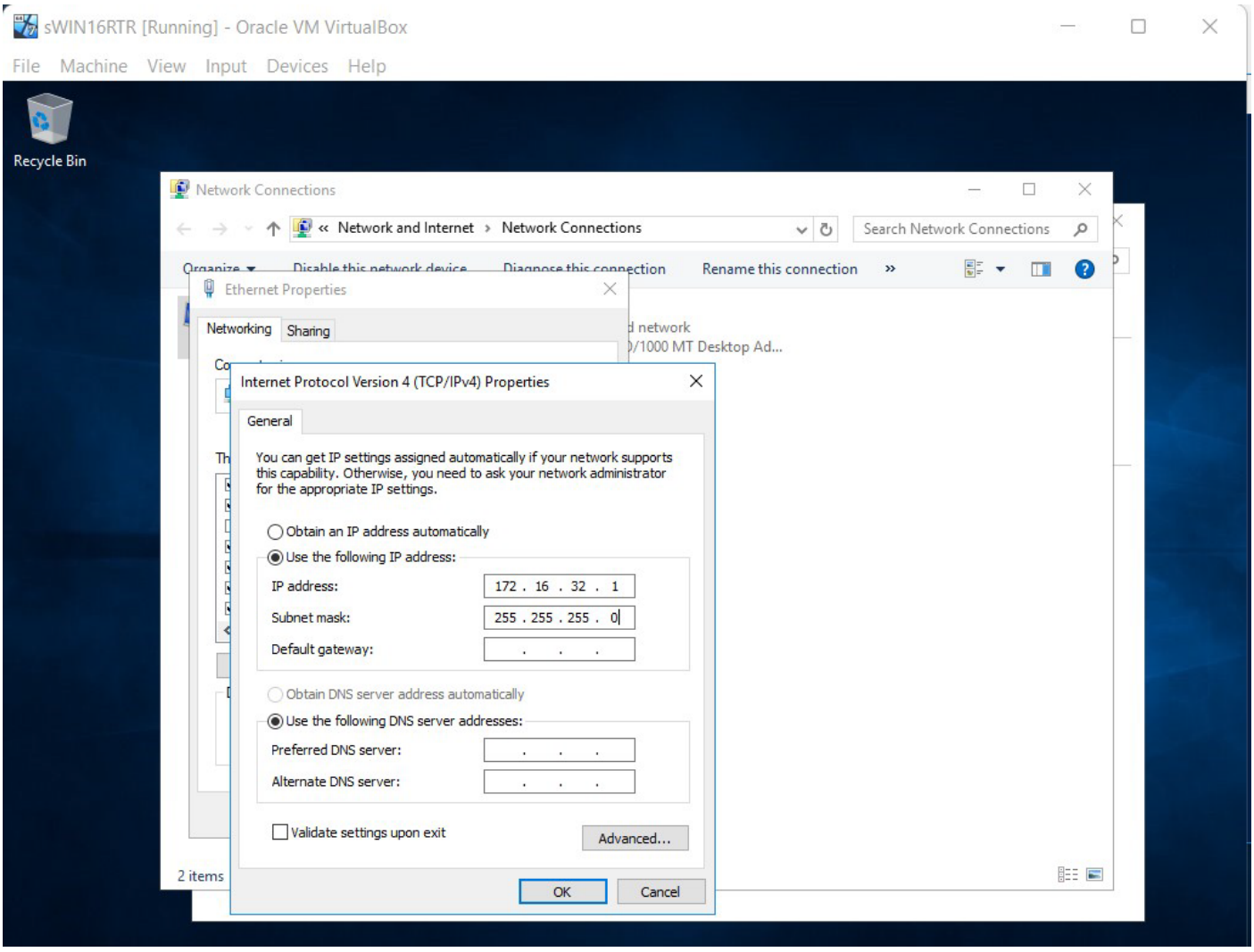
Step #2 instructed us to Change the network to Internal Network and name it Sarawak for sWin10PC2 and for Adapter 2 of sWin16RTR



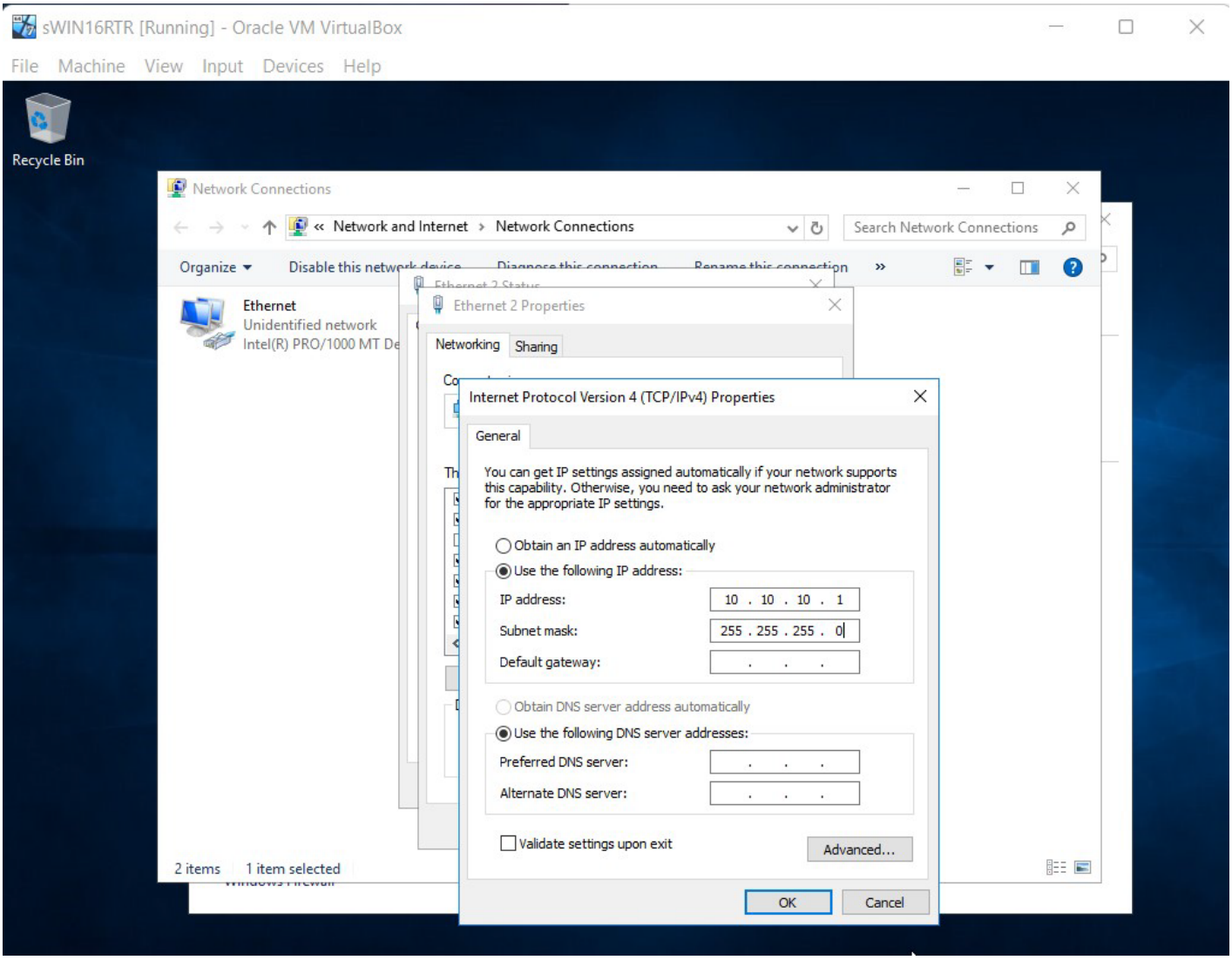
Step #3 instructed us to configure the IP Address of sWin10PC1 to 172.16.32.101 and subnet mask to 255.255.255.0 according to the Topology Diagram



Step #3 instructed us to configure the IP Address of sWin10PC2 to 10.10.10.102 and subnet mask to 255.255.255.0 according to the Topology Diagram



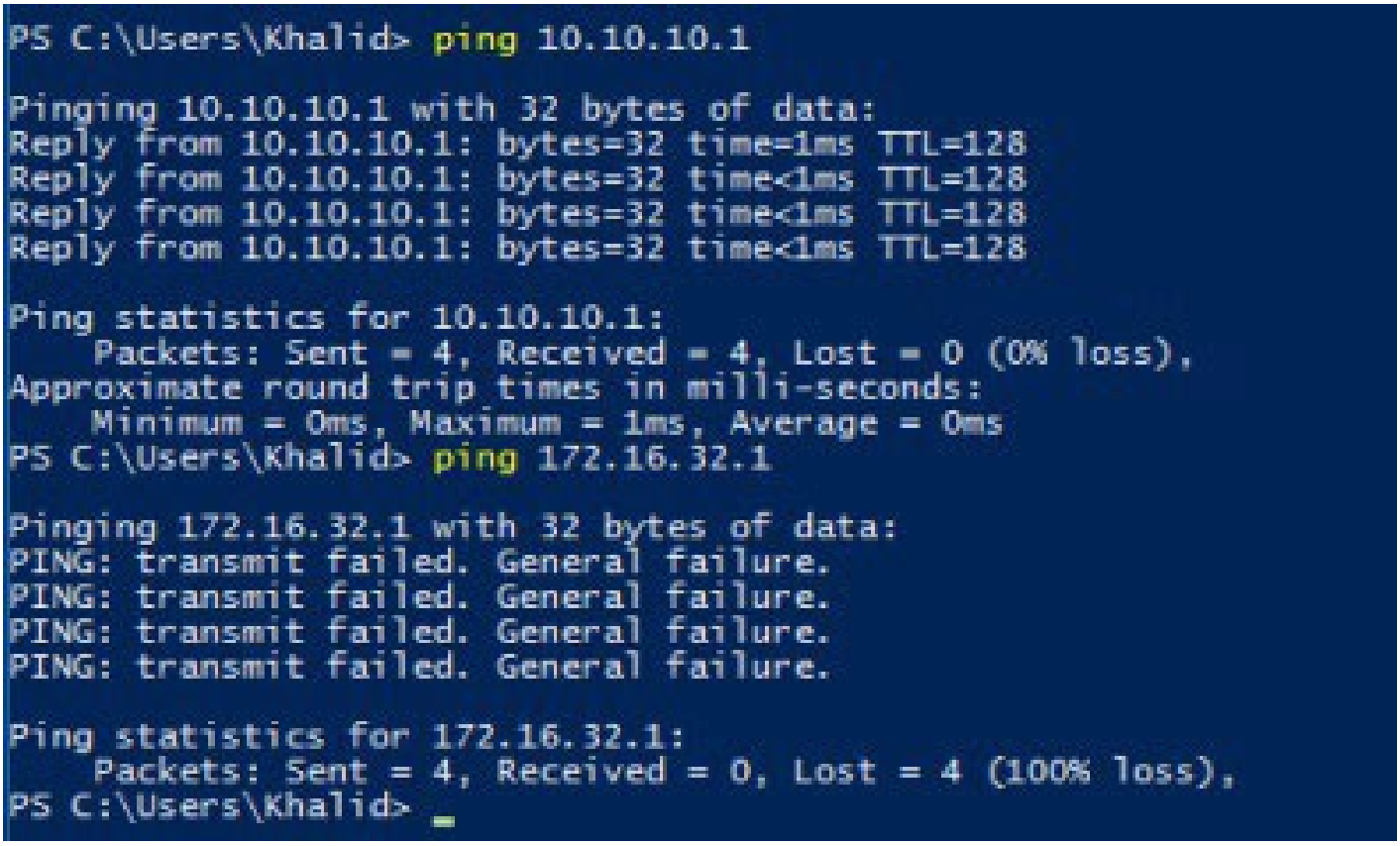
Configuring the IP Address of Adapter 1 of sWIN16RTR to 172.16.32.1 and subnet mask to 255.255.255.0 according to the Topology Diagram



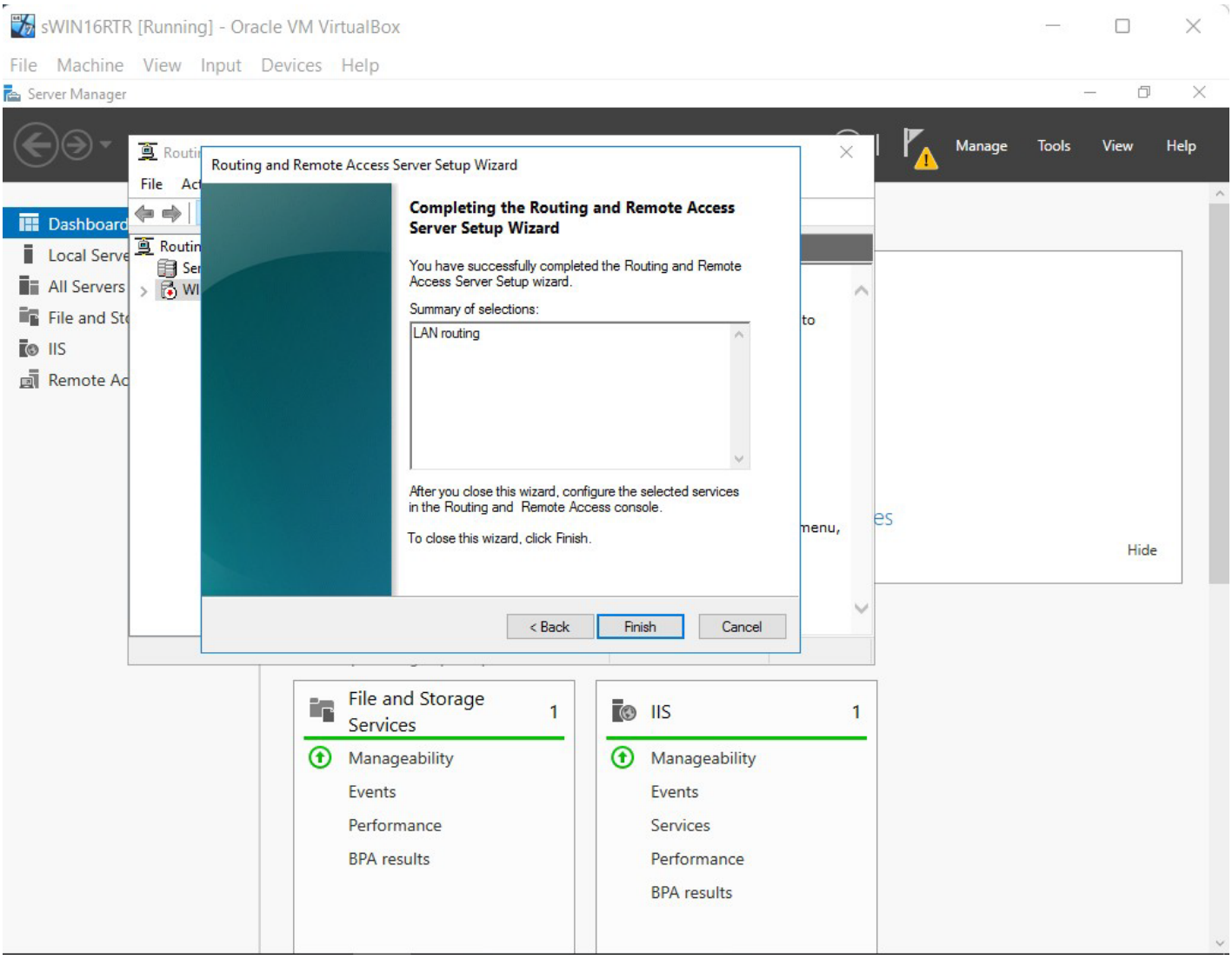
Configuring the IP Address of Adapter 2 of sWIN16RTR to 10.10.10.1 and subnet mask to 255.255.255.0 according to the Topology Diagram

```
PS C:\Users\Khalid> ping 172.16.32.1

Pinging 172.16.32.1 with 32 bytes of data:
Reply from 172.16.32.1: bytes=32 time=1ms TTL=128
Reply from 172.16.32.1: bytes=32 time<1ms TTL=128
Reply from 172.16.32.1: bytes=32 time<1ms TTL=128
Reply from 172.16.32.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.32.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Khalid> ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Khalid> _
```

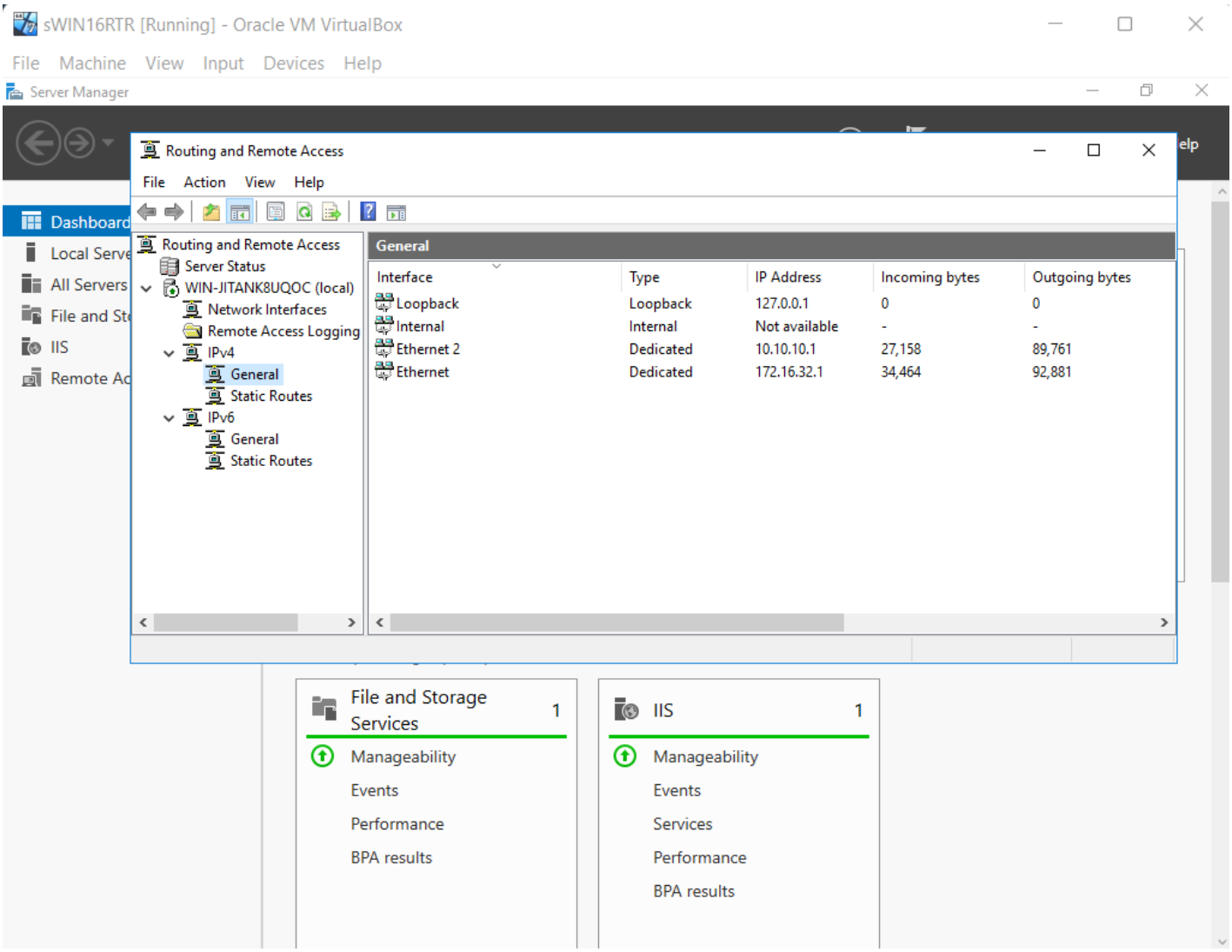
Step #8 instructed us to ping the IP Address of Adapter 1 sWin16RTR (172.16.32.1) from sWin10PC1 and it was successful. Step #9 wanted us to try pinging the IP Address of SWin10PC2 from sWIn10PC1 and it failed.



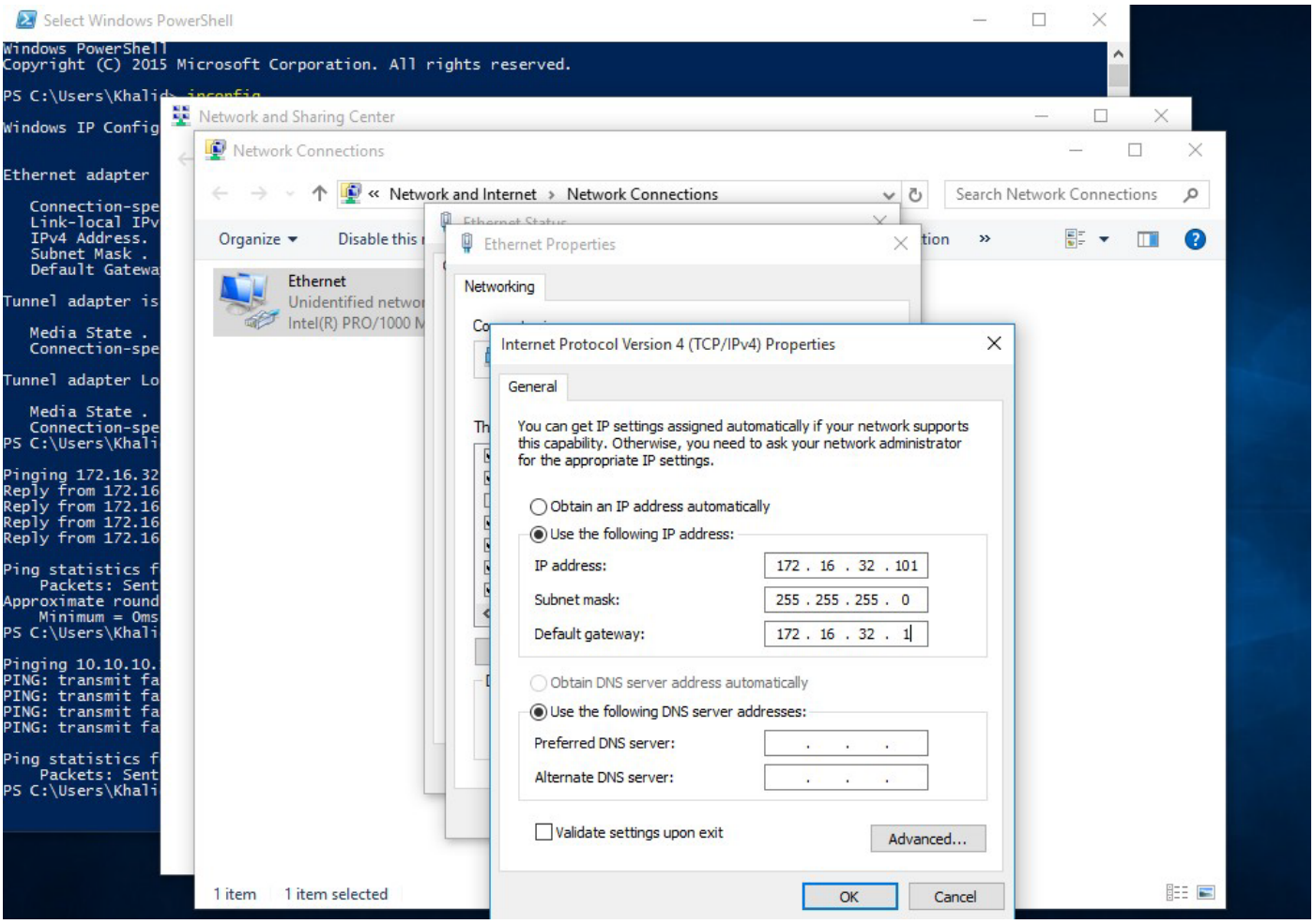
Step #8 instructed us to ping the IP Address of Adapter 2 of sWin16RTR (10.10.10.1) from sWin10PC2 and it was successful. Step #9 wanted us to try pinging the IP Address of SWin10PC1 from sWIn10PC2 and it failed.



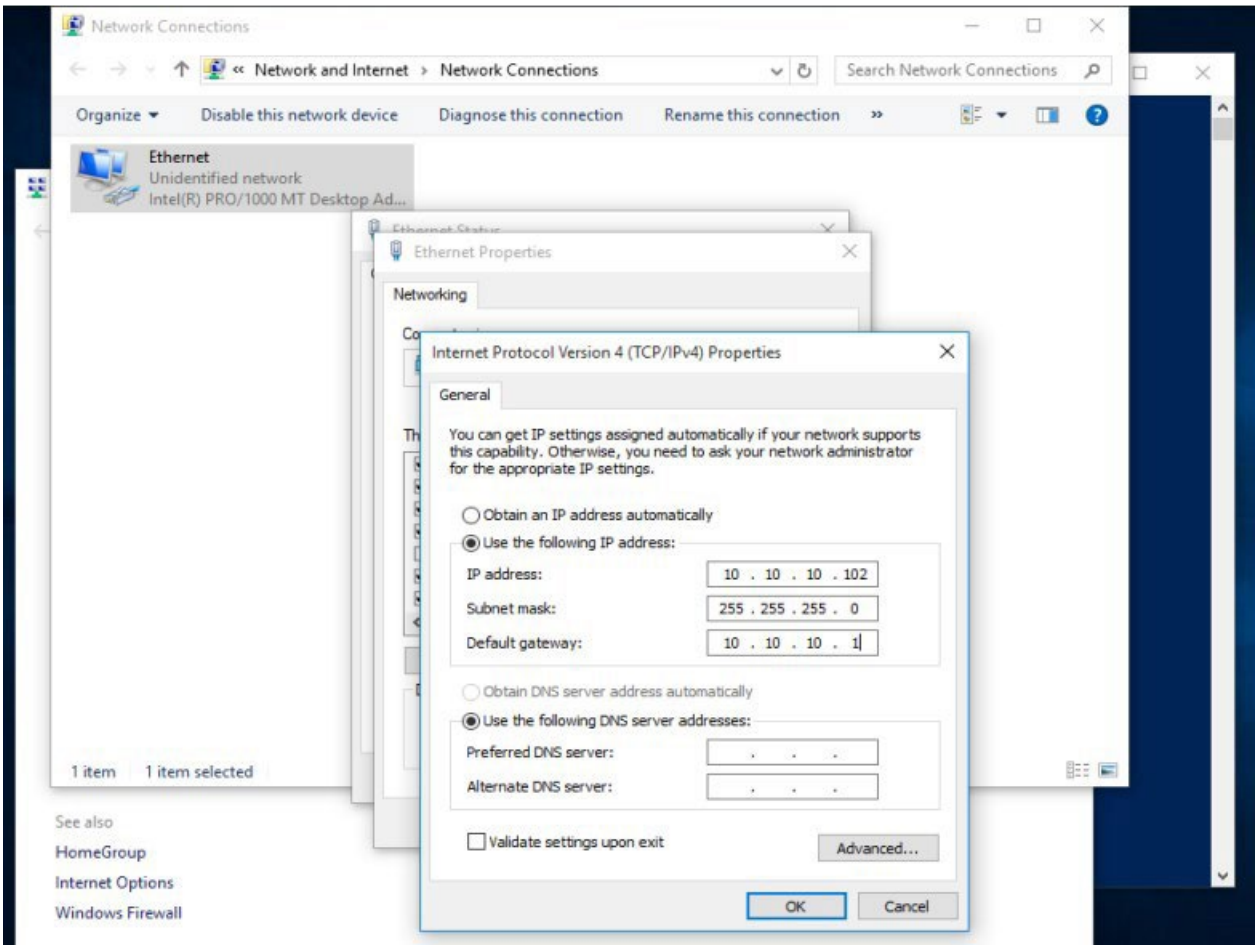
Configuring and Setting up of Routing and Remote Access of the sWin16RTR to act as a router between two networks, Hawthorn and Sarawak.



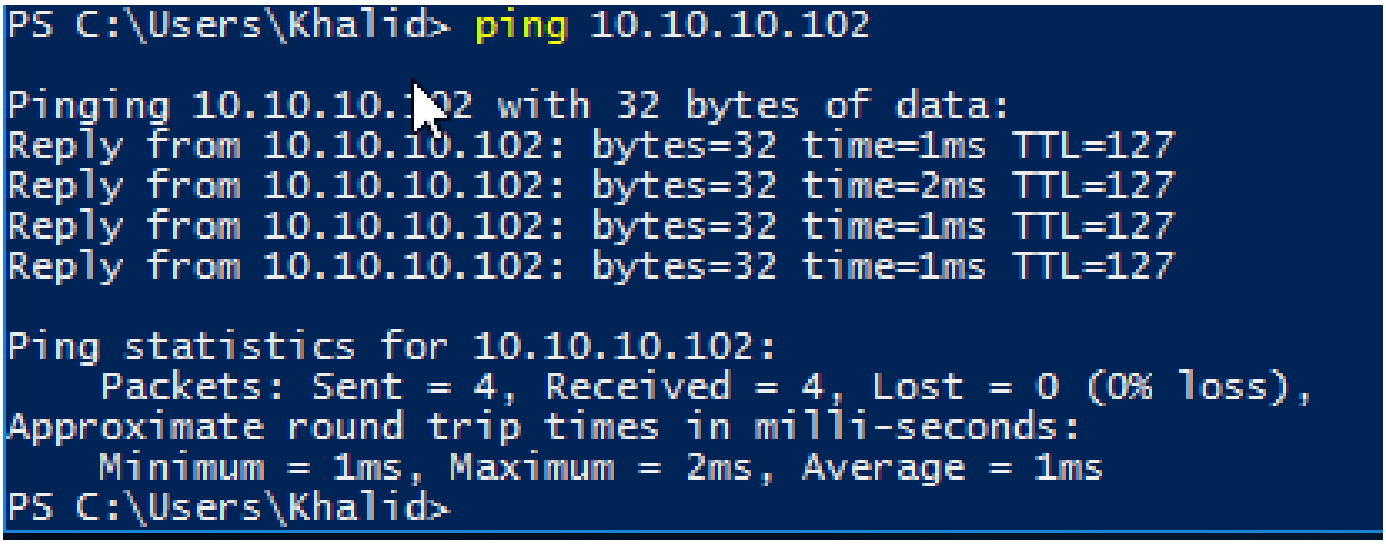
Successfully setting up the sWin16RTR to act as a router between two networks, Hawthorn and Sarawak.



Step #11 instructed us to setup the Default Gateway IP Address for sWin10PC1 according to the Topology Diagram so it can successfully communicate with sWin10PC2



Step #11 instructed us to setup the Default Gateway IP Address for sWin10PC2 according to the Topology Diagram so it can successfully communicate with sWin10PC1



Step #13 wanted us to Test if the Routing Default Gateway Configuration worked successfully by Pinging 10.10.10.102 from sWin10PC1 and it was successful.

14. Question: Look at the source and destination addresses of Frame 1 and Frame 2.

a. Which addresses change?

b. Which addresses stay the same?

c. Try to explain why some change and others don't:

17. Question: Do PCc and PCd have the same network address?

PCc IP:192.168.100.103

PCc SN: 255.255.255.0

PCd IP: 192.168.111.104

We will now look at this from a practical perspective.

```
PS C:\Users\Khalid> ping 172.16.32.1

Pinging 172.16.32.1 with 32 bytes of data:
Reply from 172.16.32.1: bytes=32 time=1ms TTL=128
Reply from 172.16.32.1: bytes=32 time<1ms TTL=128
Reply from 172.16.32.1: bytes=32 time=1ms TTL=128
Reply from 172.16.32.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.32.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Khalid> ping 172.16.32.1

Pinging 172.16.32.1 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 172.16.32.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Khalid>
```

Step #18 wanted us to Ping the IP Address of the Local Router Interface (172.16.32.1) from sWin10PC1 and it was successful. Step #19 wanted us to Change the Subnet Mask to 255.255.255.192 and delete the Default Gateway Address and then Ping the IP Address of the Local Router Interface (172.16.32.1) from sWin10PC1 and it failed.

TNE10005 Journal Lab (#4)

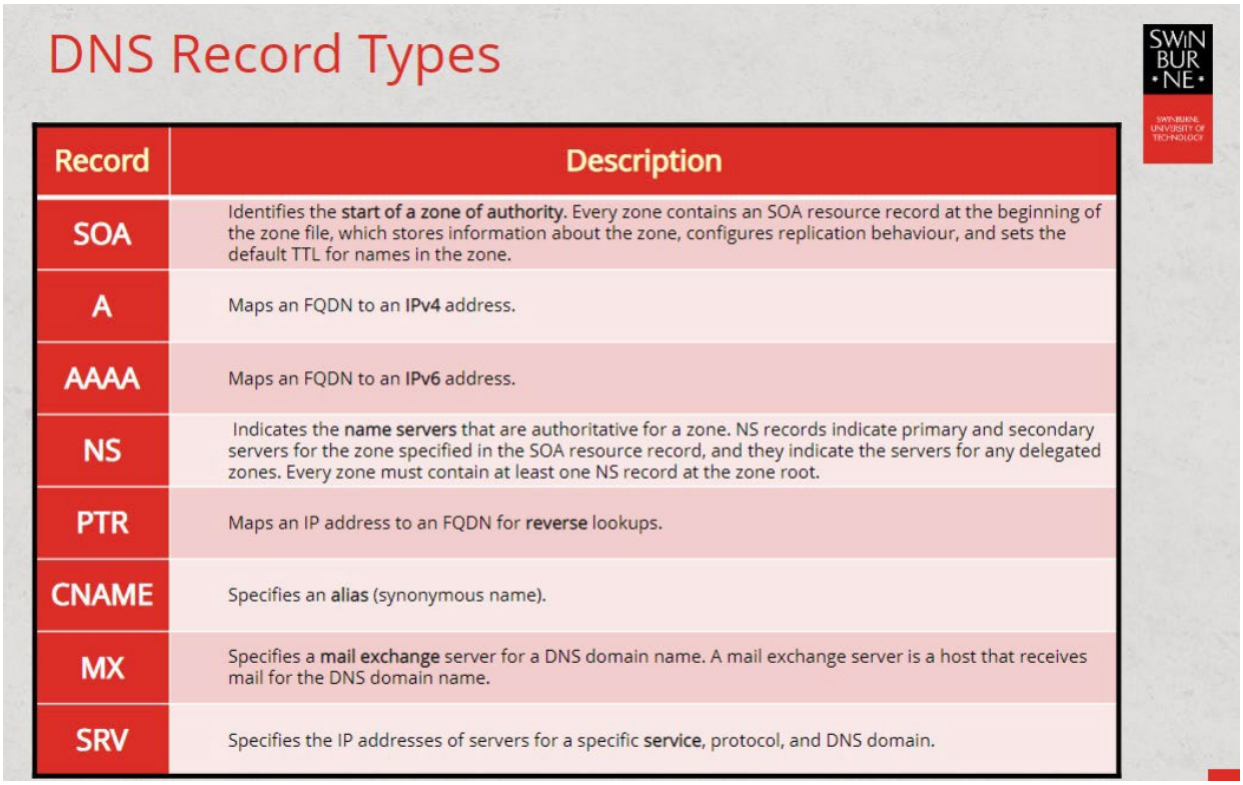
Khalid Yaseen Baig / ID #102763240

What I learned in this week's Lecture.

- Domain names are resolved to IP addresses via the DNS Domain Name System. A Fully Qualified Domain Name (FQDN) consists of the following elements: <Host Name>.<Domain Name>.<Top-level Domain>.

- The DNS is a worldwide distributed database.
  - Resolve FQDNs to IP addresses
  - Locate domain controllers and global catalog servers
  - Resolve IP addresses to host names
  - Locate mail servers during email delivery

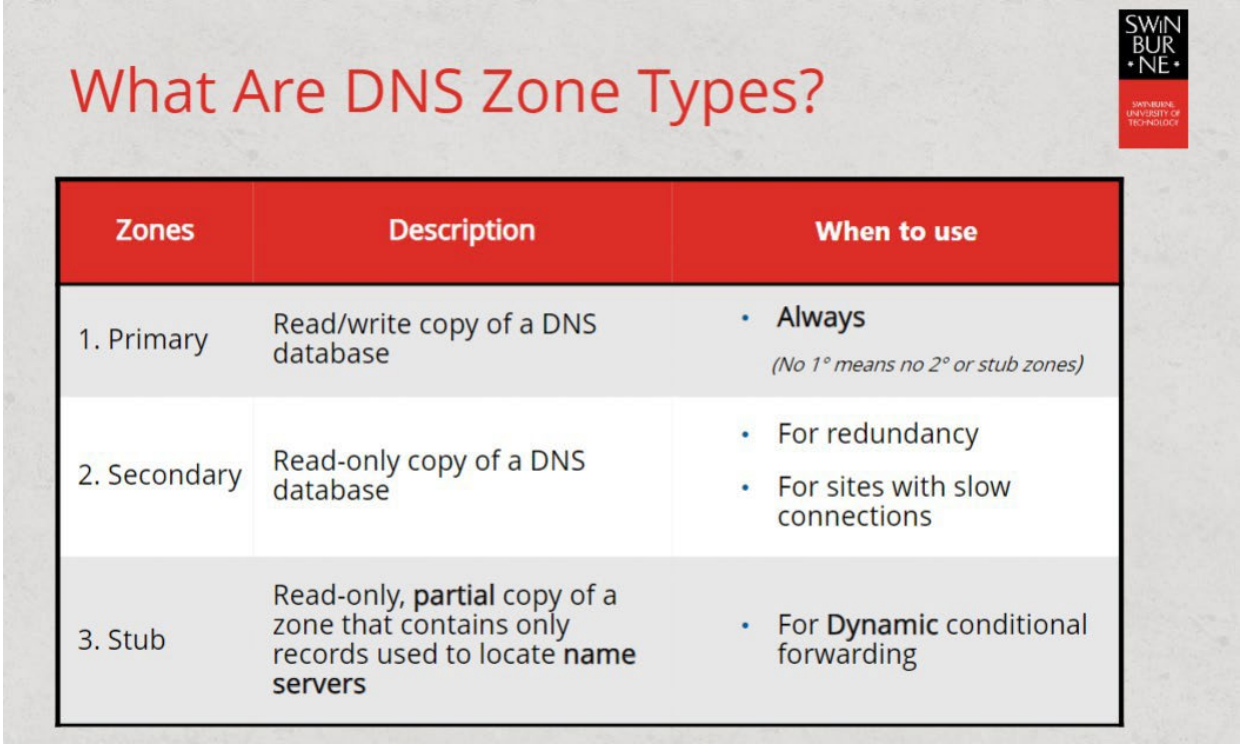
- A DNS zone is a subset of the DNS namespace that contains DNS records.

- 

Record	Description
SOA	Identifies the **start of a zone of authority**. Every zone contains an SOA resource record at the beginning of the zone file, which stores information about the zone, configures replication behaviour, and sets the default TTL for names in the zone.
A	Maps an FQDN to an **IPv4** address.
AAAA	Maps an FQDN to an **IPv6** address.
NS	Indicates the **name servers** that are authoritative for a zone. NS records indicate primary and secondary servers for the zone specified in the SOA resource record, and they indicate the servers for any delegated zones. Every zone must contain at least one NS record at the zone root.
PTR	Maps an IP address to an FQDN for **reverse** lookups.
CNAME	Specifies an **alias** (synonymous name).
MX	Specifies a **mail exchange** server for a DNS domain name. A mail exchange server is a host that receives mail for the DNS domain name.
SRV	Specifies the IP addresses of servers for a specific **service**, protocol, and DNS domain.

- DNS Queries are iterative or recursive. When a DNS server gets a Recursive query, it gives either the needed response or an error; the DNS server does not send the DNS client to another server. When a DNS server gets an Iterative query, it either delivers the requested result or forwards the request to another server that may be authoritative for the requested record.

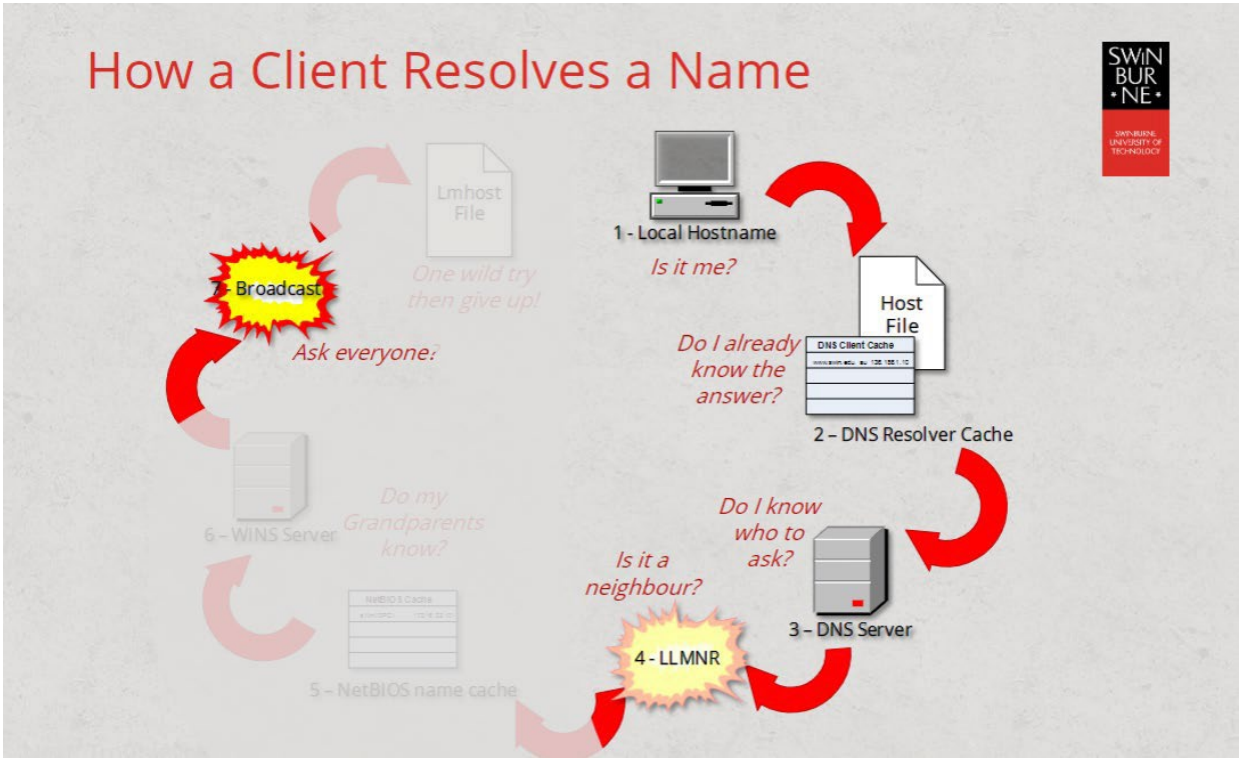
- Queries that cannot be handled by a DNS server are passed to an ISP's DNS server, a Head office DNS server, or a parent Domain's DNS server through forwarders.

- 

- Secondary and Stub zones must be configured to receive zone records from the Master Server. A Master Server is a DNS server that hosts a duplicate of the domain's zone. The Master DNS data must eventually come from a Primary Zone. Master servers, by default, do not allow data to be exchanged.

- If a device is assigned a different IP address through DHCP, dynamic updates allow it to change the IP address of its A record. If a hacker gains access to a device, they can utilize Dynamic updates to alter the record to a different IP address. It is advisable to restrict secure dynamic updates to Active Directory and AD-integrated DNS zones.

- DNSSec - confirms identity and encrypts DNS communication using Public/Private Key Infrastructure.

- 

- **Server Roles :** File Server, Print Server, Web Server (IIS), Application Server, Database Server and Domain Controller.

This week's lab activities.

5. **`Set-NetIPInterface -InterfaceAlias Ethernet -dhcp enabled`**

   Wait about 20 seconds, then type **`ipconfig`** and press **Enter**.

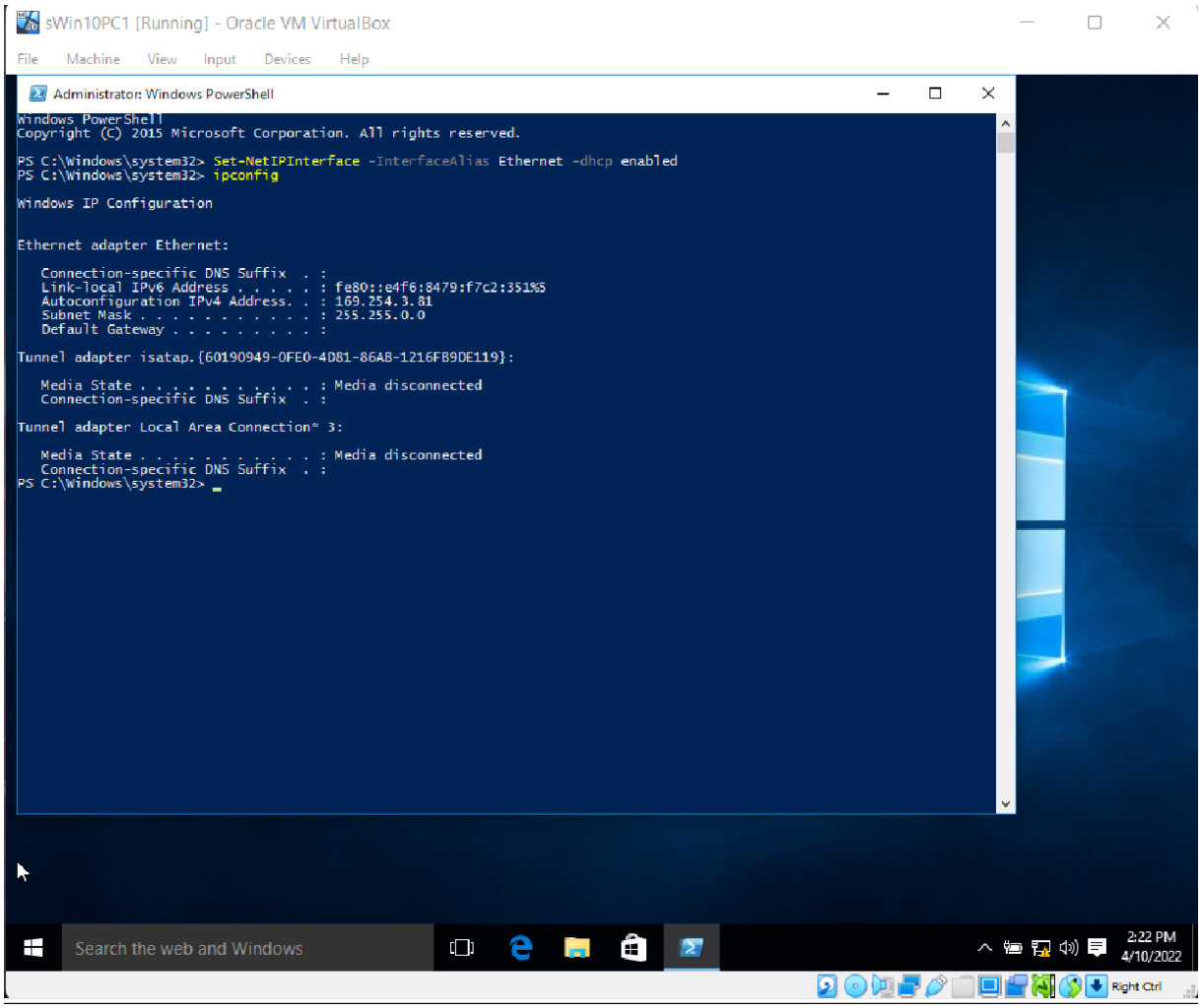
   Record your IPv4 Address, Subnet Mask and Default Gateway here: **IPv4**

   Address: 169.254.3.81

   Subnet Mask: 255.255.0.0

   Default Gateway: NIL

   What type of address is this? This is IPV4 Address given to any devices without any configuration.



23. To test if our DHCP server is now working change to **sWin10PC1** and go to **Powershell**. Type:

```
ipconfig /renew
```

And press**Enter.**

This triggers the computer to send out a **DHCP discover** packet.

Record your IPv4 Address, Subnet Mask and Default Gateway here: **IPv4**

Address: 172.16.32.150

Subnet Mask: 255.255.255.0

Default Gateway: NIL

This address should be from the scope you have just configured.

25. On sWin10PC1, type **`ipconfig /release`** press enter and type **`ipconfig /renew`**, (hint: you can press the up arrow to recall past commands) and press enter. Record the output here:

IPv4 Address: 172.16.32.160

Subnet Mask: 255.255.255.0

Default Gateway: NIL

What has changed? The IPv4 Address has changed from 172.16.32.150 to 172.16.32.160 as the IP Addresses ranging from 172.16.32.150 to 172.16.32.159 have been added to exclusion range.

29. Locate the line **Physical Address** and record it here: 08-00-27-AE-00-19

32. Record your address here:

IPv4 Address: 172.16.32.199

Subnet Mask: 255.255.255.0

Default Gateway: **NIL**

What has changed? The IPv4 Address has changed from 172.16.32.160 to 172.16.32.199 as this IP address has been reserved for sWin10PC1 through its MAC Address.

36. Back on **sWin10PC1** release and renew your IP address.

Verify that your new settings have been applied and record your new IP configurationhere:

DNS suffix: NetAdmin.edu

IPv4 Address: 172.16.32.199

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.32.2

39. Verify that your new settings have been applied.

What has changed? What has remained the same?

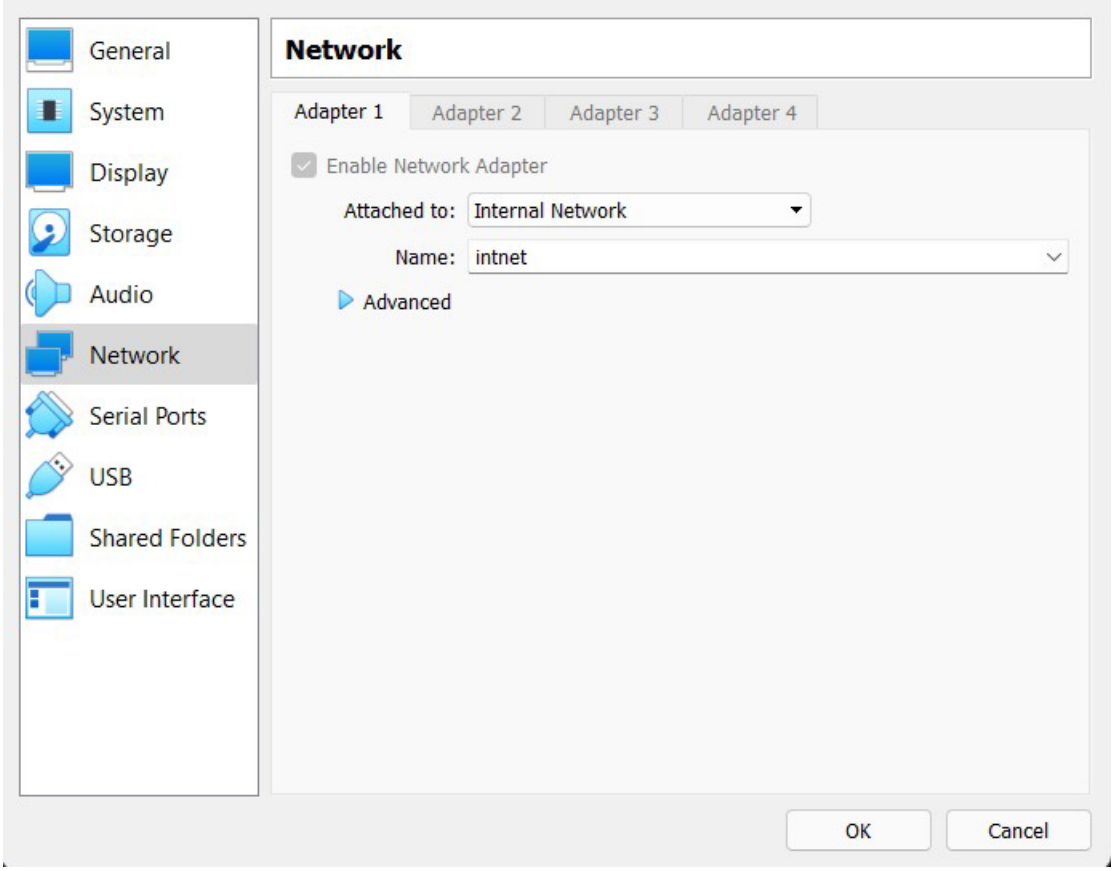
The Default Gateway has been changed from 172.16.32.2 to 172.16.32.1 and The DNS suffix has remained the same.

42. On sWin10PC1, at a command prompt, release and renew your IP address. Type ipconfig /all, what is the Hostname that appears?

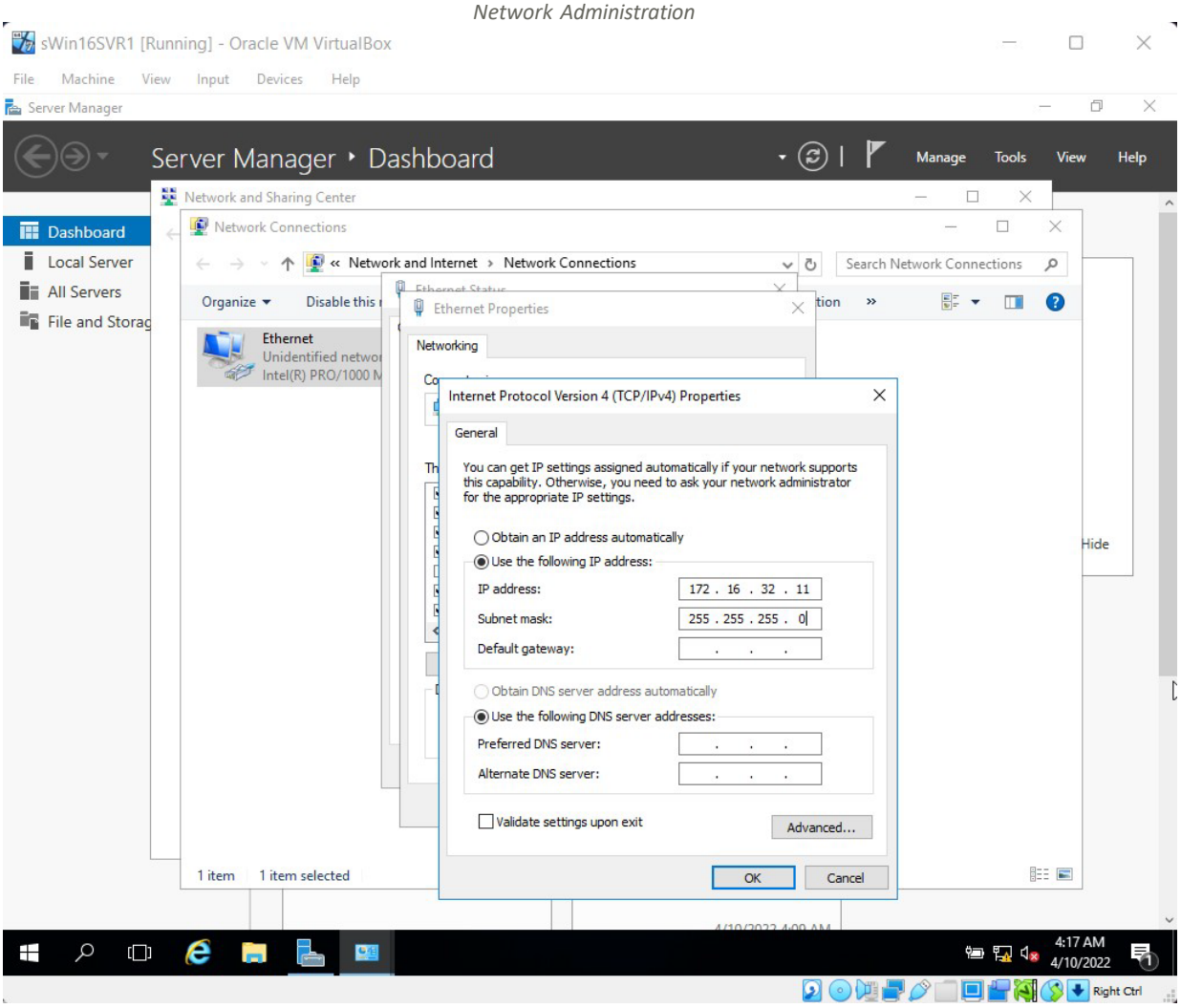
ResSetDNS

Which option rules them all? The Reservation Option Rules them all.

Screenshots of Important Steps Required for Lab

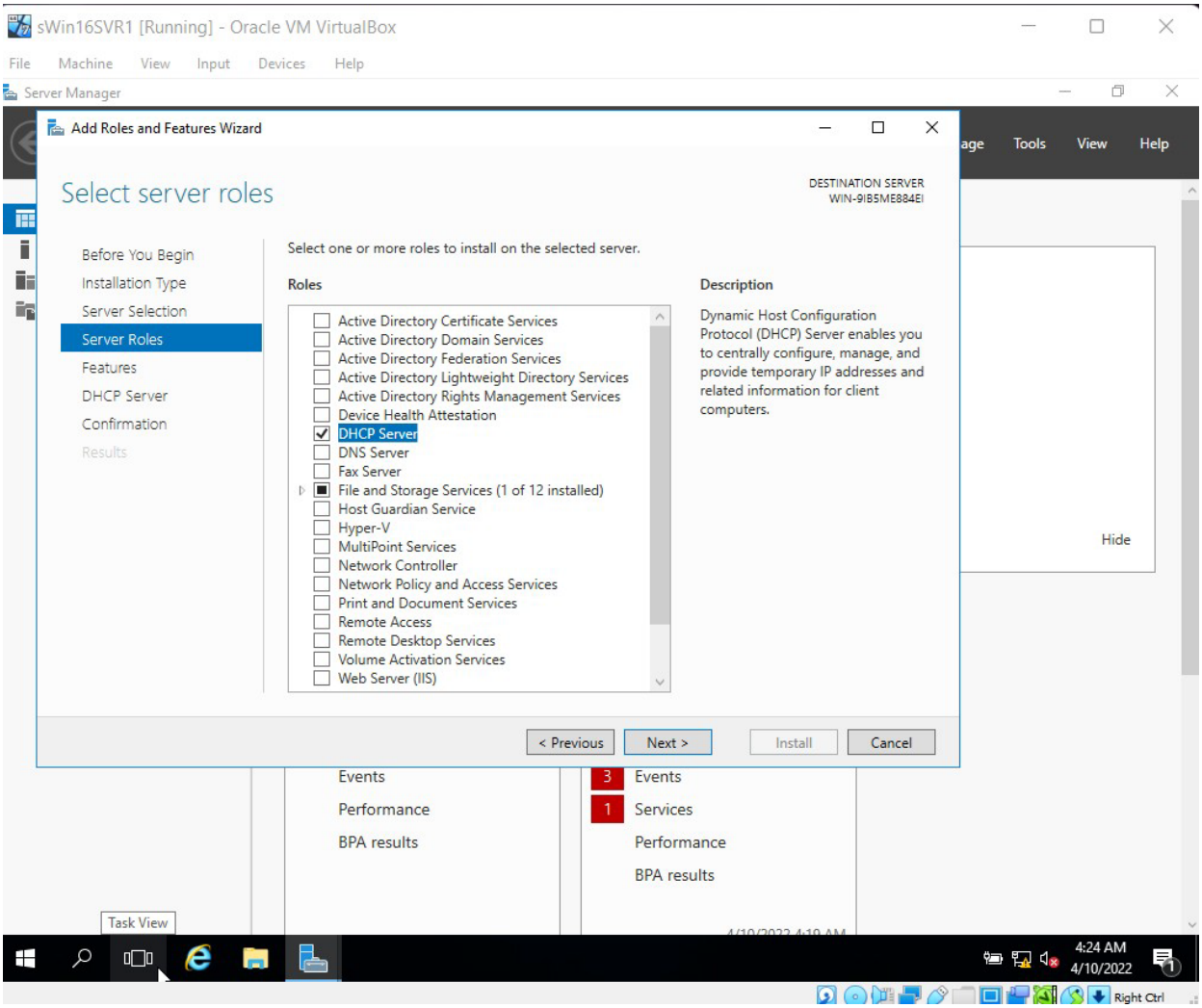


#Step 3 required us to connect both virtual machines, sWIN10PC1 and sWINSVR1 to the “Intnet” Internal Network.



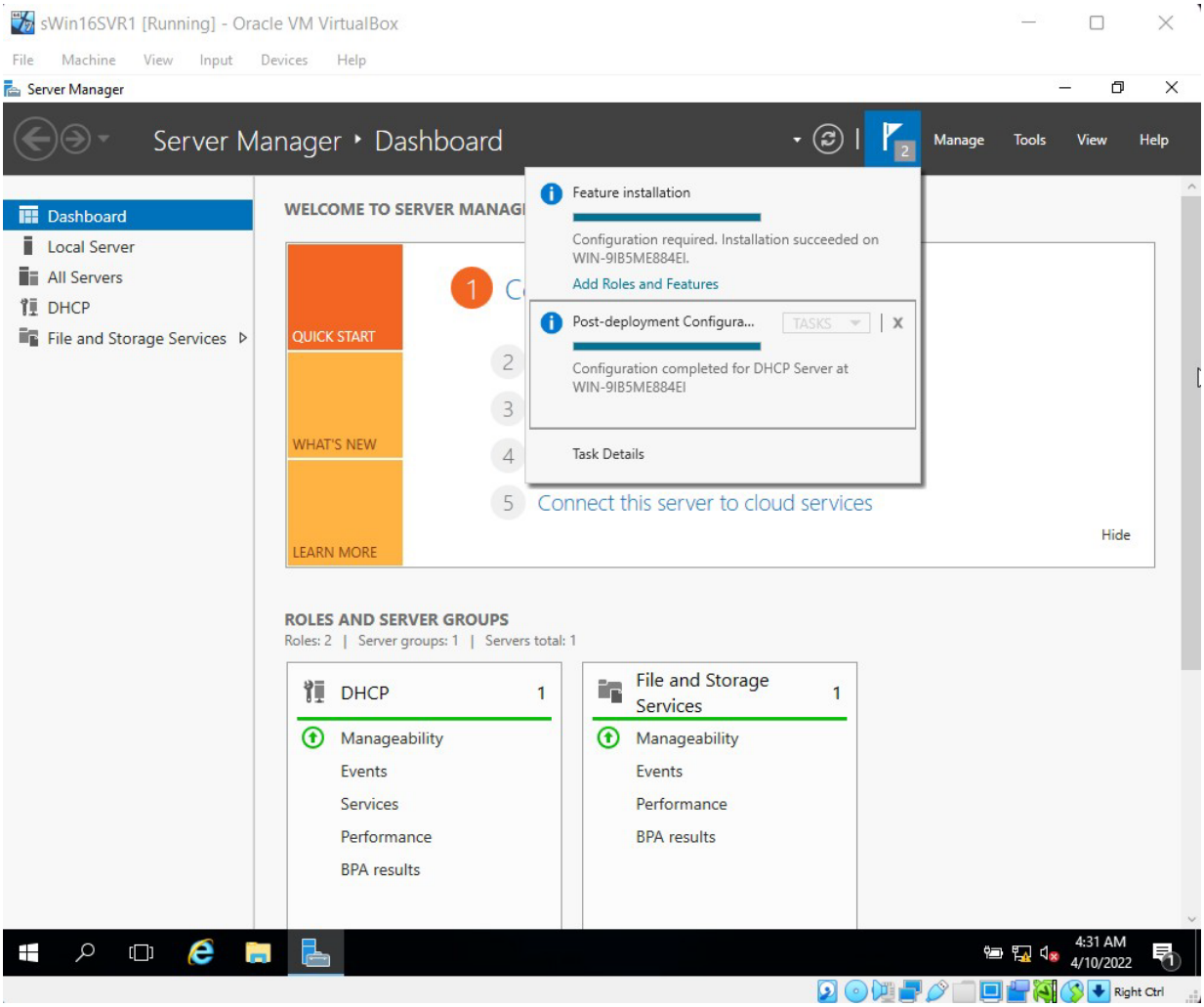
#Step3 required us to configure the IPv4 Address of the sWin16SVR1 Virtual Machine to 172.16.32.11.

Installing DHCP



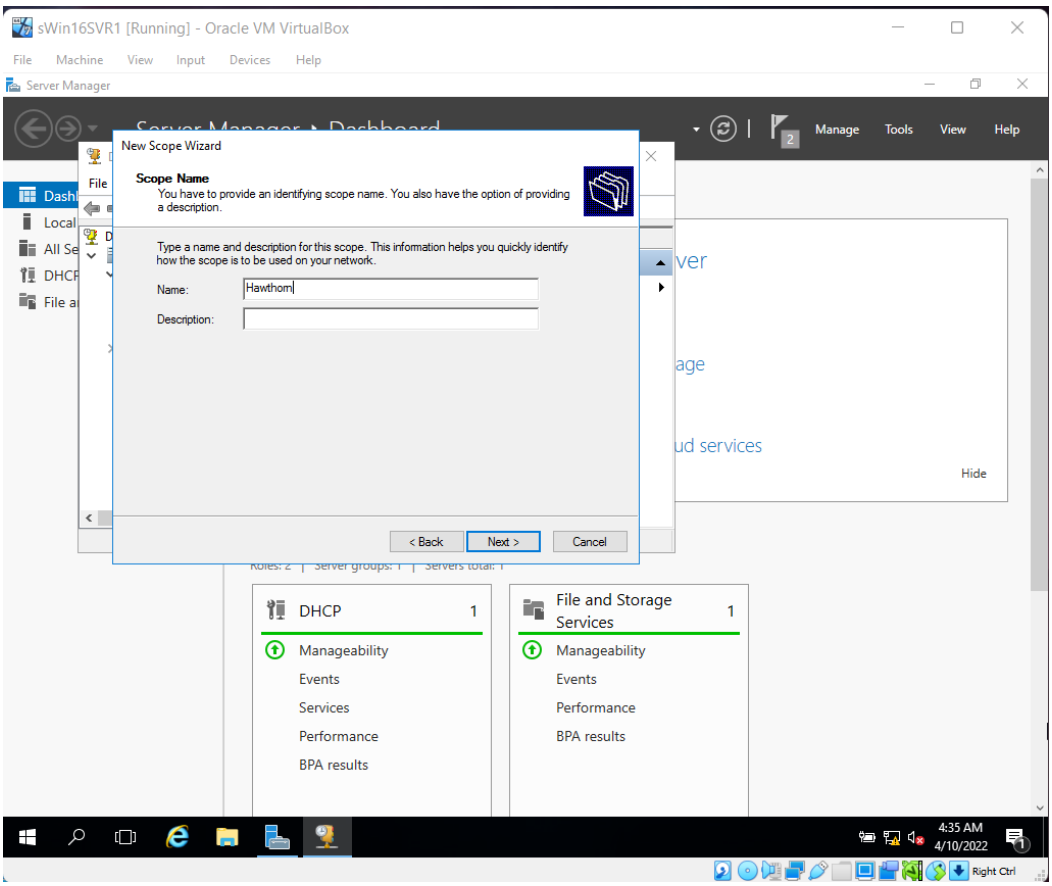
Steps #6 to #10 required us to install DHCP in the sWin16SVR1. It was done from the Manage Menu, then selecting add roles and features and then checking the DHCP Server box from the Select server roles page. Then confirming installation selections.

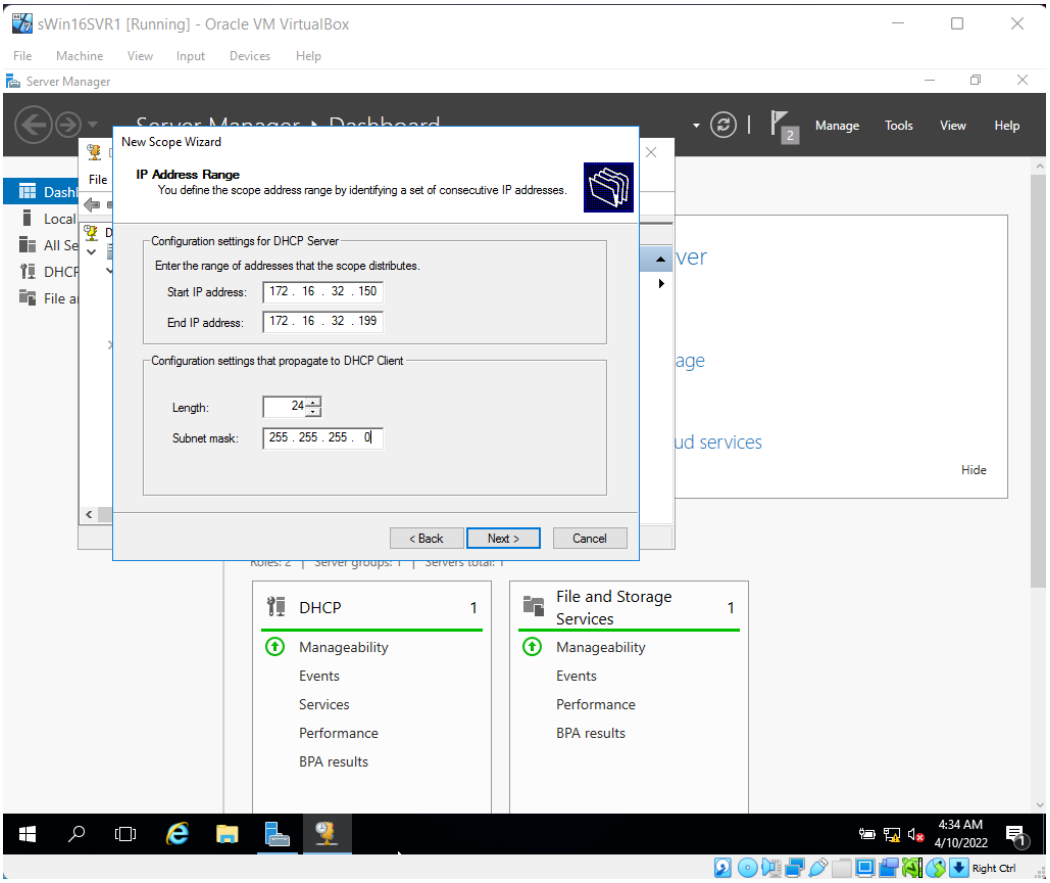
Post-deployment configuration

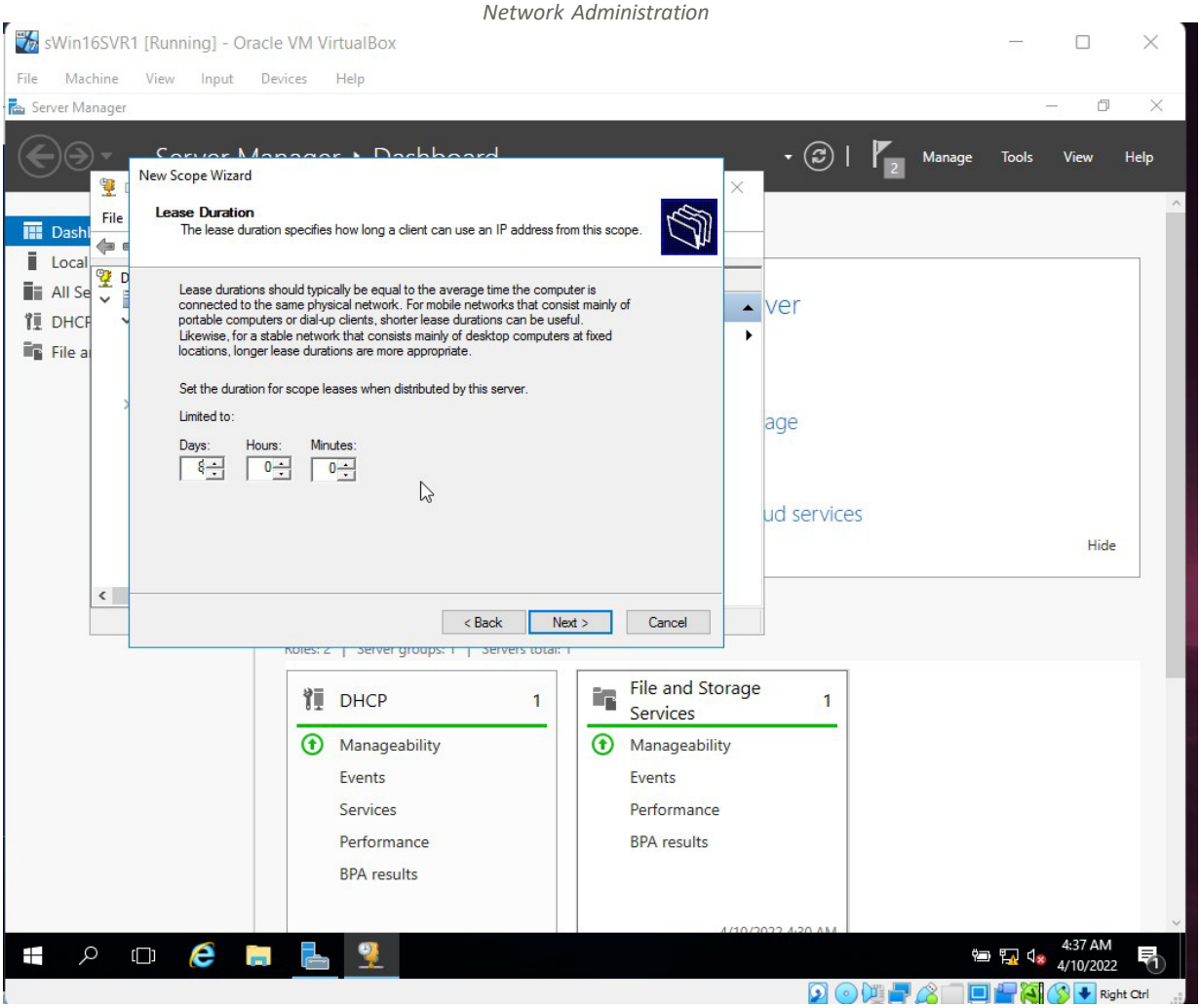


Steps #11 and #12 guided us on post deployment configuration. Above is screenshot of successful post-deployement configuration.

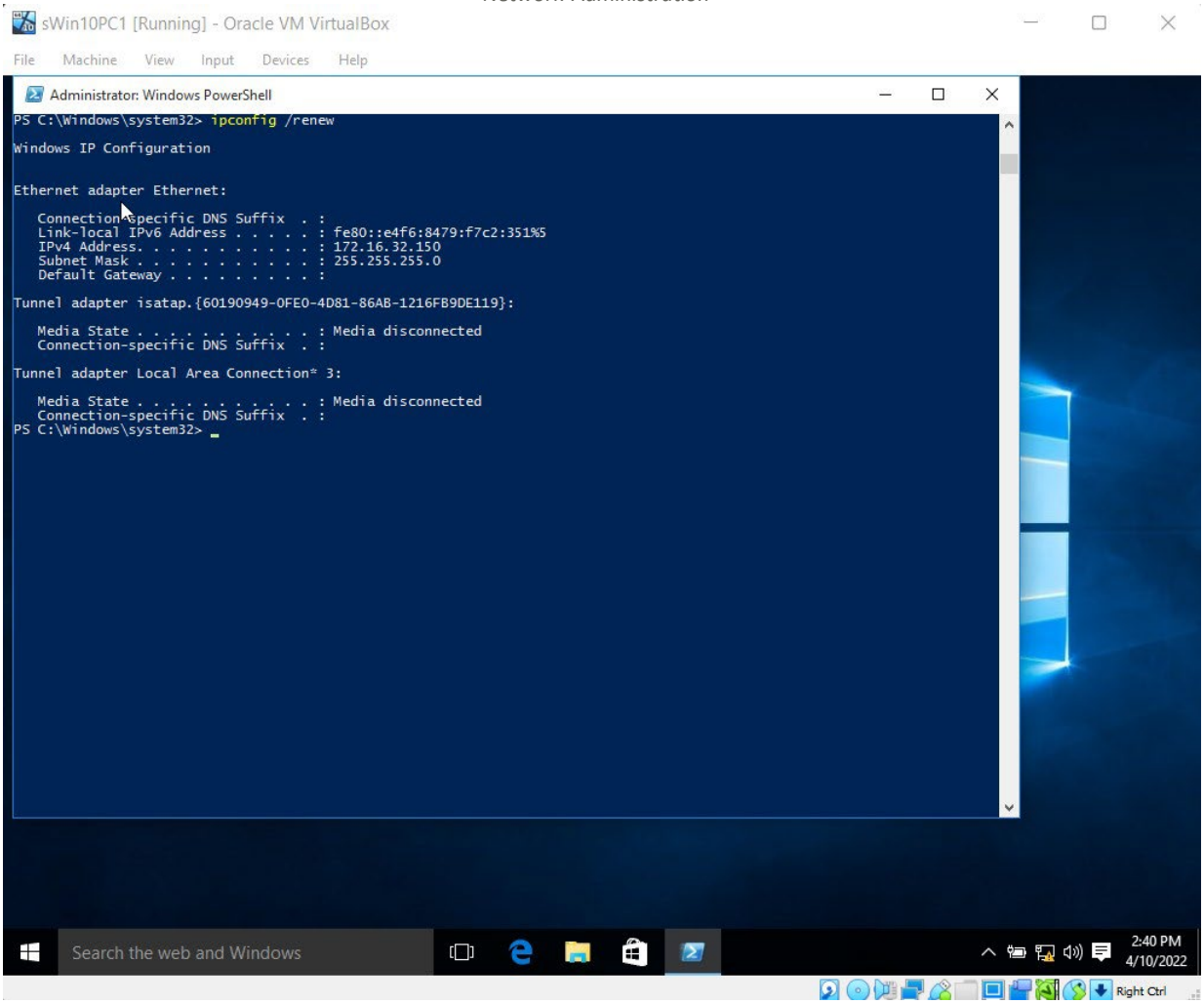
Creating a Scope





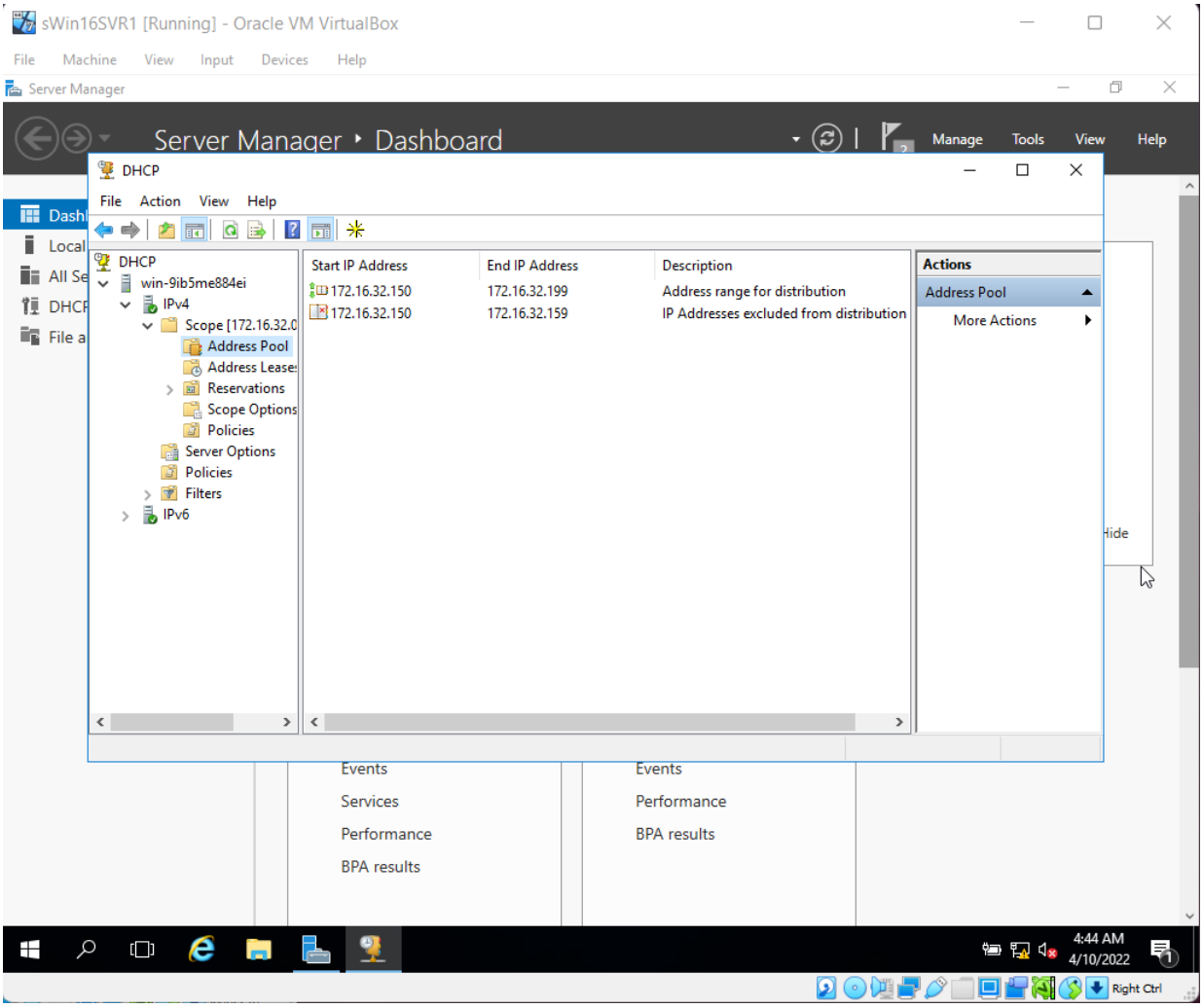


Steps #13 to #22 guided us in creating a scope, above are the screenshots of creation of a scope. It was accessed from the server manager, tools menu then DHCP, then right click on IPv4 and select New Scope. In the first page of scope setup wizard, Scope was named Hawthorn as shown in first screenshot. Then an IP range of 172.16.32.150 to 172.16.32.199 was entered with a length of 24 as shown in screenshot two. Then on the Lease Duartion Page, The limit was set to 8 Days, as the rule of thumb states that devices on cable, the lease time should be 8 days as shown in the last screenshot. Then the setup wizard concluded after DHCP Options Configurations. Then to remove the red arrow mark, the Scope was activated from the Context Menu.

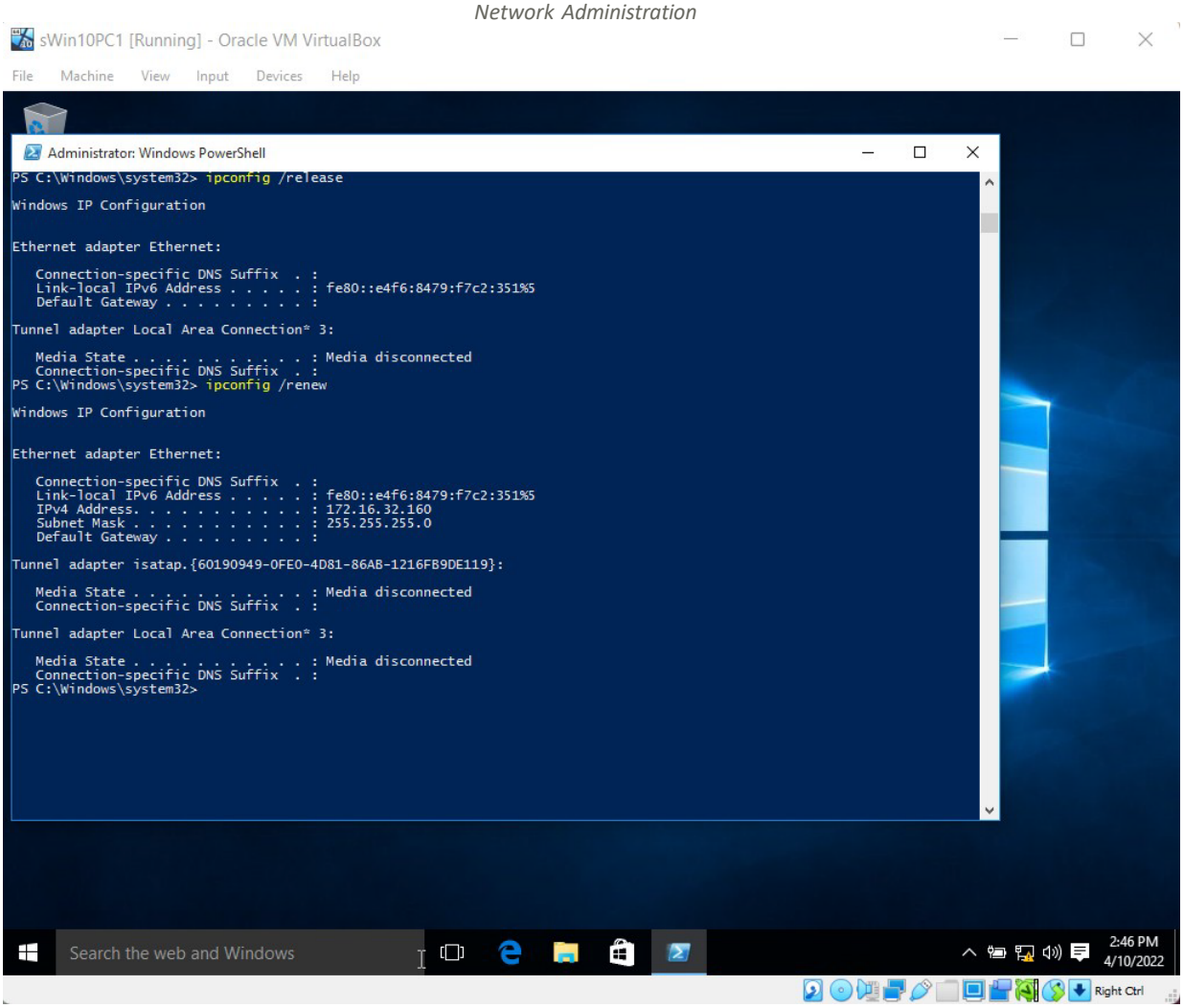


Step #23 required us to check if DHCP Server is working from the sWIn10Pc1 Virtual machine by entering ipconfig/renew in windows powershell and checking if correct IPv4 Address was shown.

Configuring Exclusions

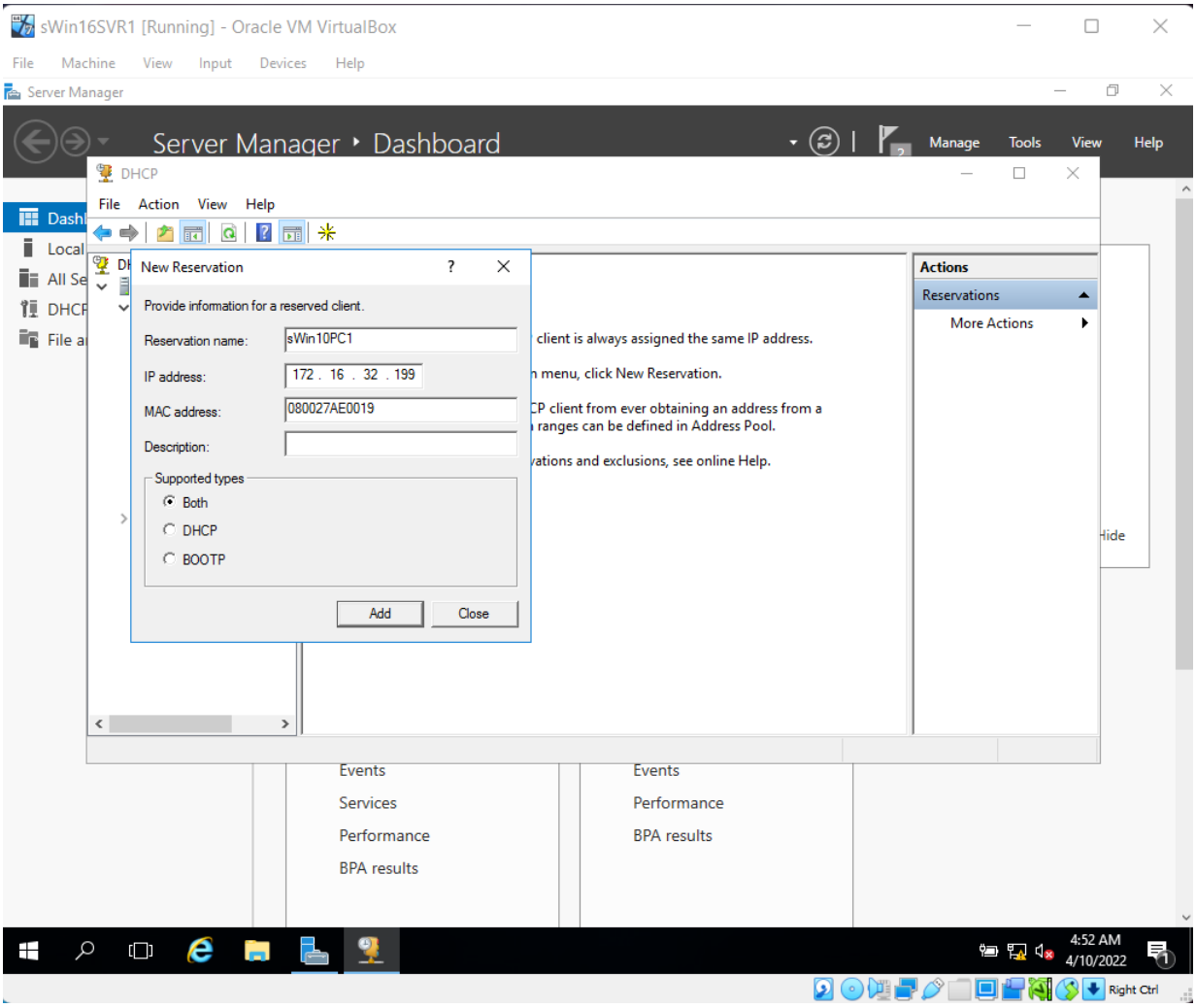


Steps #24 and #25 guided us in configuring Exclusions. IP Addresses ranging from 172.15.32.150 to 172.15.32.159 were excluded from distribution.

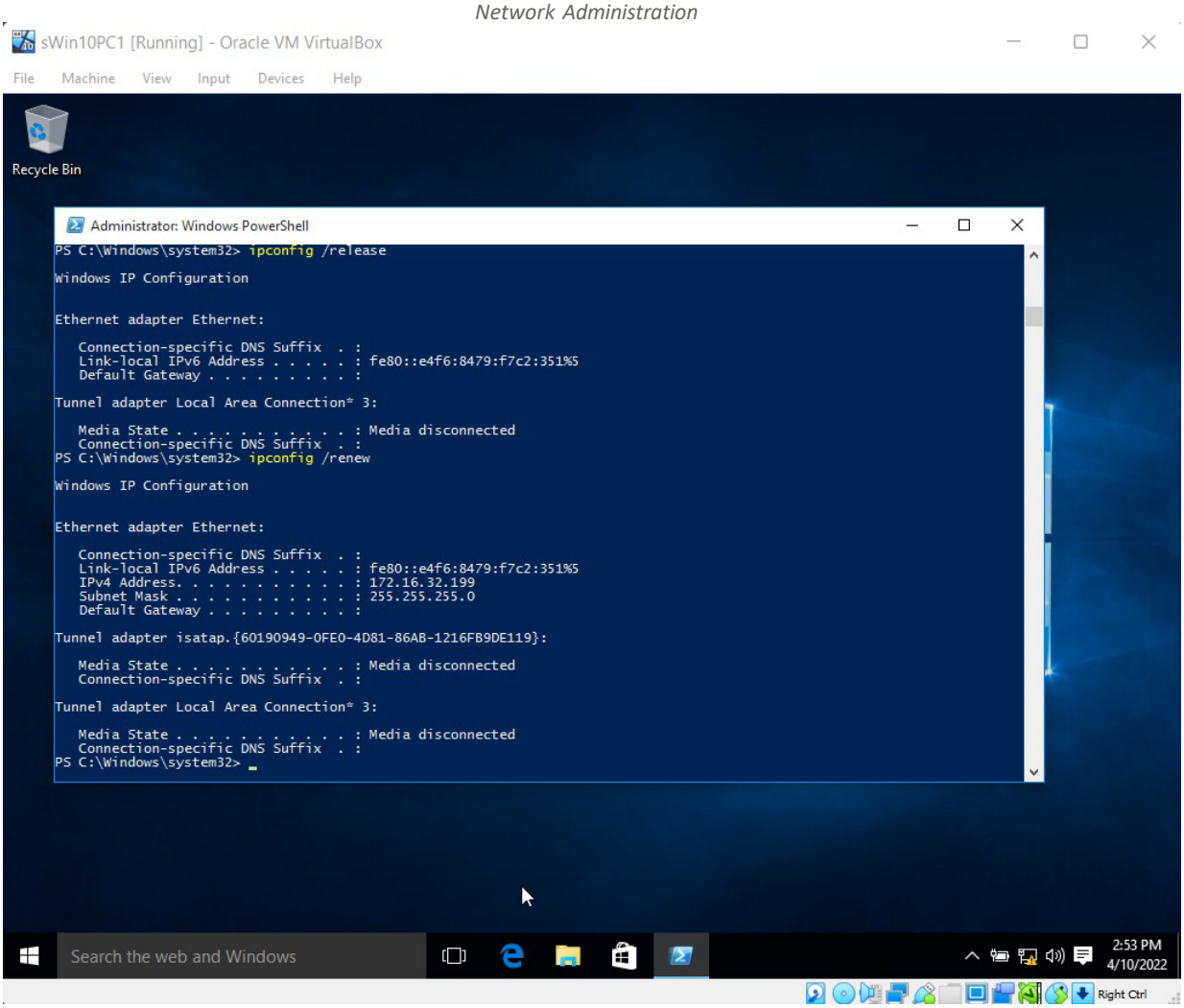


Step #25 wanted us to check if the exclusion range was successfully applied from the sWin10Pc1 virtual machine through the command prompt and indeed the exclusion range was applied as the IP Address alloted to the sWin10PC1 virtual machine was changed to 172.16.32.160 from 172.16.32.150. It no longer displayed 172.16.32.150 as it was included in the exclusion range.

Configuring a Reservation

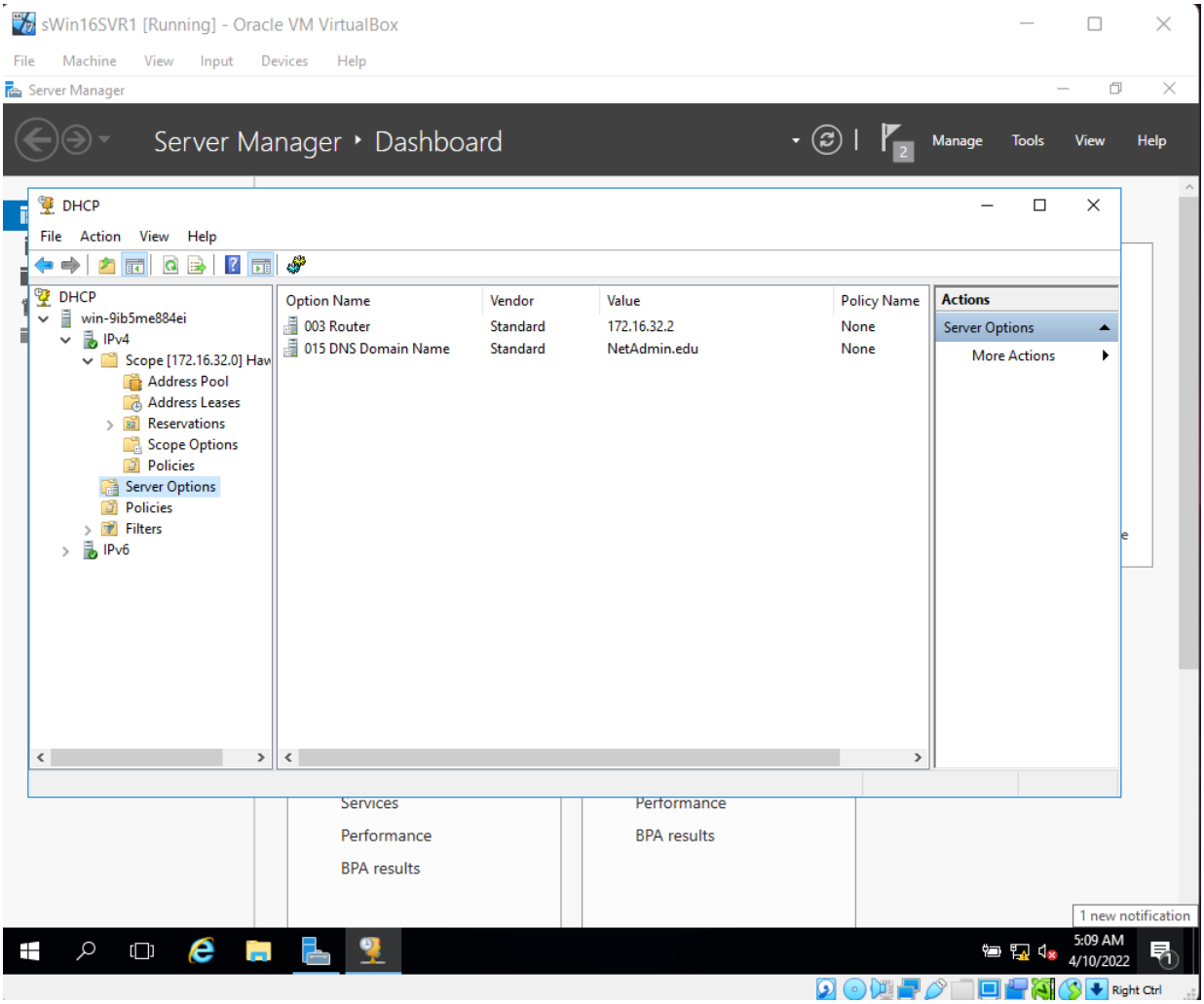


Steps #26 to #31 required us to configure a reservation of IPv4 Address 172.16.32.199 for sWin10PC1 virtual machine . It was done through the reservation configuration in the DHCP by resrving the IPv4 Address 172.16.32.199 for MAC Address of sWin10PC1.

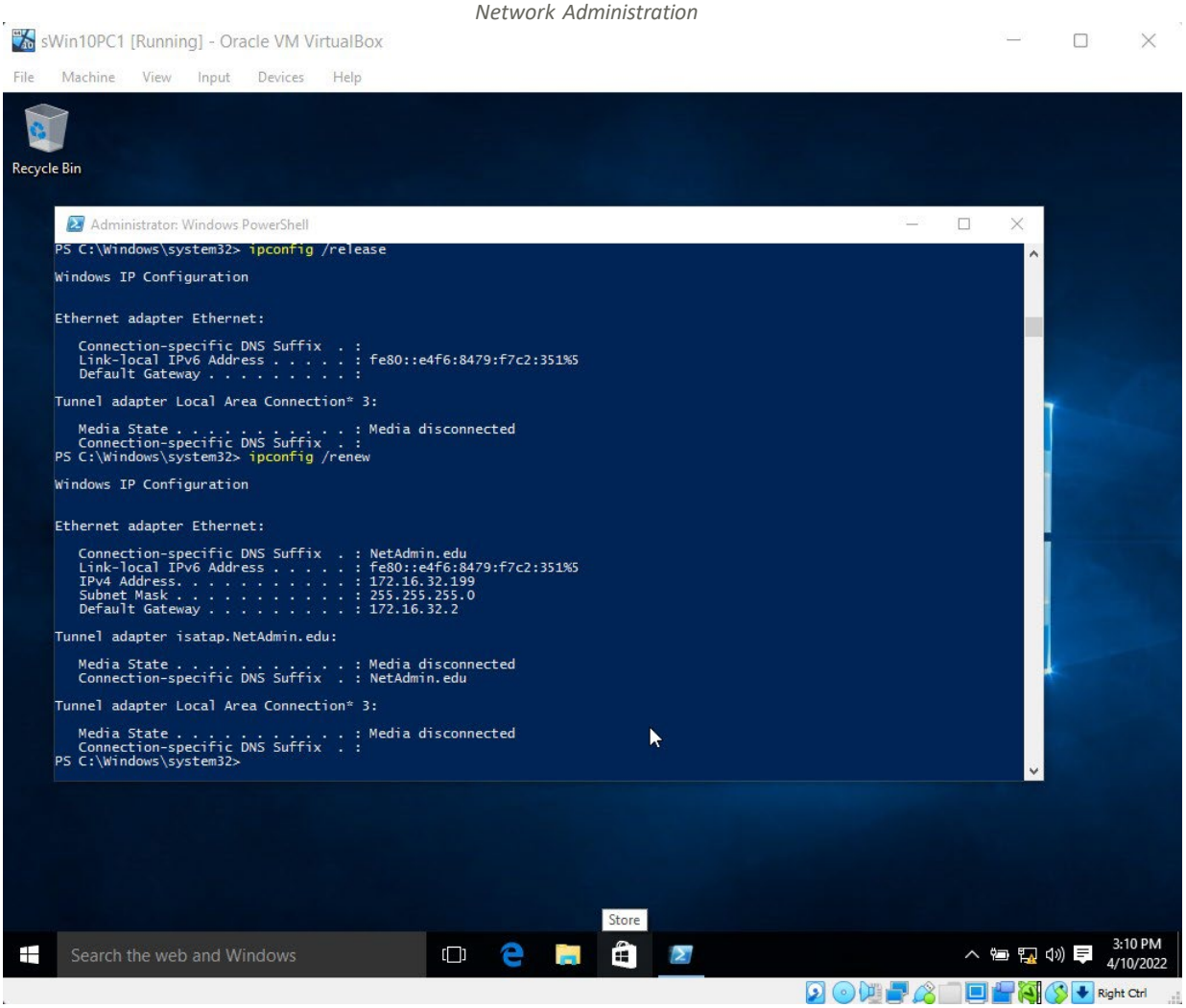


Step #32 wanted us to check if the IP Address Reservsation worked successfully and as shown in above screenshot, The IPv4 Adress for sWin10PC1 is shown as 172.16.32.199 which is the exact IP Address reserved for it.

DHCP Options

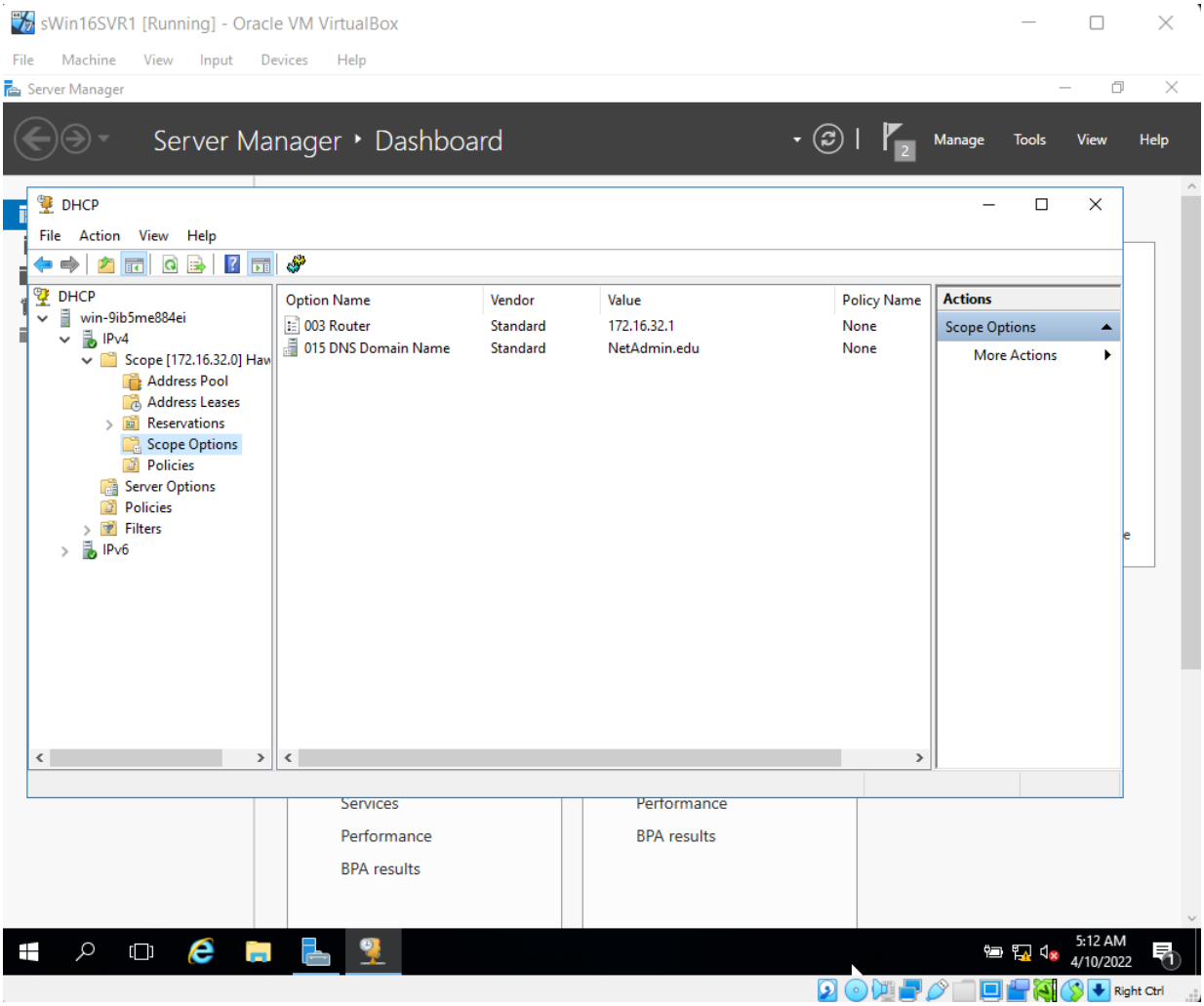


Step #35 instructed us on configuring the Server Options, from the server option, 003 Router option was set to **172.16.32.2** and the 015 DNS Domain Name was set to **NetAdmin.edu**.

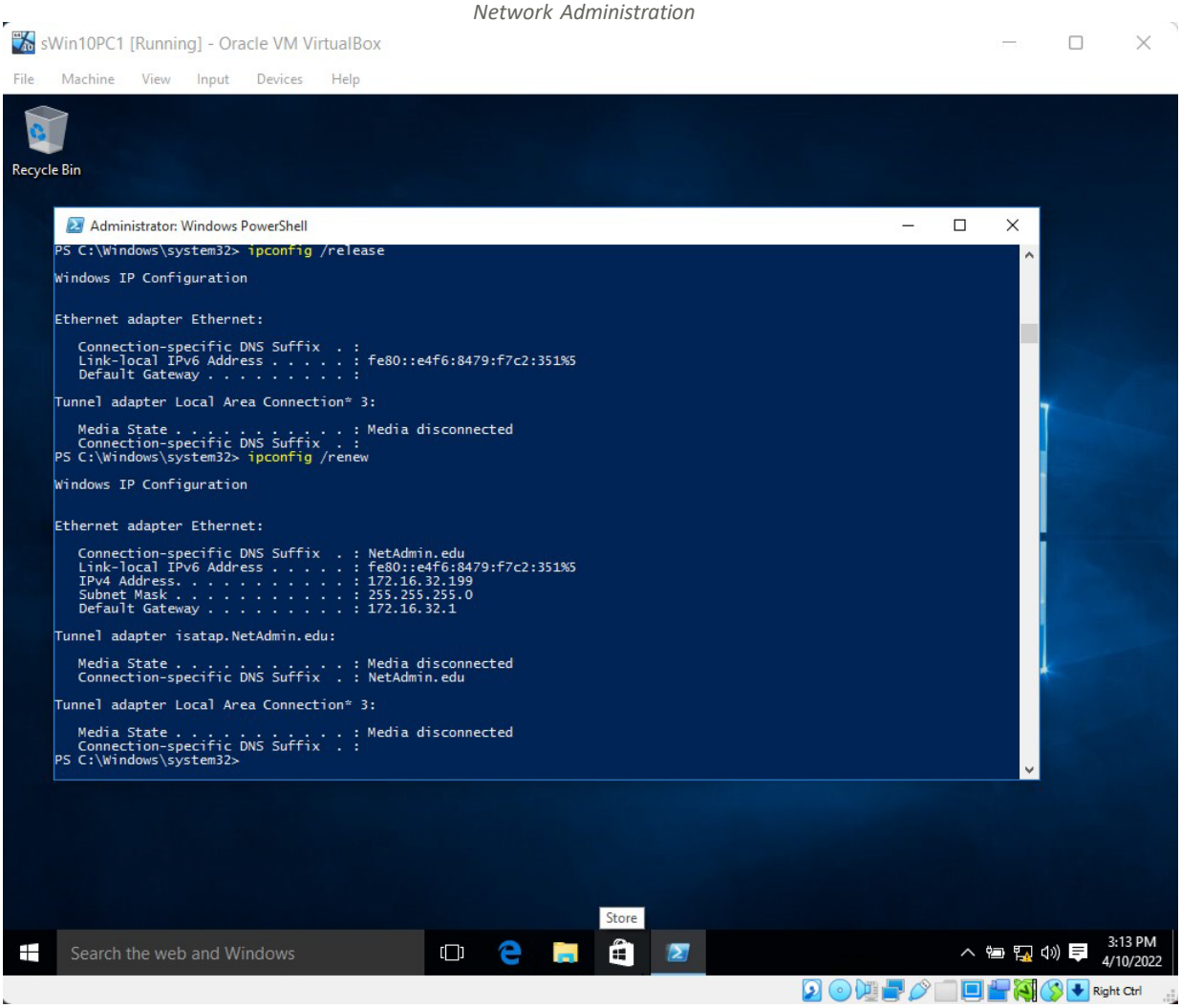


Step #36 intructed us on checking weather the Server Options configuratons worked successfully. As per the above screenshot, the Default Gateway was shown as 172.16.32.2 from the sWin10PC1 Virtual Machine, which was set by the sWin16Svr1's DHCP Server Options.

Scope Options

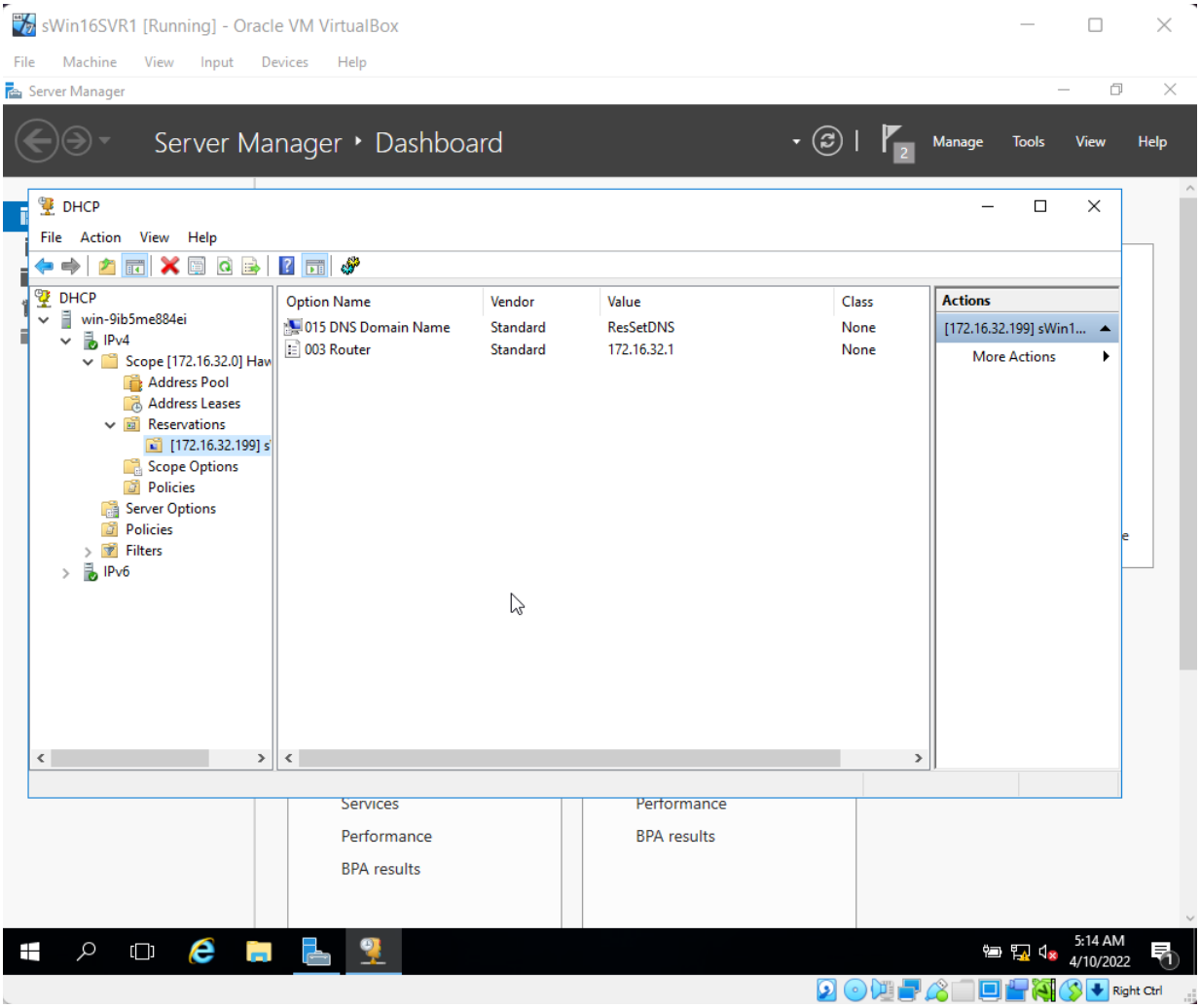


Step #37 instructed us on configuring the Scope Options, from the scope option, 003 Router option was set to **172.16.32.1.**



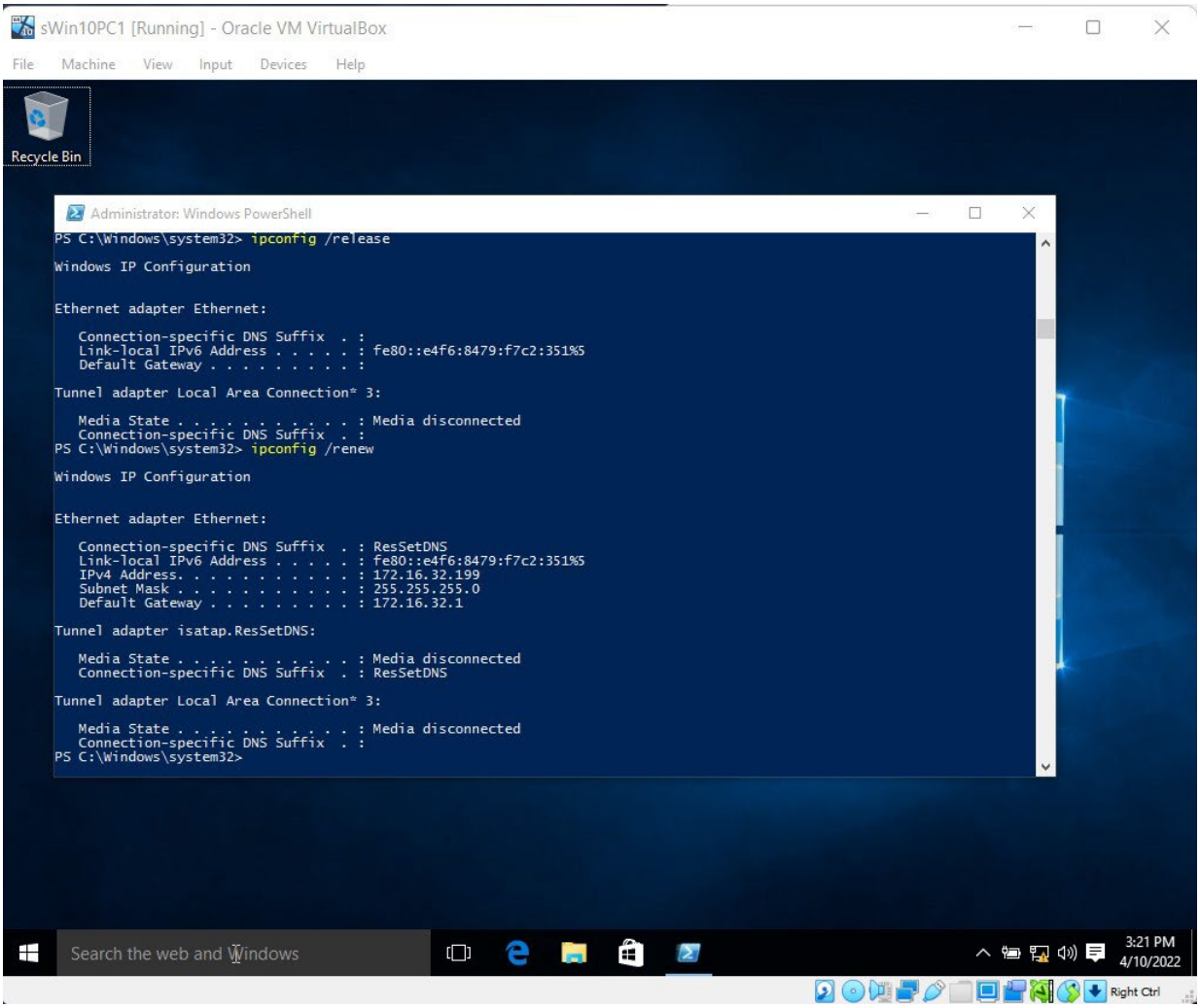
Step #36 intructed us on checking weather the Scope Options configuratons worked successfully. As per the above screenshot, the Default Gateway was shown as 172.16.32.1 from the sWin10PC1 Virtual Machine, which was set by the sWin16Svr1's DHCP Scope Options.

Reservation Options



Step #40 instructed us on configuring the Reservation Options, from the Reservation option, 015 DNS Domain Name was set to **ResSetDNS.**

Option Precedence



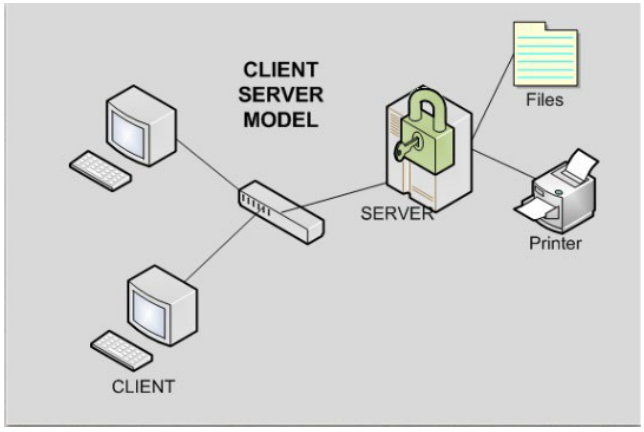
Steps #41 and #42 instruced us on checking which Configuration Option had the most Precedence. As all three Options DNS Domain Name had been set, when called from the sWin10PC1 Virtual Machine, which options DNS Domain Name would show up? As per the above screenshot, the Reservation Options DNS Domain Name showed up, which proved Reservation Option had the most Precedence

TNE10005 Journal Lab (#5)

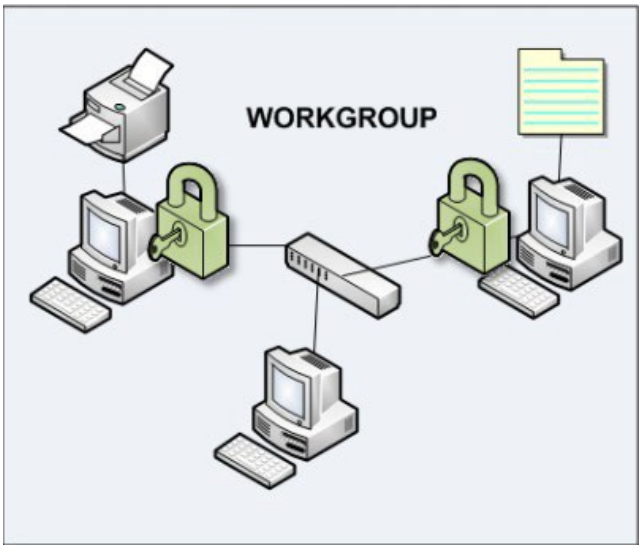
Khalid Yaseen /baig / ID #102763240

What I learned in this week's Lecture.

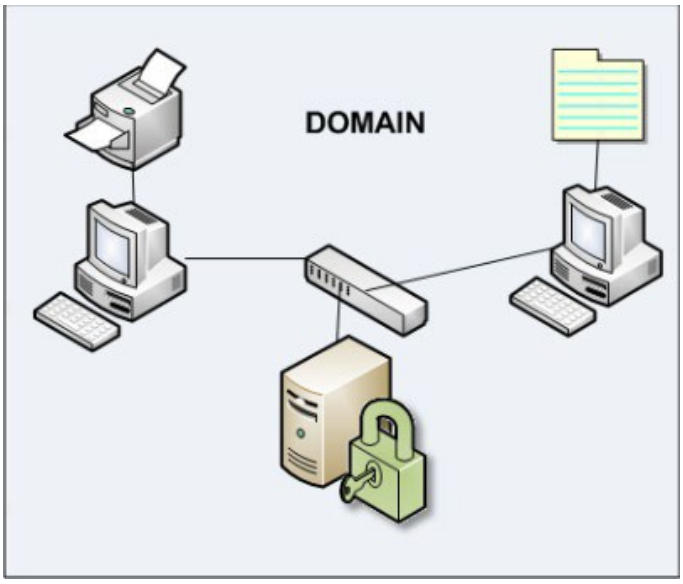
- According to a Historical Network (Client Server), all resources are shared and managed by the server..



- A Workgroup is a peer-to-peer network, with one password for each user on each computer they visit, each PC that shares a resource acting as a server, and each PC that accesses a shared resource acting as a client.



- According to the domain model, resources can be found anywhere on the network. Users and computer accounts are authenticated by the domain controller. The domain controller grants access to resources.



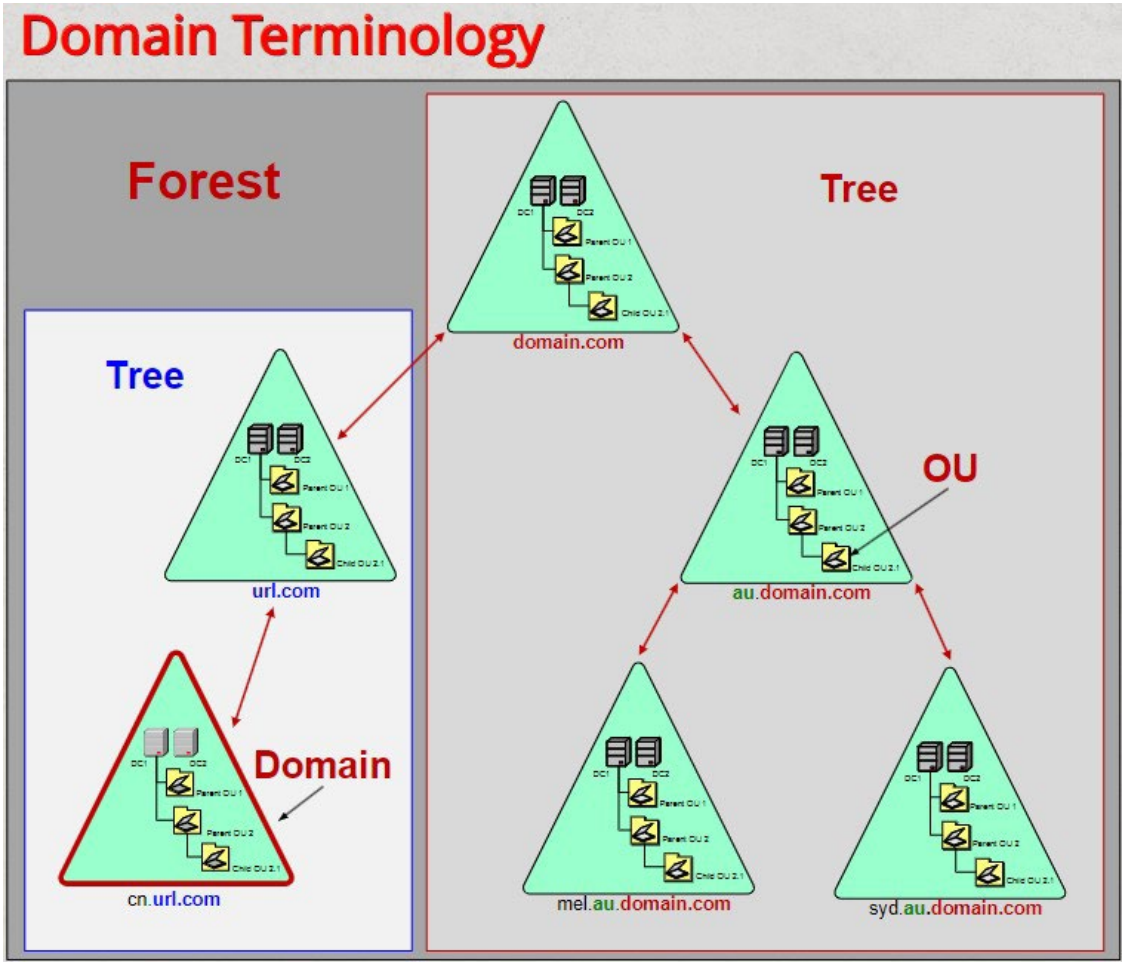
- User Accounts allow us to regulate access to computers and computer objects. Every user account has a unique Security Identifier (SID) across the system. Every time a user accesses an item, this SID is utilized.

- An Access Token is produced each time a user logs into a system. This access token comprises the SID of the user account. This token is displayed when an object is accessed and is used to authorize the object's access.

- The SIDs in the Access Token are compared to the ACEs in the Discretionary Access Control List when a user seeks to access an object (e.g., a file, folder, or printer) (DACL). When a match is detected, the user is given the option of granting or denying access to the object. The user is refused if no match is discovered.

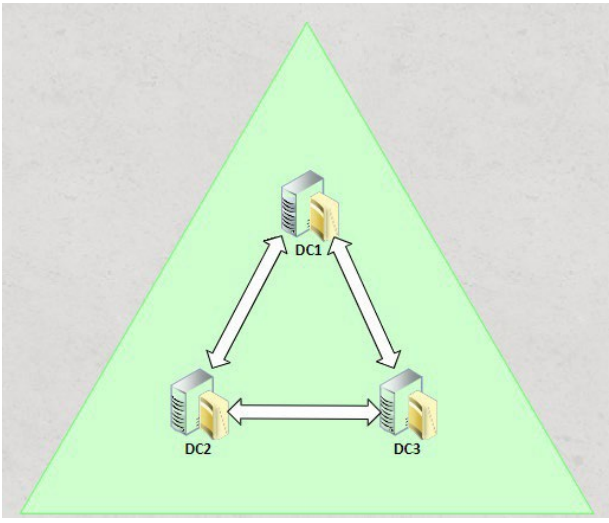
- Active Directory (AD) is a database that is Object Oriented (it has a schema). Users, Computers, Printers, Sites, and Volumes are examples of items in this database (e.g. HDDs). We can utilize Active Directory to regulate who has access to and can manage these things. We may utilize Active Directory (AD) to distribute software and settings to machines.

- A forest is a group of AD DS domains linked by two-way trust relationships that are formed automatically. A domain is a logical administrative unit in which people, computers, and other items are housed. A Tree is a group of AD DS domains with a continuous namespace and a shared root domain. Within a domain, an Organizational Unit (OU) is a container that organizes people, computers, and other OUs.



- To set up a domain, the operating system must be Windows Server, DNS must be pre-installed or installed at the same time, the Active Directory Domain Service (ADDS) role must be installed first, and the server must subsequently be promoted to a Domain Controller.

- Any object created on one Domain Controller (e.g., a user account, a computer account, etc.) will be replicated to the other Domain Controllers in the Active Directory Domain. As a result, all AD objects and records are automatically backed up. If one DC fails, the logins can be authenticated by other DCs.



Group Scopes – a brief overview – Memorise last 3!

- **Local** – used by 'non-Administrators' to share resources on a local computer in a workgroup or a domain. *(We will not use Local groups in Network Admin)*
- **Global** – used to group user and computer **accounts** from the **local** domain.
  (Can also be used to group other Global groups from the local domain)
- **Domain Local** – used to provide access to **resources** in the **local** domain
- **Universal** – used to group **Global** groups from **multiple domains**

GROUP SCOPES for Network Admin

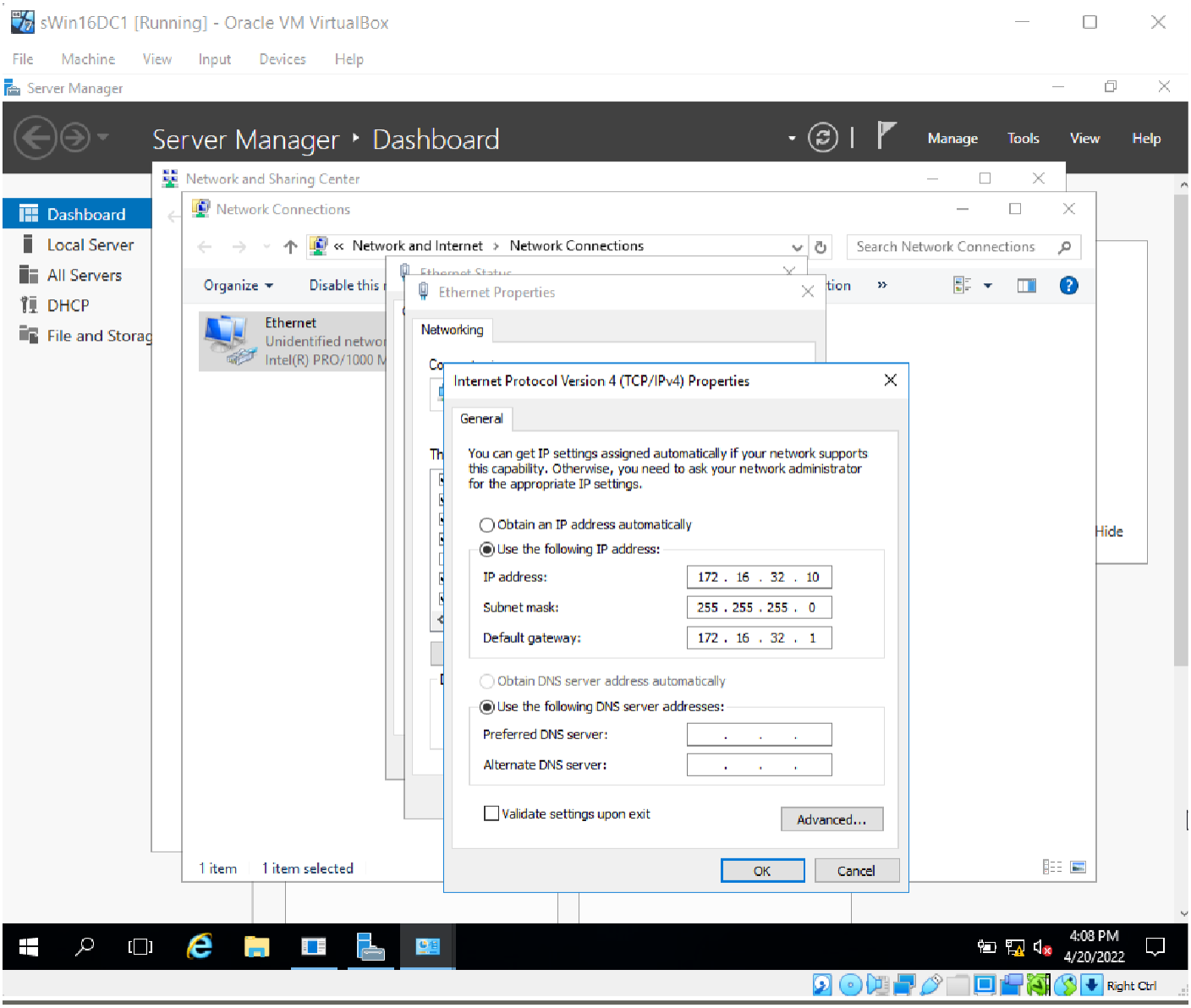
Scope	Purpose	Membership (i.e. who can be a member of this group)		Resources (i.e. where are the resources that this group can have permissions to?)		Limitations
		From the same domain	From another domain	In the same domain	In another domain	
G Global	**Role** *To group **Identities** (i.e. user and computer accounts) that have similar requirements*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ ~~Universal Groups~~	**No**	**Yes**	**Yes**	Cannot have members from another domain
DL Domain Local	**Resource** *To control **Access** to resources (e.g. files, folders & printers)*	User Accounts Computer Accounts Global Groups Domain Local Grps Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups* **Only from the same forest*	**Yes**	**No**	Cannot give access to resources in another domain
U Universal	*To collect groups from multiple domains in the forest.*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	**Yes**	**Yes**	Do not belong to any one domain, but to the whole forest. Hence has an overhead that can slow all DCs in the forest down

Local groups will not be used in Network Admin.

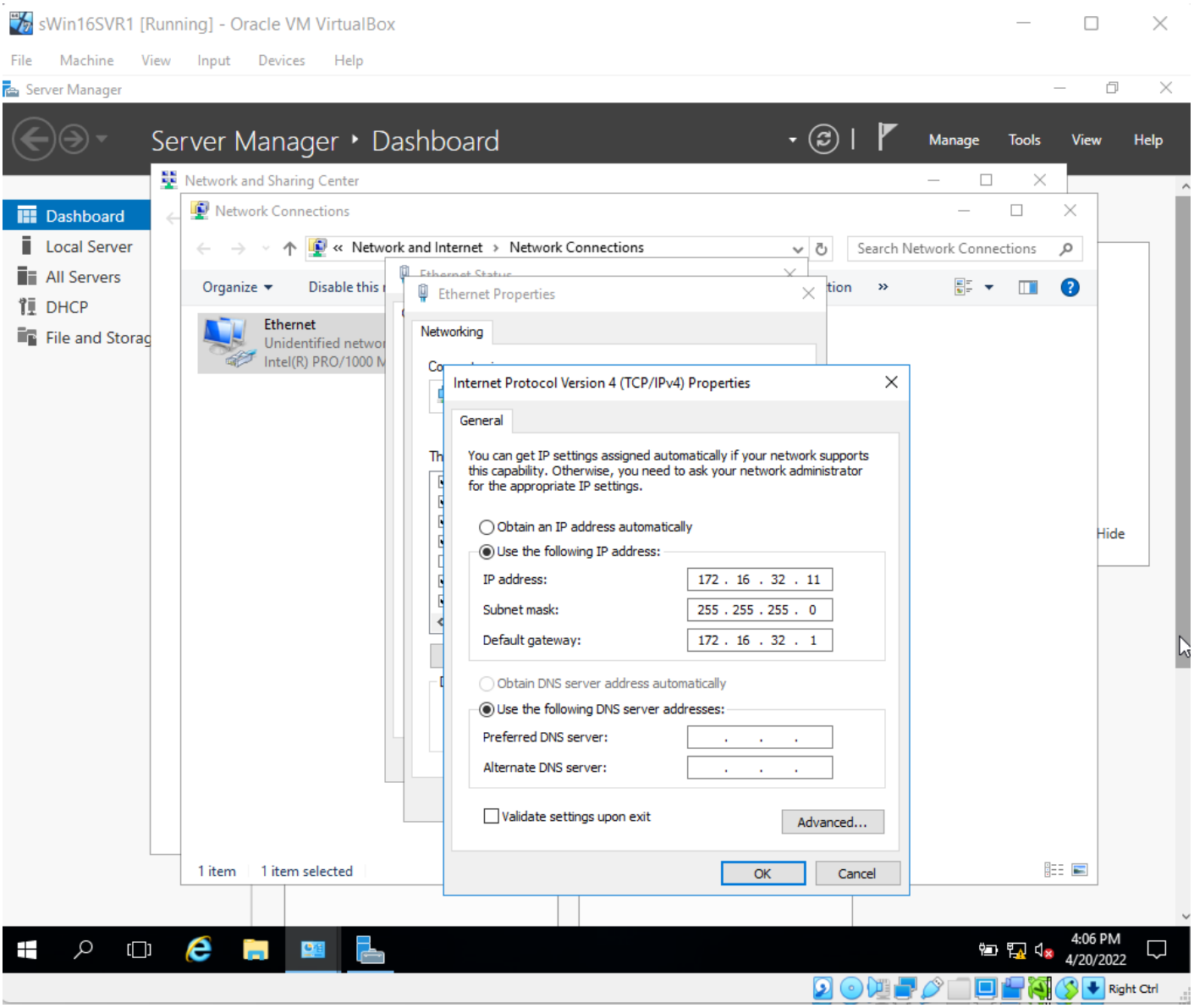
Apply groups using an **I ➡ G ➡ DL⬅ A** *like strategy.*

This week’s lab activities.

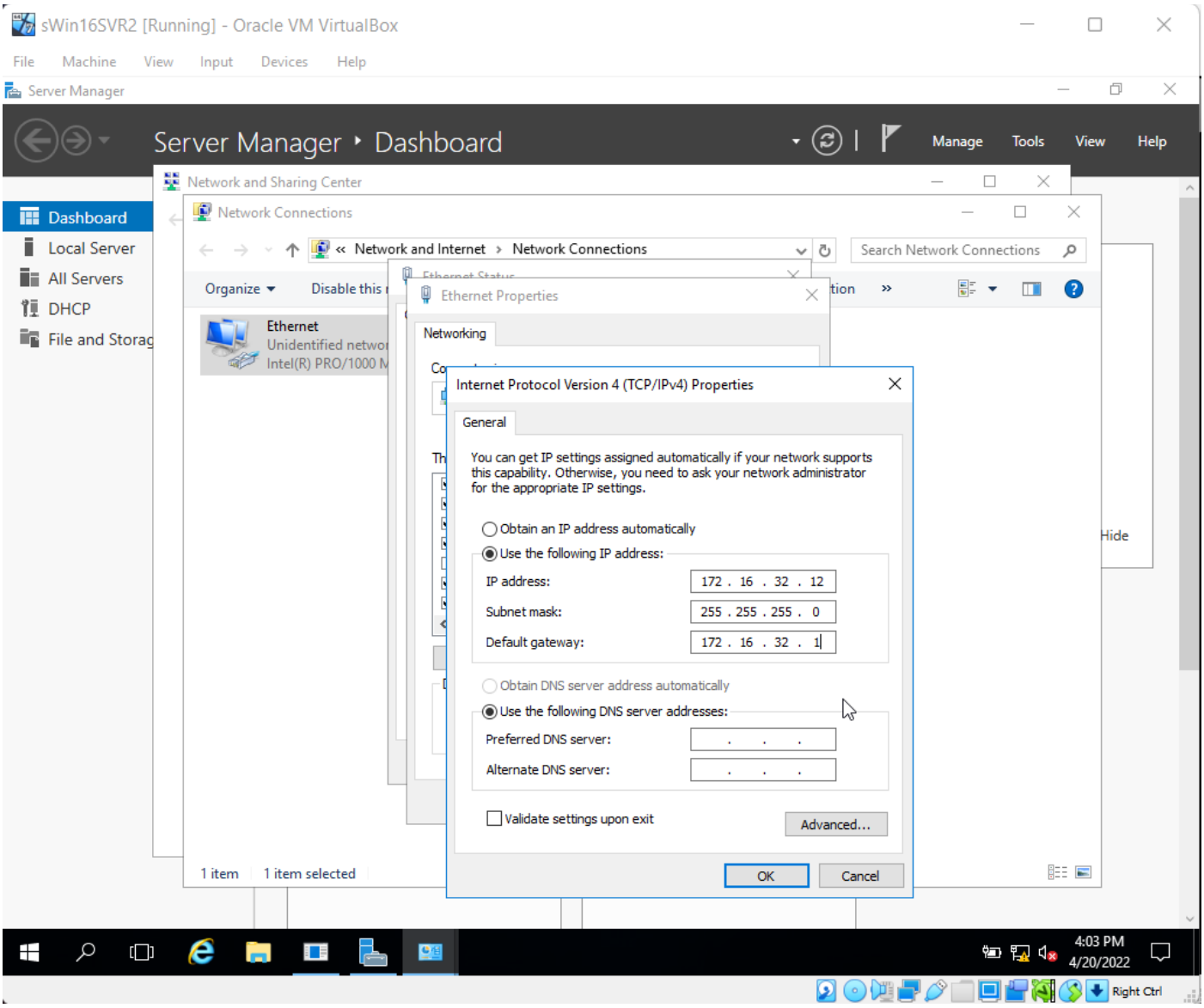
Screenshots of important steps required for Lab



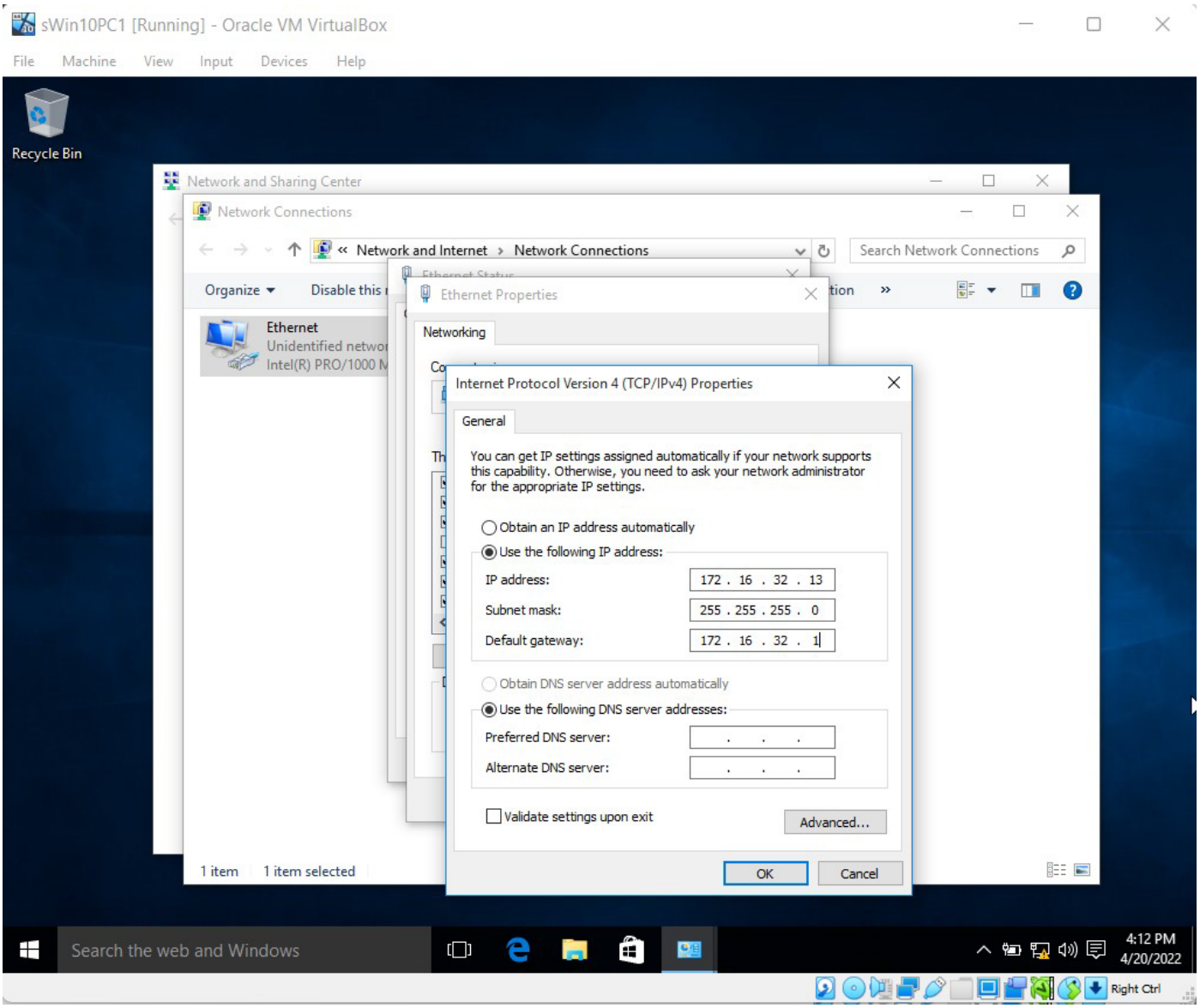
Step #1 required us to_configure the IP Address of sWin16DC1 Virtual Machine to 172.16.32.10, Subnet Mask to 255.255.255.0 and default gateway to 172.16.32.1 and turn off the firewall settings as well.



Step #1 required us to configure the IP Address of sWin16SVR1 Virtual Machine to 172.16.32.11, Subnet Mask to 255.255.255.0 and default gateway to 172.16.32.1 and turn off the firewall settings

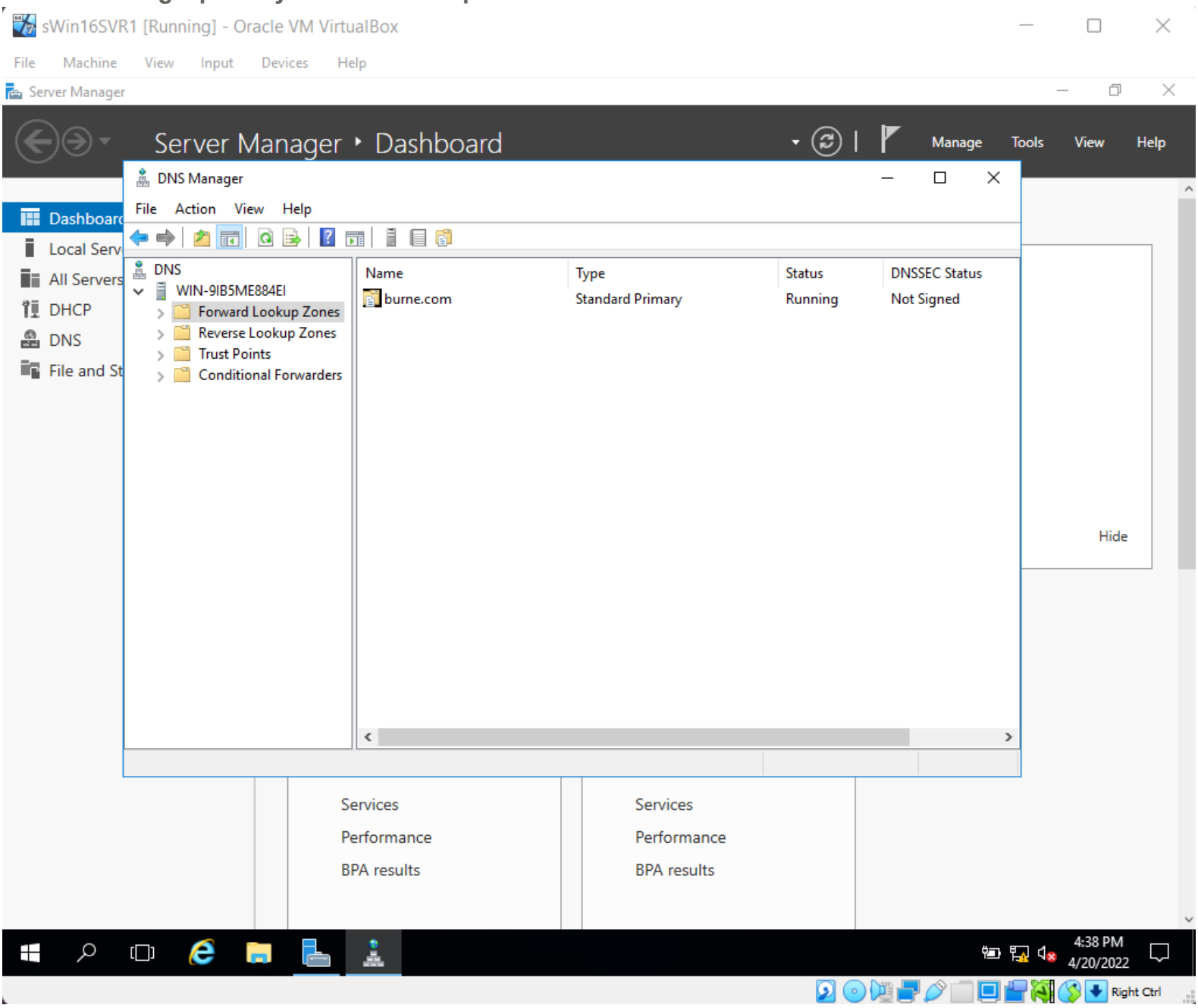


Step #1 required us to configure the IP Address of sWin16SVR2 Virtual Machine to 172.16.32.12, Subnet Mask to 255.255.255.0 and default gateway to 172.16.32.1 and turn off the firewall settings



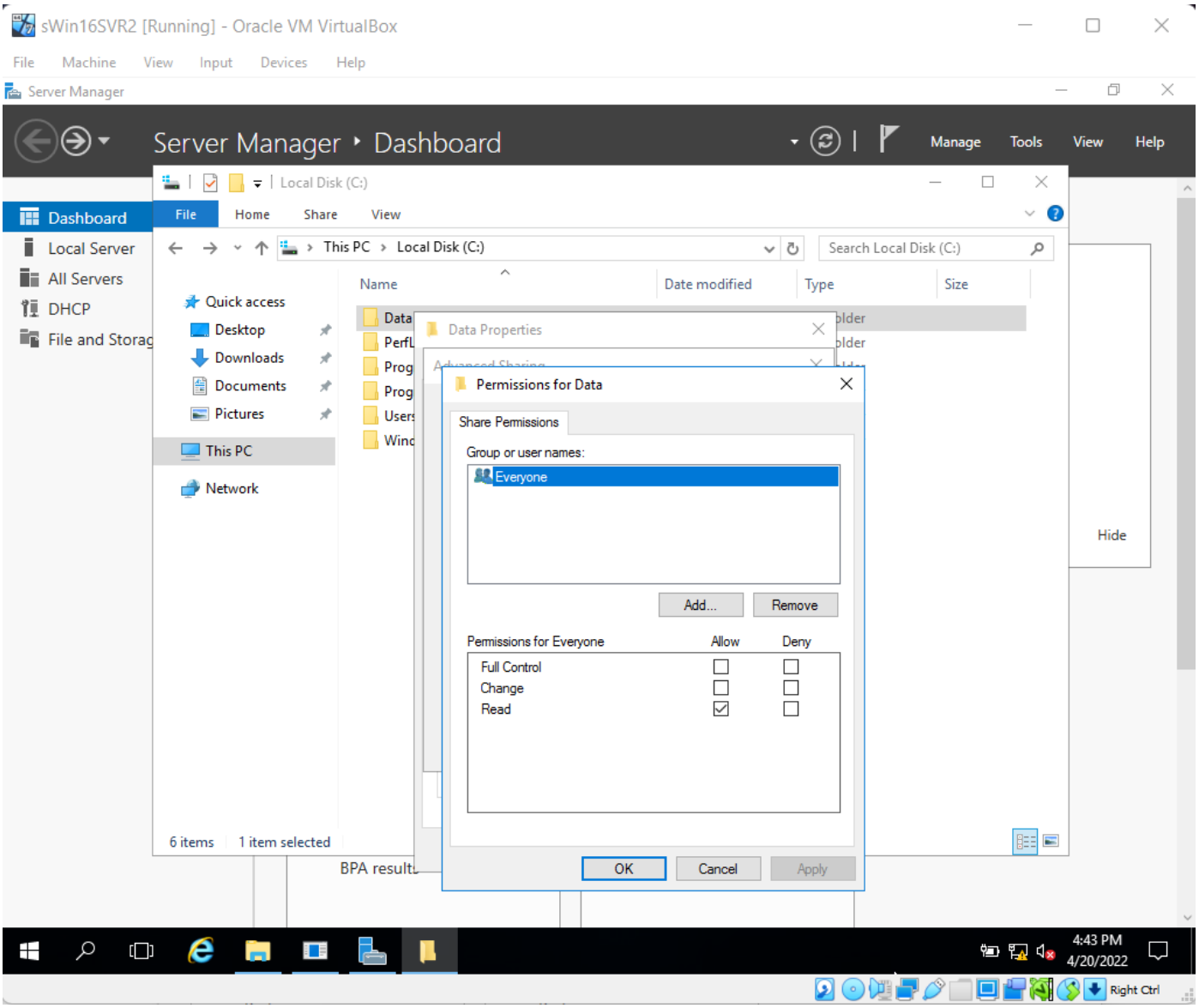
Step #1 required us to configure the IP Address of sWin10PC1 Virtual Machine to 172.16.32.13, Subnet Mask to 255.255.255.0 and default gateway to 172.16.32.1 and turn off the firewall settings

Creating a primary forward Lookup zone



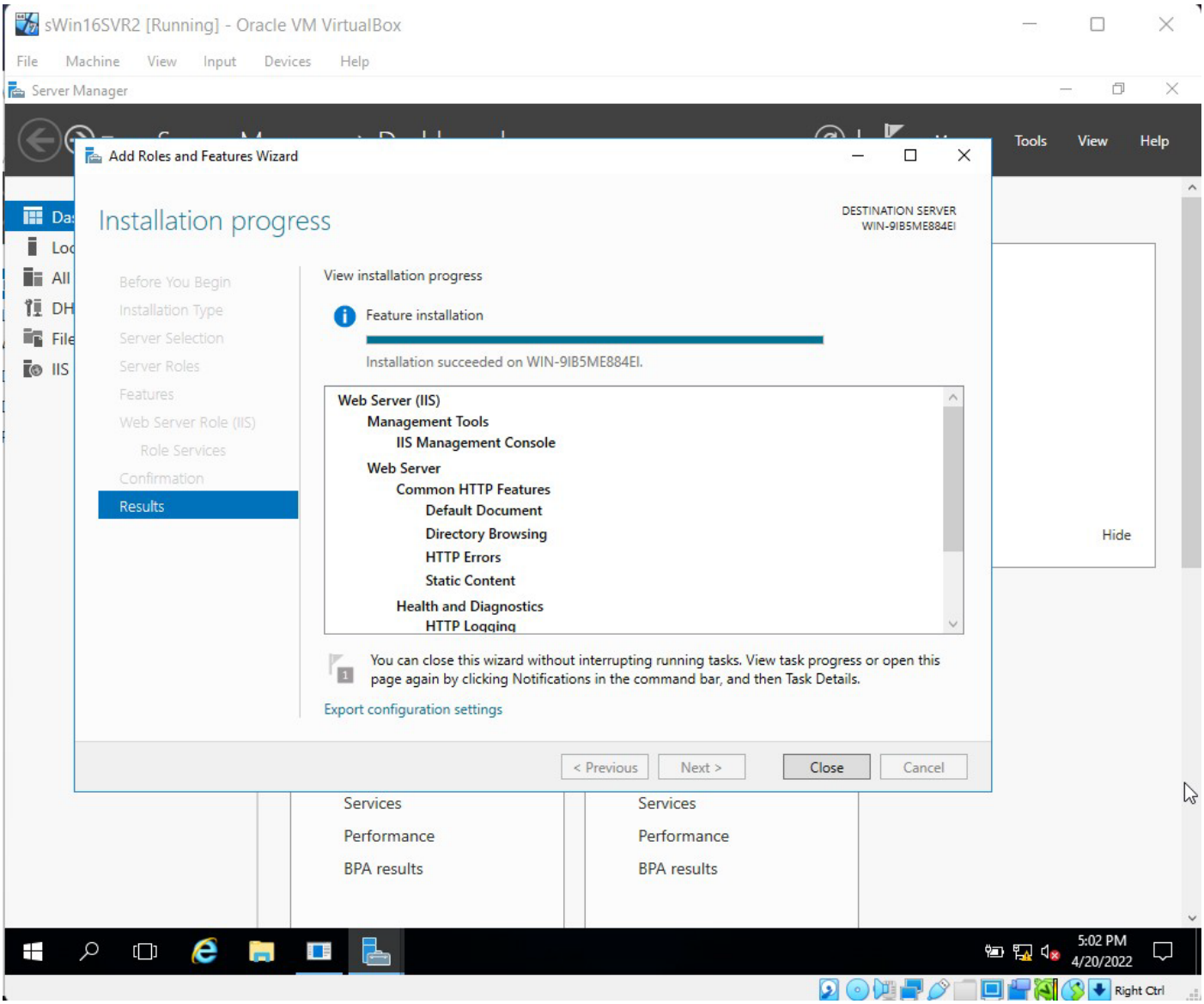
After Successful installation of DNS Server in the sWin16SVR1 virtual Machine, Steps #6 to #10 required us to create a primary forward lookup zone in the DNS manager. The zone was named “burne.com”.

Creating Network Resources.

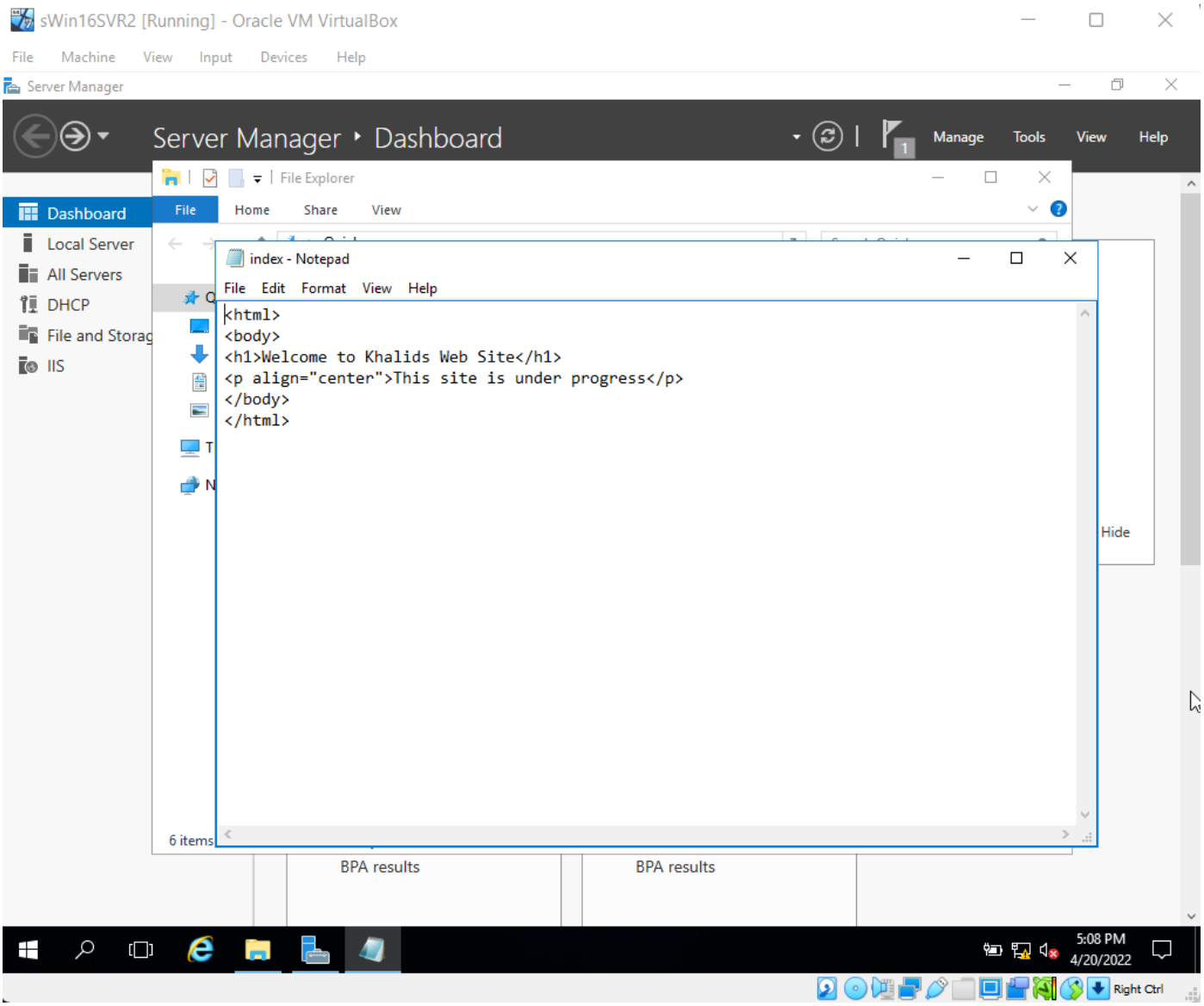


Steps #11 to #14 required us to configure a folders sharing setting as such that everyone with the network path of the folder are able to access the folder and read its contents.

Web Server

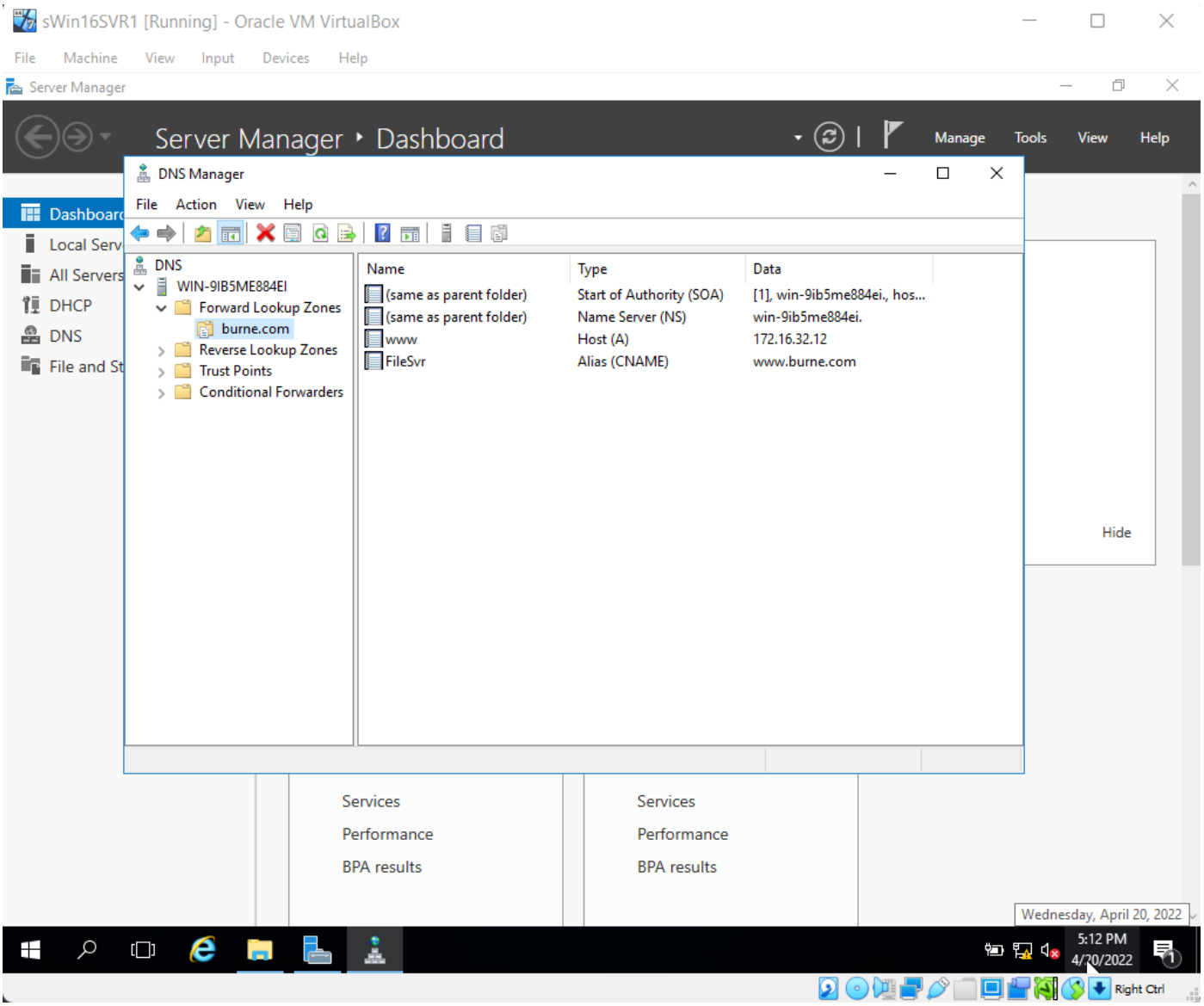


Steps #15 and #16 required us to add Web Server(IIS) role from the Add Roles and Features wizard in the sWin16SVR2 Virtual Machine.



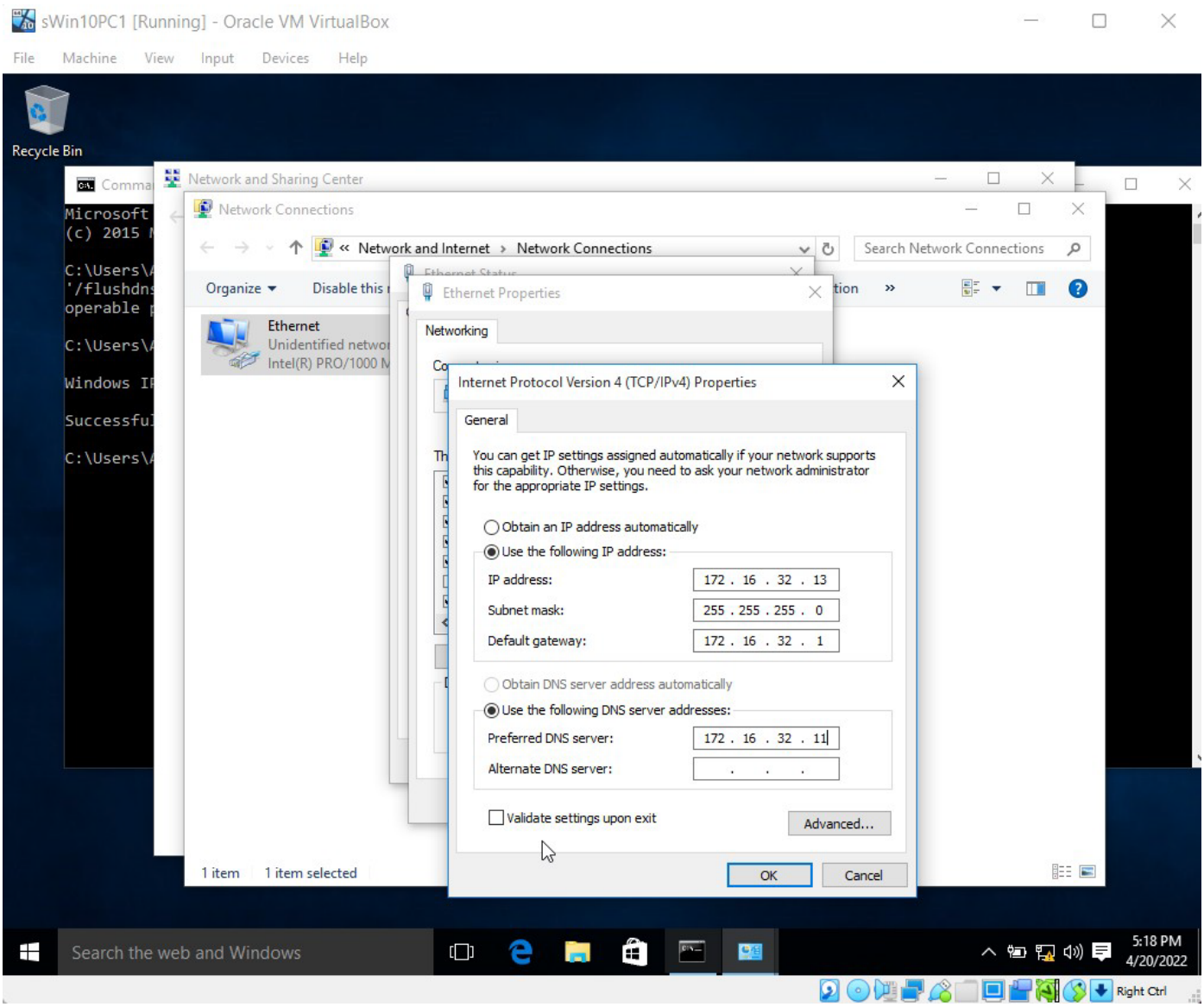
Steps #17 to #19 required us to run notepad as administrator in the sWin16SVR2 Virtual Machine, and type html code as in the above picture and then save it as index.html in C:\inetpub\wwwroot folder.

Creating DNS Records

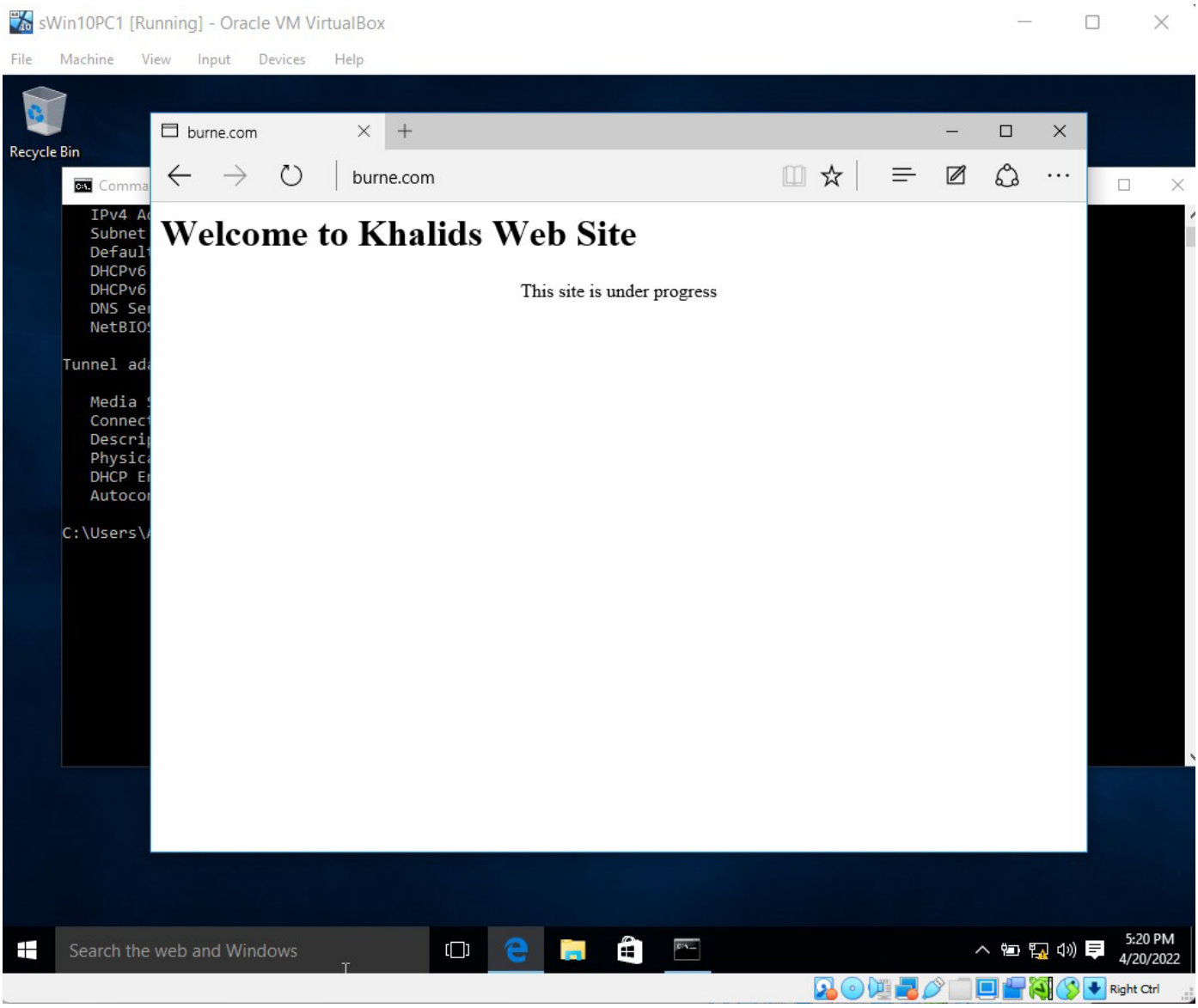


Steps #20 and #21 required us to create DNS Records in the sWin16SVR1 virtual machine. A new Host(A) was created with Host Name “www”, “www.burne.com” as FQDN and IP Address of sWIn16SVR2 Virtual Machine. a New Alias(CNAME) was created with “FileSvr” as Alias Name, “FileSvr.burne.com” and “www.burne.com” as FQDN for target host. A CNAME record points to an existing record and allows an alias name to be attached to it.

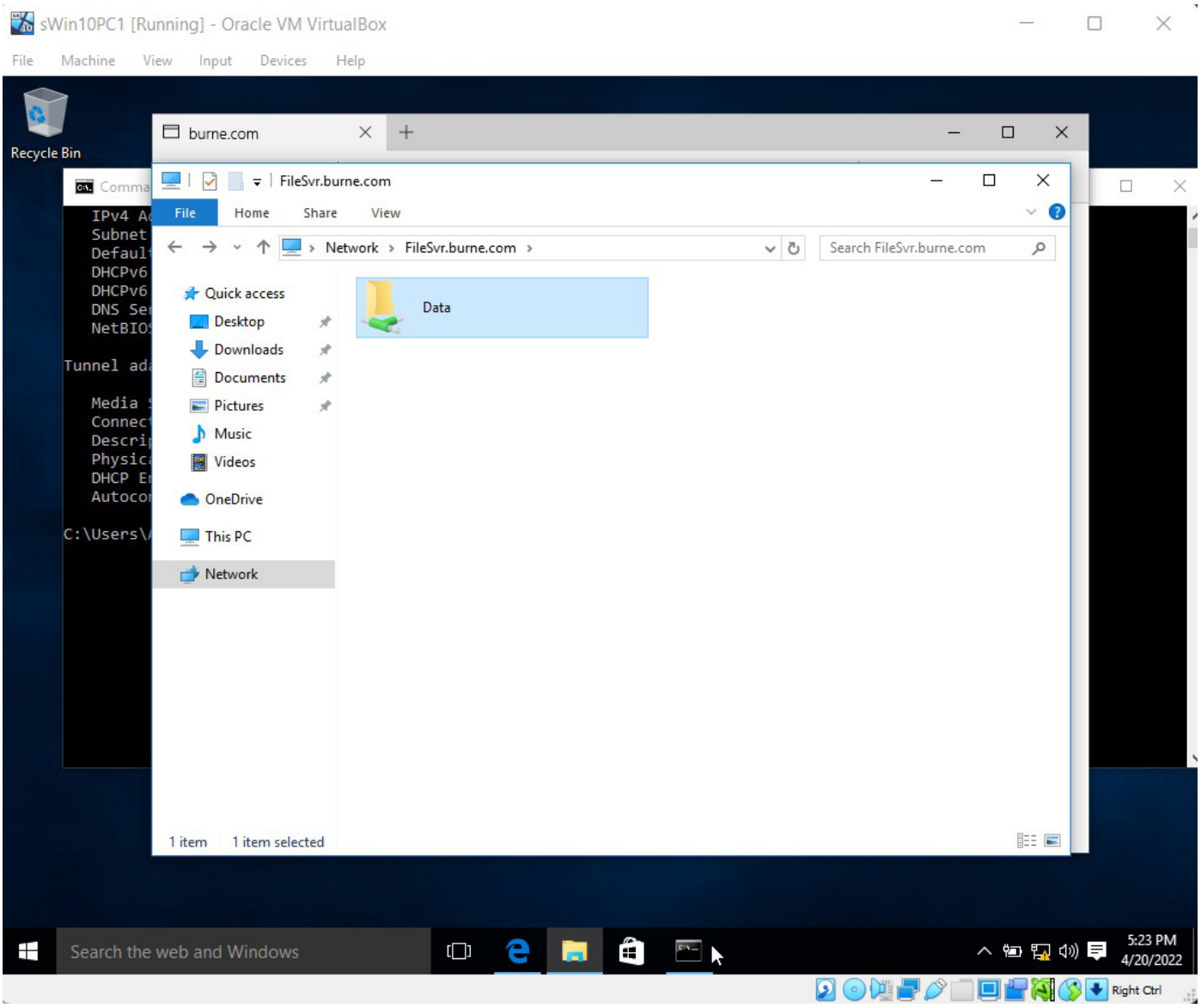
Testing DNS



Step #22 required us to add sWin16SVR1's IP Address as sWin10PC1's preferred DNS server Address so that sWin10PC1 can access "www.burne.com".

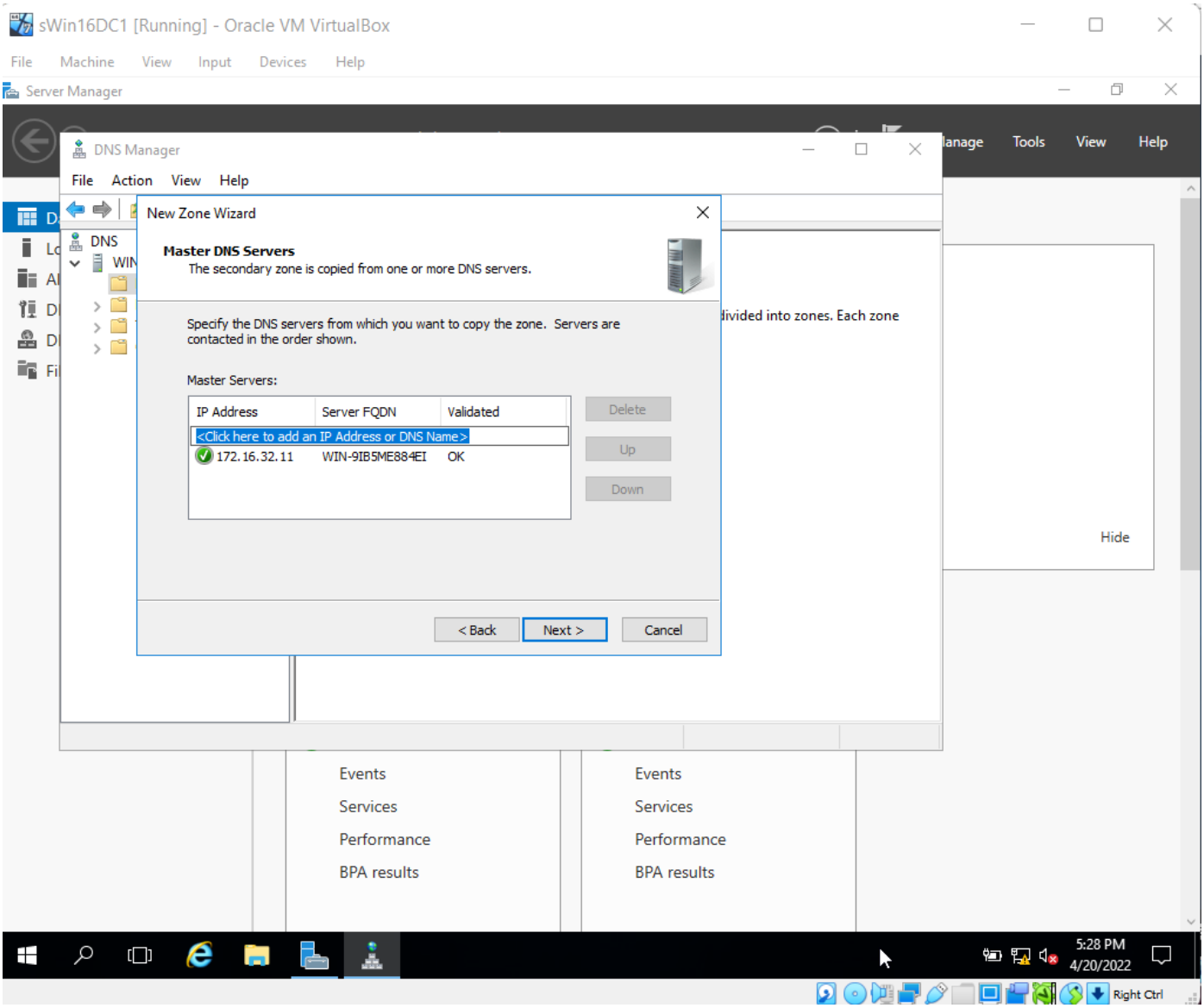


After Modifying sWin10PC1's preferred DNS server to sWin16SVR1's IP Address. We can successfully access "www.burne.com" from sWin10PC1.

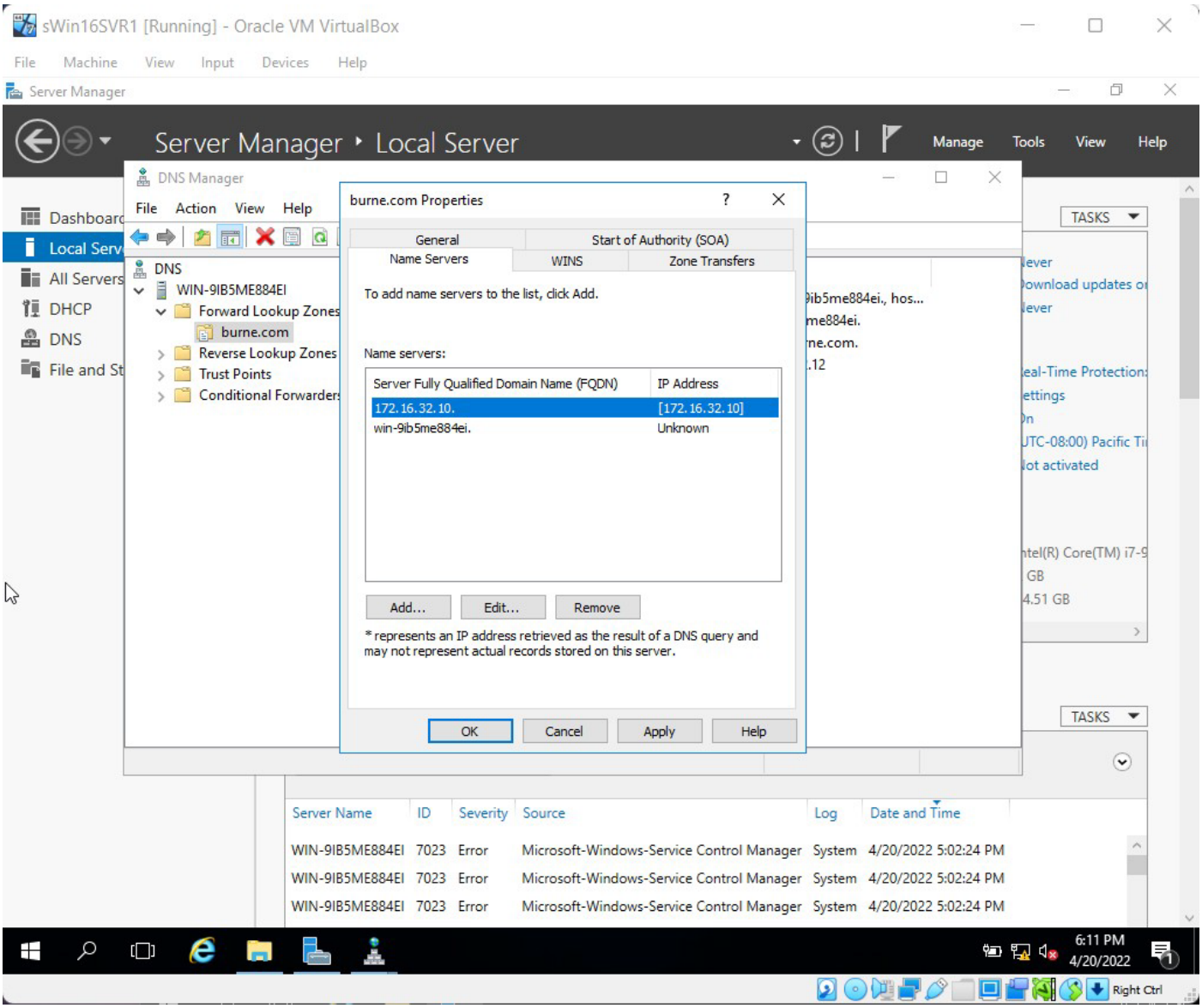


We can also access the Data folder by Opening File Explorer and typing \\FileSvr.burne.com, and then entering the Username and password when prompted.

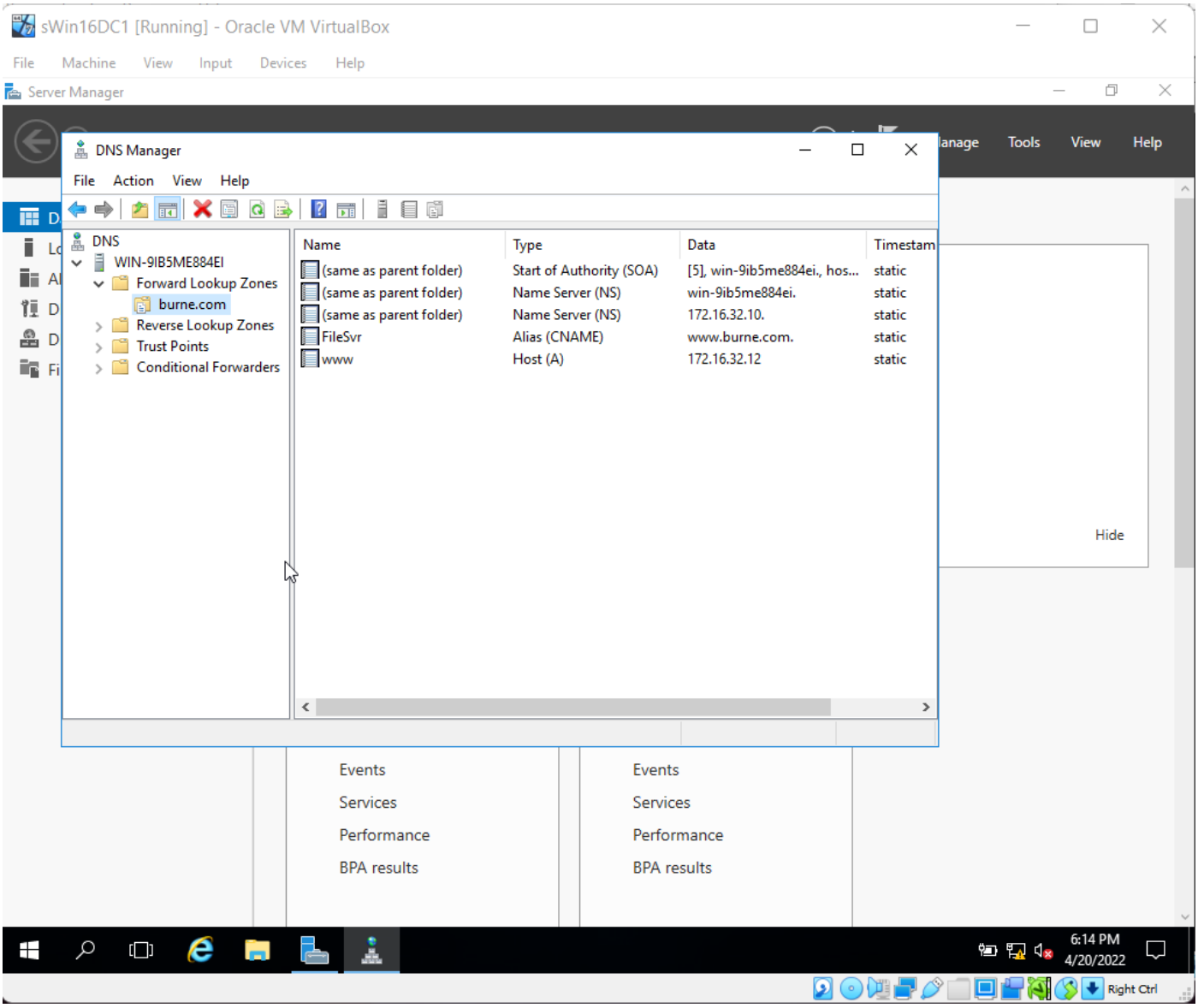
Zone Transfers



Steps #23 to #27 required us to Create a Second secondary zone called burne.com on sWin16DC1 through the Forward Lookup zone. As seen above, On the Master DNS server dialog, enter sWin16SVR1's IP address.



Steps #28 and #29 required us to add sWin16DC1's IP Address in the Name server's column, so that it is among the zone transfer approved list.

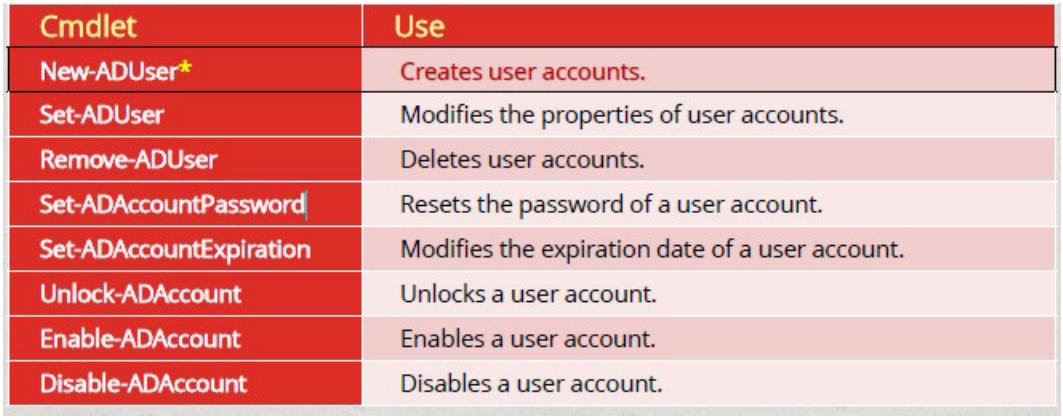


Step #30 required us to check if the data appears after the zone transfer, and it successfully does.

TNE10005 Journal Lab (#6)

Khalid Yaseen Baig / ID #102763240

What I learned in this week's Lecture.

- 

Cmdlet	Use
New-ADUser*	Creates user accounts.
Set-ADUser	Modifies the properties of user accounts.
Remove-ADUser	Deletes user accounts.
Set-ADAccountPassword	Resets the password of a user account.
Set-ADAccountExpiration	Modifies the expiration date of a user account.
Unlock-ADAccount	Unlocks a user account.
Enable-ADAccount	Enables a user account.
Disable-ADAccount	Disables a user account.

- CSVDE-Can import/export new user account details from a Comma Separated Values Encoding (CSVDE) file (i.e. spreadsheet text).

- LDIFDE-Can import/export new user account information from an LDAP database.

- OUs provide a logical framework for identifying things, as well as the ability to delegate administration privileges to users and target configurations using Group Policy.

- The hierarchy of OUs is usually determined by the following factors: location, business unit, and resources.

- AD containers by default GPOs cannot be connected to Users or Computers since they are not OUs. Using redircmpand redirusr, it is recommended to alter the default locations.

- NTFS permissions, which are frequently referred to as NTFS permissions, always apply whether the user is local (i.e. interactive), network, or distant, and are attached to the object (i.e. File or Folder) rather than the User

account.

- Permission provided to an object are Explicit, permissions assigned to a parent object are Inherited, and Explicit permissions override Inherited permissions, according to Permission Inheritance.

- For Security Permissions connected to an object, Explicit Deny overrides Explicit Allow, Explicit Allow overrides Inherited Deny, and Inherited Deny overrides Inherited Allow, according to Permission Precedence. The Effective Access tab in Advanced Security can confirm a user's or group's effective access.

- Account Groups are used to group accounts with similar criteria. Global groups almost usually serve this purpose, and the group's name represents the accounts.

- Resource Groups (ACL) are used to regulate access to resources; Domain Local Groups almost invariably serve this purpose. The name of the resource(s) and the permissions being granted is reflected in the name.

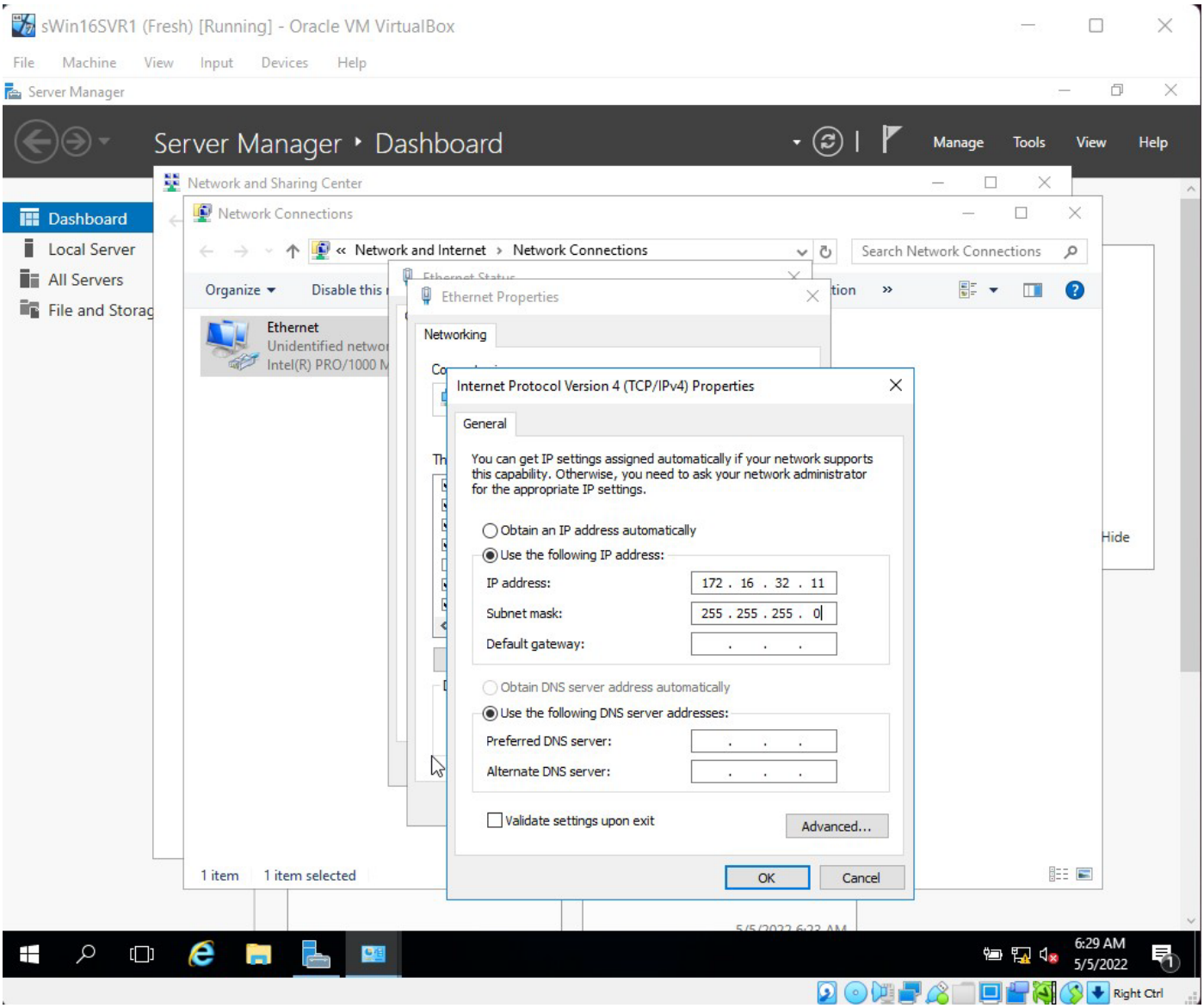
-

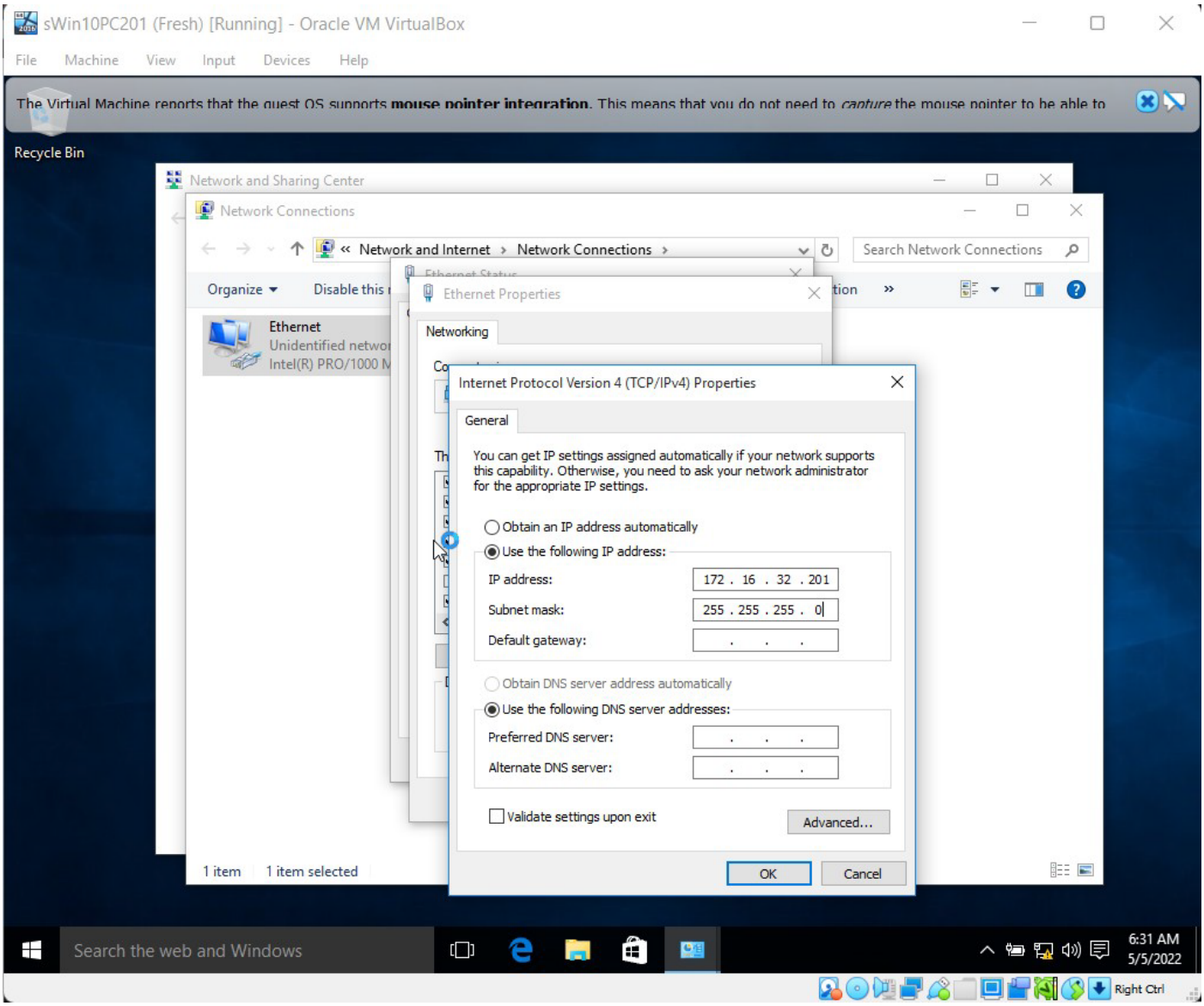
Scope	Purpose	Membership i.e. who can be a member of this group		Resources i.e. where are the resources that this group can have permissions to?		Limitations
		From the same domain	From another domain	In the same domain	In another domain	
G Global	**Role** *To group Identities (i.e. user and computer accounts) that have similar requirements*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ ~~Universal Groups~~	**No**	**Yes**	**Yes**	Cannot have members from another domain
DL Domain Local	**Resource** *To control Access to resources (e.g. files, folders & printers)*	User Accounts Computer Accounts Global Groups Domain Local Grps Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups* *Only from the same forest	**Yes**	**No**	Cannot give access to resources in another domain
U Universal	*To collect groups from multiple domains in the forest.*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	**Yes**	**Yes**	Do not belong to any one domain, but to the whole forest. Hence has an overhead that can slow all DCs in the forest down

- A Global group should be used if the 2nd account group is gathering groups from inside a single domain. It should be a Universal group if the 2nd account group contains groups from several domains.

This week’s lab activities.

Preliminary settings

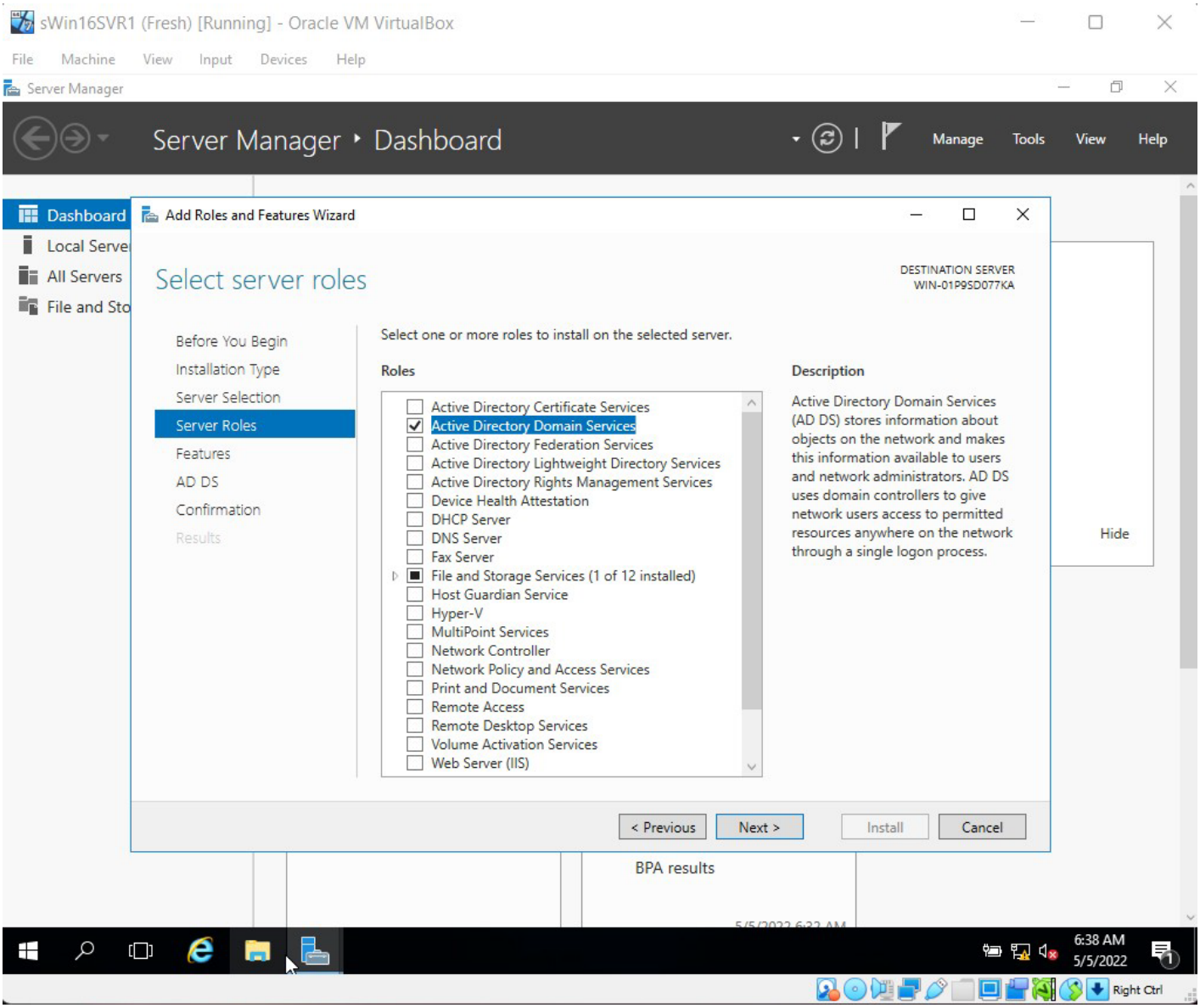




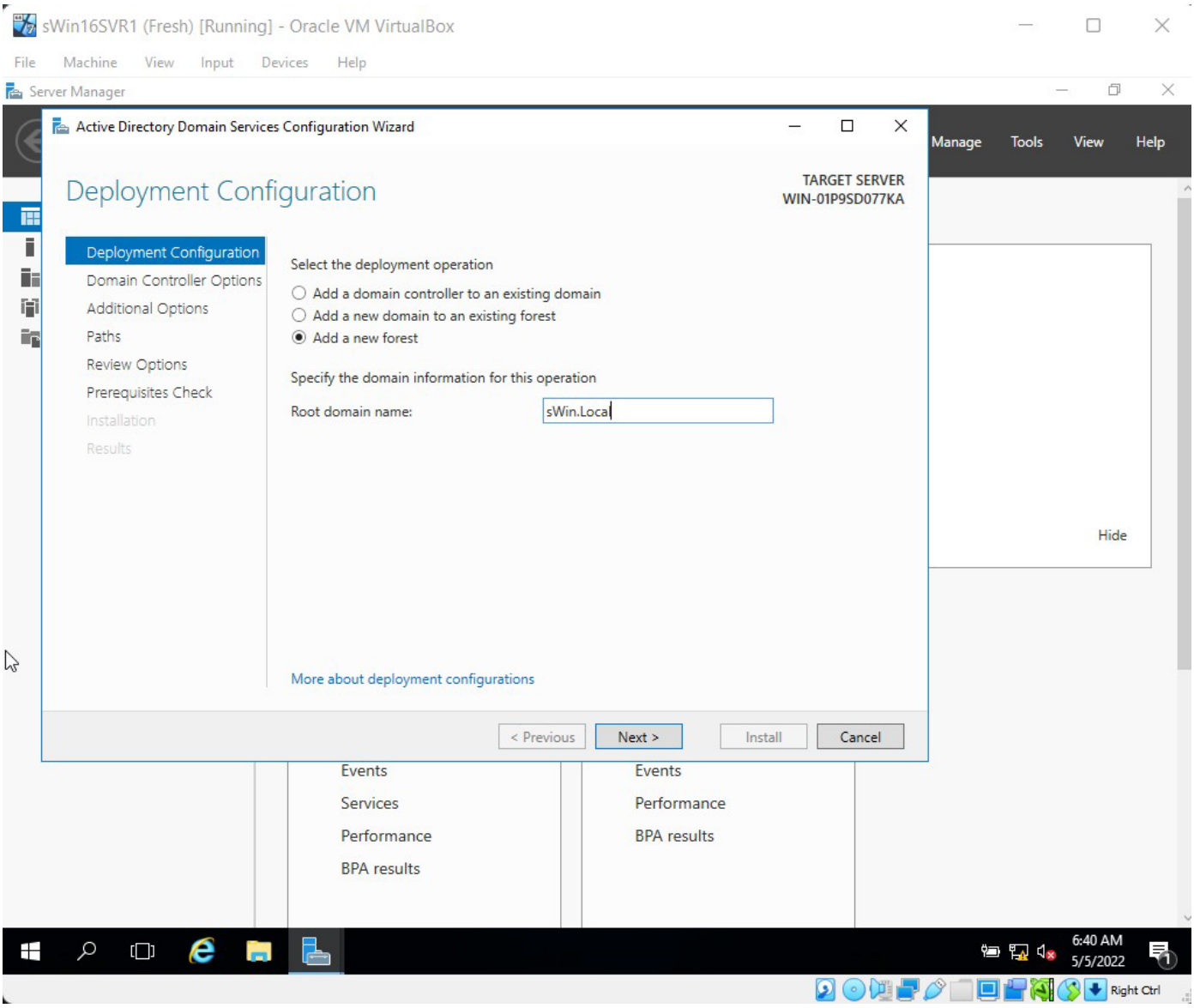
Ensure that both virtual machines have IP addresses in the subnet 172.16.32.0/24.

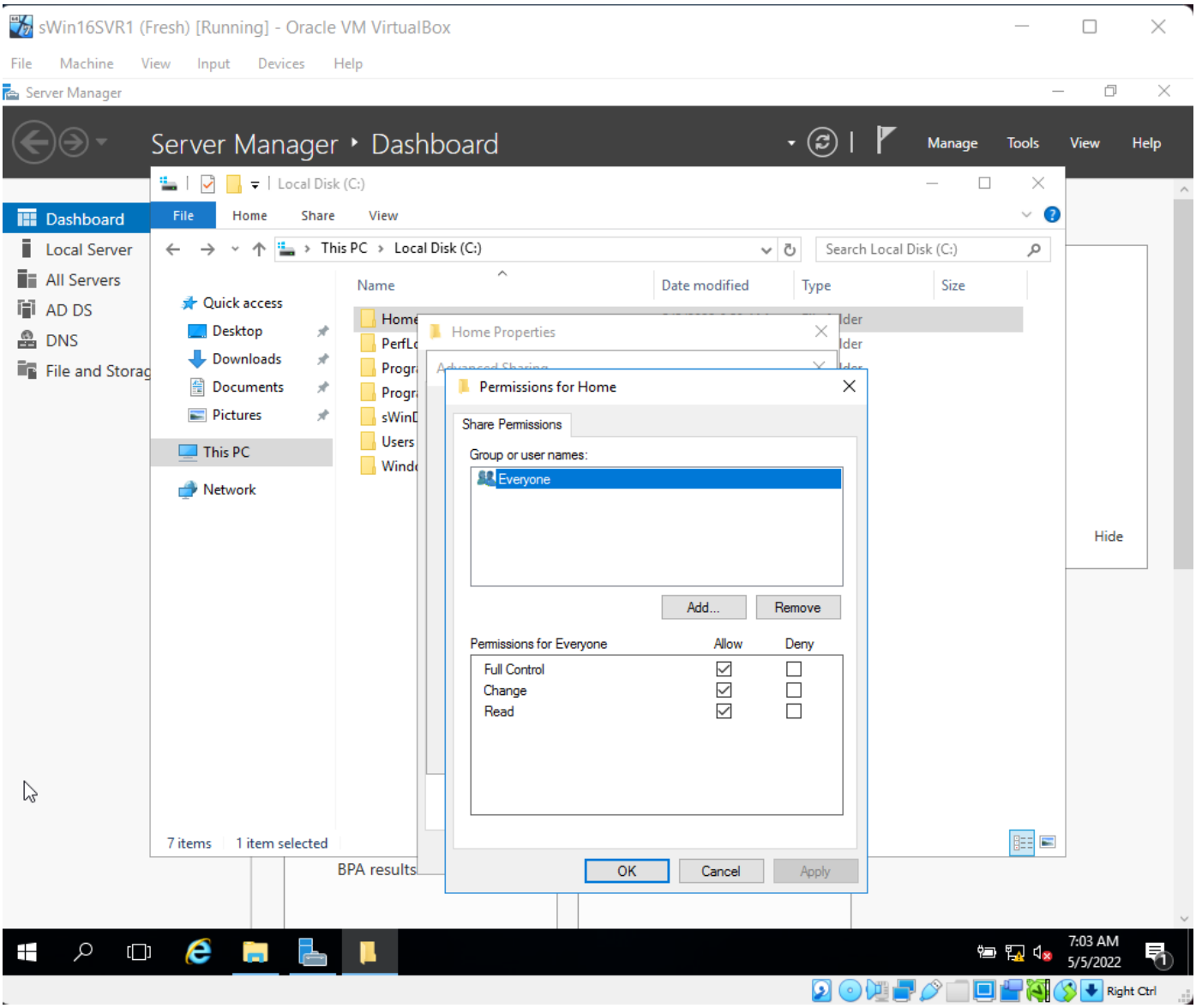
Creating a Domain

Configuring a Domain Controller



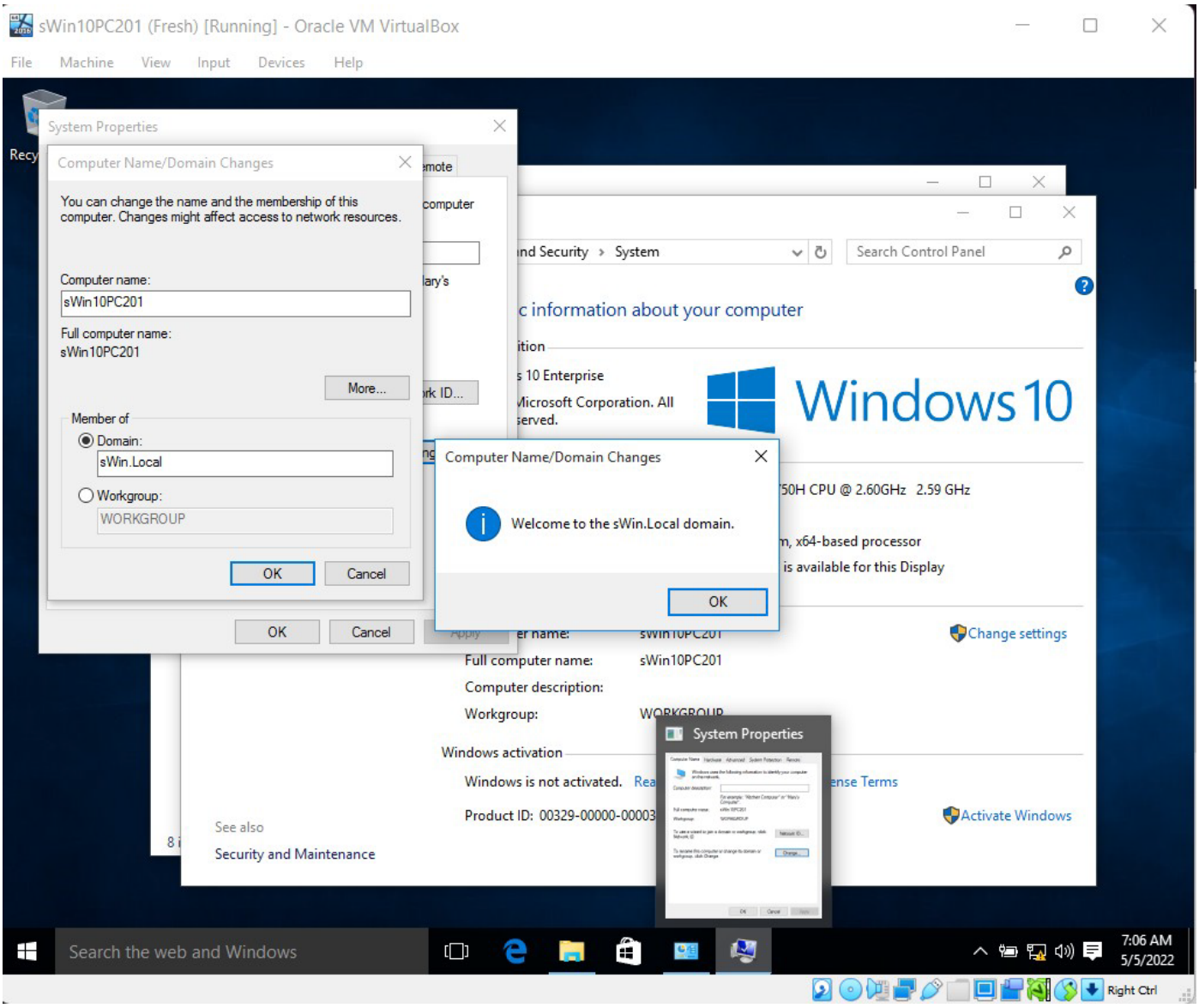
Steps 4 to 10 required to install Active /directory domain SERVICES.


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Manage Tools View Help
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-01P9SD077KA
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
sWin.Local
More about deployment configurations
< Previous
Next >
Install
Cancel
Hide
Events
Services
Performance
BPA results
Events
Performance
BPA results
6:40 AM
5/5/2022
Right Ctrl



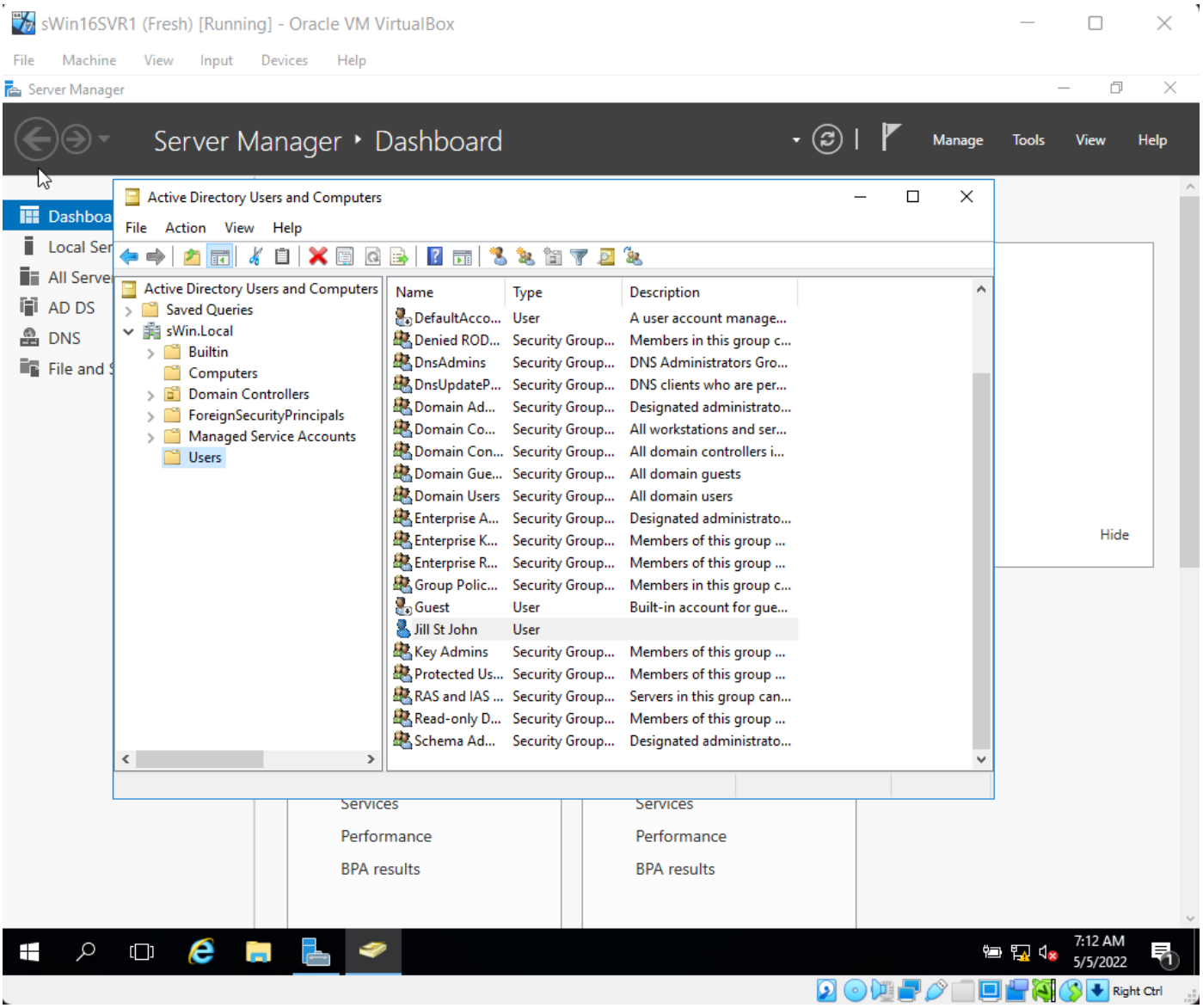
To give the Everyone group full control to the Home folder

Joining a Domain



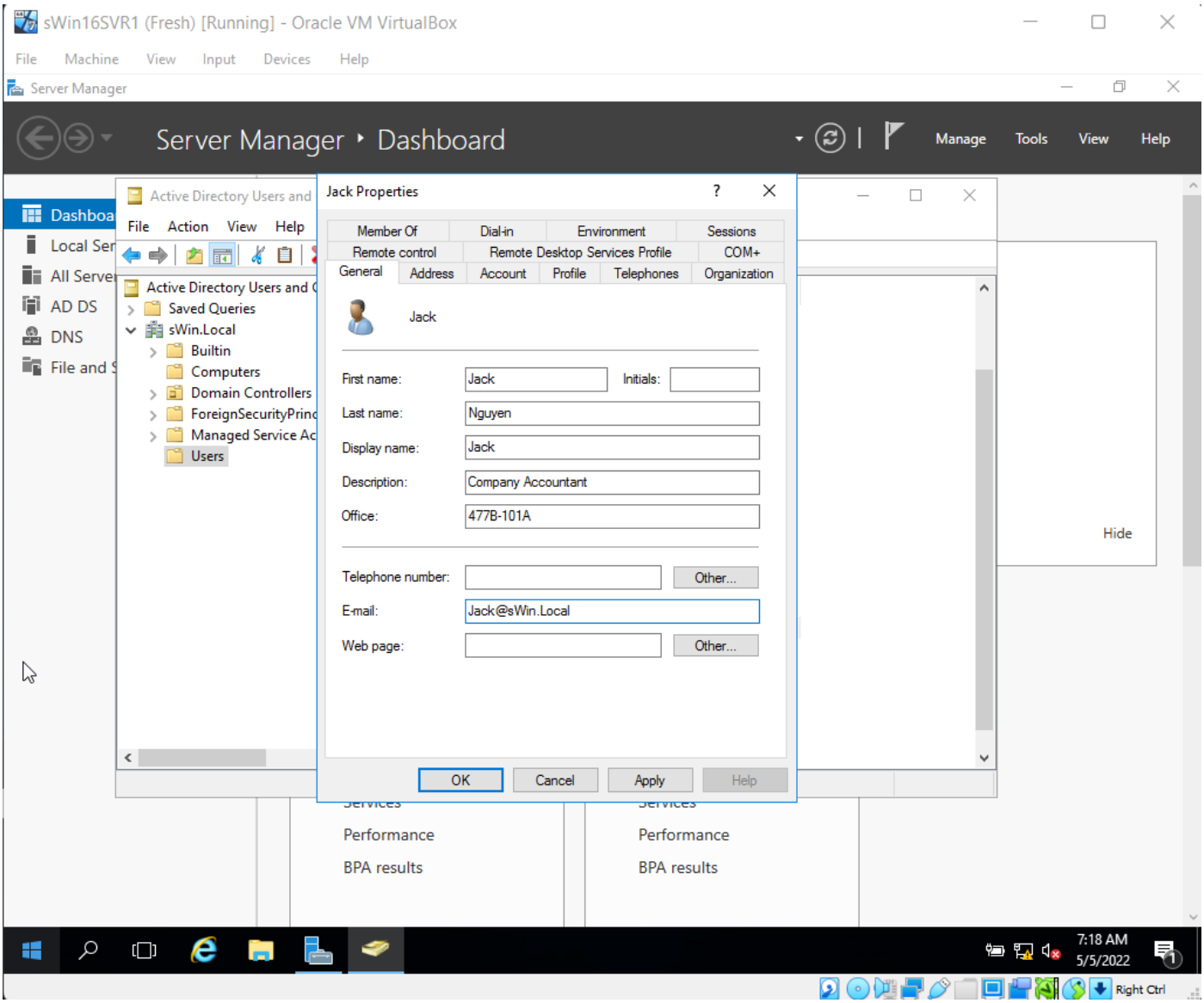
Creating Accounts

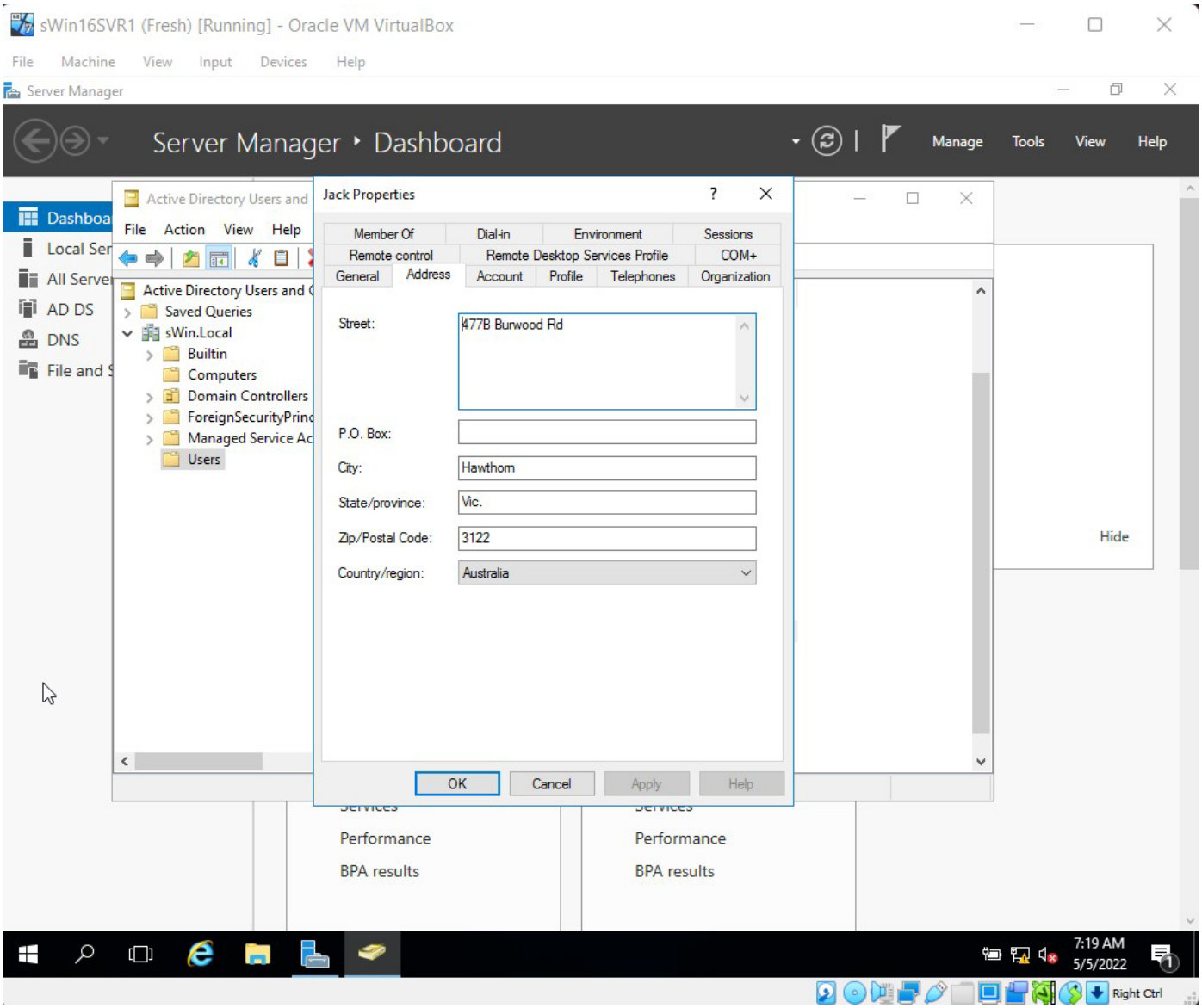
Logging on With an Existing User Account

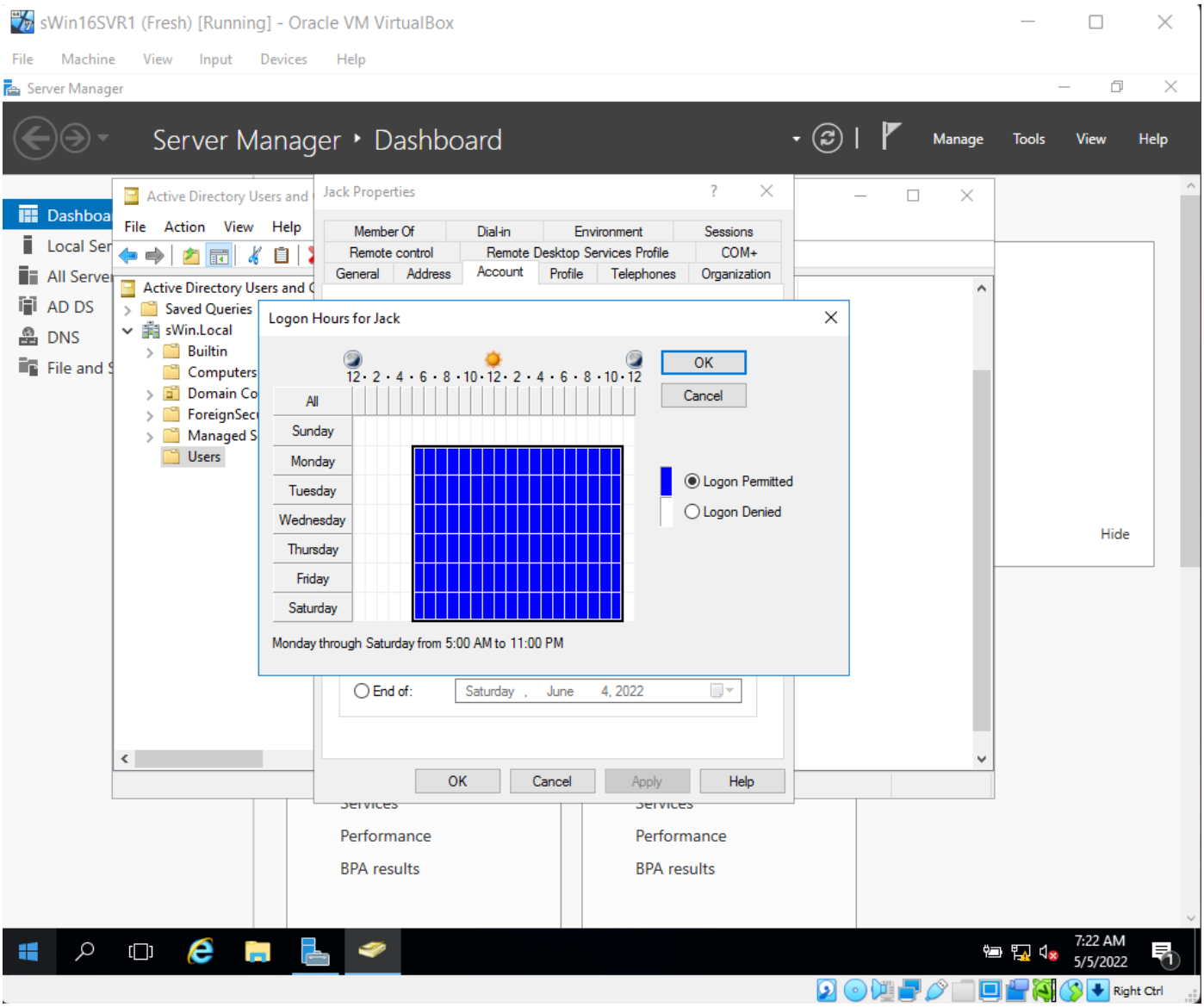


Configuring Account Properties

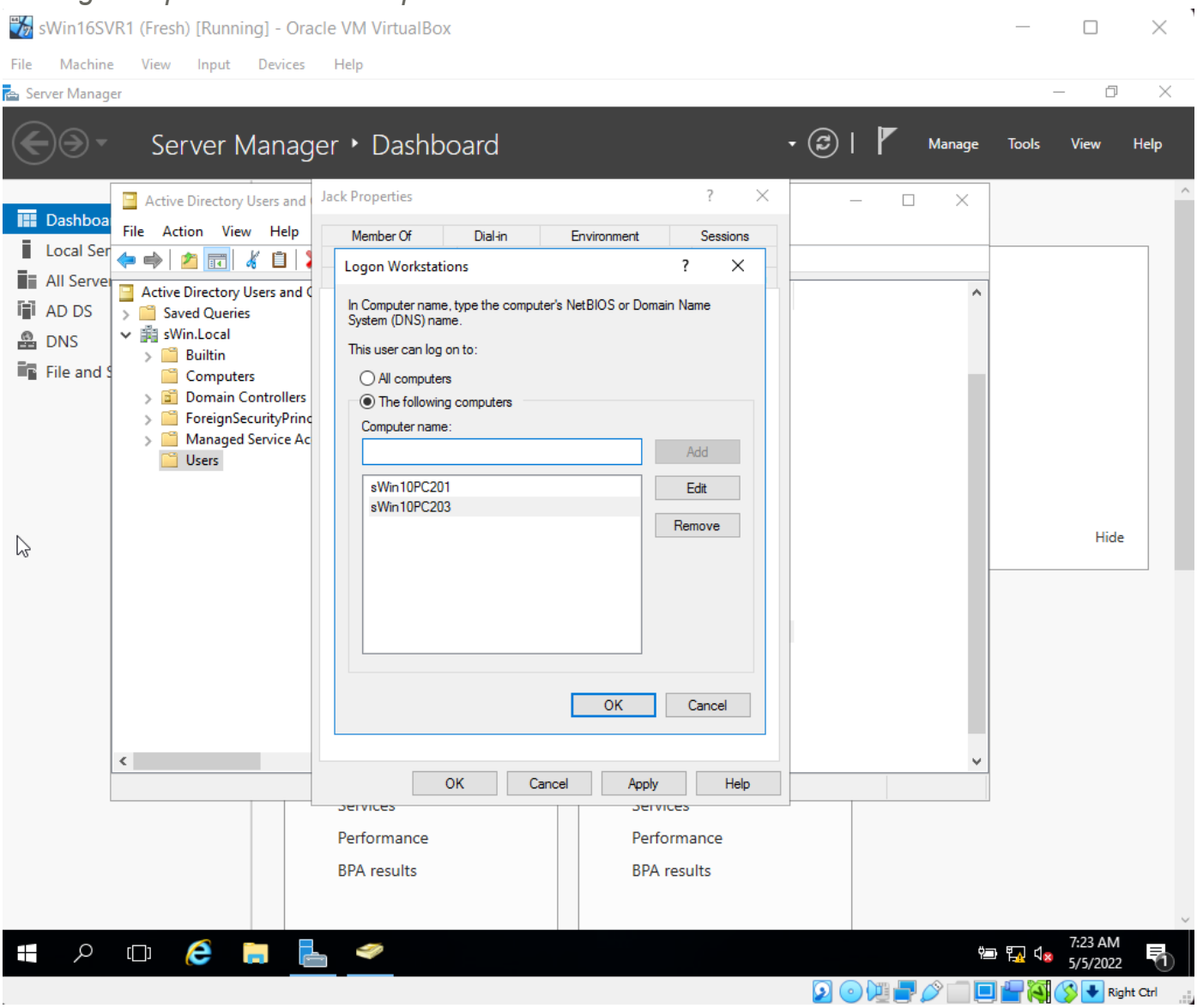
Setting User Account Properties



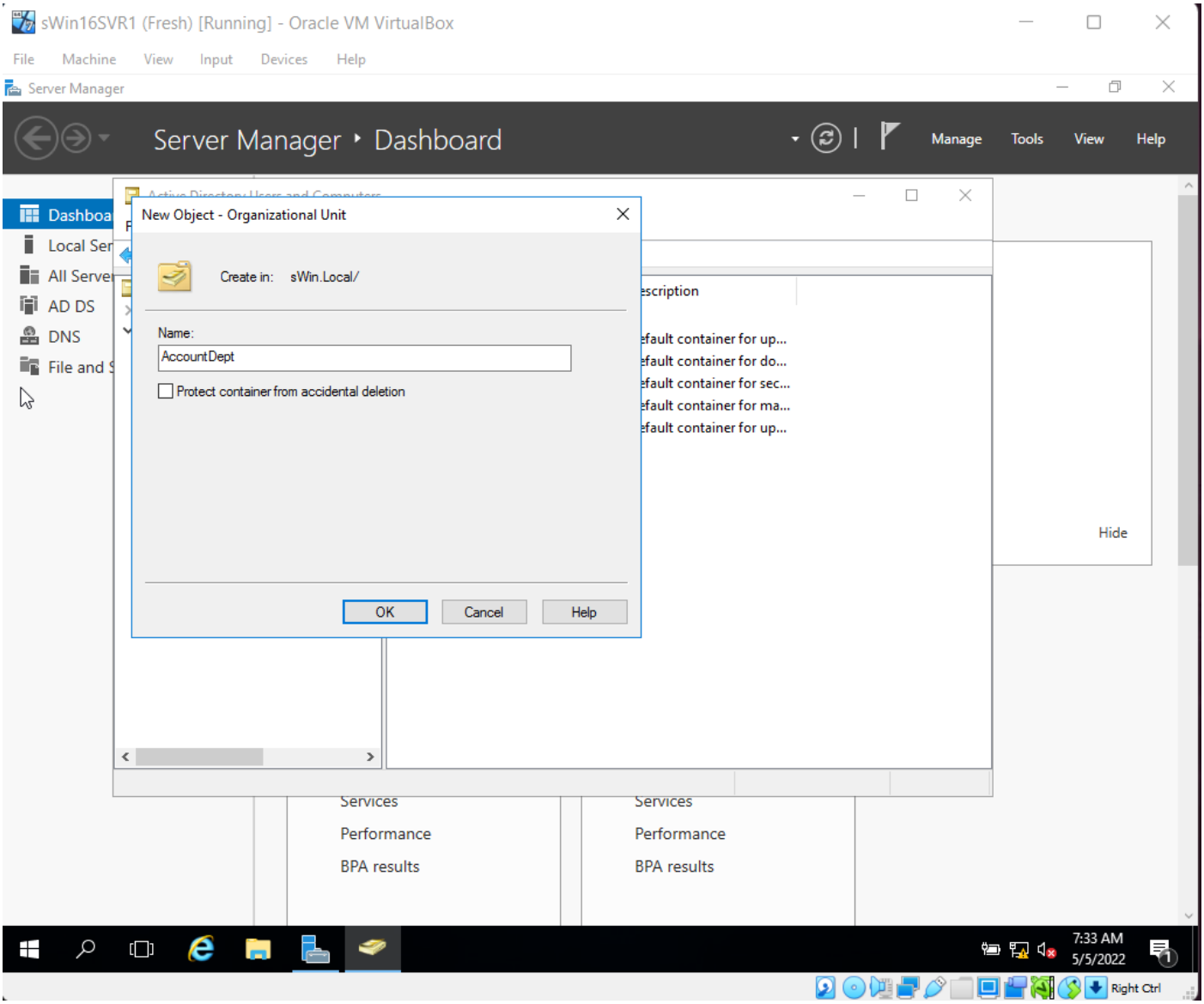

sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and
File Action View Help
Active Directory Users and
Saved Queries
sWin.Local
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Ac
Users
Jack Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Street:
477B Burwood Rd
P.O. Box:
City:
Hawthorn
State/province:
Vic.
Zip/Postal Code:
3122
Country/region:
Australia
OK
Cancel
Apply
Help
Hide
Performance
BPA results
Performance
BPA results
7:19 AM
5/5/2022
Right Ctrl


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and
File Action View Help
Jack Properties
Member Of Dial-in Environment Sessions
Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization
Logon Hours for Jack
12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Logon Permitted
Logon Denied
Monday through Saturday from 5:00 AM to 11:00 PM
End of: Saturday , June 4, 2022
OK Cancel Apply Help
Saved Queries
sWin.Local
Builtin
Computers
Domain Co
ForeignSec
Managed S
Users
Hide
Performance
BPA results
Performance
BPA results
7:22 AM
5/5/2022
Right Ctrl

Setting Computer Account Properties

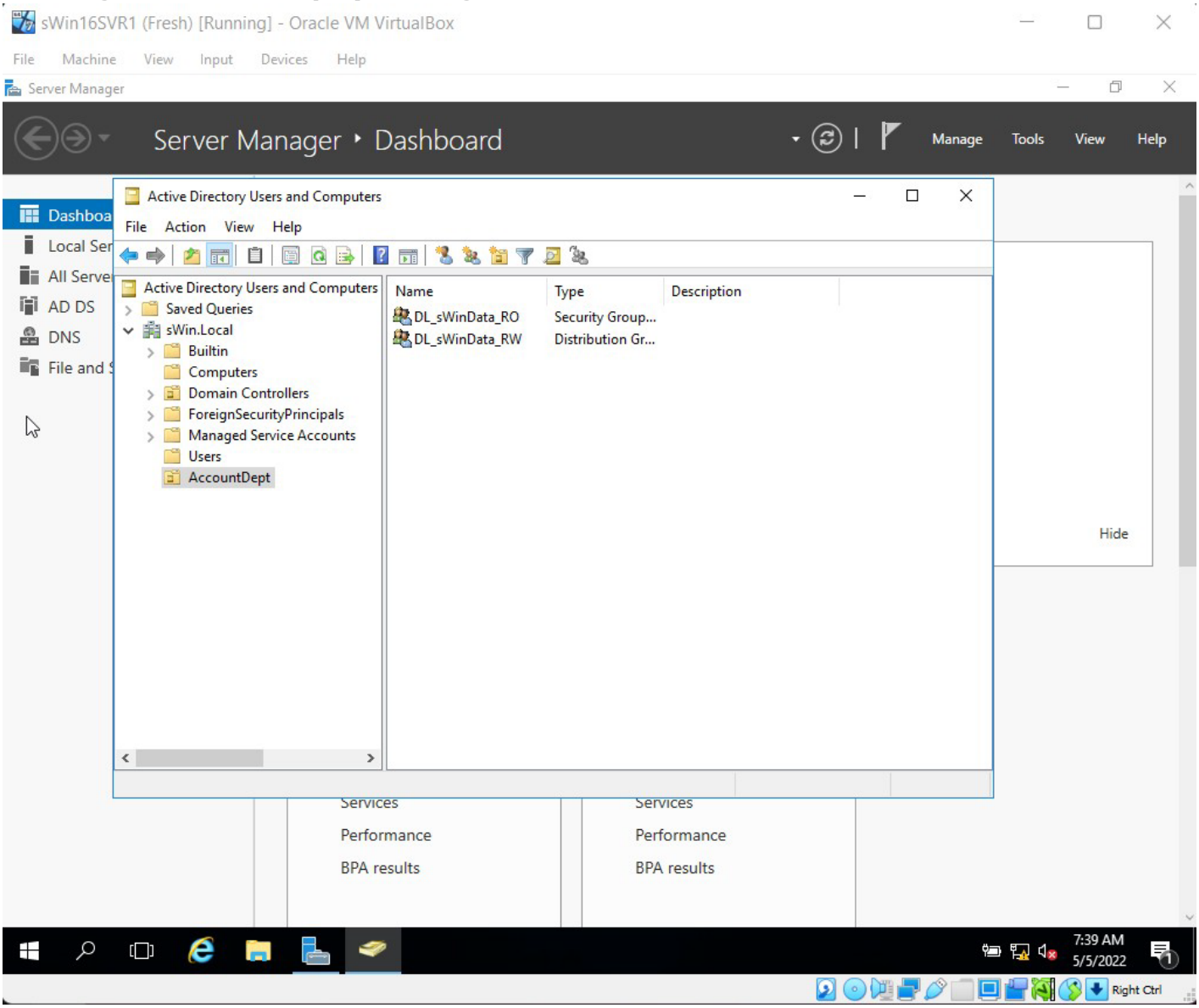


Creating an Organisational Unit

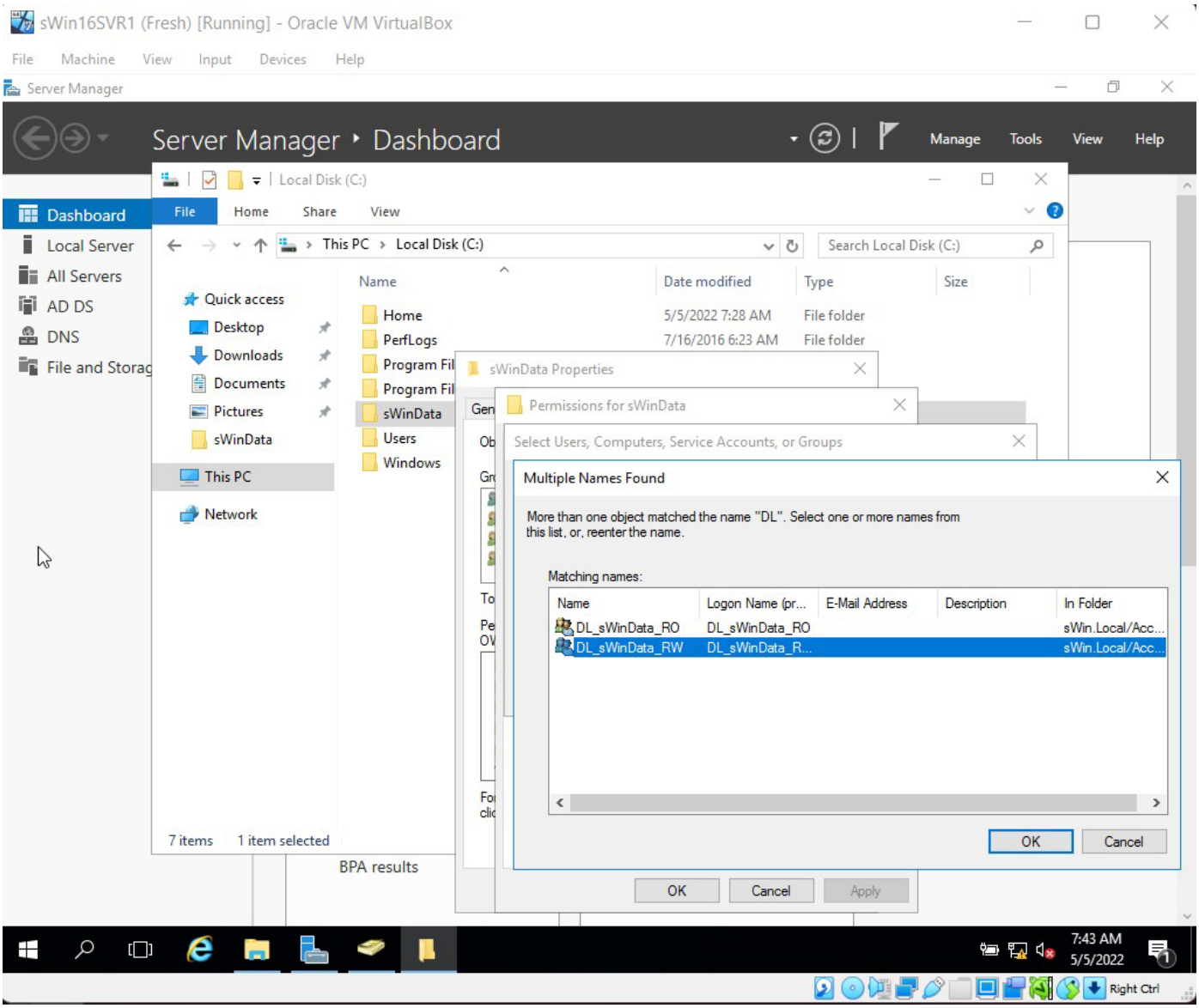


Creating Group Accounts

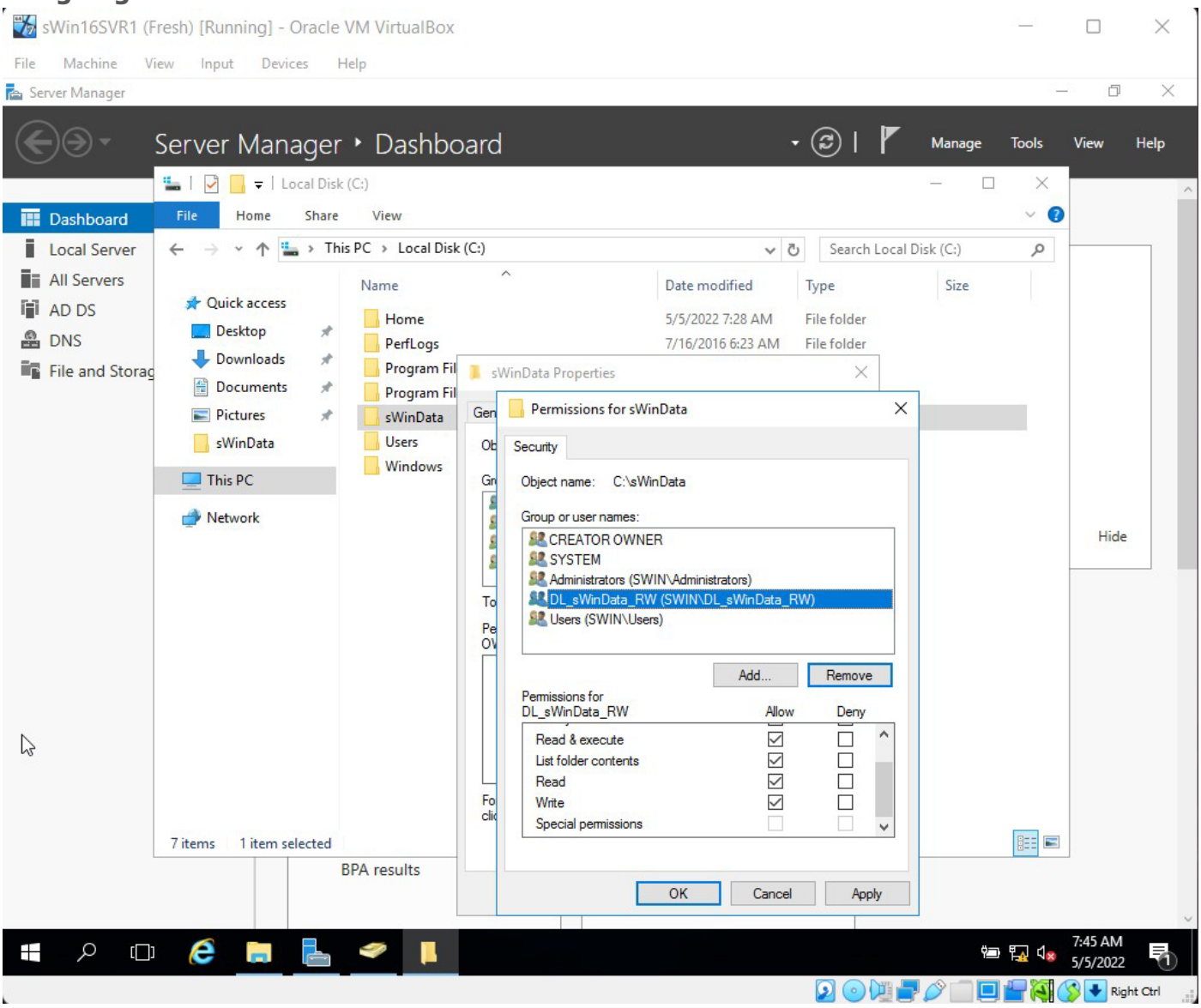
Creating Resource Groups (For assign



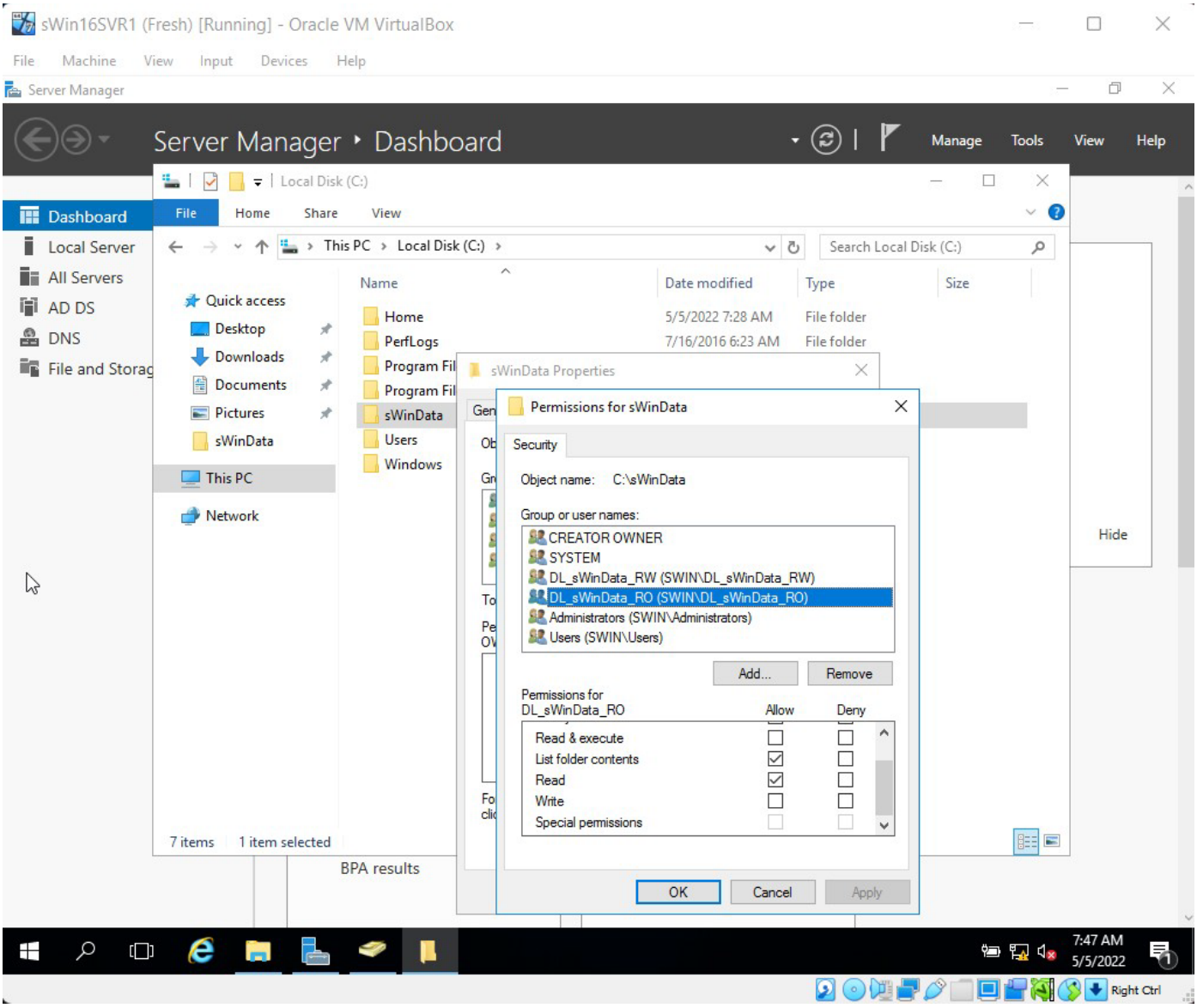
ing permission)


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
Local Disk (C:)
File Home Share View
This PC › Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
sWinData
This PC
Network
Name
Date modified
Type
Size
Home 5/5/2022 7:28 AM File folder
PerfLogs 7/16/2016 6:23 AM File folder
Program Fil
Program Fil
sWinData
Users
Windows
7 items 1 item selected
BPA results
sWinData Properties
Permissions for sWinData
Select Users, Computers, Service Accounts, or Groups
Multiple Names Found
More than one object matched the name "DL". Select one or more names from this list, or, reenter the name.
Matching names:
Name Logon Name (pr... E-Mail Address Description In Folder
DL_sWinData_RO DL_sWinData_RO sWin.Local/Acc...
DL_sWinData_RW DL_sWinData_R... sWin.Local/Acc...
OK Cancel
OK Cancel Apply
7:43 AM
5/5/2022
Right Ctrl

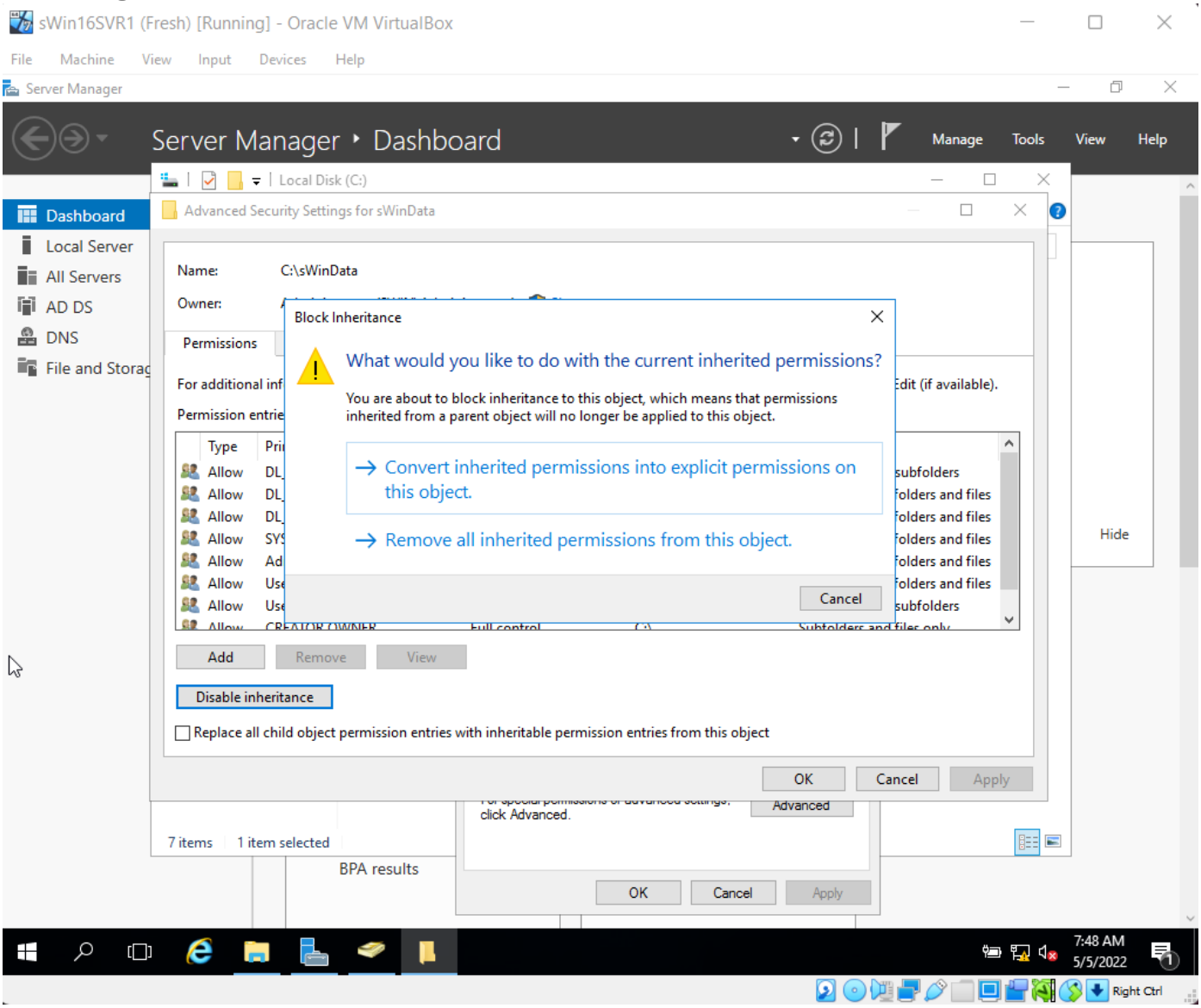
Assigning NTFS Permissions

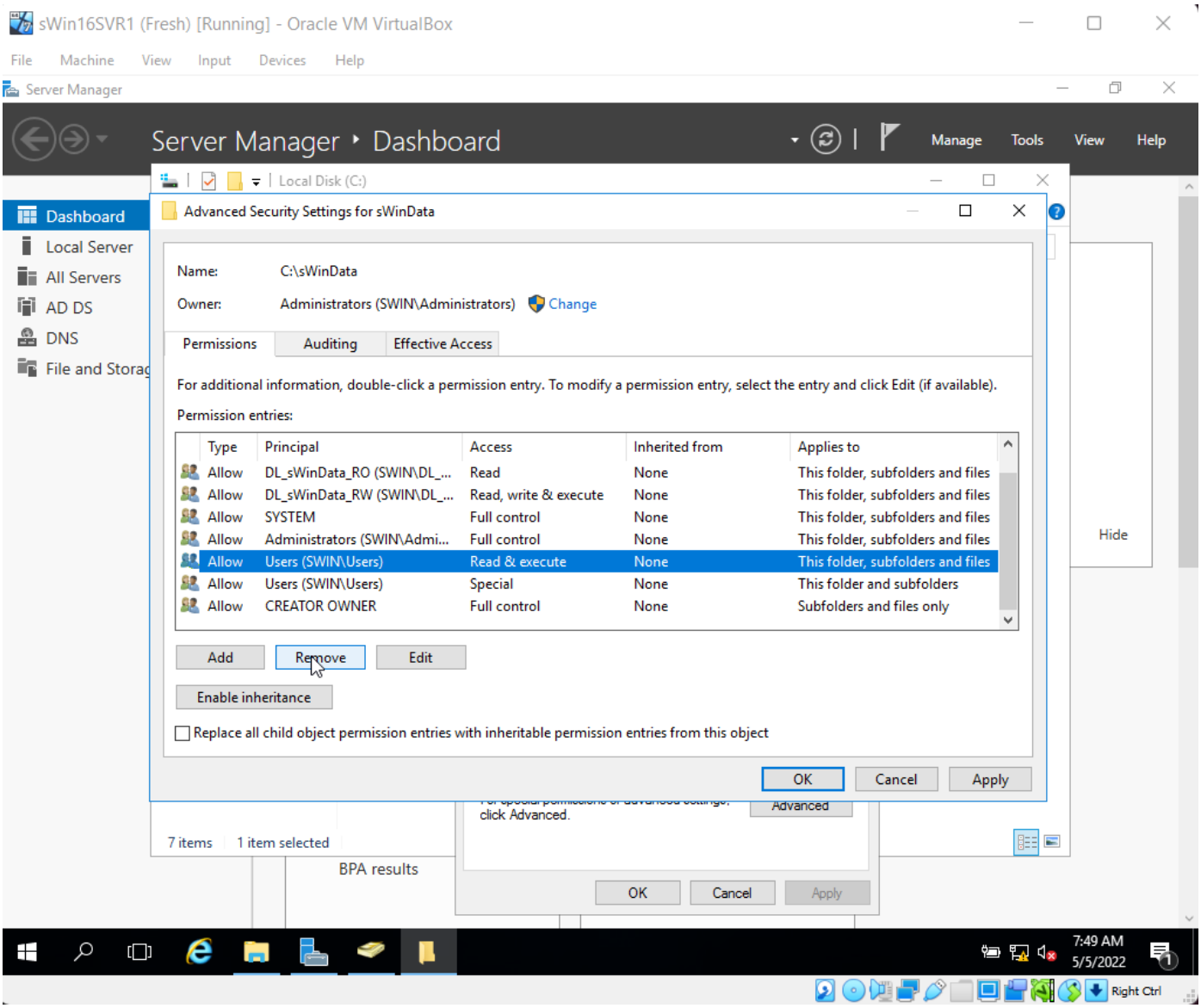


ns

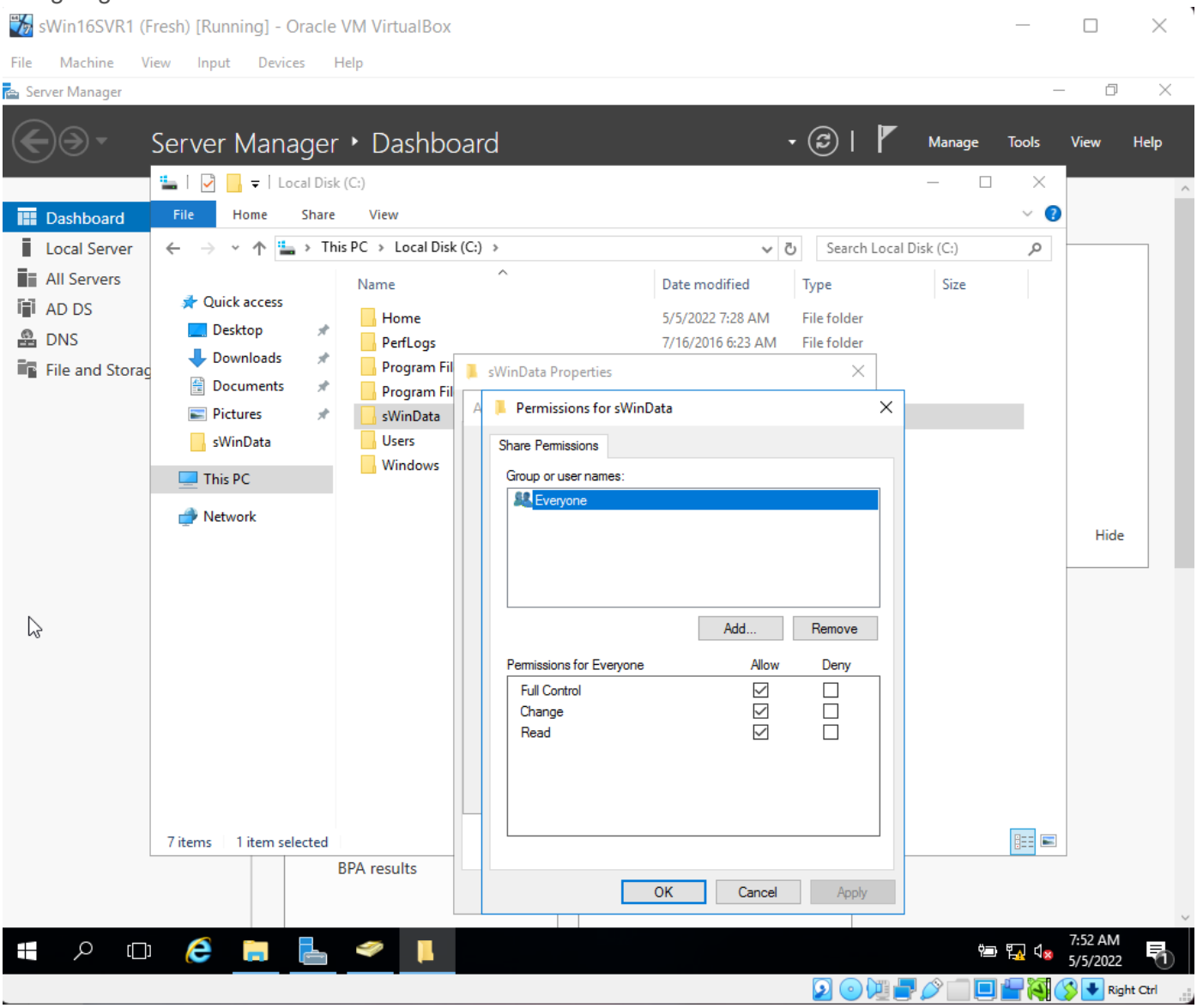

sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
Local Disk (C:)
File Home Share View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
sWinData
This PC
Network
Name
Date modified
Type
Size
Home 5/5/2022 7:28 AM File folder
PerfLogs 7/16/2016 6:23 AM File folder
Program Fil
Program Fil
sWinData
Users
Windows
7 items 1 item selected
BPA results
Hide
sWinData Properties
Permissions for sWinData
Security
Object name: C:\sWinData
Group or user names:
CREATOR OWNER
SYSTEM
DL_sWinData_RW (SWIN\DL_sWinData_RW)
DL_sWinData_RO (SWIN\DL_sWinData_RO)
Administrators (SWIN\Administrators)
Users (SWIN\Users)
Add... Remove
Permissions for DL_sWinData_RO
Allow Deny
Read & execute
List folder contents
Read
Write
Special permissions
OK Cancel Apply
7:47 AM
5/5/2022
Right Ctrl

Removing Inherited Permissions

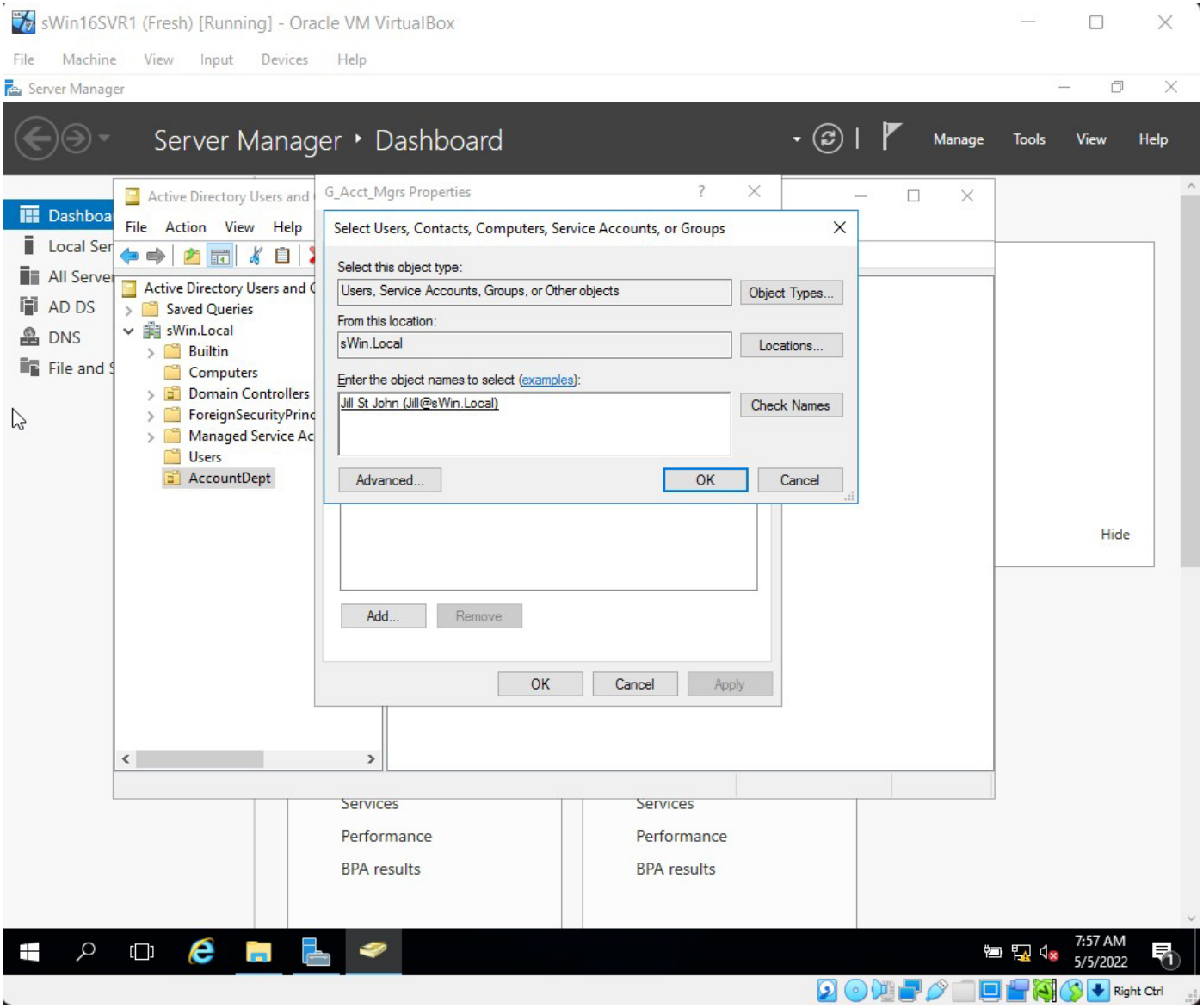


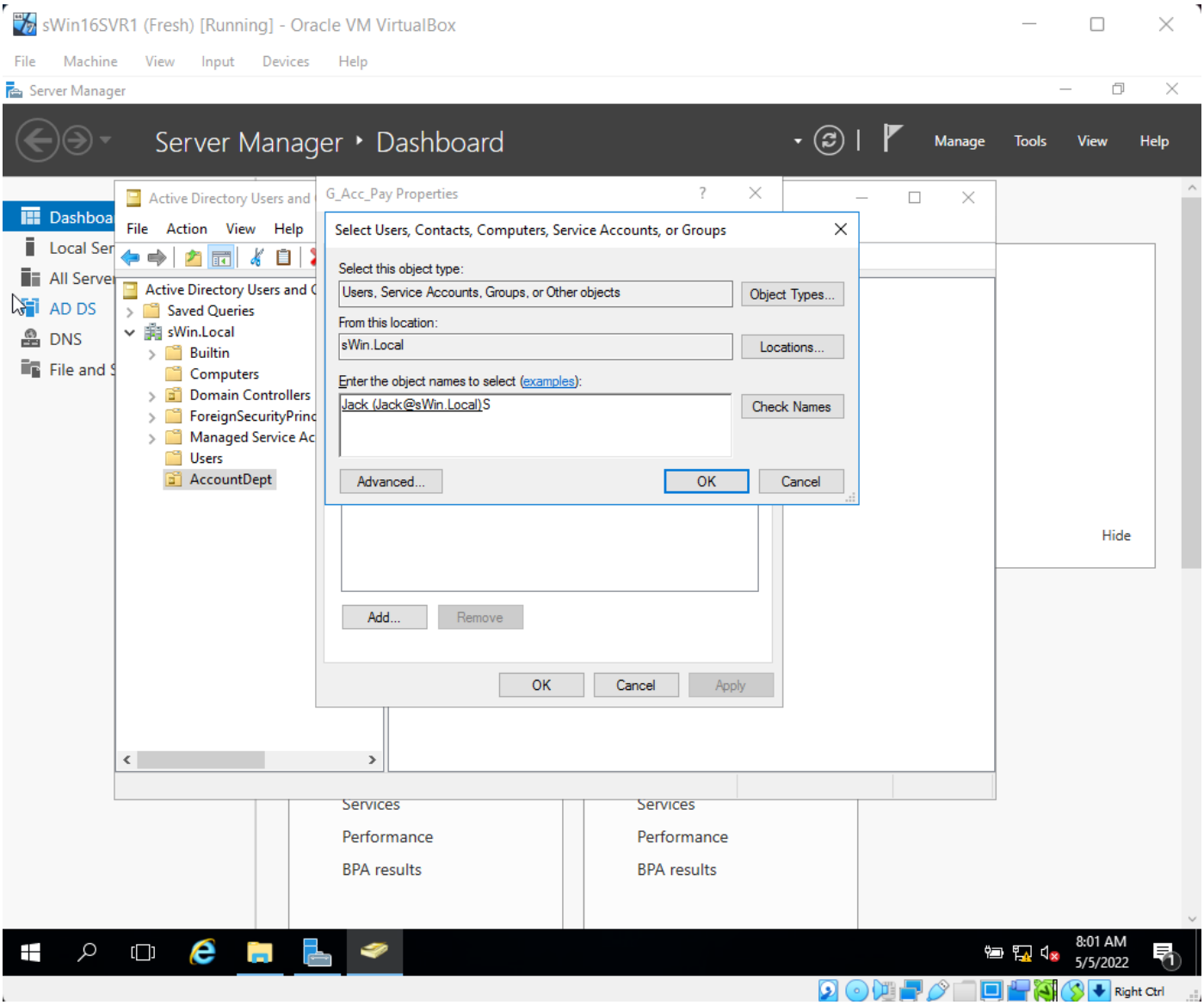

sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
Local Disk (C:)
Advanced Security Settings for sWinData
Name: C:\sWinData
Owner: Administrators (SWIN\Administrators) Change
Permissions Auditing Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type Principal Access Inherited from Applies to
Allow DL_sWinData_RO (SWIN\DL_... Read None This folder, subfolders and files
Allow DL_sWinData_RW (SWIN\DL_... Read, write & execute None This folder, subfolders and files
Allow SYSTEM Full control None This folder, subfolders and files
Allow Administrators (SWIN\Admi... Full control None This folder, subfolders and files
Allow Users (SWIN\Users) Read & execute None This folder, subfolders and files
Allow Users (SWIN\Users) Special None This folder and subfolders
Allow CREATOR OWNER Full control None Subfolders and files only
Add Remove Edit
Enable inheritance
Replace all child object permission entries with inheritable permission entries from this object
OK Cancel Apply
Advanced
click Advanced.
OK Cancel Apply
Hide
7 items 1 item selected
BPA results
7:49 AM
5/5/2022
Right Ctrl

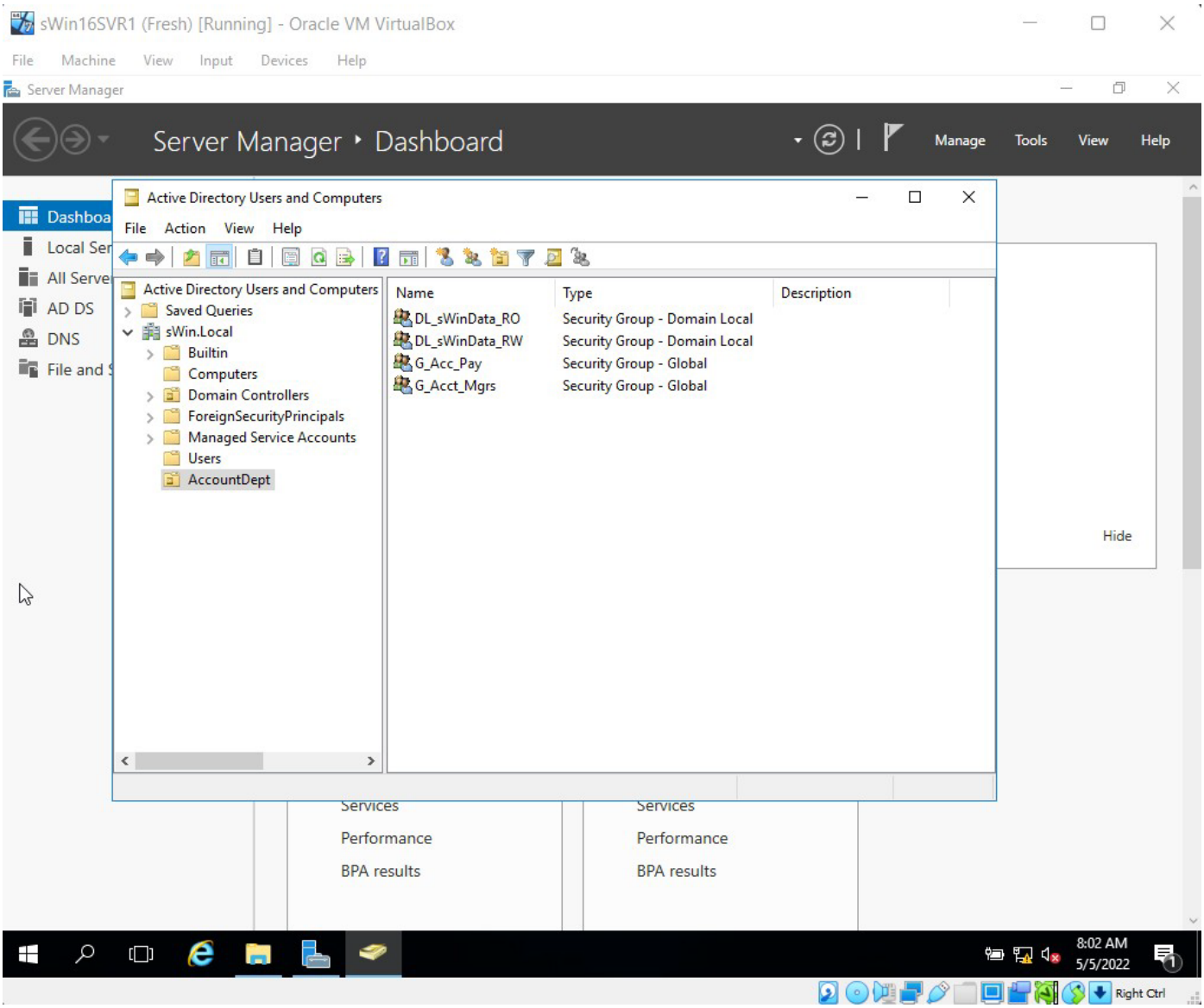
Assigning Share Permissions

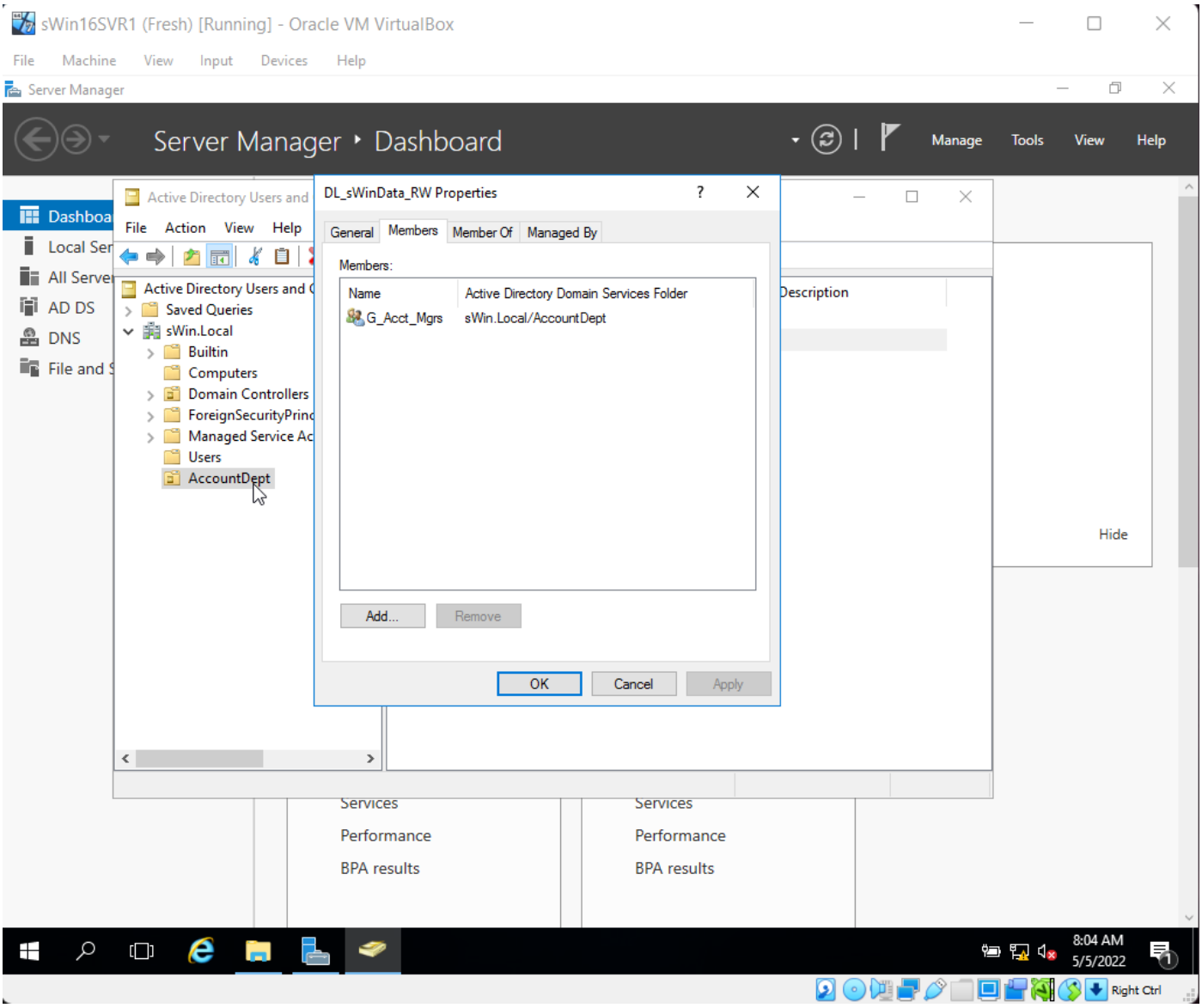


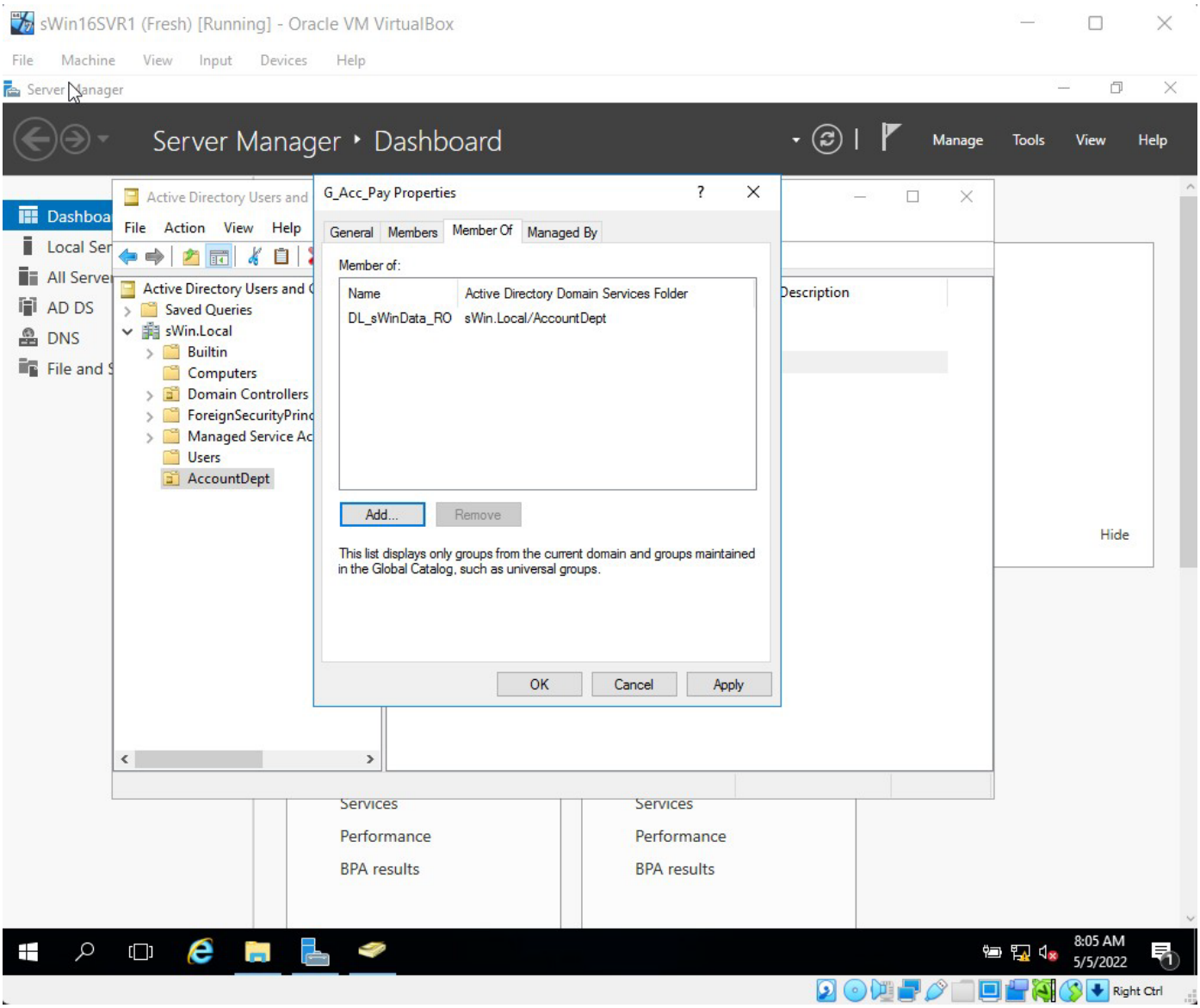
Creating Account Groups




sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Ser
All Server
AD DS
DNS
File and S
Active Directory Users and
File Action View Help
Active Directory Users and C
Saved Queries
sWin.Local
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Ac
Users
AccountDept
G_Acc_Pay 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:
sWin.Local
Locations...
Enter the object names to select (examples):
Jack (Jack@sWin.Local)S
Check Names
Advanced...
OK
Cancel
Add...
Remove
OK
Cancel
Apply
Hide
Services
Performance
BPA results
Services
Performance
BPA results
8:01 AM
5/5/2022
Right Ctrl


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers
Saved Queries
sWin.Local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
AccountDept
Name
Type
Description
DL_sWinData_RO
Security Group - Domain Local
DL_sWinData_RW
Security Group - Domain Local
G_Acc_Pay
Security Group - Global
G_Acct_Mgrs
Security Group - Global
Hide
Services
Performance
BPA results
Services
Performance
BPA results
8:02 AM
5/5/2022
Right Ctrl


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Ser
All Server
AD DS
DNS
File and S
Active Directory Users and
File Action View Help
Active Directory Users and
Saved Queries
sWin.Local
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Ac
Users
AccountDept
DL_sWinData_RW Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
G_Acct_Mgrs
sWin.Local/AccountDept
Add...
Remove
OK
Cancel
Apply
Description
Hide
Services
Performance
BPA results
Services
Performance
BPA results
8:04 AM
5/5/2022
Right Ctrl


sWin16SVR1 (Fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Active Directory Users and
File Action View Help
Active Directory Users and
Saved Queries
sWin.Local
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Ac
Users
AccountDept
G_Acc_Pay Properties
General Members Member Of Managed By
Member of:
Name
Active Directory Domain Services Folder
DL_sWinData_RO
sWin.Local/AccountDept
Add...
Remove
This list displays only groups from the current domain and groups maintained in the Global Catalog, such as universal groups.
OK
Cancel
Apply
Description
Hide
Services
Performance
BPA results
Services
Performance
BPA results
8:05 AM
5/5/2022
Right Ctrl

TNE10005 Journal Lab (#7)

Khalid Yaseen Baig / ID#102763240

What I learned in this week's Lecture.

- If resources are accessed locally, aggregate NTFS Allow rights from all ACL groups the account is a 'member' of, keeping in mind that deny takes precedence over other permissions.

- When a computer is disconnected from the domain, GPOs can be implemented using Local Computer Policies.

- Computer Config's functions include applying settings to a single computer account, deploying software to all users who use that computer, startup/shutdown routines, deploying printers, and controlling updates.

- User Account Settings, Deploy Software to Where the User Logs On, Logon/Logoff Scripts, and Deploy Printers are all features of User Config.

- Group Policy Container is stored in AD, duplicated automatically to other domain DCs, and points to GPT for settings.

- Policy for the Group GPO settings are contained in the template, which will not duplicate if placed in the incorrect location and is stored in Sysvol (default location).

- GPO must be associated with a Site, Domain, or OU. It can't be connected to Groups, Users, Computers, or Computers containers in Active Directory.

- Multiple GPOs can be linked to a single organizational unit. Many organizational units can be linked to a GPO. The organizational unit is a container that may have GPOs attached to it, although the general Container (discovered during the formation process) does not.

- Unlinking a GPO stops it from being applied. Quick troubleshooting is possible with this tool.

- It is possible to delegate permissions to link GPOs to an OU. Delegate Control wizard may be used to do this.

- The Order of Precedence is the inverse of the Order of Application. The GPO with the highest precedence wins. When many GPOs configure distinct settings, the settings are accumulated.

- Blocking Inheritance stops GPOs from applying to items in the OU that are related to any parent container. You can't stop inheritance selectively; you can only prevent it entirely.

- Enforcing a GPO overrides inheritance blocking, conflicts, and allows 'Head Office' to override rogue branch administrators.

- ADML supports different languages, for example, a global corporation can have domains where administrators can view the GPO interface in their native language.

- Product developers may produce ADMX, xml files with code for GPO settings, and ADMX files for their software.

- Group Policy Modelling, Group Policy Results, or gpresult may be used to troubleshoot GPOs.

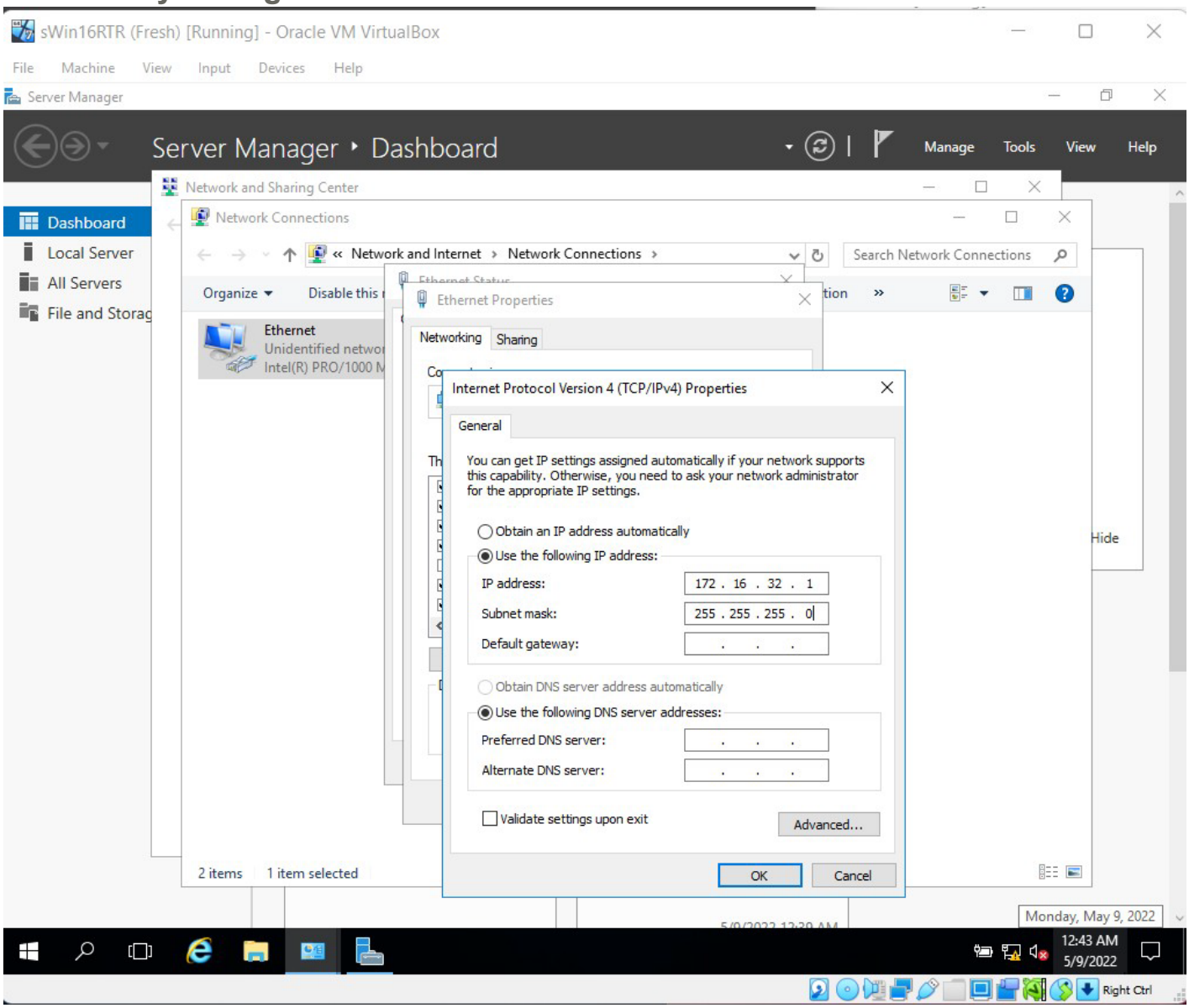
- Using GPOs to deploy printers It's possible to accomplish this using the Print Management console.

- Preferences can be conditional using GP Preference Level Targeting (Item Level Targeting).

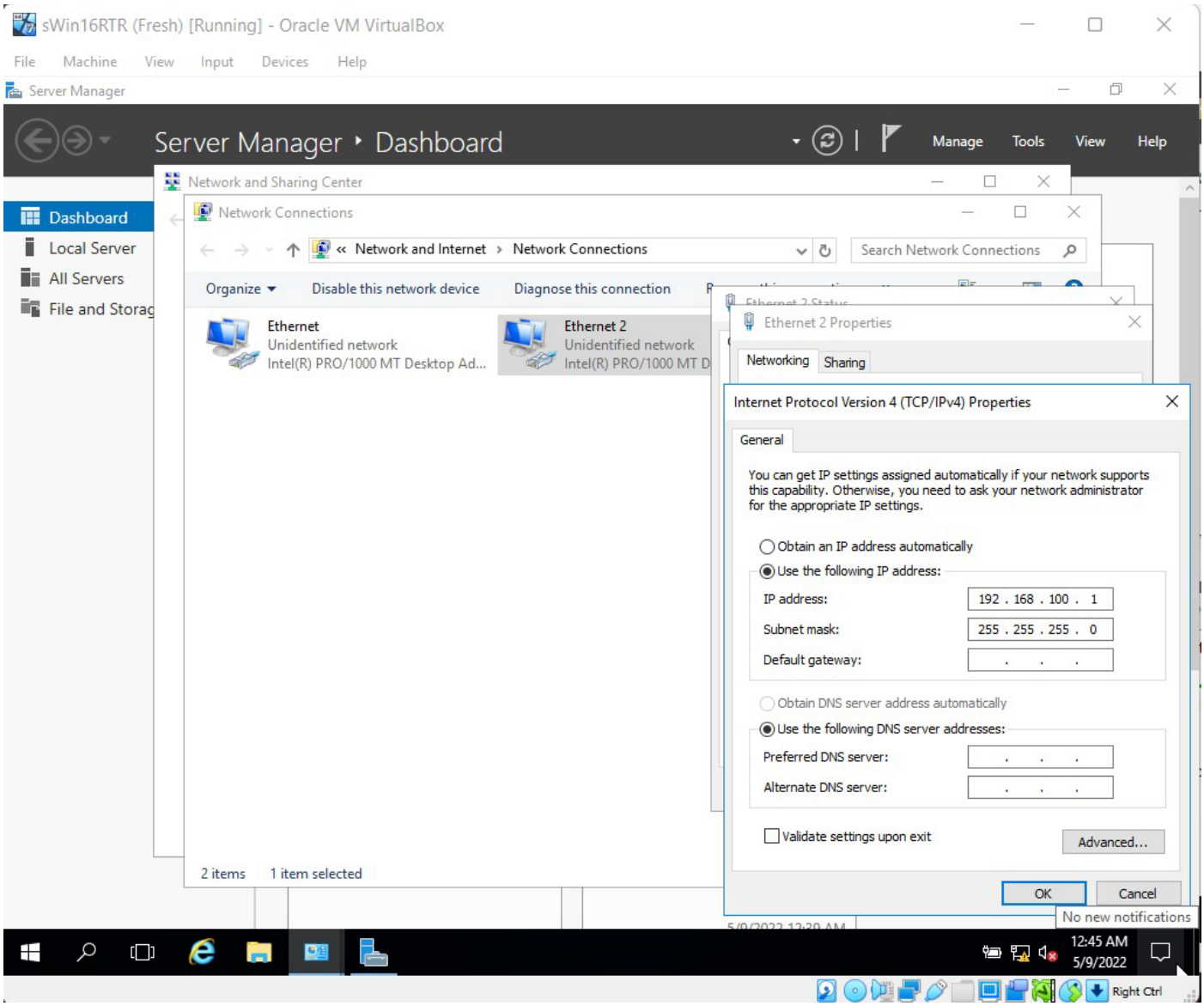
This week’s lab activities.

Screenshot the important steps required when doing the lab.

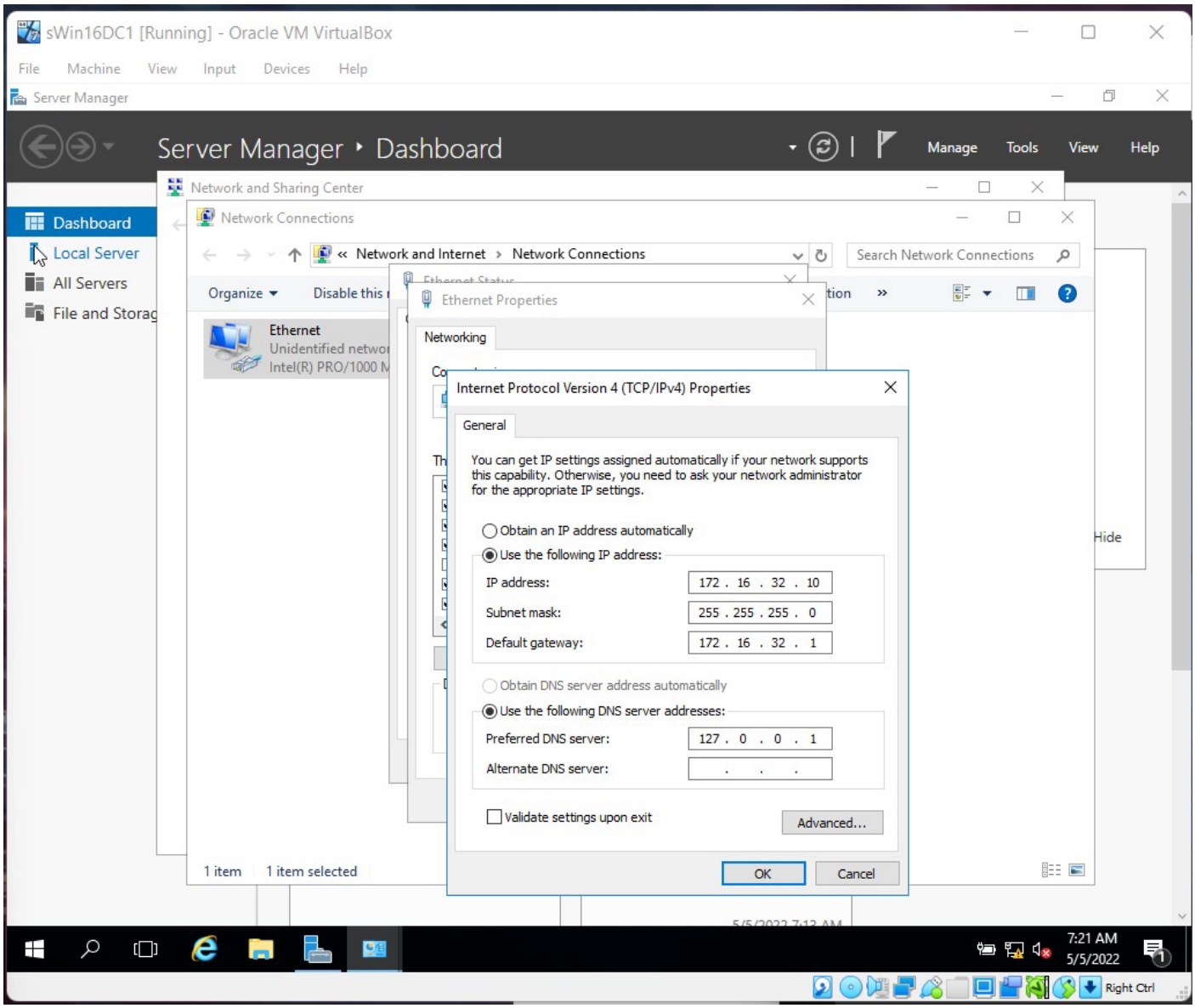
- **Preliminary settings**



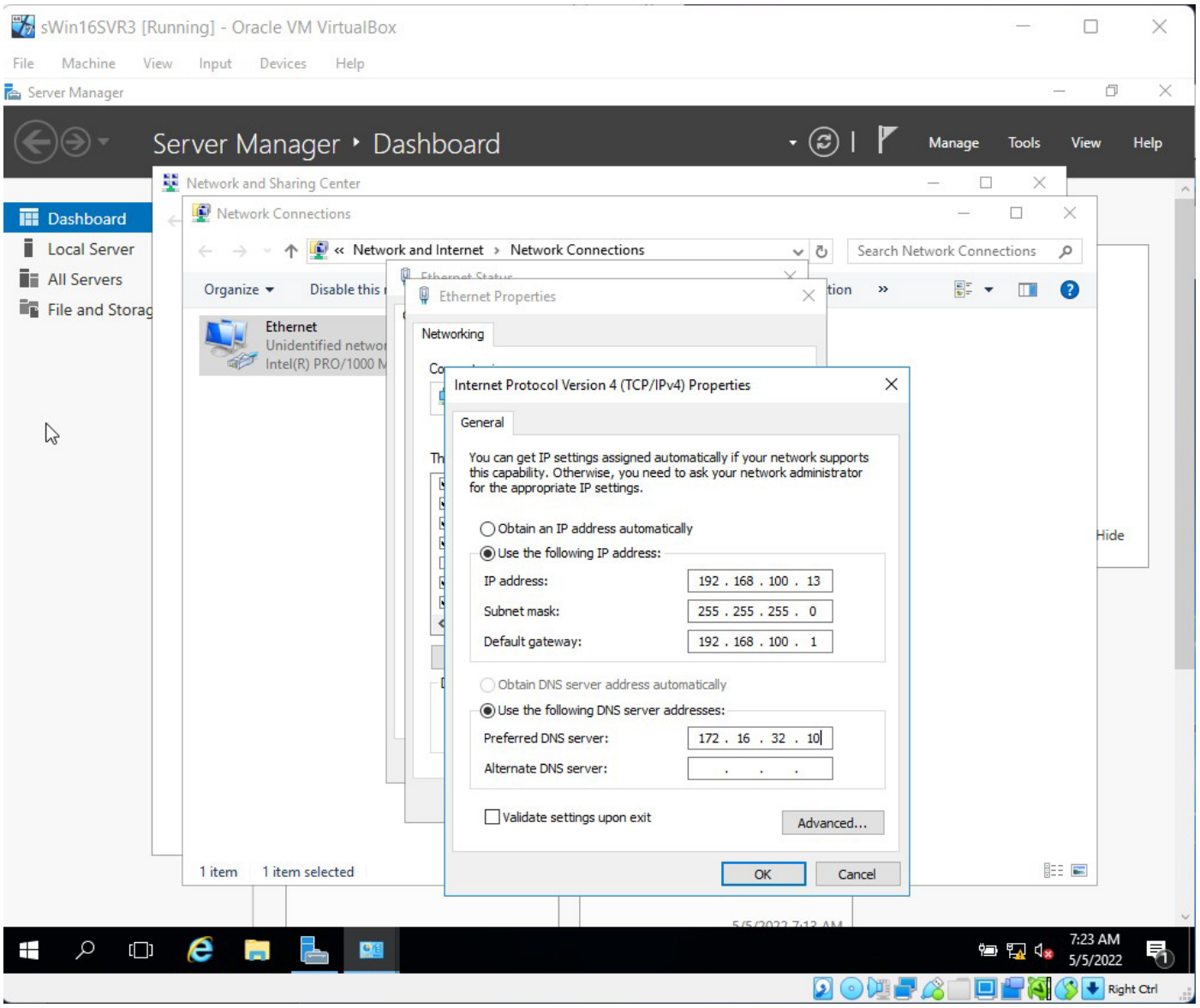
Preliminary settings of the sWin16RTR for the Hawthorn Internal Network.



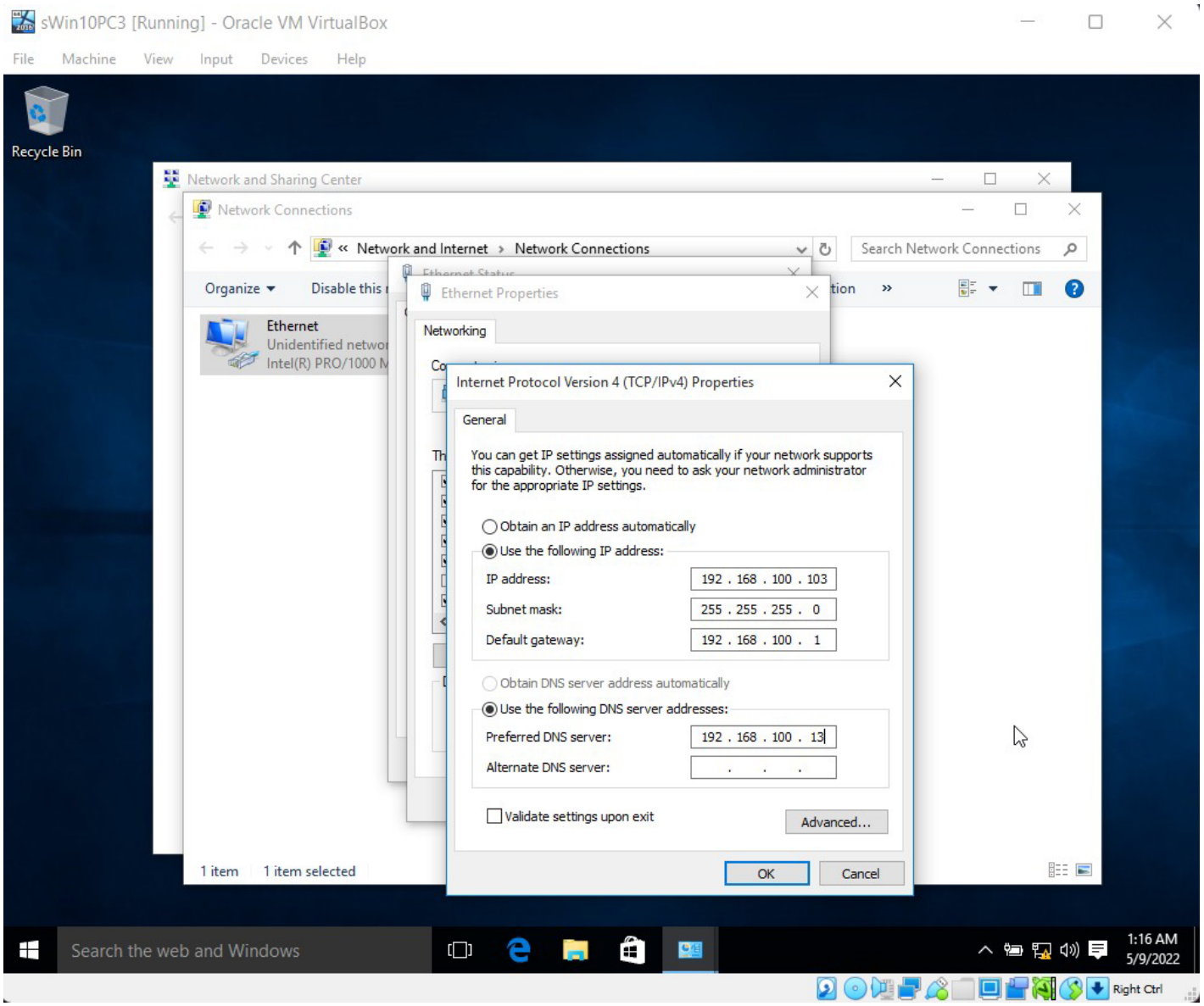
Preliminary settings of the sWin16RTR for the Wantirna Internal Network.



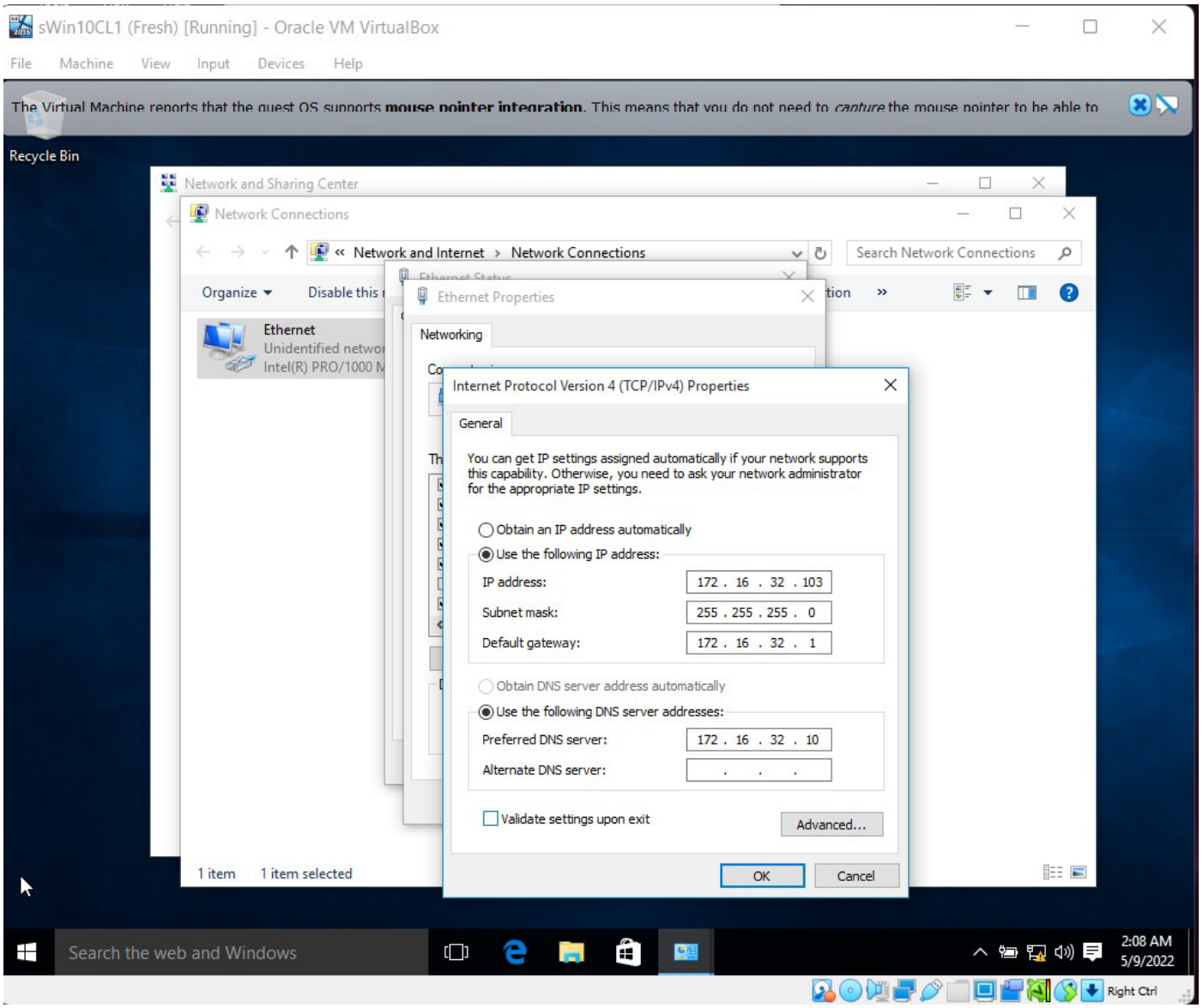
Preliminary settings of the sWin16DC1 for the Hawthorn Internal Network.



Preliminary settings of the sWin16SVR3 for the Wantirna Internal Network.

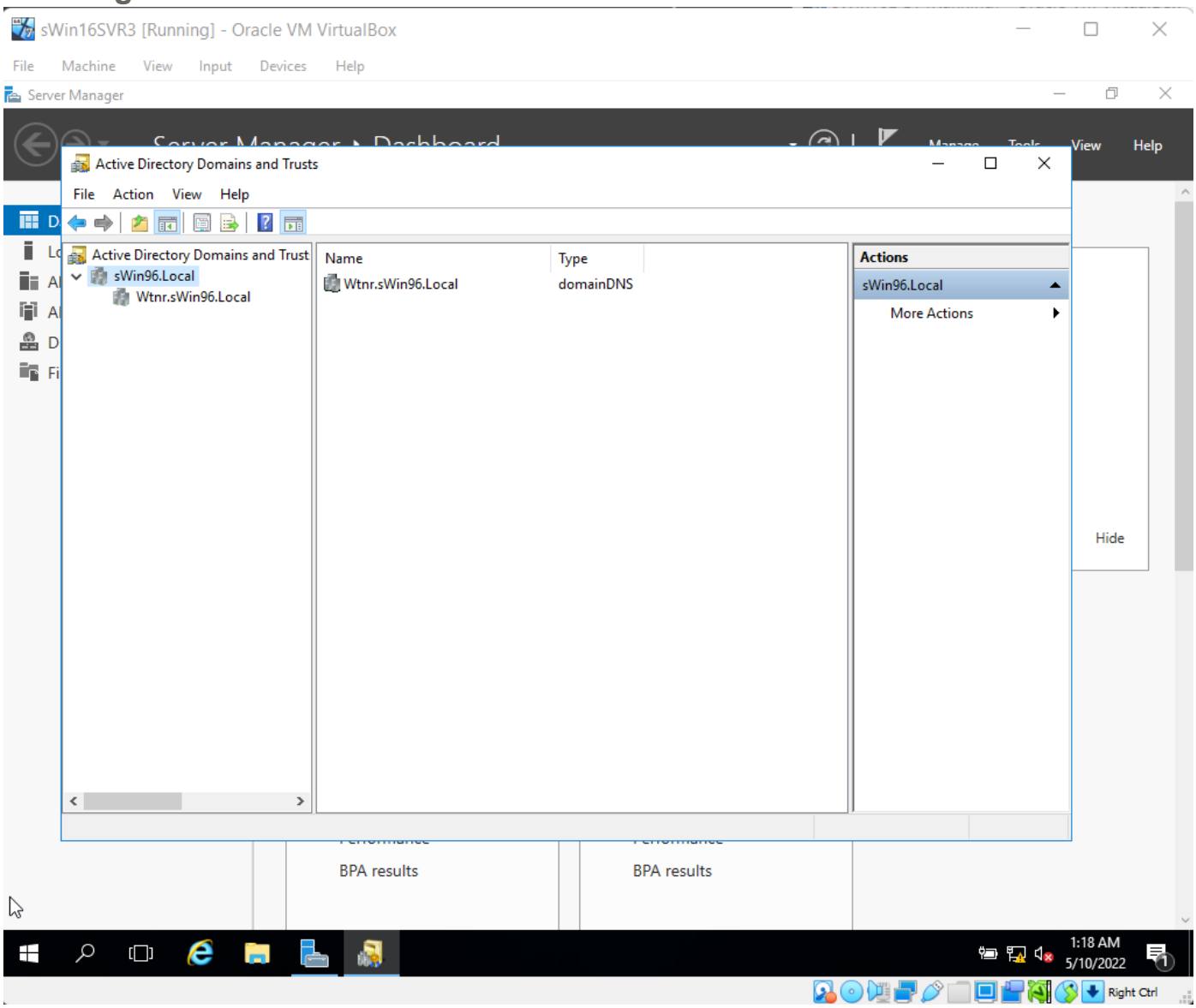


Preliminary settings of the sWin10OC3 for the Wantirna Internal Network.



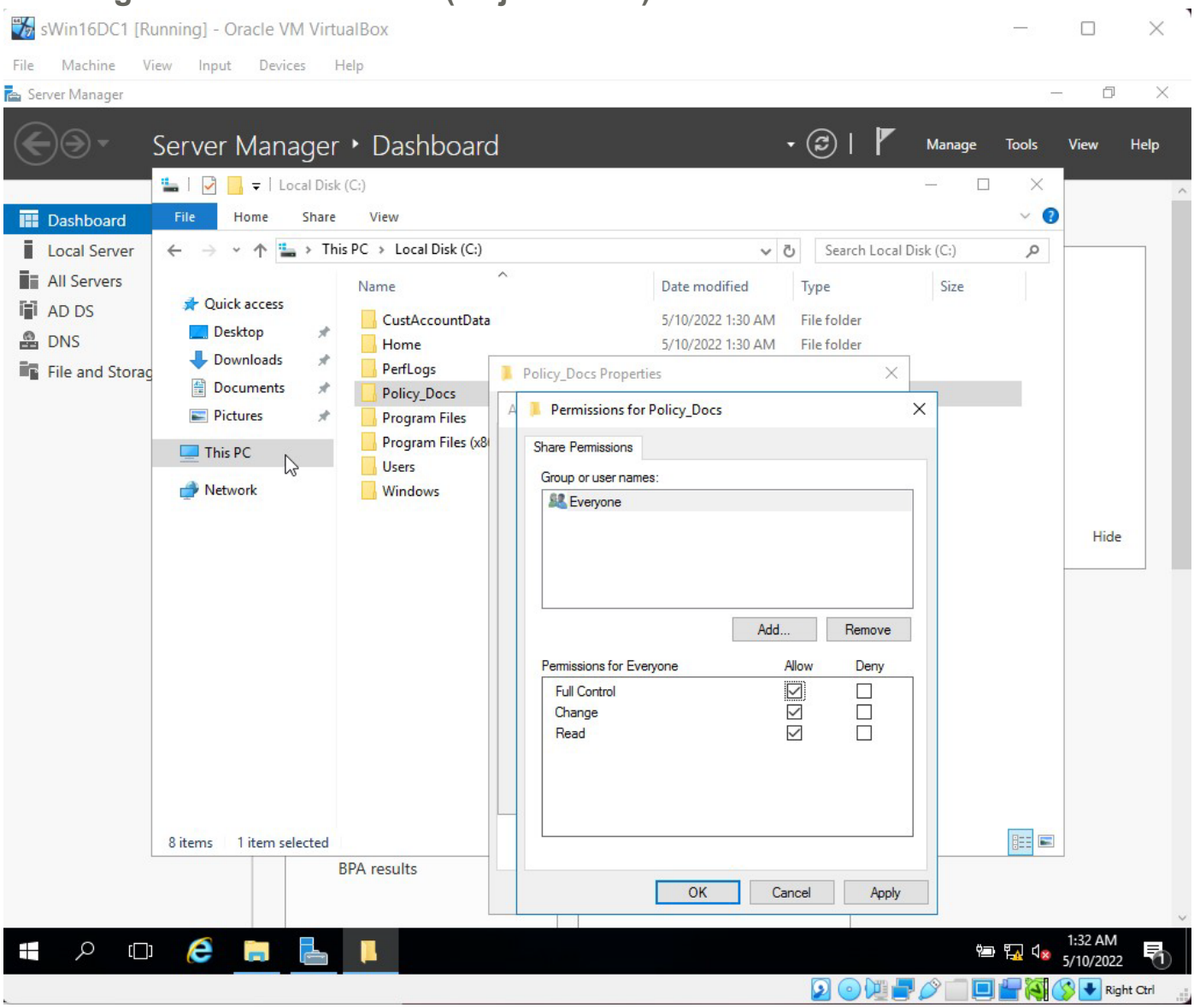
Preliminary settings of the sWin10CL1 for the Hawthorn Internal Network.

- **Creating a Child Domain**

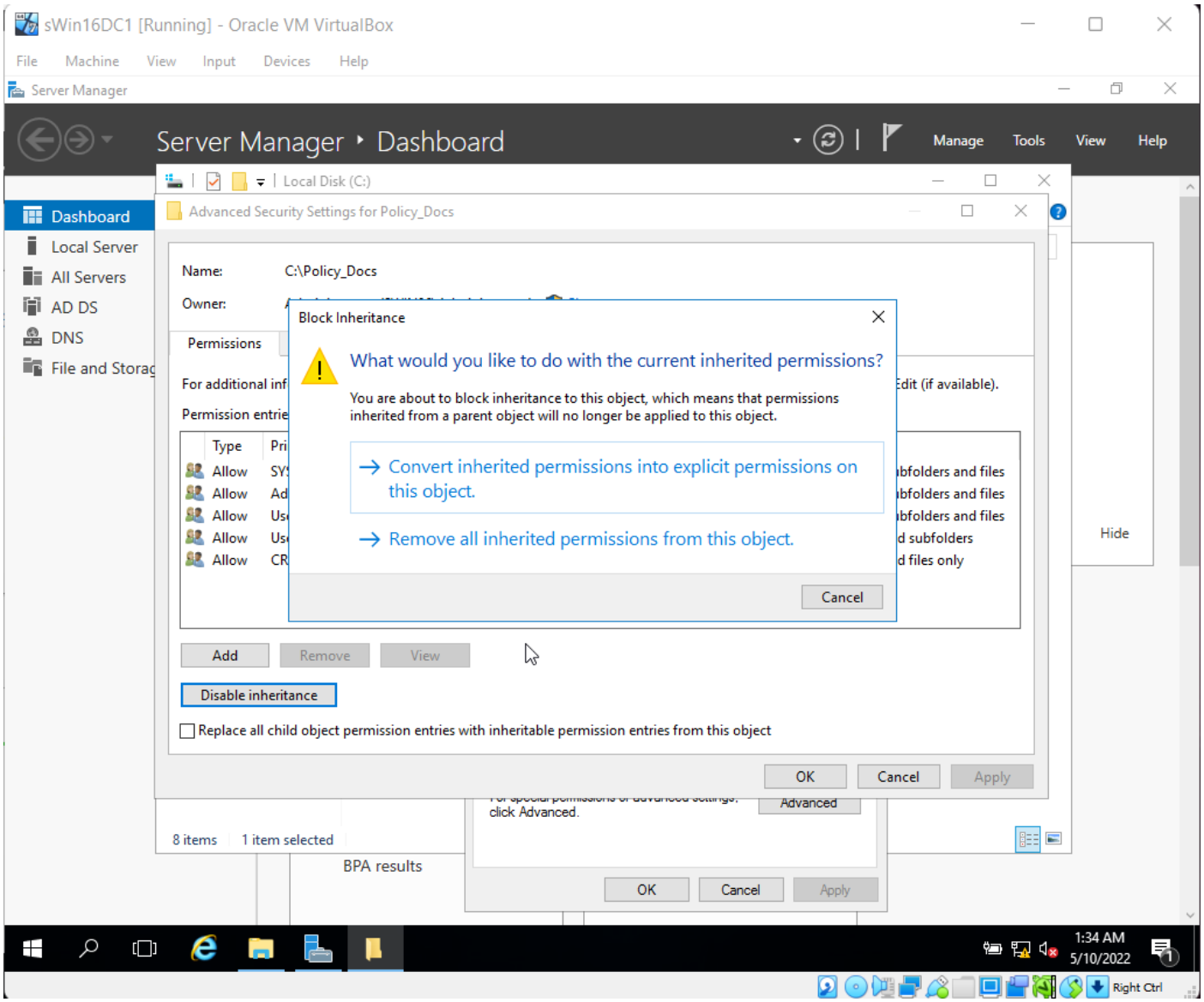


Successful creation of child domain in the sWin16SVR3 Virtual Machine named “Wtnr” with “sWin96.Local” as parent Domain.

- **Creating Network Resources (Object / files)**

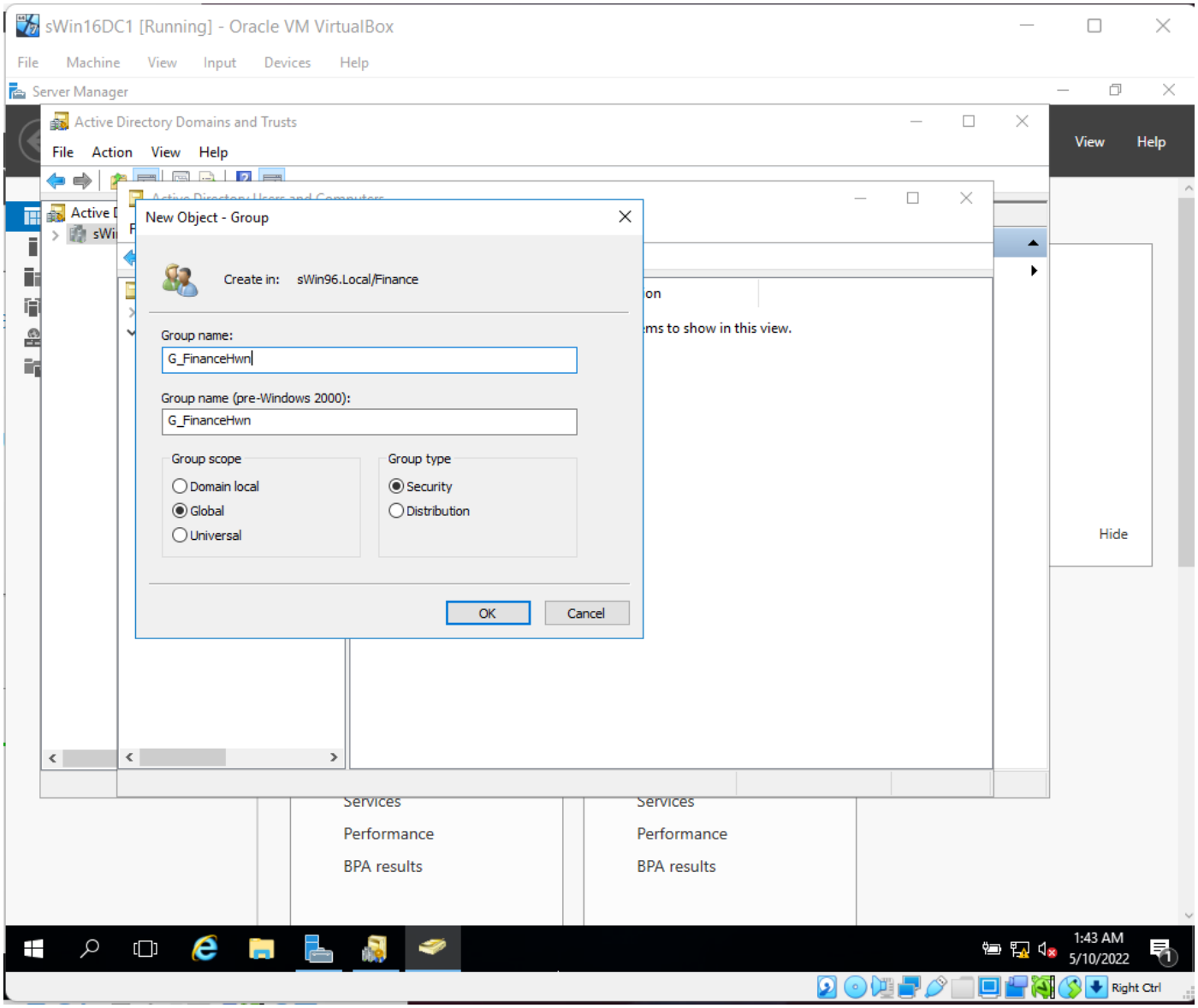


Sharing Policy_Docs, CustAccountData and Home with share permissions = Full control.



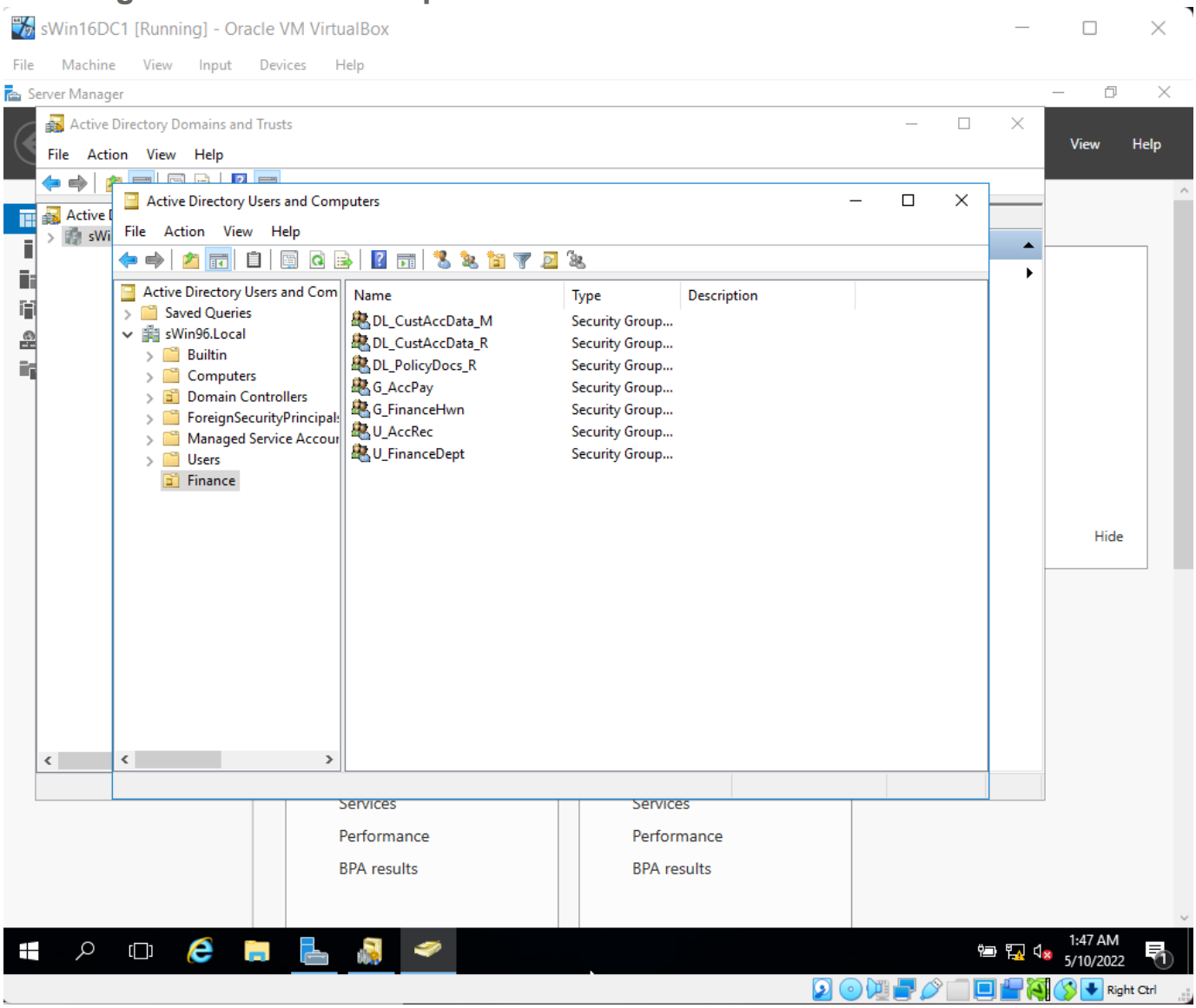
Removing Inherited Permissions on the folders Policy_docs and CustAccountData.

Create an OU



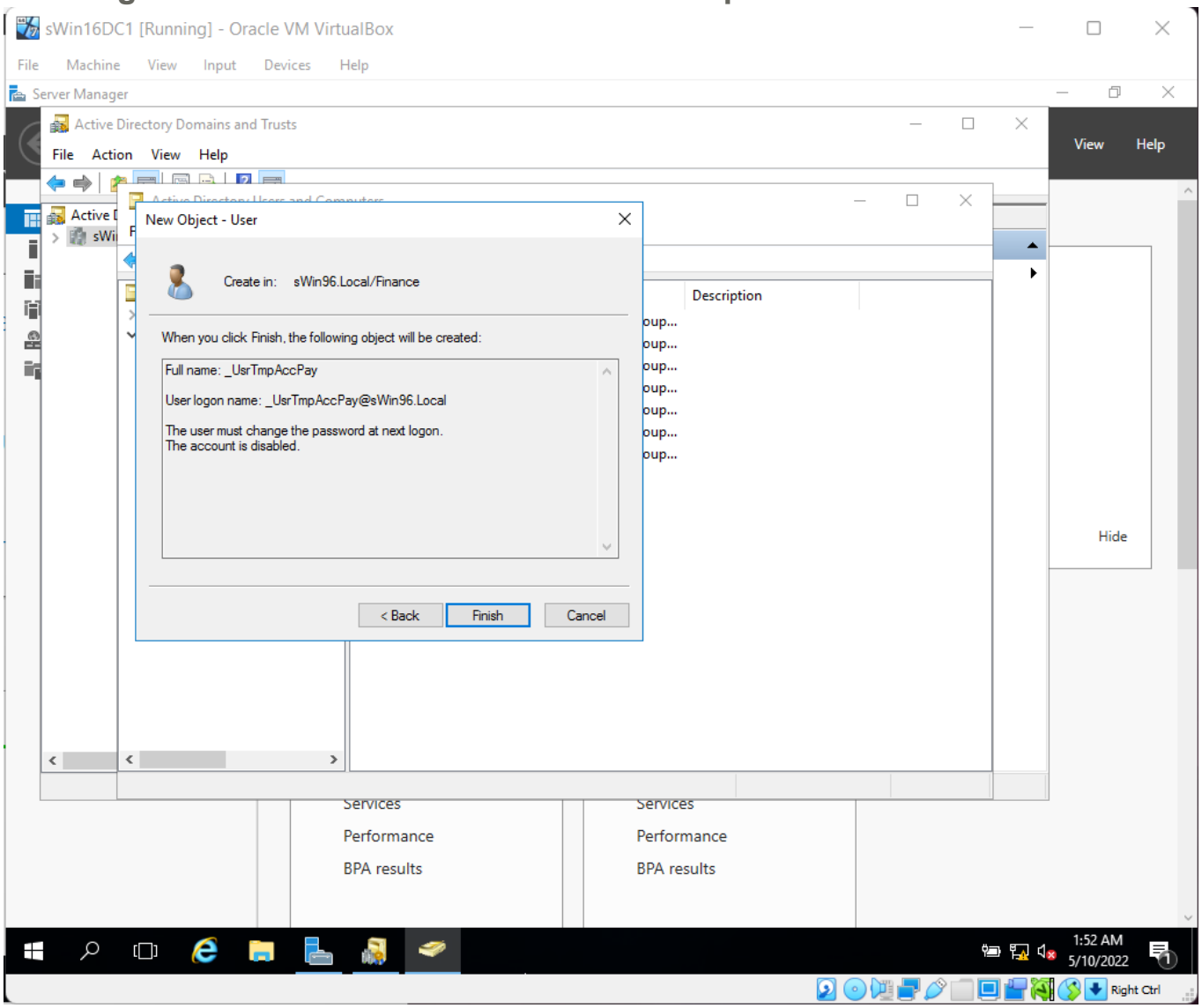
Creating new Organizational Unit named Finance under the sWin96.Local Domain on sWin16DC1

Creating sWin96.local Groups

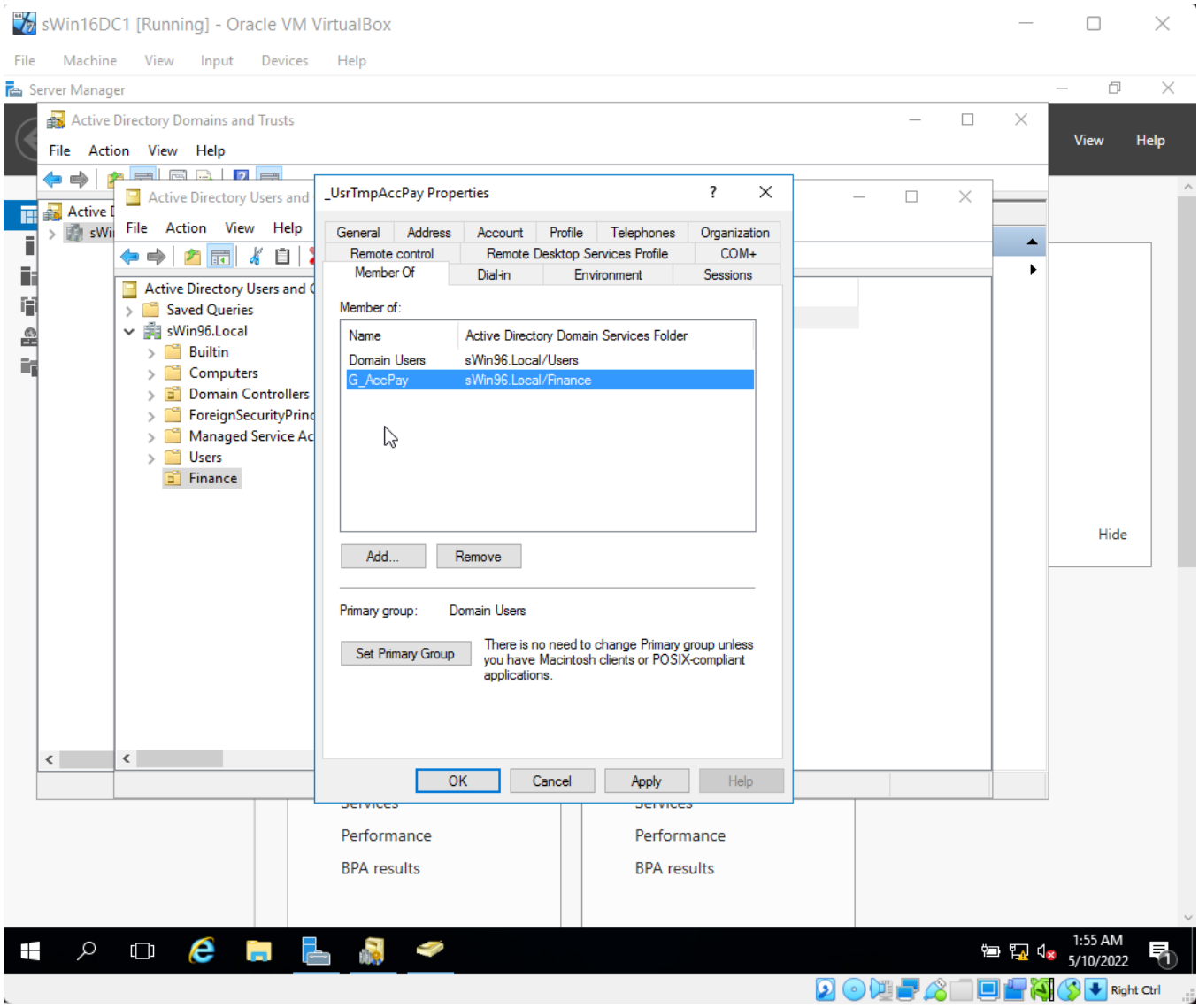


Creating Groups under the Finance OU.

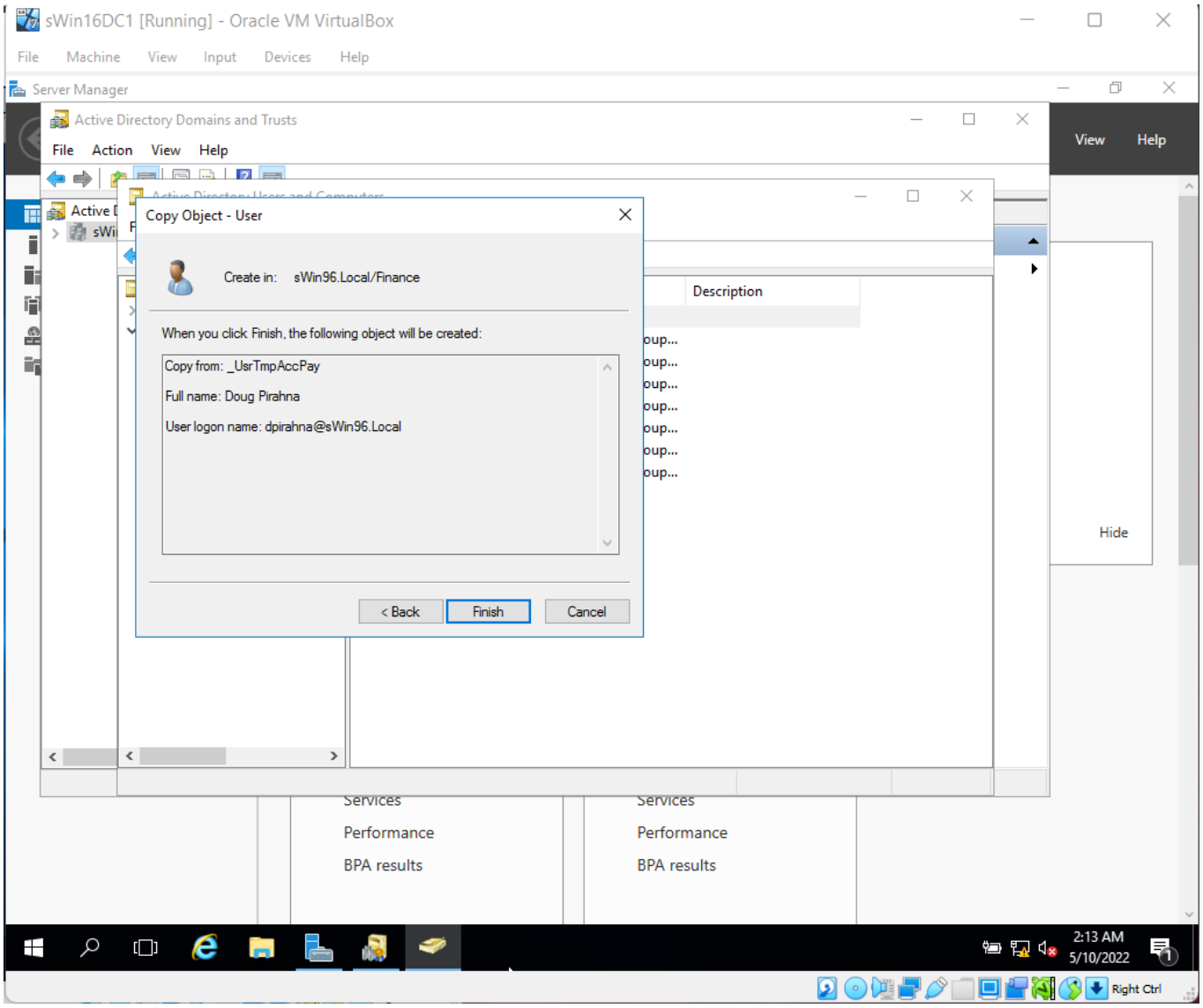
Creating sWin96.local User Accounts and Templates



Creating New users under Finance OU, with _UsrTmpAccPay as both the First name, and User logon name.

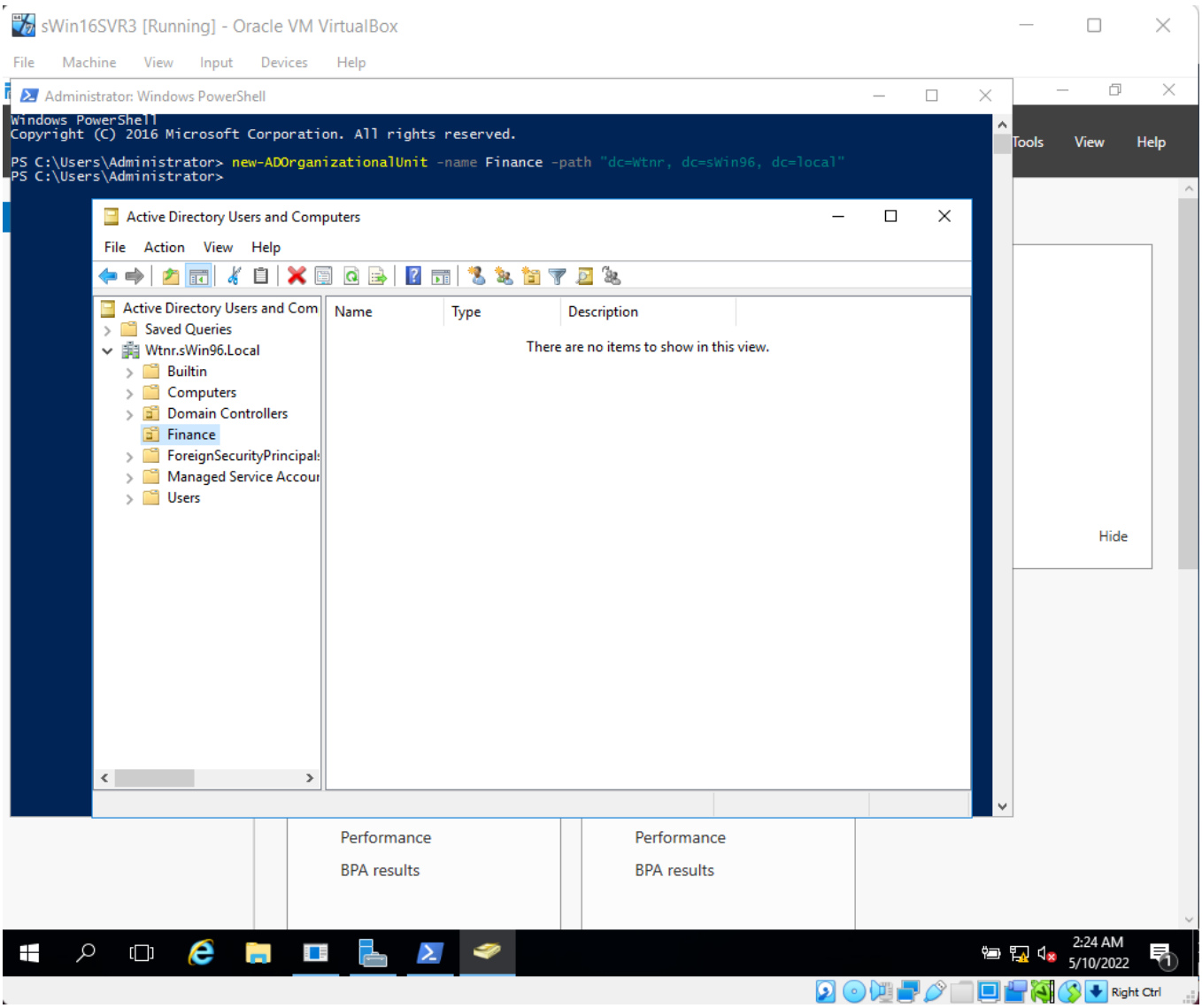


Adding _UsrTmpAccPay as a member of G_AccPay



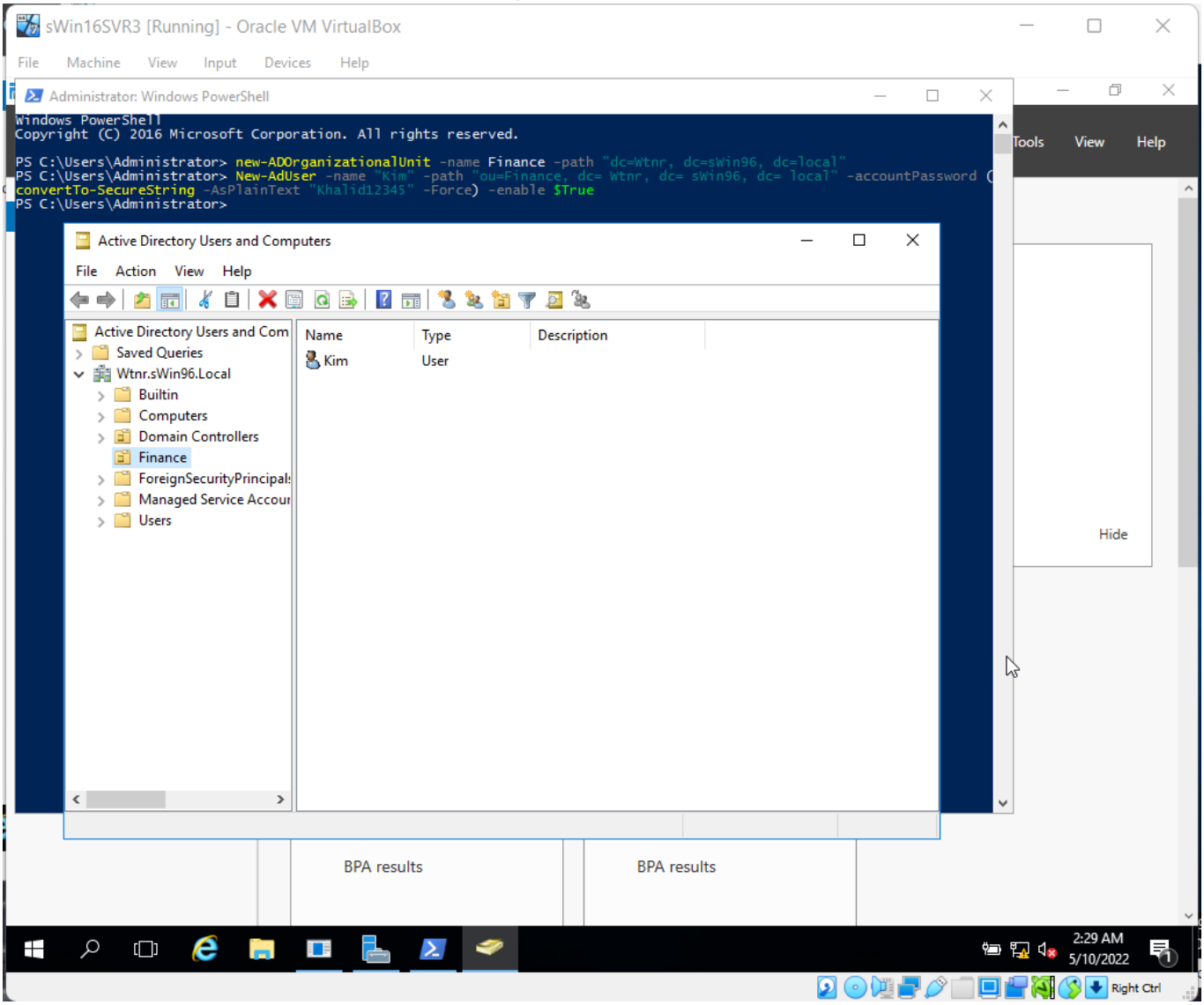
Copying the _UsrTmpAccPay user profile and creating new users with it.

- # Create Wtnr.sWin.local Objects
Create an OU in PowerShell



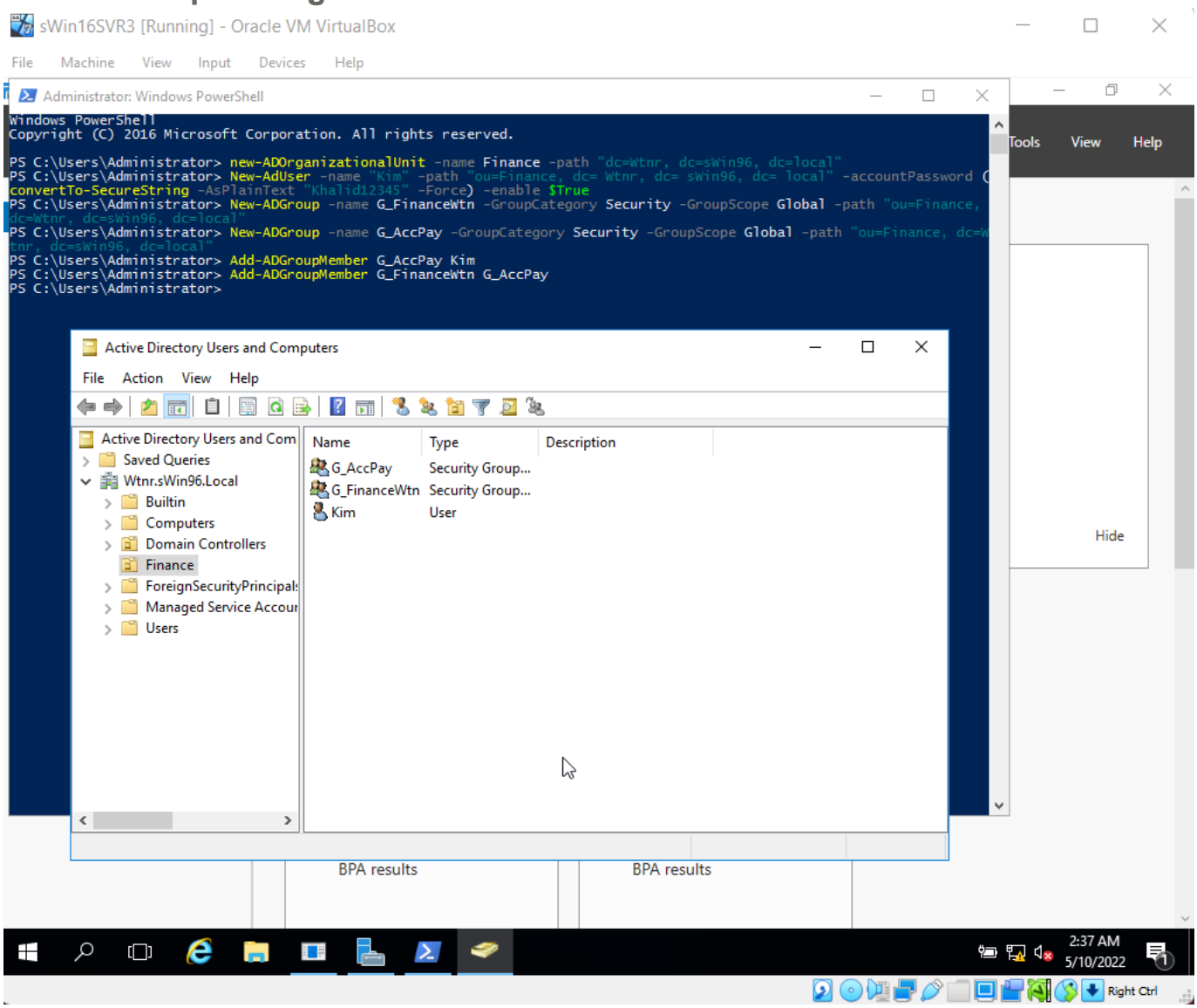
Creation of Ou Finance in sWin16SVR3 using powershell.

- **Create a New User Account Using PowerShell**



Creation of New User Account named Kim under OU Finance in sWin16SVR3 using powershell.

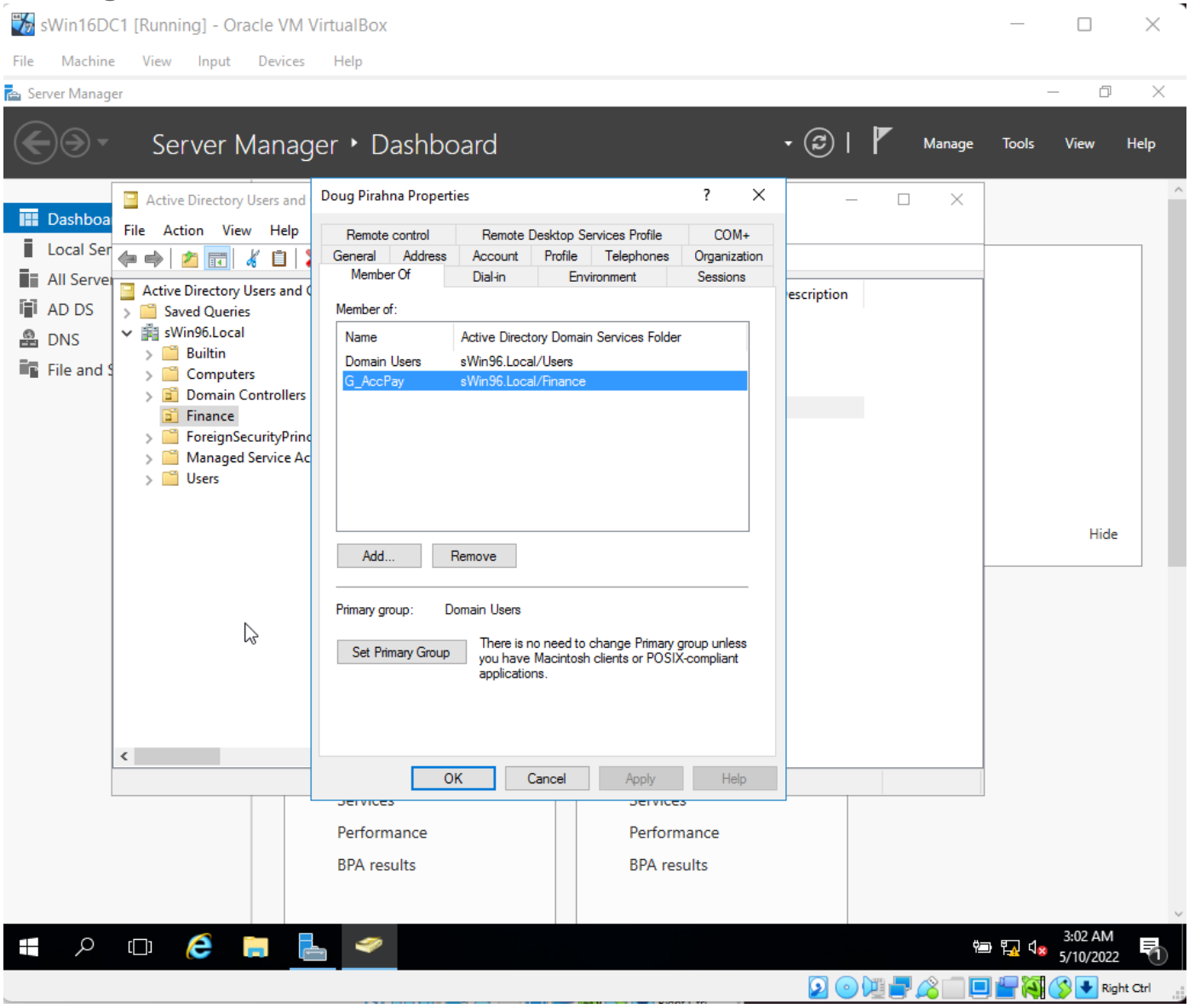
Create Groups Using PowerShell



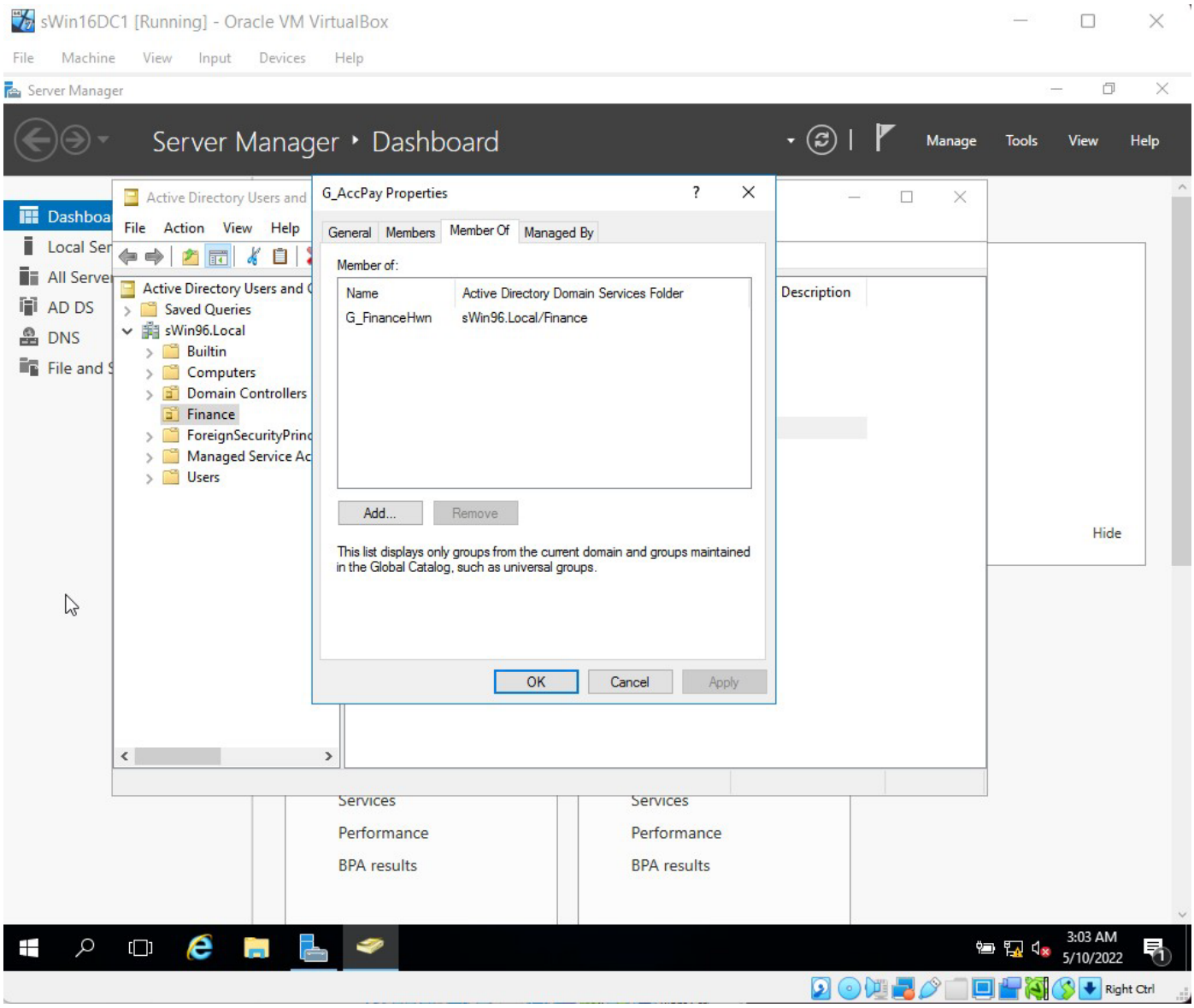
Creation of New Groups named G_FinanceWtn and G_AccPay under OU Finance and setting the membership and nesting of theb groups in sWin16SVR3 using powershell

Nesting the Groups in the Forest

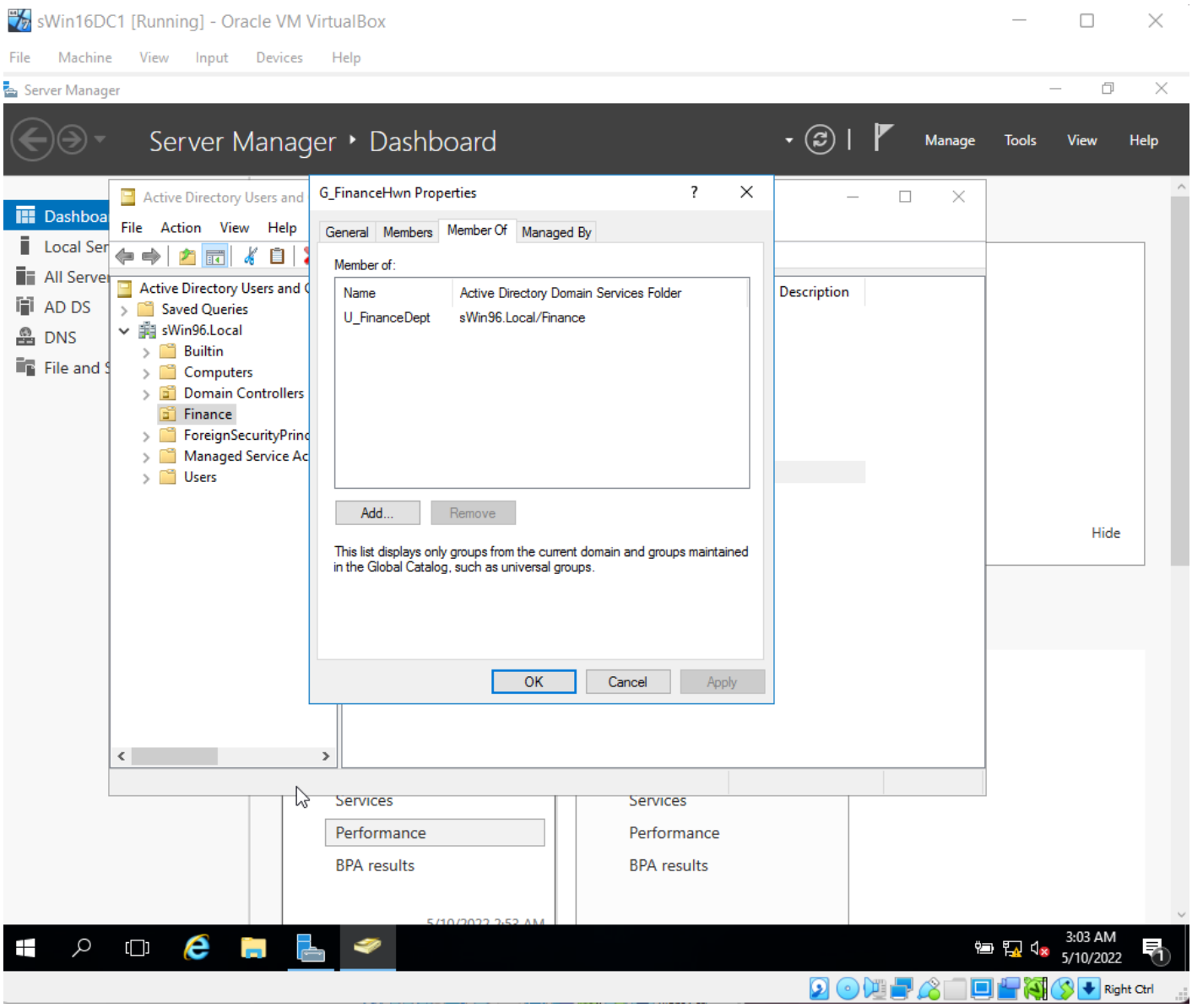
Nesting Within the Hawthorn Domain



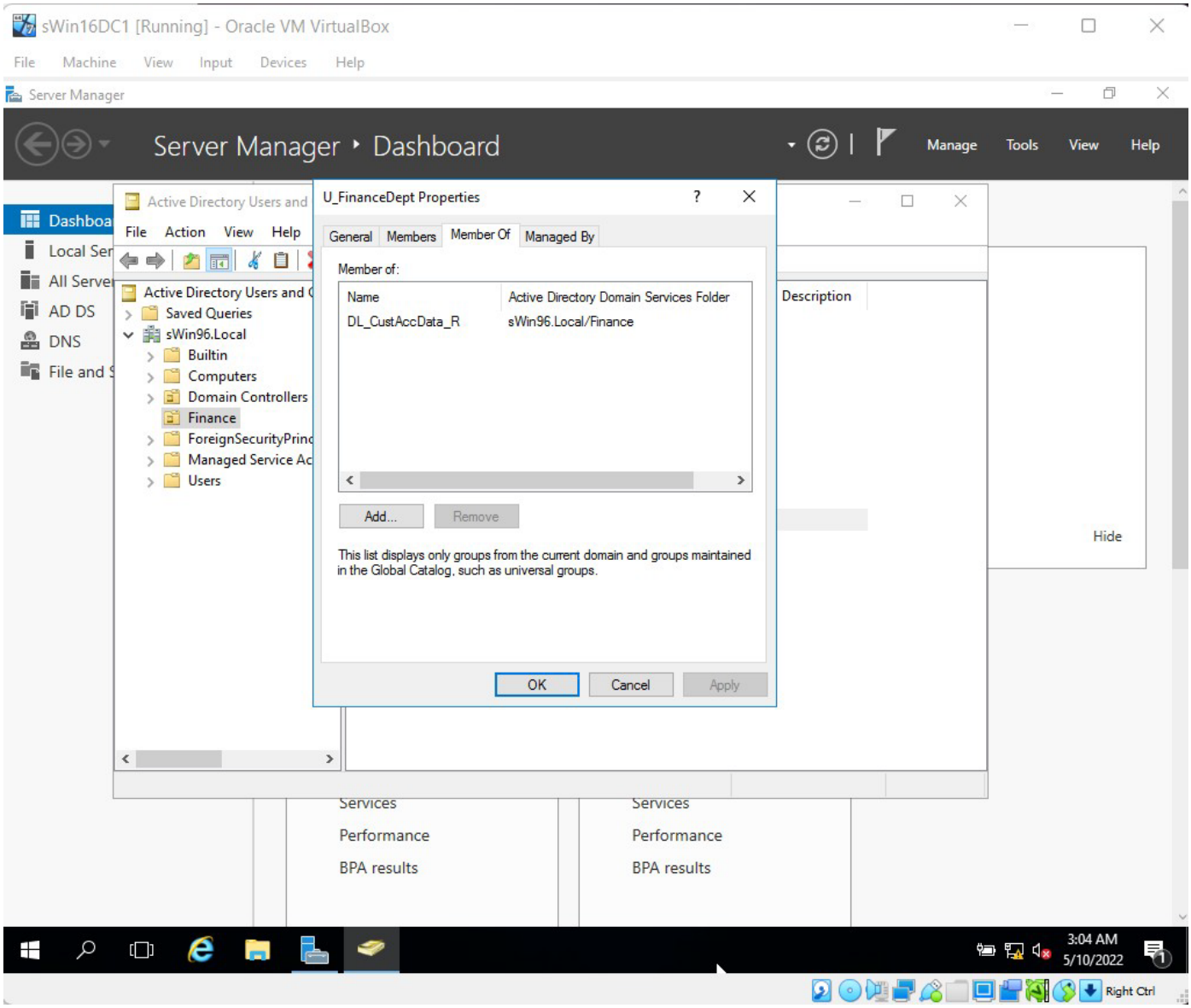
Doug Pirahna is a member of G_AccPay



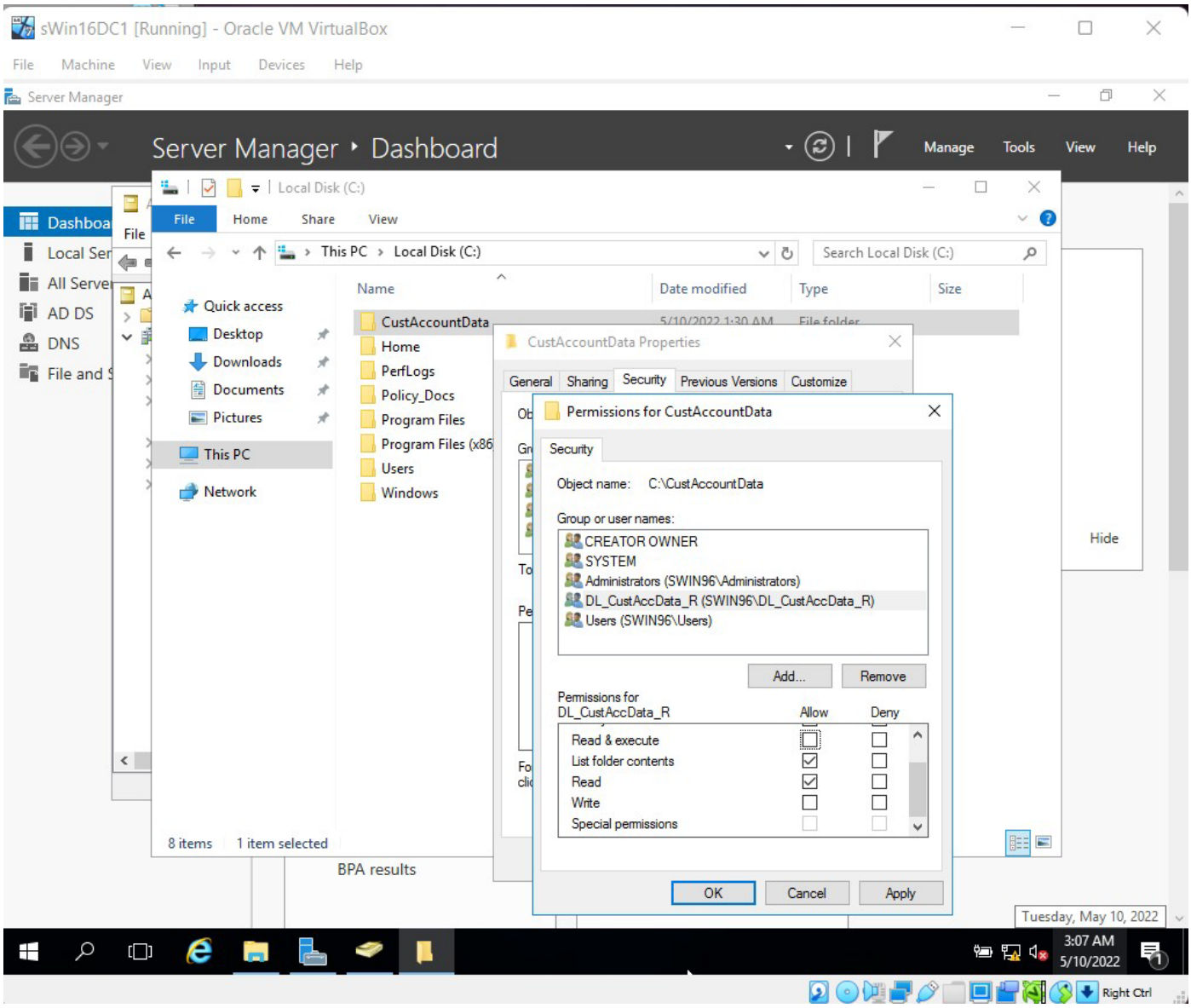
G_AccPay is a member of G_FinanceHwn.



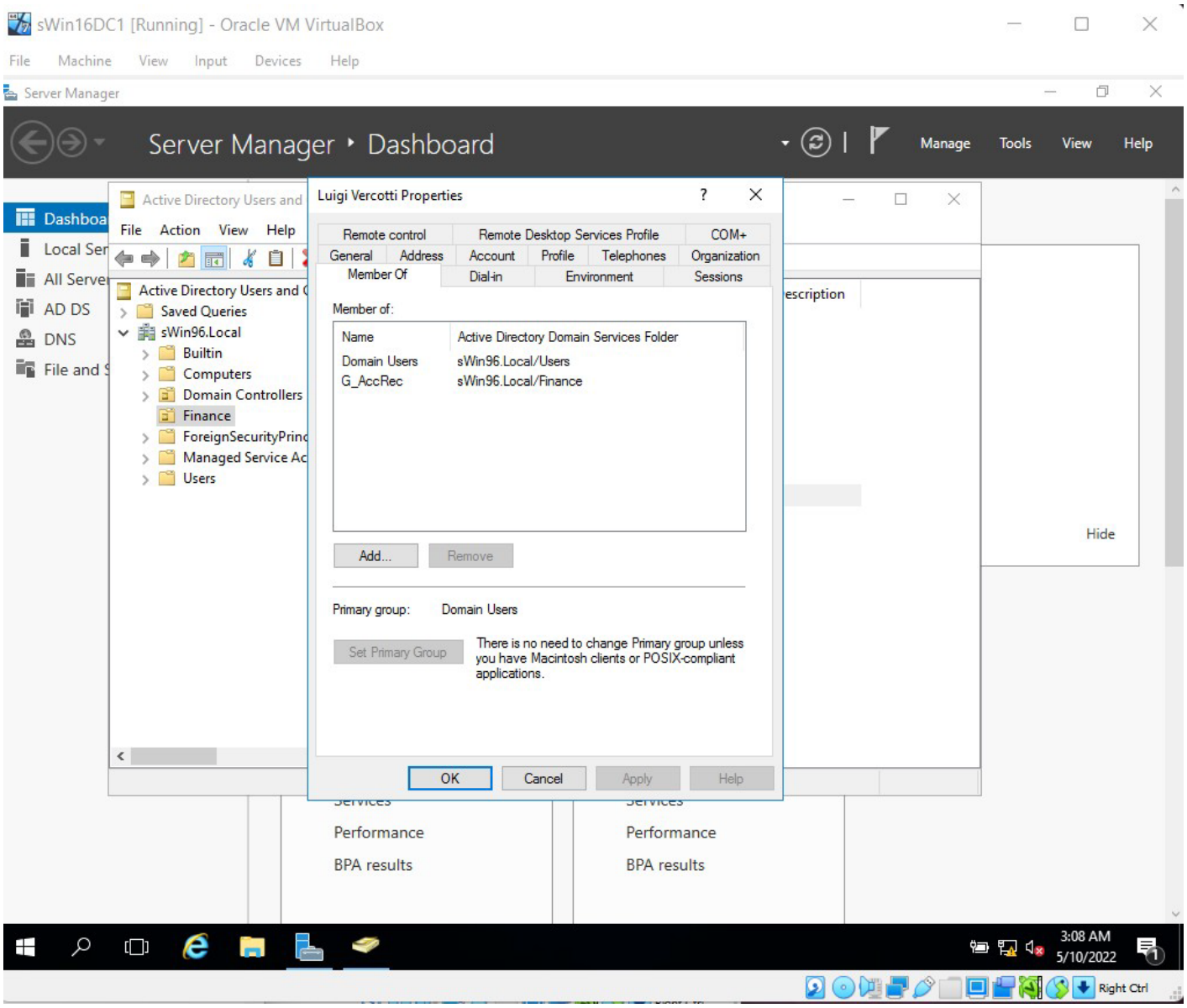
G_FinanceHwn is a member of U_FinanceDept



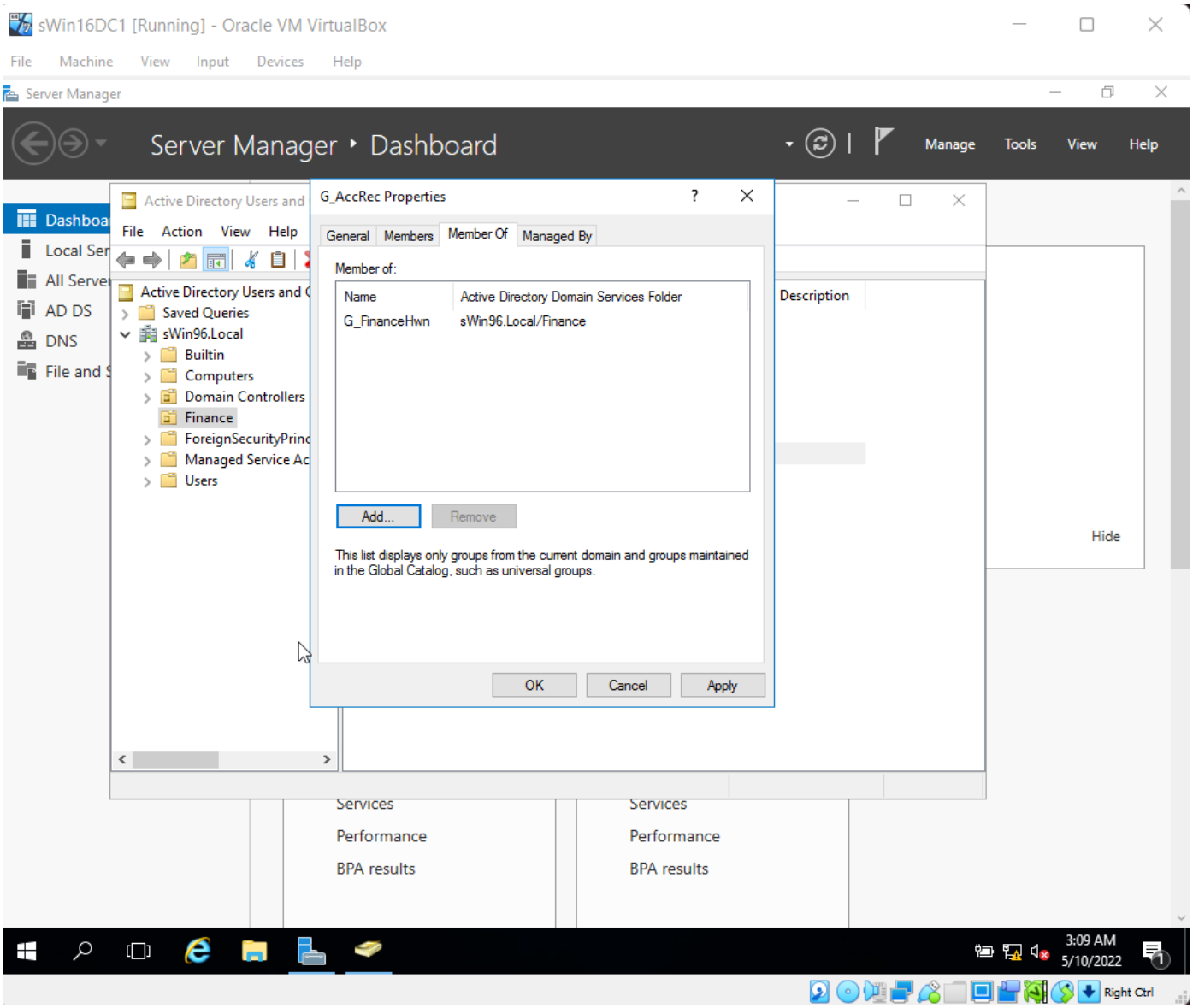
U_FinanceDept is a member of DL_CustAccData_R.



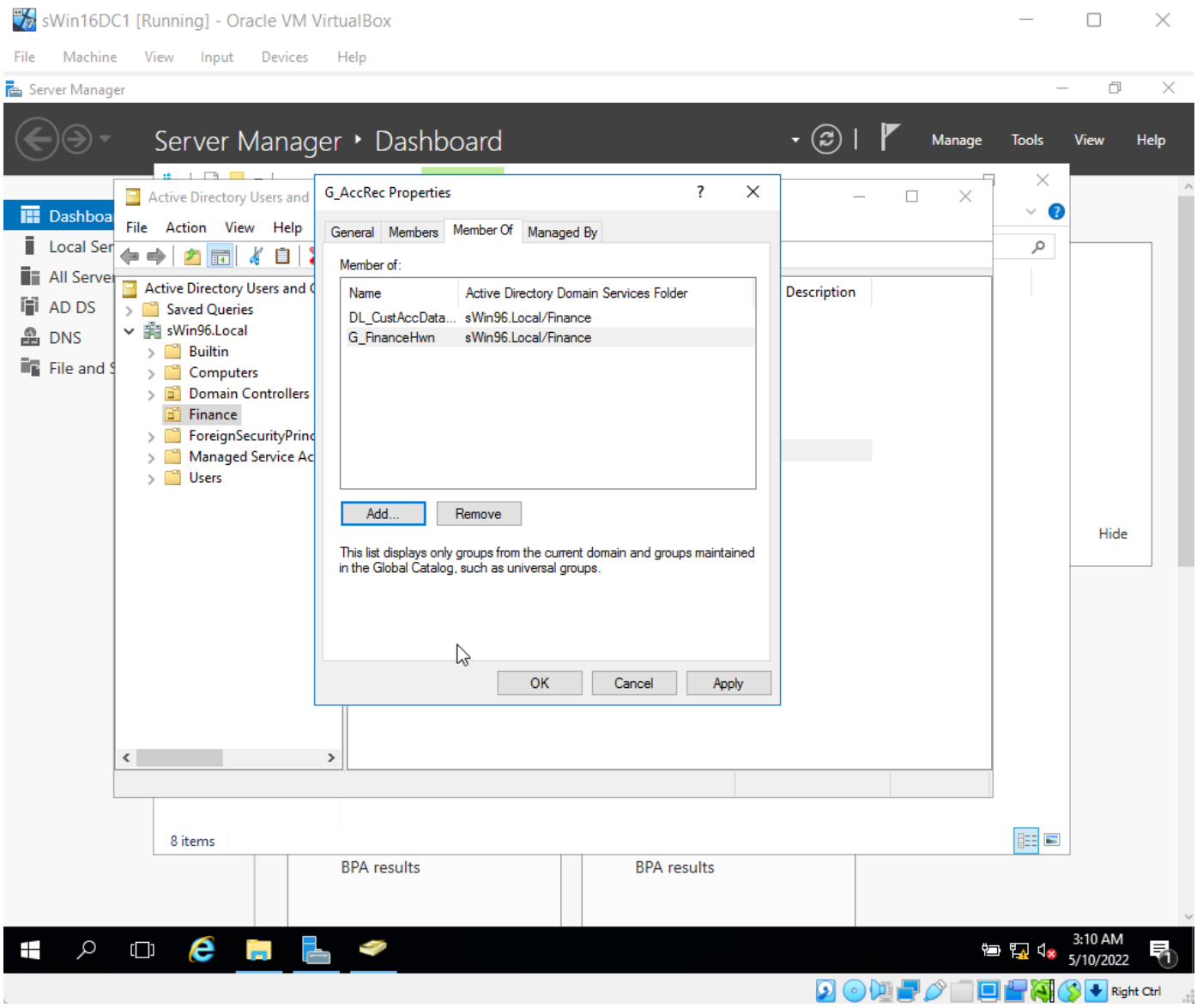
Assigning DL_CustAccData_R the permissions to Read and List folder contents to the CustAccountData folder.



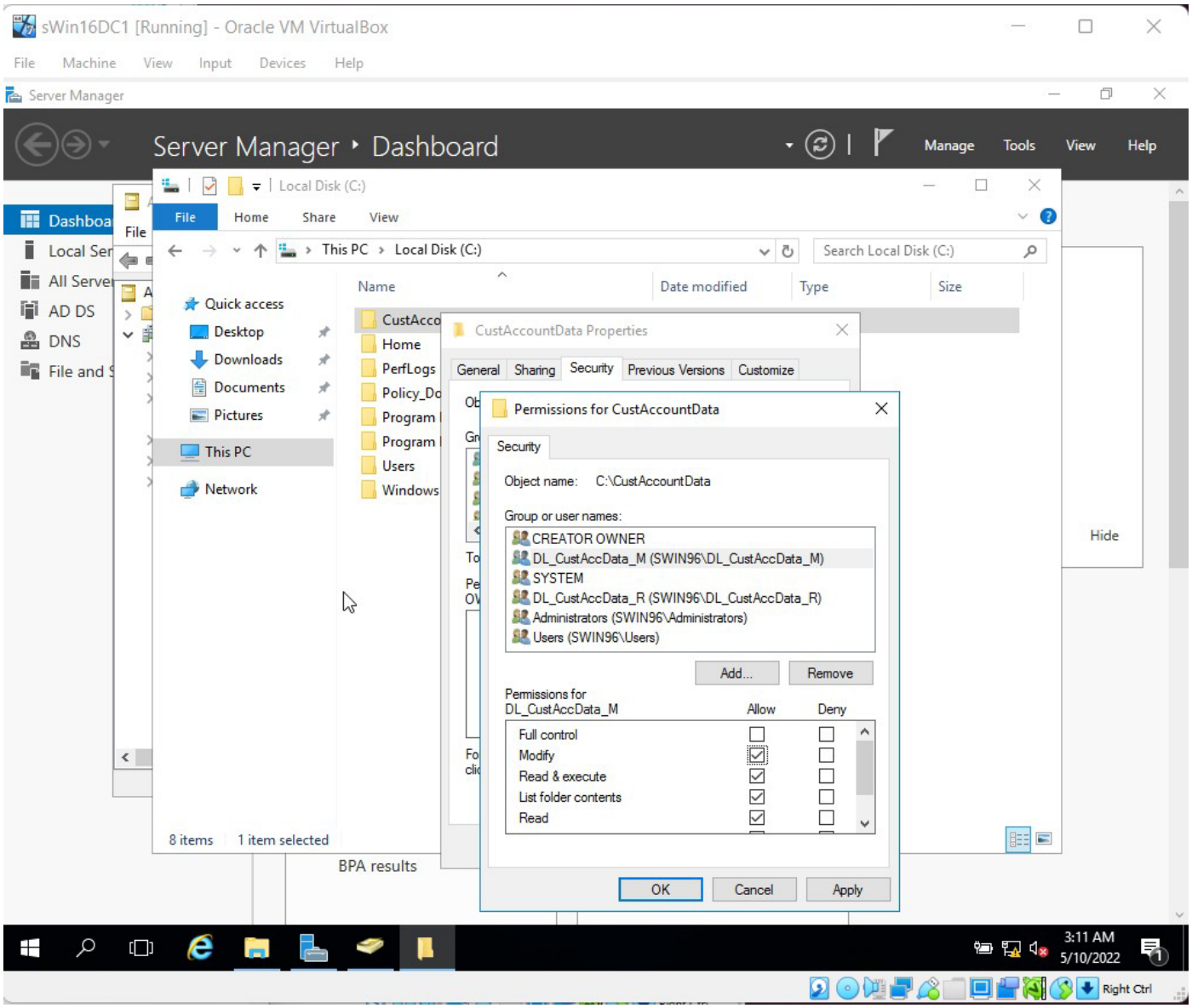
Luigi Vercotti is a member G_AccRec.



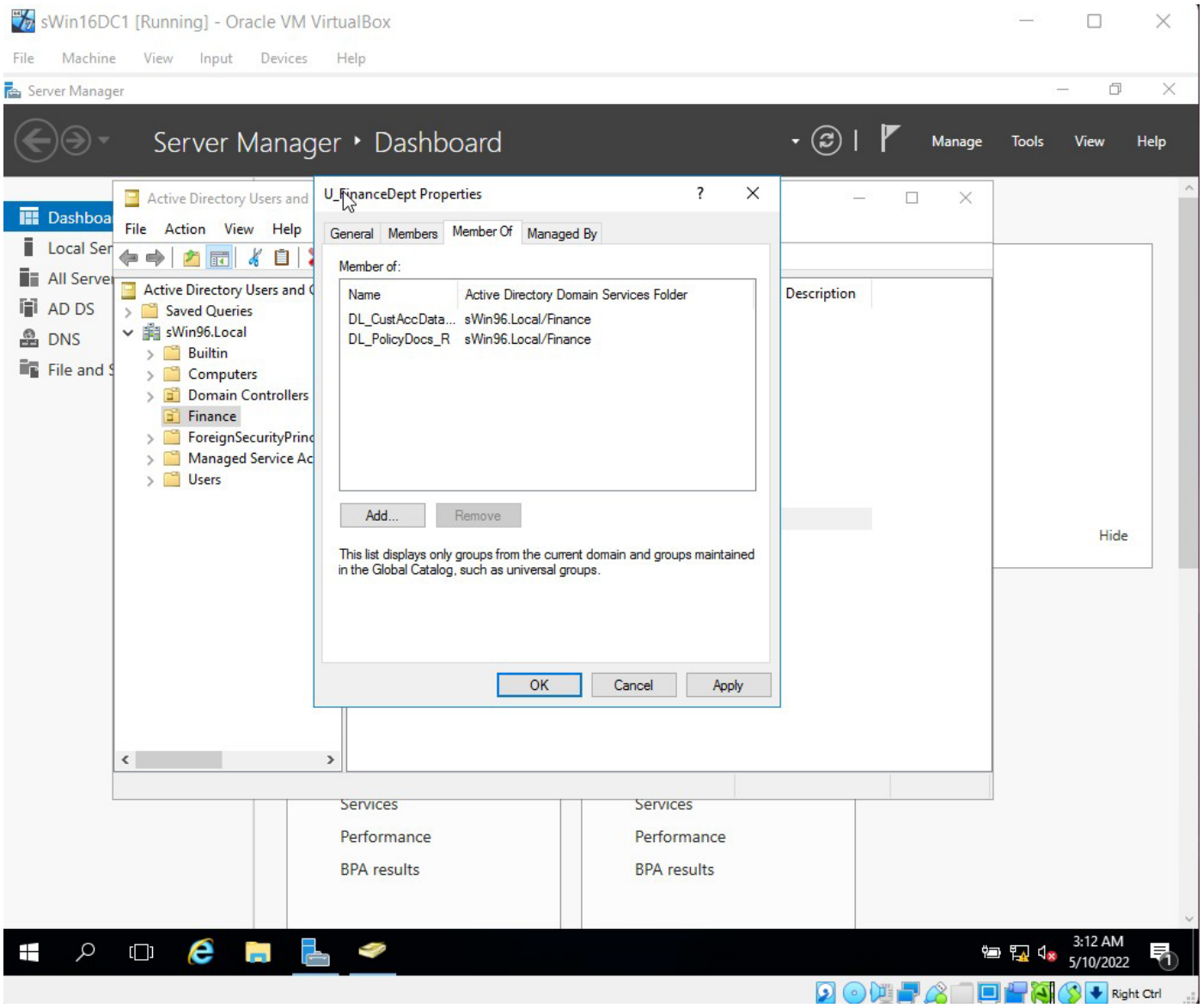
G_AccRec is a member of G_FinanceHwn.



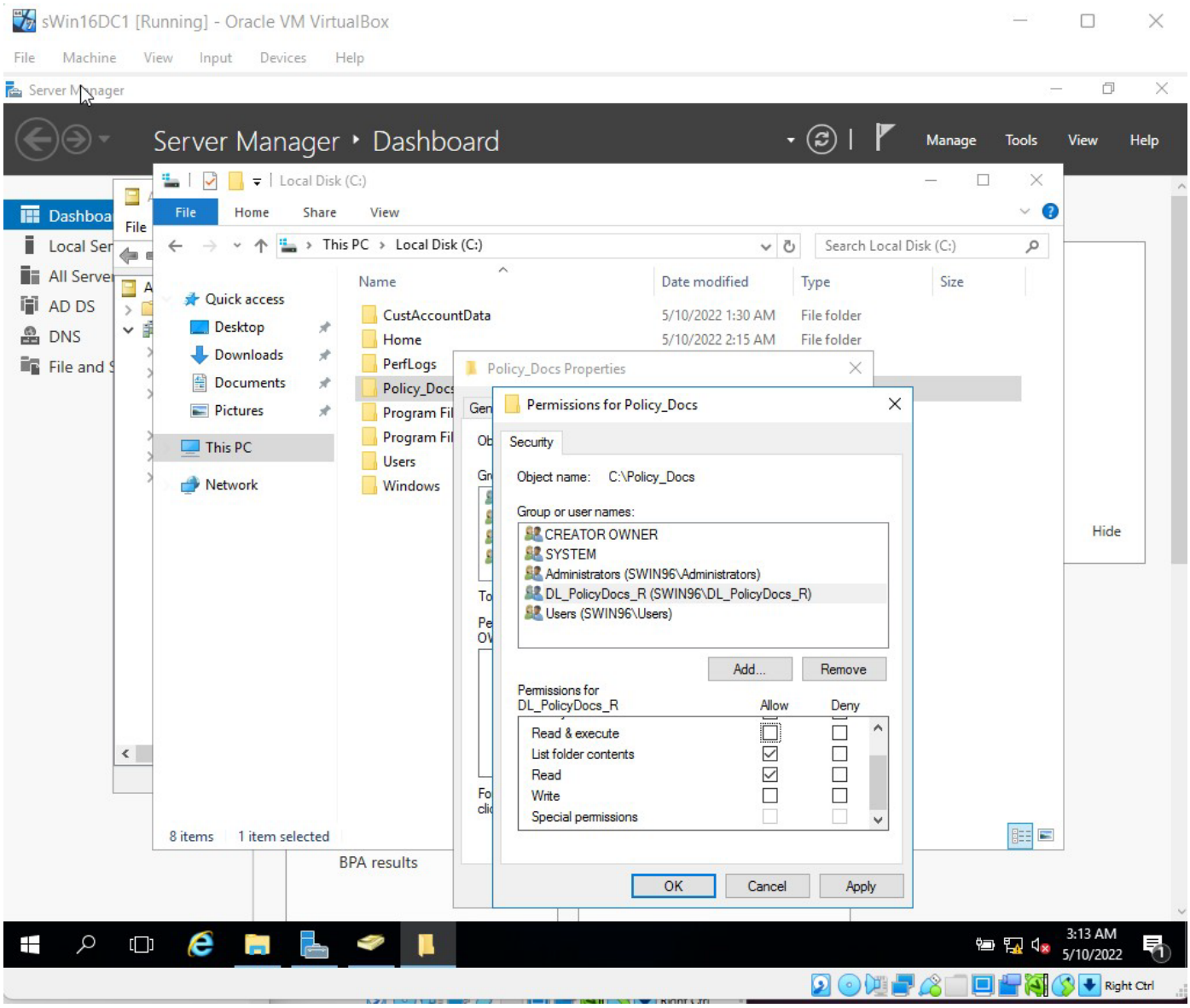
G_AccRec is a member of G_FinanceHwn.



G_FinanceHwn is a member of U_FinanceDept.

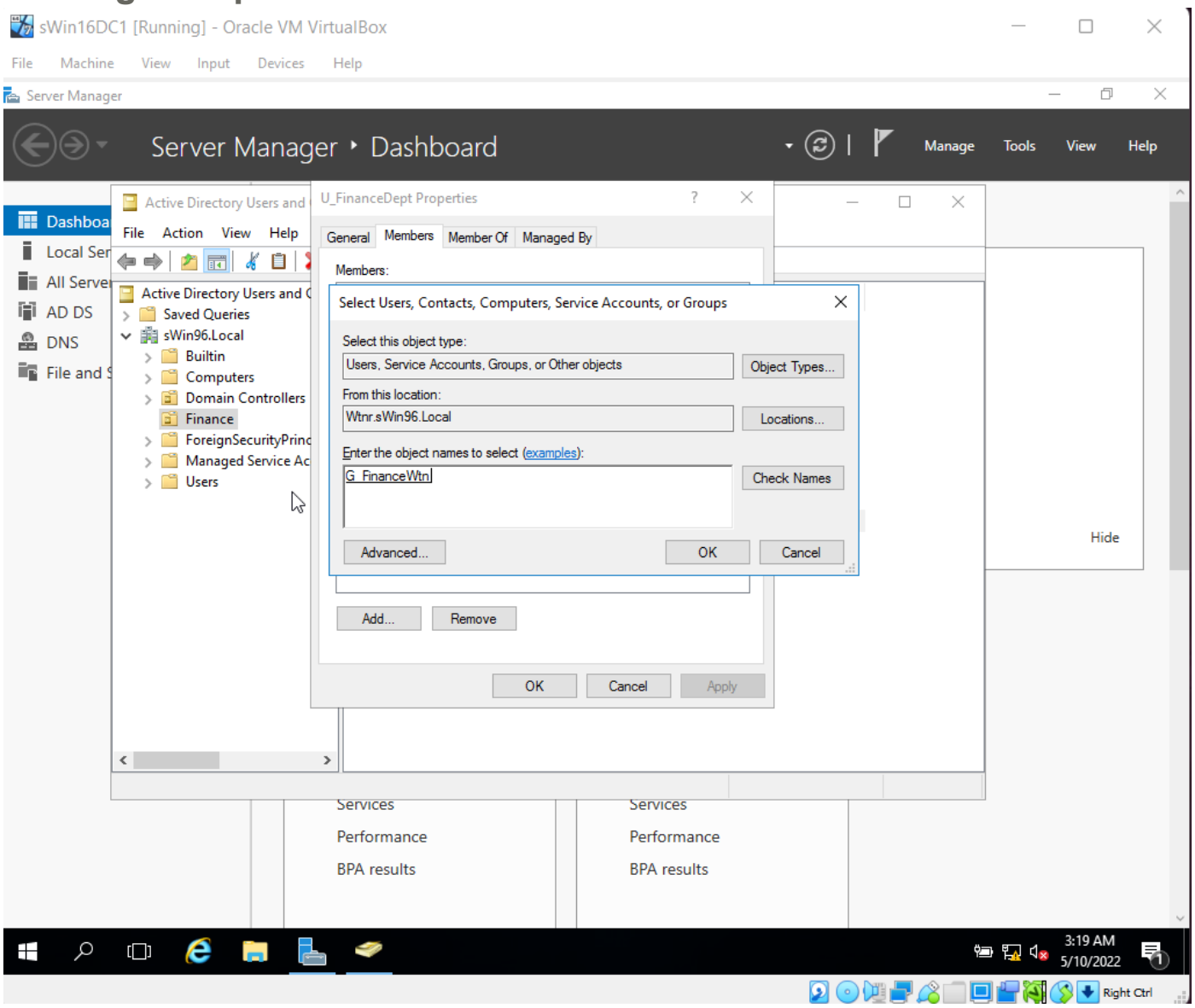


G_AccRec is a member of DL_CustAccData_M.



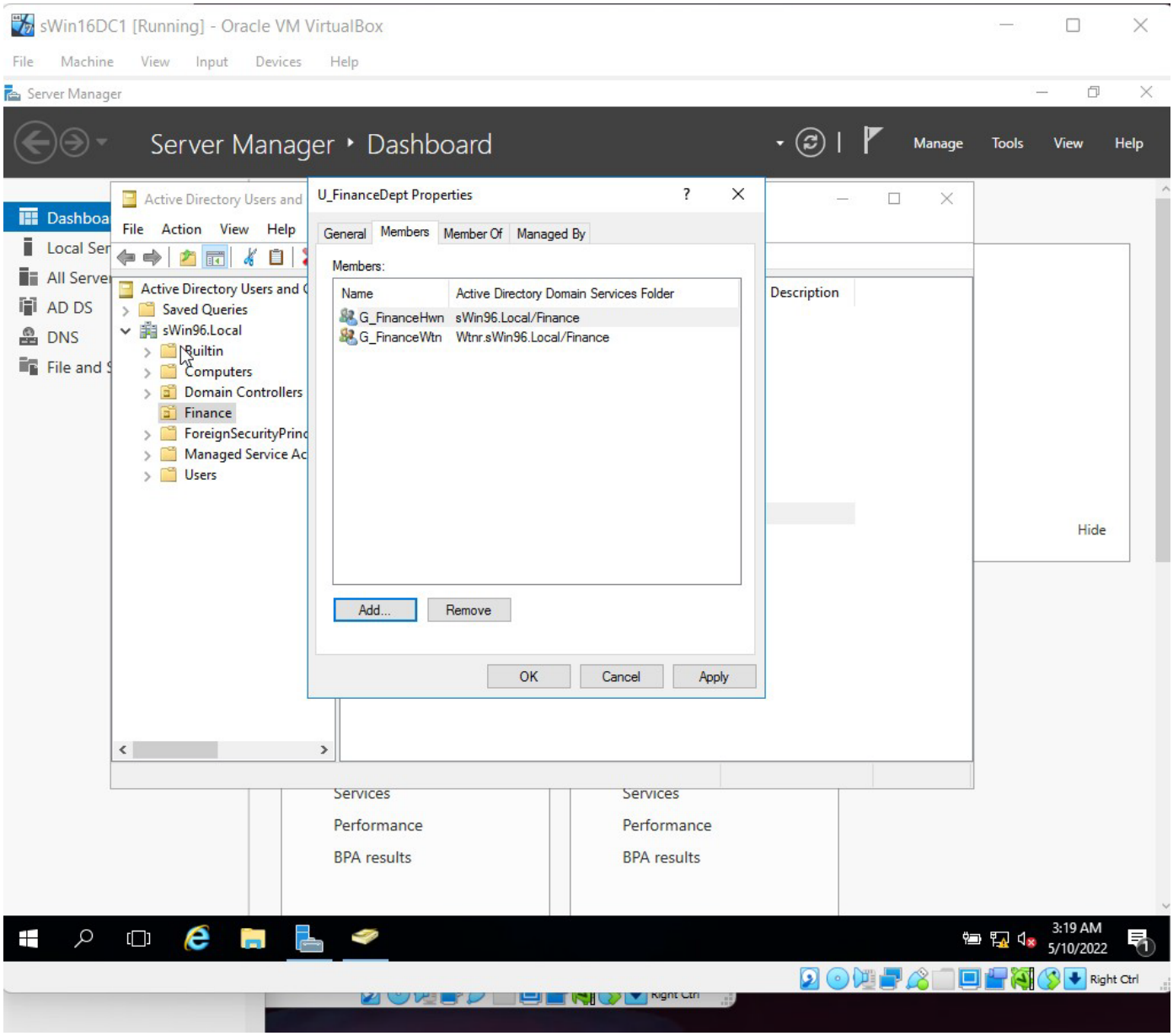
Assigning DL_PolicyDocs_R the permissions to Read and List folder contents to the PolDocs folder.

Nesting Groups Between Domains

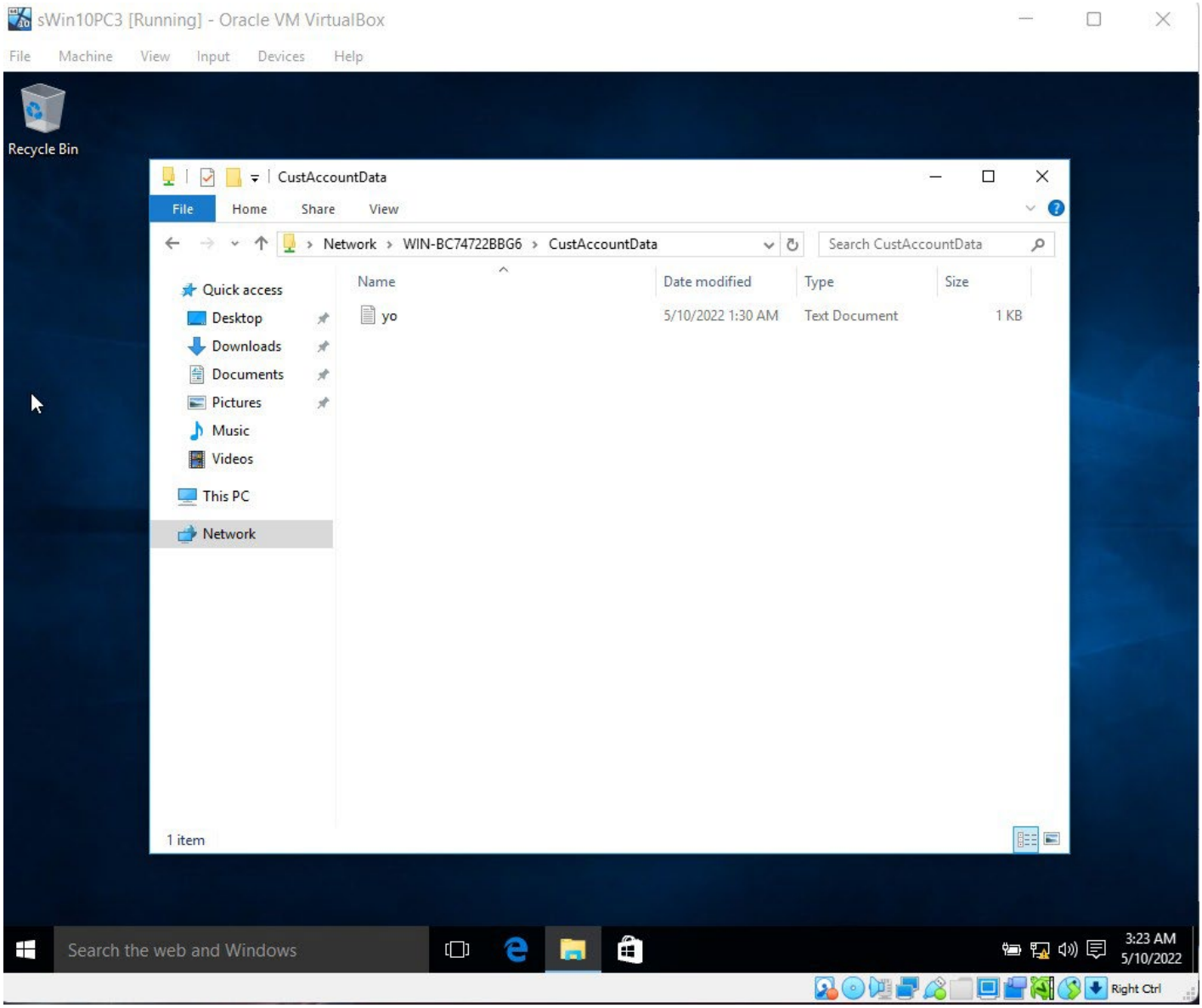


Nesting Groups between domains is done by launching the Main domain sWin96.Local Computer adding the child domain (Wtnr.sWin96.Local) in the Location tab of the targeted group, U_FinanceDept(main domains group) in this case and then adding G_FinanceWtn(child

domains group) in this case to the objects name field.



Testing the Access Permissions



Inorder to test everything, we logged into sWin10PC3 as Kim and entered the UNC for sWin16DC1 and it worked successfully.

TNE10005 Journal Lab (#8)

Khalid Yaseen Baig / ID #102763240

What I learned in this week's Lecture.

- Before we can manage a project, we must determine The Impact that the occurrence of this risk would have on the project, as well as the Likelihood or chance that this risk would occur over the project's lifetime. We prioritize the risks based on these characteristics, and then implement ways to reduce the likelihood of the risk occurring and the resulting damage.

- Disconnecting the computer from the network, disconnecting the machine from its power supply, and locking the computer in a safe are the Three Rules for Failsafe Security.

- Following the concept of least privilege, using distinct administrative accounts, and restricting administrator console sign-in are all best practices for strengthening security.

- Defense-in-depth is a tiered approach to security that reduces the chances of an attacker succeeding while also increasing the risk of detection.

- According to D-in-D Policy & Procedures, we must develop and explain policies on optimal security practices, as well as test our policies.

- D-in-D Physical security recommends that important gear be kept in secure rooms behind lock and key, backups be kept in a safe, and RFID door locks be used to track access.

- D-in-D Data states that ACLs and Encrypted File System (EFS) should be used.

- Windows Server Update Services (WSUS) is a server role that centralizes and handles updates. Before accepting modifications for deployment, administrators can test them. The updates are downloaded from Microsoft via the WSUS server. Updates are downloaded from the WSUS server by computers in the domain.

- There are are two types of user rights: privileges and logon rights. GPO may be used to configure them.

- We may configure security auditing to record security-related events according to our company's security standards and filter the Security Event Log in Event Viewer to locate particular security-related events when using security auditing to log security-related events.

- By applying a Group Policy Object (GPO) to the Organizational Unit (OU) holding the computer account, Group Policy may manage group membership for any group on a domain-joined computer, as well as for any group in AD DS, by applying a GPO to the Domain Controller's OU.

- Login to your account When users log on or attempt to log on, an event is logged. The information is saved in Event Viewer.

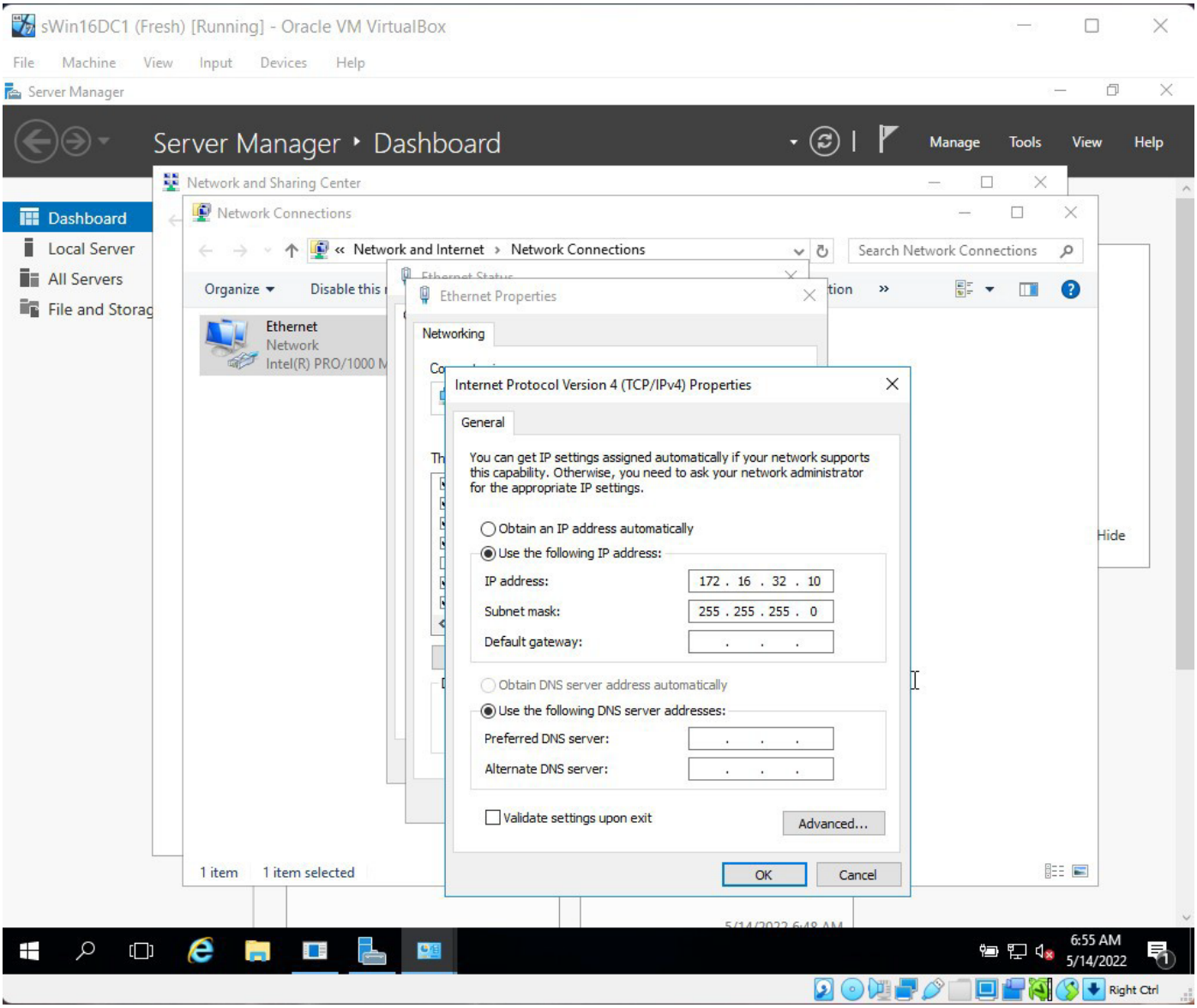
- There are three main stages to setting up Applocker. You may quickly limit all versions of a piece of software, or all applications from a certain business, with Applocker. Applocker may also be used in Audit mode, which allows you to see who is using the software.

- Windows Firewall is a host-based stateful firewall that permits or blocks network traffic based on its setup.

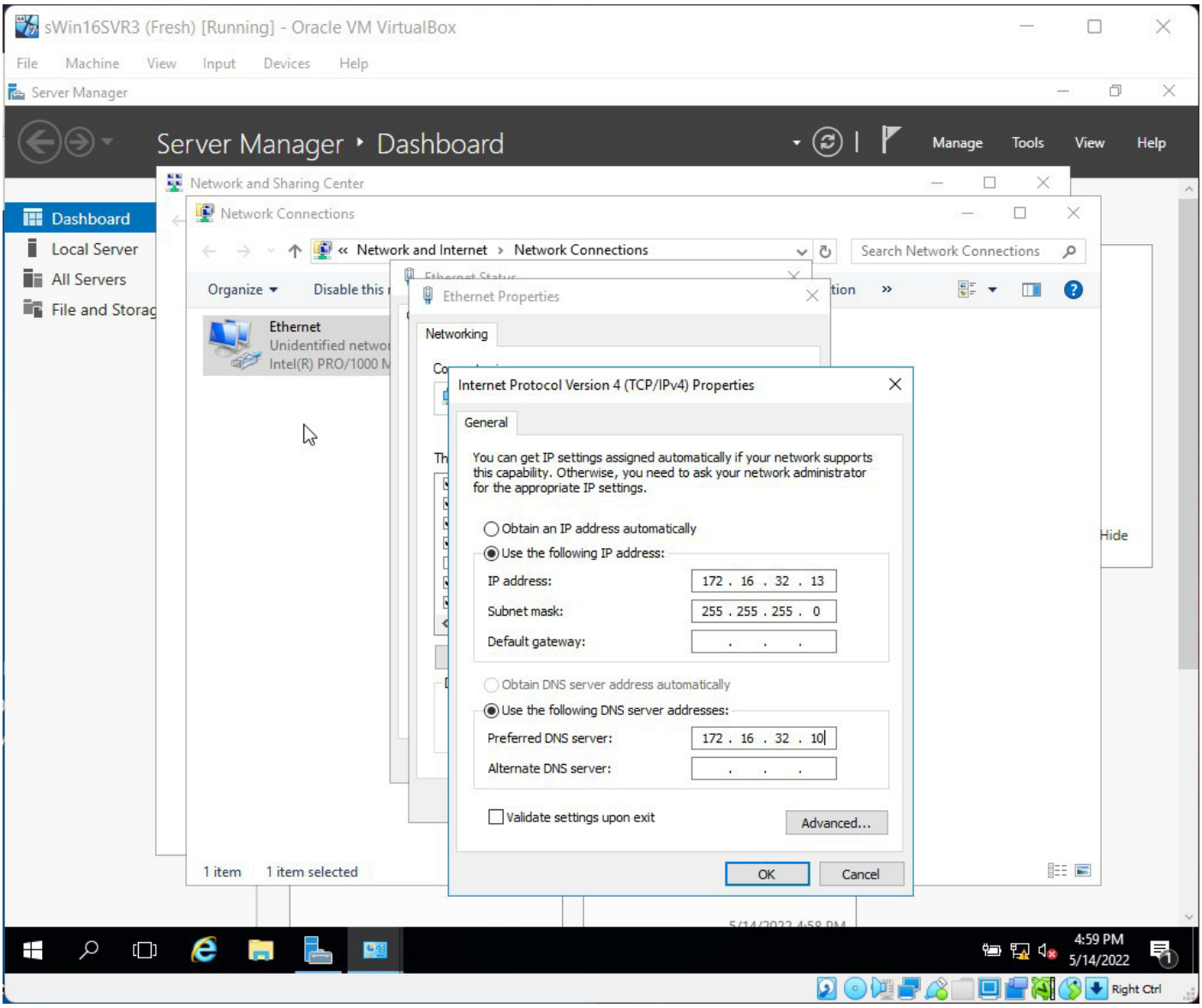
This week’s lab activities.

Screenshots of Important Steps Required for Lab with LAB Question/Answers.

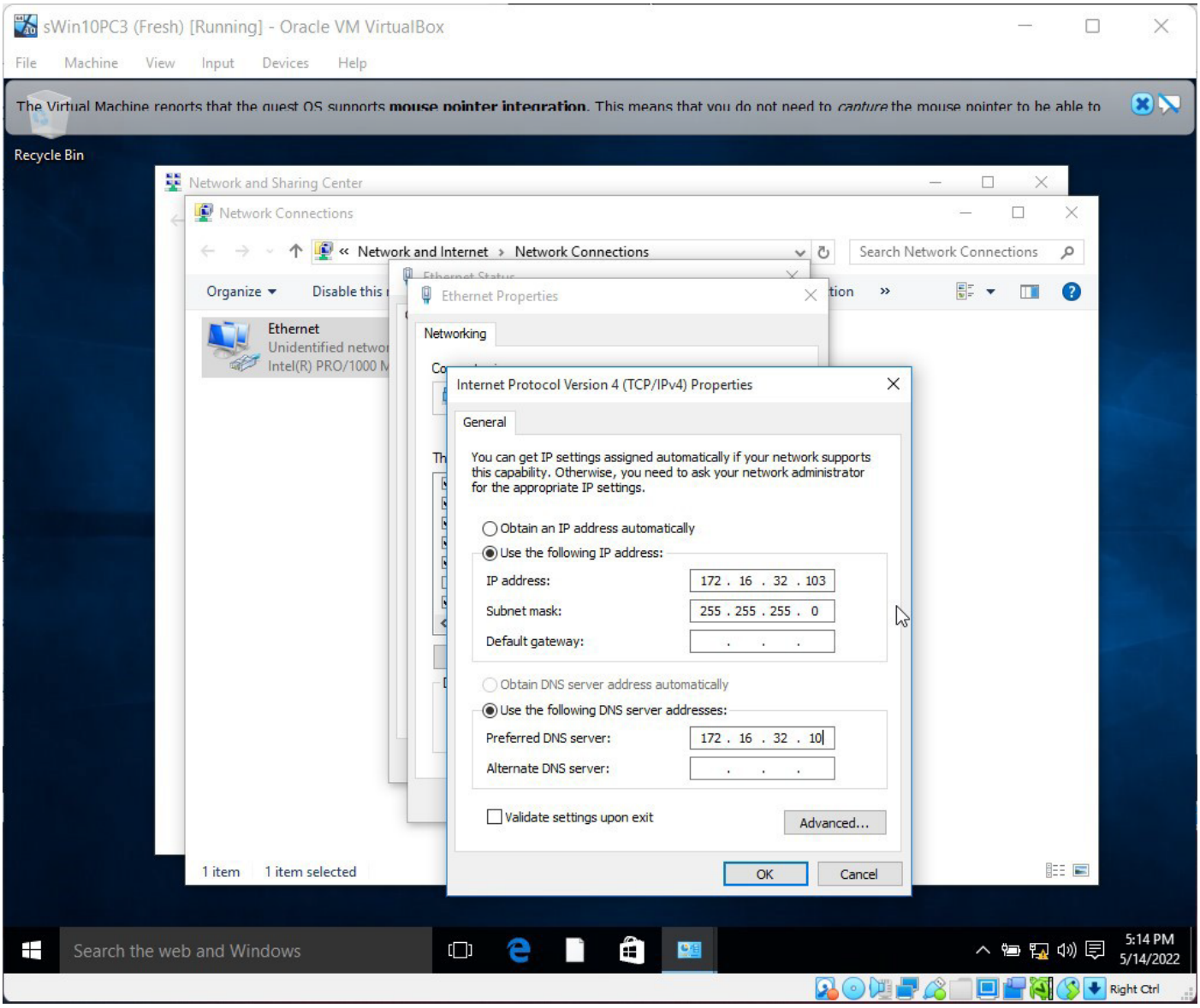
Preliminary settings



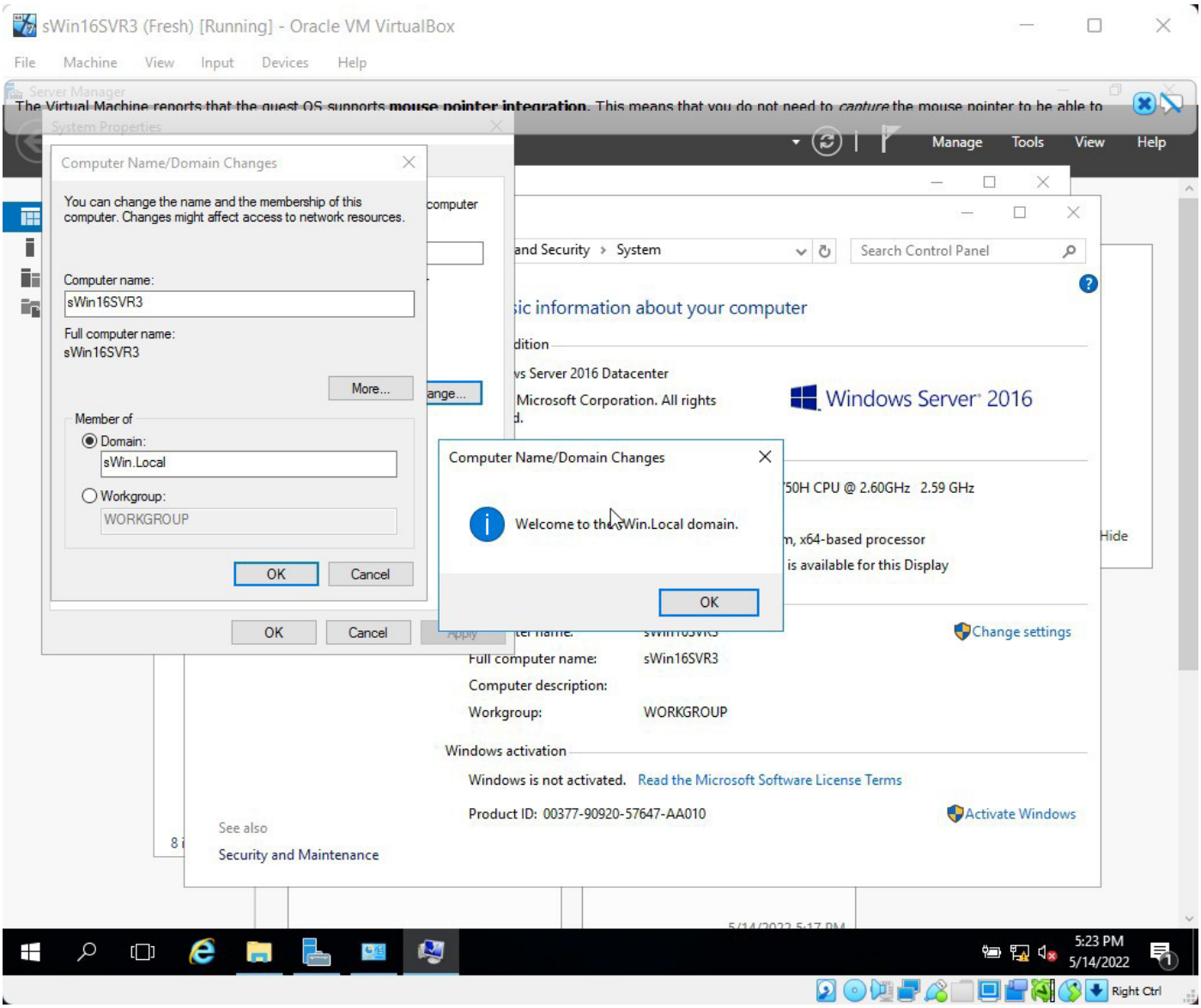
Preliminary settings for sWin16DC1 Virtual Machine required for lab



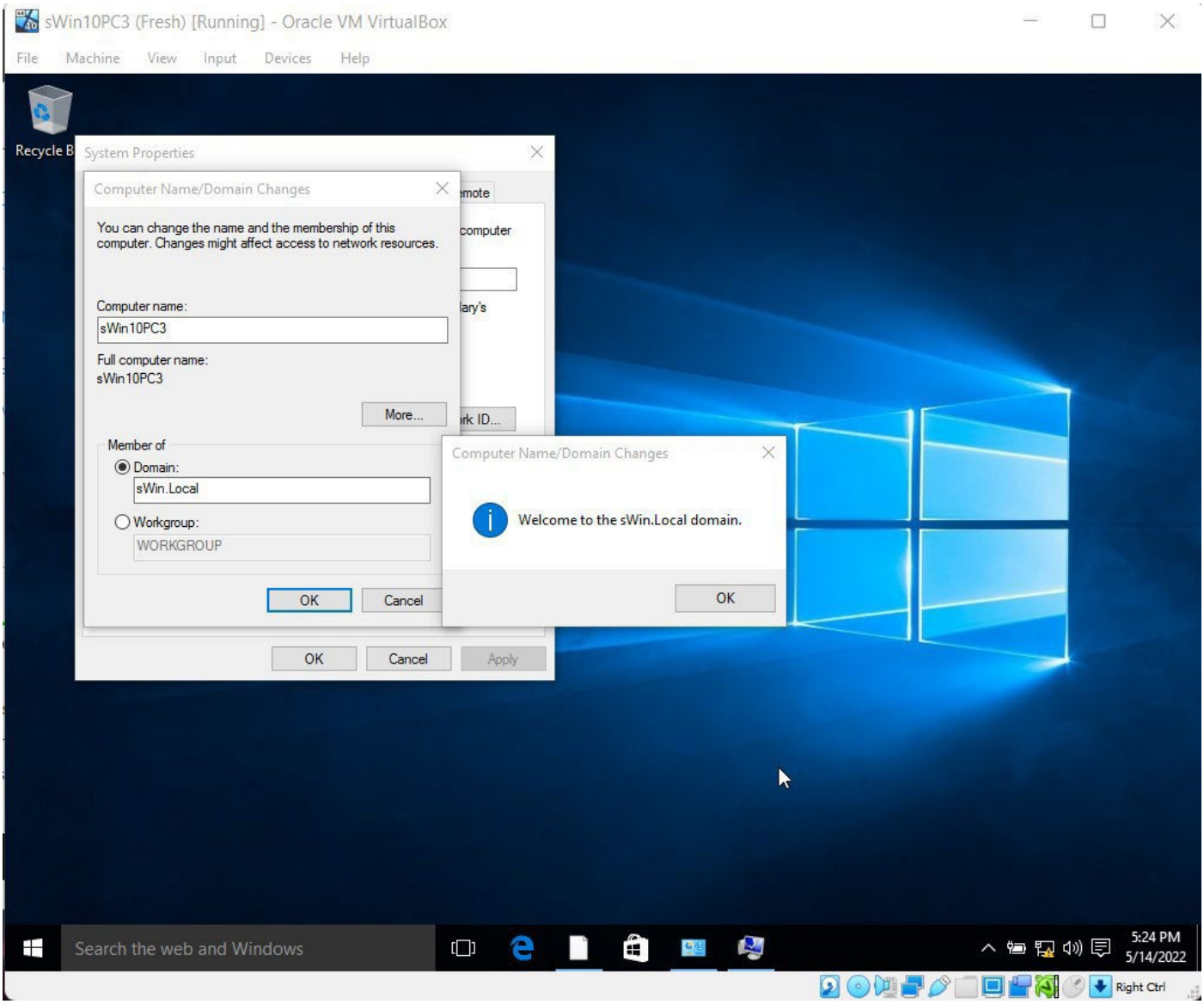
Preliminary settings for sWin16SVR3 Virtual Machine required for lab



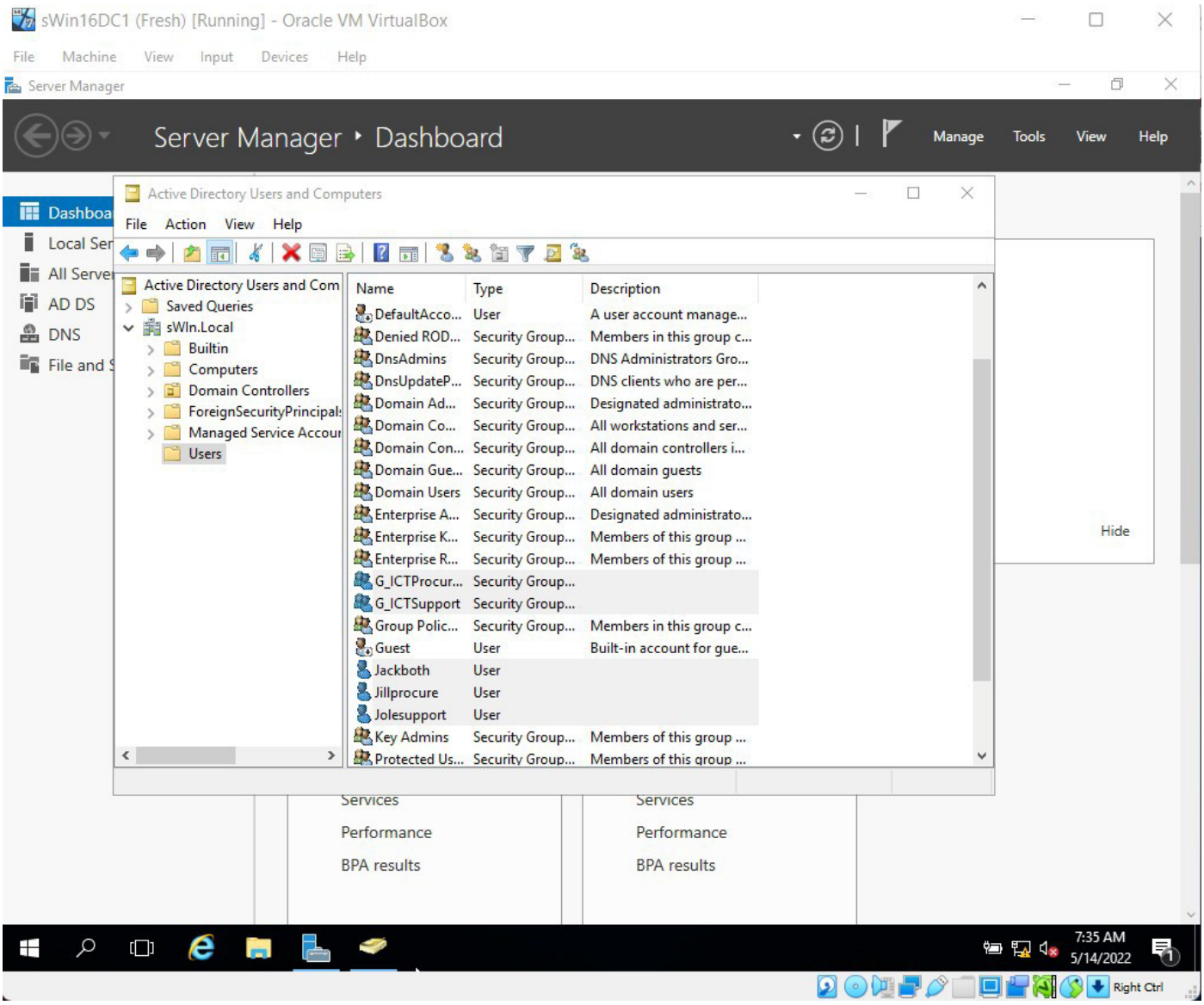
Preliminary settings for sWin10PC3 Virtual Machine required for lab.



Successfully Joining the sWin.Local Domain from the sWin16SVR3 Virtual Machine

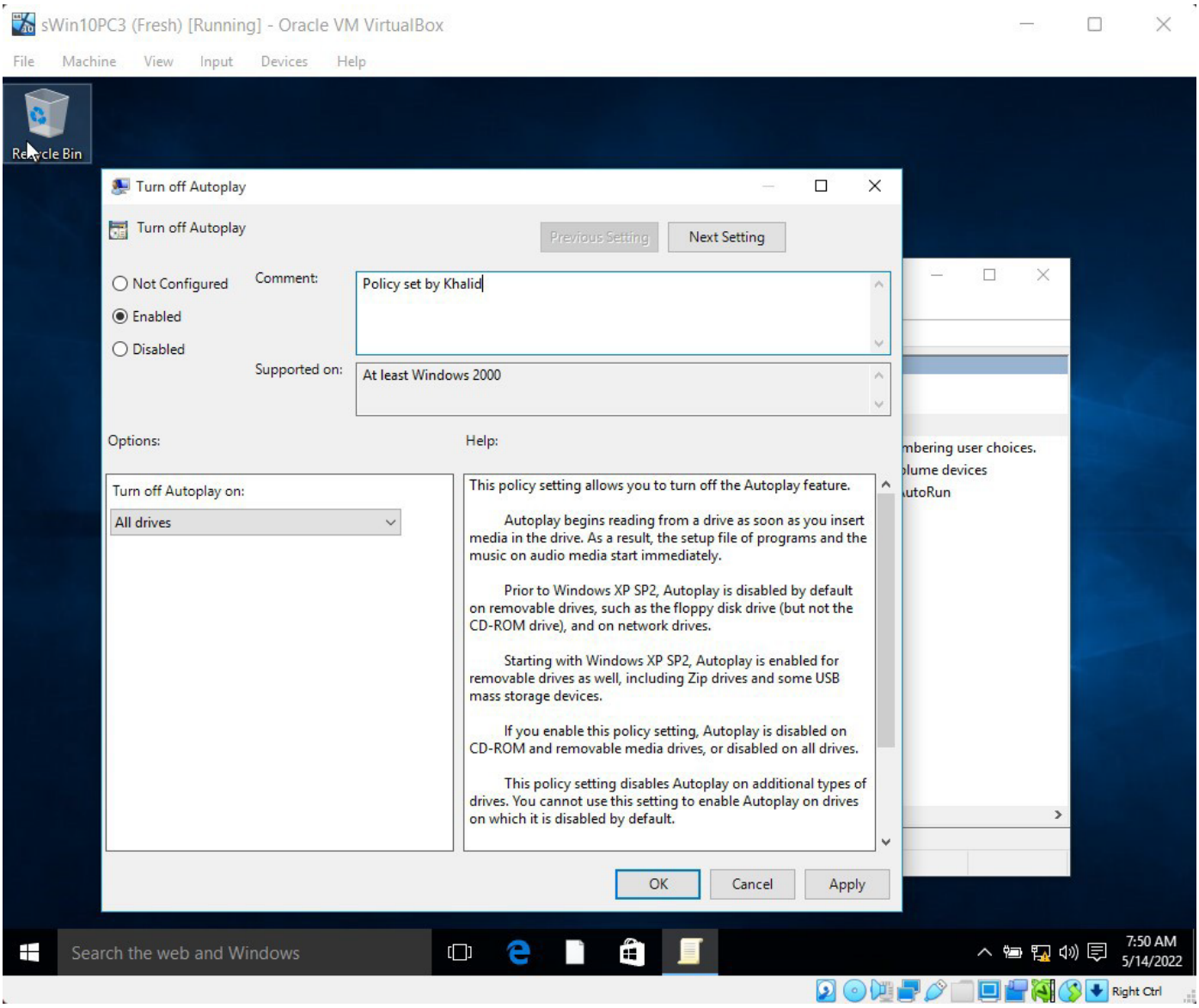


Successfully Joining the sWin.Local Domain from the sWin10PC3 Virtual Machine



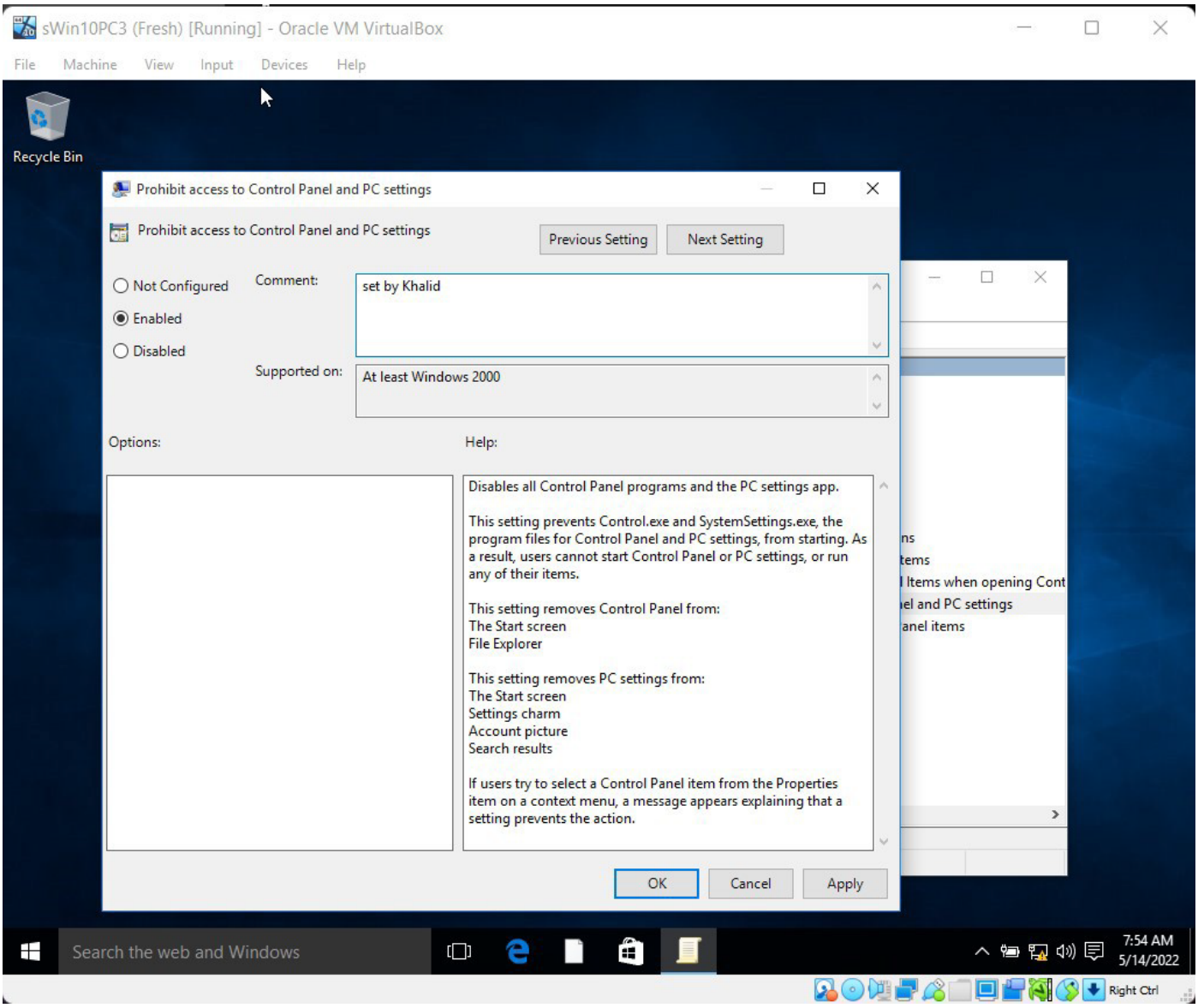
Successful creation of Three user accounts and two global groups in sWin.Local Domain and assigning Global groups to users.

Local Policies



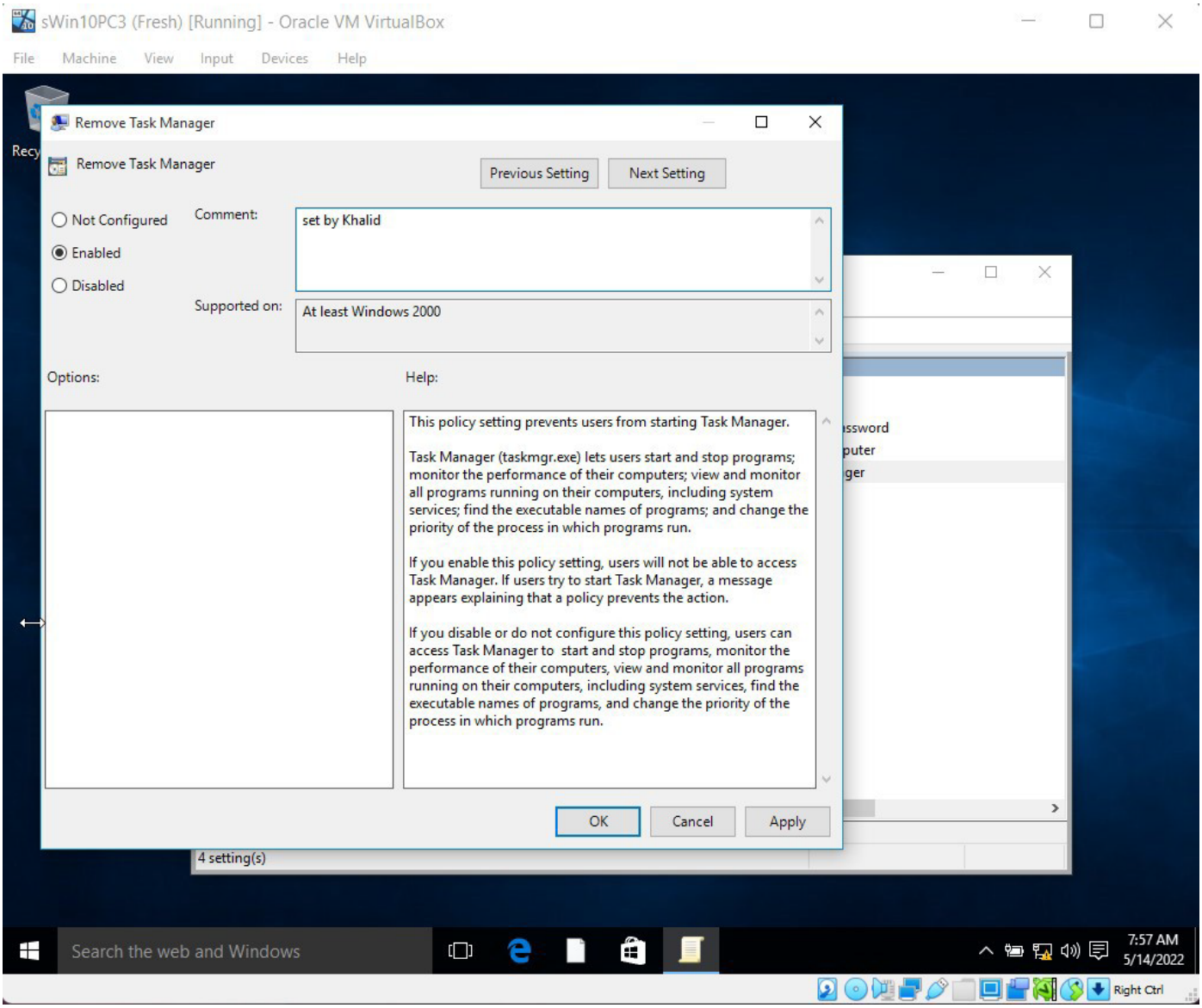
Turning off Autoplay Locally, so when a user inserts a CD or USB device, it will not automatically load the autorunscript.

Prohibiting access to the Control Panel



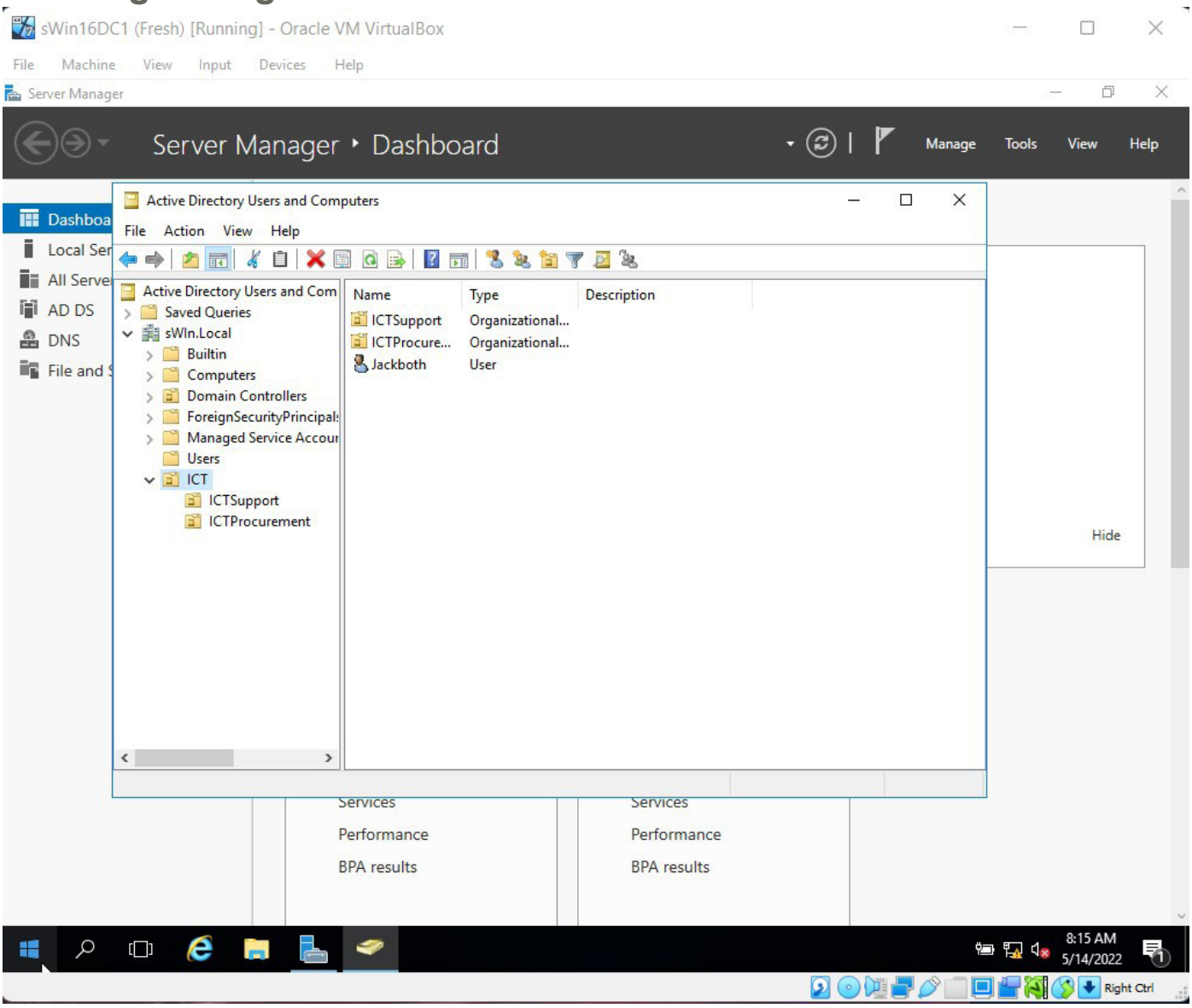
Restricting users from accessing Control Panel locally.

Ctrl+Alt+Del Options



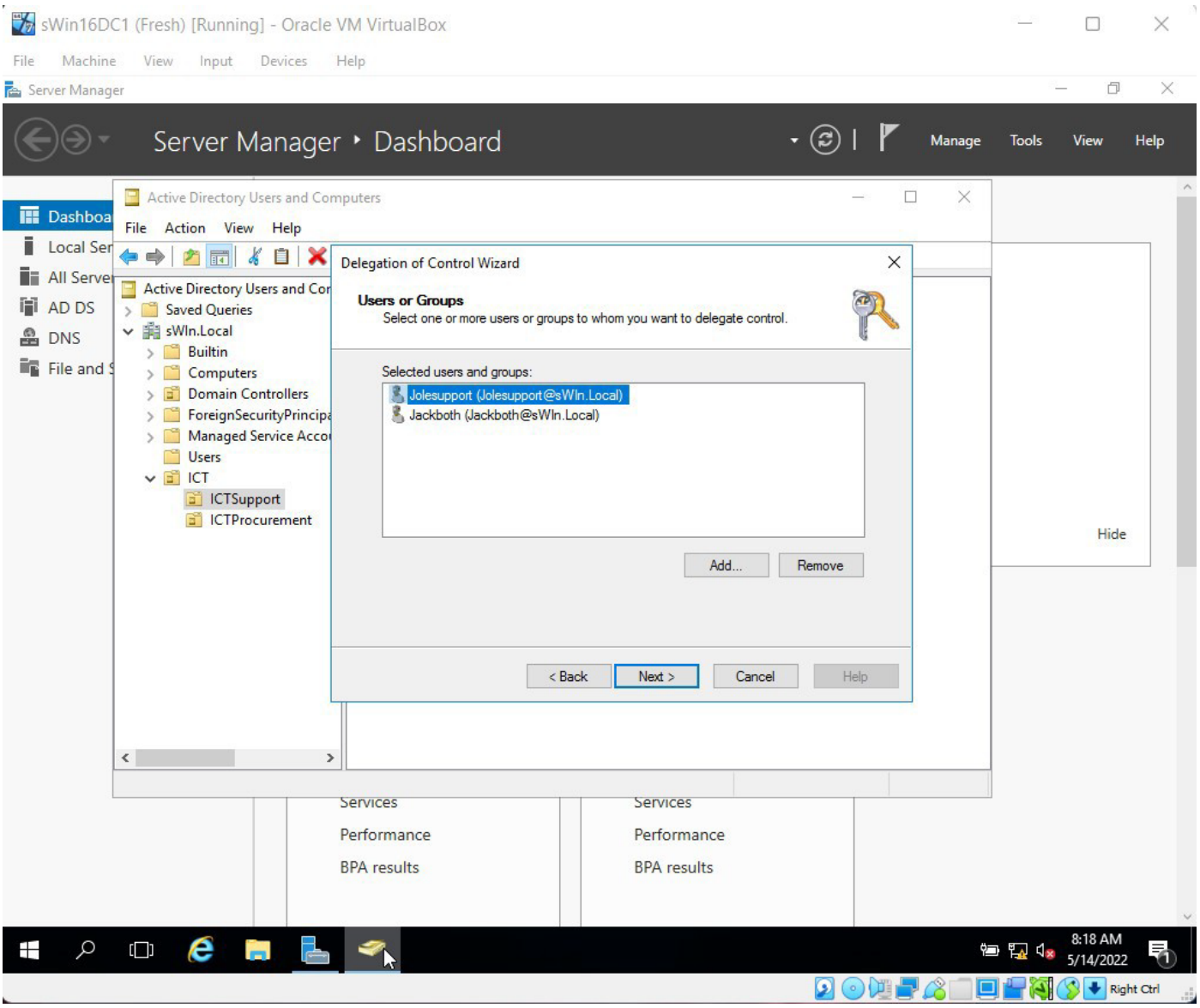
Restricting user from accessing Task Manager or lock this computer option from the Ctrl + Alt + Del Options

Creating an Organisational Unit Structure



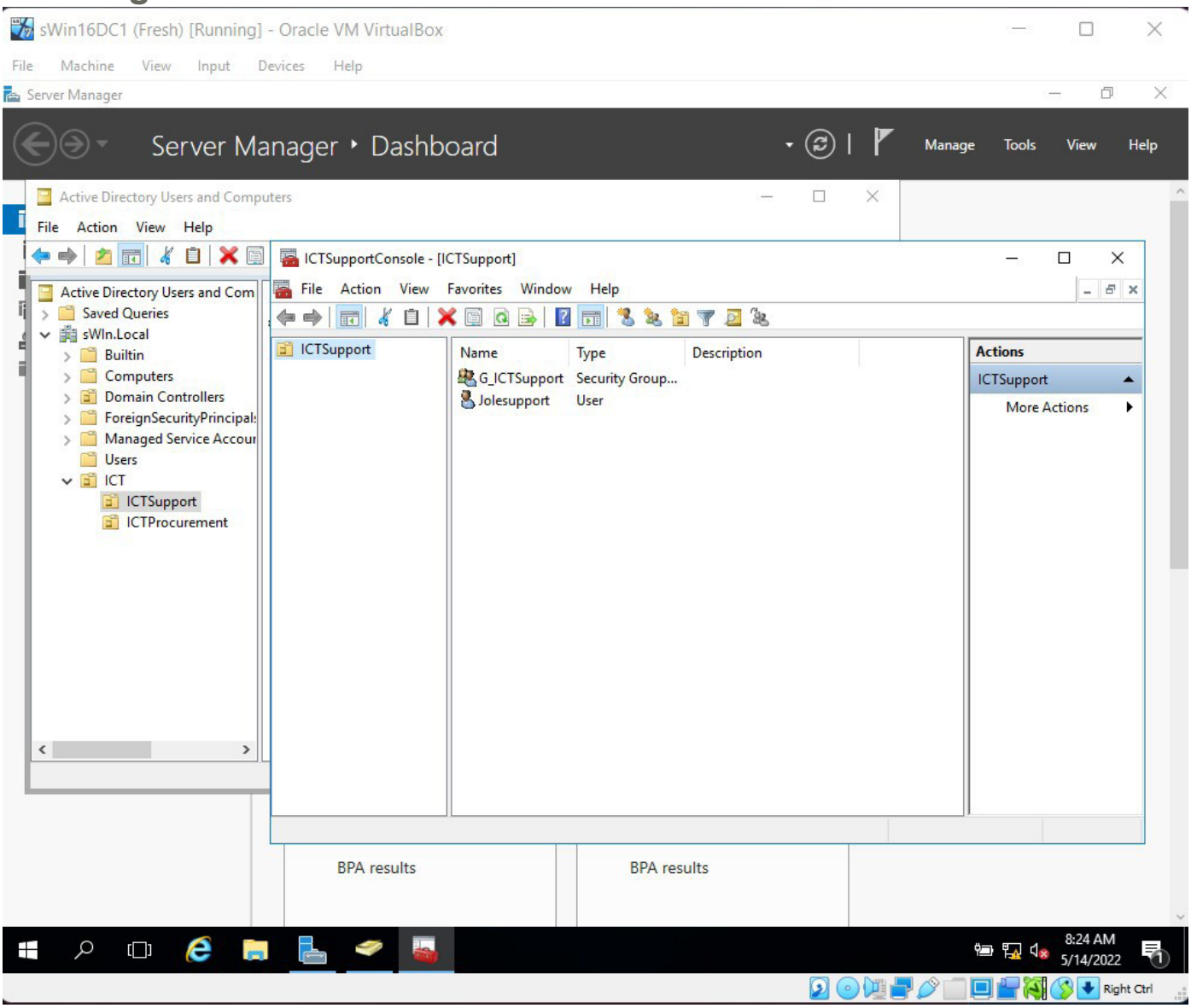
Creating an organizational unit Called ICT and creating another Two OUs under ICT named ICT Support and ICT Procurement and then moving Users and Global groups to them accordingly.

Delegating Control of an OU



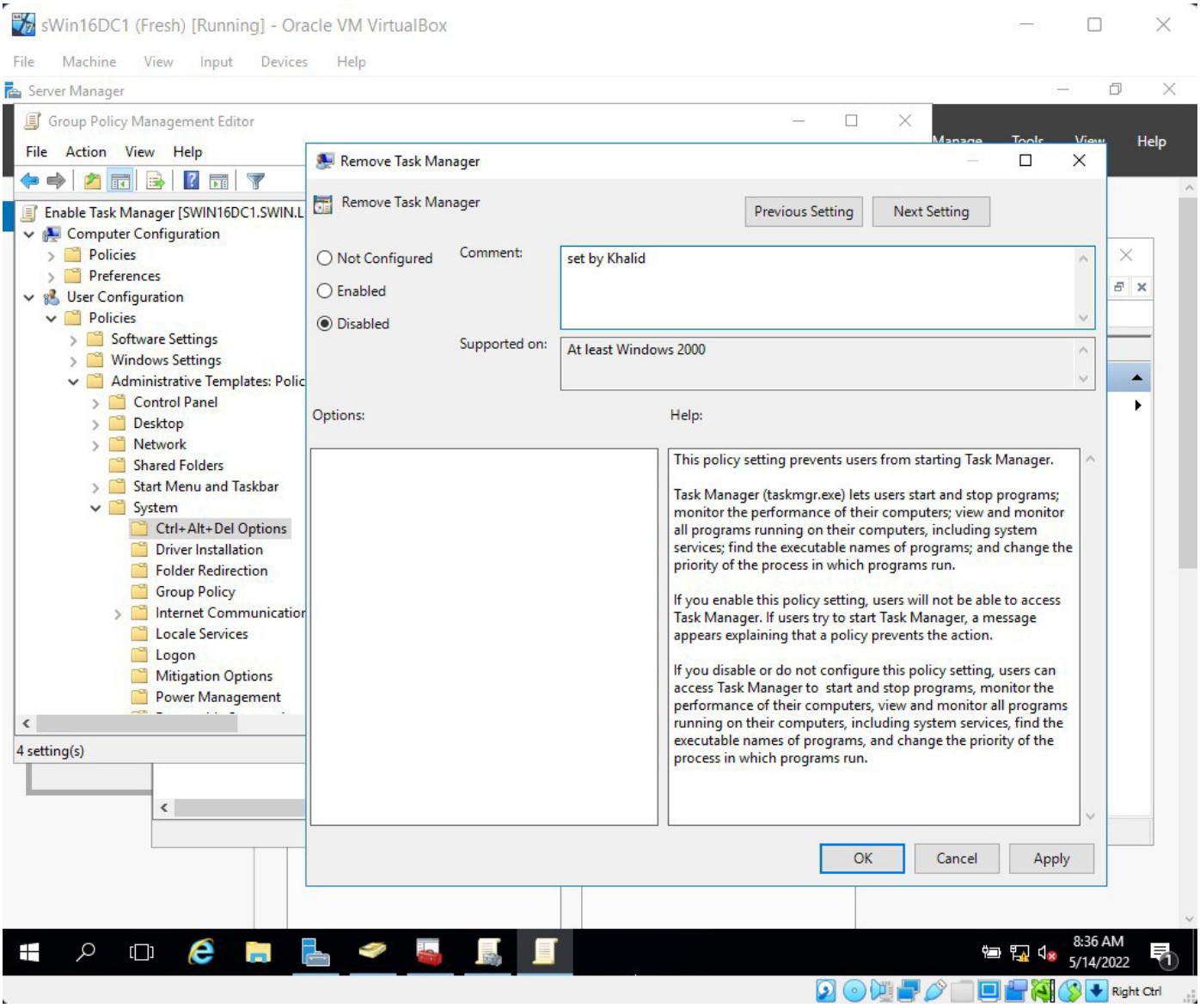
Delegating control of ICTSupport OU to required user so take over the management of the user account passwords and groups in the ICTSupport OU.

Creating a Custom Console



create a new custom console for these users with delegated permissions so that they only see the objects.

Creating a Group Policy Objects



Enabling users in the sWin.Local Domain to access the Task Manager.

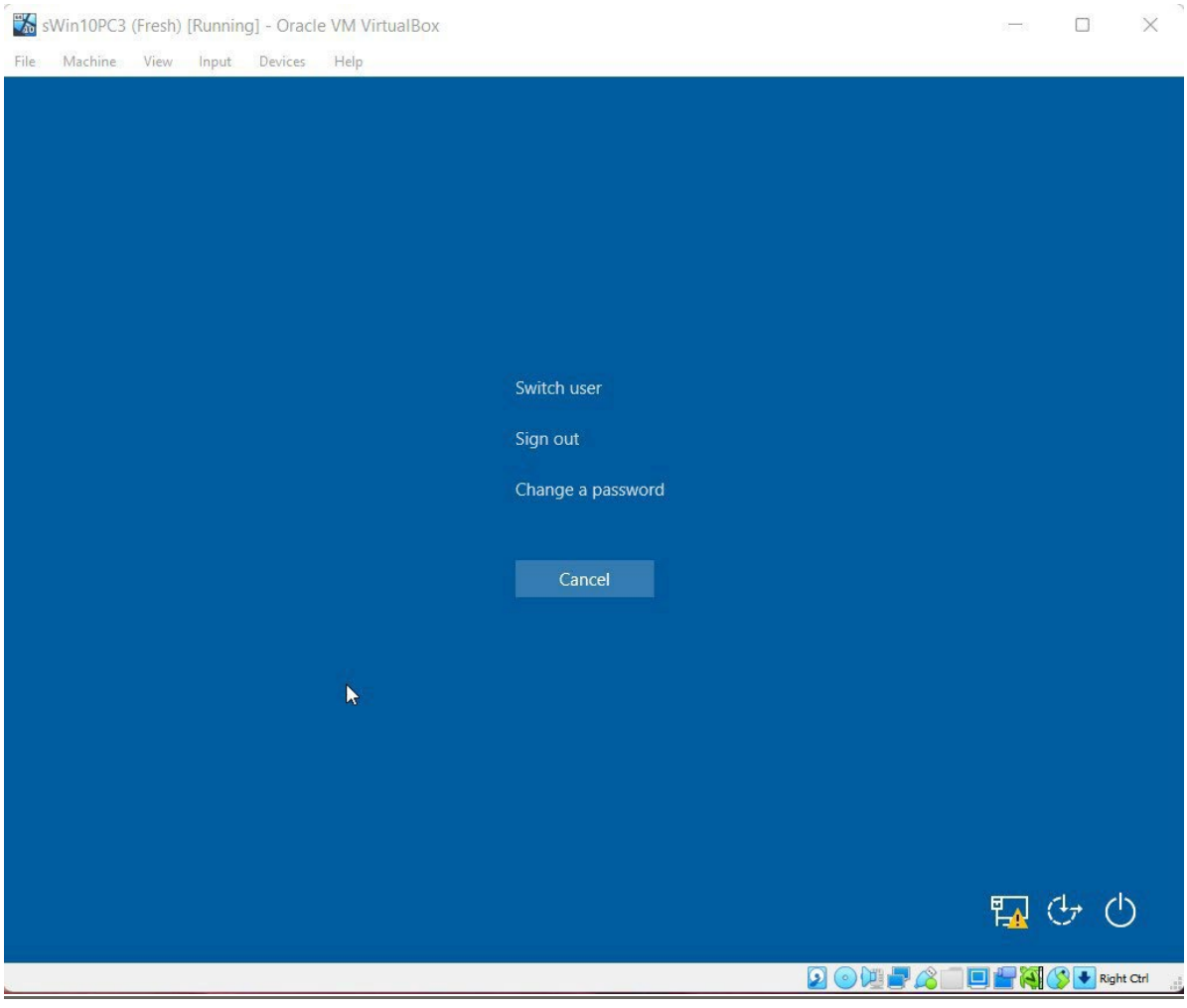
32. Drill down to the Ctrl+Alt+Del options and in the Remove Task Manager properties, click on the Disabled option button.

Notice that we now have a double negative. We have disabled the removing of the task manager. This means that the task manager should be available.

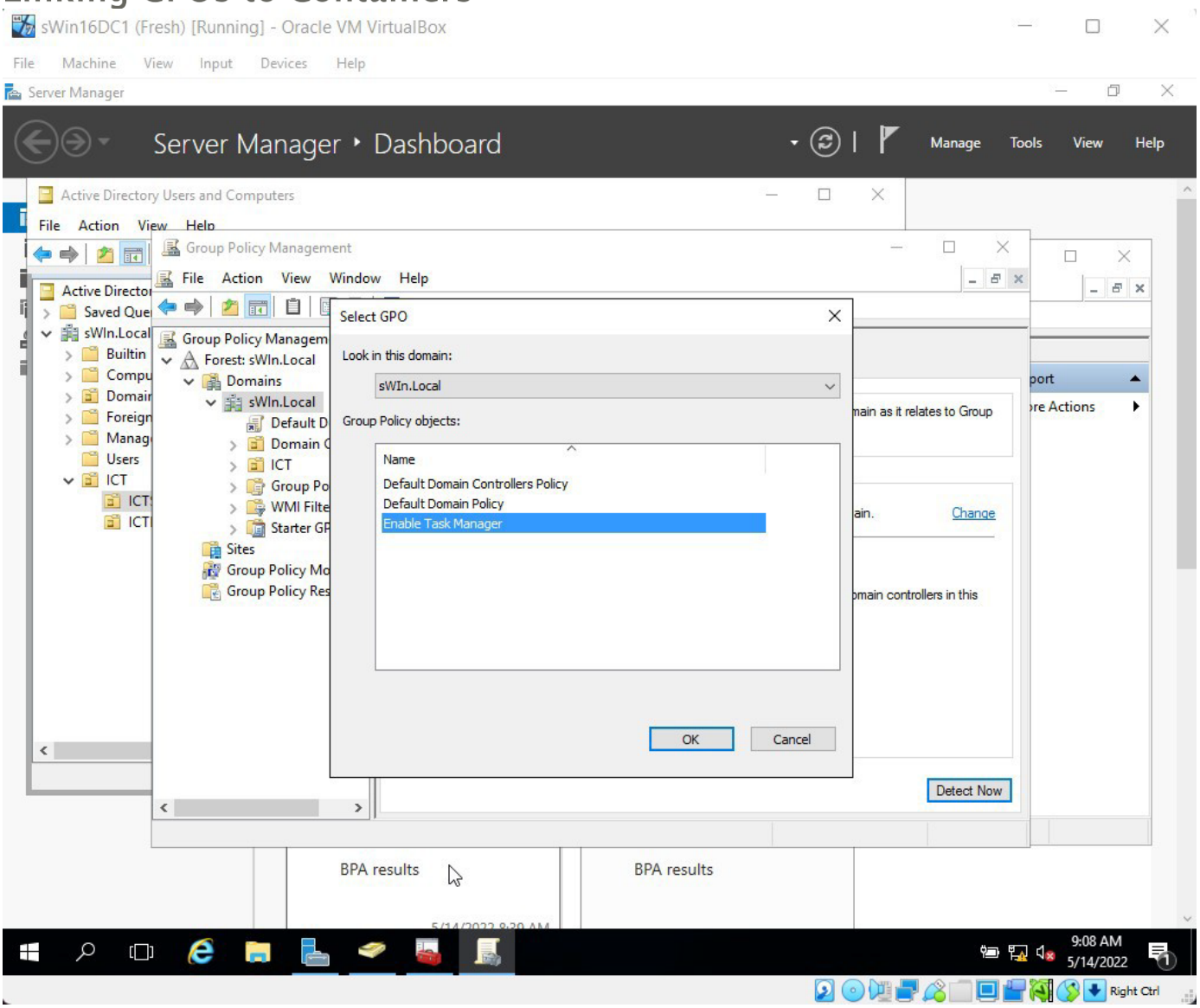
Predict what the result of this GPO will now be:

The Task Manager will be available

On sWin10PC3 verify if your prediction was correct. Was it? No



Linking GPOs to Containers

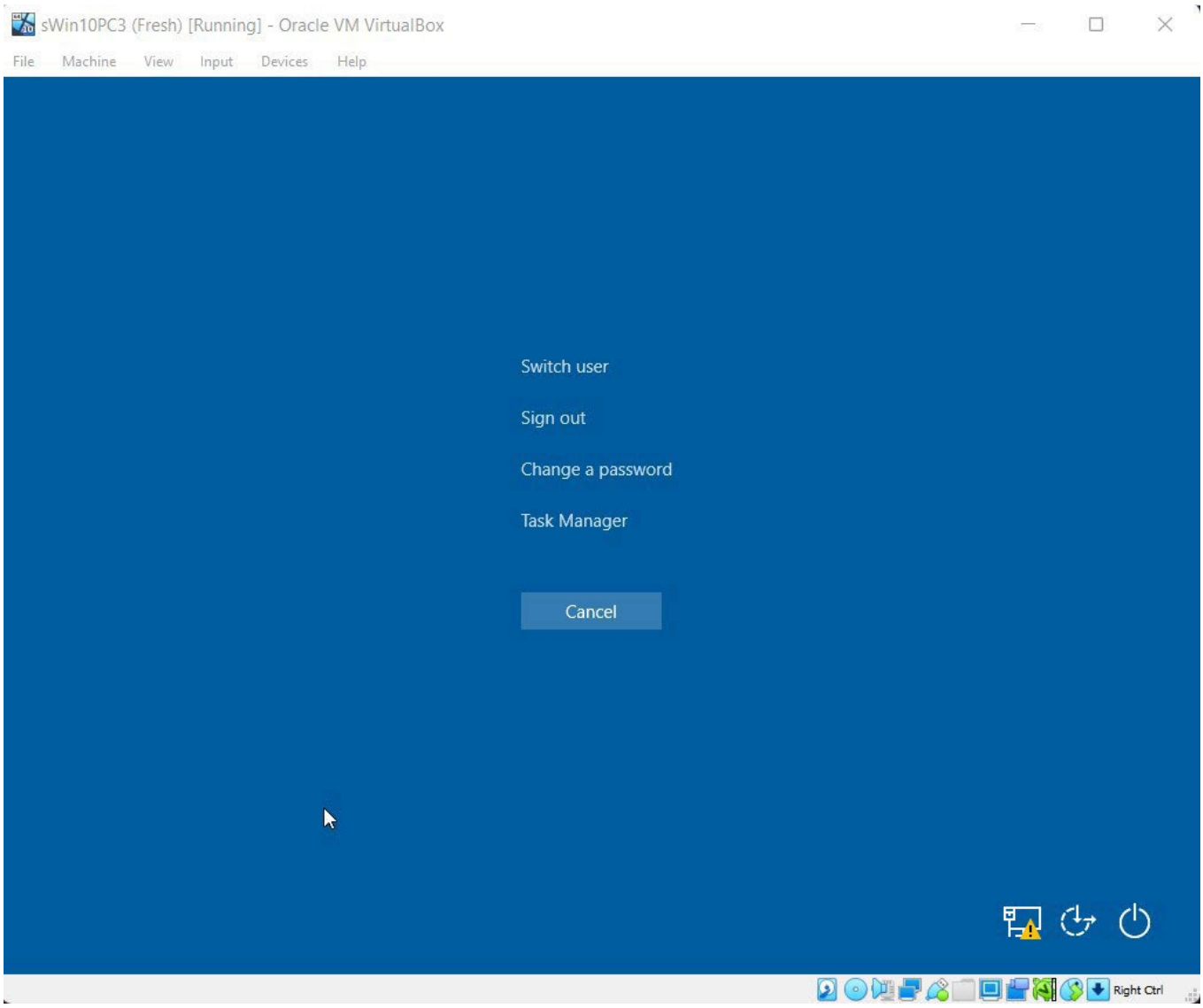


Linking the Enable Task Manager to the sWin.Local Domain

35. View your Ctrl+Alt+Del options on **sWin10PC3**

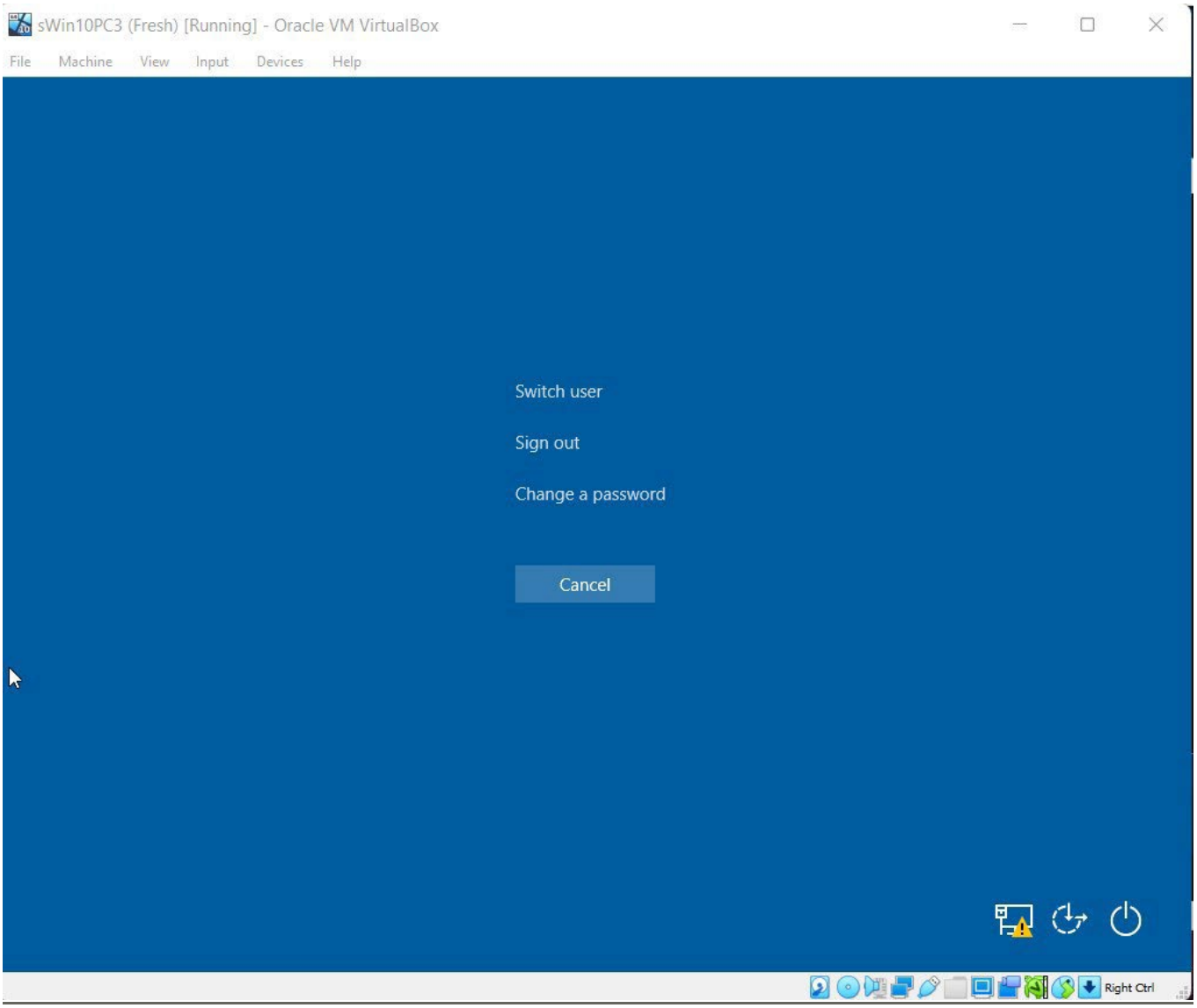
What is the setting? Task Manager is available

Which GPO is applied? Enable Task Manager


sWin10PC3 (Fresh) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Switch user
Sign out
Change a password
Task Manager
Cancel
Right Ctrl

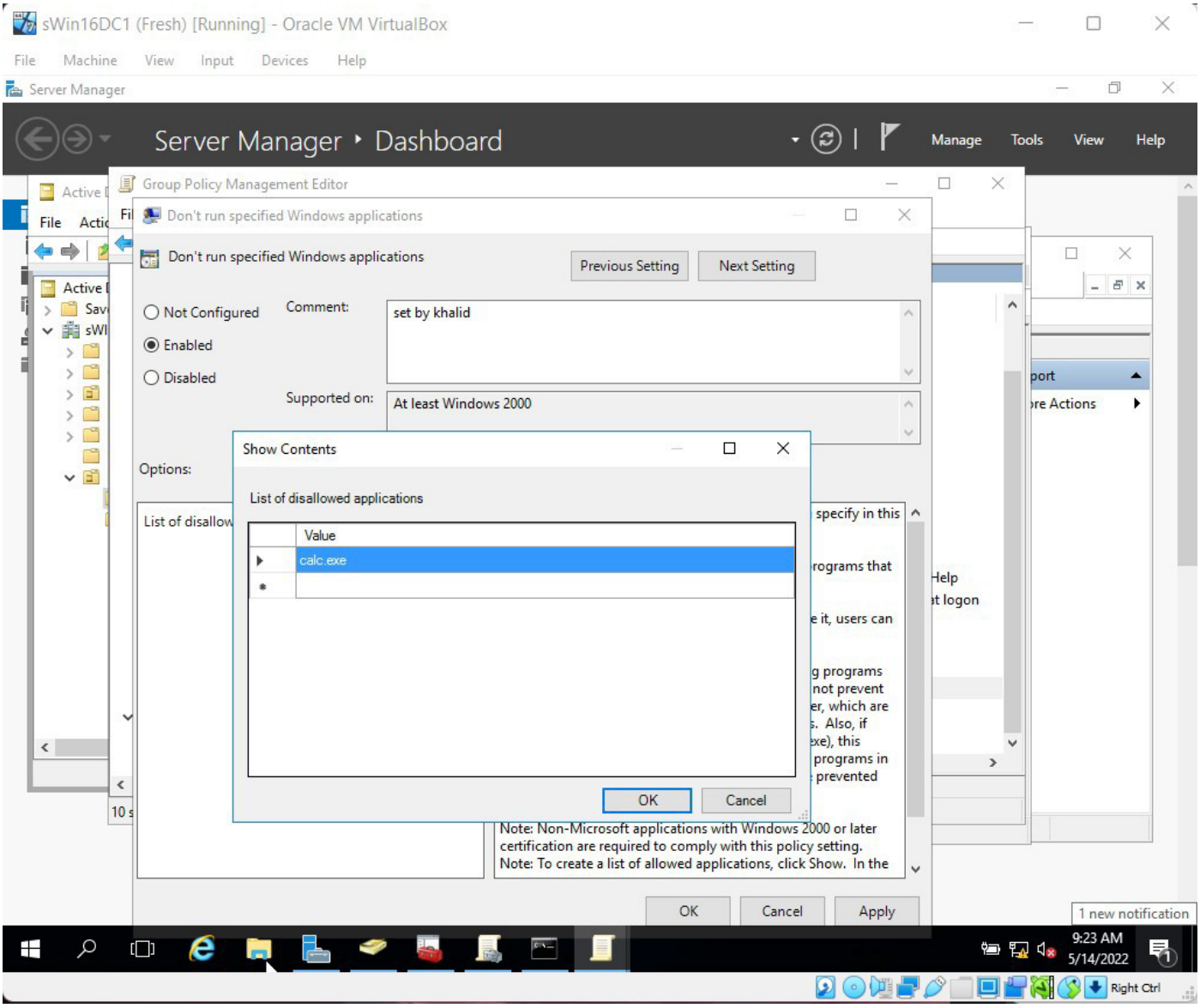
36. Back on **sWin16DC1**, create a GPO called **Remove Task Manager** and link it to the **ICTSupport** OU. This time, remembering the double negative, set the **Remove Task Manager** setting to **Enabled**.

Run **gpupdate /force** on both guest machines. Record the result of this change to sWin10PC3: Task Manager was no longer available



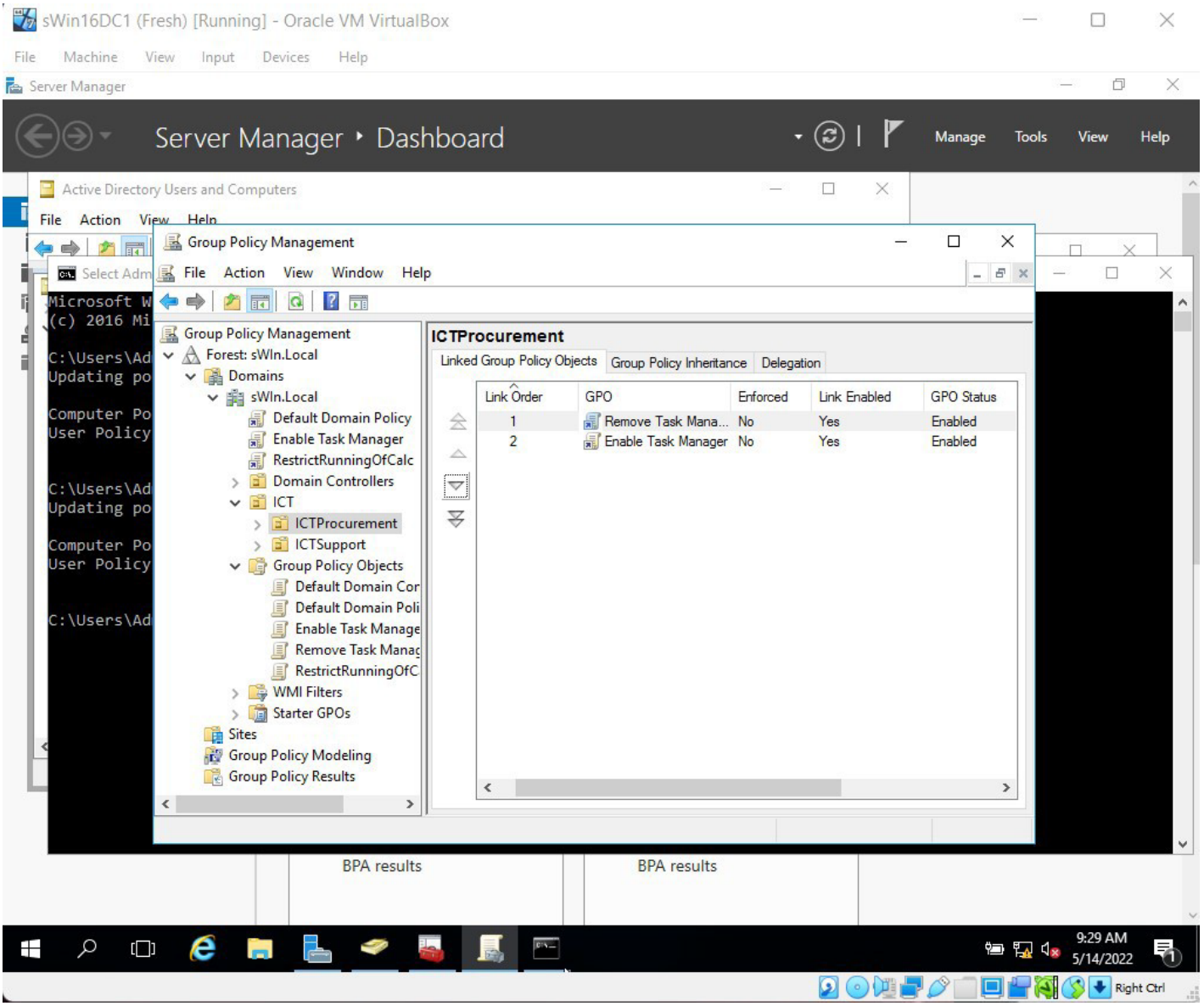
37. Now log on to **sWin10PC3** as the user account from **ICTSupport**. Explain any differences: Task Manager was no longer available

More GPO Settings



Restricting users in the sWin.Local Domain from accessing calc.exe.

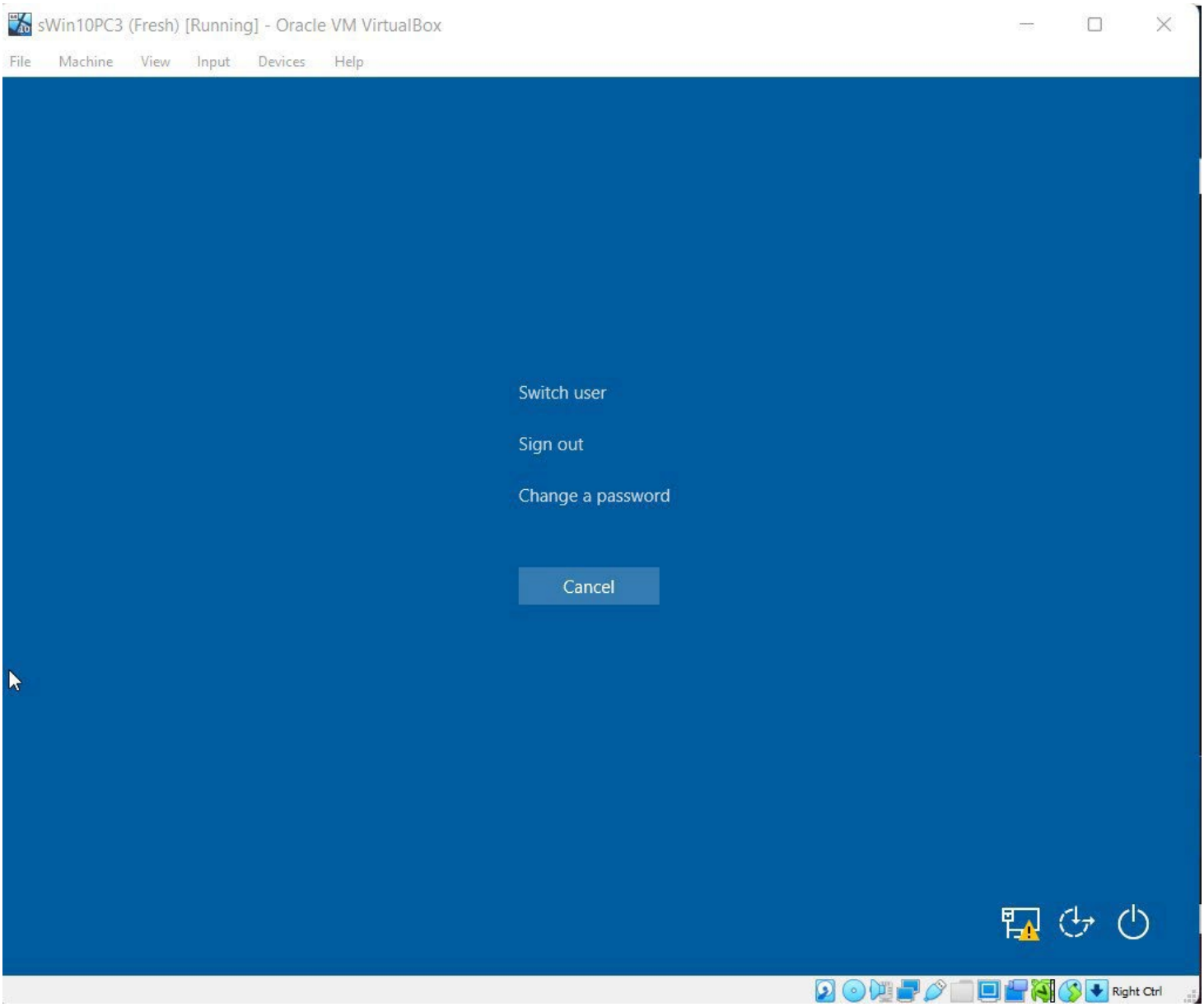
Linking Multiple GPOs



Linking Multiple GPOs to the ICTProcurement OU which have conflicting settings, in such case the first setting will have precedence.

44. On sWin10PC3, log in as the user account located in the ICTProcurement OU

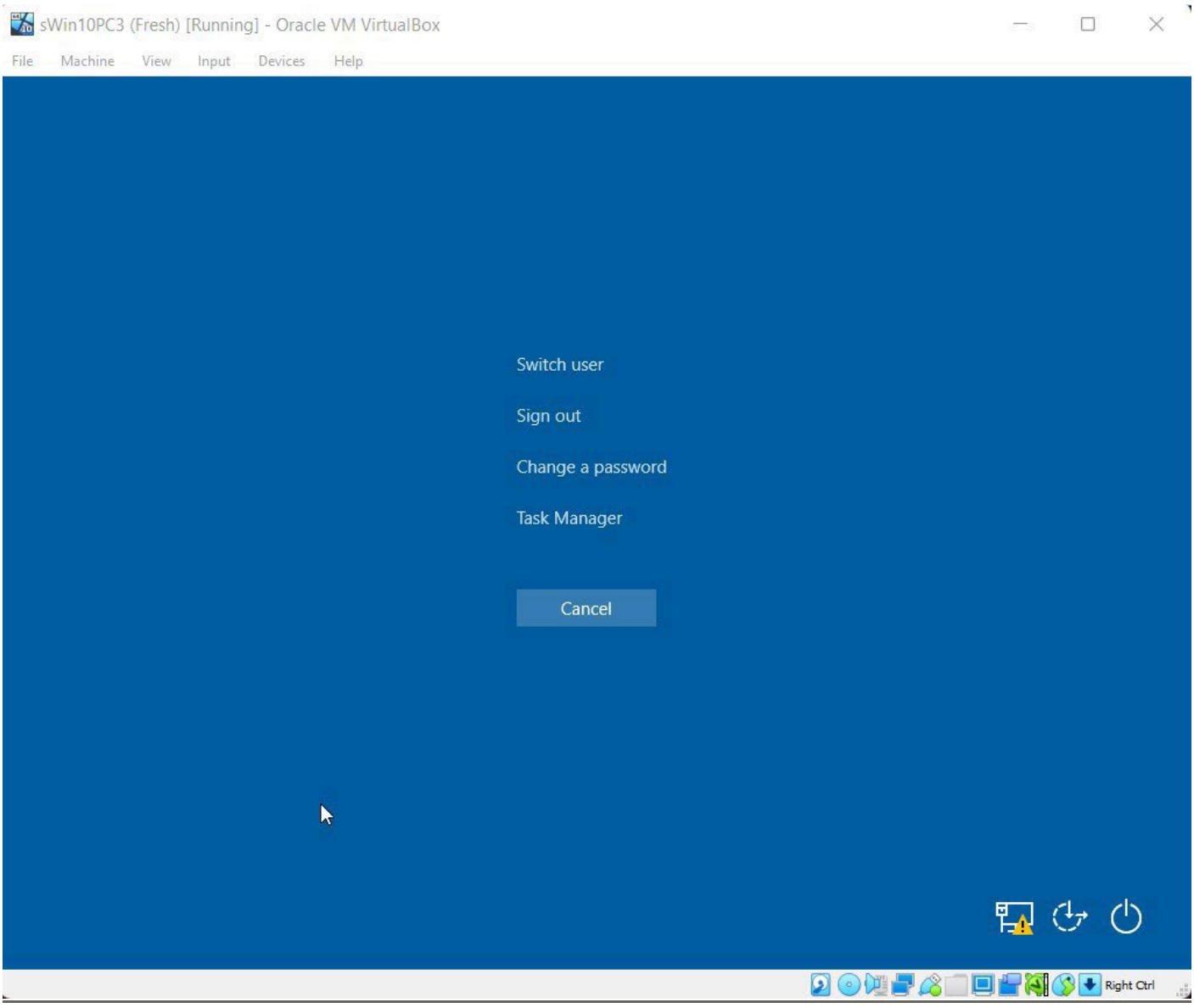
Which GPO is being applied? Remove Task Manager



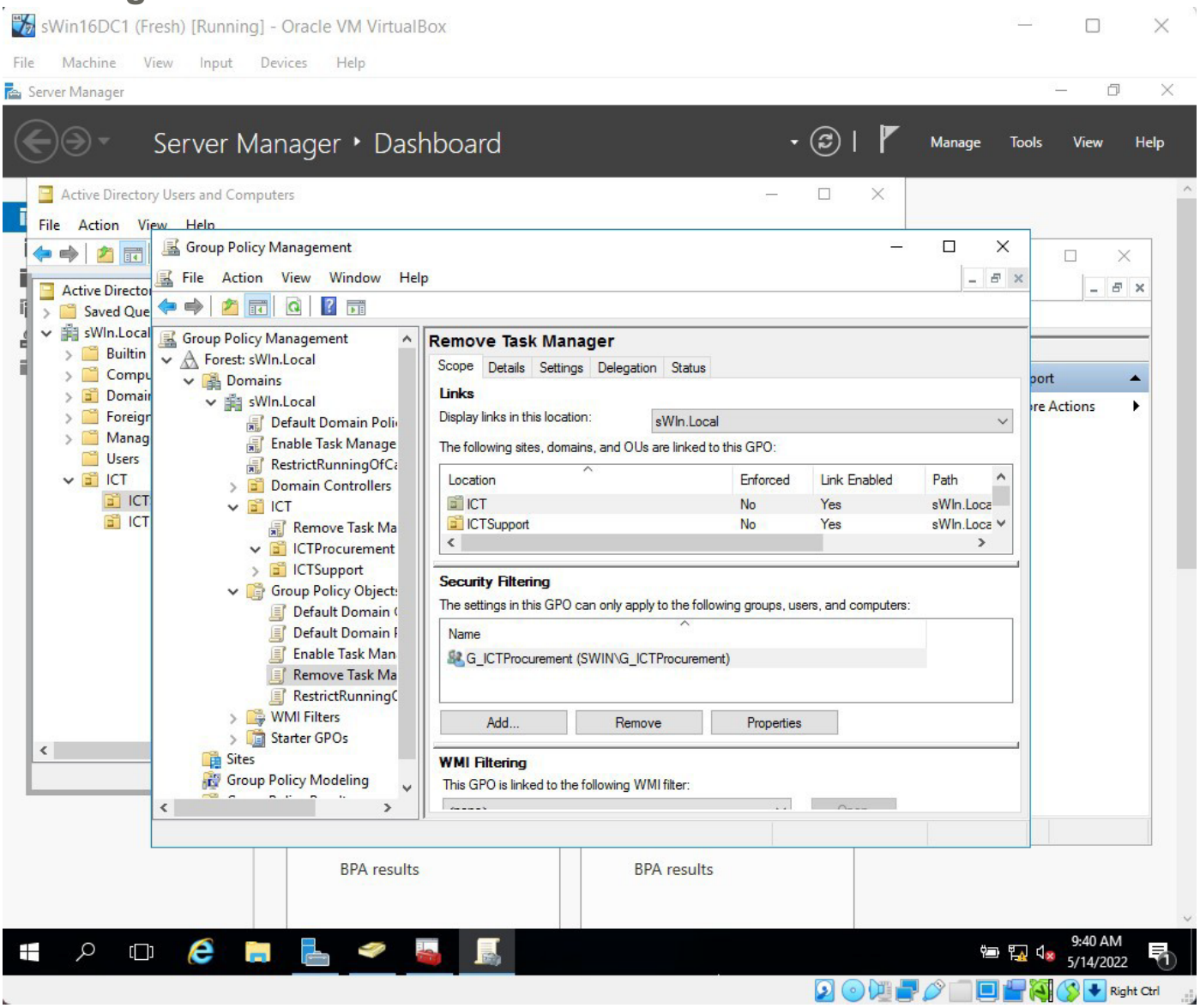
45. Back in GPMC at the ICTProcurement OU, observe thelink order of the Remove Task Manager and Enable Task Manger GPOs.

Change the order of the GPOs so that Enable Task Manager is at position 1. Do this by selection the Enable Task Manager GPO and clicking on the arrow.

46. Test sWin10PC3, which GPO setting has been applied? Enable Task Manager

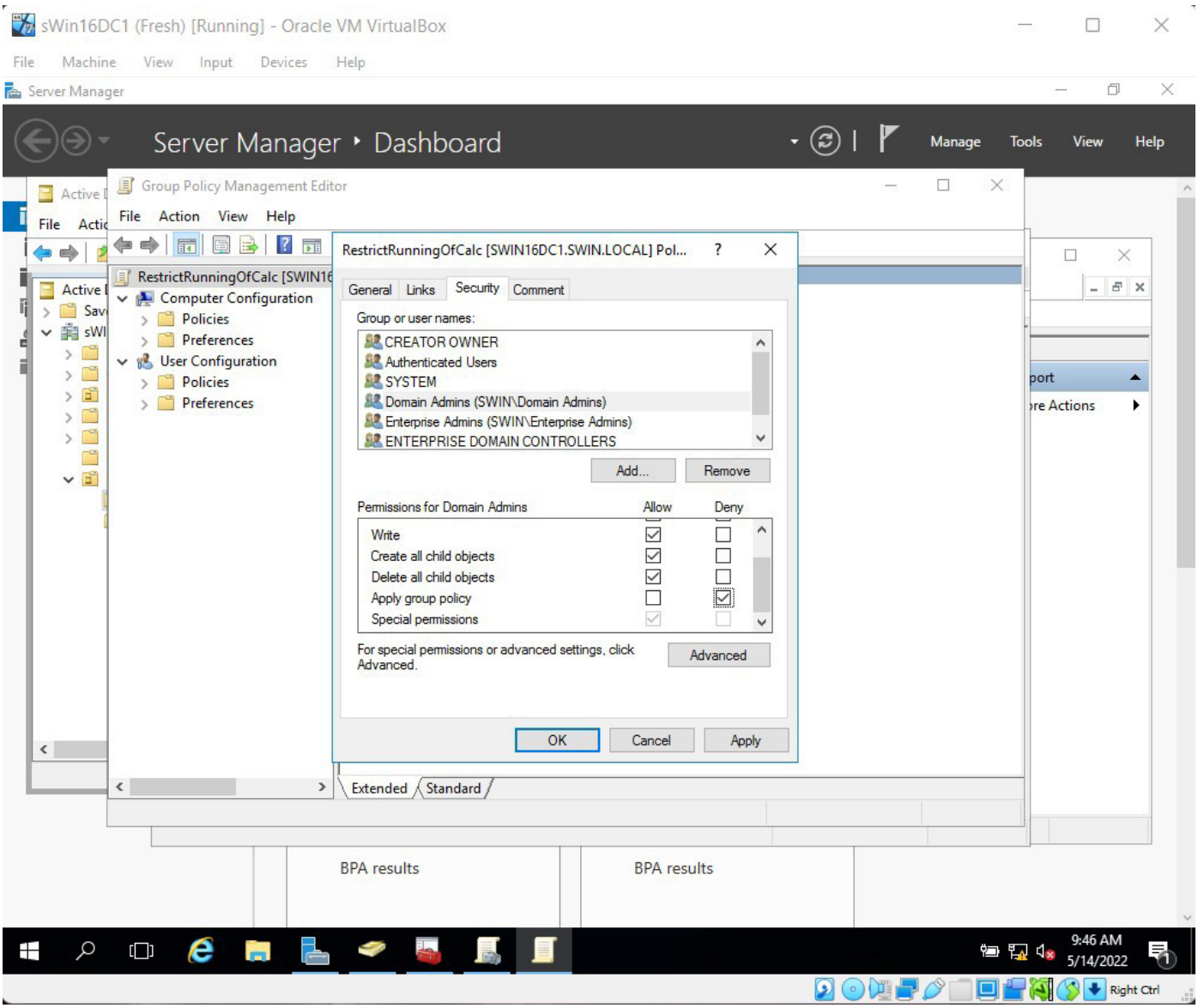


Filtering GPOs



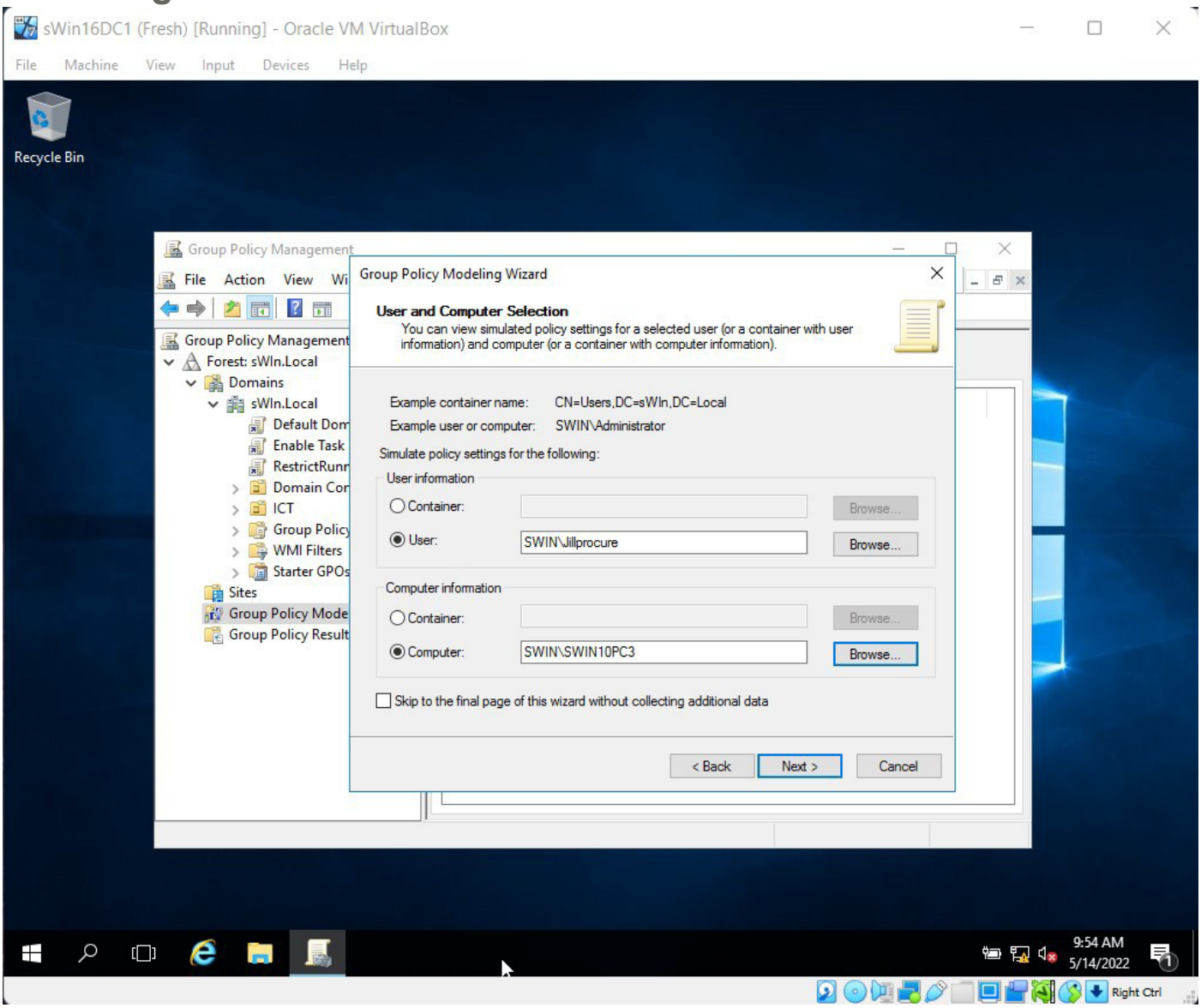
Filtering the **Remove Task Manager** as such it will be only applied to the members of G_ICTProcurement Group.

Filtering with GPO Security



Filtering with GPO Security as that the GPO will apply to everyone except those in the administrators Group.

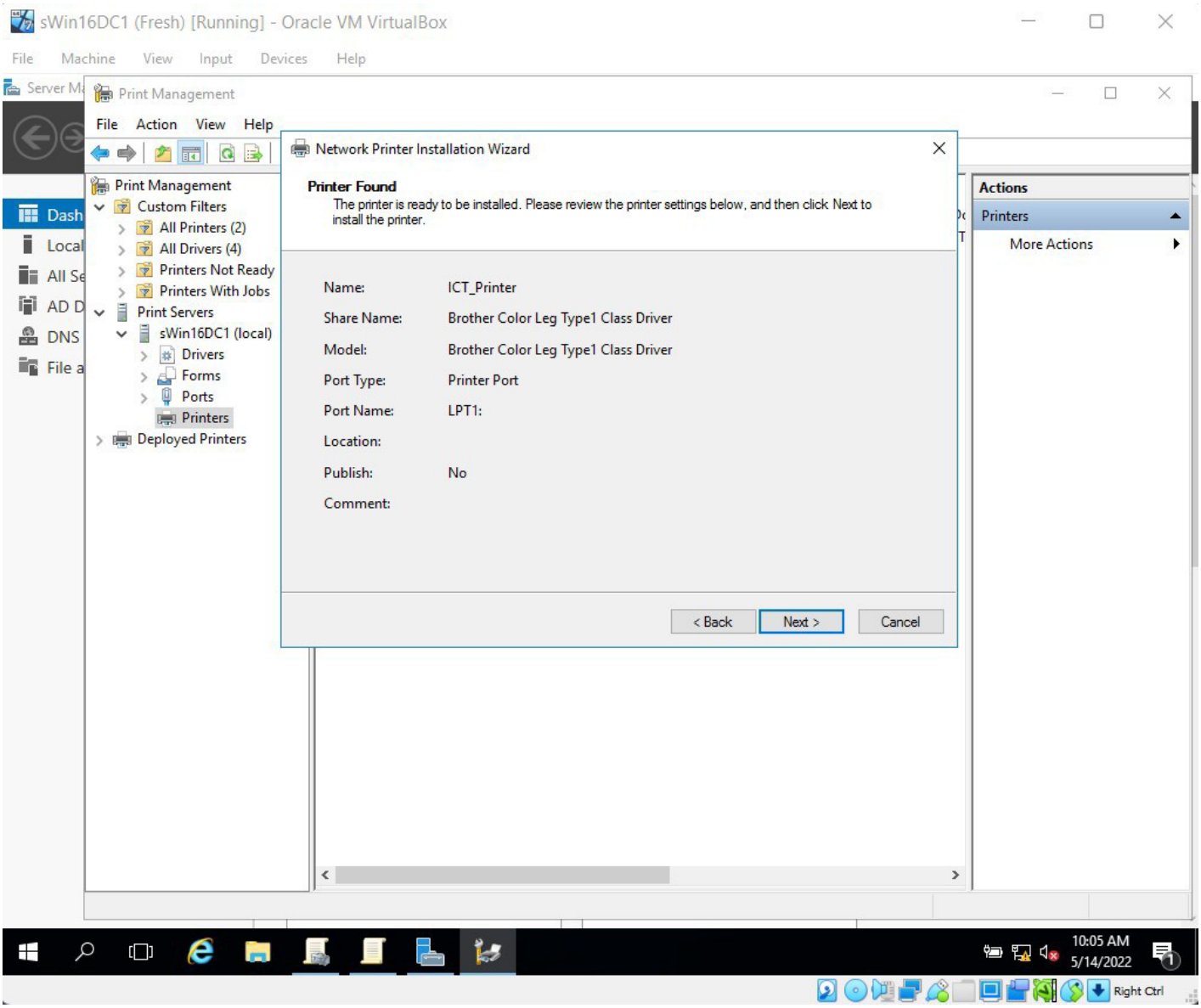
Modelling GPOs



Group Policy Modelling is a wizard that will allow you to select a container, a user or a computer. It will then apply all of the group policies that apply and generate a report that tells you which GPO is causing what setting.

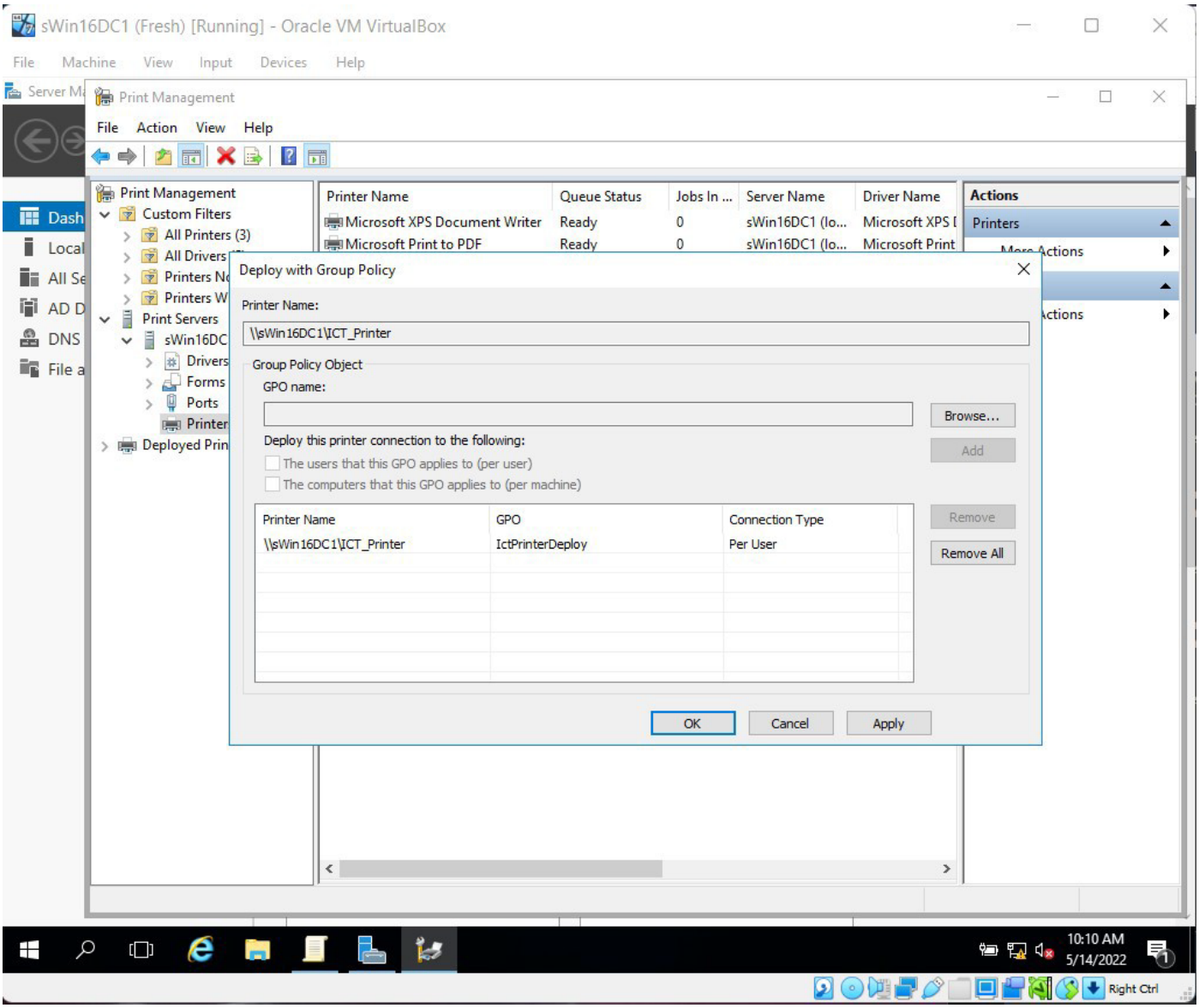
Deploying Printers with GPOs

Create a new Printer



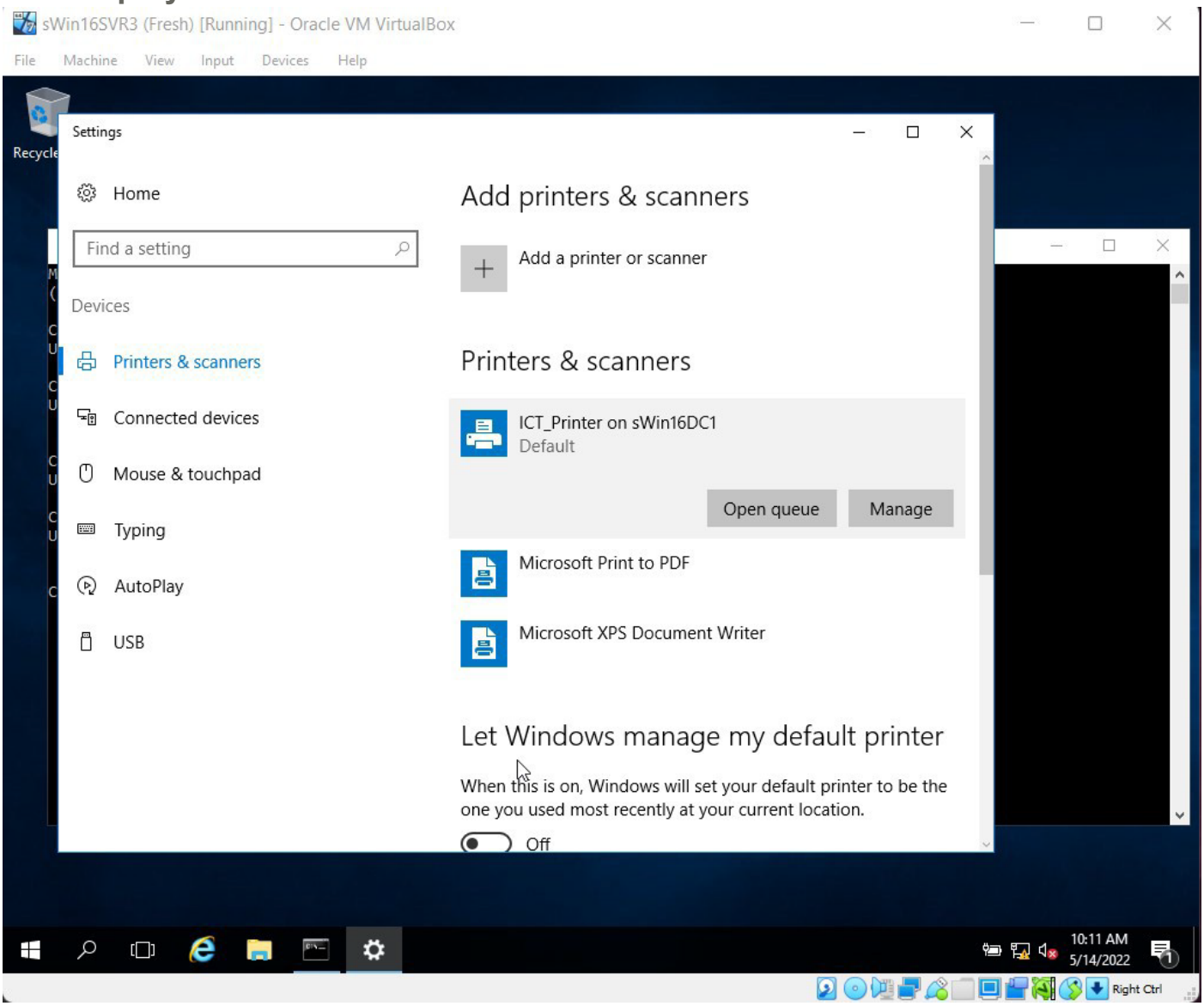
Creation of new printer from the Print Management tool in the sWin16DC1 Virtual Machine

Deploying the Printer Using GPOs



Deploying printers using IctPrinterDeploy GPO, to the users in the ICT Organizational Unit.

Test Deployment



Printer Successfully deployed for users.

TNE10005 Journal Lab (#9)

Khalid Yaseen Baig / ID #102763240

What I learned in this week's Lecture.

- The Industry Standard for Telecommunications Servers should be accessible 99.999 percent of the time, according to the Rule of Five Nines. In other words, the annual downtime is merely 5 minutes and 15 seconds.

- Disaster recovery is the process of restoring company or organizational activities following a disaster by putting in place a disaster recovery strategy.

- Backup systems, volumes, or folders, back up to disks or network shares, and restore from backups are all possible using Windows Server Backup.

- A minimum of two disks is required for RAID 0 (Disk Striping). As a result, both read and write performance has improved. There is no redundancy in the data. There is no capacity loss as a result of the overhead.

- A minimum of two disks is required for RAID 1 (Disk Mirroring). There has been no improvement in performance. Data redundancy exists. Overhead, there is a 50% capacity reduction.

- Improves read speed with RAID 5 (Disk Stripe with Distributed Parity). Data redundancy exists. A minimum of three HDDs is required. There is a 1/n overhead capacity loss.

- Windows Recovery Environment is a feature of the operating system that comes preinstalled with Windows 10 and Windows Server 2016. You can boot into Windows RE if the primary installation of Sever 2016 becomes corrupted.

- Shadow Volume Copy NTFS can keep track of file versions by transferring them to a different location when they are written to the disk. Users can then go back in time as needed.

- ReFS is a new file system introduced in Windows Server 2012 R2 that offers near-infinite file and volume capacities, as well as increased resilience that eliminates the need for error-checking tools. A ReFS volume can be up to 280 bytes in size, or 1 yobibyte. The maximum file size is 16 exabytes (or one million terabytes), far beyond the capacity of any known storage device. File compression, the Encrypted File System (EFS), and disk quotas are not supported by ReFS. Operating systems previous to Windows Server 2012 R2 and Windows 8 are also unable to access ReFS disks.

- Real-time monitoring gives you quick feedback on how well your system is doing. It's useful for identifying bottlenecks that slow down the system, but it necessitates continual monitoring to catch sporadic problems.

- While the administrator is occupied with other tasks, logged monitoring records data. Data is saved in a file, and patterns in usage may be observed, as well as new bottlenecks discovered and addressed before they become an issue.

- Real Time Task Manager is a program that runs on all Windows machines. It provides real-time information on RAM, processor, and network performance. It may be used to locate memory and processing 'hogs.'

- Resource Monitor in Real Time Allows the administrator to have more control over which performance items and metrics are tracked.

- Resource Overview with Real-Time Reliability and Performance Monitor Metrics for disk performance are now available. It may be used to find 'hogs' in each of the four main sub-systems.

- Data Collector Sets were used to log monitoring counter logs. Allow administrators to pick and choose which counters to run in the background. Perfmon takes a sample of the data at the specified interval. By default, data is stored in file%systemdrive%\PerfLogs\<user>The administrator reads the file at a later date or sends the data as a report. Trends may be determined by comparing current data to past data.

- Properties of the Counter Log (Run As) The Administrators or Performance Log Users groups must be members of the user account. If you use an administrator account to monitor distant systems, you're putting your security at risk. It is safer to utilize a service account that has been created just for this purpose and has no additional access or rights.

- Properties of the Counter Log (Scheduling) Monitoring may be set up to focus on times when the administrator is not present, peak usage periods, usage trends over time, and specific bottleneck periods.

- Properties of the Counter Log (Stop Condition) Counter logs can be set to run for a specific length of time and data.

- When a counter's threshold is achieved, an alert is recorded. It is possible to specify the Alert Action tab to log an event in the Application and Services Logs in the event viewer. The alert may be customized to send e-mails, SMS, and other notifications to administrators when problems develop on the Alert Task tab with the proper coding.

- Event Viewer program is used to see a variety of system logs. The command line or a script used to run Event Viewer is eventvwr.msc.

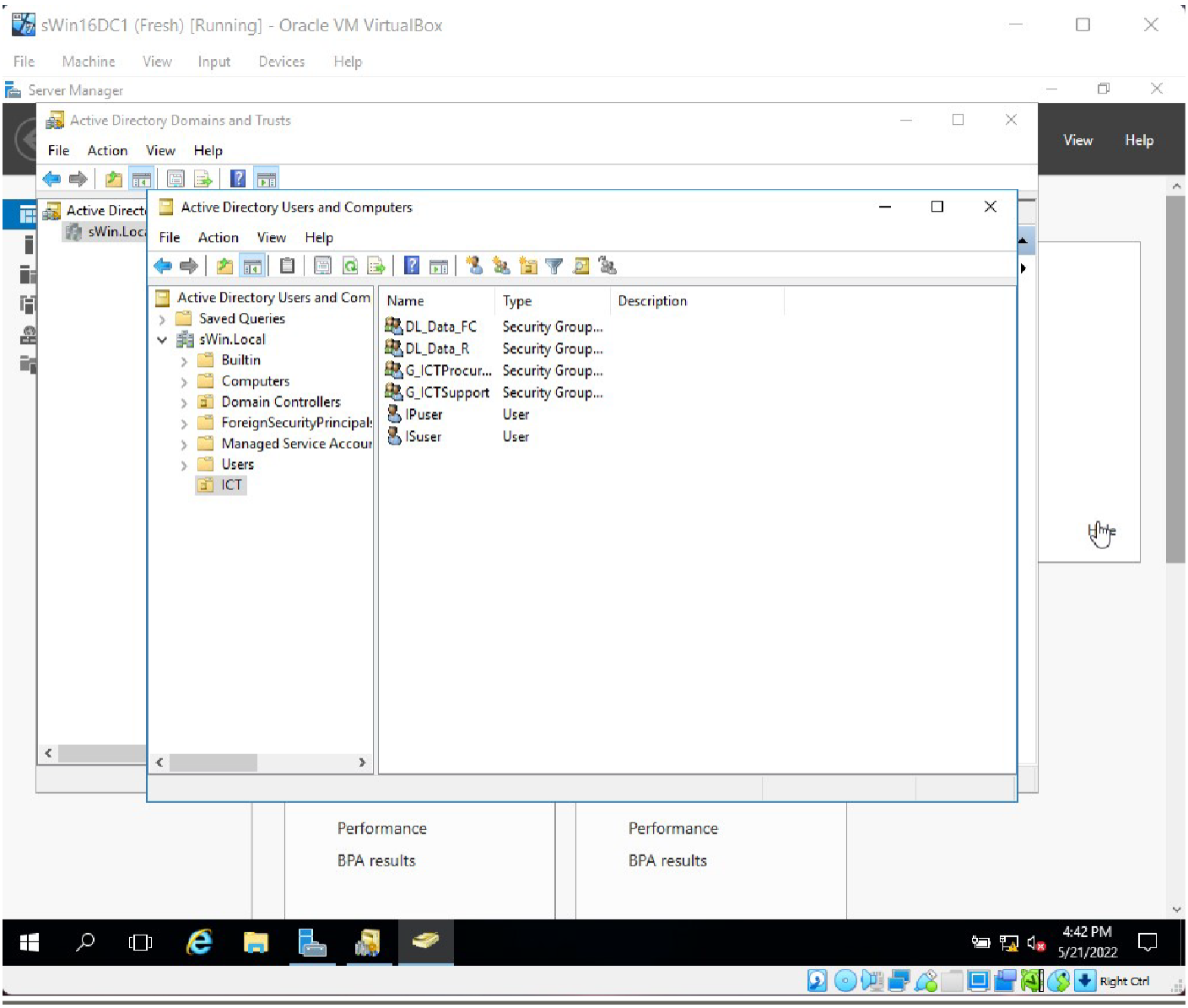
- A Baseline is a set of measures used to establish a starting point. A baseline against which subsequent measurements can be compared. Baselines should be established post-installation, early in a system's life cycle, to define Typical Usage. The same tests should be repeated on a regular basis to uncover patterns.

- When used locally, the performance monitor might contribute to the server's burden. Remote monitoring has a lower impact on the monitored server. When an administrator has a lot of servers to manage, it gets difficult to keep track of them all. It is more convenient to monitor from a distance.

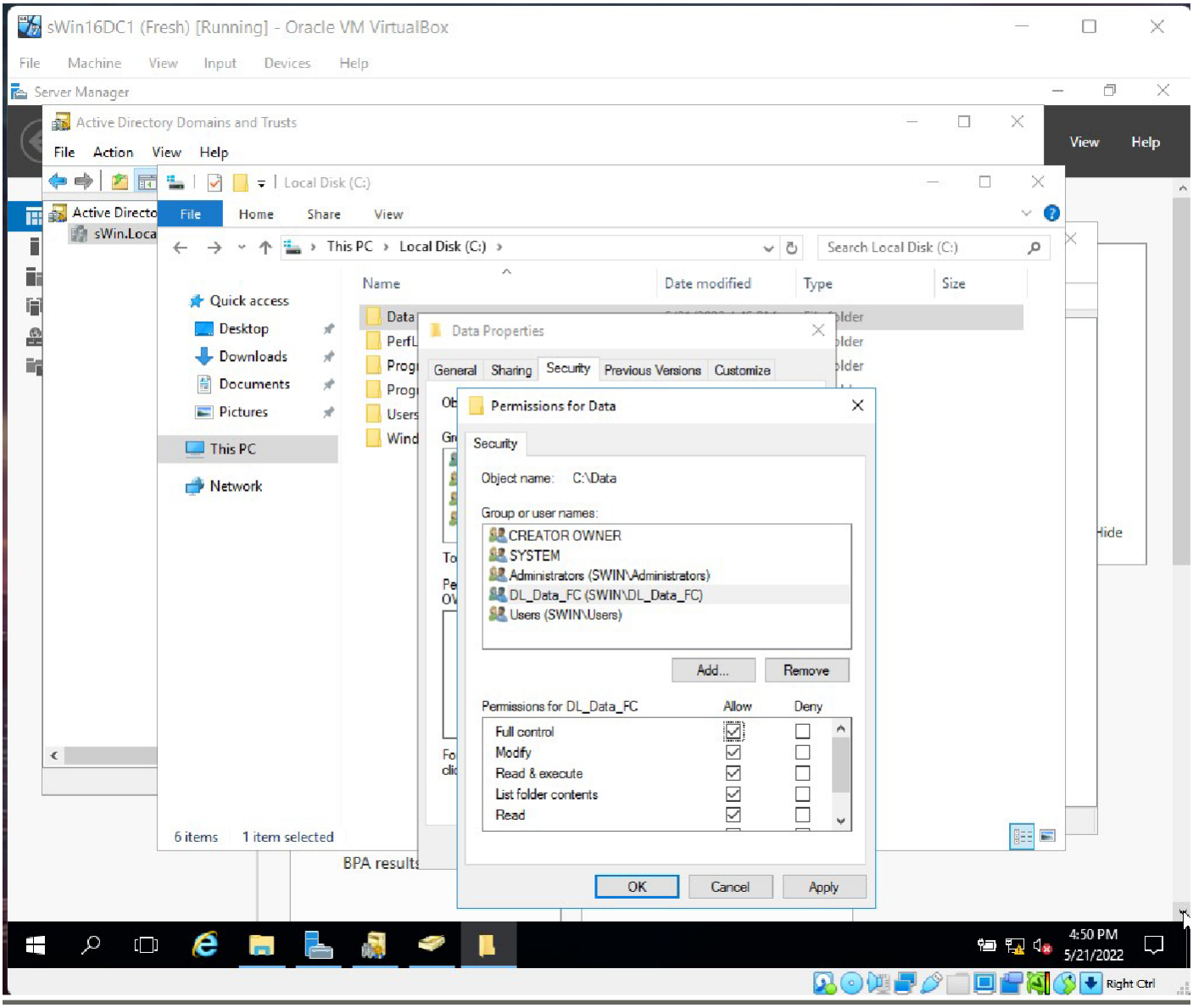
This week’s lab activities.

Screenshots of Important Steps Required for Lab with LAB Question/Answers.

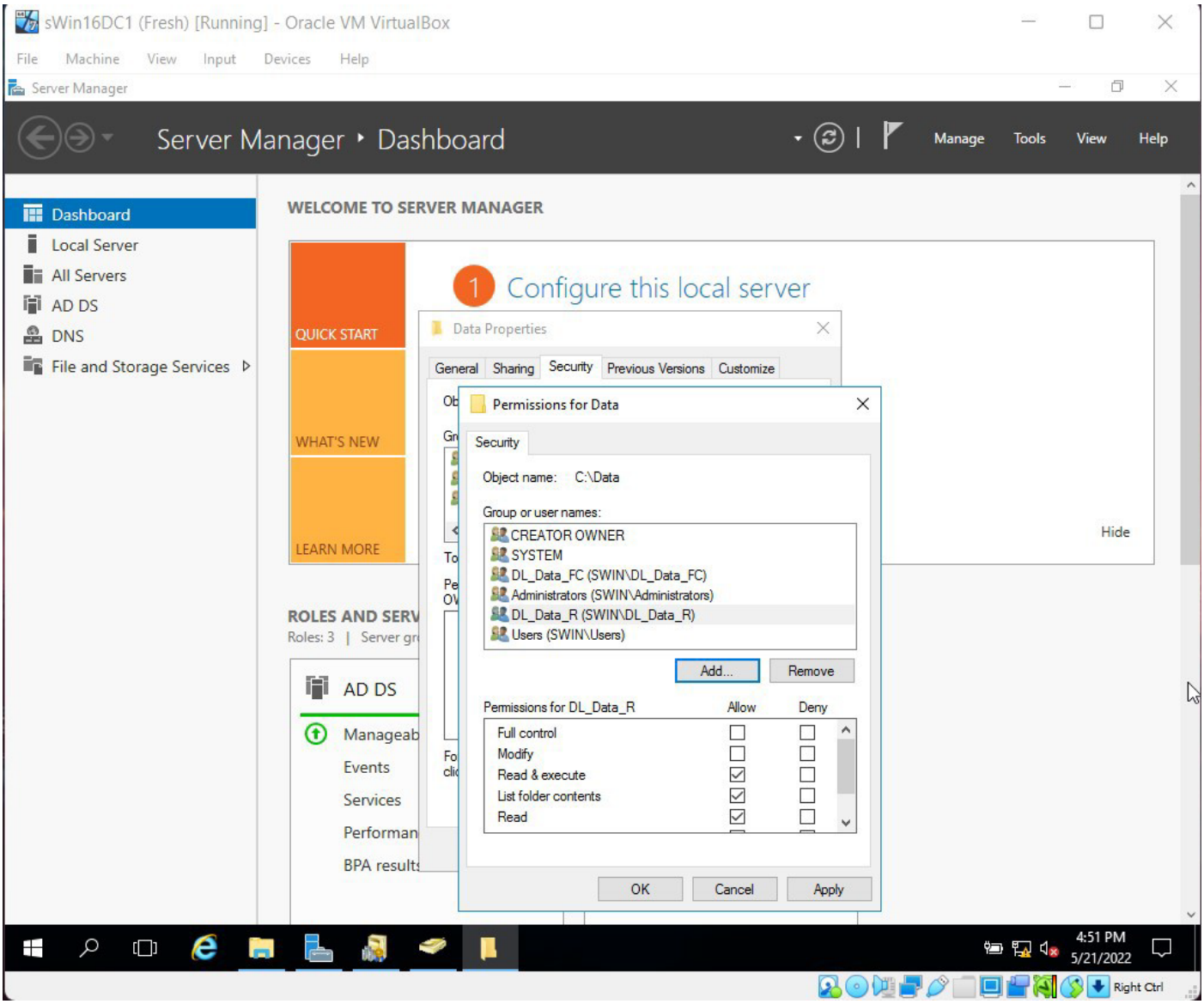
Preliminary settings



Creation of two user accounts (IPuser, ISuser), Two global groups (G_ICTProcurement, G_ICTSupport) and two Dommain Local groups (DL_Data_FC, DL_Data_R) and nesting them accordingly.

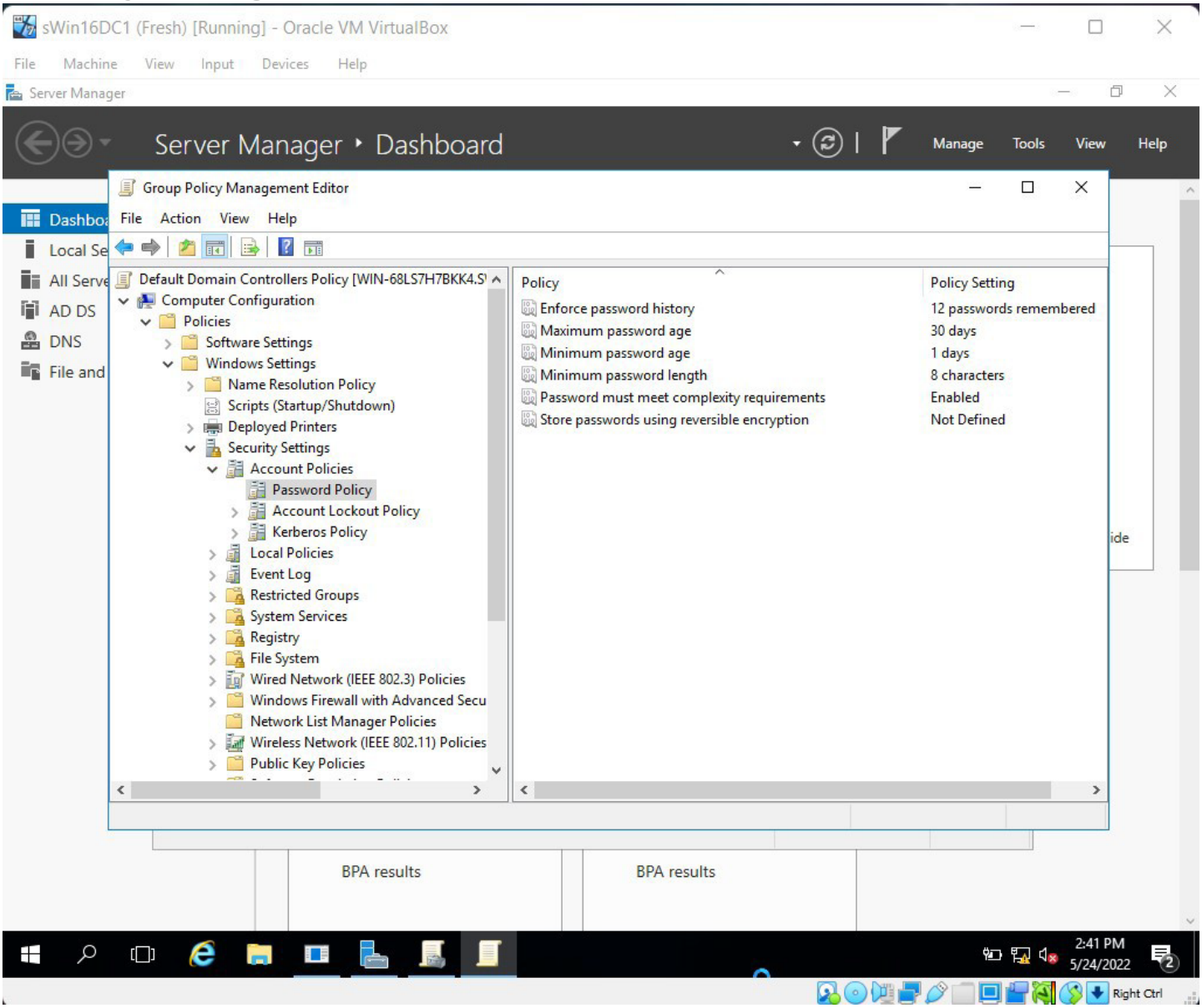


Allocating Share permissions of Data folder for DL_Data_FC as required.

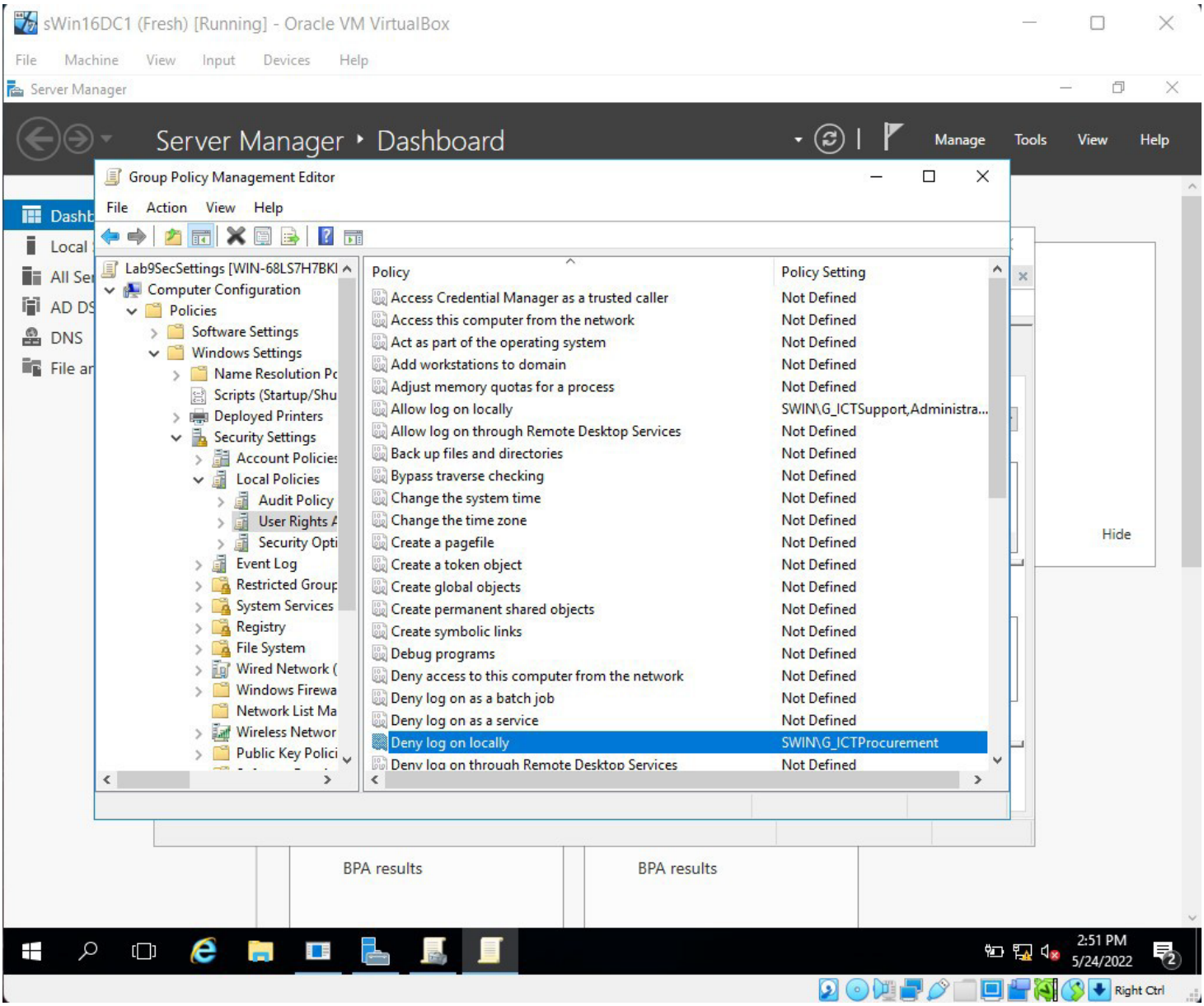


Allocating Share permissions of Data folder for DL_Data_R as required.

Security settings



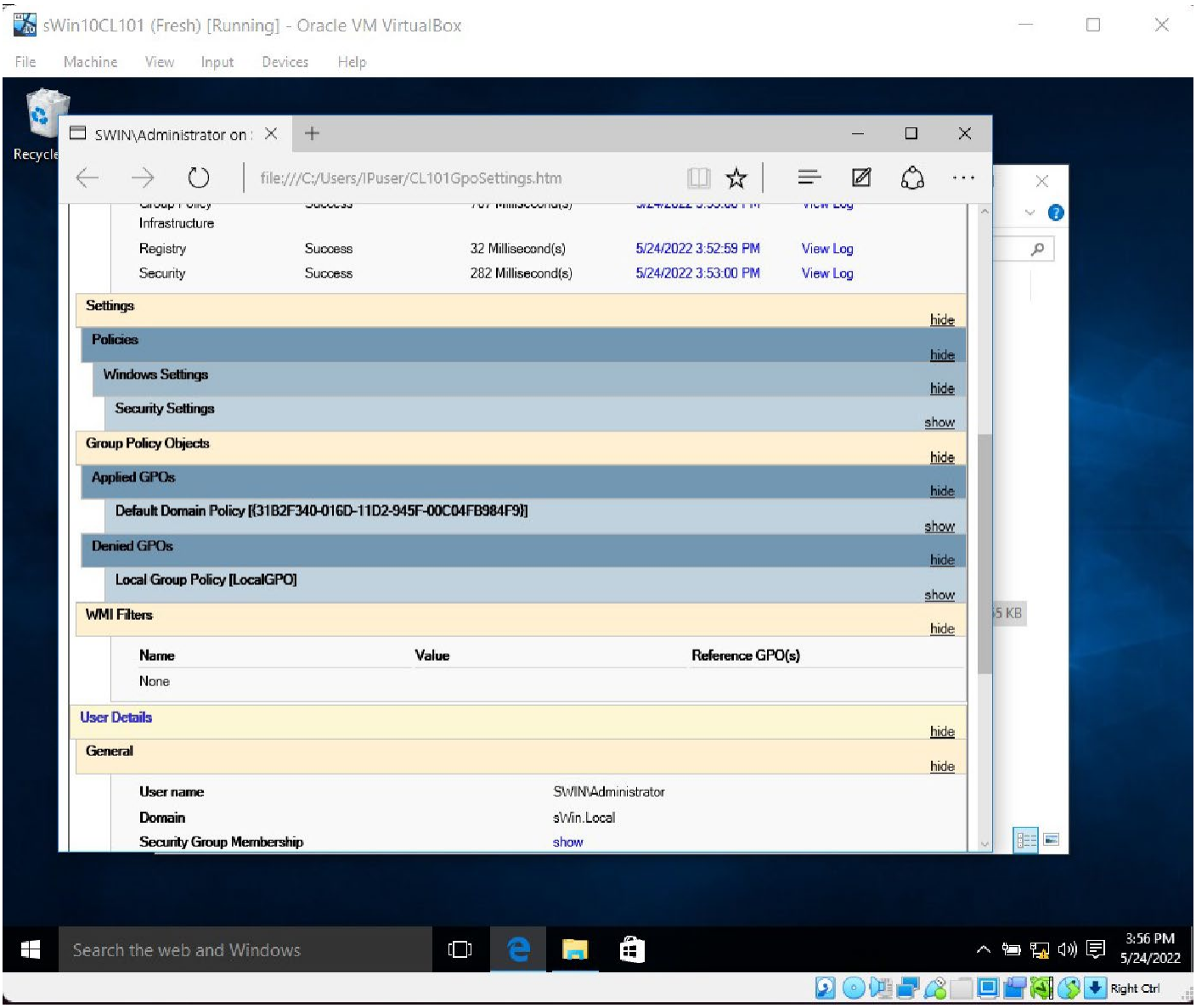
Editing the default domain controllers policy and configuring the settings for Password Policies and Account Lockout Policy as required.



Editing the Lab09SecSettings GPO and configuring the settings for User Rights Assignment as required.

Predict whether the user can successfully log on the Client PC as IPuser? No

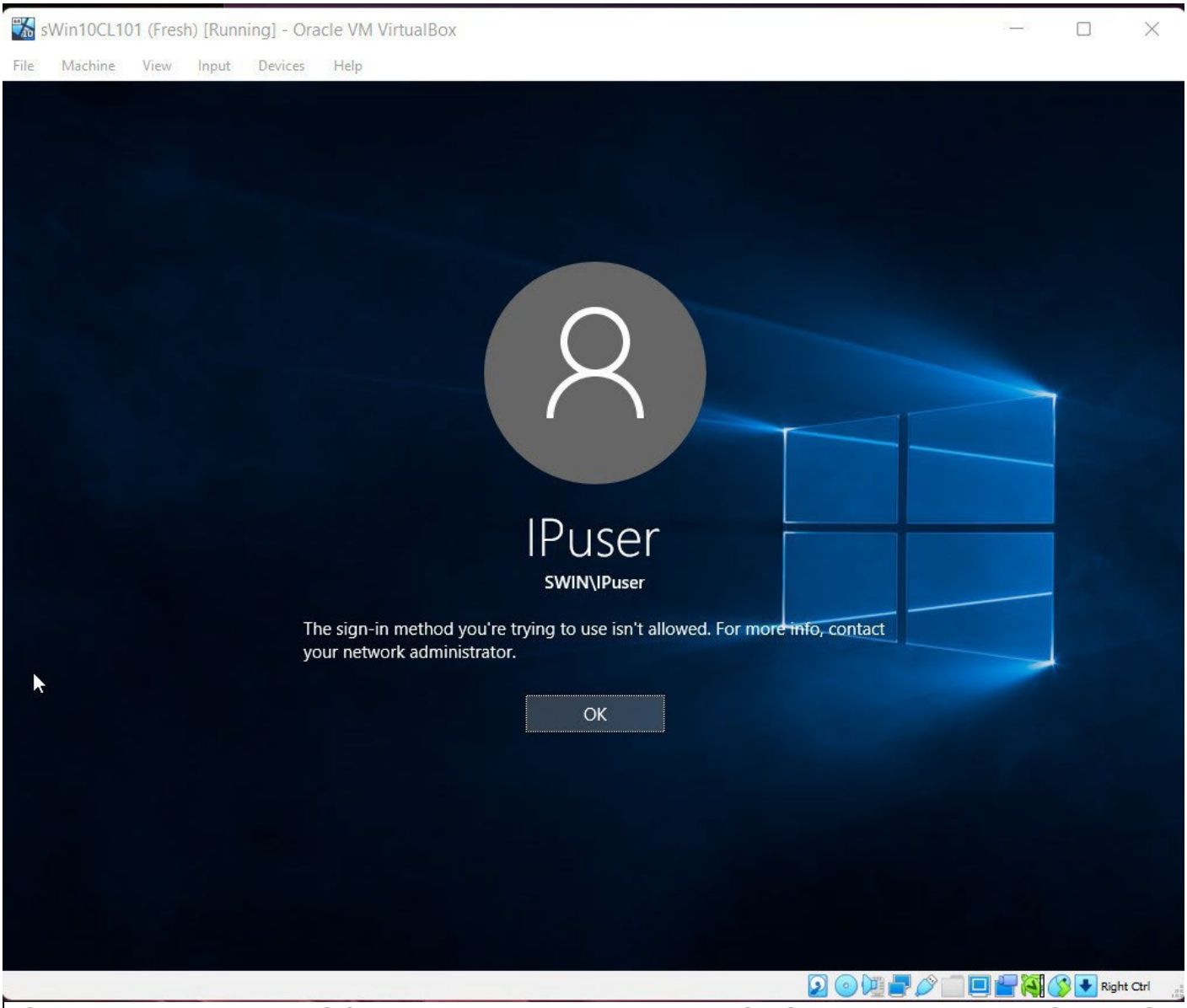
Log on as IPuser, Is your prediction correct? No, We could successfully Log on to IPuser



IPuser's GPO report, inorder to check which GPOs have been applied.

15. When the report loads, scroll down until you find the Applied GPOs section. Was the Lab9SecSettings GPO applied?

Explain your observations: No, it wasn't applied.



After moving the client's PC from computers container to the ICT OU and rebooting the Client PC, When tried to login as IPuser, theres an error message as the intended GPO settings have been applied now.

Reboot the Client PC, and log in as IPuser Were you successful? No

Explain your observation: Theres and error message and we are instructed to contact Administrator

Predict whether ISuser can log on, then log on to the Client PC as ISuser! We will be able to LogIn as ISuser without any issues as there were no such restrictions placed for ISuser like IPuser.

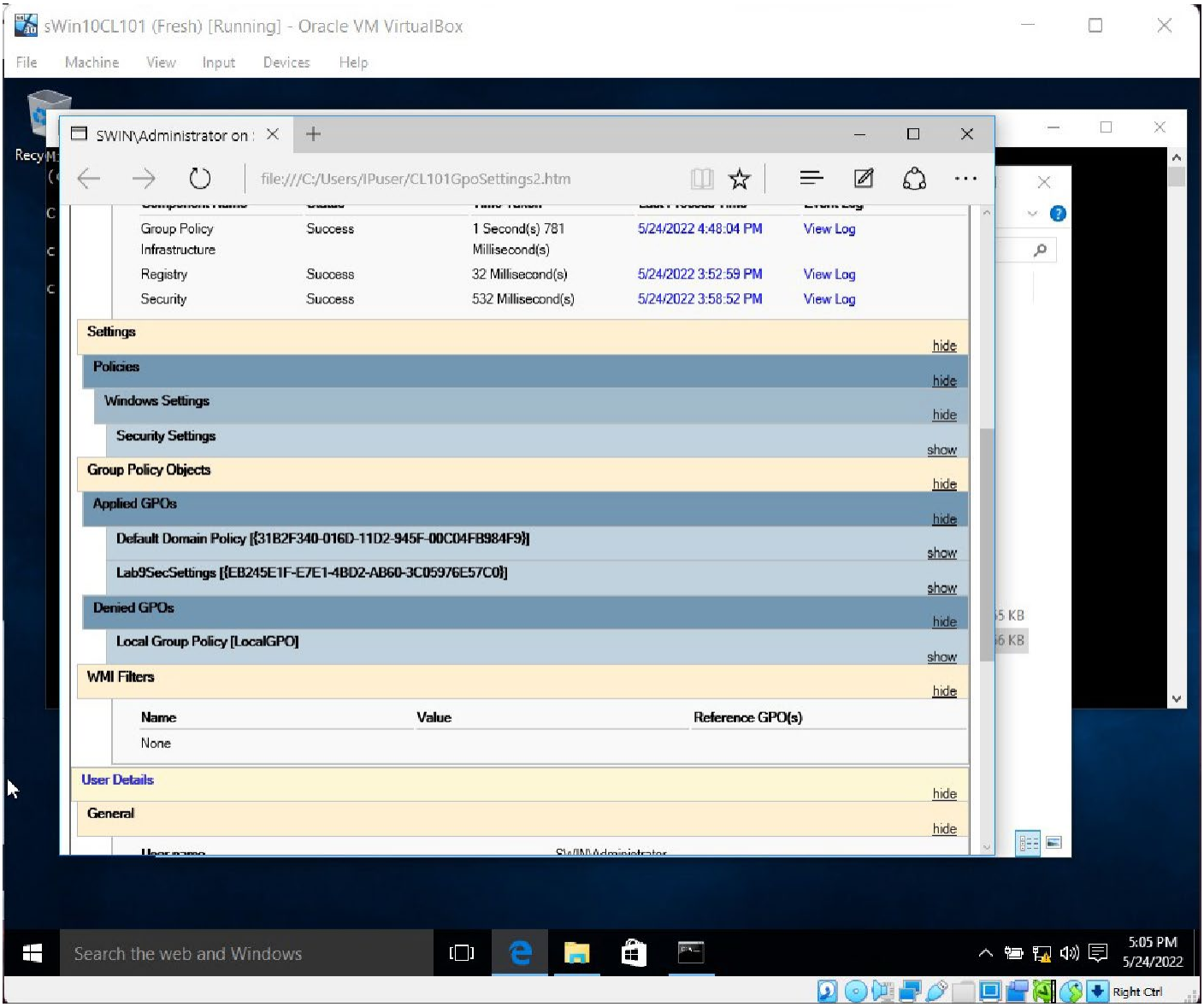
17. From a command line run gpresult /h CL101GpoSettings2.htm

Which of the following settings have changed?

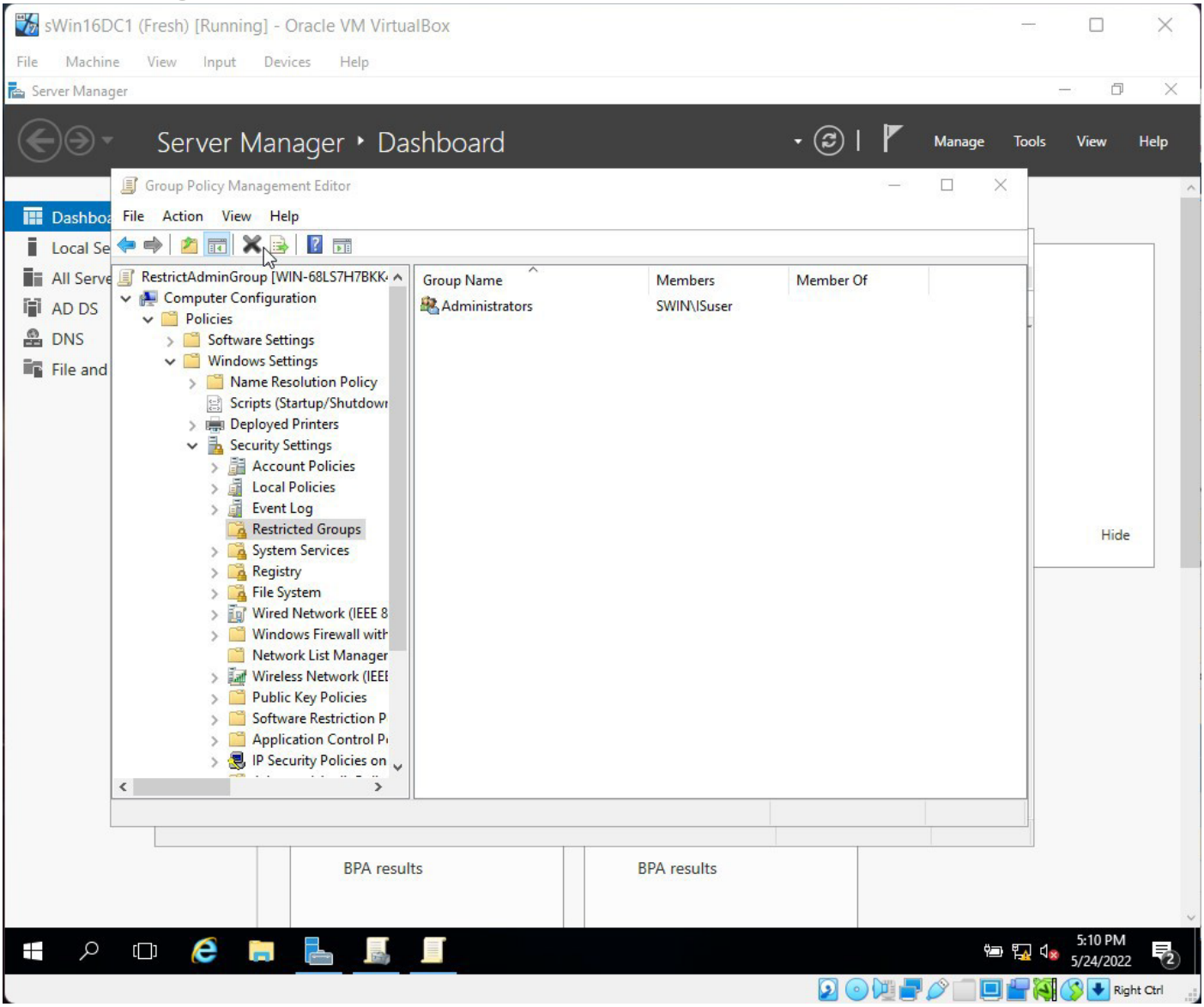
Account Policies/Password Policy: Not Changed

Local Policies/User Rights Assignment: Changed

Try to explain your observation: The Lab9Settings GPO has been successfully.

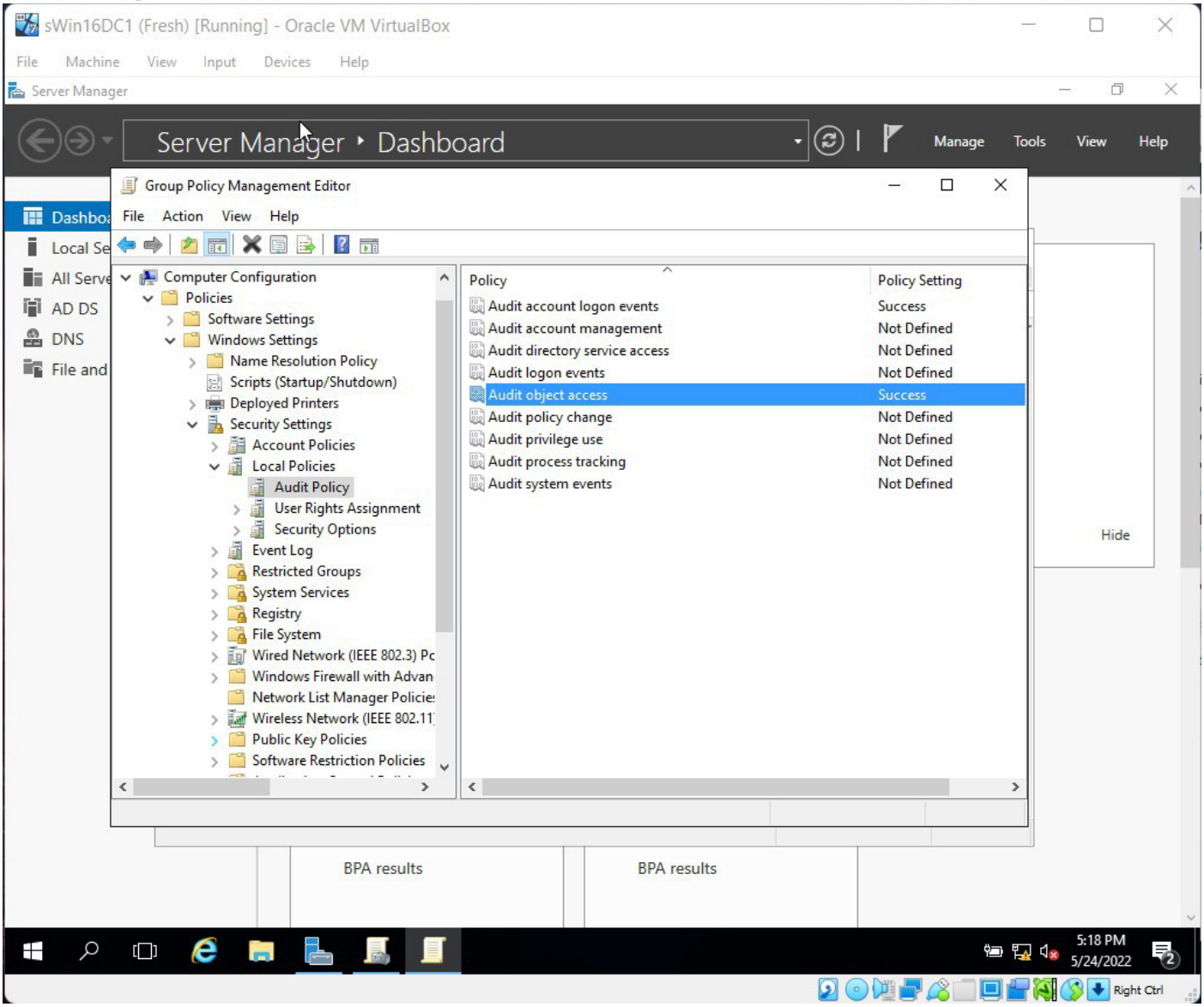


Restricting Groups

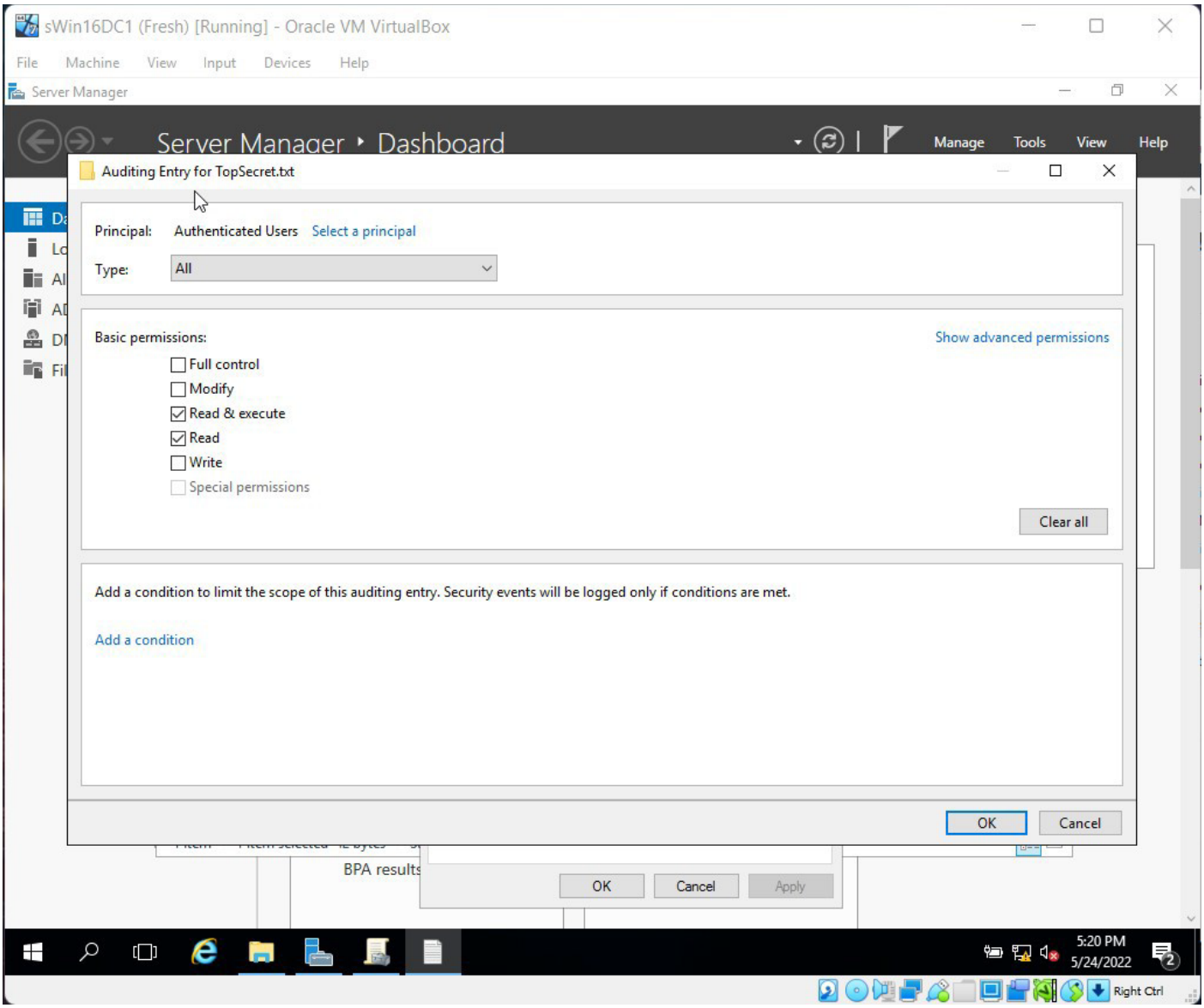


Configuring the RestrictAdminGroup GPO Adding ISuser among restricted groups.

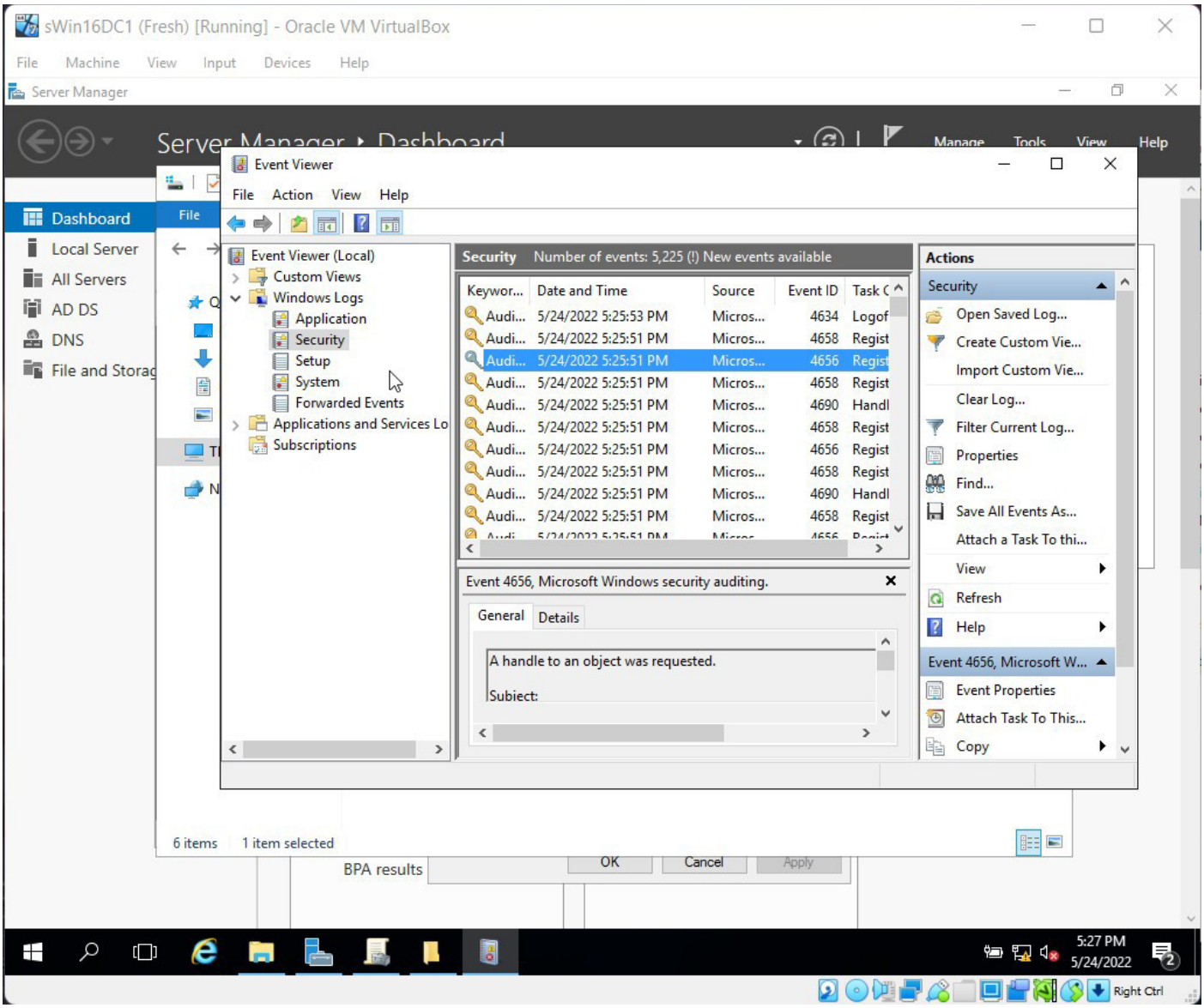
Auditing



Editing the default domain policy and configuring the settings for Audit Account Logon Events and Audit Objects Access as required

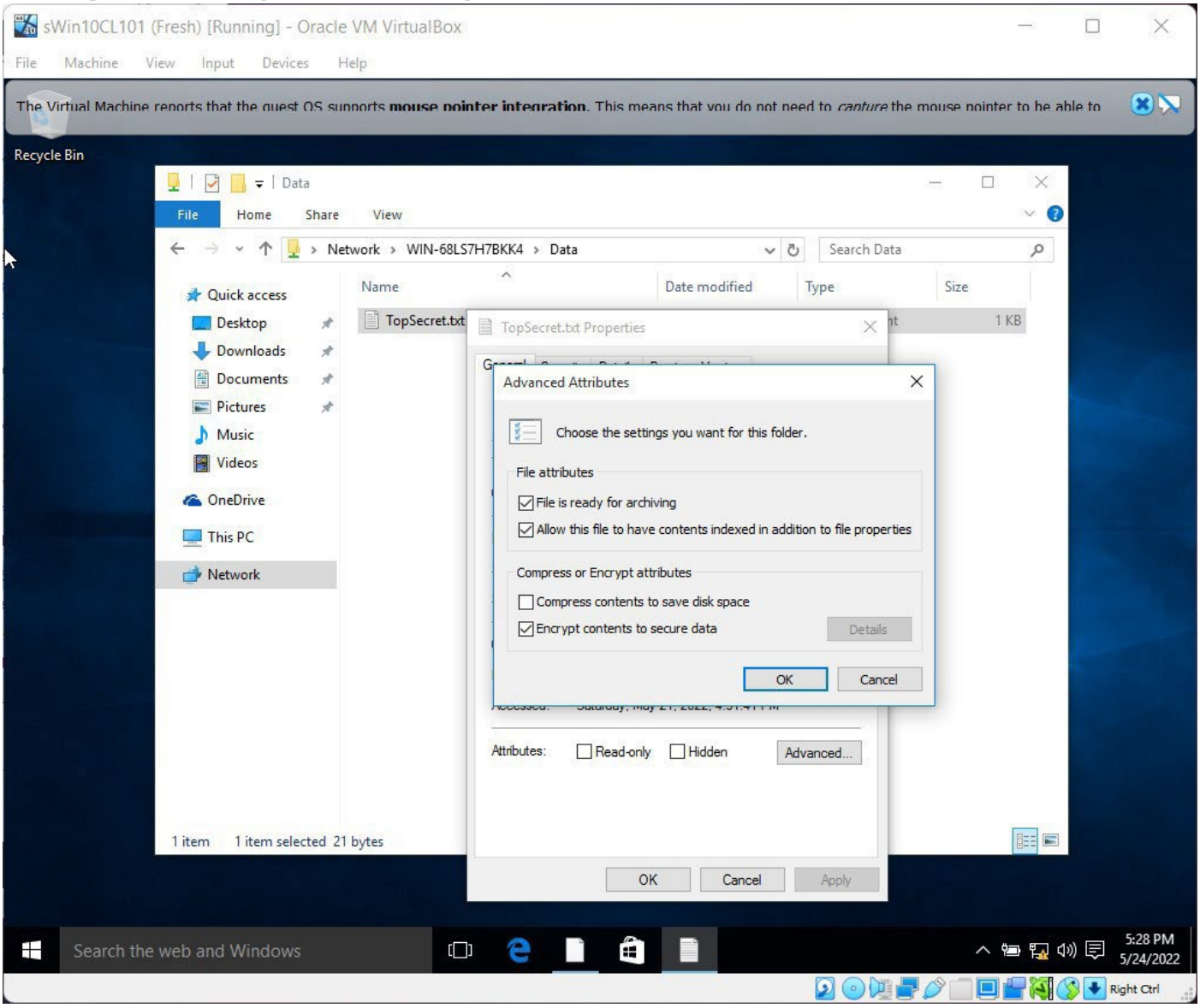


Configuring the Auditing Tab for TopSecret.txt as required.



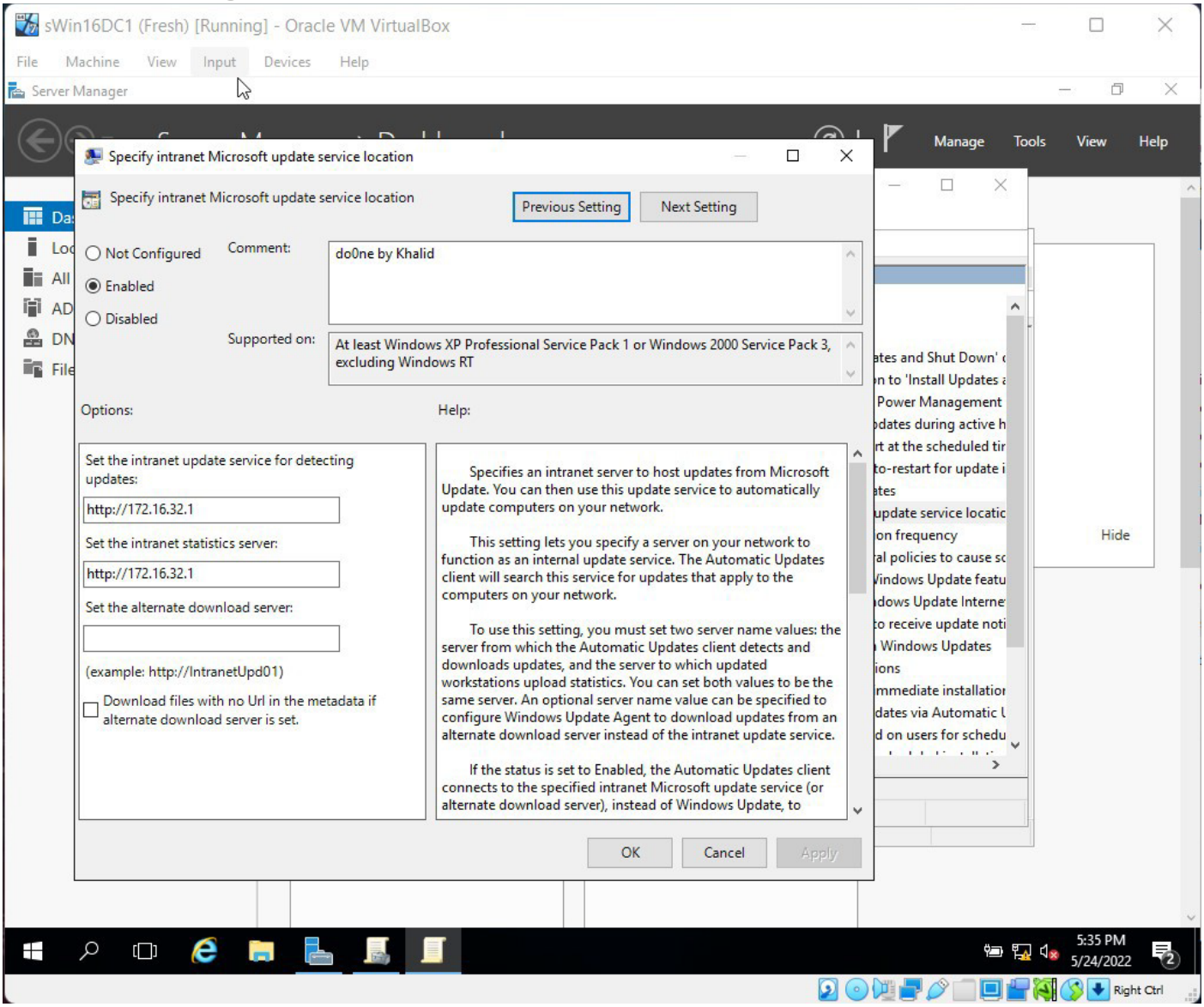
Viewing the Security Log from the Event Viewer App, and looking for required ids.

Using the Encrypted File System

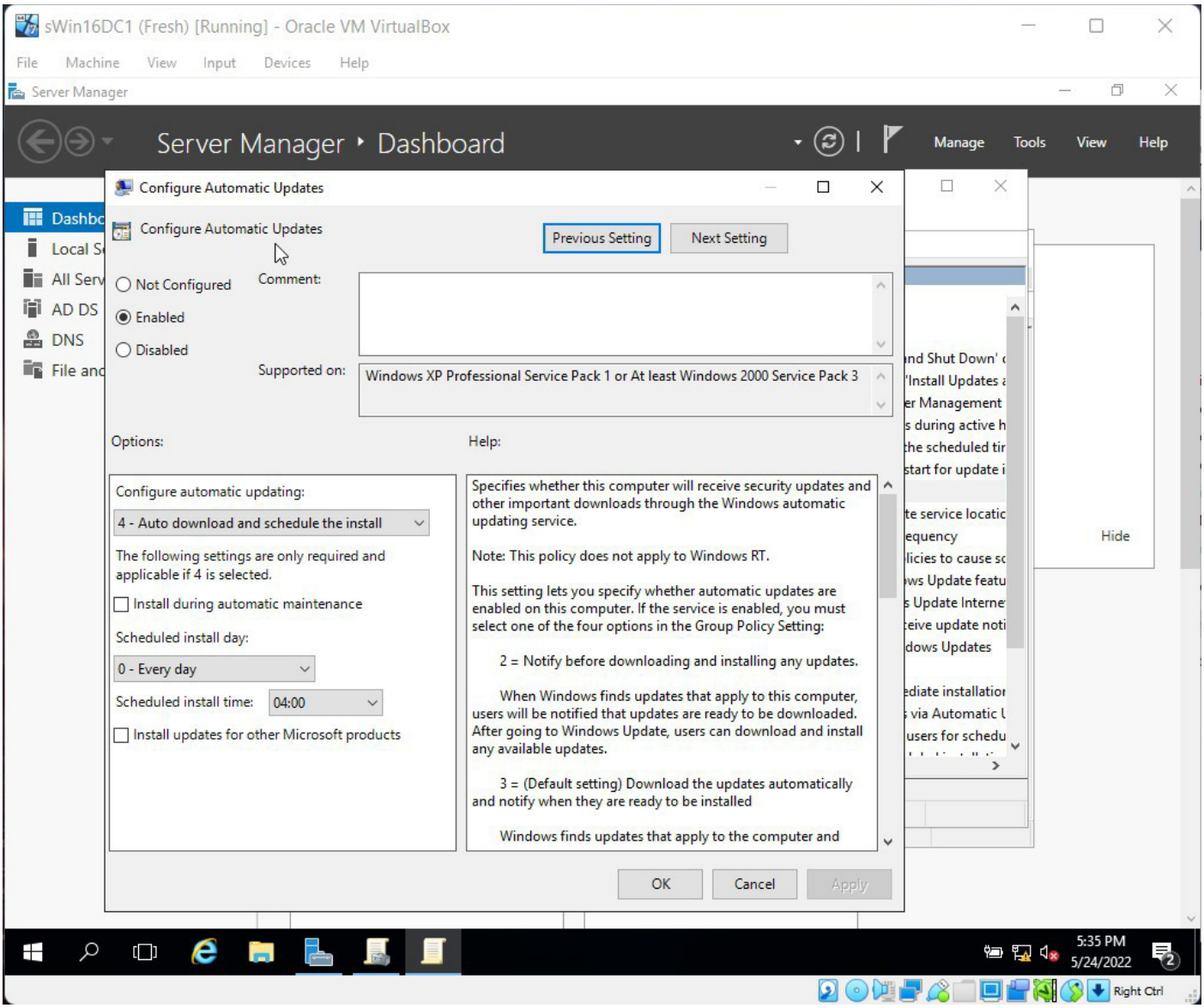


Enabling Encrypt contents to secure data from the advanced attributes settings of the TopSecret.txt file properties.

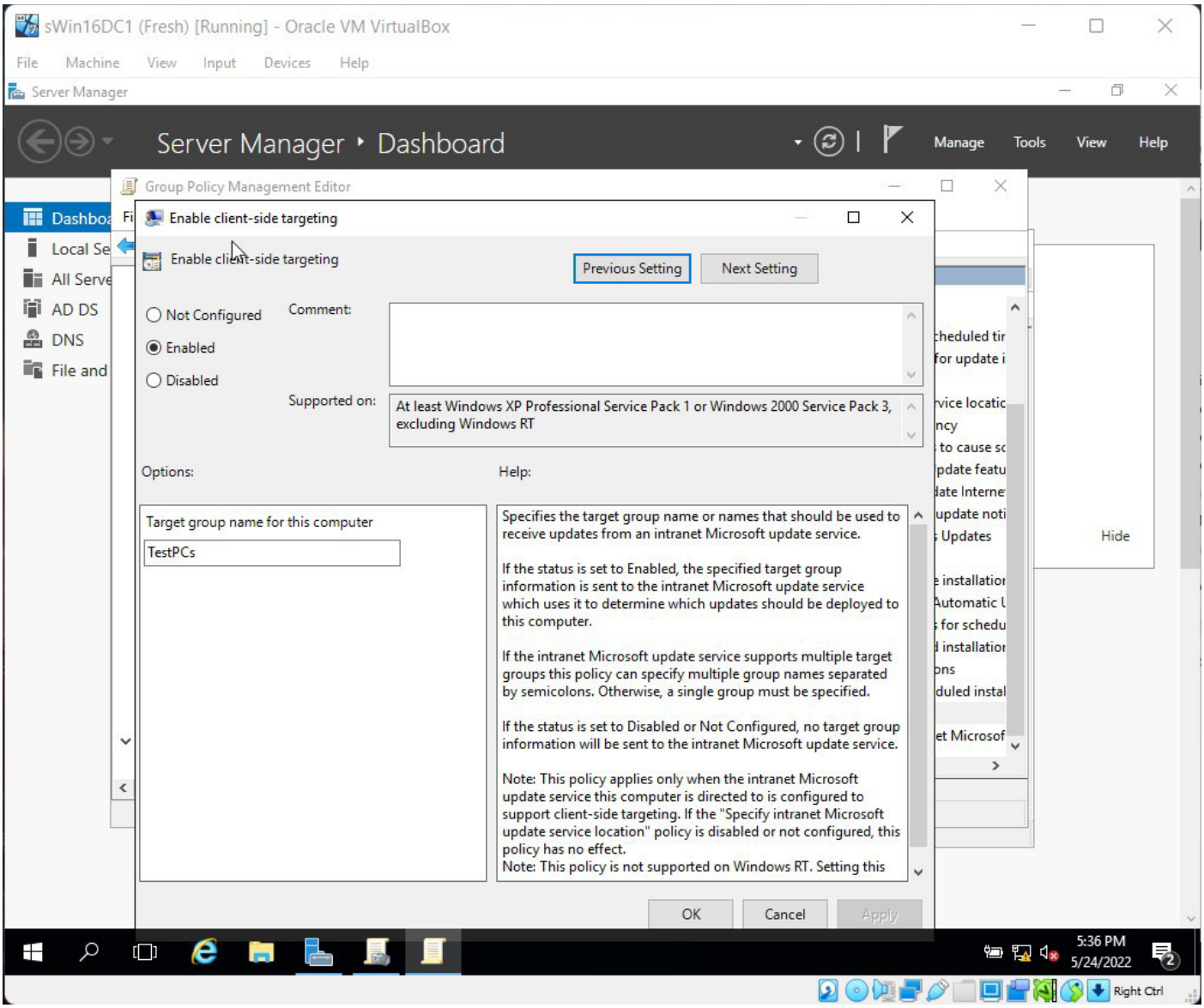
WSUS settings with GPO



Editing the default domain policy and configuring the settings for Specify Intranet Microsoft update service location.

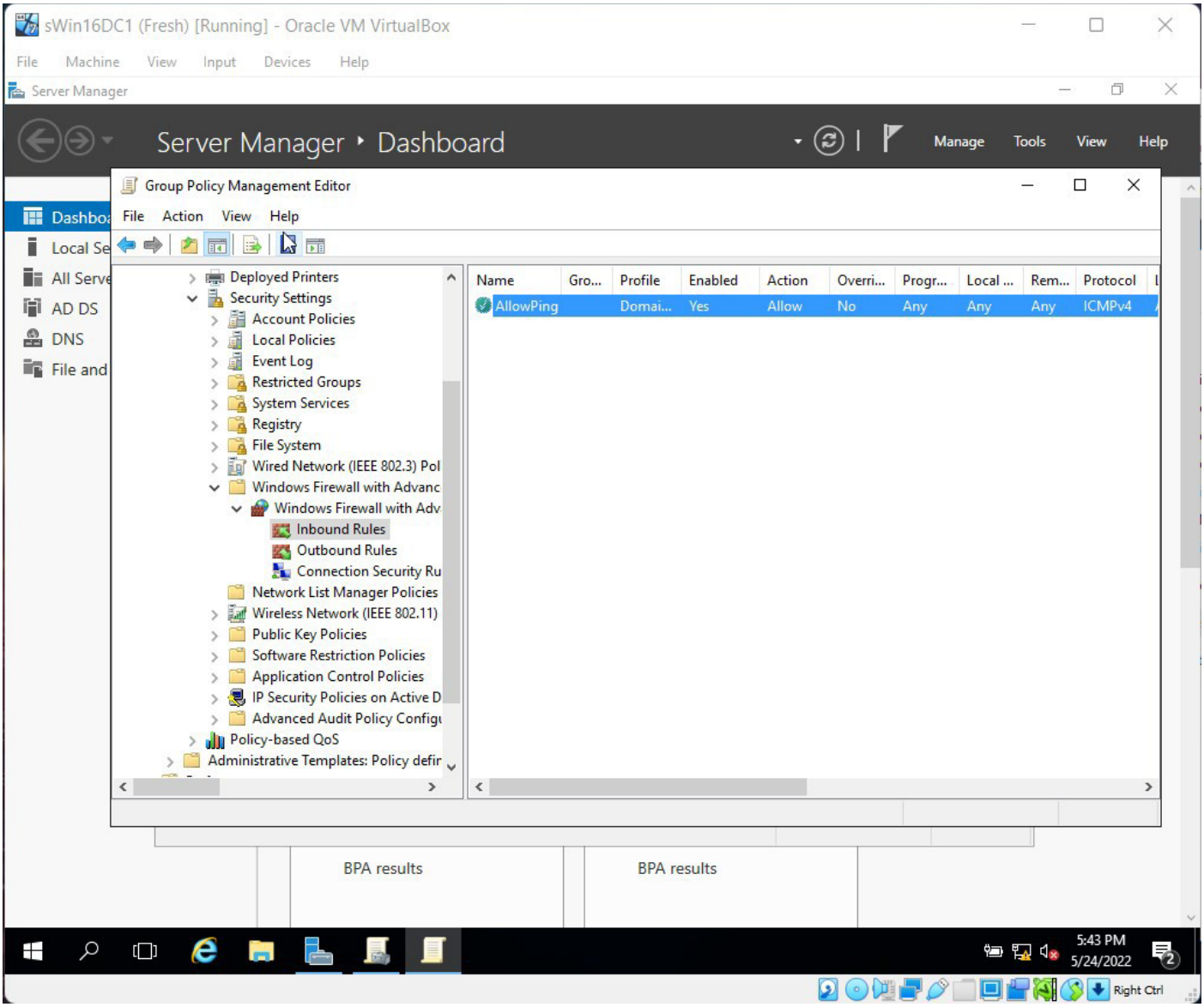


Editing the default domain policy and configuring the settings for Configure Automatic Updates.



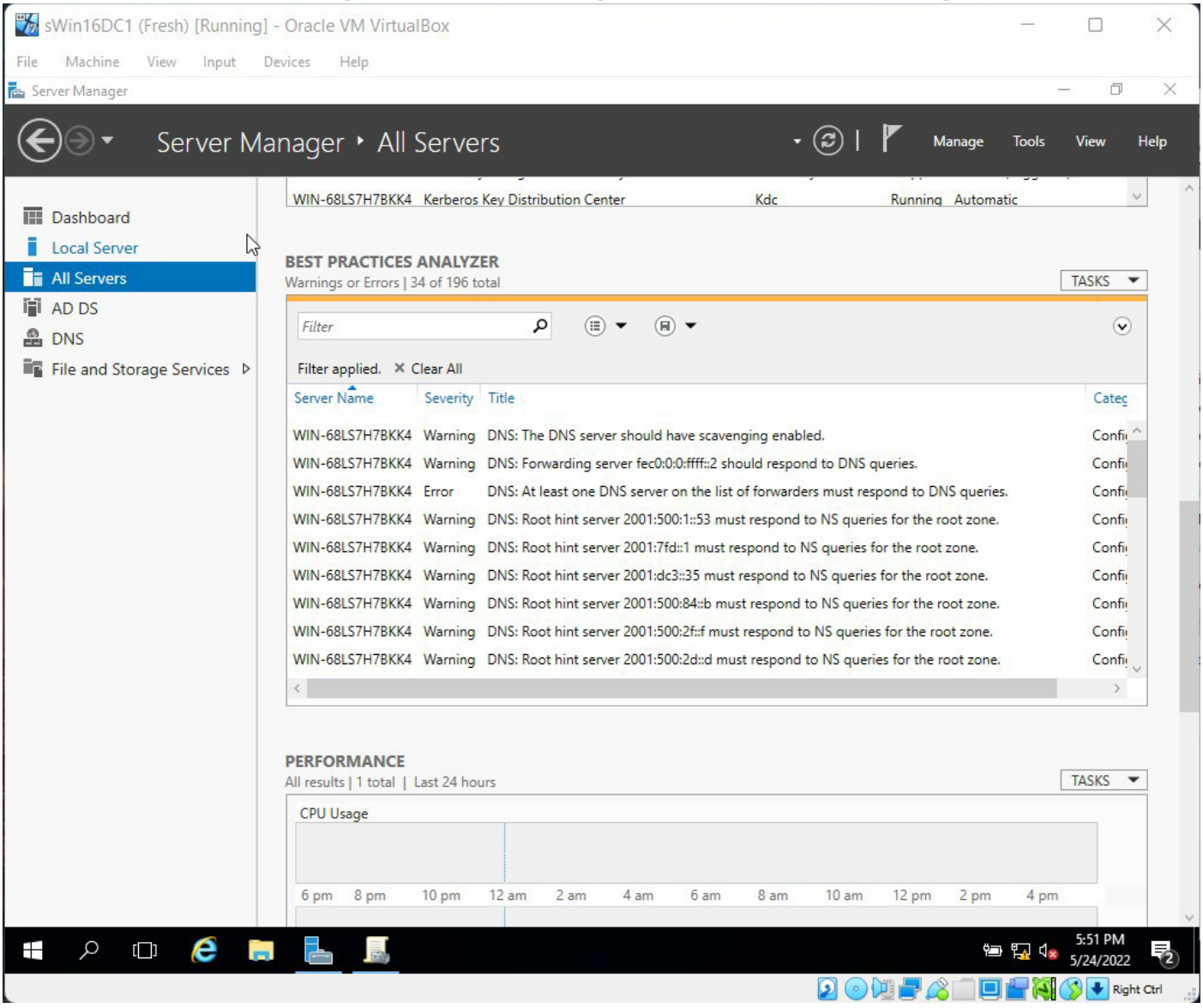
Editing the default domain policy and configuring the settings Enable client-side targeting.

GPO with Firewall



Editing the Firewall-AllowPing GPO and configuring a new rule for Inbound Rules of Windows Firewall with advance security.

Best Practices Analyzer or Security Compliance Manager



Results of BPA Scan from the Best Practices Analyser.