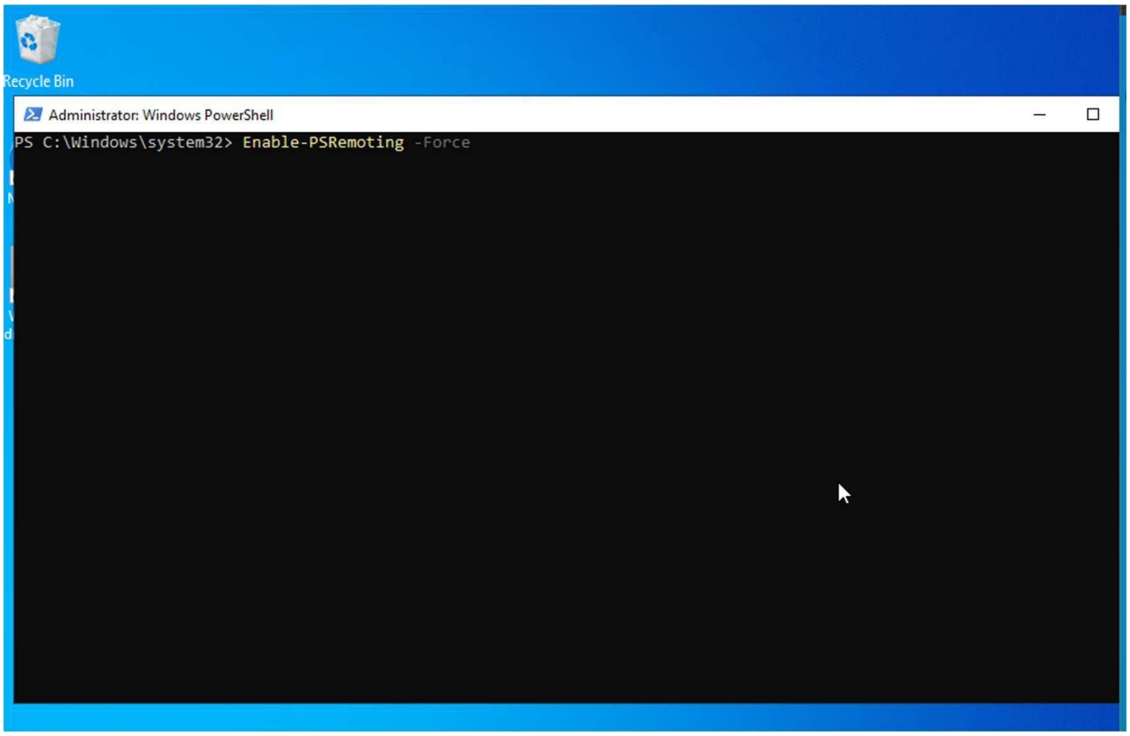
Name: Mahimaa Vardini Balaji Ramathaal

Management server: Windows 10

Remote server : Windows 2022

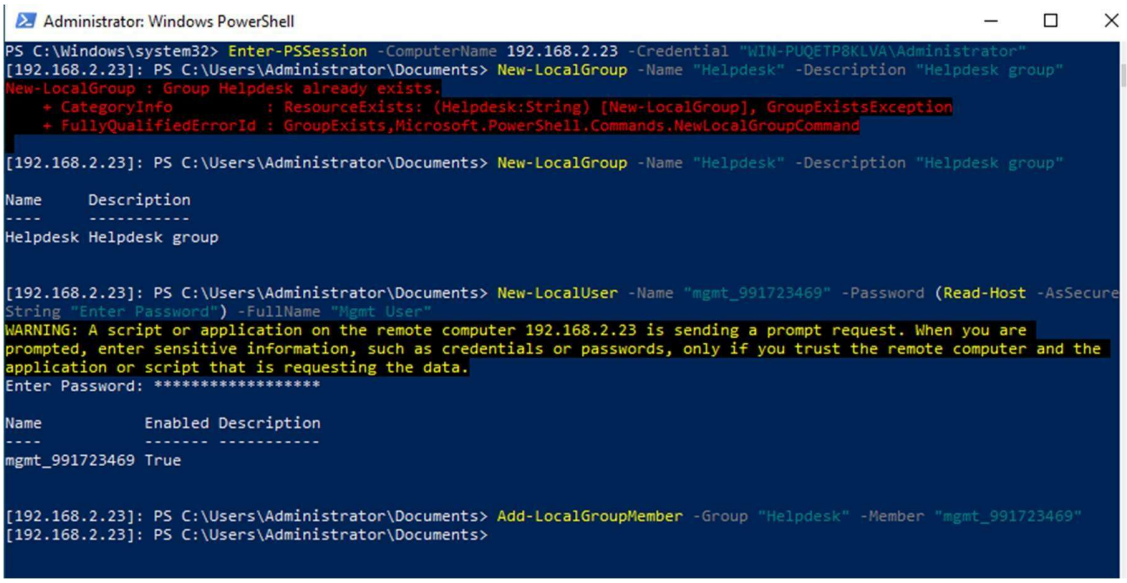
PART 1

WINDOWS POWERSHELL ADMINISTRATION

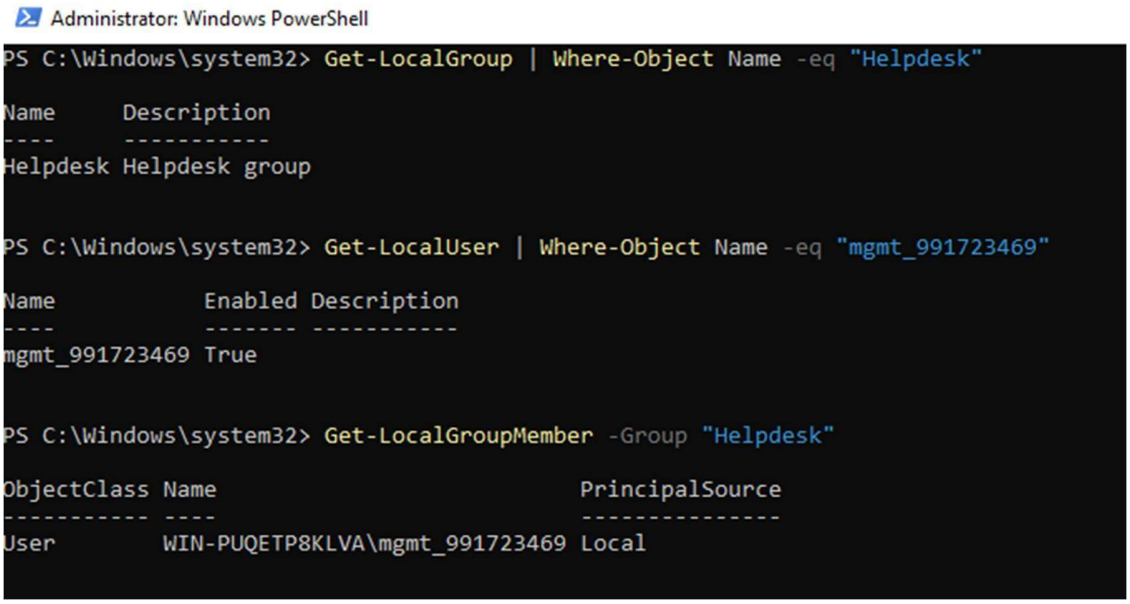


LOCAL USERS AND GROUPS

Creating a group “Helpdesk” and adding a user called “mgmt._991723469” to the group



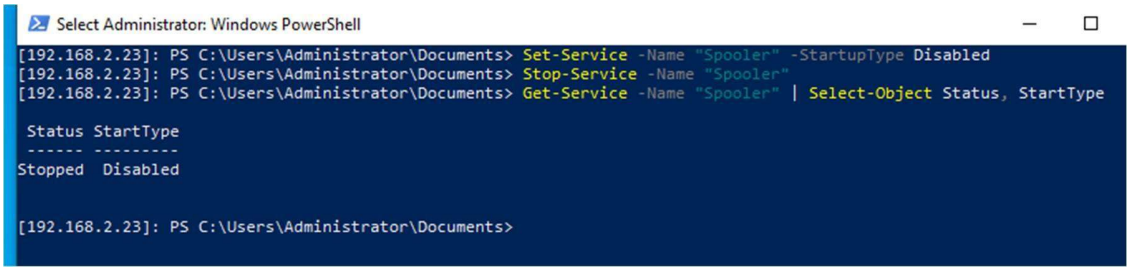
Checking if everything worked on Windows 2022



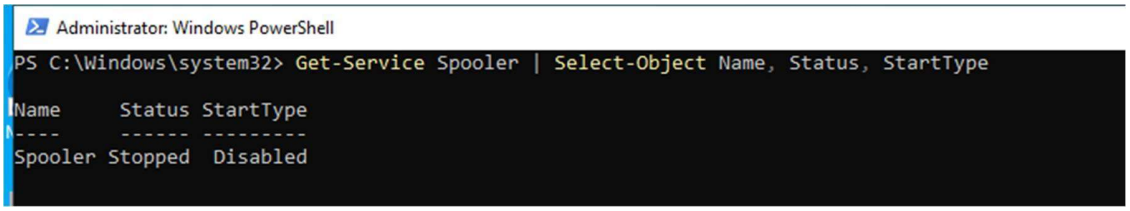
SERVICES

Modifying the Print Spooler service so it does not automatically start Then stopping

the service



Checking from remote server

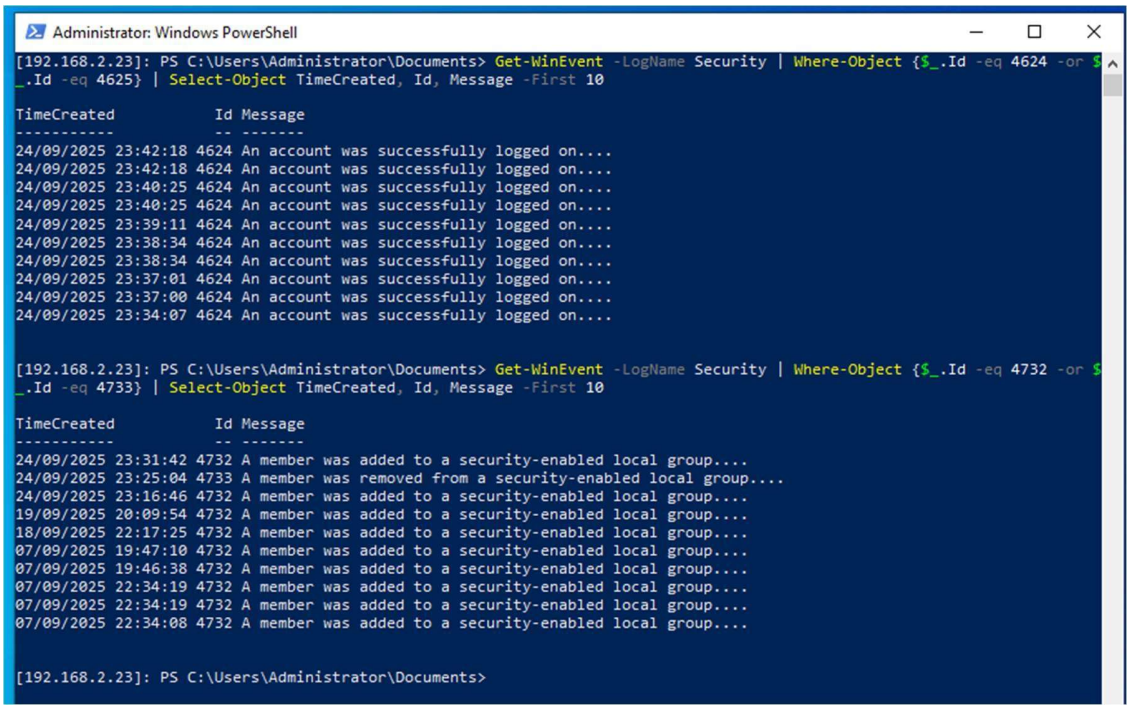


SECURITY EVENT LOGS

View security event logs

Logon Success / failure events – 4624 / 4625

Group membership changes - 4728



FIREWALL RULE

Adding an inbound firewall rule to allow RDP (3389)

```
[192.168.2.23]: PS C:\Users\Administrator\Documents> New-NetFirewallRule -DisplayName "RDP Management Subnet" -Direction
 Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress "192.168.2.23/24" -Action Allow


Name                          : {bfabf4b7-26bb-43f8-9fa0-662e80511e92}
DisplayName                   : RDP Management Subnet
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}



[192.168.2.23]: PS C:\Users\Administrator\Documents> Disable-NetFirewallRule -DisplayName "RDP Management Subnet"
[192.168.2.23]: PS C:\Users\Administrator\Documents>
```

Checking from remote server

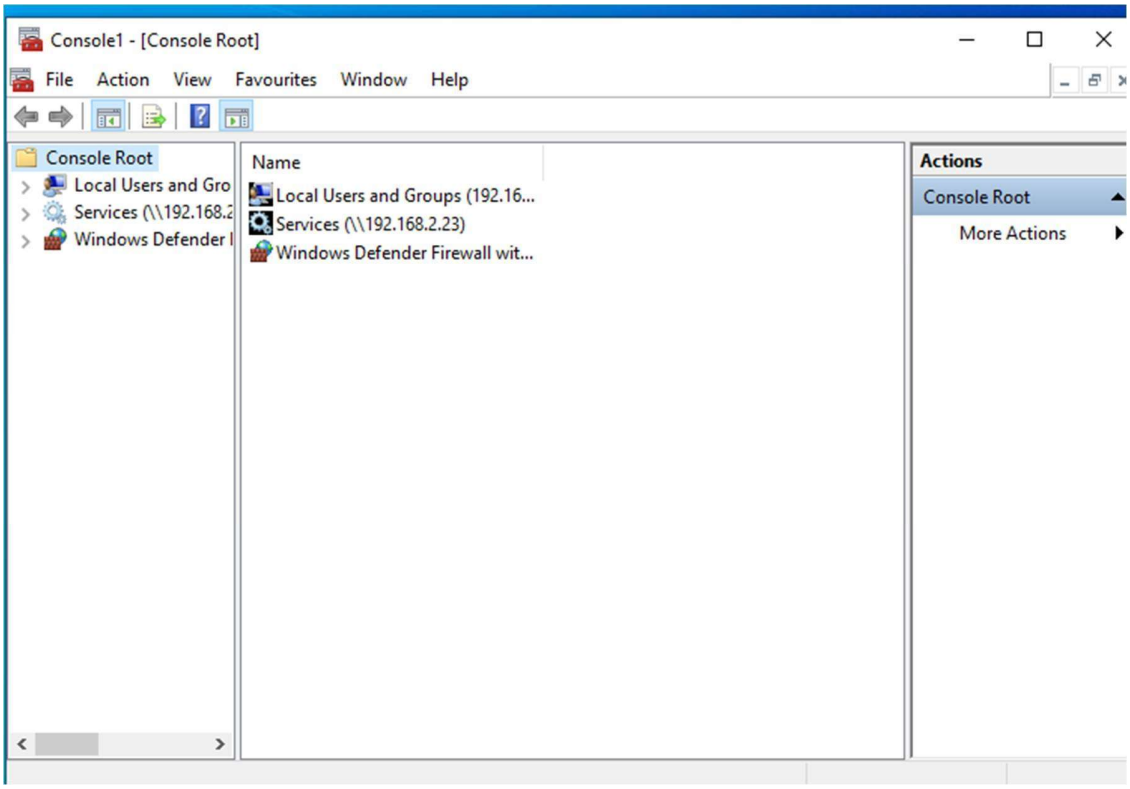
```
PS C:\Windows\system32> Get-NetFirewallRule | Where-Object DisplayName -eq "RDP Management Subnet"


Name                          : {bfabf4b7-26bb-43f8-9fa0-662e80511e92}
DisplayName                   : RDP Management Subnet
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : False
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
```

PART 2

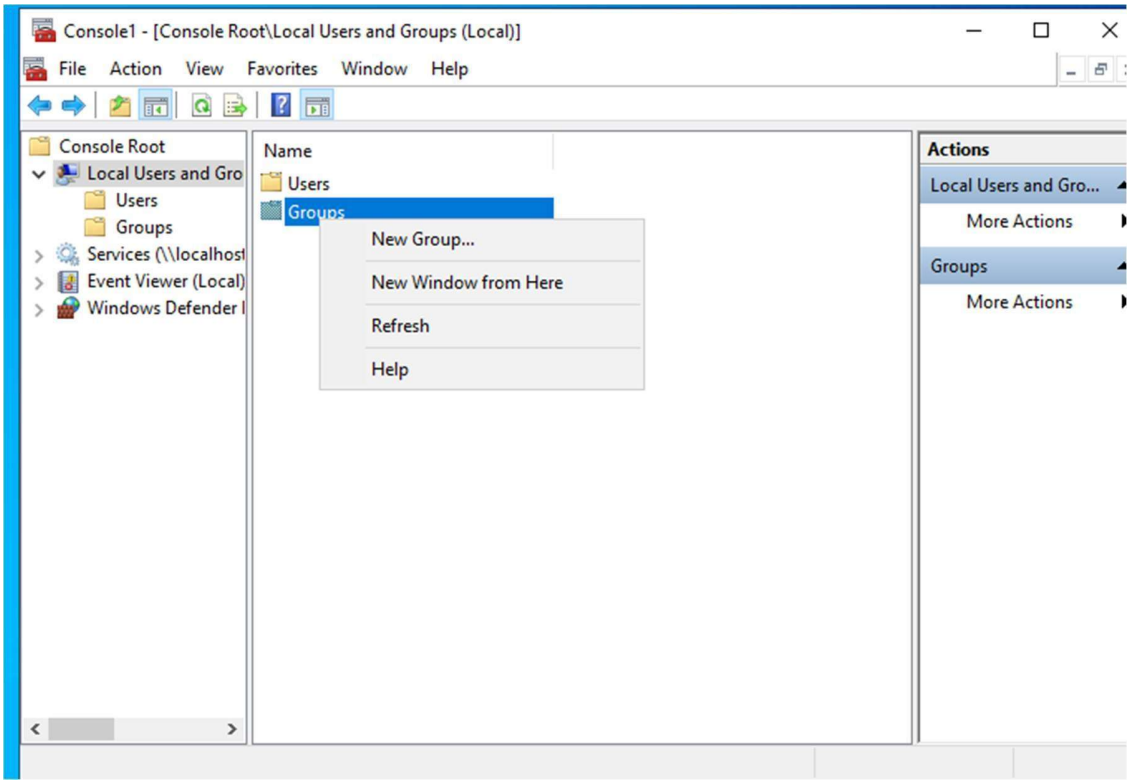
MICROSOFT MANAGEMENT CONSOLE (MMC)

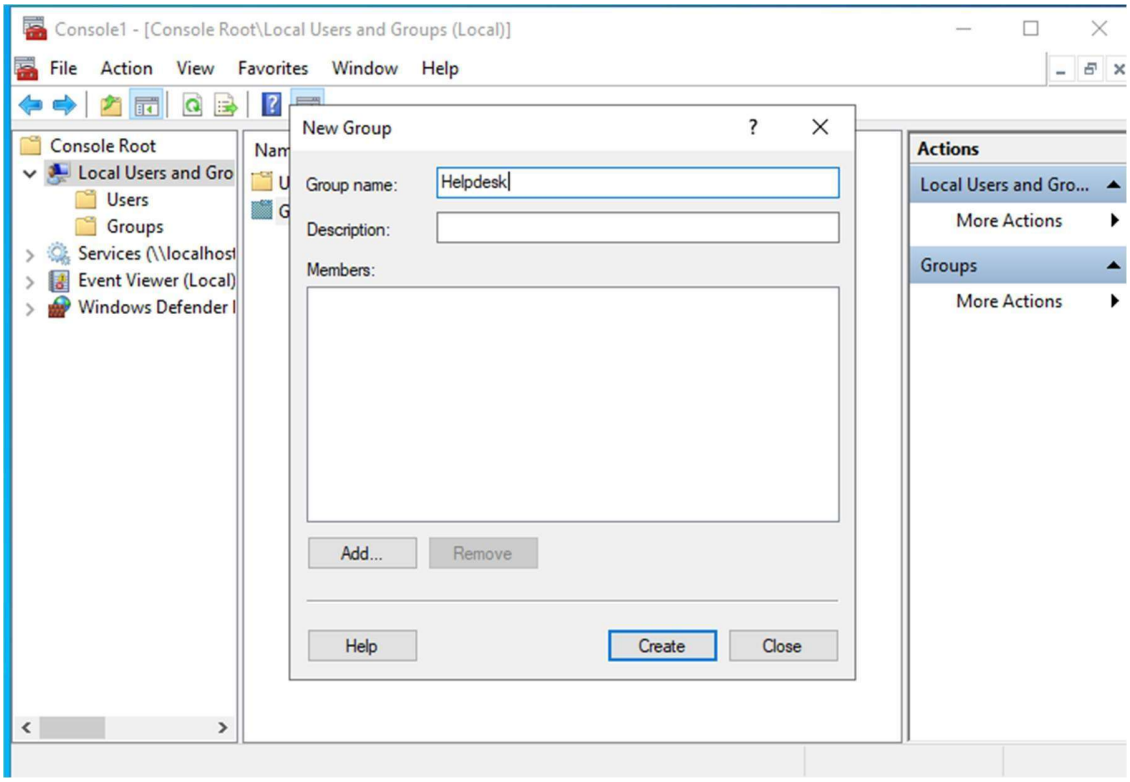
LOCAL USERS AND GROUPS

Firstly adding all the service snap-ins

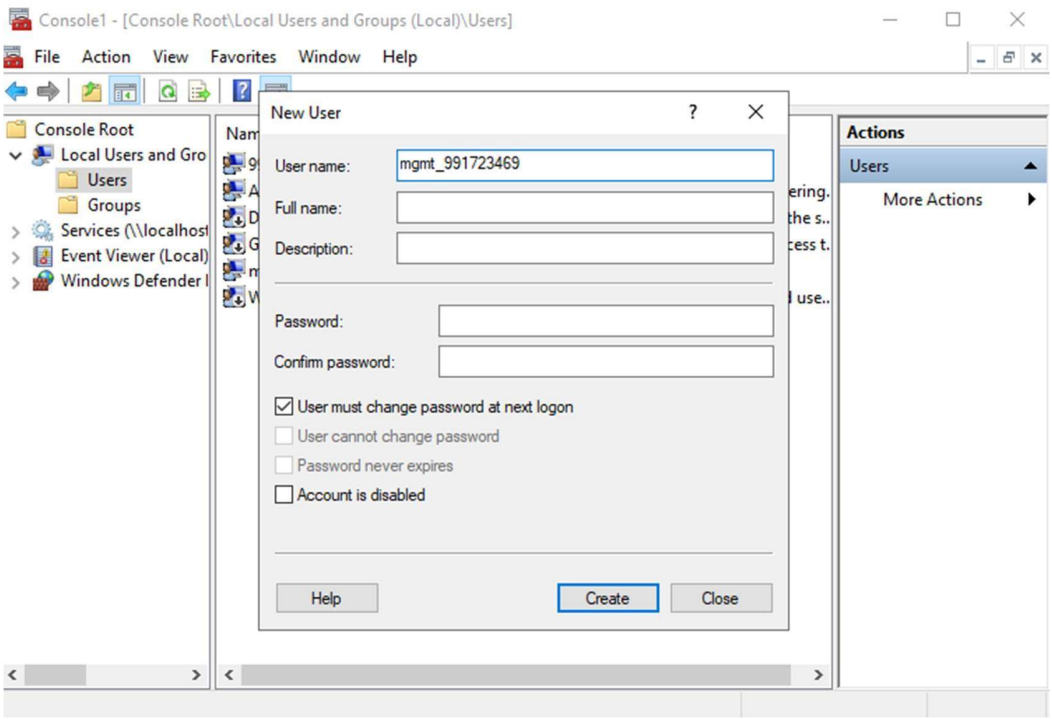


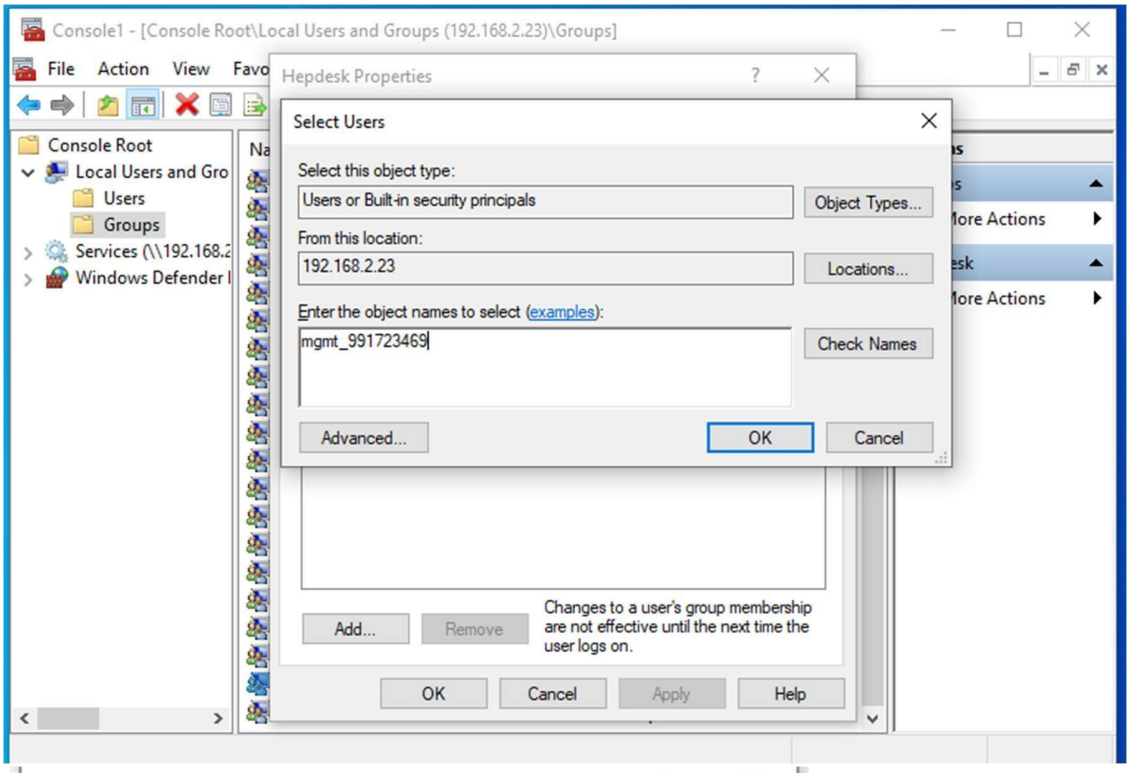
Adding a new group and adding the user to the helpdesk group

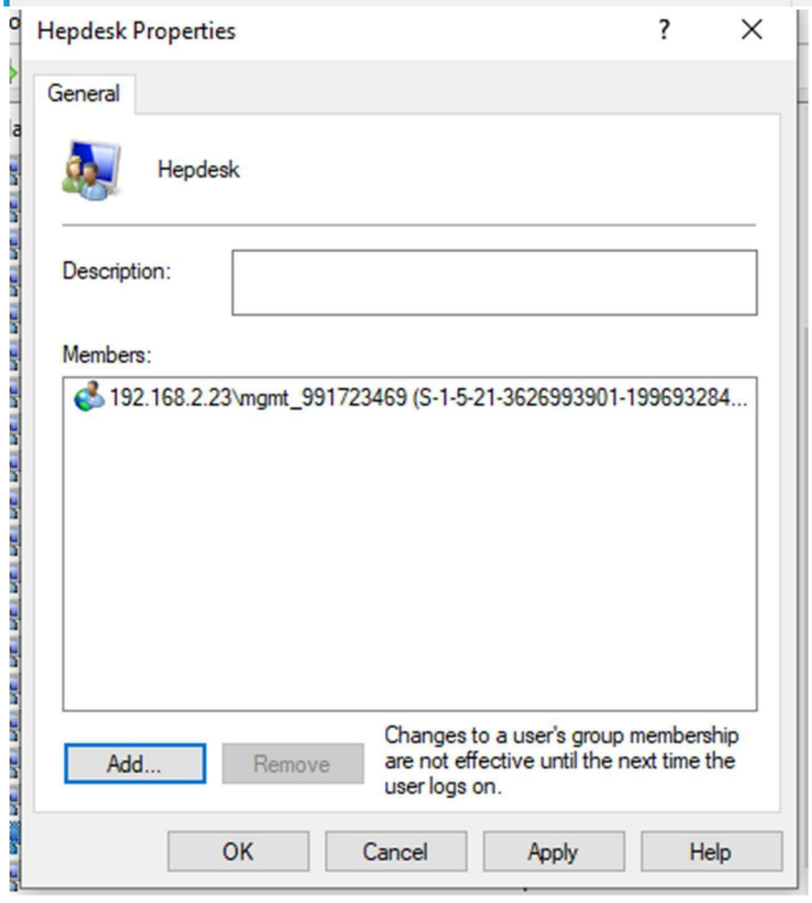




Adding new user

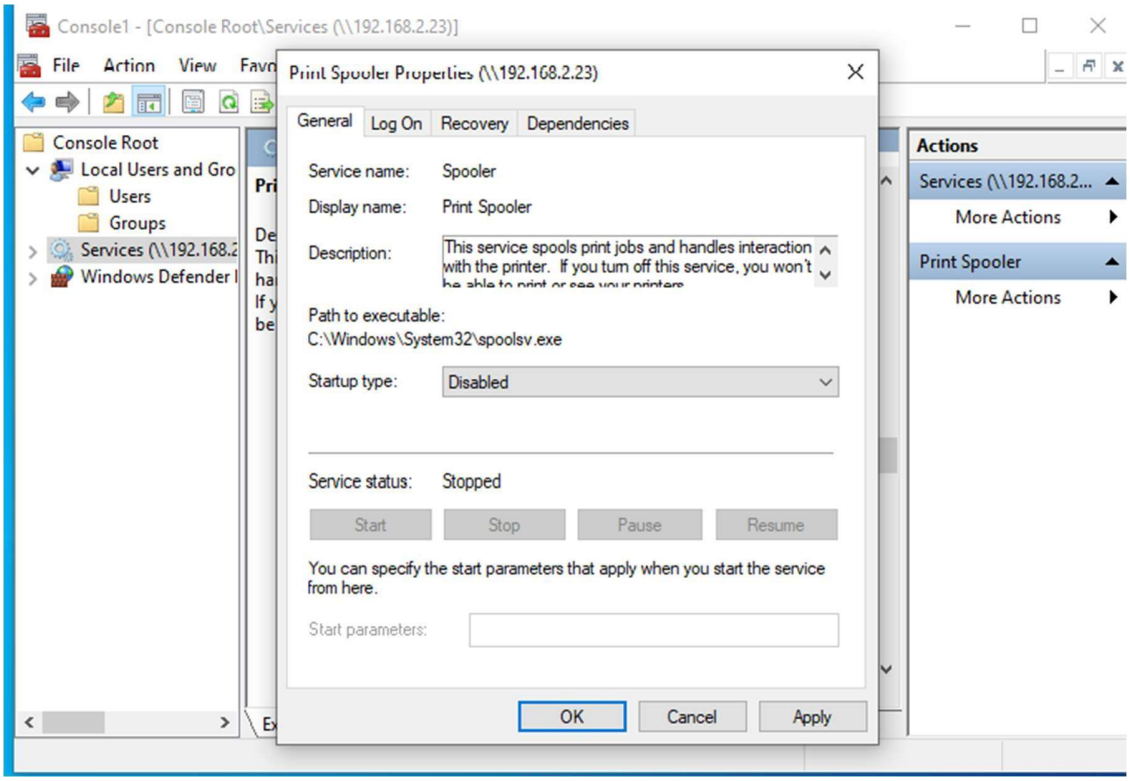


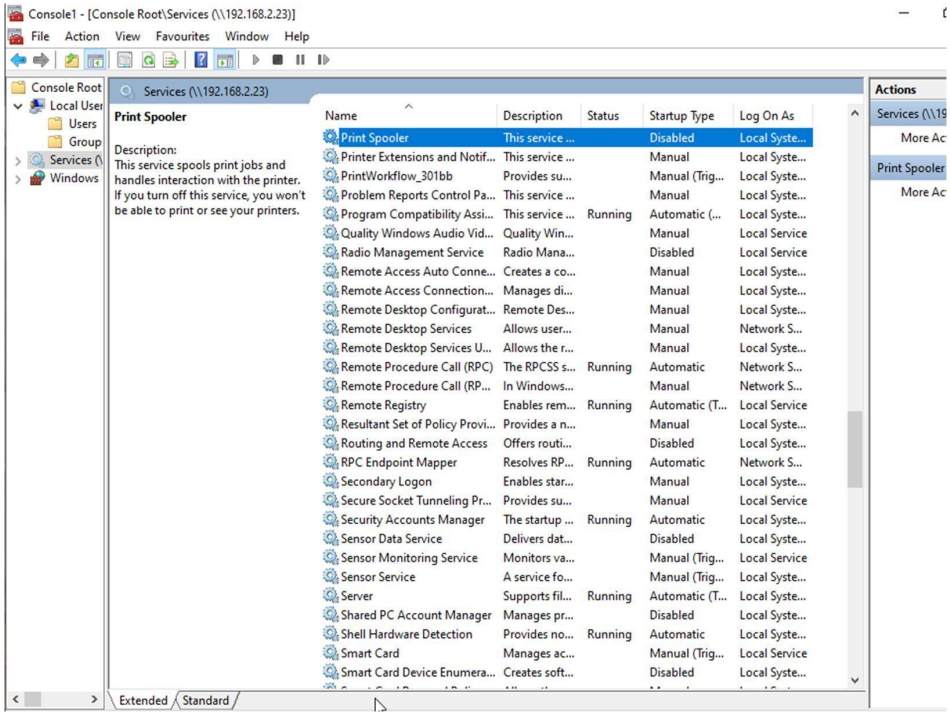

Console1 - [Console Root\Local Users and Groups (192.168.2.23)\Groups]
File Action View Favo
Console Root
Local Users and Gro
Users
Groups
Services (\\192.168.2
Windows Defender
Hepdesk Properties
Select Users
Select this object type:
Users or Built-in security principals
Object Types...
From this location:
192.168.2.23
Locations...
Enter the object names to select (examples):
mgmt_991723469
Check Names
Advanced...
OK
Cancel
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
More Actions
More Actions


Hepdesk Properties
General
Hepdesk
Description:
Members:
192.168.2.23\mgmt_991723469 (S-1-5-21-3626993901-199693284...
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

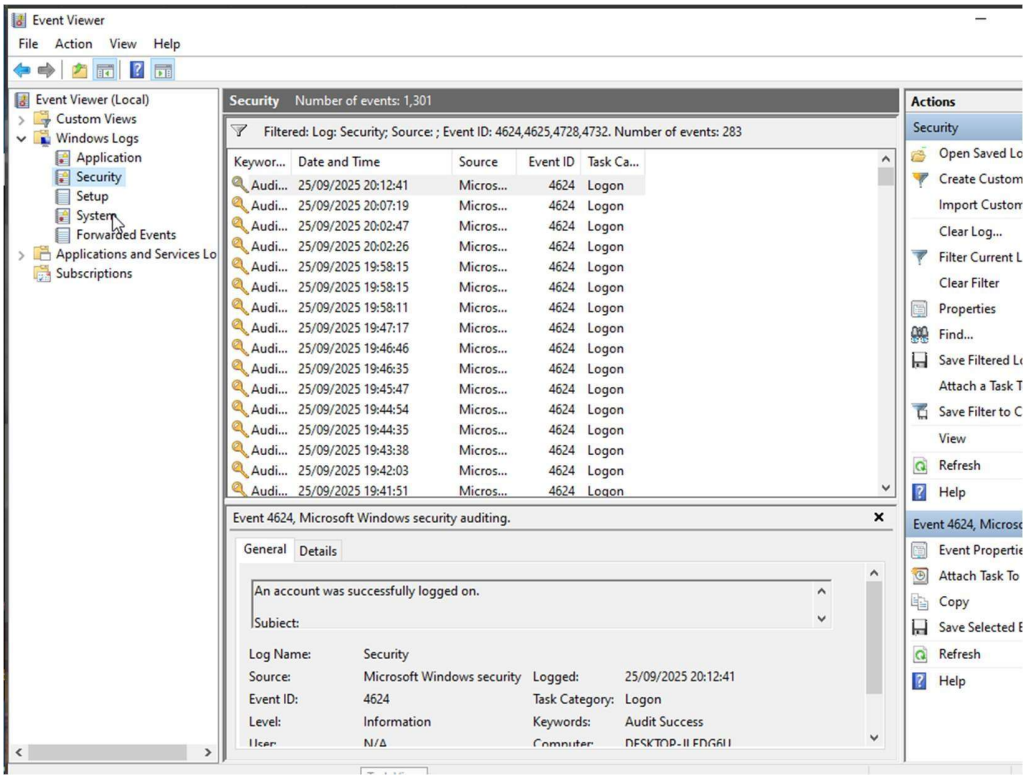
SERVICES

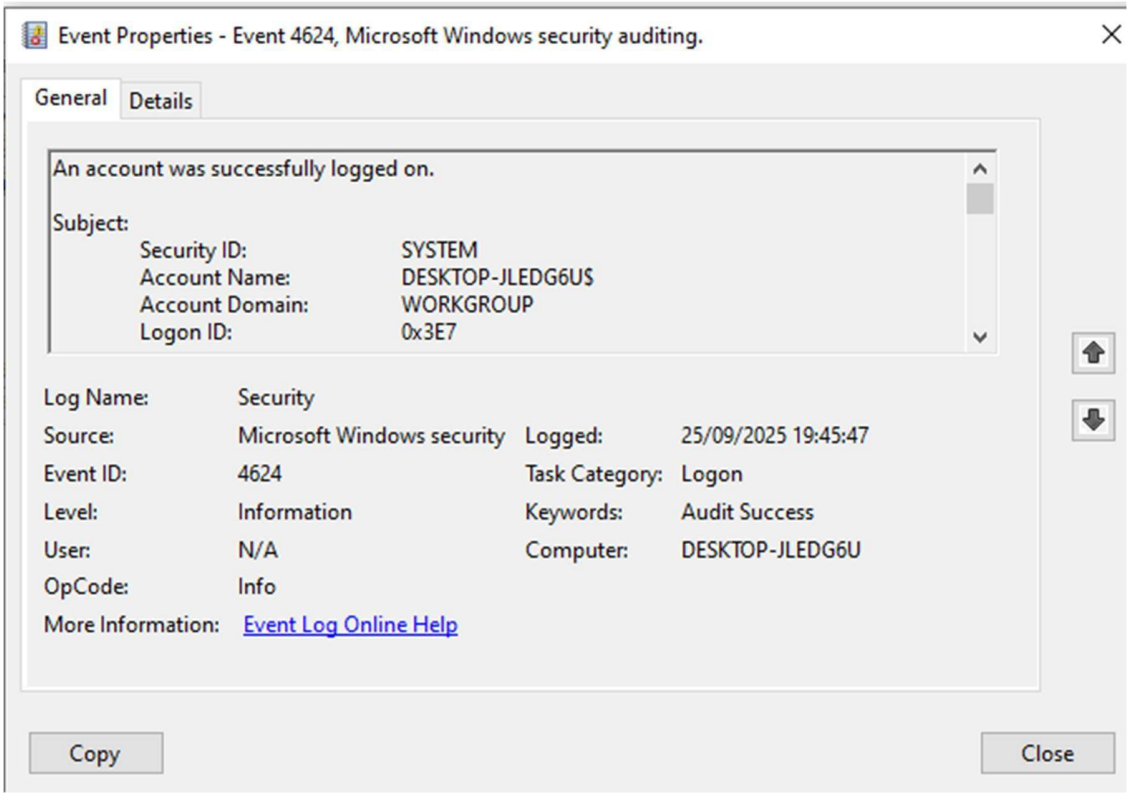
Print spooler configuration

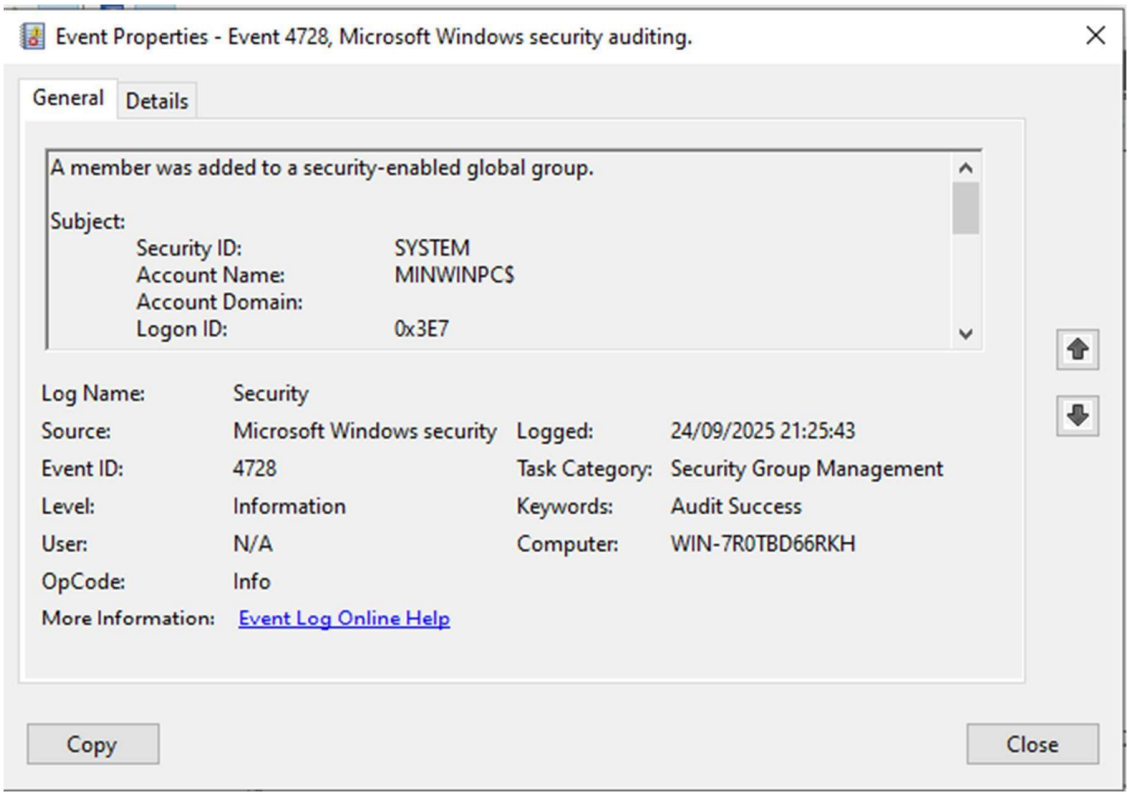




SECURITY EVENT LOGS



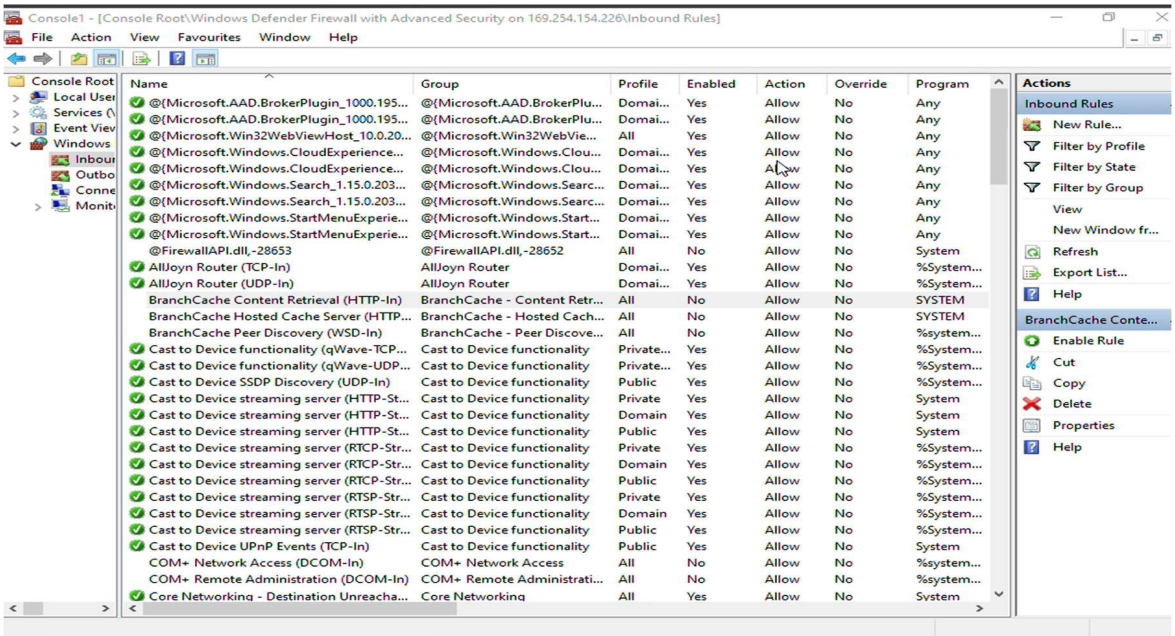


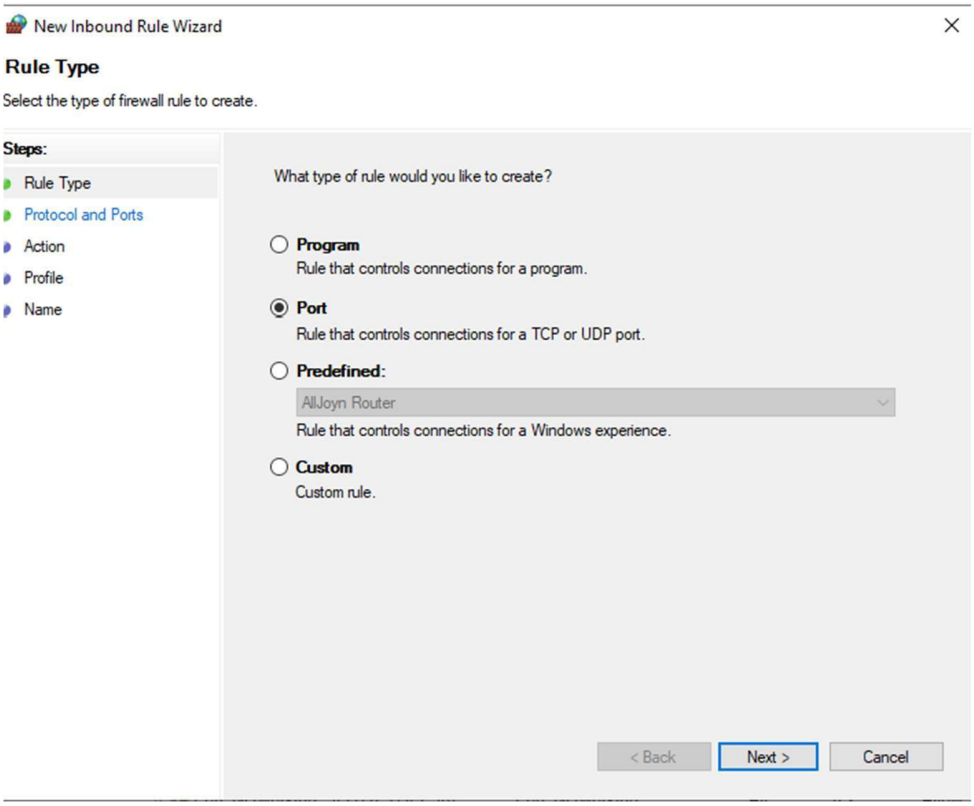


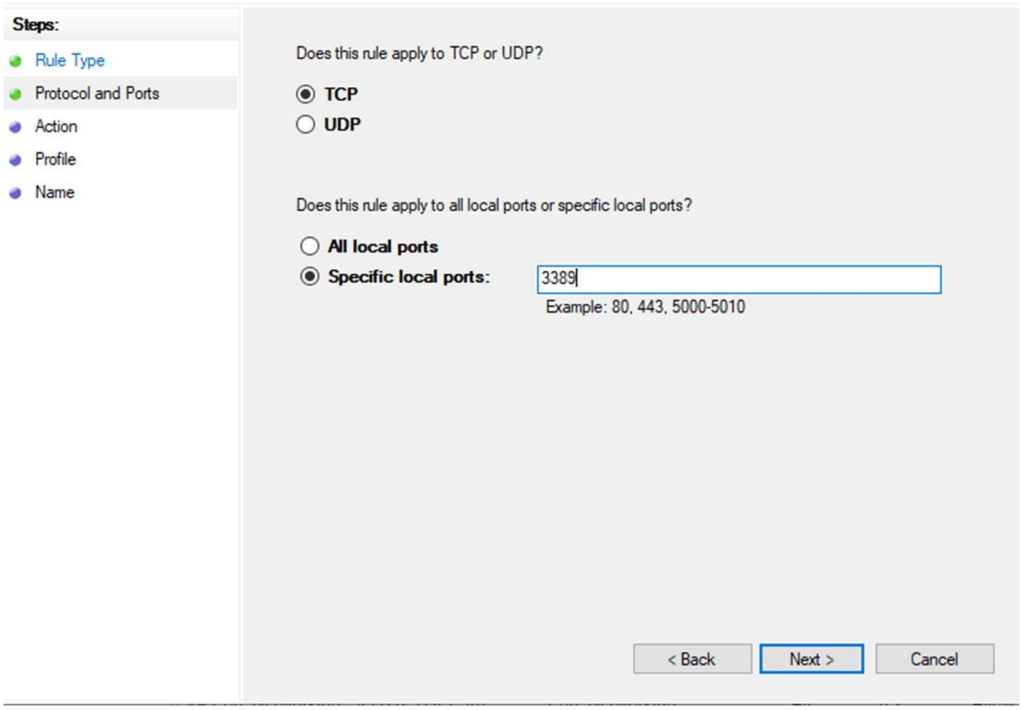
FIREWALL RULE

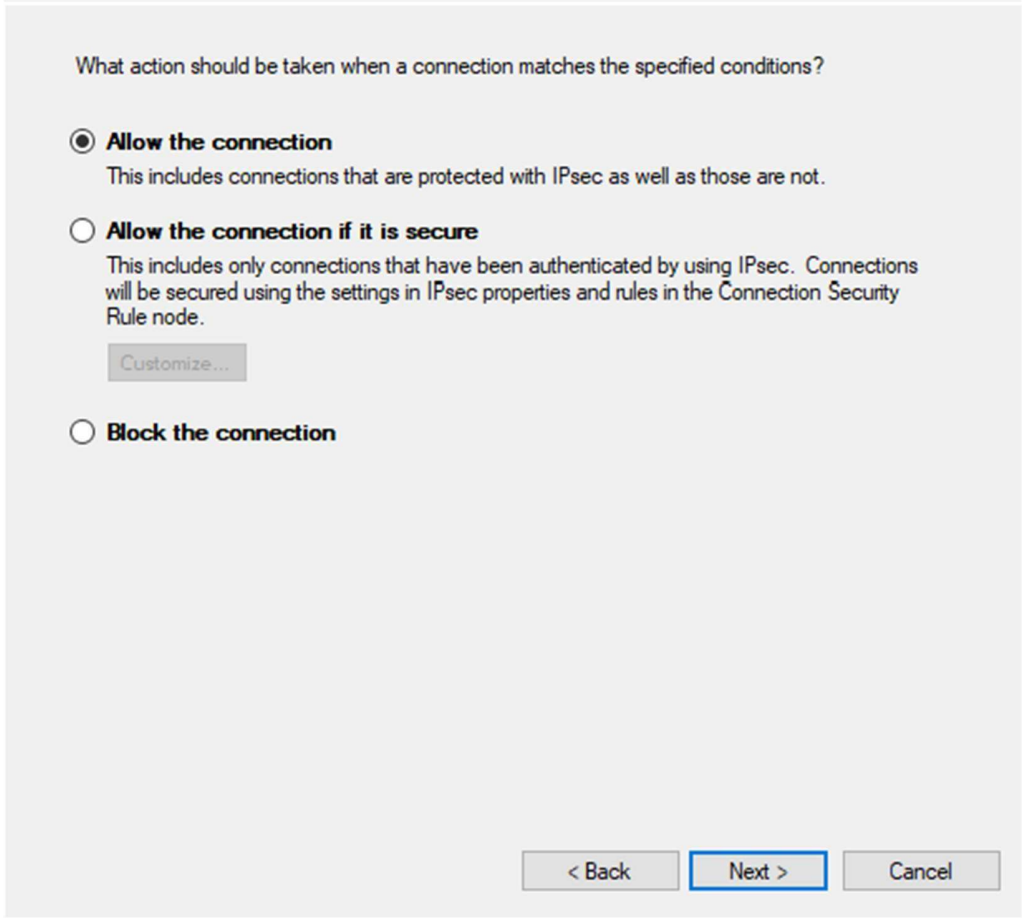
So for this part, I could not open firewall from the management server so I just connected to localhost on my Windows 2022 server and configured all rules from there

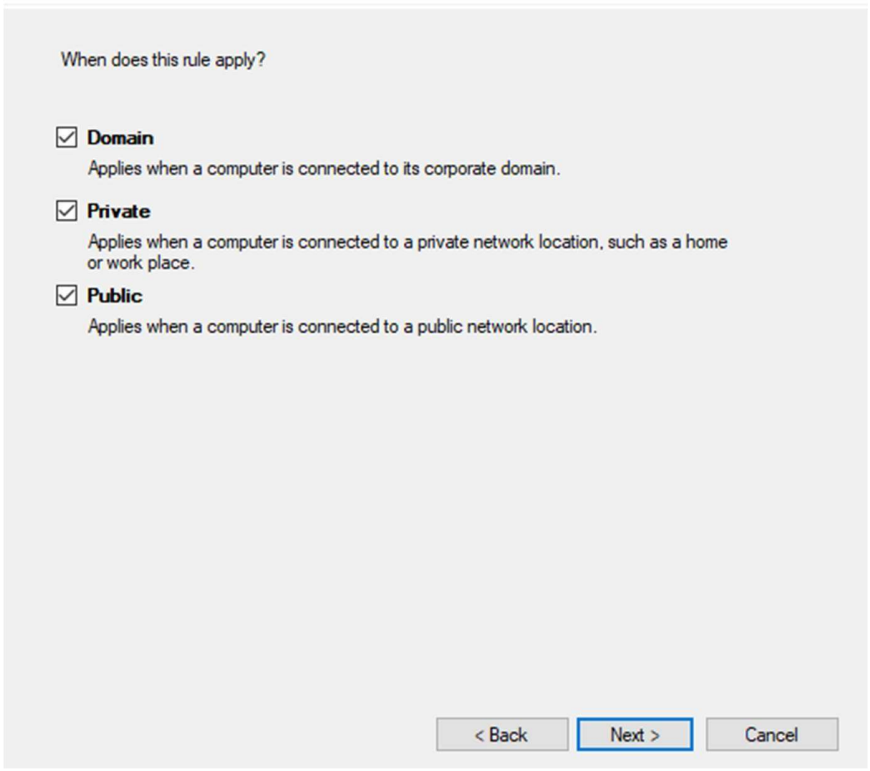
Creating a new rule in windows firewall

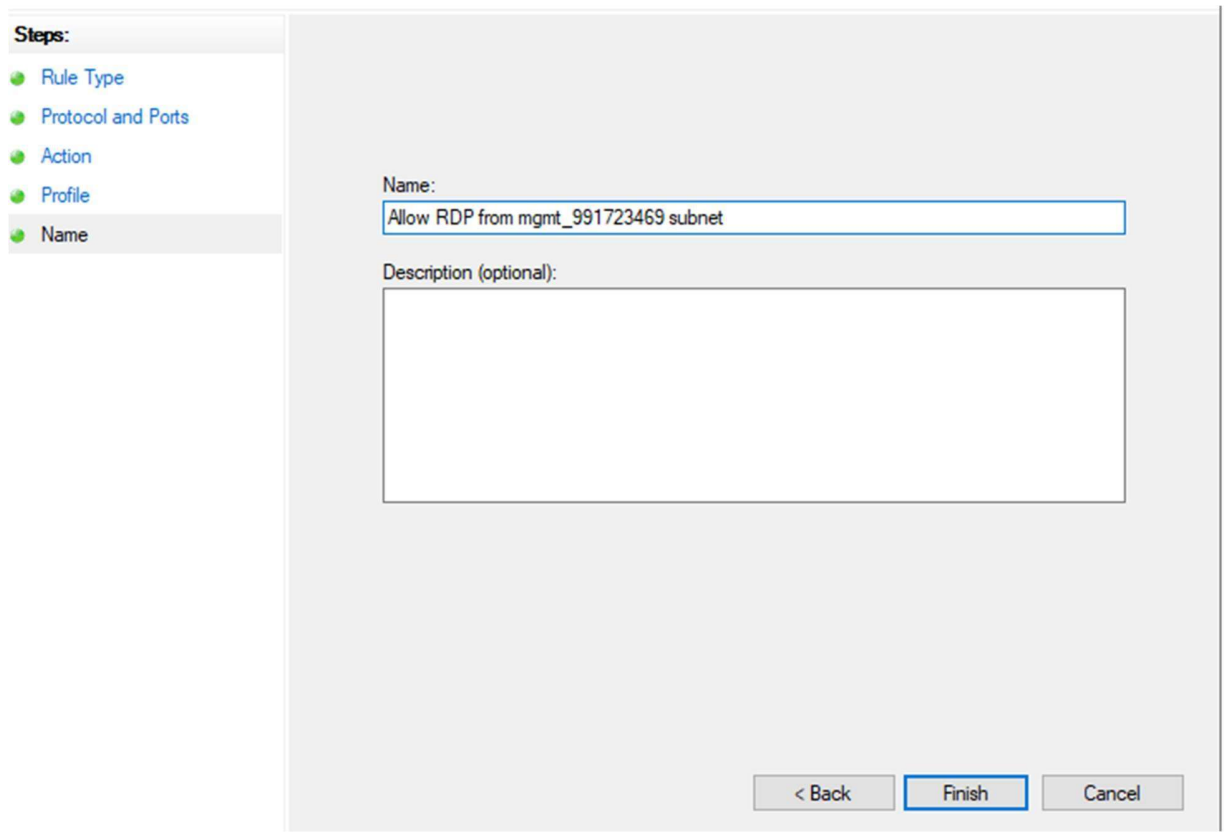


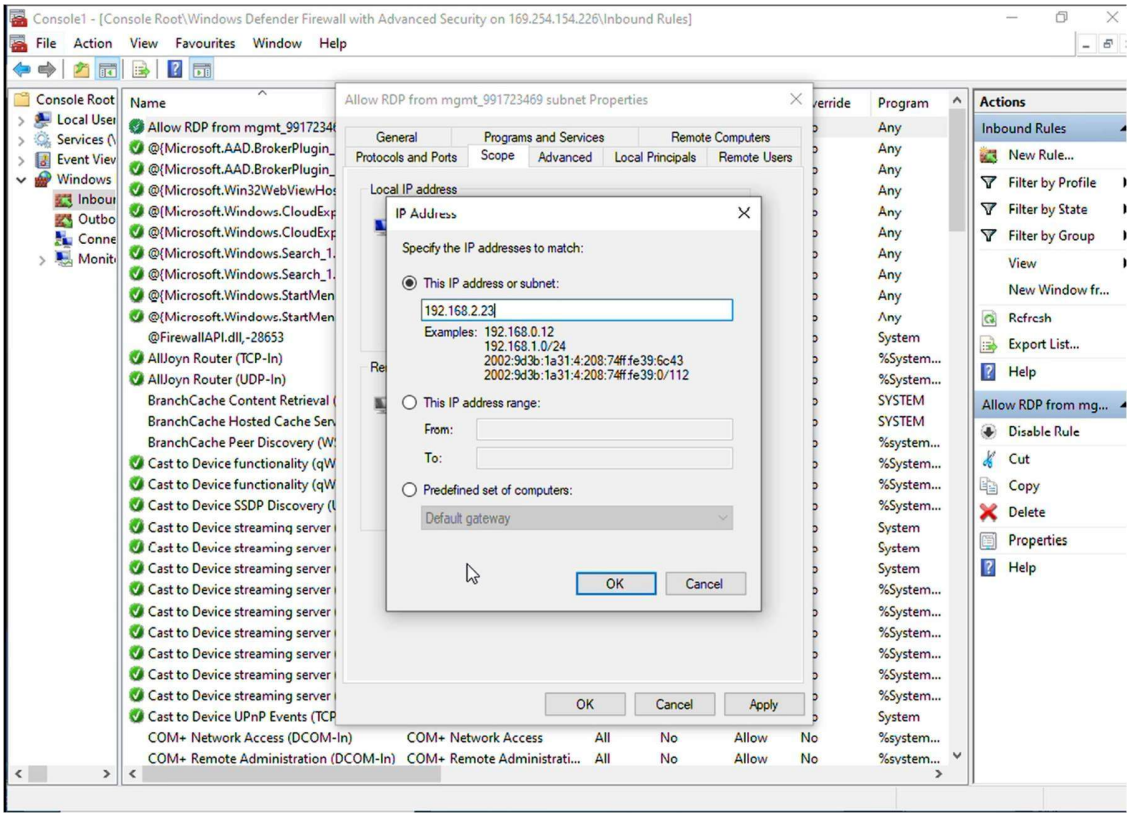

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
3389
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel


Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Allow RDP from mgmt_991723469 subnet
Description (optional):
< Back
Finish
Cancel

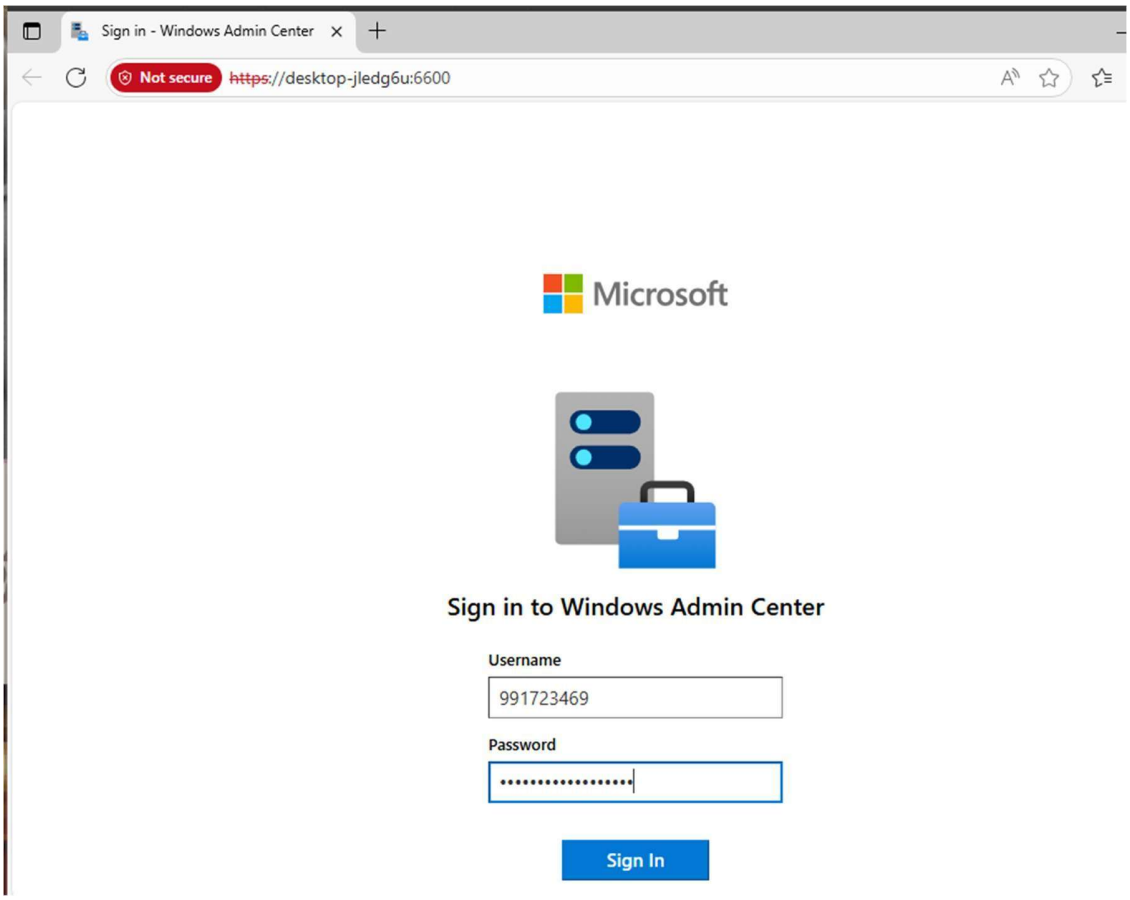


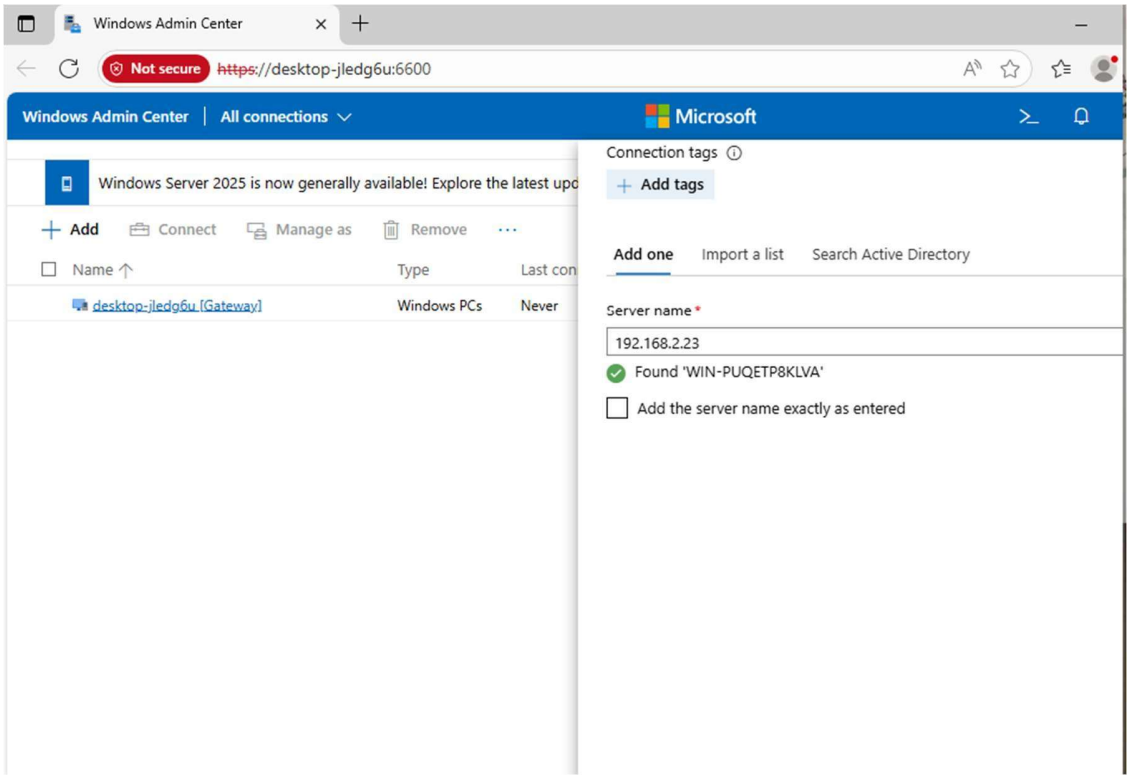
Name	Group	Profile	Enabled	Action	Override	Program
Allow RDP from mgmt_991723469 subnet		All	No	Allow	No	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any
@{Microsoft.Win32WebViewHost_10.0.20...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any
@{Microsoft.Windows.Search_1.15.0.203...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any
@{Microsoft.Windows.Search_1.15.0.203...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any
@FirewallAPI.dll,-28653	@FirewallAPI.dll,-28652	All	No	Allow	No	System
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...

PART 3

WINDOWS ADMIN CENTER (WAC)

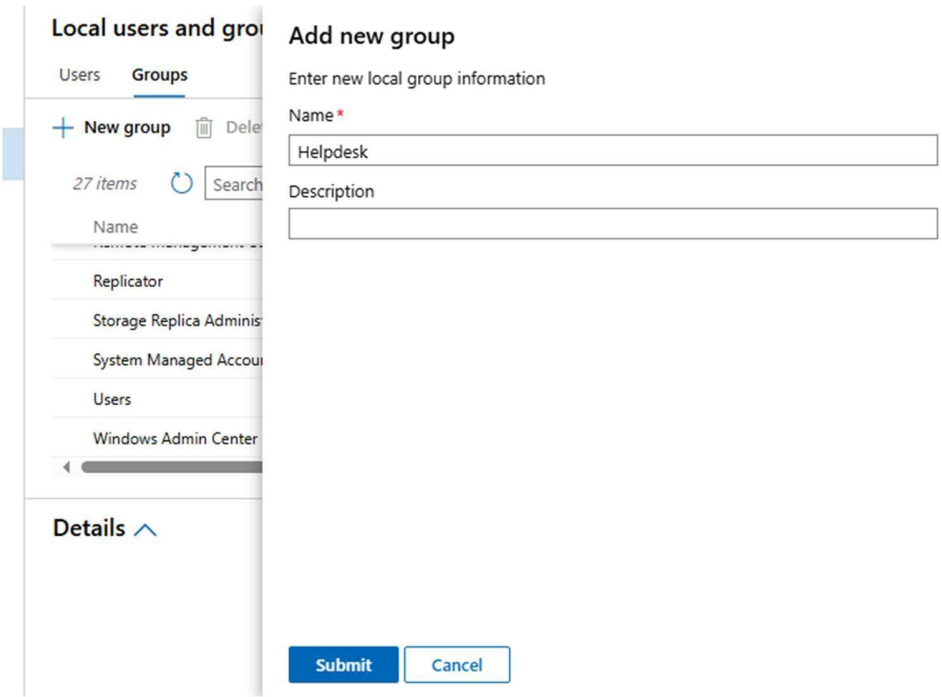
Login into WAC



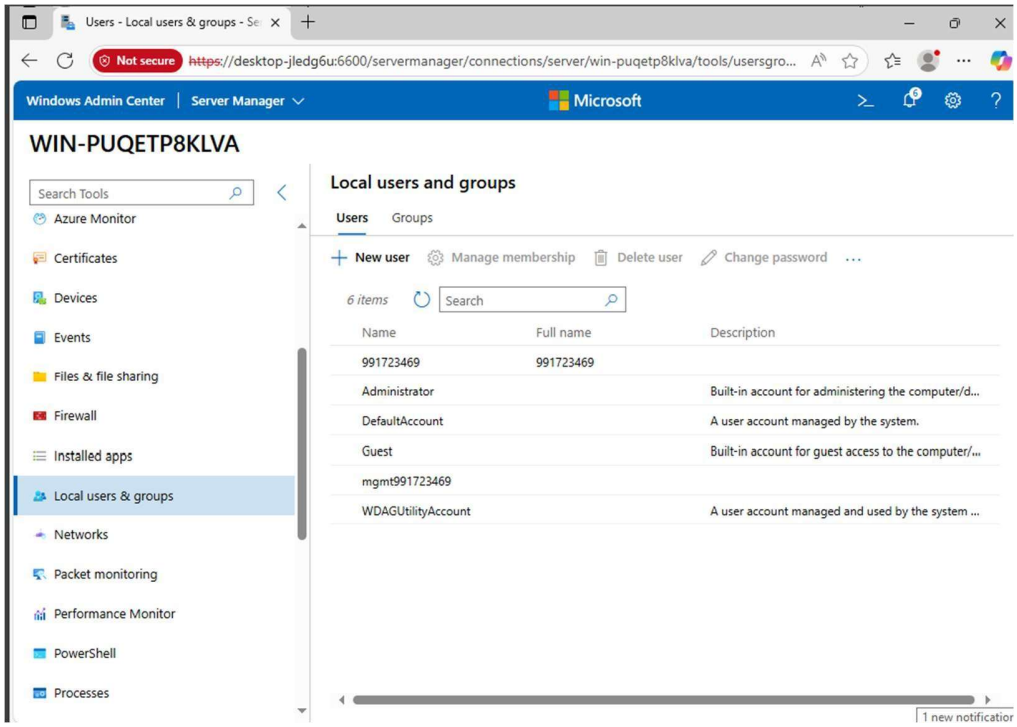


LOCAL USERS AND GROUPS

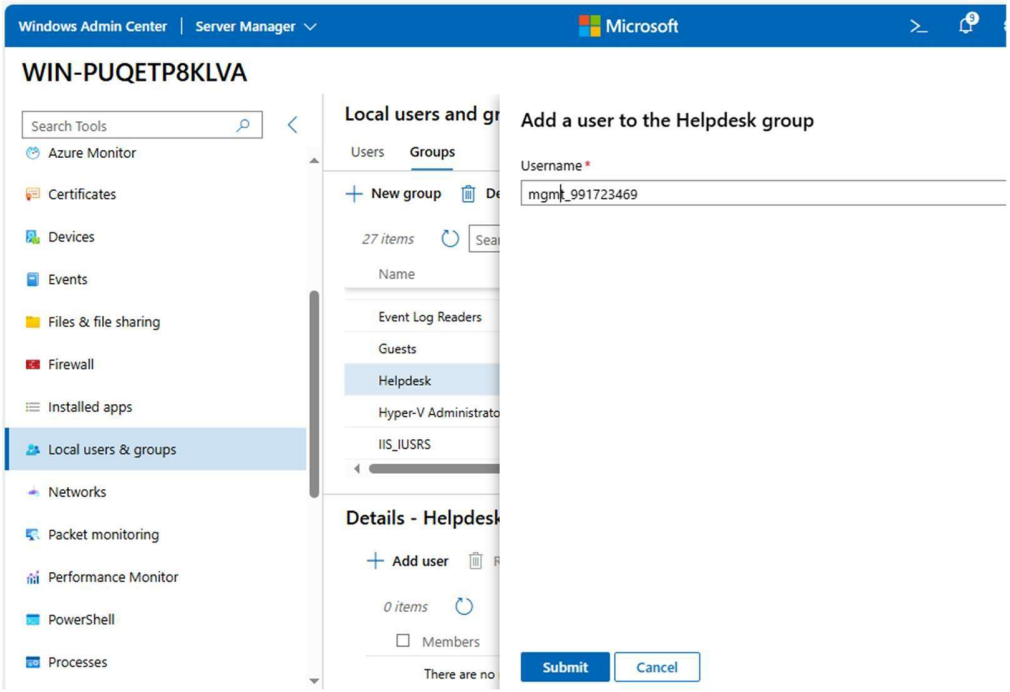
Adding a group called Helpdesk and adding the user

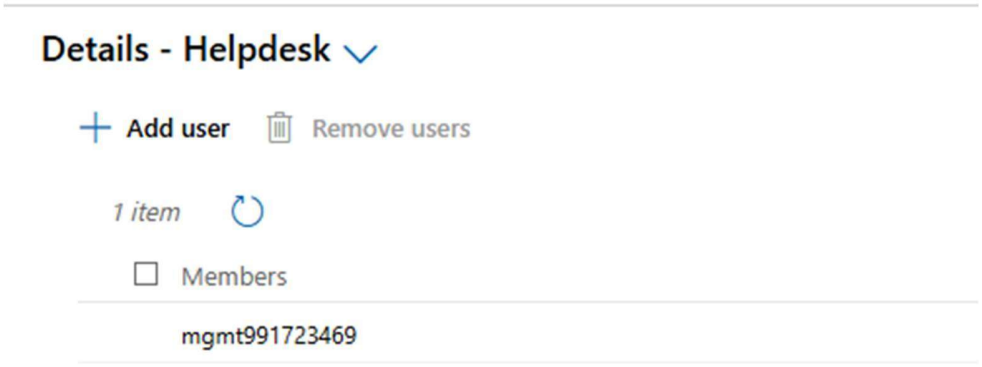


Adding a new user



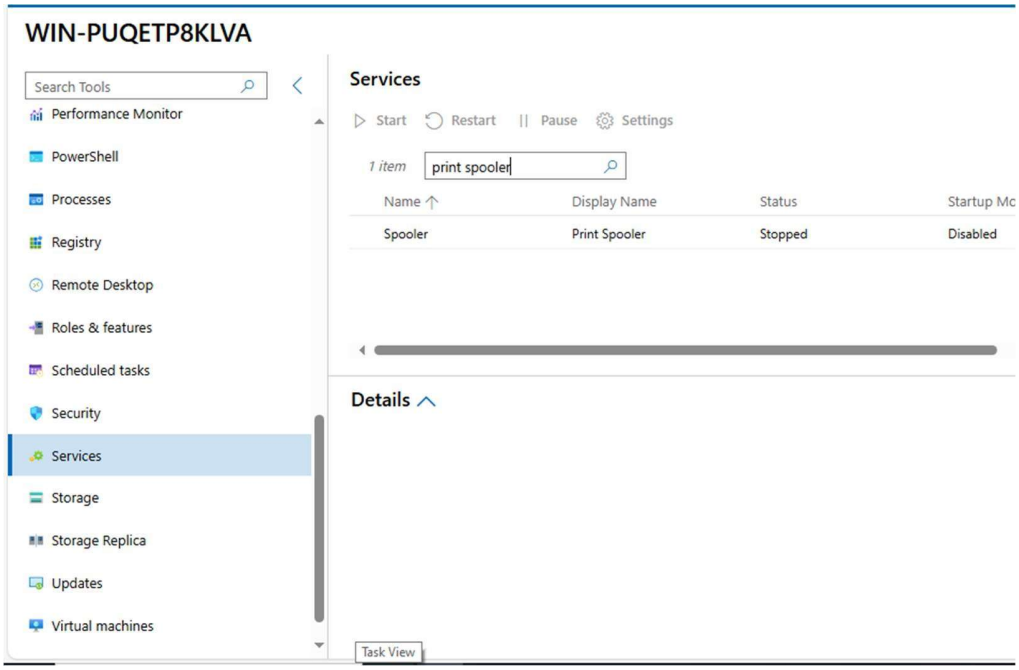
Adding user to helpdesk group





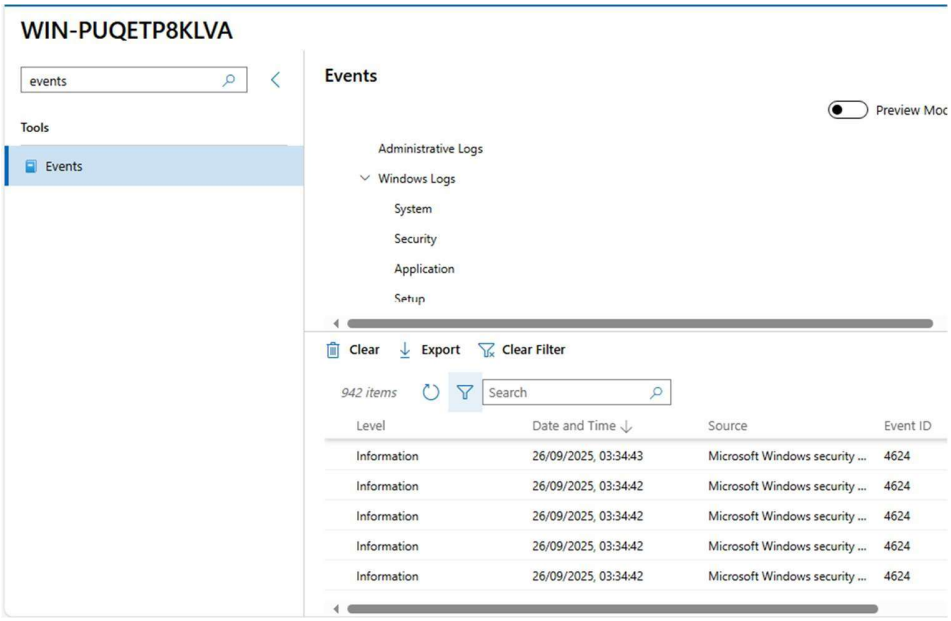
SERVICES

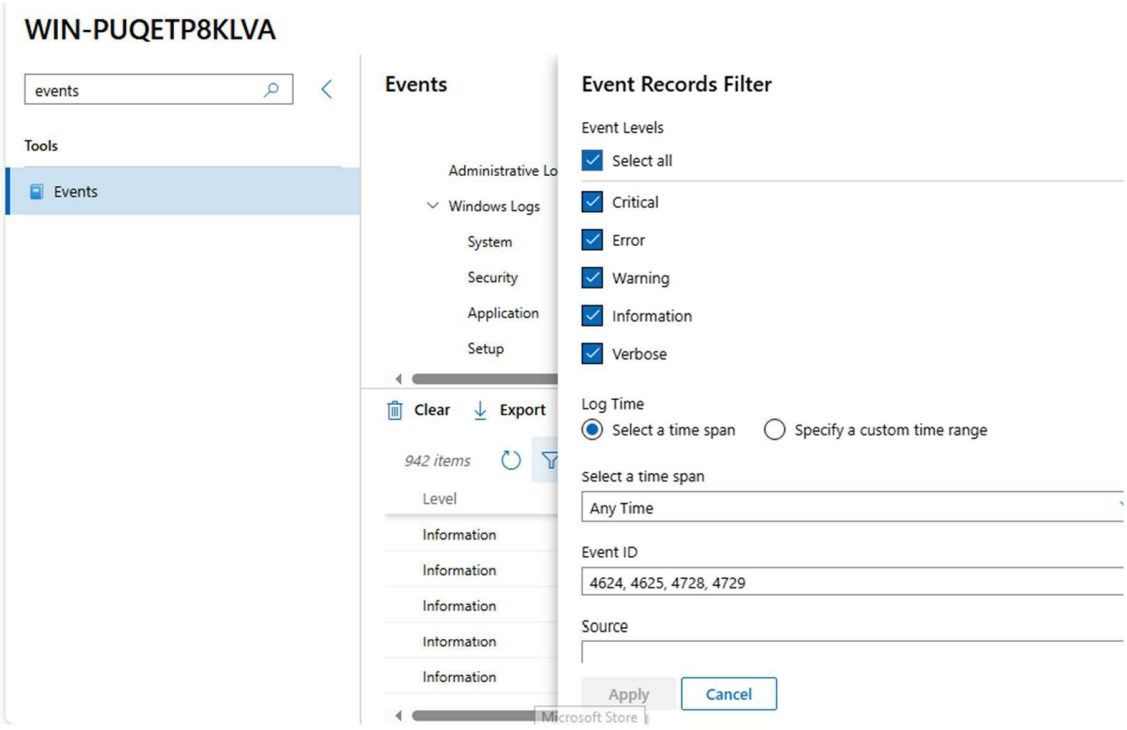
Disabling the print spooler



SECURITY EVENT LOGS

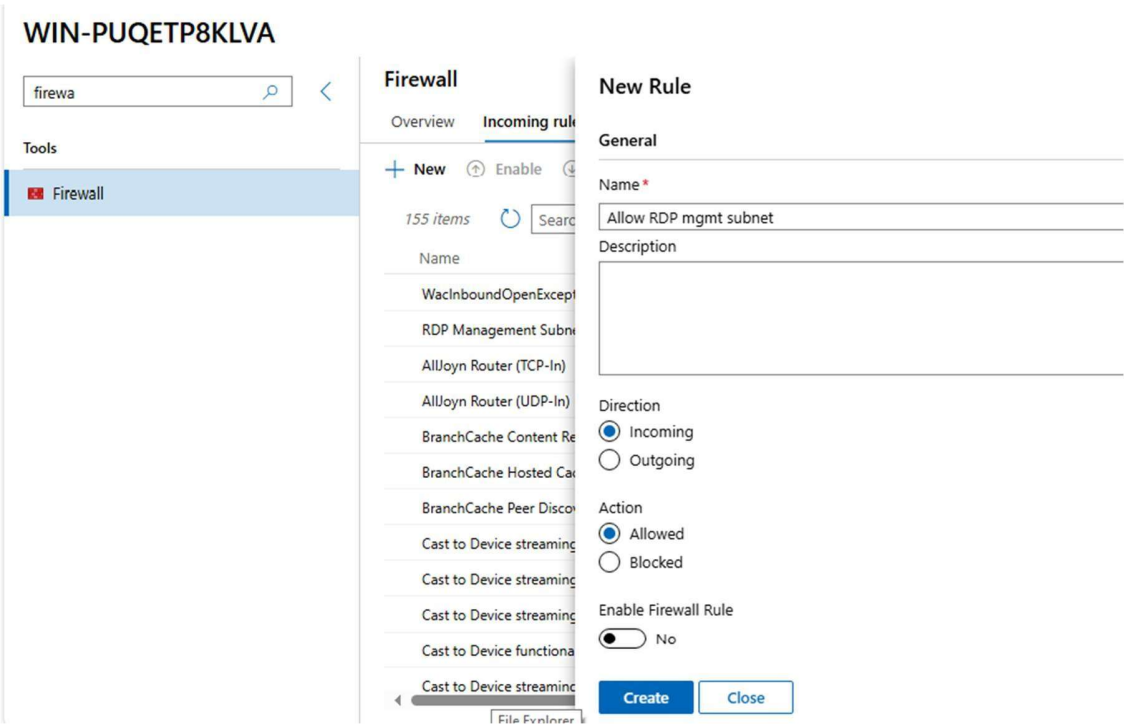
Applying a filter to sort by event id





FIREWALL RULE

Creating a new inbound rule in firewall

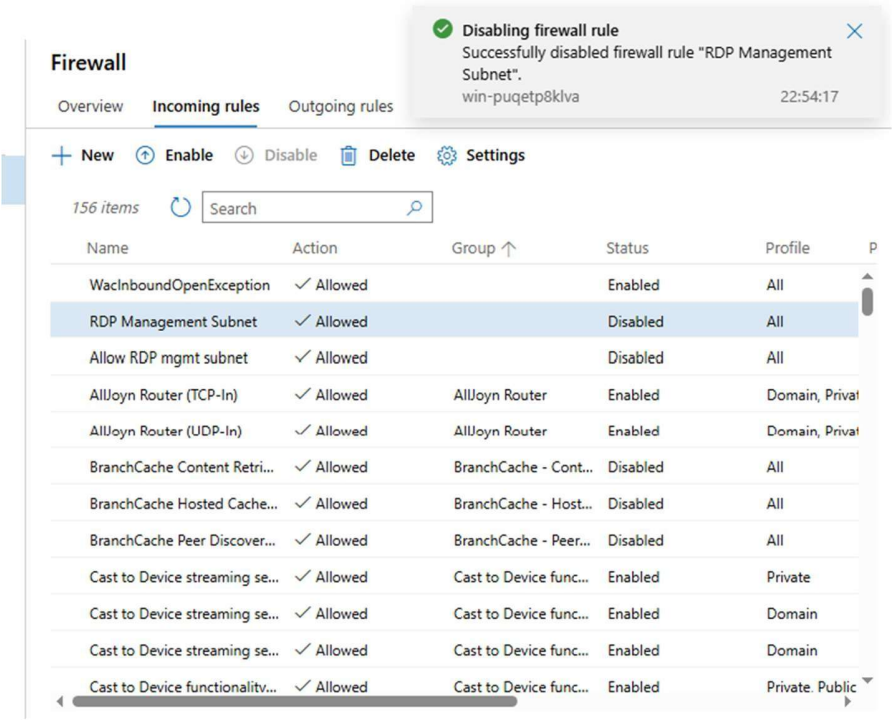


Name	Action	Group	Status	Profile
WacInboundOpenException	✓ Allowed		Enabled	All
RDP Management Subnet	✓ Allowed		Enabled	All
Allow RDP mgmt subnet	✓ Allowed		Disabled	All
AllJoyn Router (TCP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Privat
AllJoyn Router (UDP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Privat
BranchCache Content Retri...	✓ Allowed	BranchCache - Cont...	Disabled	All
BranchCache Hosted Cache...	✓ Allowed	BranchCache - Host...	Disabled	All
BranchCache Peer Discover...	✓ Allowed	BranchCache - Peer...	Disabled	All
Cast to Device streaming se...	✓ Allowed	Cast to Device func...	Enabled	Private
Cast to Device streaming se...	✓ Allowed	Cast to Device func...	Enabled	Domain
Cast to Device streaming se...	✓ Allowed	Cast to Device func...	Enabled	Domain

IP addresses

Local IP addresses	Any
Remote IP addresses	192.168.1.0/255.255.255.0
Interface alias	Any
Interface type	All

Disabling the rule after



Reflection (5–7 sentences)

- A short comparison table of PowerShell vs MMC vs WAC (columns: speed, auditability, security).

METHOD	SPEED	AUDITABILITY	SECURITY
POWERSHELL	Fast and scriptable	High (logs)	Strong encryption techniques but
			requires more privilege control
MMC	Medium/ manual	Low (minimized logging)	Weak (outdated protocols)
WAC	Medium	High (balanced audit logs)	Strong encryption methods and secure by default

- Which method would I adopt in a security-conscious environment, and why?

  Based on my observation, while doing the lab, I found it easier to do the lab using WAC method as it provided the best balance between usability and security with built in HTTPS, RBAC and good logging features. It is more centralized and has more modern encryption methods. PowerShell on the other hand is the fastest and most automatable option but MMC is more outdated and has weaker encryption standards.