Secure Private File Server Workflow

https://docs.google.com/document/d/1f5rvNUwAIA-uCdC8hYXMm-GHH27hiLNsijqTgvflvWU/edit?usp=sharing

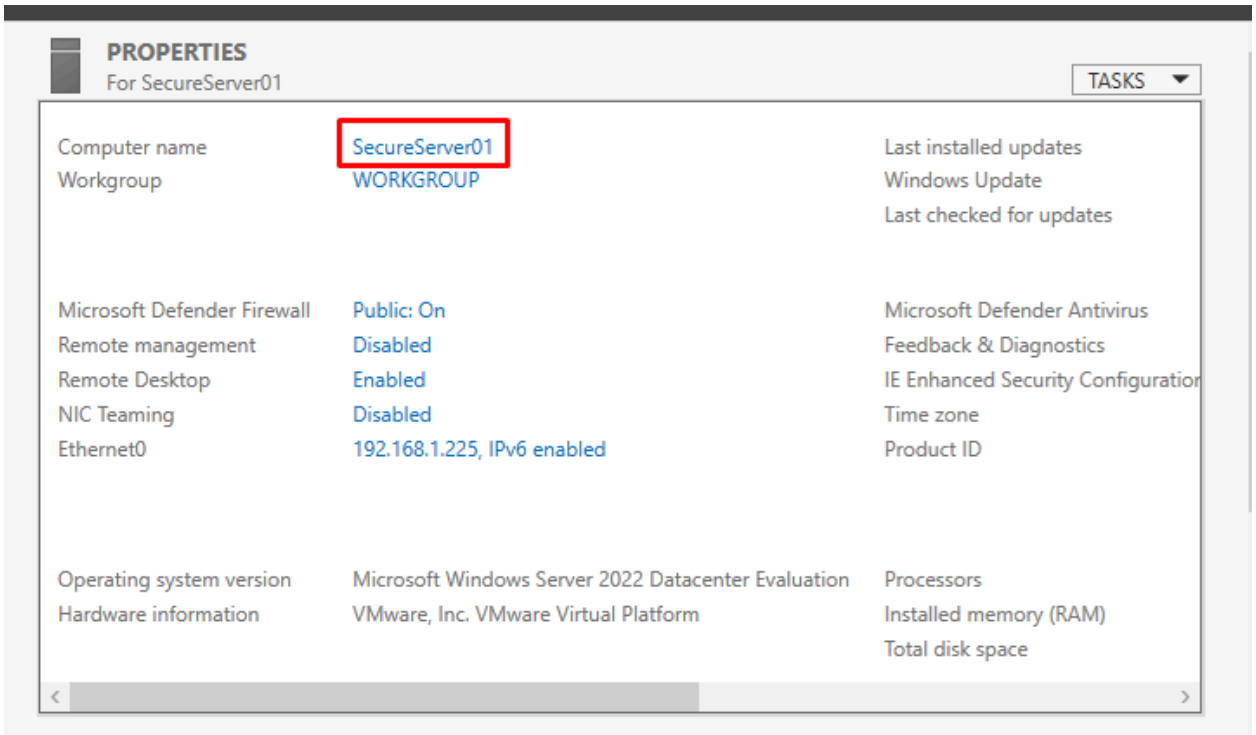
Author: Brennan Tong

STEP 1. Windows Server 2022 Setup

Initial Configuration (First Boot)

After Windows Server 2022 boots up, you'll usually see the **Server Manager** pop up automatically.

- **Set a password** for the Administrator account if not already set.
- **Rename the machine**:
  - Open **Server Manager** → Local Server → click on **Computer Name** → **Change** → Give it a hostname like SecureServer01.

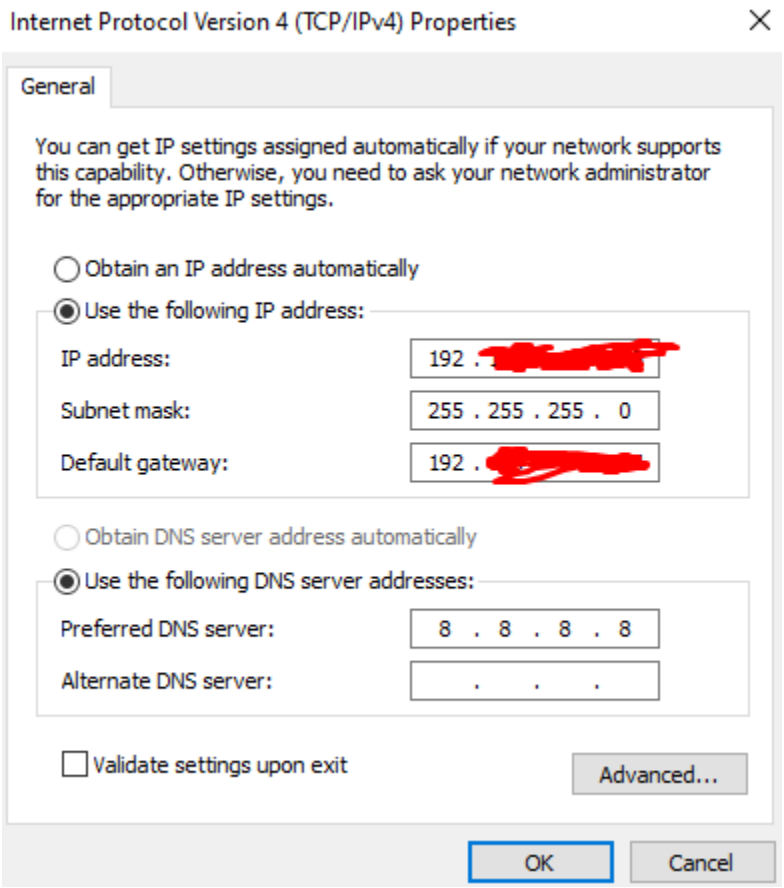


Configure Static IP

We want a *static IP address* so that your server doesn't change IP after reboots.

- Open **Control Panel > Network and Sharing Center** → **Change adapter settings** → Right-click your Ethernet adapter → **Properties**.
- Select **Internet Protocol Version 4 (TCP/IPv4)** → **Properties**.

Set Static IP



Turn Windows Firewall ON (default usually ON)

We will later adjust it to allow only SSH (port 22).

Check:

- **Windows Defender Firewall** > should be ON for Domain, Private, Public profiles.

Enable Remote Desktop

If you want to manage the server remotely:

- Server Manager > Local Server > **Remote Desktop** > Enable.
- Allow connections from machines with Network Level Authentication.

STEP 2. Install OpenSSH Server on Windows Server 2022

Open PowerShell as Administrator:

(Click Start > Search "PowerShell" > Right-click > Run as Administrator)

Then type:

Install OpenSSH Server

Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

```
PS C:\Users\Administrator> Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
>>


Path           :
Online         : True
RestartNeeded  : False
```

Start the SSH server service

Start-Service sshd

Make the SSH server start automatically on boot

Set-Service -Name sshd -StartupType 'Automatic'

Confirm sshd is running

Get-Service -Name sshd

```
PS C:\Users\Administrator> Start-Service sshd
PS C:\Users\Administrator> Set-Service -Name sshd -StartupType 'Automatic'
>>
PS C:\Users\Administrator> Get-Service -Name sshd
>>

Status   Name               DisplayName
------   ----               -----------
Running  sshd               OpenSSH SSH Server
```

It should show Running.

Allow SSH Port 22 Through the Firewall

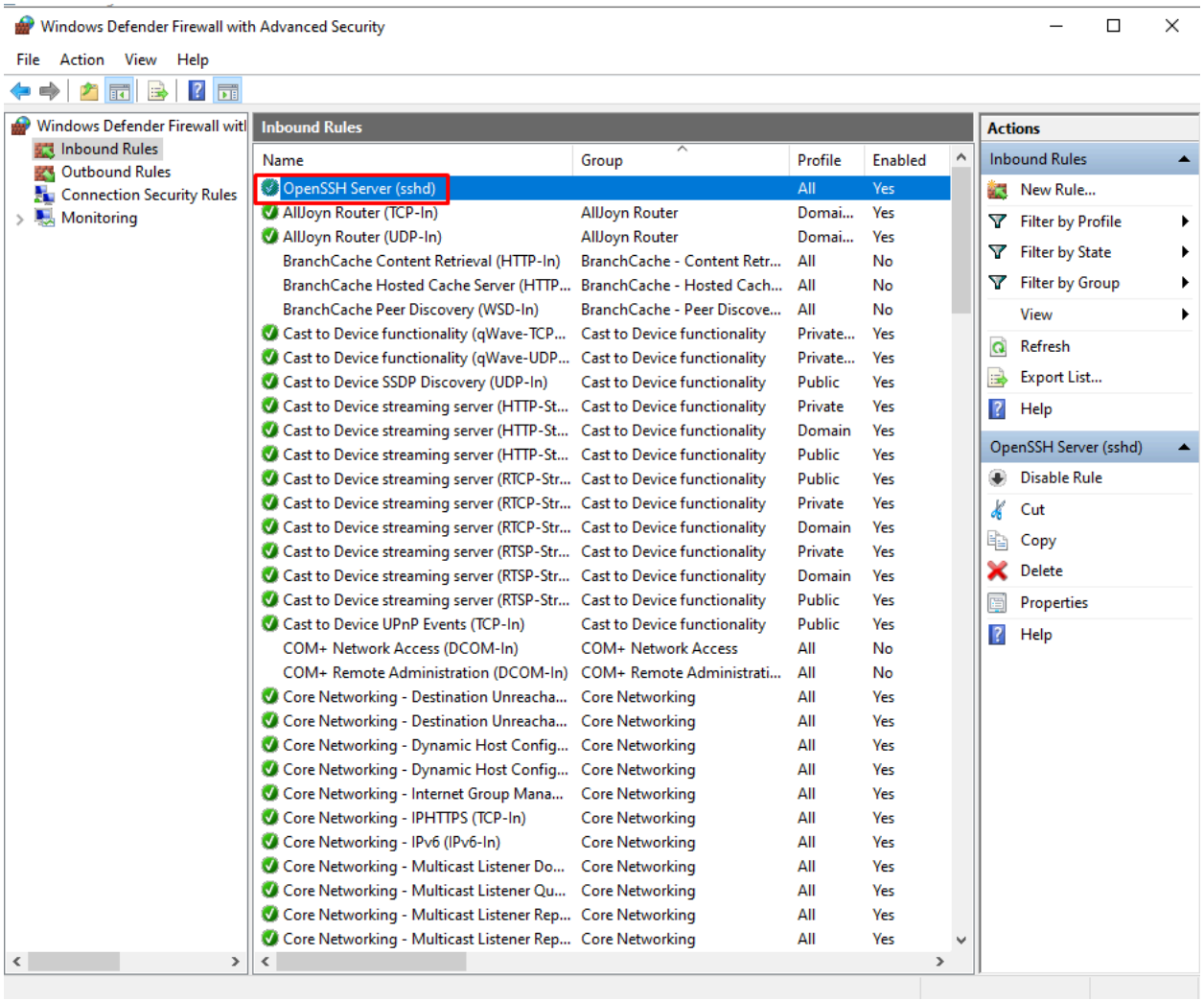
Even though Windows Firewall is ON, it may not allow Port 22 yet.

Still in **PowerShell**, run:

Add firewall rule for SSH

New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

```
PS C:\Users\Administrator> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True
 -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
>>


Name                          : sshd
DisplayName                   : OpenSSH Server (sshd)
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 : {}
```



Why?

We're opening only the port needed, PORT 22.

Set Up Public Key Authentication (very important)

This makes your server immune to brute-force password attacks

On Your Local Machine (Client)

If you don't already have an SSH key:

On Linux/Mac:

ssh-keygen -t rsa -b 4096

On Windows (PowerShell):

ssh-keygen.exe

Press Enter to accept defaults (it saves in ~/.ssh/id_rsa and id_rsa.pub).

You now have:

- id_rsa (Private Key) - **keep it a secret**.
- id_rsa.pub (Public Key) - **you upload this to the server**.

```
PS C:\Users\brenn> ssh-keygen -t rsa -b 4096 -f C:\Users\brenn\.ssh\id_rsa
```

On the Windows Server 2022 VM

Set proper owner and permissions

$acl = Get-Acl "C:\ProgramData\ssh\administrators_authorized_keys"

$acl.SetOwner([System.Security.Principal.NTAccount]"Administrators")

Set-Acl "C:\ProgramData\ssh\administrators_authorized_keys" $acl

icacls "C:\ProgramData\ssh\administrators_authorized_keys" /inheritance:r

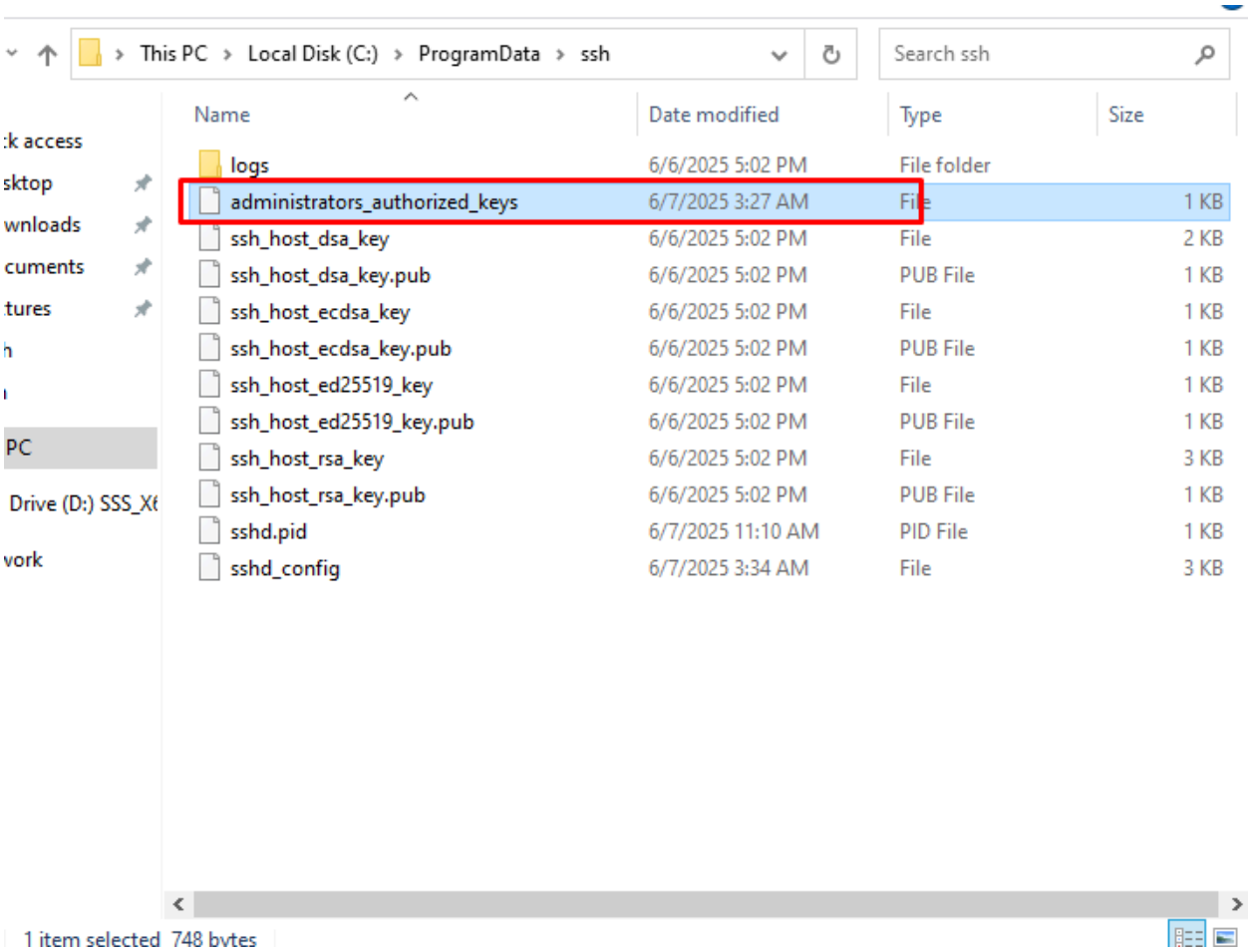
icacls "C:\ProgramData\ssh\administrators_authorized_keys" /grant:r "Administrators:F"

```
PS C:\Users\Administrator> $acl = Get-Acl "C:\ProgramData\ssh\administrators_authorized_keys"
>> $acl.SetOwner([System.Security.Principal.NTAccount]"Administrators")
>> Set-Acl "C:\ProgramData\ssh\administrators_authorized_keys" $acl
>>
PS C:\Users\Administrator> icacls C:\ProgramData\ssh\administrators_authorized_keys /inheritance:r
>> icacls C:\ProgramData\ssh\administrators_authorized_keys /grant:r "Administrators:F"
```

Create the authorized_keys file

notepad C:\ProgramData\ssh\administrators_authorized_keys

Paste your **public key** (id_rsa.pub) contents into administrators_authorized_keys.



Save and exit.

Enforce Public Key Login, Disable Password Authentication

Edit the SSH config file:

notepad C:\ProgramData\ssh\sshd_config

Find and change these settings:

Hardening Settings

PasswordAuthentication no

PubkeyAuthentication yes

StrictModes yes

PermitRootLogin no

MaxAuthTries 7

ClientAliveInterval 600

ClientAliveCountMax 2

Match Group administrators

AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys

Save and exit and restart SSHD:

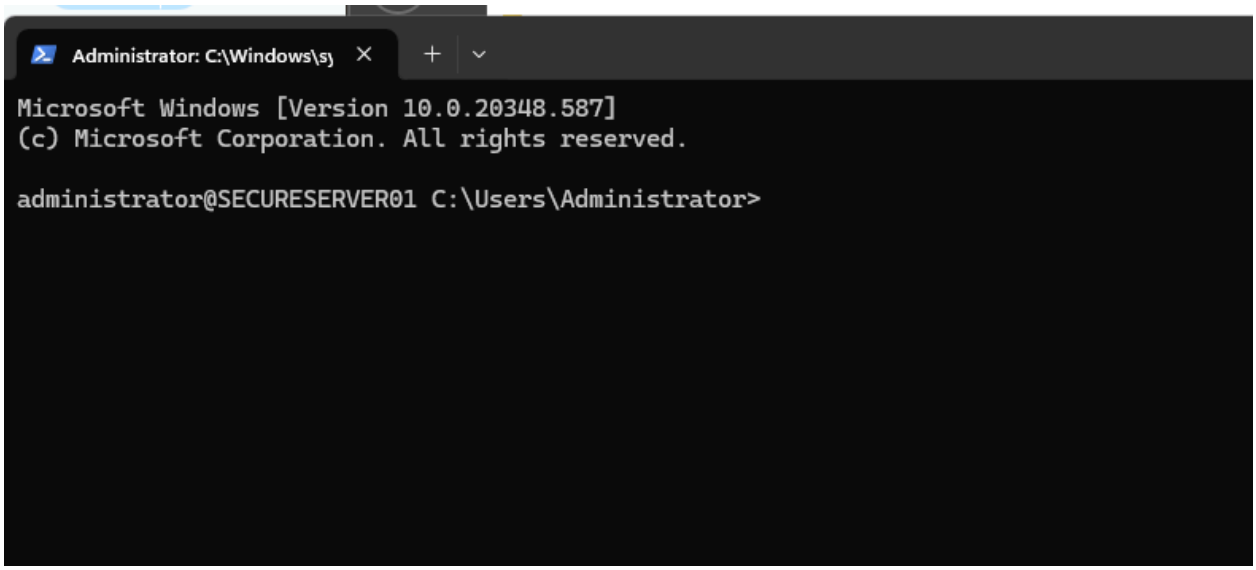
Restart-Service sshd

```
PS C:\Users\Administrator> Restart-Service sshd
```

Test SSH (on local machine)

Try to SSH into your server:

ssh administrator@<your-server-ip>



If successful it should show administrator@SECURESERVER01

Step 3: Download Microsoft Security Compliance Toolkit

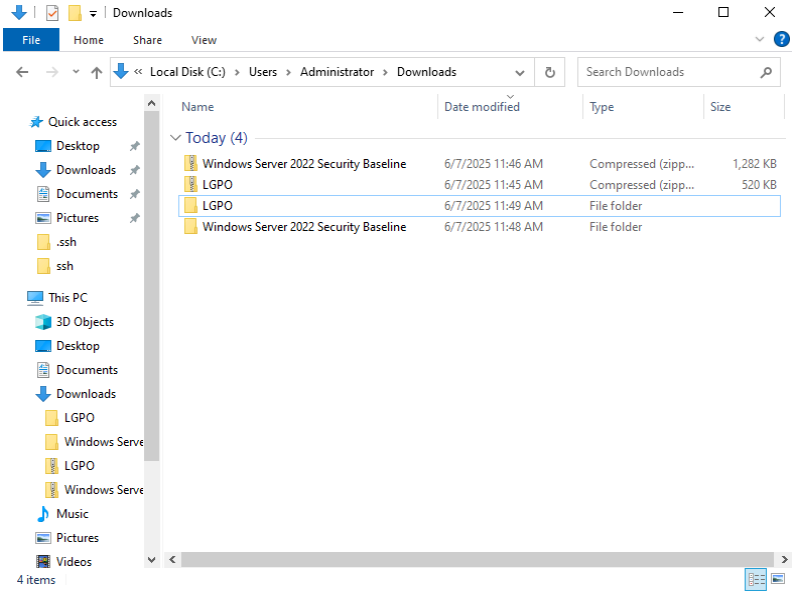
1. Open and download from official Microsoft link:

Microsoft Security Compliance Toolkit Download Page

2. **Select Only**:

☑ Windows Server 2022 Security Baseline.zip	1.3 MB
☐ Windows 10 Update Baseline.zip	452.4 KB
☐ SetObjectSecurity.zip	313.9 KB
☐ PolicyAnalyzer.zip	1.5 MB
☑ LGPO.zip	519.2 KB

Extract and Open It



Step 1: CD to LGPO Folder

cd "C:\Users\Administrator\Downloads\LGPO\LPGO_30"

Step 2: Apply Security Baseline

Run:

.\LGPO.exe /g "C:\Users\Administrator\Downloads\Windows Server 2022 Security Baseline\GPOs\WS2022 Member Server"

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> .\LGPO.exe /g "C:\Users\Administrator\Downloads\Windows Server
22 Security Baseline\GPOs\WS2022 Member Server"
>>

LGPO.exe - Local Group Policy Object Utility
Version 3.0.2004.13001
Copyright (C) 2015-2020 Microsoft Corporation
Security Compliance Toolkit - https://www.microsoft.com/download/details.aspx?id=55319

Invalid directory name for GPO backup: C:\Users\Administrator\Downloads\Windows Server 2022 Security Baseline\GPO
WS2022 Member Server

LGPO.exe has four modes:
  * Import and apply policy settings;
  * Export local policy to a GPO backup;
  * Parse a registry.pol file to "LGPO text" format;
  * Build a registry.pol file from "LGPO text".

To apply policy settings:
```

Step 3: Refresh Policies

After it finishes:

gpupdate /force

4. Disable SMBv1 (Old File Sharing Protocol)

SMBv1 is dangerous, because big exploits like WannaCry used it:

Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol

If it says Restart Required: yes

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

---

5. Disable TLS 1.0 and TLS 1.1 (Old Encryption)

Lock down old SSL/TLS versions (only TLS 1.2 or 1.3).

PowerShell run:

New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name Enabled -Value 0 -PropertyType DWORD -Force

New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name Enabled -Value 0 -PropertyType DWORD -Force

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityPr
oviders\SCHANNEL\Protocols\TLS 1.0\Server" -Force


    Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0


Name                           Property
----                           --------
Server
```

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Se
curityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name Enabled -Value 0 -PropertyType DWORD -Force
>>


Enabled      : 0
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
               viders\SCHANNEL\Protocols\TLS 1.0\Server
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
               viders\SCHANNEL\Protocols\TLS 1.0
PSChildName  : Server
PSDrive      : HKLM
PSProvider   : Microsoft.PowerShell.Core\Registry
```

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityPr
oviders\SCHANNEL\Protocols\TLS 1.1\Server" -Force
>>


    Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1


Name                           Property
----                           --------
Server
```

```
PS C:\Users\Administrator\Downloads\LGPO\LGPO_30> New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Se
curityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name Enabled -Value 0 -PropertyType DWORD -Force
>>


Enabled      : 0
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
               viders\SCHANNEL\Protocols\TLS 1.1\Server
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
               viders\SCHANNEL\Protocols\TLS 1.1
PSChildName  : Server
PSDrive      : HKLM
PSProvider   : Microsoft.PowerShell.Core\Registry
```

---

6. Enable Auto Windows Updates Security Patches

Run:
sconfig

Text-based menu opens
Press 5 (Windows Update Settings)

Choose A) Automatically scan, download, and install updates.

```
Administrator: Windows PowerShell

===============================================================================
              Welcome to Windows Server 2022 Datacenter Evaluation
===============================================================================

  1)  Domain/workgroup:                   Workgroup: WORKGROUP
  2)  Computer name:                      SECURESERVER01
  3)  Add local administrator
  4)  Remote management:                  Enabled

  5)  Update setting:                     Download only
  6)  Install updates
  7)  Remote desktop:                     Enabled (more secure clients)

  8)  Network settings
  9)  Date and time
  10) Telemetry setting:                  Required
  11) Windows activation

  12) Log off user
  13) Restart server
  14) Shut down server
  15) Exit to command line (PowerShell)

Enter number to select an option: 5
```

```
===============================================================================
                                  Update setting
===============================================================================

Current update configuration is: Download only

Select (A)utomatic, (D)ownload only, or (M)anual updates (Blank=Cancel): A
```

```
================================================================================
              Welcome to Windows Server 2022 Datacenter Evaluation
================================================================================

  1)  Domain/workgroup:                    Workgroup: WORKGROUP
  2)  Computer name:                       SECURESERVER01
  3)  Add local administrator
  4)  Remote management:                   Enabled

  5)  Update setting:                      Automatic
  6)  Install updates
  7)  Remote desktop:                      Enabled (more secure clients)

  8)  Network settings
  9)  Date and time
  10) Telemetry setting:                   Required
  11) Windows activation

  12) Log off user
  13) Restart server
  14) Shut down server
  15) Exit to command line (PowerShell)

Enter number to select an option:
```

Step 5: Monitoring Scripts

If the server stops working (SSH goes down), then are notified

---

5.1: Monitor SSHD Service with PowerShell

PowerShell Script to Monitor SSHD

Simple script:

```
# File: C:\Scripts\Monitor-SSHD.ps1

$service = Get-Service -Name 'sshd'

if ($service.Status -ne 'Running') {
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $logMessage = "$timestamp - SSHD Service is NOT running."

    # Log it to a file
    Add-Content -Path "C:\Logs\sshd_monitor.log" -Value $logMessage
```

```
    # Optional: write to Event Log
    Write-EventLog -LogName Application -Source "SSHD Monitor" -EventID 1001 -EntryType
Error -Message $logMessage
} else {
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $logMessage = "$timestamp - SSHD Service is running normally."

    # Log it to a file
    Add-Content -Path "C:\Logs\sshd_monitor.log" -Value $logMessage
}
```

---

1. Create a folder for scripts and logs:

```
New-Item -Path "C:\Scripts" -ItemType Directory
New-Item -Path "C:\Logs" -ItemType Directory
```

2. Save as:
   C:\Scripts\Monitor-SSHD.ps1

Monitor-SSHD - Notepad

File Edit Format View Help

```
# File: Monitor-SSHD.ps1

$service = Get-Service -Name 'sshd'

if ($service.Status -ne 'Running') {
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $logMessage = "$timestamp - SSHD Service is NOT running."

    # Log to file
    Add-Content -Path "C:\Logs\sshd_monitor.log" -Value $logMessage

    # Write to Event log
    Write-EventLog -LogName Application -Source "SSHD Monitor" -EventID 1001 -EntryType Error -Message $logMessage
} else {
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $logMessage = "$timestamp - SSHD Service is running normally."

    # Log to file
    Add-Content -Path "C:\Logs\sshd_monitor.log" -Value $logMessage
}
```

5.2: Automate It with Task Scheduler

If don’t want to manually run this every day.

Set up Scheduled Task:

1. Open Task Scheduler

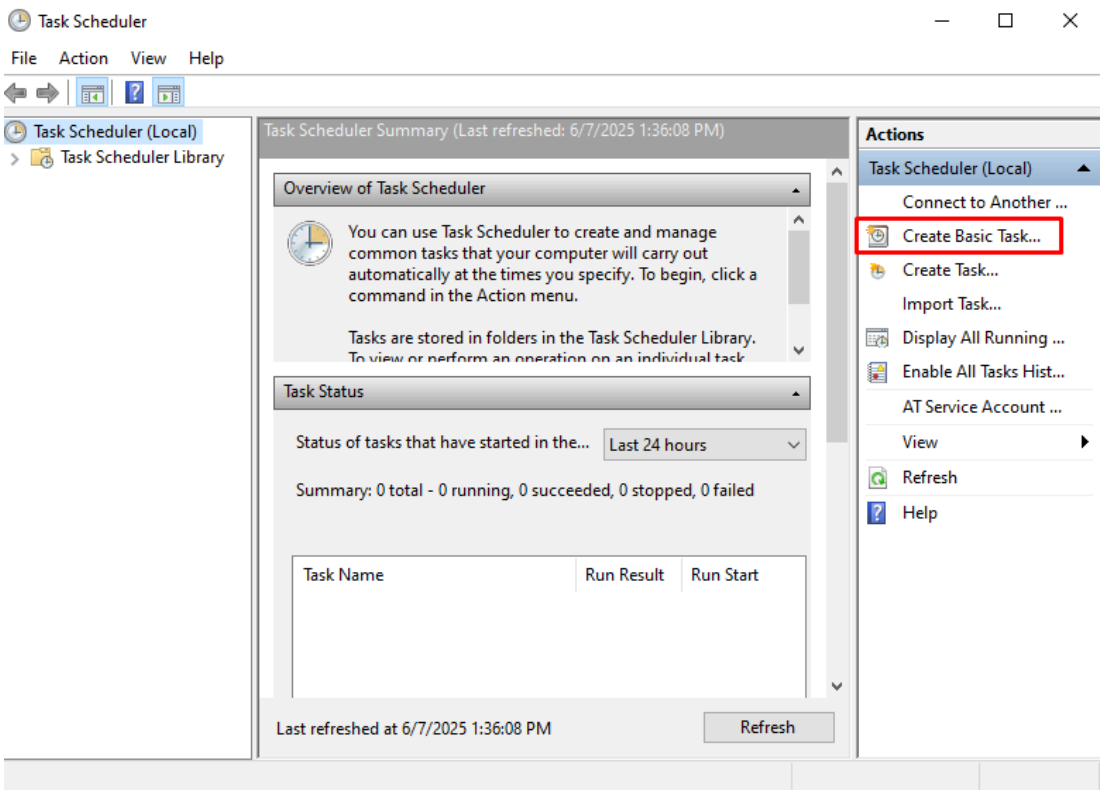
2. Create Basic Task:
   Name: Monitor SSHD Service
   Trigger: Every 5 minutes (or daily)
   Action: Start a program → powershell.exe

Arguments:

-File "C:\Scripts\Monitor-SSHD.ps1"

Every 5 minutes, it will:

Check if SSHD is alive.
Write to C:\Logs\sshd_monitor.log



Create Basic Task Wizard

Create a Basic Task

- Create a Basic Task
- Trigger
- Action
- Finish

Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: Monitor SSHD Service

Description: Monitors if SSHD is running and logs status

< Back | Next > | Cancel

Create Basic Task Wizard

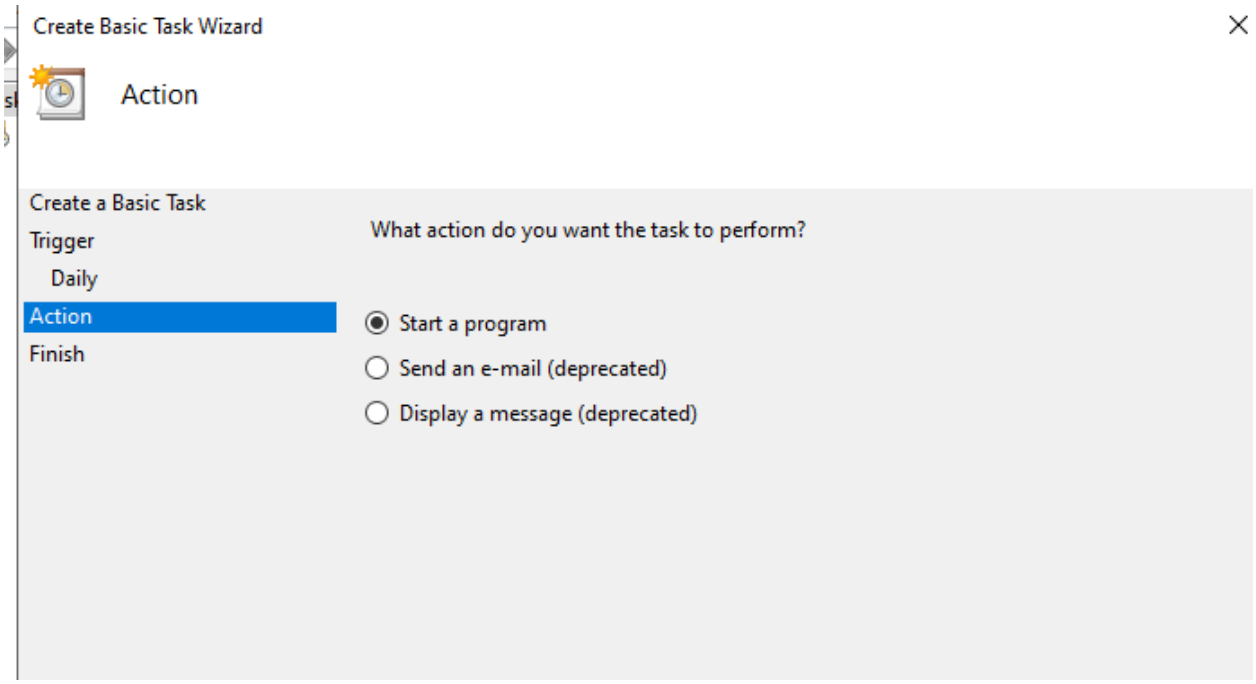
Task Trigger

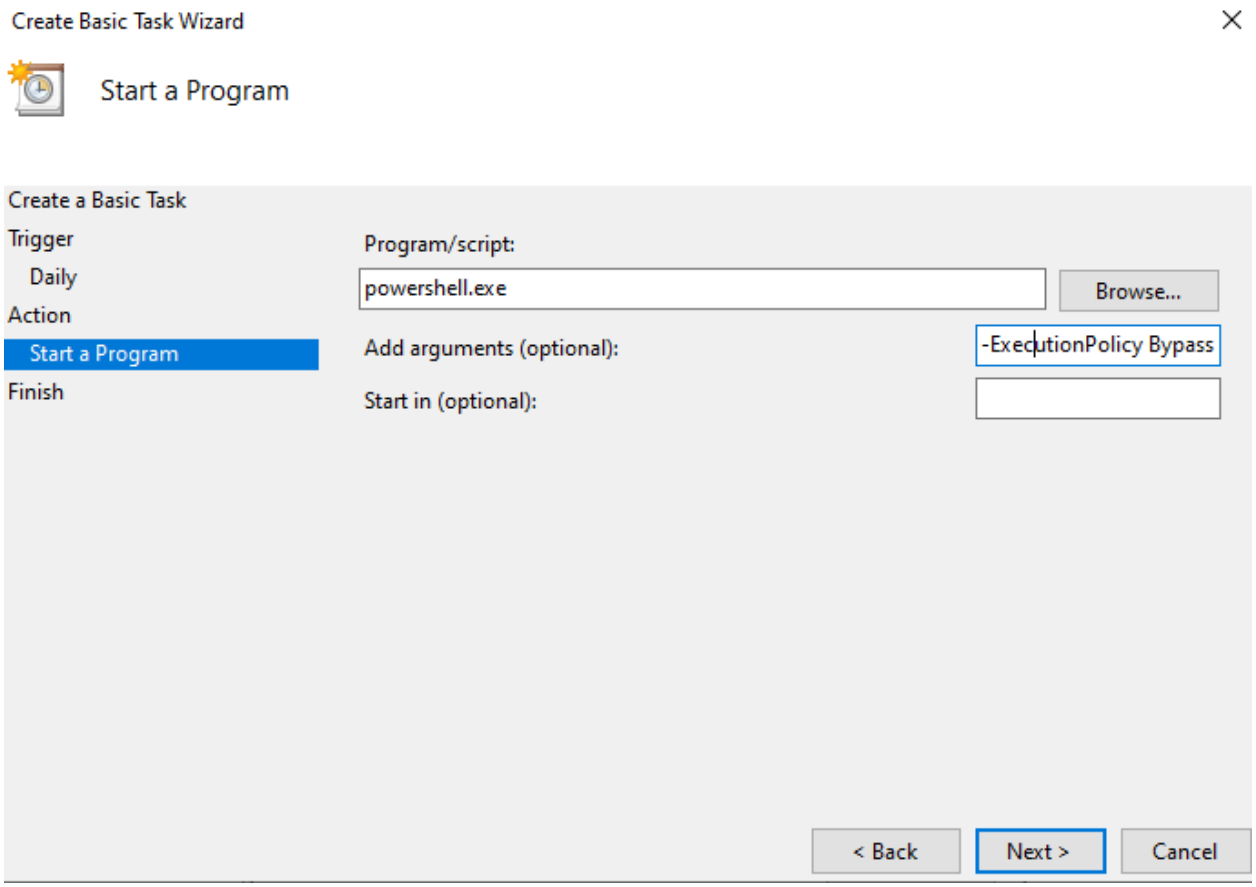
- Create a Basic Task
- Trigger
- Action
- Finish

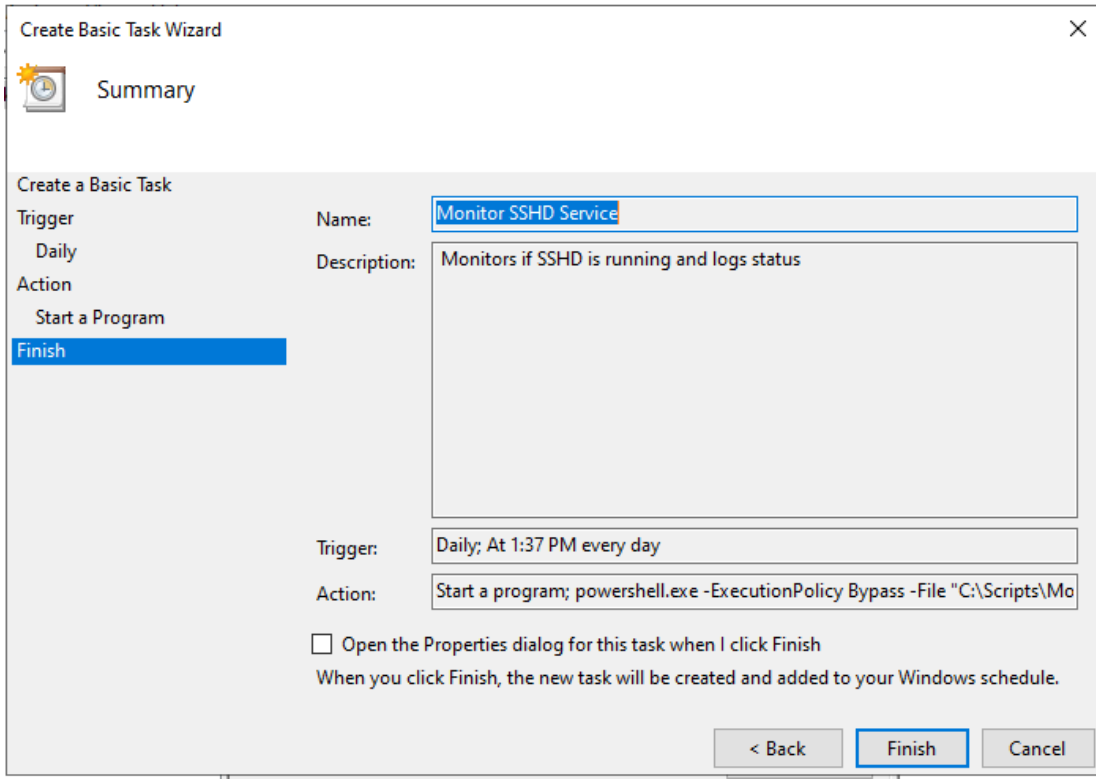
When do you want the task to start?

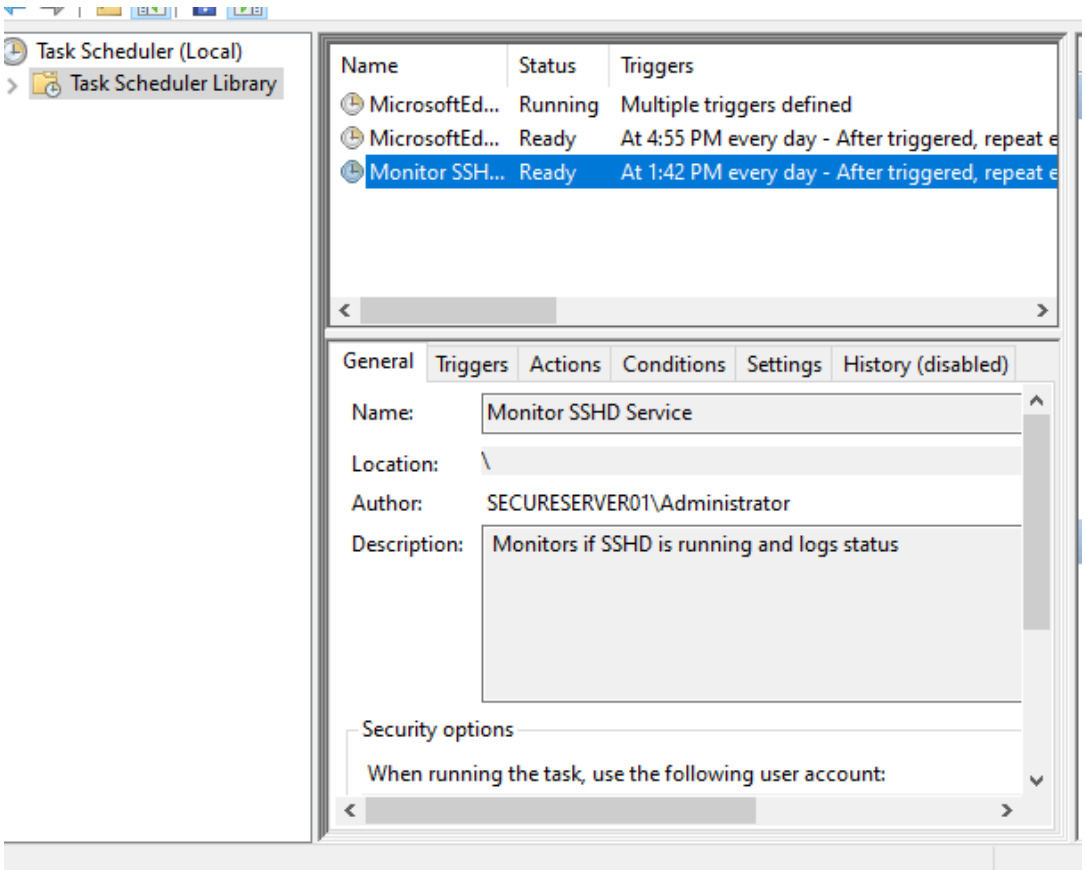
- (●) Daily
- ( ) Weekly
- ( ) Monthly
- ( ) One time
- ( ) When the computer starts
- ( ) When I log on
- ( ) When a specific event is logged

< Back | Next > | Cancel


Create Basic Task Wizard
Action
Create a Basic Task
Trigger
Daily
Action
Finish
What action do you want the task to perform?
Start a program
Send an e-mail (deprecated)
Display a message (deprecated)


Create Basic Task Wizard
Start a Program
Create a Basic Task
Trigger
Daily
Action
Start a Program
Finish
Program/script:
powershell.exe
Browse...
Add arguments (optional):
-ExecutionPolicy Bypass
Start in (optional):
< Back
Next >
Cancel


Create Basic Task Wizard
Summary
Create a Basic Task
Trigger
Daily
Action
Start a Program
Finish
Name:
Monitor SSHD Service
Description:
Monitors if SSHD is running and logs status
Trigger:
Daily; At 1:37 PM every day
Action:
Start a program; powershell.exe -ExecutionPolicy Bypass -File "C:\Scripts\Mo
Open the Properties dialog for this task when I click Finish
When you click Finish, the new task will be created and added to your Windows schedule.
< Back
Finish
Cancel


Task Scheduler (Local)
Task Scheduler Library
Name
Status
Triggers
MicrosoftEd...
Running
Multiple triggers defined
MicrosoftEd...
Ready
At 4:55 PM every day - After triggered, repeat e
Monitor SSH...
Ready
At 1:42 PM every day - After triggered, repeat e
General
Triggers
Actions
Conditions
Settings
History (disabled)
Name:
Monitor SSHD Service
Location:
\
Author:
SECURESERVER01\Administrator
Description:
Monitors if SSHD is running and logs status
Security options
When running the task, use the following user account:

Step 6: Backup and Disaster Recovery

Goal:

Set up automatic backups if server crashes, gets hacked or data lost.

6.1: Install Windows Server Backup

Windows Server Backup, need to add manually

Install It with PowerShell

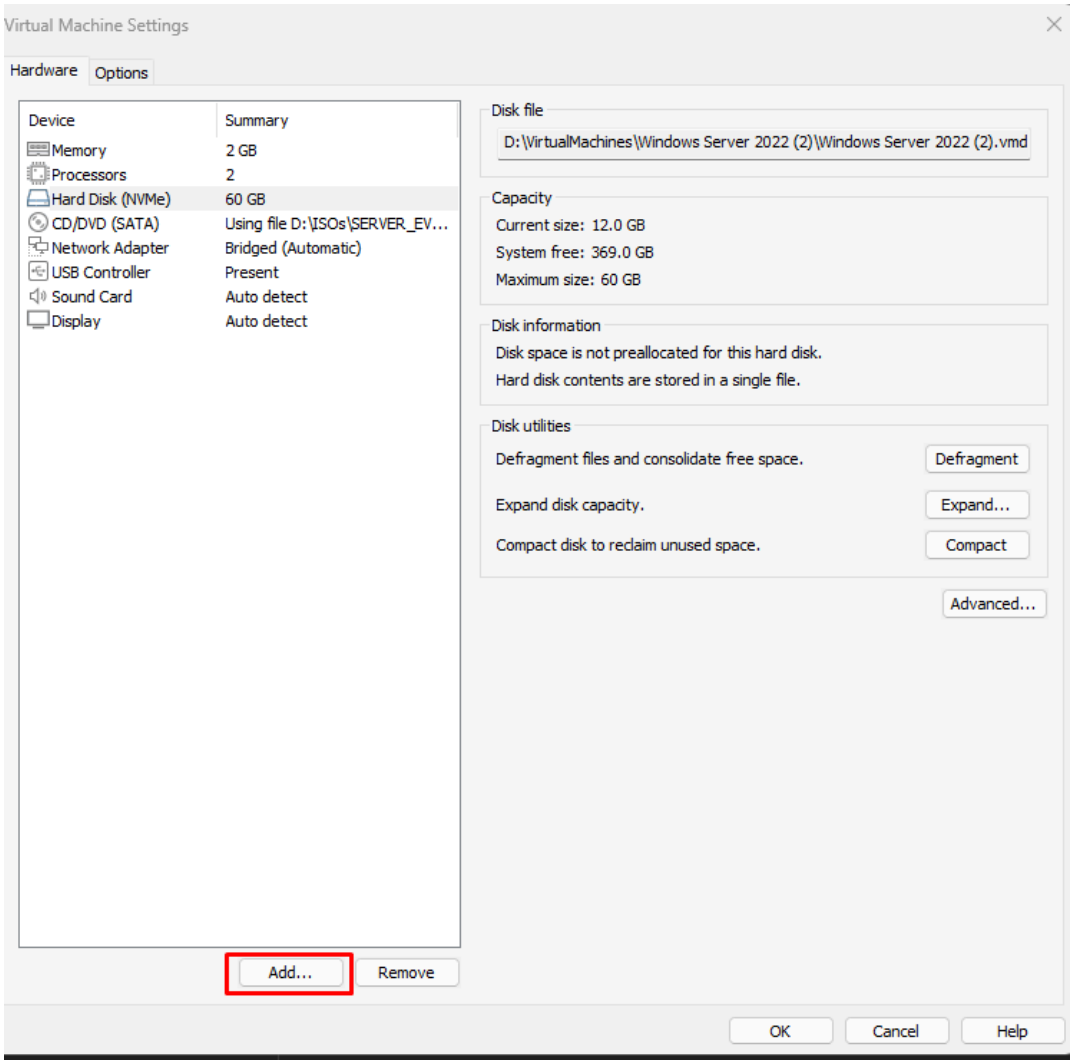
Open PowerShell as Admin:

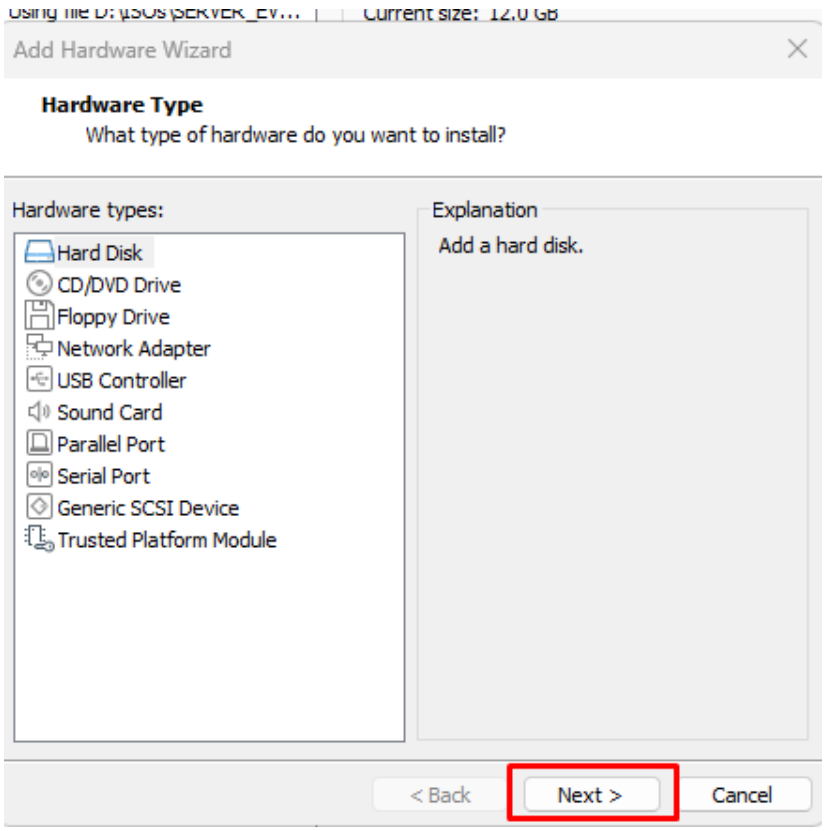
Install-WindowsFeature Windows-Server-Backup

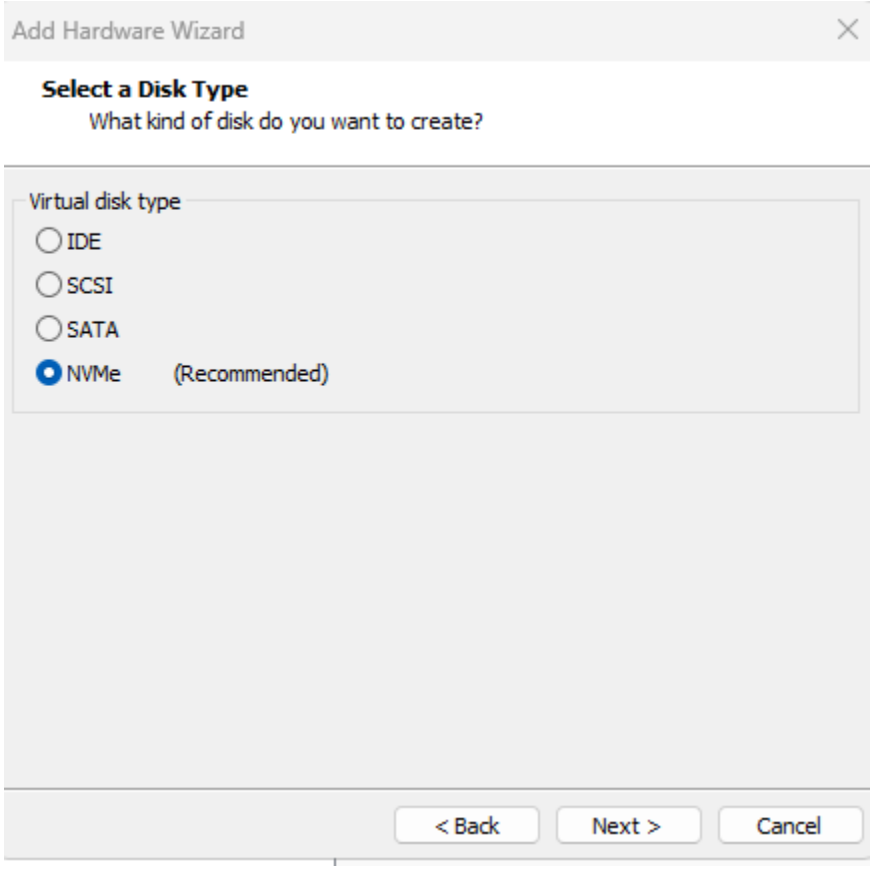
```
PS C:\> Install-WindowsFeature Windows-Server-Backup

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Windows Server Backup}


PS C:\>
```

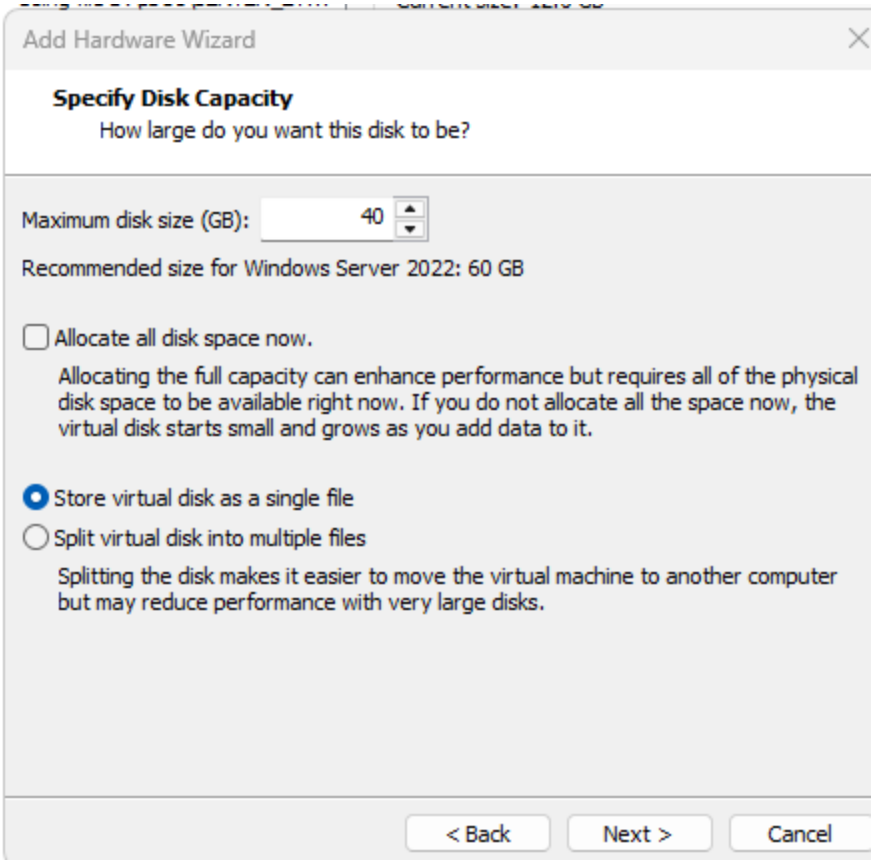
6.2: Set Up a Backup Schedule

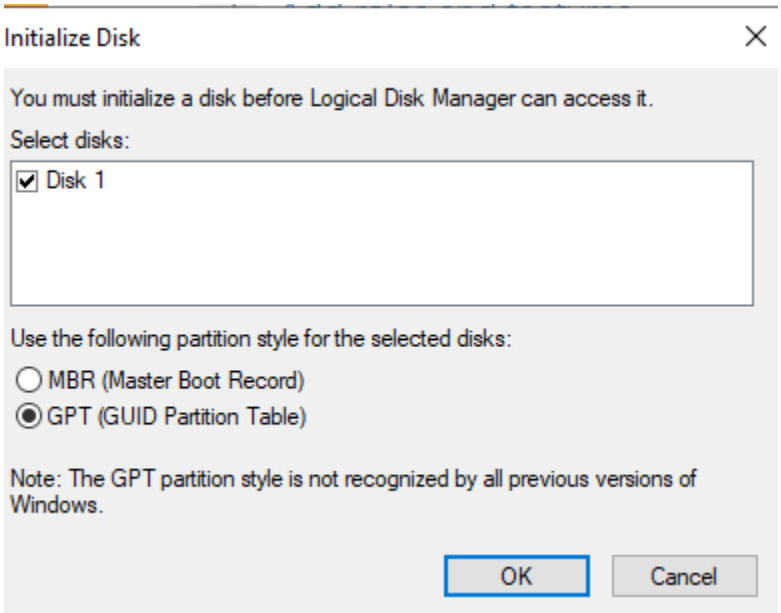
Create Another Backup Hardware on VM:


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (NVMe)
60 GB
CD/DVD (SATA)
Using file D:\ISOs\SERVER_EV...
Network Adapter
Bridged (Automatic)
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Disk file
D:\VirtualMachines\Windows Server 2022 (2)\Windows Server 2022 (2).vmd
Capacity
Current size: 12.0 GB
System free: 369.0 GB
Maximum size: 60 GB
Disk information
Disk space is not preallocated for this hard disk.
Hard disk contents are stored in a single file.
Disk utilities
Defragment files and consolidate free space.
Defragment
Expand disk capacity.
Expand...
Compact disk to reclaim unused space.
Compact
Advanced...
OK
Cancel
Help

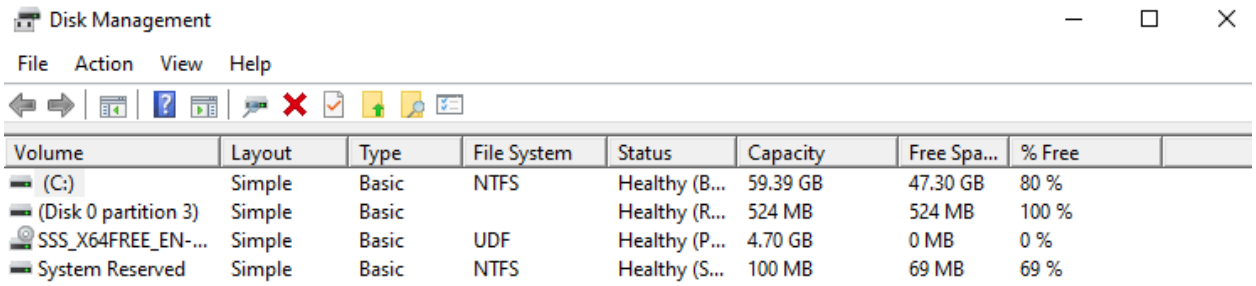

Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
CD/DVD Drive
Floppy Drive
Network Adapter
USB Controller
Sound Card
Parallel Port
Serial Port
Generic SCSI Device
Trusted Platform Module
Explanation
Add a hard disk.
< Back
Next >
Cancel

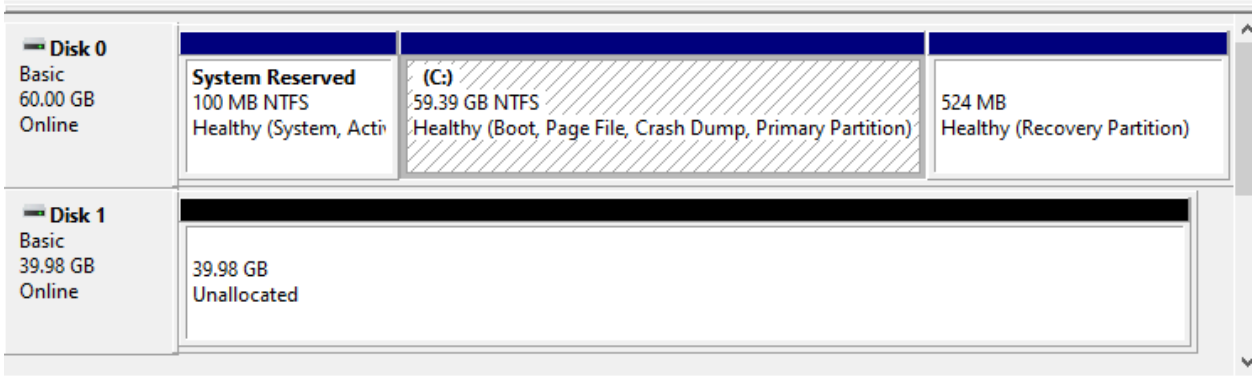

Add Hardware Wizard
Select a Disk Type
What kind of disk do you want to create?
Virtual disk type
IDE
SCSI
SATA
NVMe (Recommended)
< Back
Next >
Cancel

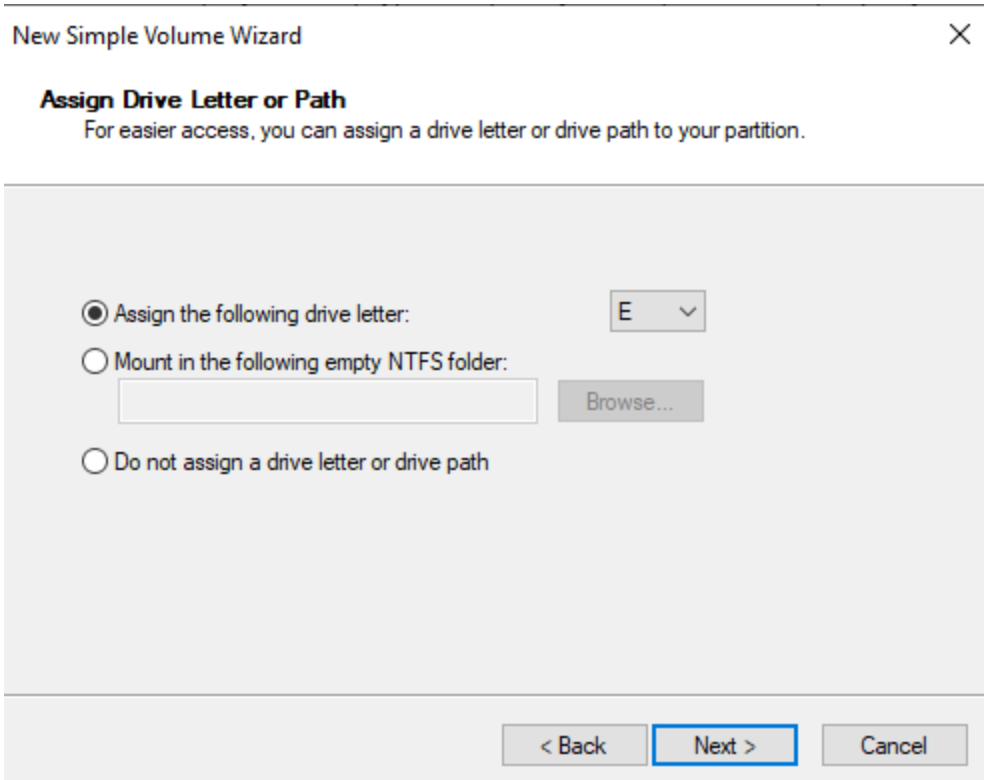

Add Hardware Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB):
40
Recommended size for Windows Server 2022: 60 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
< Back
Next >
Cancel

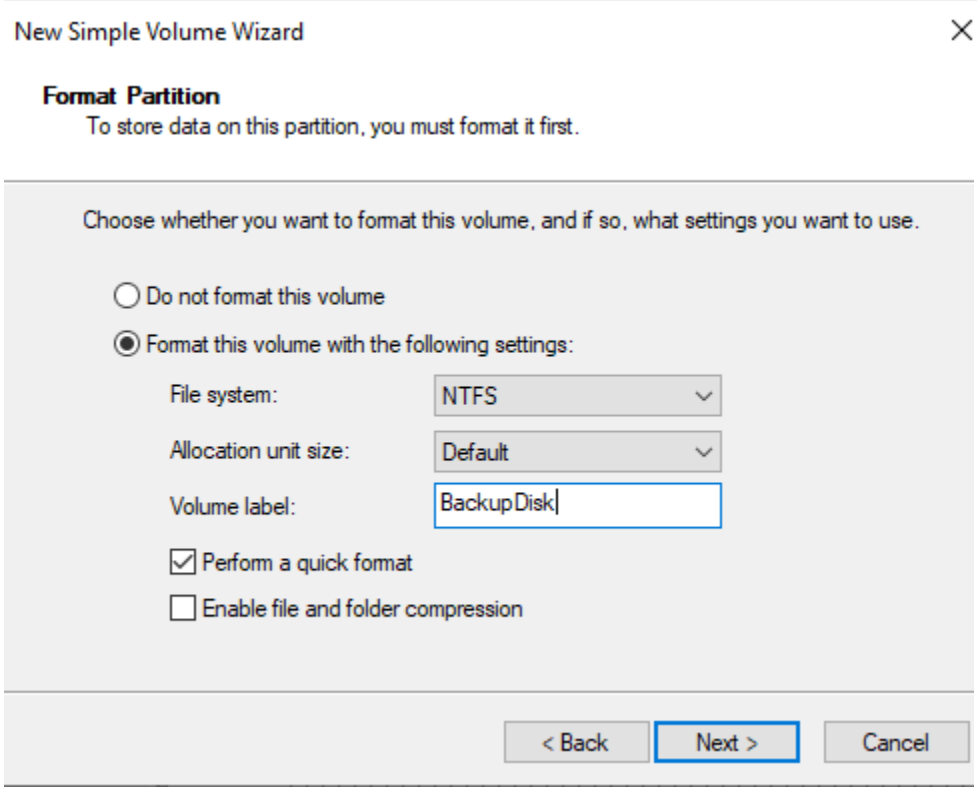

Initialize Disk
You must initialize a disk before Logical Disk Manager can access it.
Select disks:
Disk 1
Use the following partition style for the selected disks:
MBR (Master Boot Record)
GPT (GUID Partition Table)
Note: The GPT partition style is not recognized by all previous versions of Windows.
OK
Cancel

Allocate New Hard Drive:





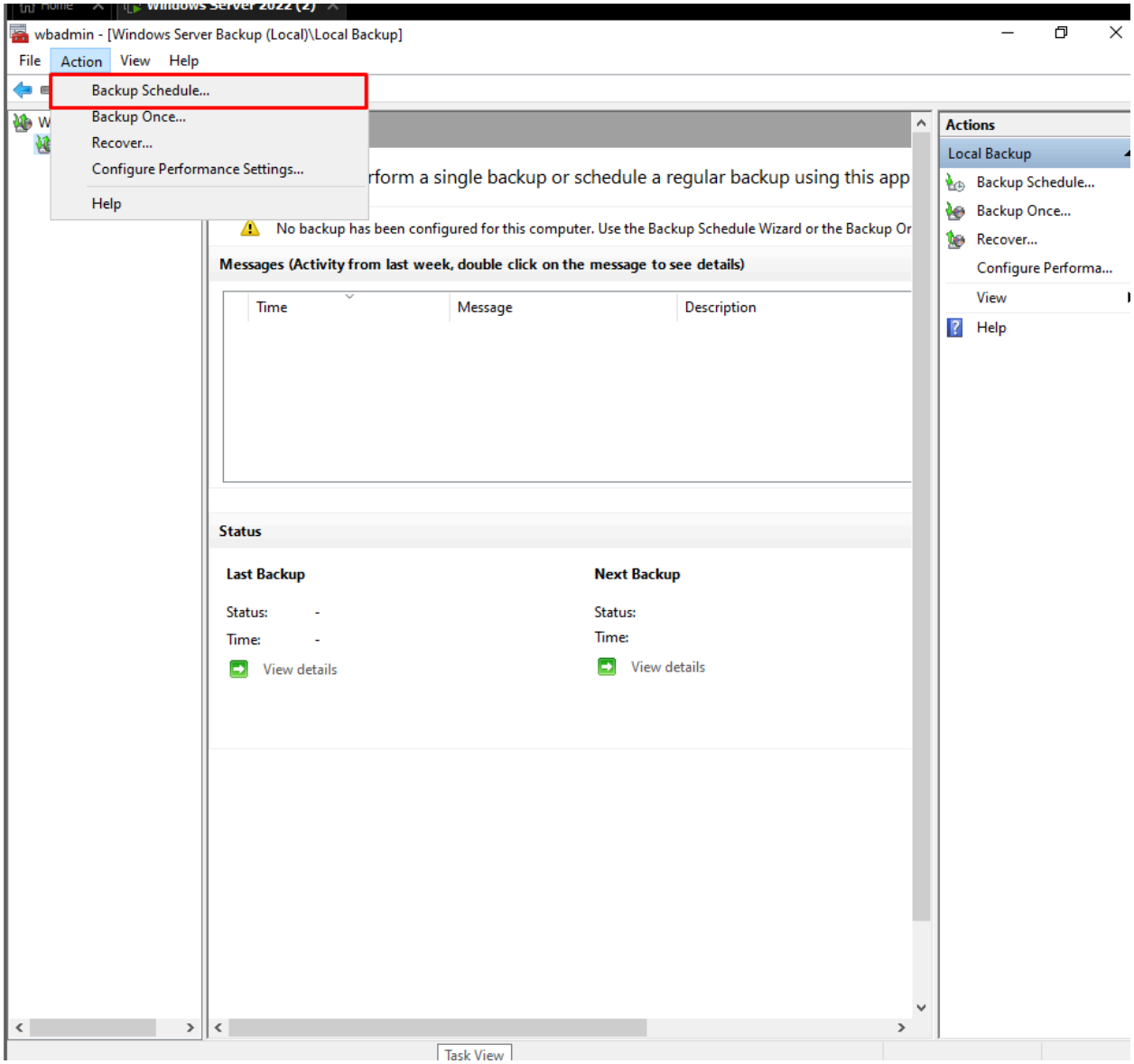




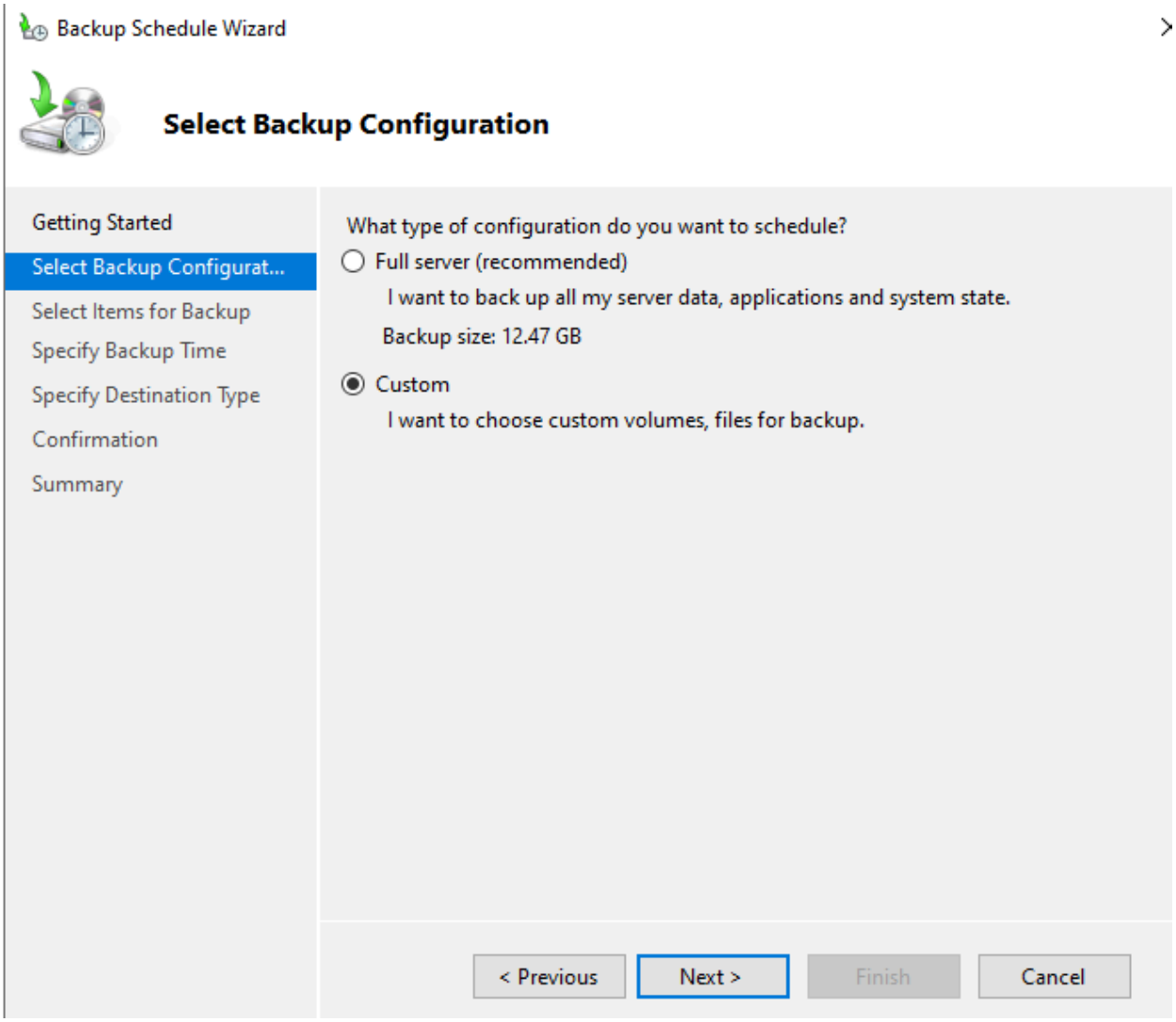
Schedule a Regular Backup

1. Open Windows Server Backup.

2. In Actions pane, click **Backup Schedule**.



Backup Configuration:
Choose **Custom**



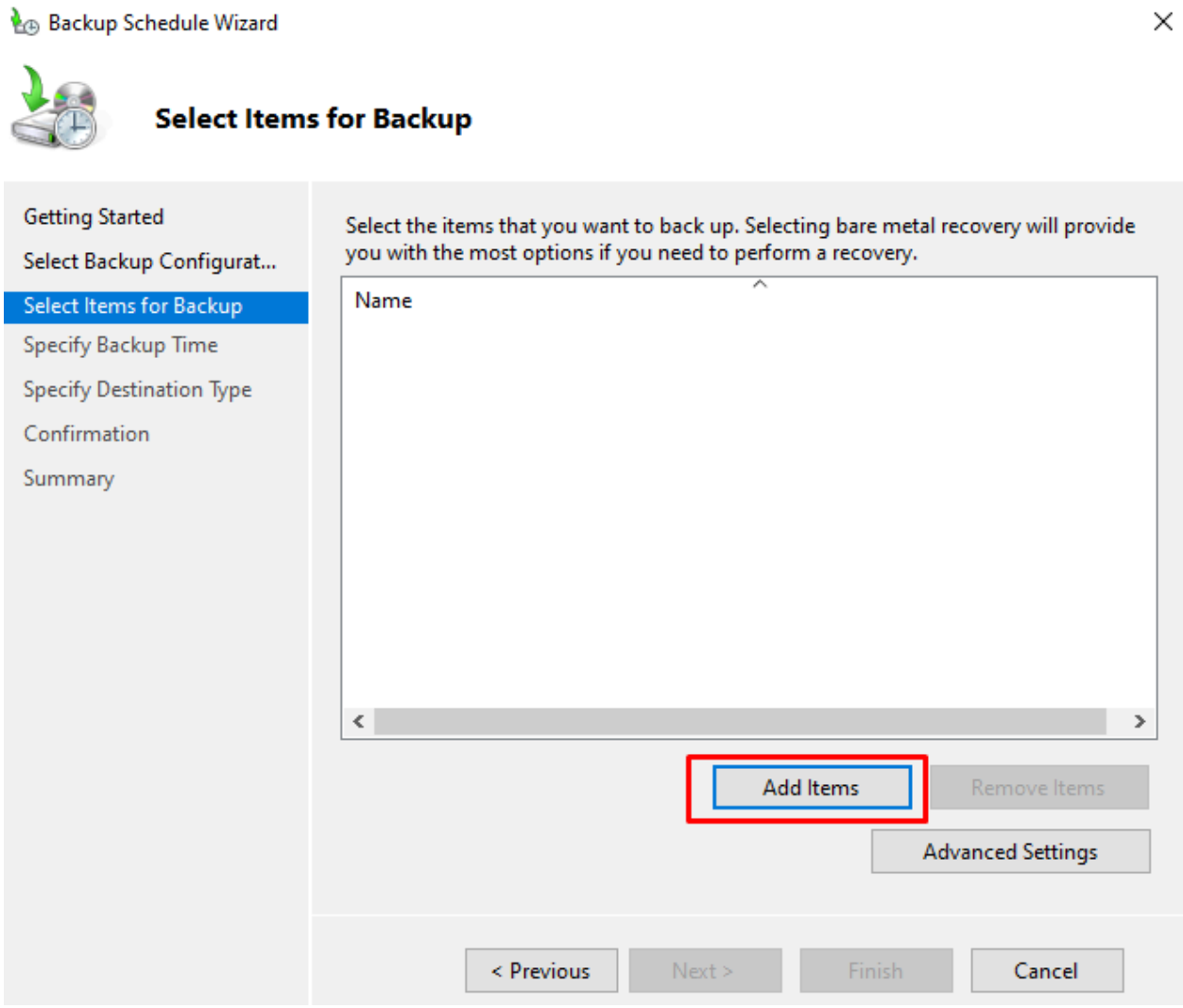
Select Items:

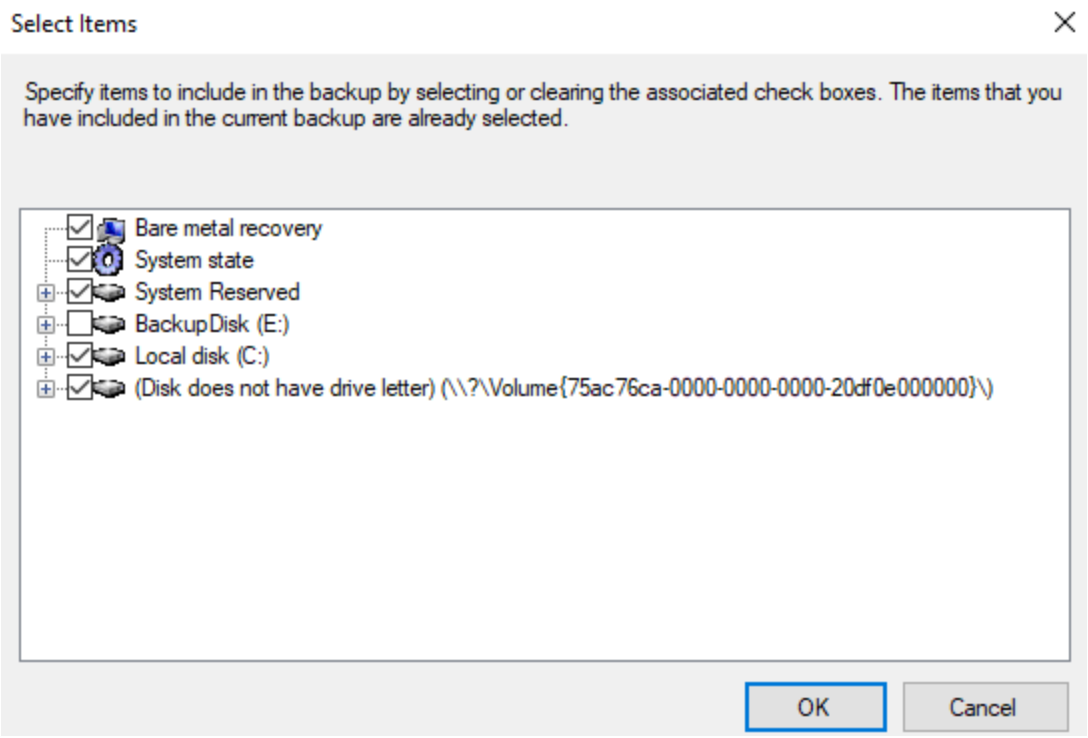
Backup:

System State (includes registry, AD, etc.)

Bare Metal Recovery (for full server recovery).

Important folders like C:\Scripts, C:\Logs, or user data.


Backup Schedule Wizard
Select Items for Backup
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Confirmation
Summary
Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.
Name
Add Items
Remove Items
Advanced Settings
< Previous
Next >
Finish
Cancel



Specify Backup Time:

Pick a time (4 AM)
Daily backup

Destination:
A second virtual hard disk (on VMware)

Backup Schedule Wizard

Specify Backup Time

- Getting Started
- Select Backup Configurat...
- Select Items for Backup
- Specify Backup Time
- Specify Destination Type
- Confirmation
- Summary

How often and when do you want to run backups?

(●) Once a day

Select time of day: 4:00 AM

( ) More than once a day

Click an available time and then click Add to add it to the backup schedule.

Available time:		Scheduled time:
12:00 AM	Add >	9:00 PM
12:30 AM	< Remove	
1:00 AM		
1:30 AM		
2:00 AM		
2:30 AM		
3:00 AM		
3:30 AM		
4:00 AM		
4:30 AM		

< Previous | Next > | Finish | Cancel

Backup Schedule Wizard

Specify Destination Type

- Getting Started
- Select Backup Configurat...
- Select Items for Backup
- Specify Backup Time
- Specify Destination Type
- Select Destination Disk
- Confirmation
- Summary

Where do you want to store the backups?

(●) Back up to a hard disk that is dedicated for backups (recommended)

Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

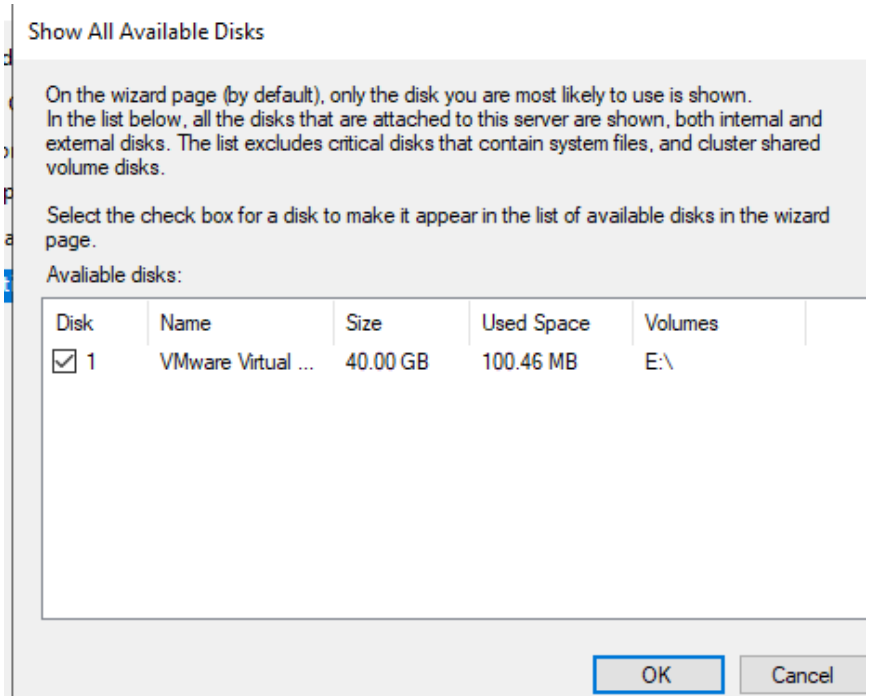
( ) Back up to a volume

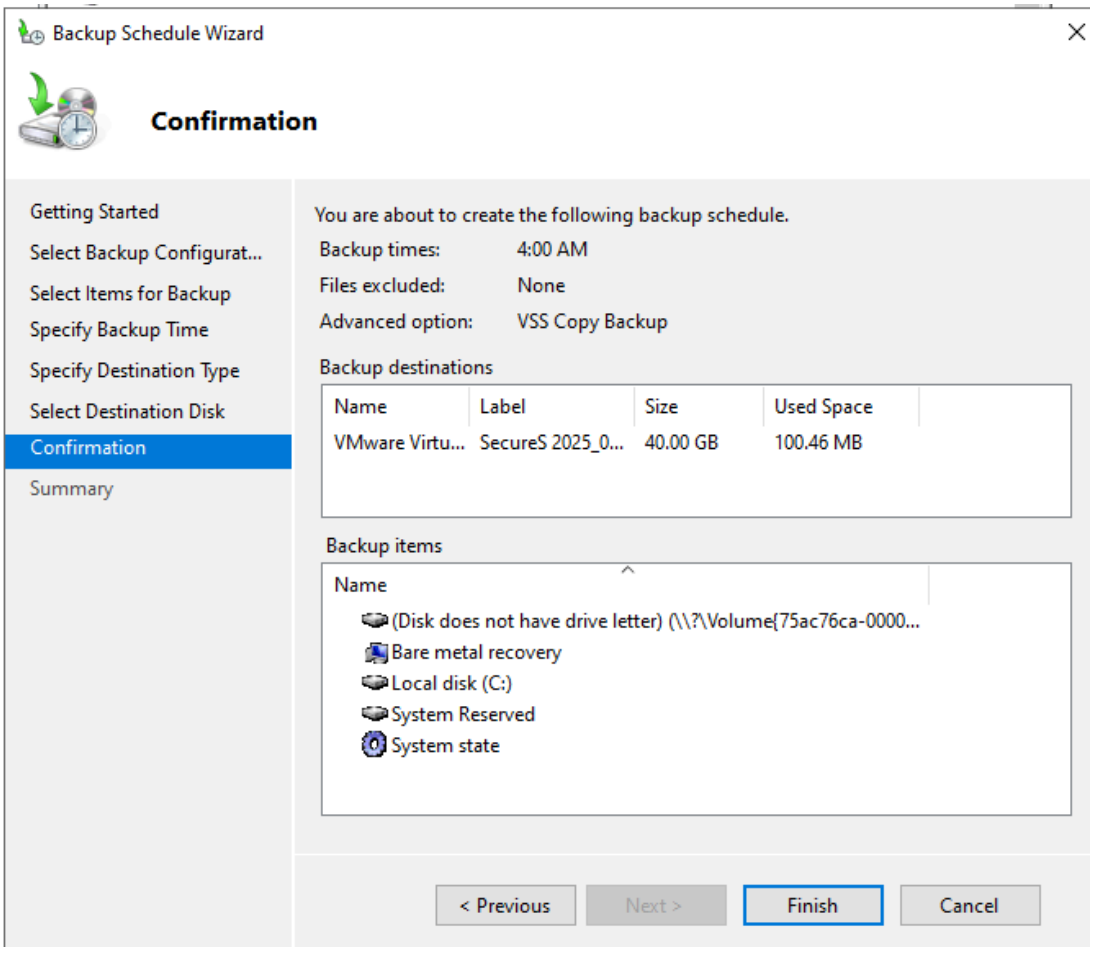
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

( ) Back up to a shared network folder

Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.

< Previous | Next > | Finish | Cancel


Show All Available Disks
On the wizard page (by default), only the disk you are most likely to use is shown.
In the list below, all the disks that are attached to this server are shown, both internal and external disks. The list excludes critical disks that contain system files, and cluster shared volume disks.
Select the check box for a disk to make it appear in the list of available disks in the wizard page.
Avaliable disks:
Disk
Name
Size
Used Space
Volumes
1
VMware Virtual ...
40.00 GB
100.46 MB
E:\
OK
Cancel


Backup Schedule Wizard
Confirmation
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
You are about to create the following backup schedule.
Backup times: 4:00 AM
Files excluded: None
Advanced option: VSS Copy Backup
Backup destinations
Name
Label
Size
Used Space
VMware Virtu...
SecureS 2025_0...
40.00 GB
100.46 MB
Backup items
Name
(Disk does not have drive letter) (\\?\Volume{75ac76ca-0000...
Bare metal recovery
Local disk (C:)
System Reserved
System state
< Previous
Next >
Finish
Cancel

Full SFTP Upload/Download Demo Commands

Imagine you have a confidential file locally, and you want to:

1. Upload (put) it to the secure server.
2. Download (get) it back to a different folder — proving encryption and security both ways.

Step-by-Step Commands

1. Prepare a Test File Locally

On your local laptop **before** you SFTP:

echo "This is top secret." > confidential.txt

```
PS C:\WINDOWS\system32> echo "This is top secret." > confidential.txt
```

Creates confidential.txt with "This is top secret." inside it.

---

2. Open Secure SFTP Session

sftp administrator@192.XXX.XXX.X

You should now see:

sftp>

```
PS C:\WINDOWS\system32> sftp administrator@[redacted]
Connected to [redacted].
sftp> lpwd
Local working directory: c:\windows\system32
sftp> lls
 Volume in drive C is Windows-SSD
 Volume Serial Number is 7ADF-8A7F

 Directory of C:\Windows\System32
```

---

3. Check Your Local Working Directory (Where SFTP Is Pulling From)

lpwd

Example output:

Local working directory: C:\Users\YourName

Confirms where your local confidential.txt is coming from.

---

4. Check Local Files (List Them)

lls

Example output:

confidential.txt
otherdocument.docx

You see your confidential.txt.

---

5. Check Server Directory (Where You Are on the Server)

pwd

Example output:

Remote working directory: /C:/Users/Administrator

You are in the server's Administrator home folder.

---

6. Upload the File to the Server

put confidential.txt

This uploads confidential.txt to the server securely.

Output:

Uploading confidential.txt to /C:/Users/Administrator/confidential.txt
confidential.txt 100% 21 3.2KB/s 00:00

```
sftp> put confidential.txt
Uploading confidential.txt to /C:/Users/Administrator/confidential.txt
confidential.txt
```

---

7. List Files on the Server (Check Upload)

ls

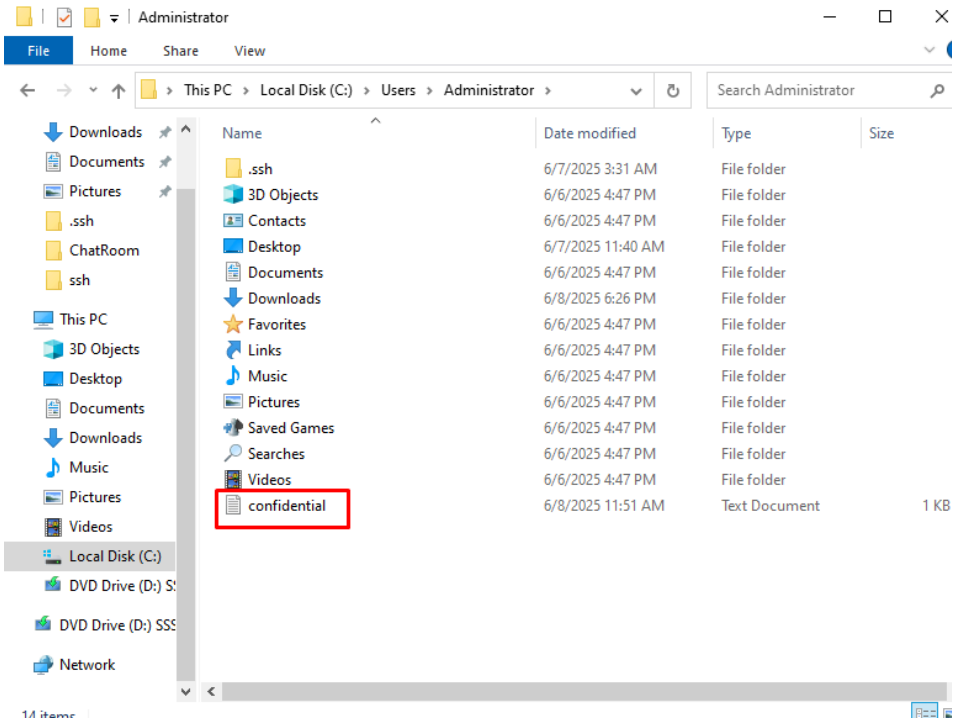
You should see:

Desktop
Documents
Downloads
confidential.txt

Confirms the file is now on the server.

```
Recent

Saved Games

Searches

SendTo

Start Menu

Templates

Videos

confidential.txt

ntuser.dat.LOG1

ntuser.dat.LOG2

ntuser.ini

sftp>
```

Server VM successfully received file from local machine:



8. Download the File Back to Another Folder (Optional Proof)

Change your **local** directory to a different folder first:

lcd C:\Users\YourName\Downloads
lpwd

Example:

Local working directory: C:\Users\YourName\Desktop

```
sftp> lcd C:\Users\brenn\Downloads
sftp> lpwd
Local working directory: c:\users\brenn\downloads
```

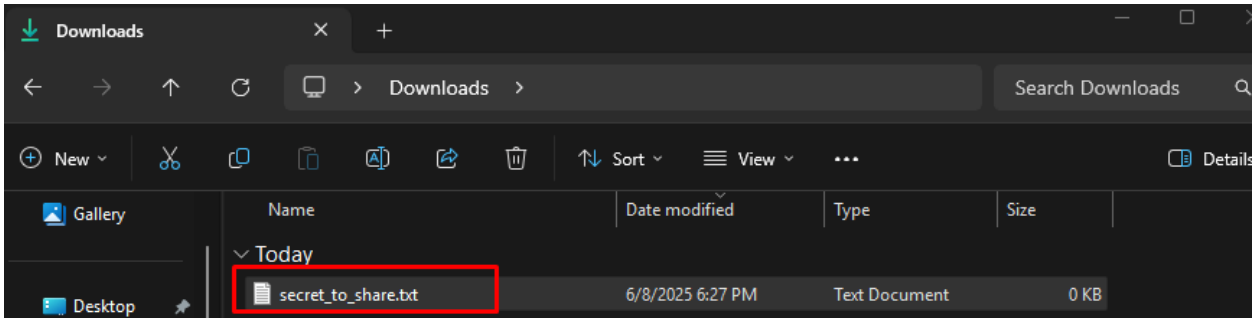
Now download:

get secret_to_share.txt

It downloads the file securely **to your Desktop**.

```
sftp> get secret_to_share.txt
Fetching /C:/Users/Administrator/Downloads/secret_to_share.txt to secret_to_share.txt
sftp>
```

Local Machine, got file from server:



9. Exit SFTP

exit

Result

- confidential.txt was safely sent to the server.
- You securely retrieved it back, showing **both upload and download are encrypted**.

All of this went through an SSH encrypted tunnel, 100% protected.