

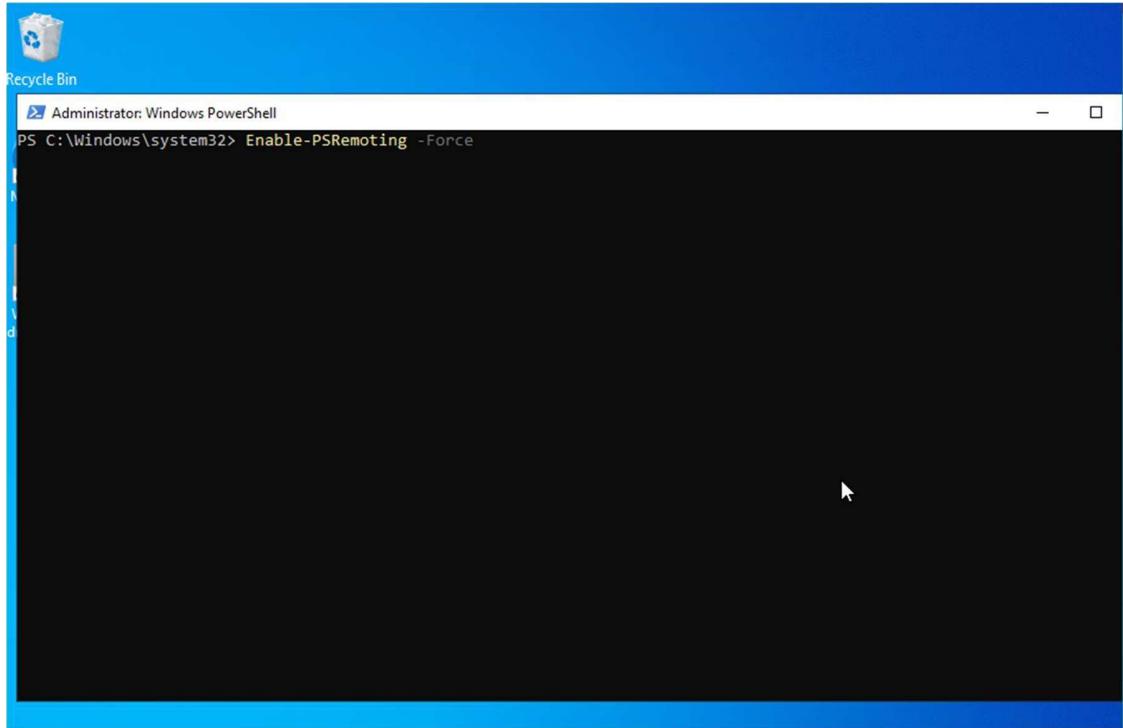
Name: Mahimaa Vardini Balaji Ramathaal

Management server: Windows 10

Remote server : Windows 2022

PART 1

WINDOWS POWERSHELL ADMINISTRATION



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Enable-PSRemoting -Force
```

LOCAL USERS AND GROUPS

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Enter-PSSession -ComputerName 192.168.2.23 -Credential "WIN-PUQETP8KLVA\Administrator"
[192.168.2.23]: PS C:\Users\Administrator\Documents> New-LocalGroup -Name "Helpdesk" -Description "Helpdesk group"
New-LocalGroup : Group Helpdesk already exists.
+ CategoryInfo          : ResourceExists: (Helpdesk:String) [New-LocalGroup], GroupExistsException
+ FullyQualifiedErrorId : GroupExists,Microsoft.PowerShell.Commands.NewLocalGroupCommand
[192.168.2.23]: PS C:\Users\Administrator\Documents> New-LocalGroup -Name "Helpdesk" -Description "Helpdesk group"
Name      Description
----      -----
Helpdesk  Helpdesk group

[192.168.2.23]: PS C:\Users\Administrator\Documents> New-LocalUser -Name "mgmt_991723469" -Password (Read-Host -AsSecureString "Enter Password") -FullName "Mgmt User"
WARNING: A script or application on the remote computer 192.168.2.23 is sending a prompt request. When you are prompted, enter sensitive information, such as credentials or passwords, only if you trust the remote computer and the application or script that is requesting the data.
Enter Password: *****
Name      Enabled Description
----      ----- -----
mgmt_991723469 True

[192.168.2.23]: PS C:\Users\Administrator\Documents> Add-LocalGroupMember -Group "Helpdesk" -Member "mgmt_991723469"
[192.168.2.23]: PS C:\Users\Administrator\Documents>
```

Checking if everything worked on Windows 2022

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-LocalGroup | Where-Object Name -eq "Helpdesk"
Name      Description
----      -----
Helpdesk  Helpdesk group

PS C:\Windows\system32> Get-LocalUser | Where-Object Name -eq "mgmt_991723469"
Name      Enabled Description
----      ----- -----
mgmt_991723469 True

PS C:\Windows\system32> Get-LocalGroupMember -Group "Helpdesk"
ObjectClass Name          PrincipalSource
----          -----
User        WIN-PUQETP8KLVA\mgmt_991723469 Local
```

SERVICES

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

```
[Select Administrator: Windows PowerShell
[192.168.2.23]: PS C:\Users\Administrator\Documents> Set-Service -Name "Spooler" -StartupType Disabled
[192.168.2.23]: PS C:\Users\Administrator\Documents> Stop-Service -Name "Spooler"
[192.168.2.23]: PS C:\Users\Administrator\Documents> Get-Service -Name "Spooler" | Select-Object Status, StartType
Status StartType
-----
Stopped Disabled

[192.168.2.23]: PS C:\Users\Administrator\Documents>
```

Checking from remote server

```
[Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Service Spooler | Select-Object Name, Status, StartType
Name      Status StartType
----      ----- -----
Spooler   Stopped Disabled
```

SECURITY EVENT LOGS

View security event logs

Logon Success / failure events – 4624 / 4625

Group membership changes - 4728

```
[Administrator: Windows PowerShell
[192.168.2.23]: PS C:\Users\Administrator\Documents> Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -or $_.Id -eq 4625} | Select-Object TimeCreated, Id, Message -First 10
TimeCreated          Id Message
-----
24/09/2025 23:42:18 4624 An account was successfully logged on....
24/09/2025 23:42:18 4624 An account was successfully logged on....
24/09/2025 23:49:25 4624 An account was successfully logged on....
24/09/2025 23:40:25 4624 An account was successfully logged on....
24/09/2025 23:39:11 4624 An account was successfully logged on....
24/09/2025 23:38:34 4624 An account was successfully logged on....
24/09/2025 23:38:34 4624 An account was successfully logged on....
24/09/2025 23:37:01 4624 An account was successfully logged on....
24/09/2025 23:37:00 4624 An account was successfully logged on....
24/09/2025 23:34:07 4624 An account was successfully logged on....
```



```
[192.168.2.23]: PS C:\Users\Administrator\Documents> Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4732 -or $_.Id -eq 4733} | Select-Object TimeCreated, Id, Message -First 10
TimeCreated          Id Message
-----
24/09/2025 23:31:42 4732 A member was added to a security-enabled local group....
24/09/2025 23:25:04 4733 A member was removed from a security-enabled local group....
24/09/2025 23:16:46 4732 A member was added to a security-enabled local group....
19/09/2025 20:09:54 4732 A member was added to a security-enabled local group....
18/09/2025 22:17:25 4732 A member was added to a security-enabled local group....
07/09/2025 19:47:10 4732 A member was added to a security-enabled local group....
07/09/2025 19:46:38 4732 A member was added to a security-enabled local group....
07/09/2025 22:34:19 4732 A member was added to a security-enabled local group....
07/09/2025 22:34:19 4732 A member was added to a security-enabled local group....
07/09/2025 22:34:08 4732 A member was added to a security-enabled local group....
```



```
[192.168.2.23]: PS C:\Users\Administrator\Documents>
```

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"

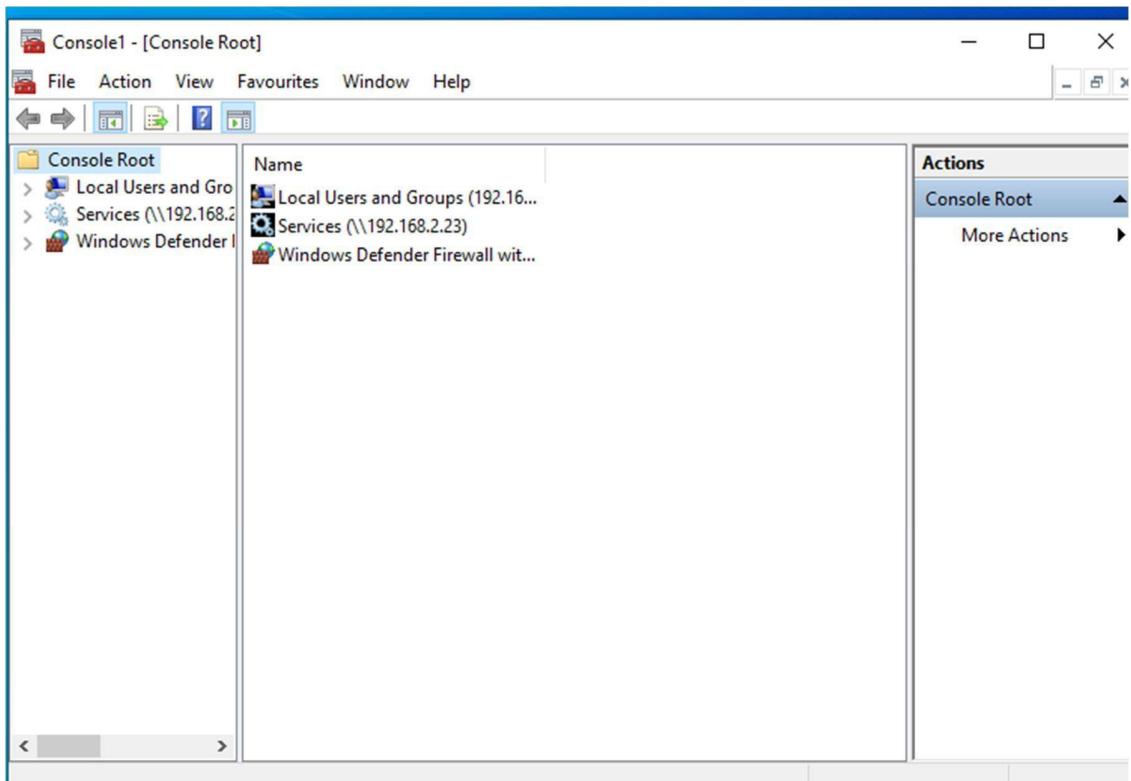
Name : {bfabf4b7-26bb-43f8-9fa0-662e80511e92}
DisplayName : RDP Management Subnet
Description :
DisplayGroup :
Group :
Enabled : False
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus :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

PART 2

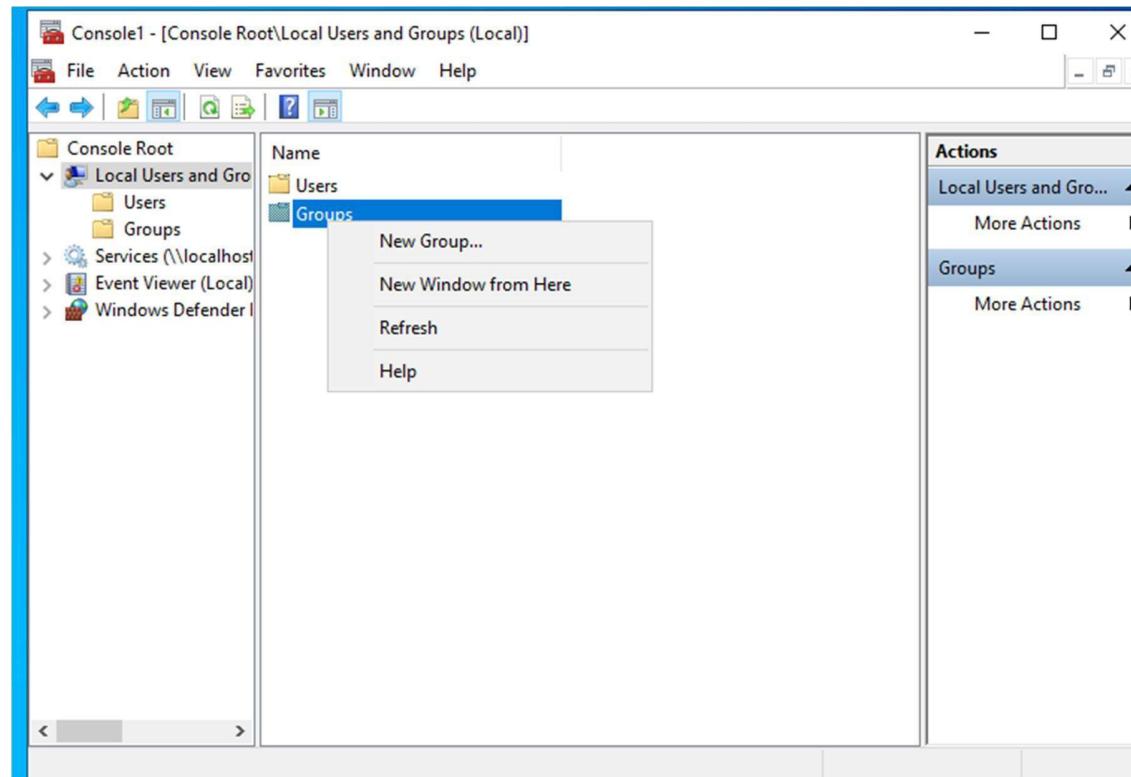
MICROSOFT MANAGEMENT CONSOLE (MMC)

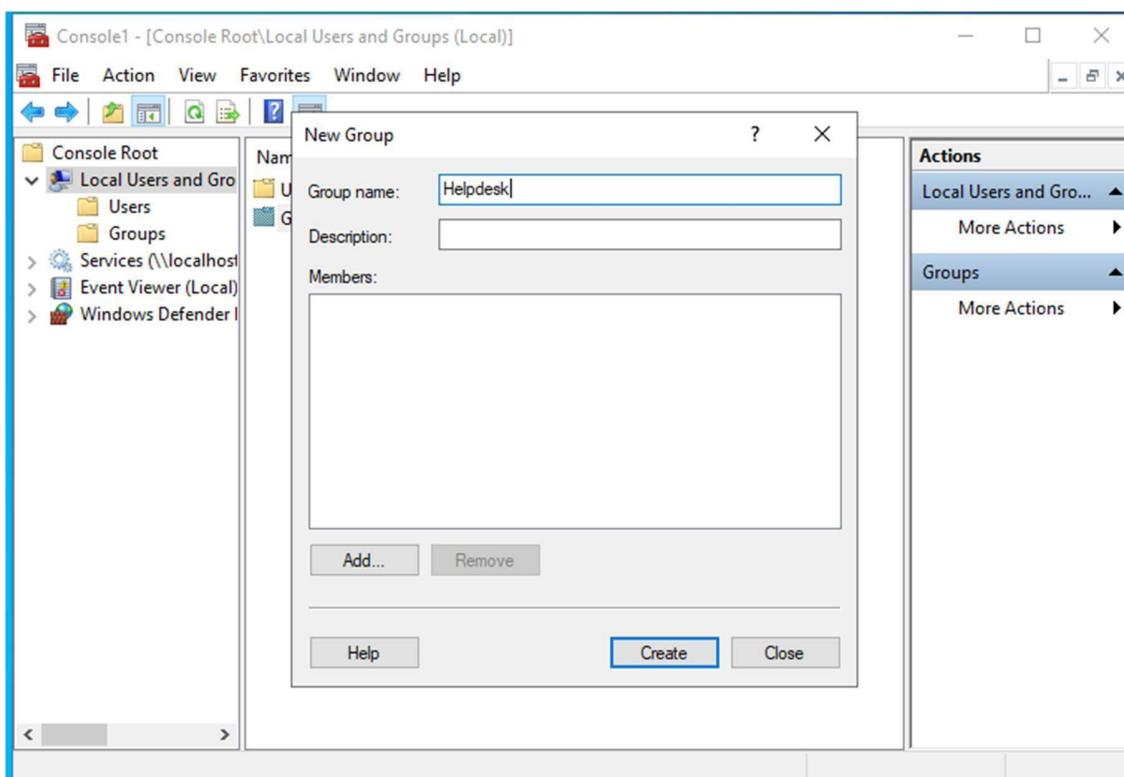
LOCAL USERS AND GROUPS

Firstly adding all the service snap-ins

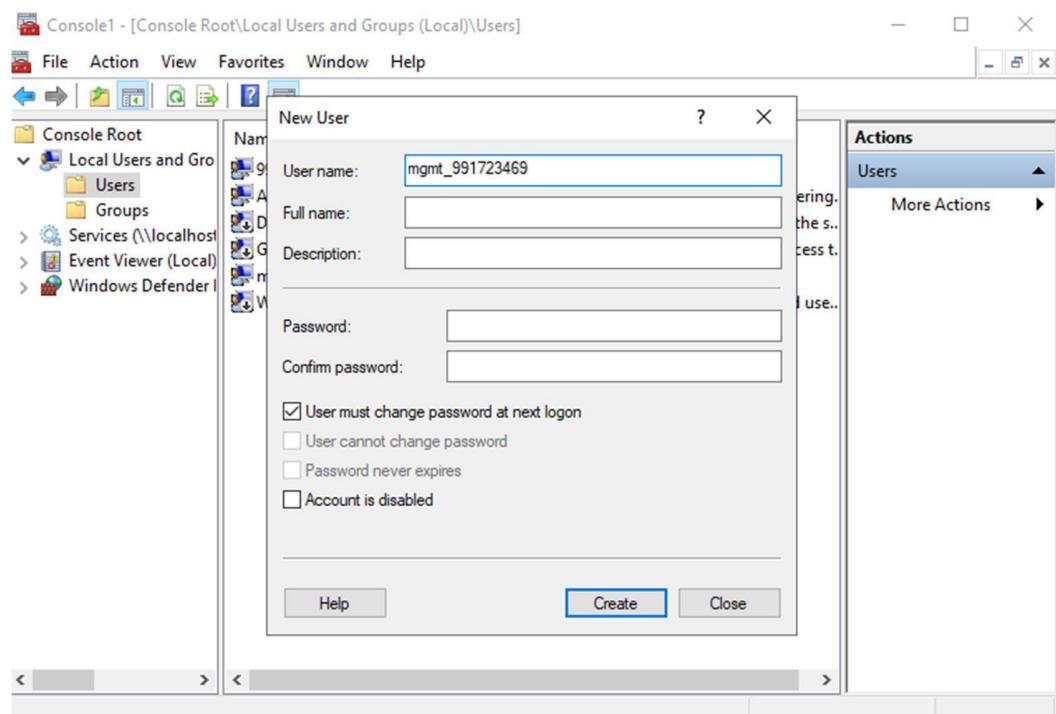


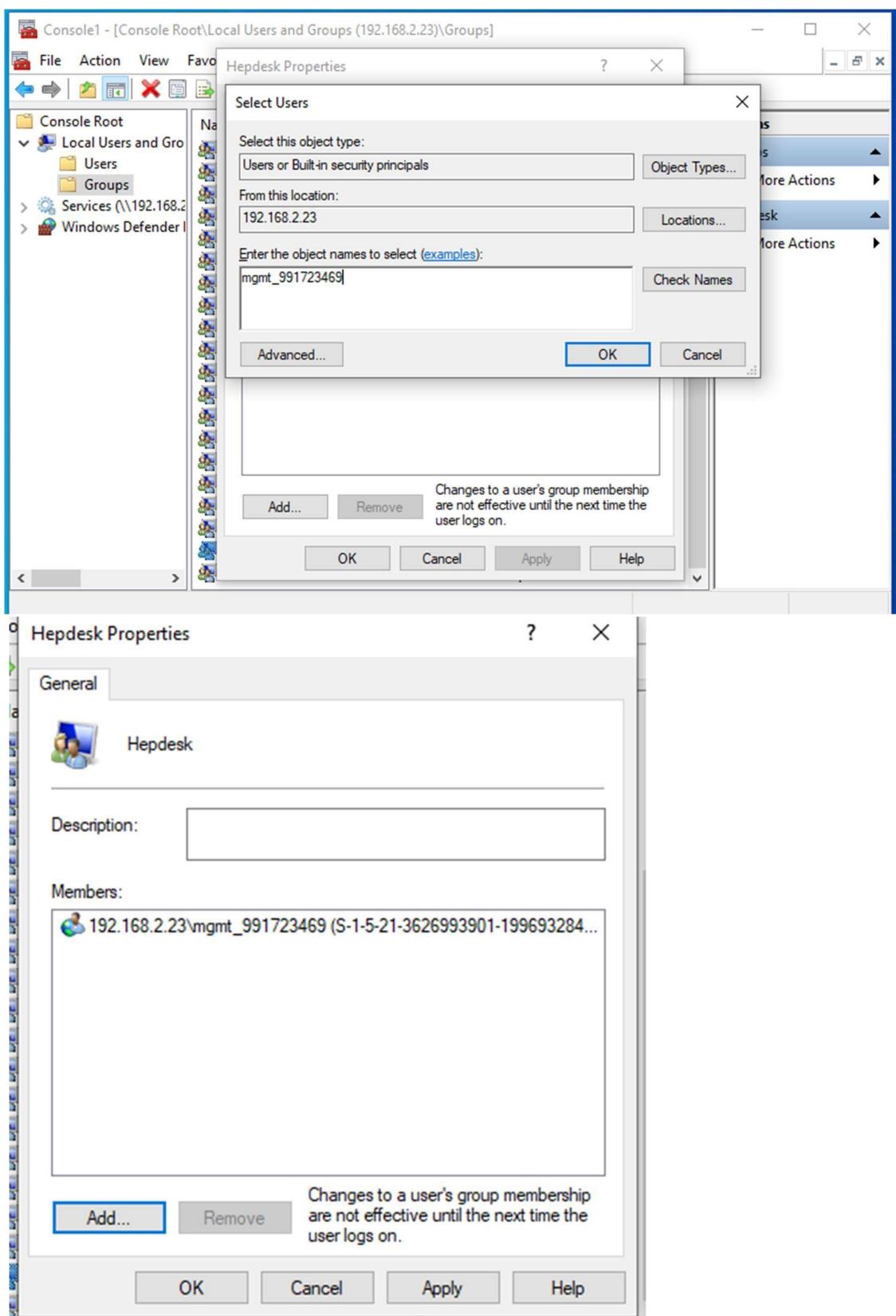
Adding a new group and adding the user to the helpdesk group





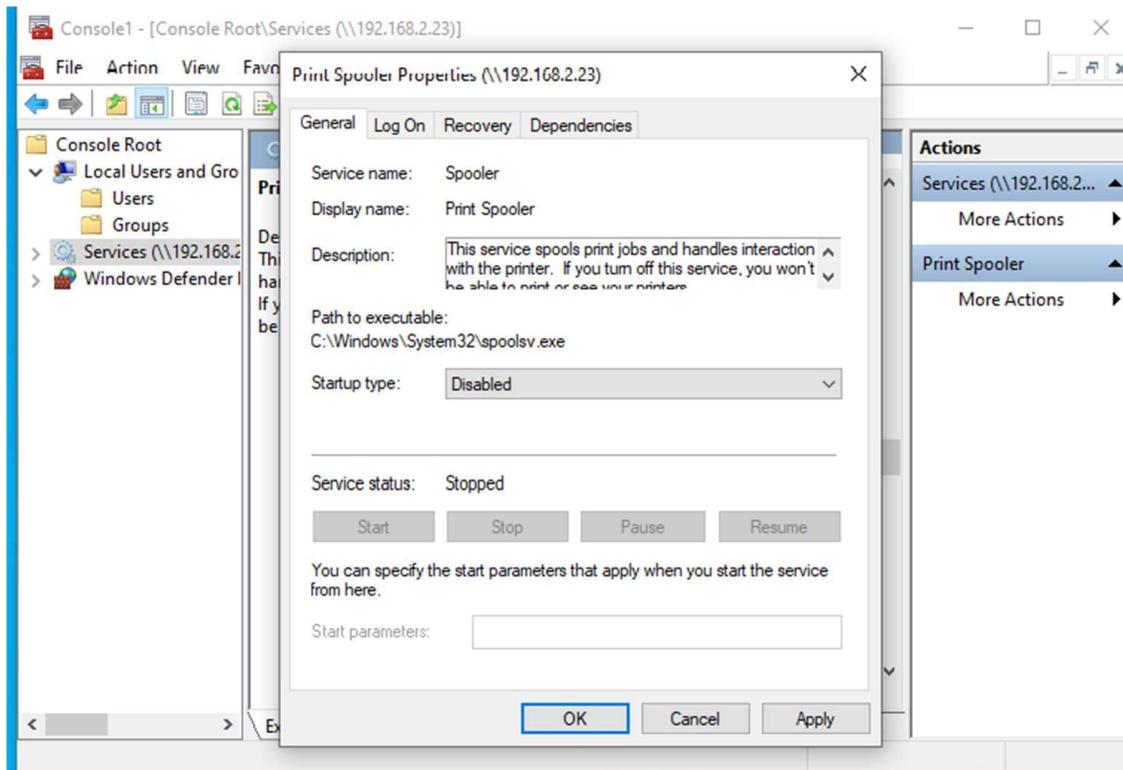
Adding new user





SERVICES

Print spooler configuration



Name	Description	Status	Startup Type	Log On As
Print Spooler	This service ...	Disabled	Local Syst...	
Printer Extensions and Notif...	This service ...	Manual	Local Syst...	
PrintWorkflow_301bb	Provides su...	Manual (Trig...	Local Syst...	
Problem Reports Control Pa...	This service ...	Manual	Local Syst...	
Program Compatibility Assis...	This service ...	Running	Automatic (...)	Local Syst...
Quality Windows Audio Vid...	Quality Win...	Manual	Local Service	
Radio Management Service	Radio Mana...	Disabled	Local Service	
Remote Access Auto Connec...	Creates a co...	Manual	Local Syst...	
Remote Access Connection...	Manages di...	Manual	Local Syst...	
Remote Desktop Configuration...	Remote Des...	Manual	Local Syst...	
Remote Desktop Services	Allows user...	Manual	Network S...	
Remote Desktop Services U...	Allows the r...	Manual	Local Syst...	
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network S...
Remote Procedure Call (RPC)	In Windows...	Manual	Network S...	
Remote Registry	Enables rem...	Running	Automatic (T...)	Local Service
Resultant Set of Policy Provi...	Provides a n...	Manual	Local Syst...	
Routing and Remote Access	Offers rout...	Disabled	Local Syst...	
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...	Manual	Local Syst...	
Secure Socket Tunneling Pr...	Provides su...	Manual	Local Service	
Security Accounts Manager	The startup ...	Running	Automatic	Local Syst...
Sensor Data Service	Delivers dat...	Disabled	Local Syst...	
Sensor Monitoring Service	Monitors va...	Manual (Trig...	Local Service	
Sensor Service	A service fo...	Manual (Trig...	Local Syst...	
Server	Supports fil...	Running	Automatic (T...	Local Syst...
Shared PC Account Manager	Manages pr...	Disabled	Local Syst...	
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syst...
Smart Card	Manages ac...	Manual (Trig...	Local Service	
Smart Card Device Enumera...	Creates soft...	Disabled	Local Syst...	

SECURITY EVENT LOGS

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane displays 'Event Viewer (Local)' with sections for 'Custom Views', 'Windows Logs' (selected), 'Applications and Services Logs', and 'Subscriptions'. Under 'Windows Logs', 'Security' is selected. The main pane shows a table of security events with columns: Keyword..., Date and Time, Source, Event ID, Task Ca..., and a details expandable row. A specific event (Event ID 4624) is selected, and its details are shown in a modal window.

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	DESKTOP-JLEDG6U\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Actions

- Open Saved Log
- Create Custom
- Import Custom
- Clear Log...
- Filter Current L
- Clear Filter
- Properties
- Find...
- Save Filtered L
- Attach a Task T
- Save Filter to C
- View
- Refresh
- Help

Event 4624, Microsoft Windows security auditing.

General Details

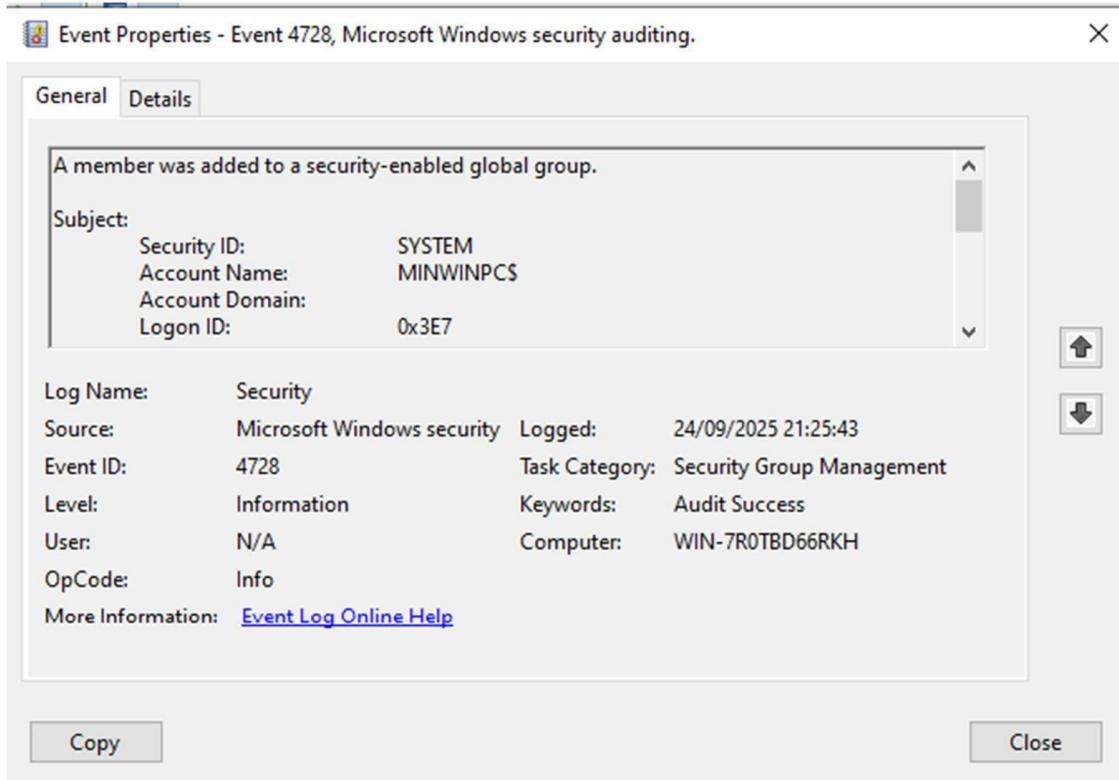
An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	DESKTOP-JLEDG6U\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

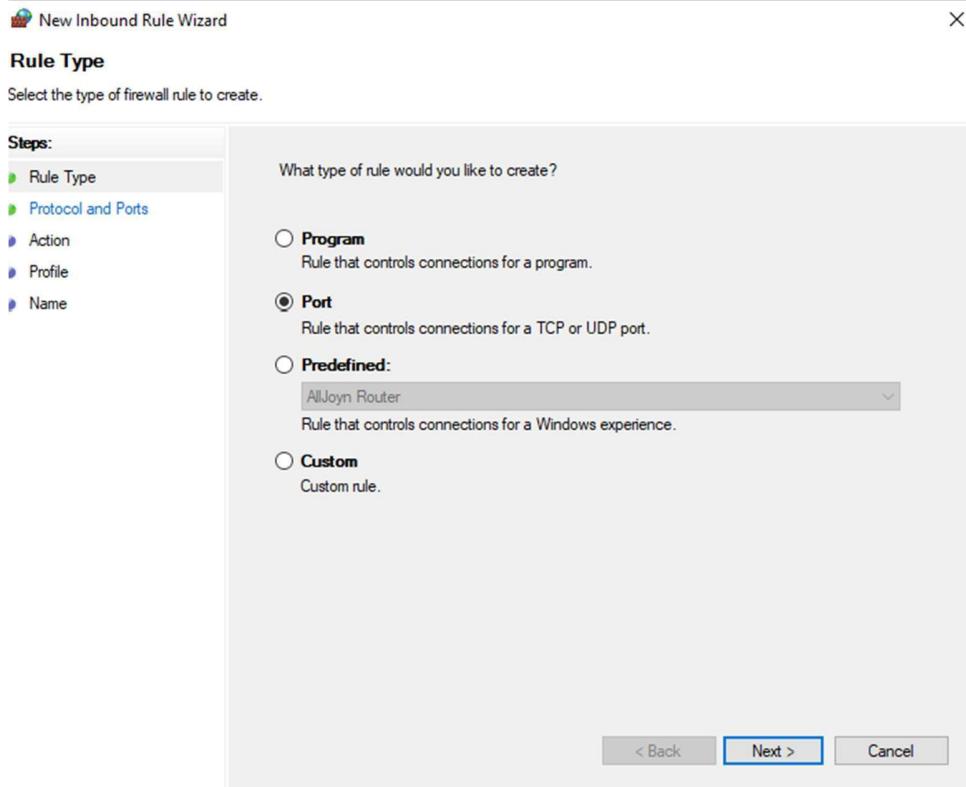


FIREWALL RULE

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

Name	Group	Profile	Enabled	Action	Override	Program
@(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.Clo...	Domai...	Yes	Allow	No	Any
@(Microsoft.Windows.CloudExperience...	@(Microsoft.Windows.Clo...	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_-28652	@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-TC...	Cast to Device functionality	Private...	Yes	Allow	No	%\$System...
Cast to Device functionality (qWave-UD...	Cast to Device functionality	Private...	Yes	Allow	No	%\$System...
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%\$System...
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%\$System...
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%\$System...
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%\$System...
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%\$System...
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	No	%\$system...
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow	No	%\$system...
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System



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:
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

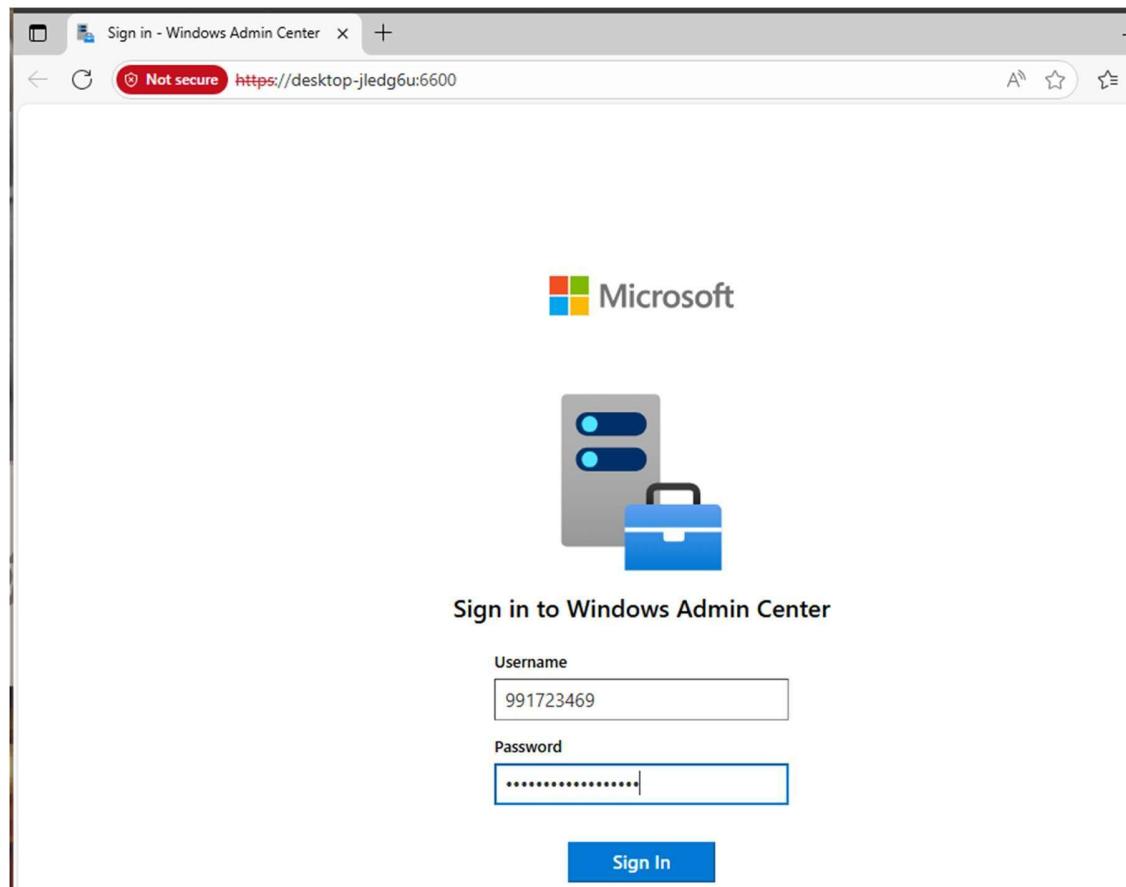
The screenshot shows the Windows Defender Firewall with Advanced Security interface. A context menu is open over a rule named "Allow RDP from mgmt_991723469 subnet". The "Properties" option is selected, opening a dialog box titled "Allow RDP from mgmt_991723469 subnet Properties". The "General" tab is selected. In the "Local IP address" section, the "IP Address" tab is active, showing the configuration for matching IP addresses or subnets. The radio button "This IP address or subnet:" is selected, and the input field contains "192.168.2.23". Below it, examples of subnet notation are listed: "192.168.0.12", "192.168.1.0/24", "2002:3d3b:1a31:4:208:74ff:fe39:6c43", and "2002:3d3b:1a31:4:208:74ff:fe39:0/112". There are also tabs for "Scope", "Advanced", "Local Principals", and "Remote Users". To the right of the dialog, the main window shows a list of rules with columns for "Override", "Program", and "Actions". The "Actions" column includes options like "New Rule...", "Filter by Profile", "Filter by State", "Filter by Group", "View", "New Window fr...", "Rfrcls", "Export List...", "Help", "Disable Rule", "Cut", "Copy", "Delete", "Properties", and "Help".

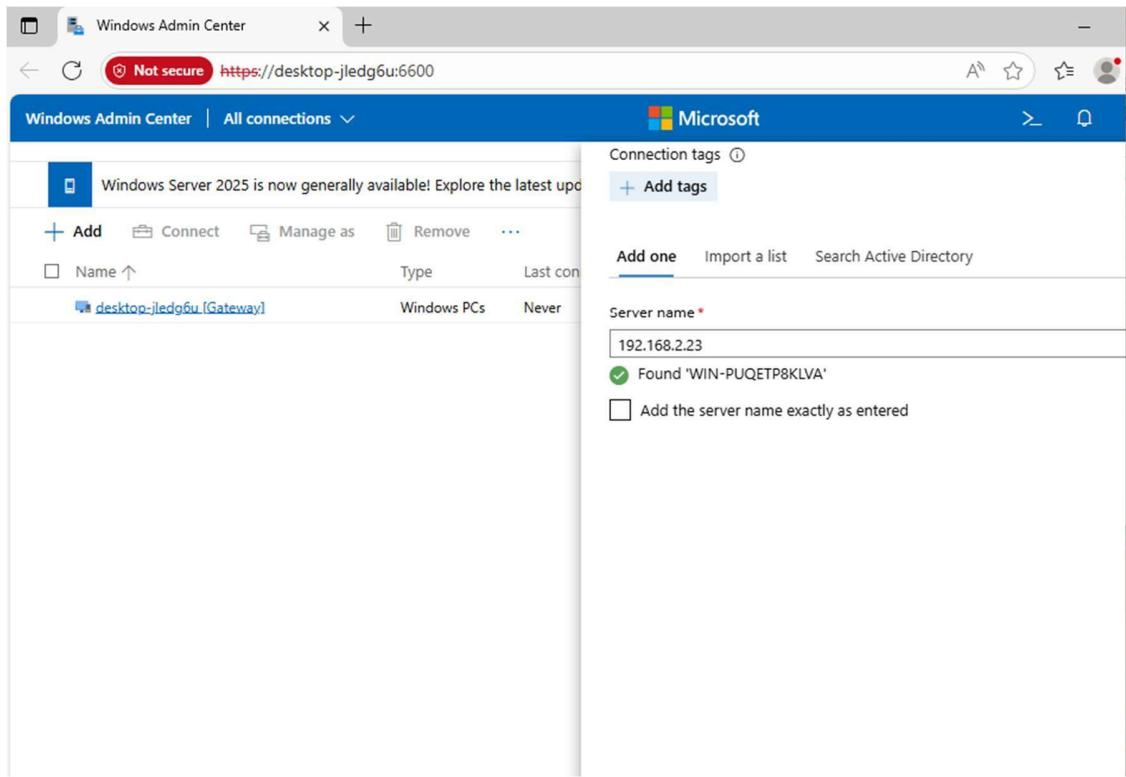
Name	Group	Profile	Enabled	Action	Override	Program
Allow RDP from mgmt_991723469 subnet		All	No	Allow	No	Any
✓ @{MicrosoftAADBrokerPlugin_1000.195...}	@{MicrosoftAADBrokerPlu...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftAADBrokerPlugin_1000.195...}	@{MicrosoftAADBrokerPlu...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWin32WebViewHost_10.0.20...	@{MicrosoftWin32WebVie...	All	Yes	Allow	No	Any
✓ @{MicrosoftWindowsCloudExperience...	@{MicrosoftWindowsClou...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWindowsCloudExperience...	@{MicrosoftWindowsClou...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWindowsSearch_1.15.0.203...}	@{MicrosoftWindowsSearc...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWindowsSearch_1.15.0.203...}	@{MicrosoftWindowsSearc...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWindowsStartMenuExperi...	@{MicrosoftWindowsStart...	Domai...	Yes	Allow	No	Any
✓ @{MicrosoftWindowsStartMenuExperi...	@{MicrosoftWindowsStart...	Domai...	Yes	Allow	No	Any
@FirewallAPI.dll,-28653	@FirewallAPI.dll,-28652	All	No	Allow	No	System
✓ AllIoyn Router (TCP-In)	AllIoyn Router	Domai...	Yes	Allow	No	%System...
✓ AllIoyn Router (UDP-In)	AllIoyn 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

A screenshot of the 'Local users and groups' interface. On the left, there's a sidebar with 'Users' and 'Groups' tabs, 'New group' button, and a list of existing groups: Replicator, Storage Replica Admins, System Managed Accounts, Users, and Windows Admin Center. Below this is a 'Details' section with a collapse arrow. On the right, the 'Add new group' dialog is open. It has a 'Name*' field containing 'Helpdesk' and an empty 'Description' field. At the bottom are 'Submit' and 'Cancel' buttons.

Adding a new user

The screenshot shows the Windows Admin Center interface for a server named WIN-PUQETP8KLVA. The left sidebar is collapsed, and the main area displays the 'Local users and groups' section under 'Users'. A table lists six users: 991723469, Administrator, DefaultAccount, Guest, mgmt991723469, and WDAGUtilityAccount. The 'Administrator' row has a detailed description: 'Built-in account for administering the computer/d...'. Below the table is a search bar and a 'New user' button.

Adding user to helpdesk group

The screenshot shows the 'Add a user to the Helpdesk group' dialog in the Windows Admin Center. The 'Groups' tab is selected in the navigation bar. In the 'Details - Helpdesk' section, there is a 'Members' list which is currently empty, indicated by the text 'There are no members'. A 'Submit' button is at the bottom right of the dialog.

Details - Helpdesk ▾

[+ Add user](#) [Remove users](#)

1 item 

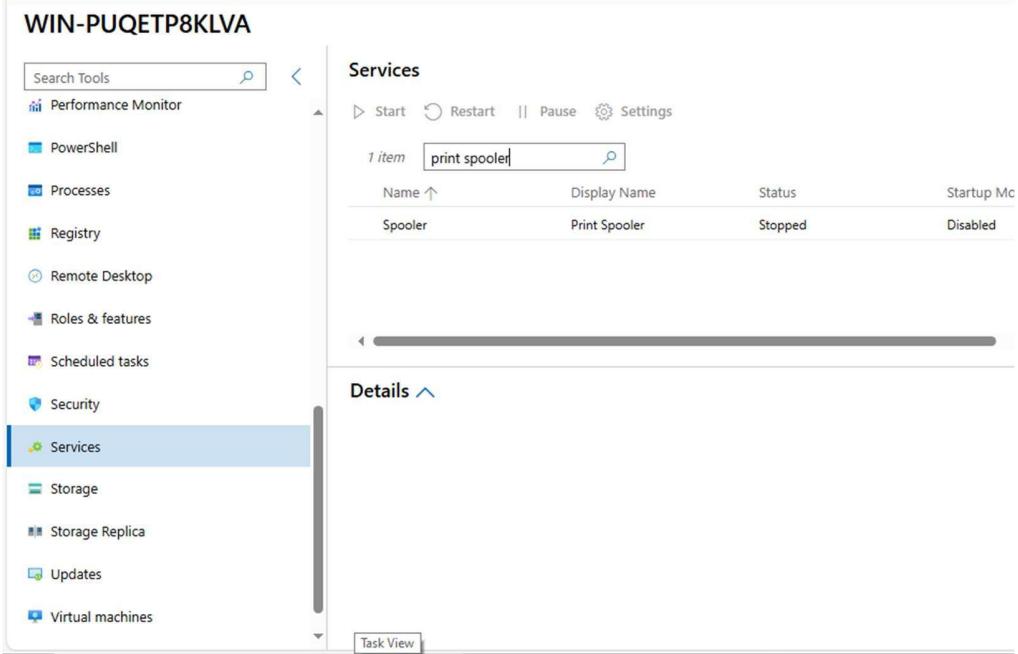
Members

mgmt991723469

SERVICES

Disabling the print spooler

WIN-PUQETP8KLVA



The screenshot shows the Windows Server 2012R2 Services Management Console. The left navigation pane lists various management tools: Performance Monitor, PowerShell, Processes, Registry, Remote Desktop, Roles & features, Scheduled tasks, Security, and Services. The Services option is selected and highlighted in blue. The main pane displays the 'Services' list with the following details:

Name ↑	Display Name	Status	Startup Mc
Spooler	Print Spooler	Stopped	Disabled

A search bar at the top right contains the text 'print spooler'. Below the table, a 'Details' section is visible.

SECURITY EVENT LOGS

Applying a filter to sort by event id

WIN-PUQETP8KLVA

The screenshot shows the Windows Event Viewer interface. The left pane displays a search bar with 'events' and a 'Tools' section with 'Events' selected. The right pane has a title 'Events' and a 'Preview Mod' toggle switch. Under 'Administrative Logs', 'Windows Logs' is expanded, showing 'System', 'Security', 'Application', and 'Setup'. Below these are buttons for 'Clear', 'Export', and 'Search'. A table lists 942 items, with columns for 'Level', 'Date and Time', 'Source', and 'Event ID'. All entries are 'Information' level, dated 26/09/2025, 03:34:43, from 'Microsoft Windows security ...' with Event ID 4624.

Level	Date and Time	Source	Event ID
Information	26/09/2025, 03:34:43	Microsoft Windows security ...	4624
Information	26/09/2025, 03:34:42	Microsoft Windows security ...	4624
Information	26/09/2025, 03:34:42	Microsoft Windows security ...	4624
Information	26/09/2025, 03:34:42	Microsoft Windows security ...	4624
Information	26/09/2025, 03:34:42	Microsoft Windows security ...	4624

WIN-PUQETP8KLVA

The screenshot shows the Windows Event Viewer interface with the 'Event Records Filter' dialog open. The left pane is identical to the previous screenshot. The right pane shows the 'Event Records Filter' dialog. It includes sections for 'Event Levels' (with checkboxes for 'Select all', 'Critical', 'Error', 'Warning', 'Information', and 'Verbose', all checked), 'Log Time' (with a radio button for 'Select a time span' and a 'Specify a custom time range' option), 'Select a time span' (set to 'Any Time'), 'Event ID' (containing '4624, 4625, 4728, 4729'), 'Source' (empty), and 'Apply' and 'Cancel' buttons. The bottom of the dialog shows a 'Microsoft Store' watermark.

FIREWALL RULE

Creating a new inbound rule in firewall

WIN-PUQETP8KLVA

The screenshot shows the Windows Firewall settings window for a computer named WIN-PUQETP8KLVA. The 'Incoming rules' tab is selected. A 'New Rule' dialog box is open on the right, titled 'General'. The 'Name*' field contains 'Allow RDP mgmt subnet'. The 'Direction' is set to 'Incoming' (radio button selected). The 'Action' is set to 'Allowed' (radio button selected). The 'Enable Firewall Rule' toggle switch is set to 'No'. At the bottom of the dialog are 'Create' and 'Close' buttons, with 'Create' being highlighted.

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, Private
AllJoyn Router (UDP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Private
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

The screenshot shows the Windows Firewall settings. The 'Incoming rules' tab is selected. A tooltip at the top right says 'Disabling firewall rule' and 'Successfully disabled firewall rule "RDP Management Subnet"'. The table below lists rules like 'WacInboundOpenException', 'RDP Management Subnet', and 'Allow RDP mgmt subnet', each with an 'Action' column showing 'Allowed' or 'Disabled'.

Name	Action	Group ↑	Status	Profile
WacInboundOpenException	✓ Allowed		Enabled	All
RDP Management Subnet	✓ Allowed		Disabled	All
Allow RDP mgmt subnet	✓ Allowed		Disabled	All
AllJoyn Router (TCP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Private
AllJoyn Router (UDP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Private
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
Cast to Device functionality...	✓ Allowed	Cast to Device func...	Enabled	Private, Public

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.
