Exercise 1 - Configuring Computer Management for Remote Administration

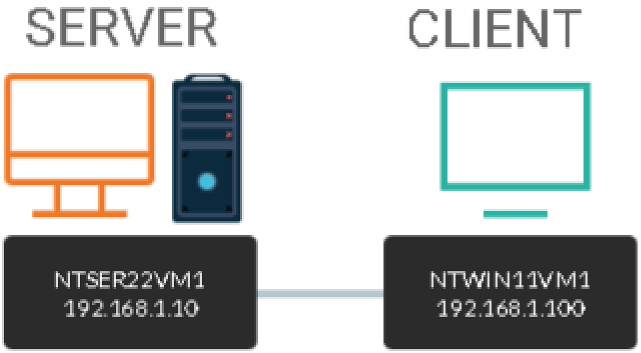
Computer Management is a centralized user interface that allows you to manage system tools, storage subsystems, and services. This puts Task Viewer, Event Viewer, Performance Monitor, Device Manager, and Disk Manager all in one location. Management and Services panel.

Computer Management, like other administration programs, can be set up to remotely manage servers and workstations. This is accomplished by allowing incoming connections from a domain-joined workstation over firewall rules.

In this exercise,

1. Enable Firewall Rules for Remote Administration
2. Perform Remote Administration via Computer Management

Topology



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTWIN11VM1 = Windows 11 – Domain Member

Prerequisite

- *VMware Workstation 16 Pro*

    - When making this tutorial, we used the “Windows Server 2019” VM Template and “Windows 10 & later” VM Template. Since VMware didn’t have the updated templates.
- *Microsoft Windows Server 2022*
- *Microsoft Windows 11*

Task 1:

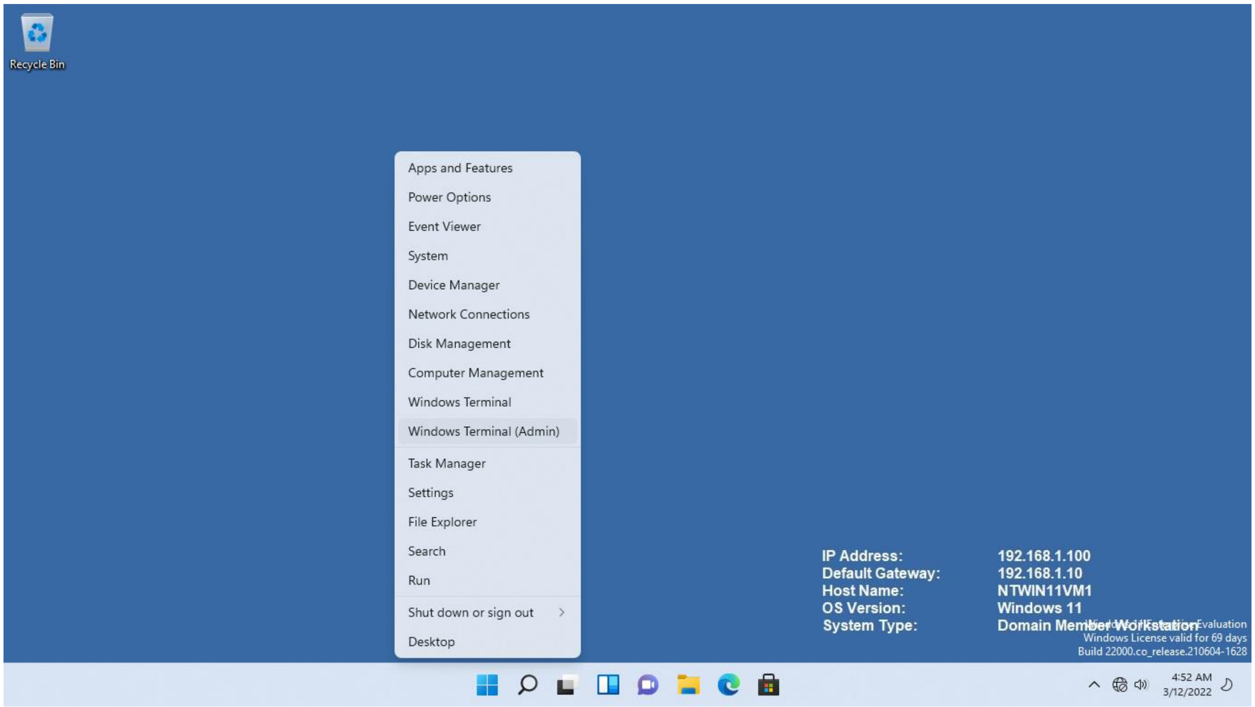
The graphical Windows Security, Windows Defender Firewall with Advanced Security, can be used to administer Windows Firewall Rules. Similarly, Windows PowerShell contains cmdlets for configuring a computer's firewall.

In this task, we will enable the required firewall rules to allow a Windows 11 workstation to connect to a Windows Server through Computer Management.

Step 1:

Ensure you are connected to **NTWIN11VM1**

Right-click on the **Start** icon and select **Windows Terminal (Admin).**



IP Address: 192.168.1.100
Default Gateway: 192.168.1.10
Host Name: NTWIN11VM1
OS Version: Windows 11
System Type: Domain Member Workstation

Windows 11 Enterprise Evaluation
Windows License valid for 69 days
Build 22000.co_release.210604-1628

Step 2:

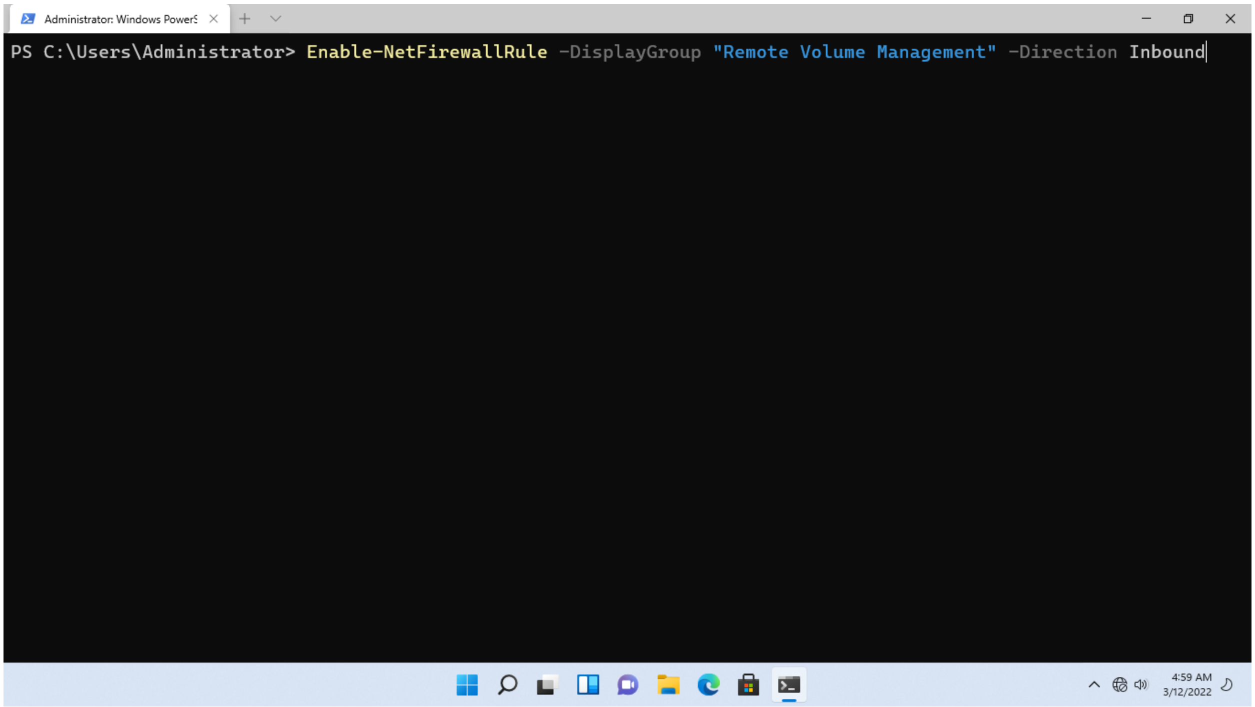
To create an inbound firewall rule that will allow management of remote disk volumes, type the following:

```
Enable-NetFirewallRule -DisplayGroup “Remote Volume Management” -Direction Inbound
```

Press **Enter**

Step 3:

Notice that there will be no successful confirmation after enabling the inbound firewall rule. This is by design.



```
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Volume Management" -Direction Inbound
```

Step 4:

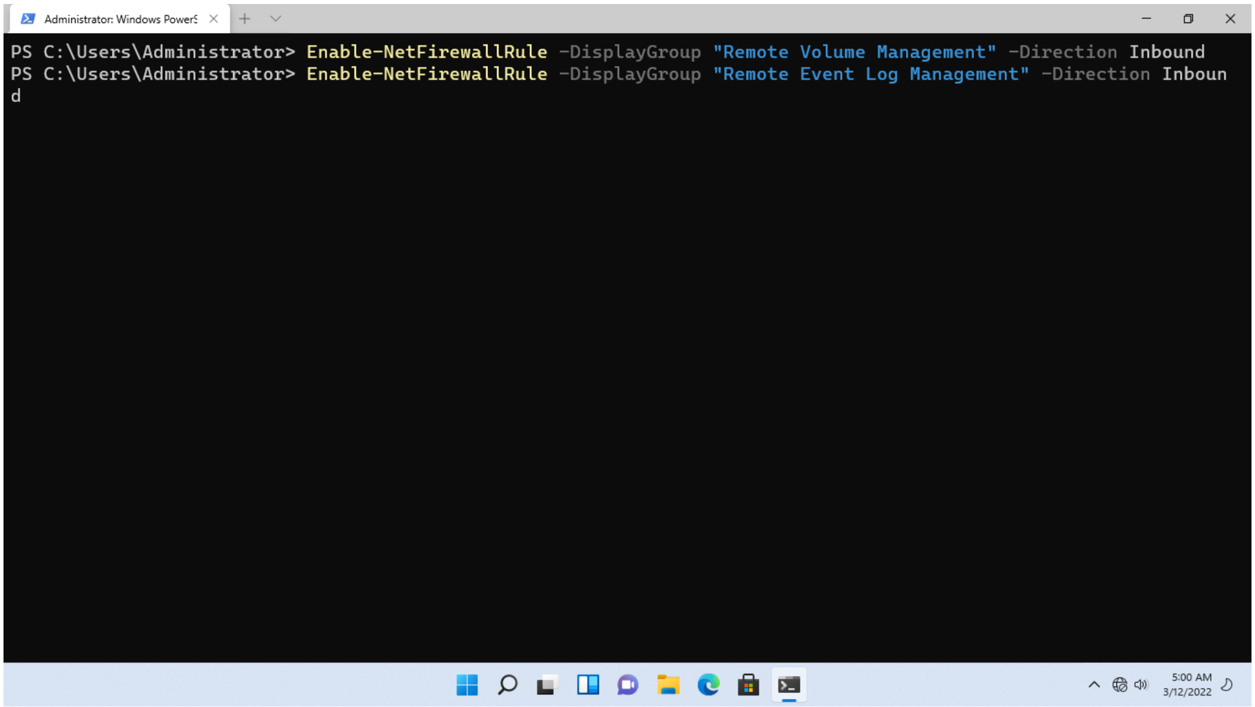
On the next prompt, to create an inbound firewall rule that will allow management of remote event logs, type the following:

```
Enable-NetFirewallRule -DisplayGroup “Remote Event Log Management” -Direction Inbound
```

Press **Enter**

Step 5:

As before, there will be no successful confirmation.



```
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Volume Management" -Direction Inbound
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management" -Direction Inboun
d
```

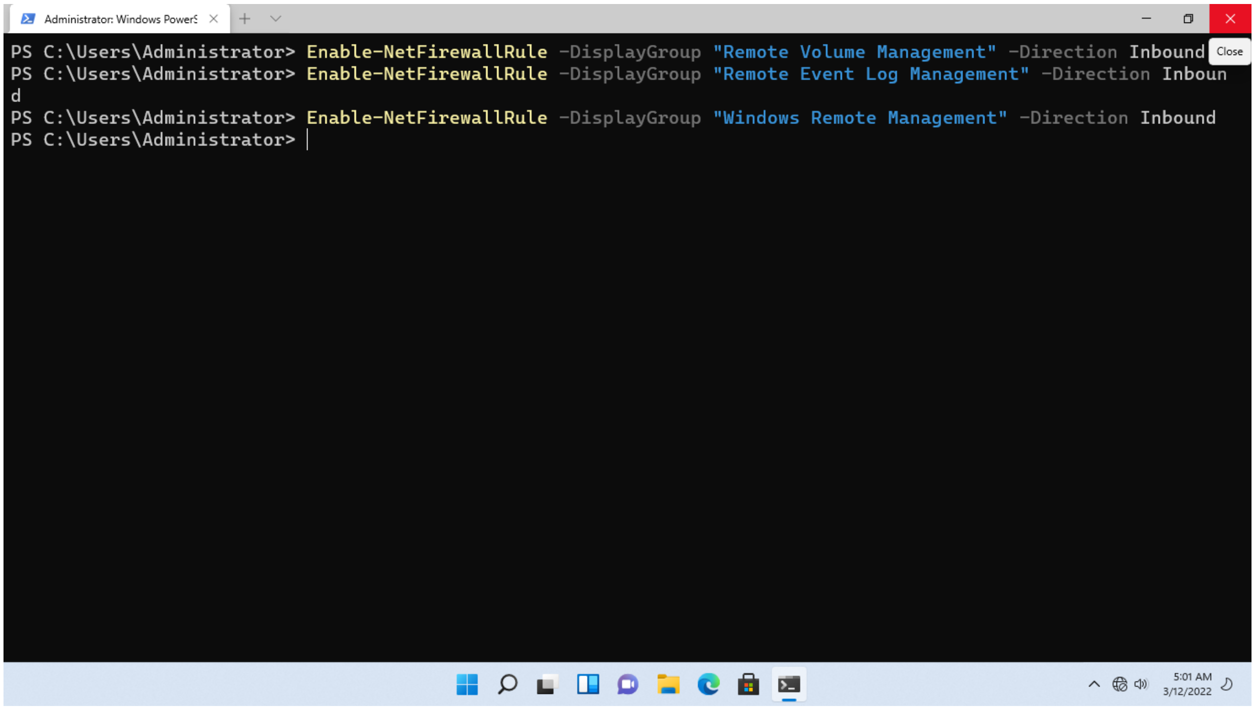
Step 6:

On the next prompt, to enable remote management of a Windows device, type:

```
Enable-NetFirewallRule -DisplayGroup “Windows Remote Management” -Direction Inbound
```

Press **Enter**

Close the **Windows Terminal** window.

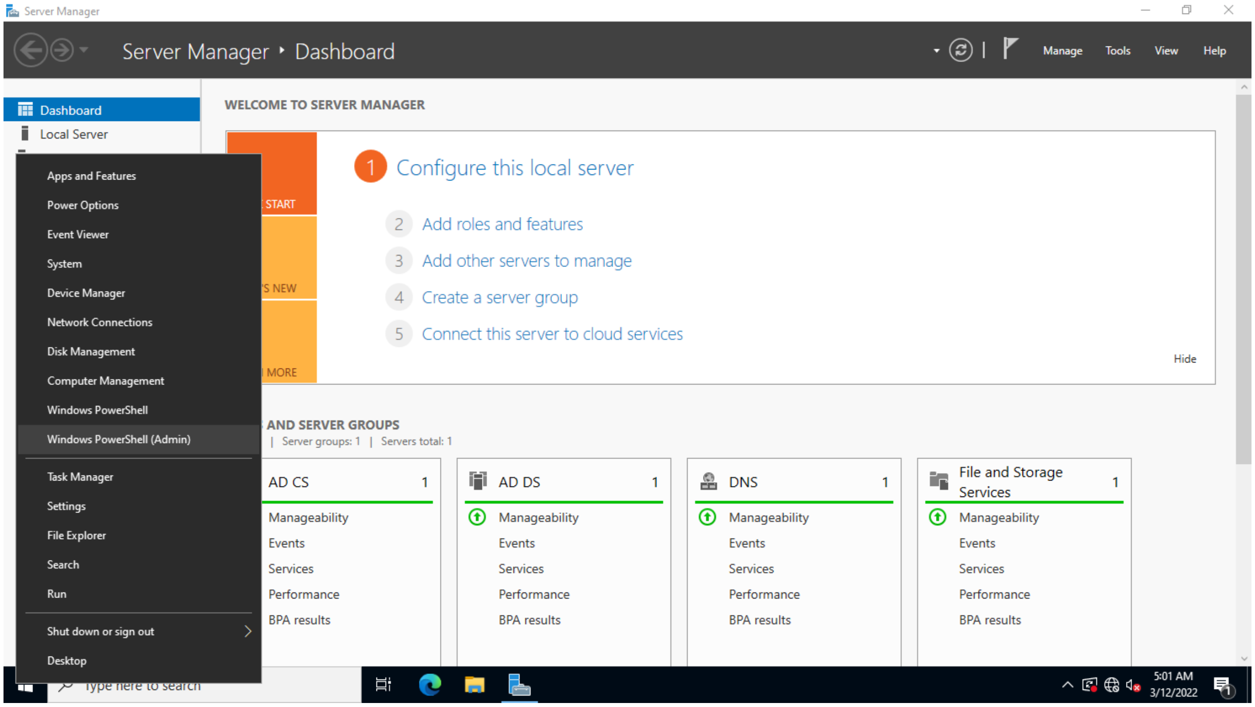


```
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Volume Management" -Direction Inbound
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management" -Direction Inboun
d
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Windows Remote Management" -Direction Inbound
PS C:\Users\Administrator>
```

Step 7:

Connect to **NTSER22VM1**

Right-click the **Start** icon and select **Windows Powershell**

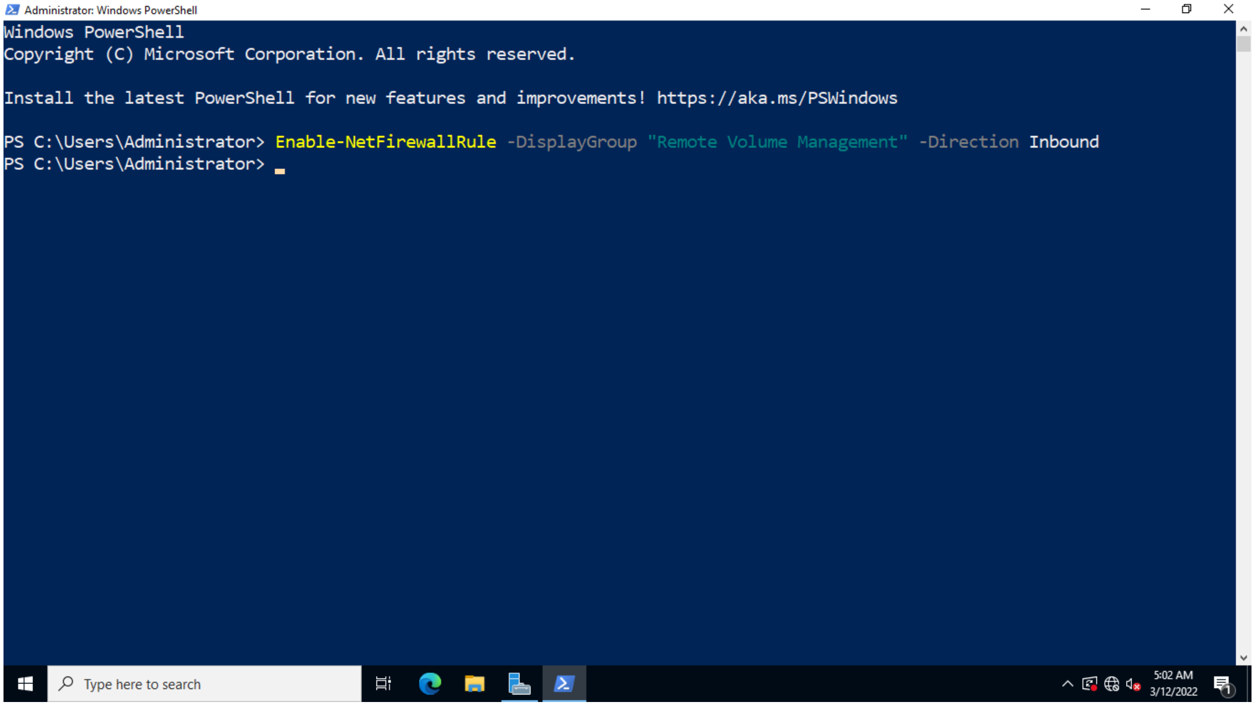


Step 8:

Type the following commands to create an inbound firewall rule that will allow management of remote disk volumes:

```
Enable-NetFirewallRule -DisplayGroup “Remote Volume Management” -Direction Inbound
```

Press **Enter**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Volume Management" -Direction Inbound
PS C:\Users\Administrator> _
```

Step 9:

On the next prompt, to create an inbound firewall rule that will allow management of remote event logs, type the following:

```
Enable-NetFirewallRule -DisplayGroup “Remote Event Log Management” -Direction Inbound
```

Press **Enter**

On the next prompt, to enable remote management of a Windows device, type:

```
Enable-NetFirewallRule -DisplayGroup “Windows Remote Management” -Direction Inbound
```

Press **Enter**

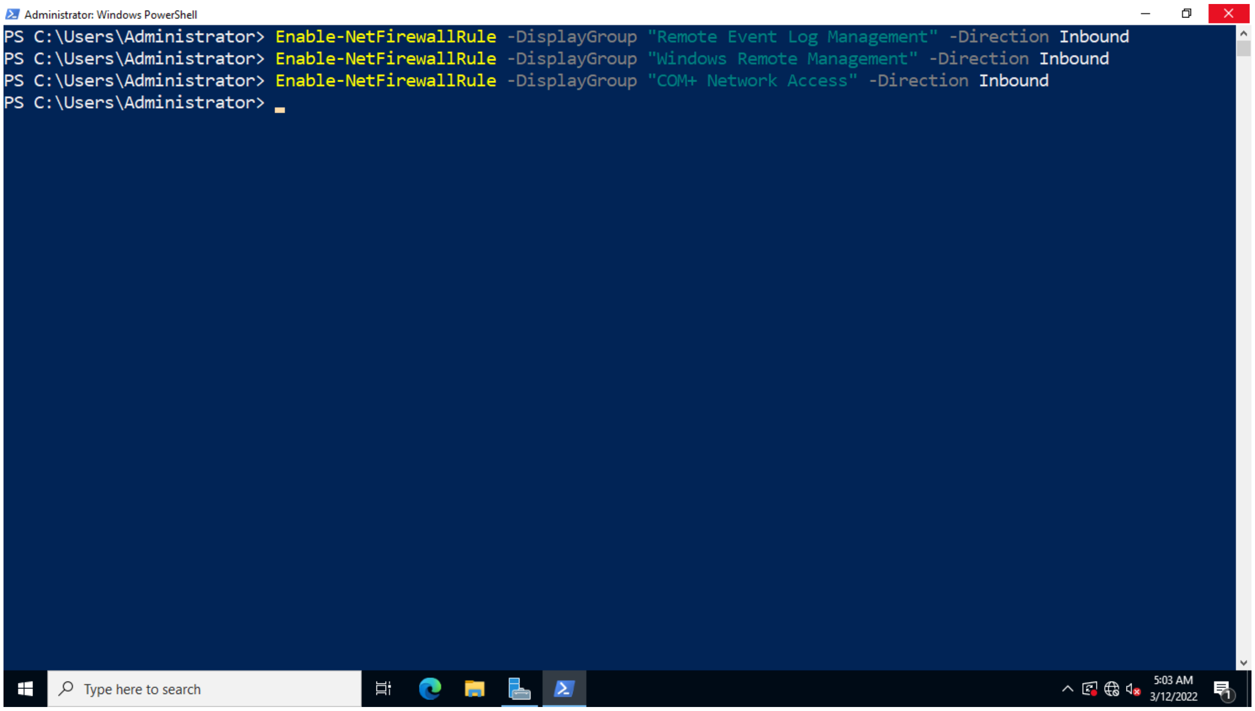
Still on the next prompt, to create a firewall rule for COM+ Network access, type:

```
Enable-NetFirewallRule -DisplayGroup “COM+ Network Access” -Direction Inbound
```

Press **Enter**

As illustrated before, there will be no successful confirmation when you enable the Windows firewall rule.

Close the **Windows Terminal** window.



```
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management" -Direction Inbound
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "Windows Remote Management" -Direction Inbound
PS C:\Users\Administrator> Enable-NetFirewallRule -DisplayGroup "COM+ Network Access" -Direction Inbound
PS C:\Users\Administrator> _
```

Task 2:

Computer Management is a suite of tools that allows you to manage a device's critical system settings. It also facilitates remote device management by enabling firewall ports required for remote administration.

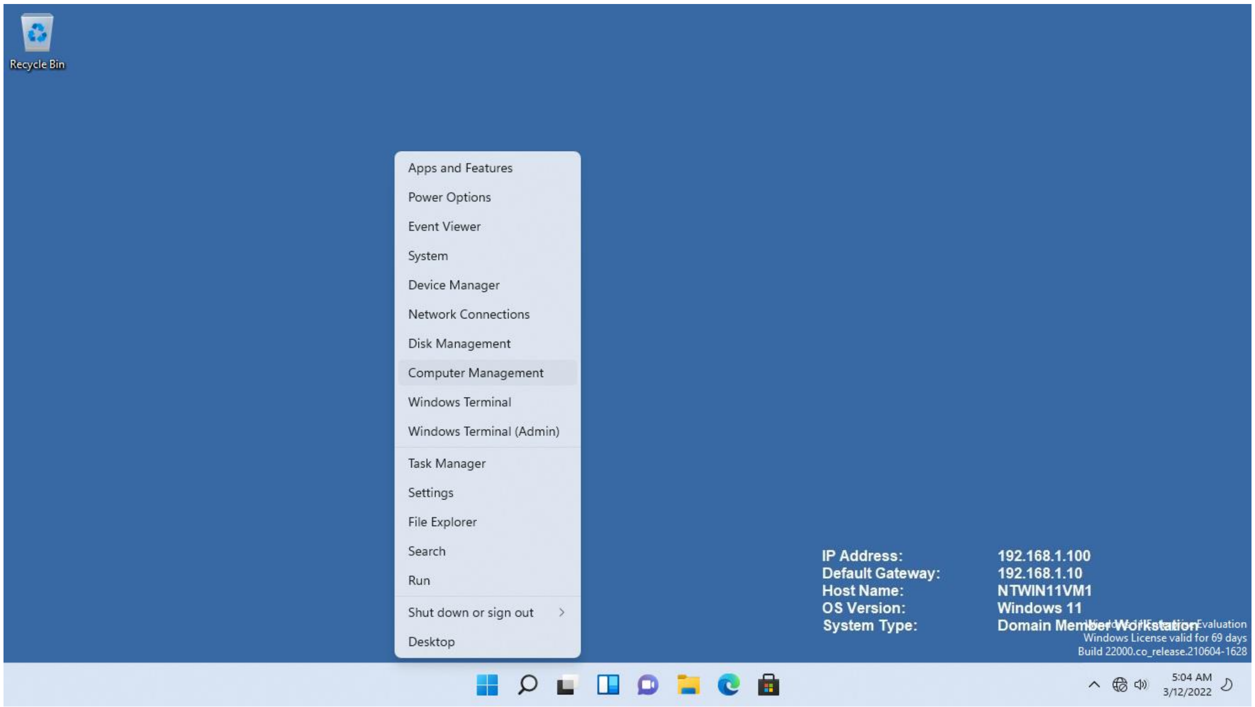
You have enabled the essential firewall rules in both devices.

In this task, we will now remotely manage the NTSER22VM1 server from the NTWIN11VM1 client workstation.

Step 1:

Connect to **NTWIN11VM1**.

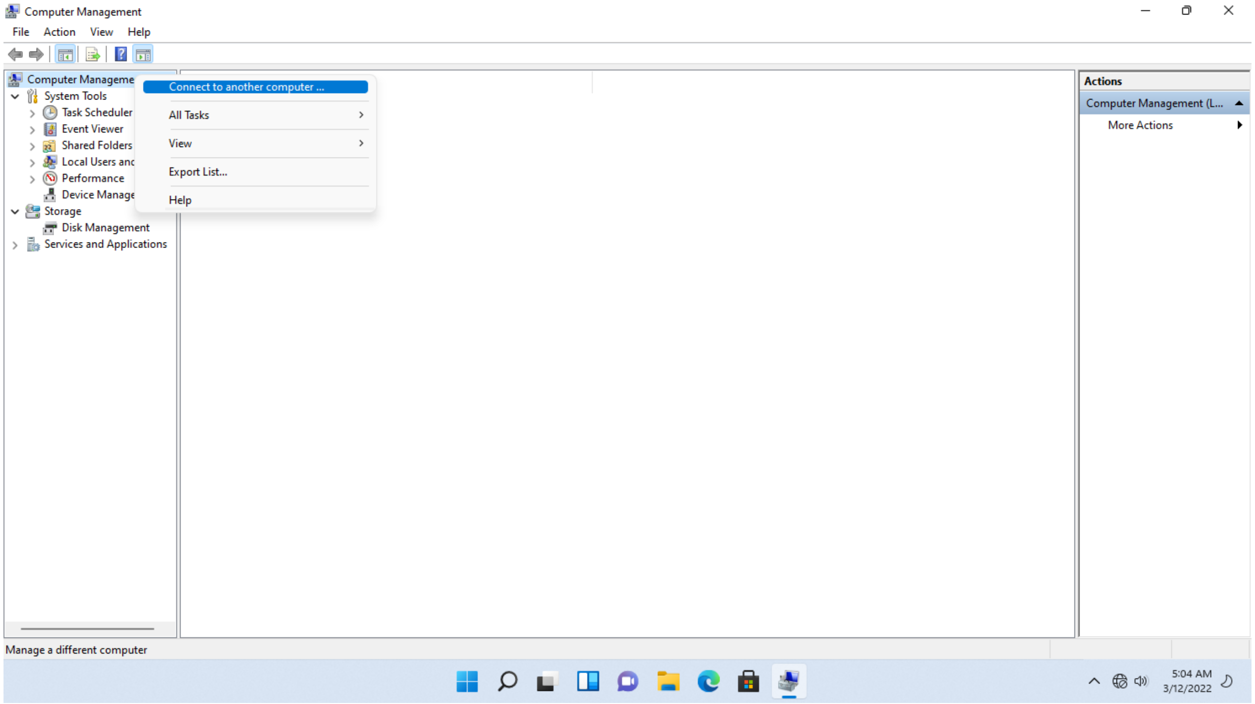
Right-click the **Start** icon and select **Computer Management**.



IP Address: 192.168.1.100
Default Gateway: 192.168.1.10
Host Name: NTWIN11VM1
OS Version: Windows 11
System Type: Domain Member Workstation

Step 2:

On the **Computer Management** console window, right-click the **Computer Management (Local)** node and select **Connect to another computer**

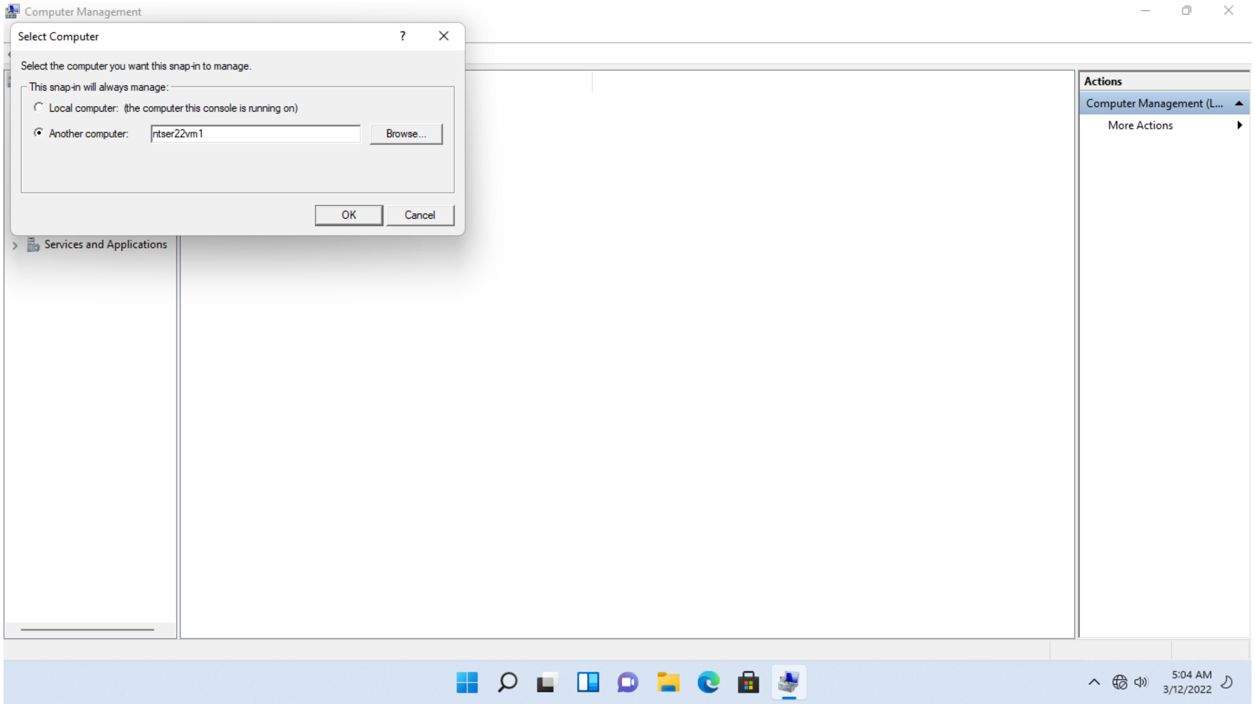


Step 3:

On the **Select Computer** dialog box, select the **Another computer** option button.

Then type the following in the textbox: ***ntser22vm1***

Click **OK**.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

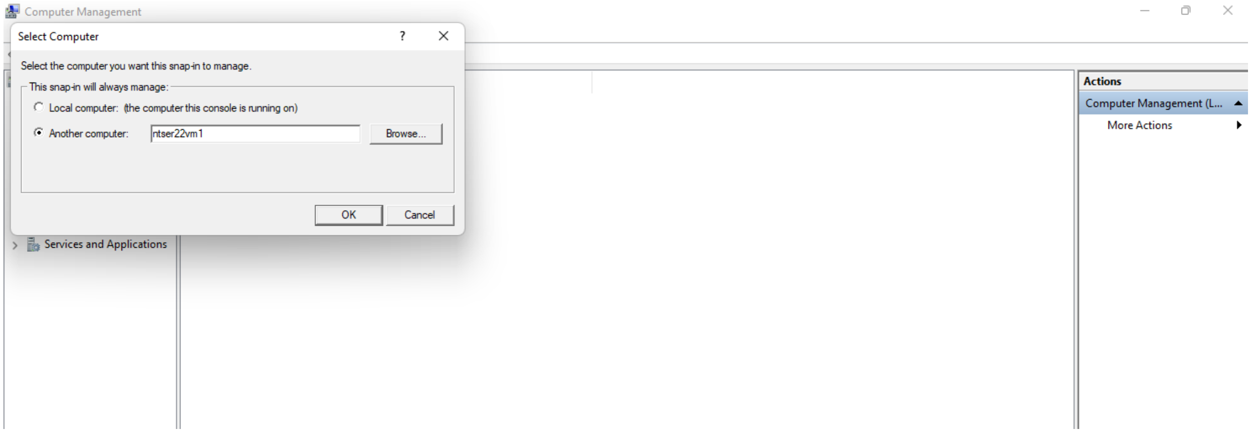
○ Local computer: (the computer this console is running on)

● Another computer: ntser22vm1

Step 4:

A connection to **NTSER22VM1** via **Computer Management** is now established.

Expand the **System Tools** node for **NTSER22VM1** to view the **Task Scheduler**, **Event Viewer**, **Shared Folders**, **Performance** and **Device Manager** tools.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

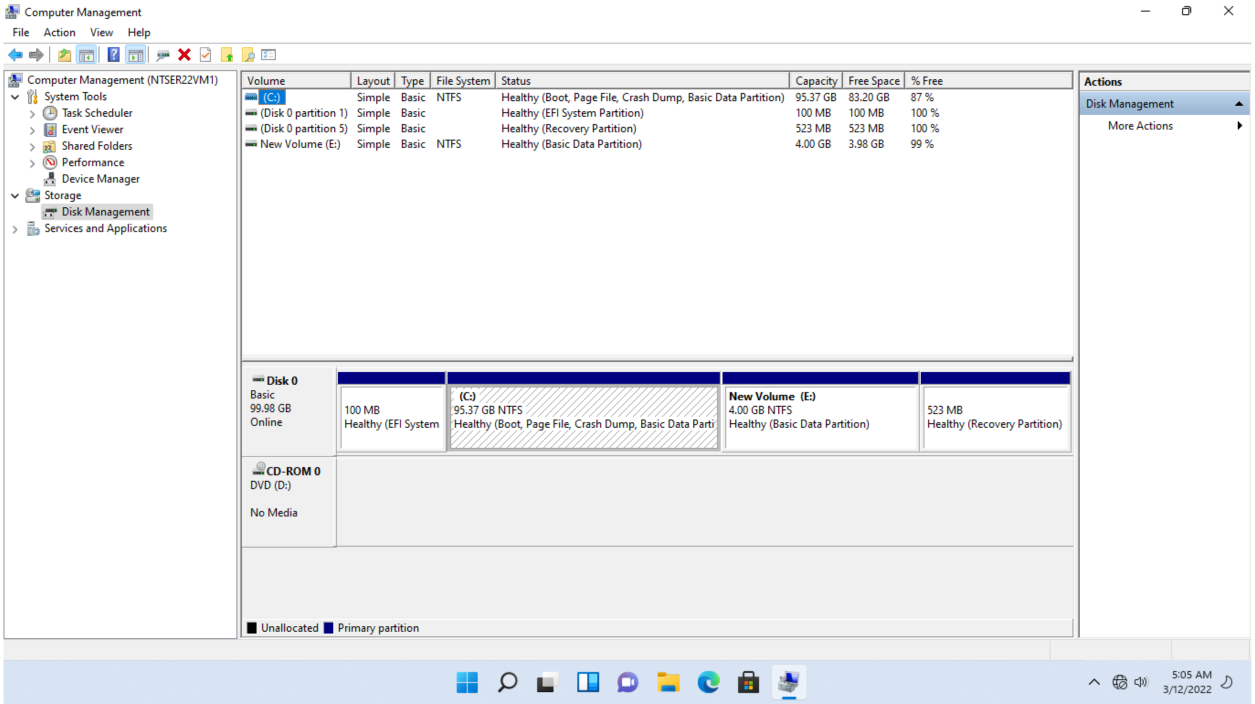
○ Local computer: (the computer this console is running on)

● Another computer: ntser22vm1

Step 5:

Expand **Storage** and click **Disk Management**.

Notice the disk volumes of **NTSER22VM1** appear.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Basic Data Partition)	95.37 GB	83.20 GB	87 %
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 MB	100 %
(Disk 0 partition 5)	Simple	Basic		Healthy (Recovery Partition)	523 MB	523 MB	100 %
New Volume (E:)	Simple	Basic	NTFS	Healthy (Basic Data Partition)	4.00 GB	3.98 GB	99 %

Disk 0 Basic 99.98 GB Online	100 MB Healthy (EFI System	(C:) 95.37 GB NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Parti	New Volume (E:) 4.00 GB NTFS Healthy (Basic Data Partition)	523 MB Healthy (Recovery Partition)
CD-ROM 0 DVD (D:) No Media				

■ Unallocated ■ Primary partition

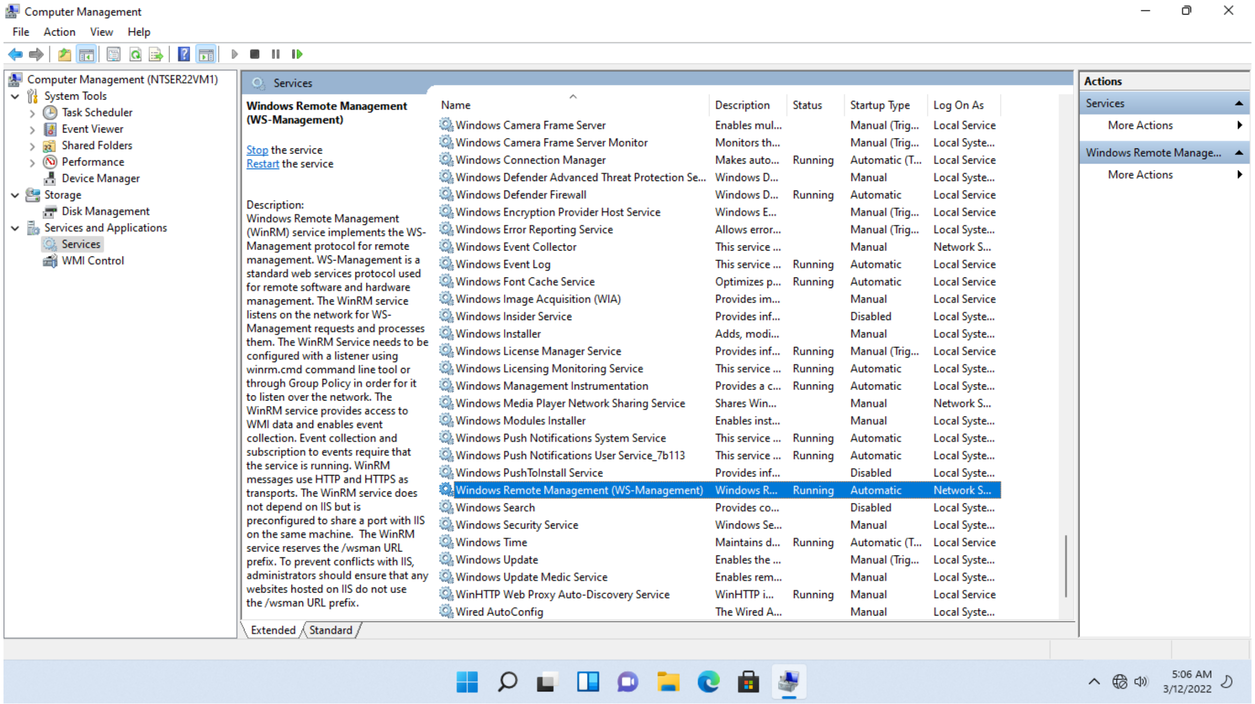
Step 6:

Now expand the **Services and Applications** node.

Click on **Services** to view the network services running on **NTSER22VM1**.

Scroll down the list and select **Windows Remote Management**.

Windows Remote Management (WS-Man) as shown in the screenshot is a service that enables administration of Windows devices from another workstation. Recall that you enabled the network firewall ports of **Windows Remote Management**.



Windows Remote Management (WS-Management)

Stop the service
Restart the service

Description:
Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix.

Name	Description	Status	Startup Type	Log On As
Windows Camera Frame Server	Enables mul...		Manual (Trig...	Local Service
Windows Camera Frame Server Monitor	Monitors th...		Manual (Trig...	Local Syste...
Windows Connection Manager	Makes auto...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Se...	Windows D...		Manual	Local Syste...
Windows Defender Firewall	Windows D...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows E...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows error...		Manual (Trig...	Local Syste...
Windows Event Collector	This service ...		Manual	Network S...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides im...		Manual	Local Service
Windows Insider Service	Provides inf...		Disabled	Local Syste...
Windows Installer	Adds, modi...		Manual	Local Syste...
Windows License Manager Service	Provides inf...	Running	Manual (Trig...	Local Service
Windows Licensing Monitoring Service	This service ...	Running	Automatic	Local Syste...
Windows Management Instrumentation	Provides a c...	Running	Automatic	Local Syste...
Windows Media Player Network Sharing Service	Shares Win...		Manual	Network S...
Windows Modules Installer	Enables inst...		Manual	Local Syste...
Windows Push Notifications System Service	This service ...	Running	Automatic	Local Syste...
Windows Push Notifications User Service_7b113	This service ...	Running	Automatic	Local Syste...
Windows PushToInstall Service	Provides inf...		Disabled	Local Syste...
Windows Remote Management (WS-Management)	Windows R...	Running	Automatic	Network S...
Windows Search	Provides co...		Disabled	Local Syste...
Windows Security Service	Windows Se...		Manual	Local Syste...
Windows Time	Maintains d...	Running	Automatic (T...	Local Service
Windows Update	Enables the ...		Manual (Trig...	Local Syste...
Windows Update Medic Service	Enables rem...		Manual	Local Syste...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...		Manual	Local Syste...