Documentation Mary Shiner Creating NFS file using Windows Server Manager

References:
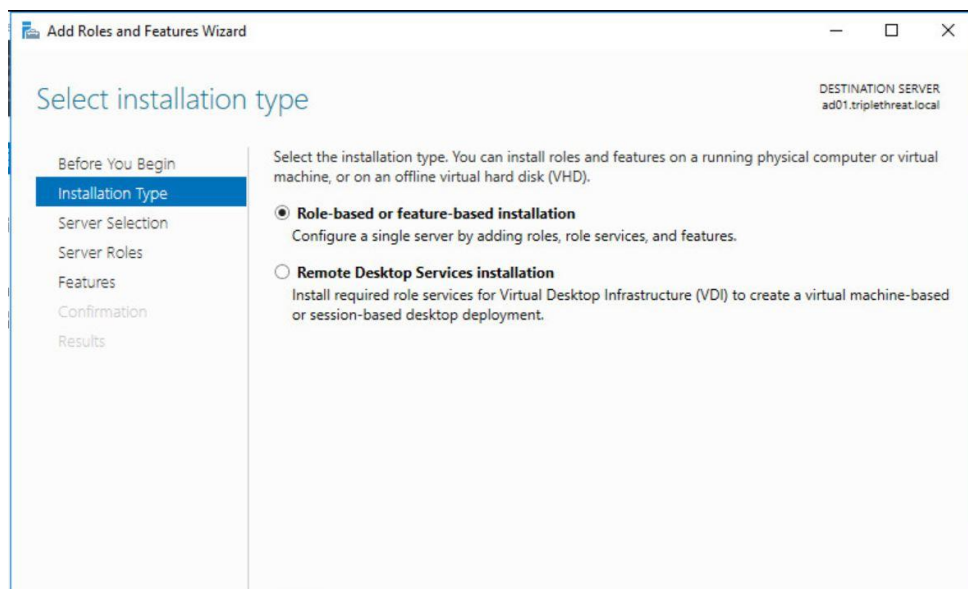
https://docs.microsoft.com/en-us/windows-server/storage/nfs/deploy-nfs configuring NFS and creating a file

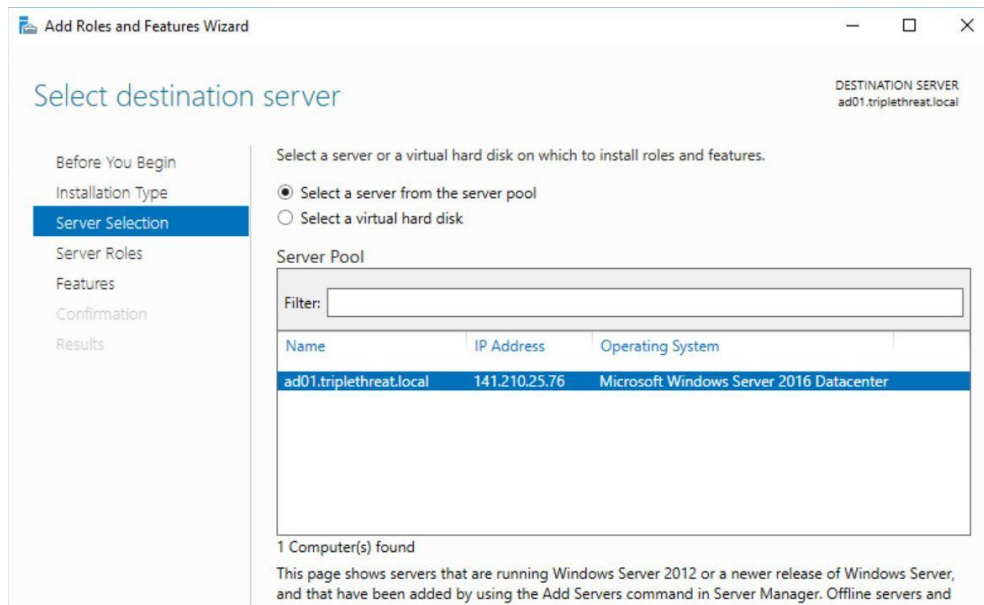# Install Network File System on the server with Server Manager

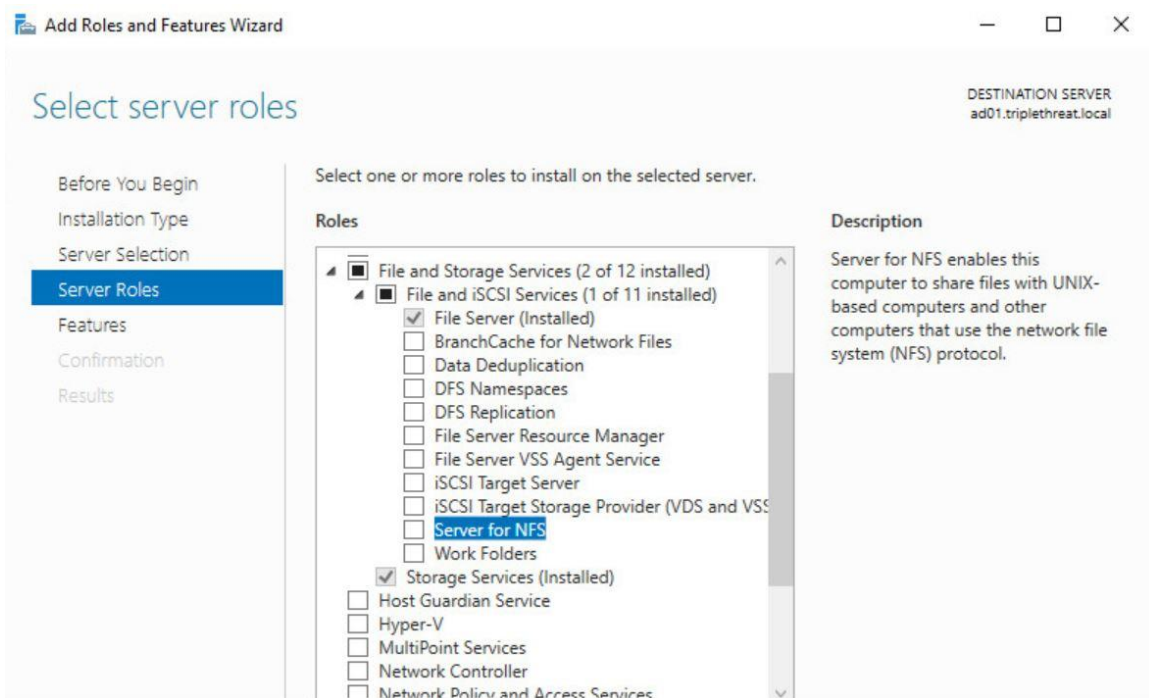1. We are now going to install NFS via Add Roles and Features.
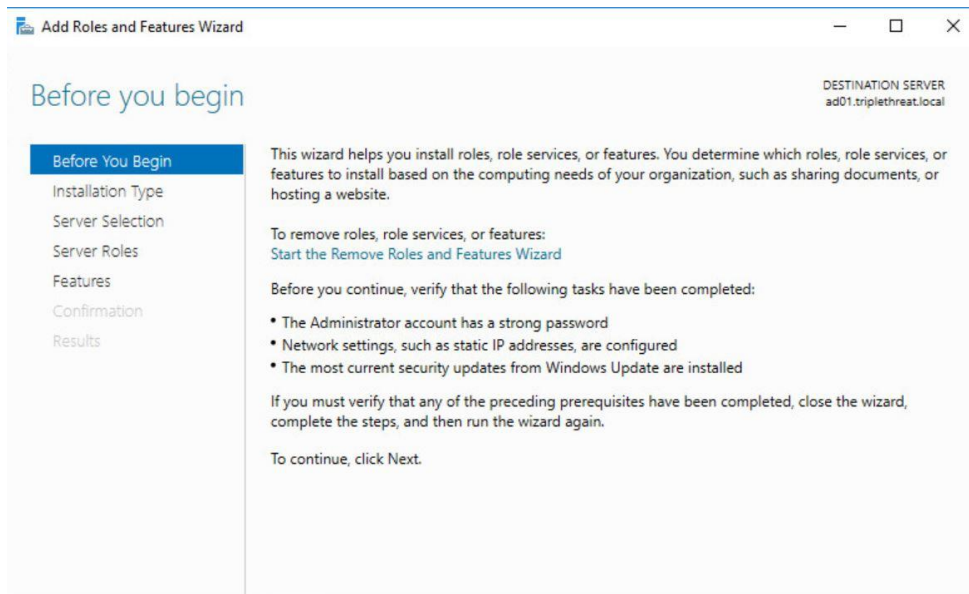
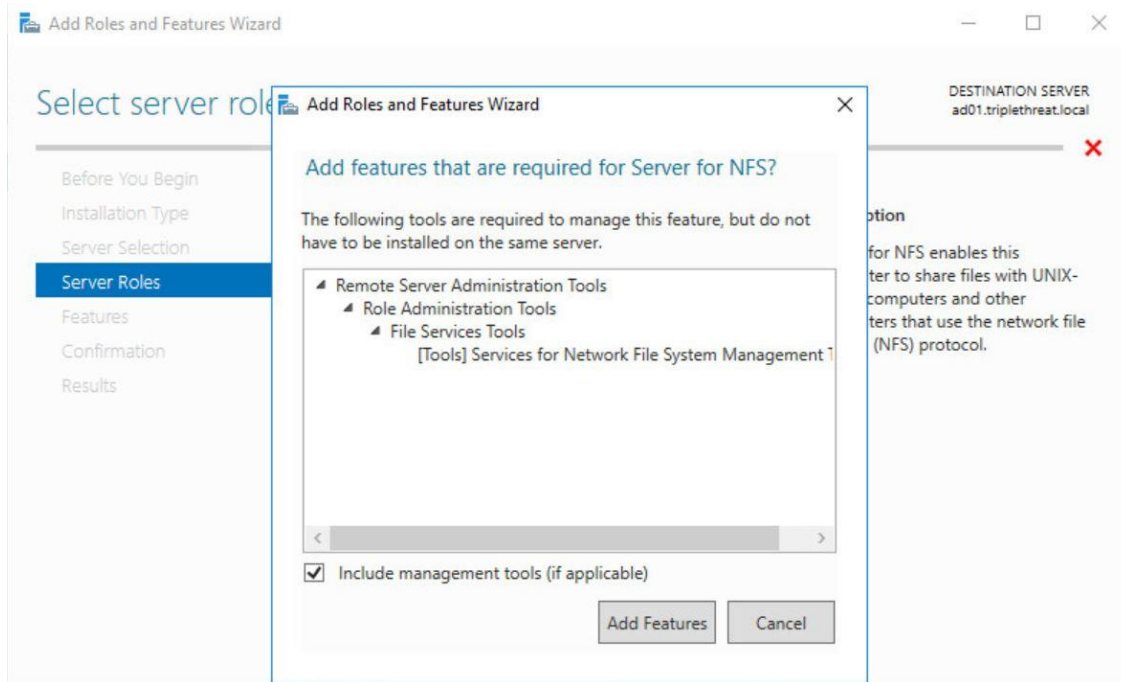2. We choose Role-based installation.

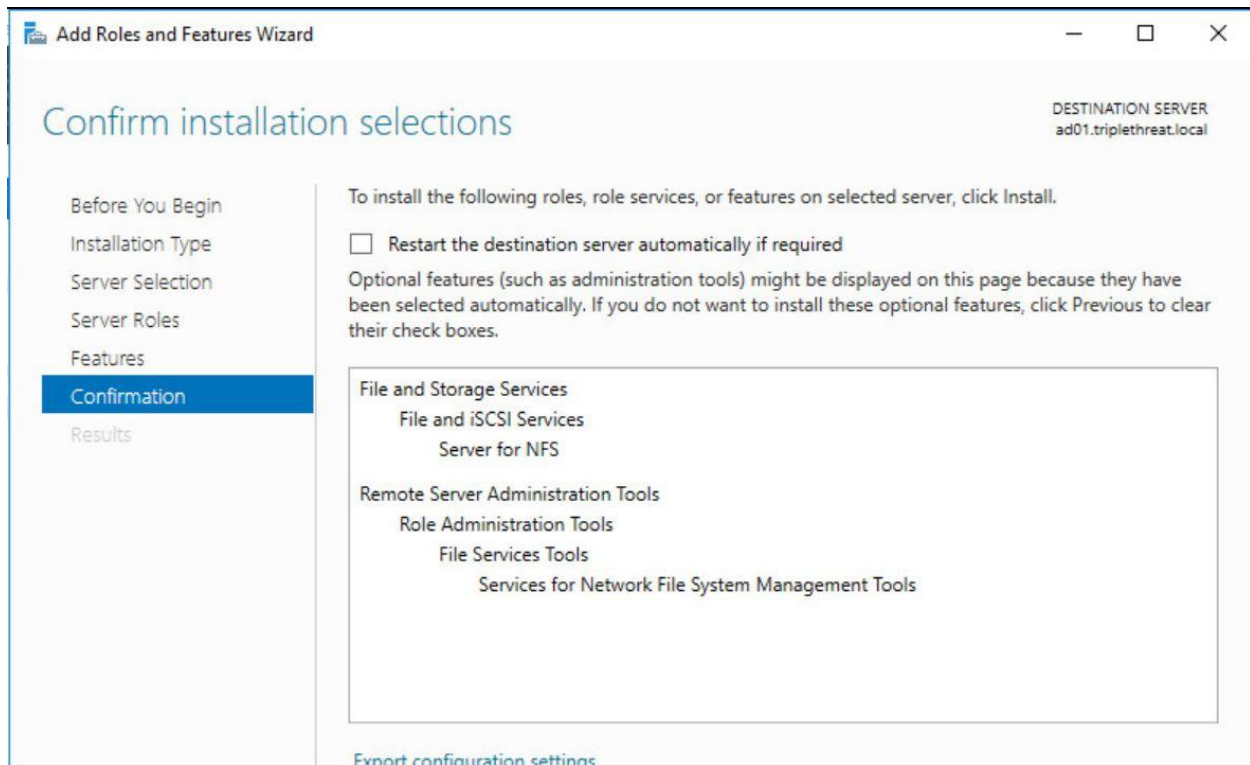3. We select a server from the server pool.
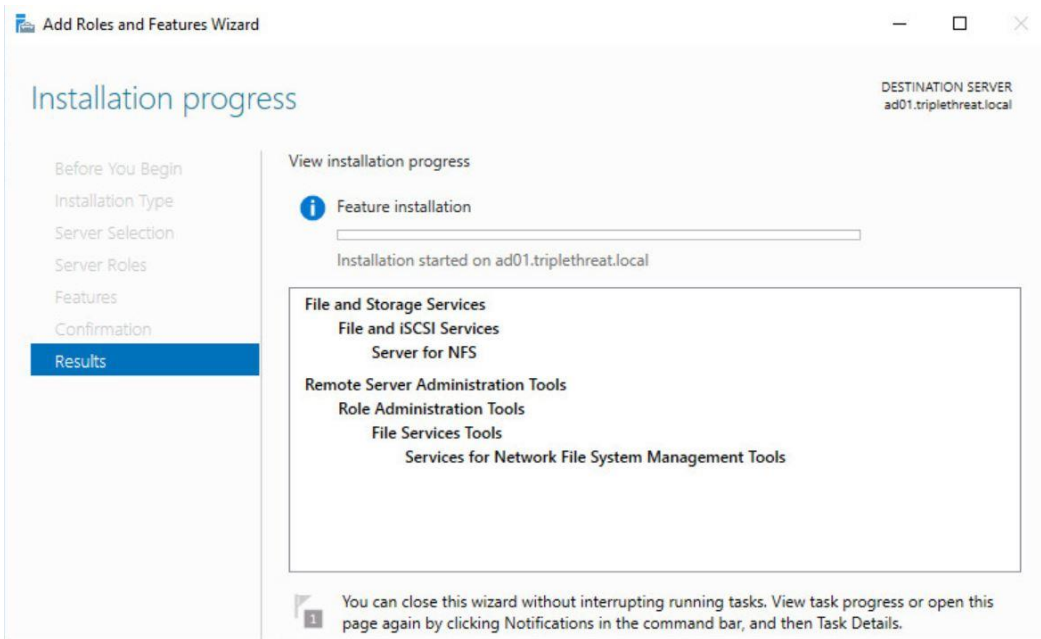

4. We select Server for NFS.

5. Selected Add Features to include selected NFS features.
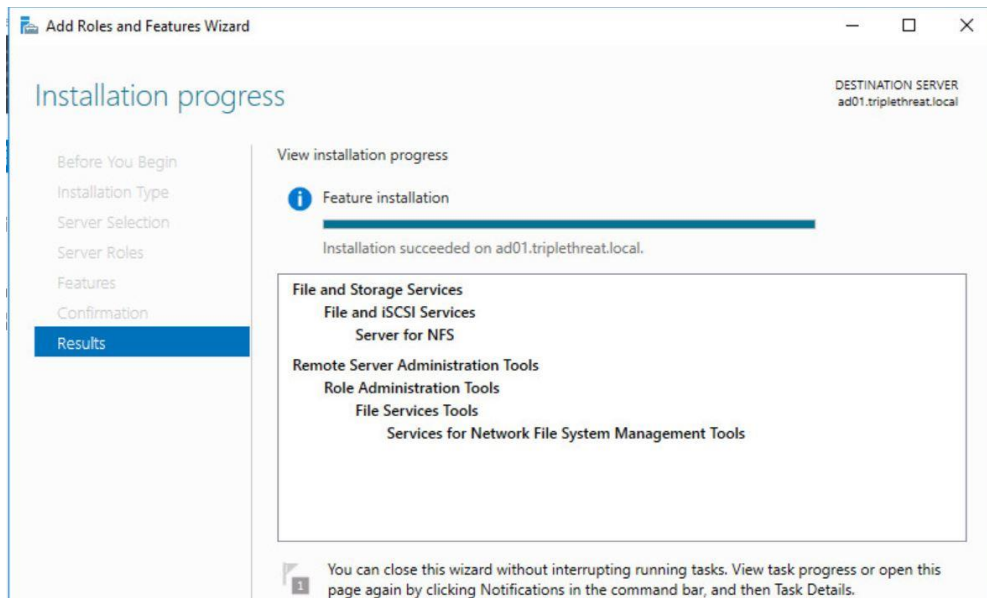

6. We then check our roles, role service and features and then install.

7. It is now installing.
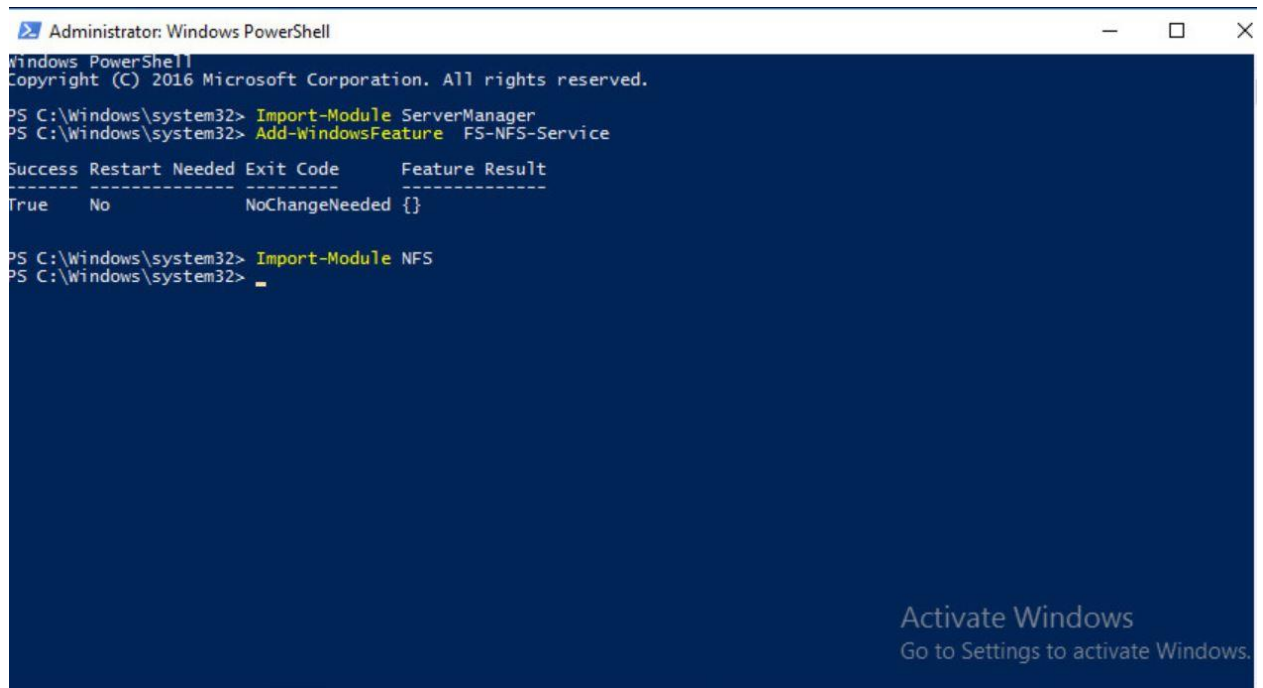

8. Installation of NFS complete.

Install Network File System on the server with Windows PowerShell

1. Start Windows PowerShell as Administrator.
2. Run the following Windows PowerShell commands:

Import-Module ServerManager

Add-WindowsFeature FS-NFS-Service

Import-Module NFS

```
Administrator: Windows PowerShell                                      —    □    ×

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module ServerManager
PS C:\Windows\system32> Add-WindowsFeature  FS-NFS-Service

Success Restart Needed Exit Code       Feature Result
------- -------------- ---------       --------------
True    No             NoChangeNeeded {}


PS C:\Windows\system32> Import-Module NFS
PS C:\Windows\system32> _




                                              Activate Windows
                                              Go to Settings to activate Windows.
```
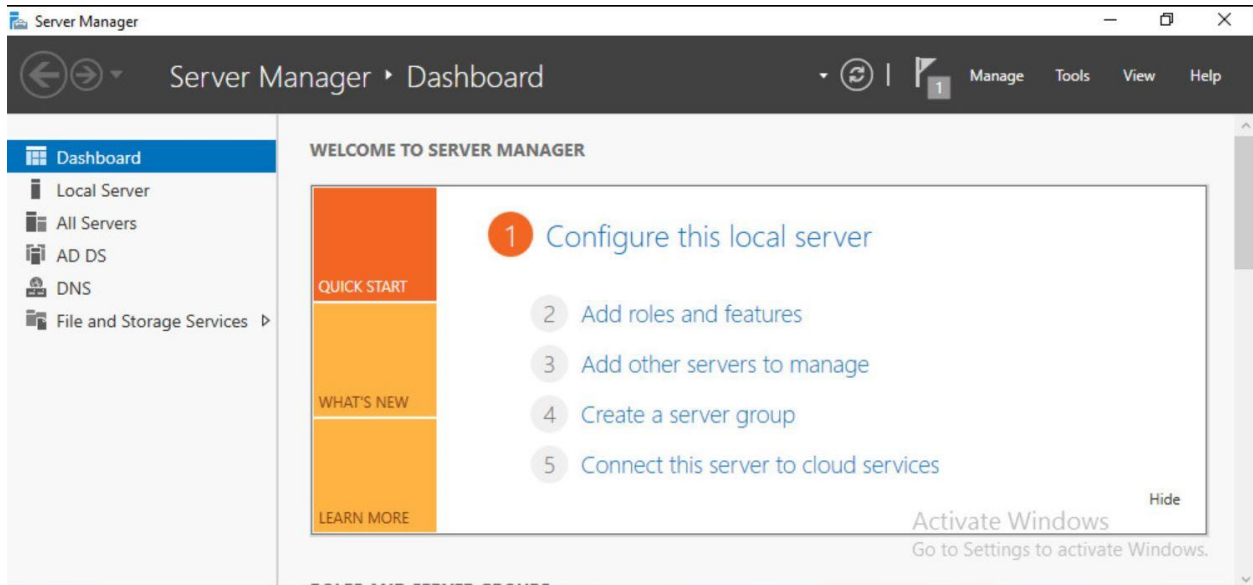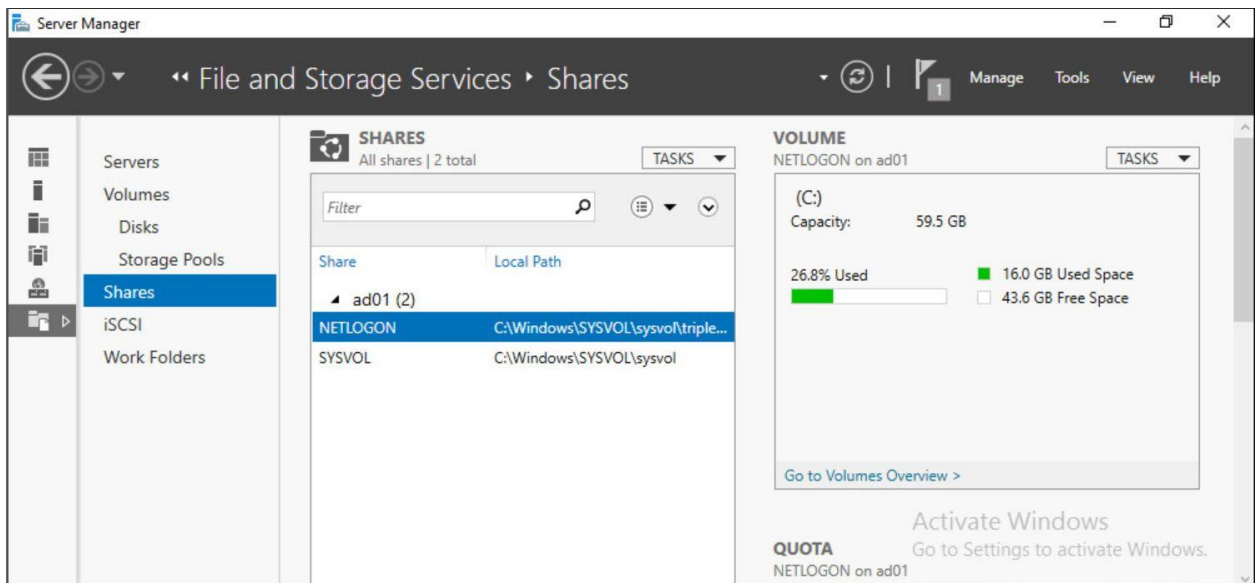
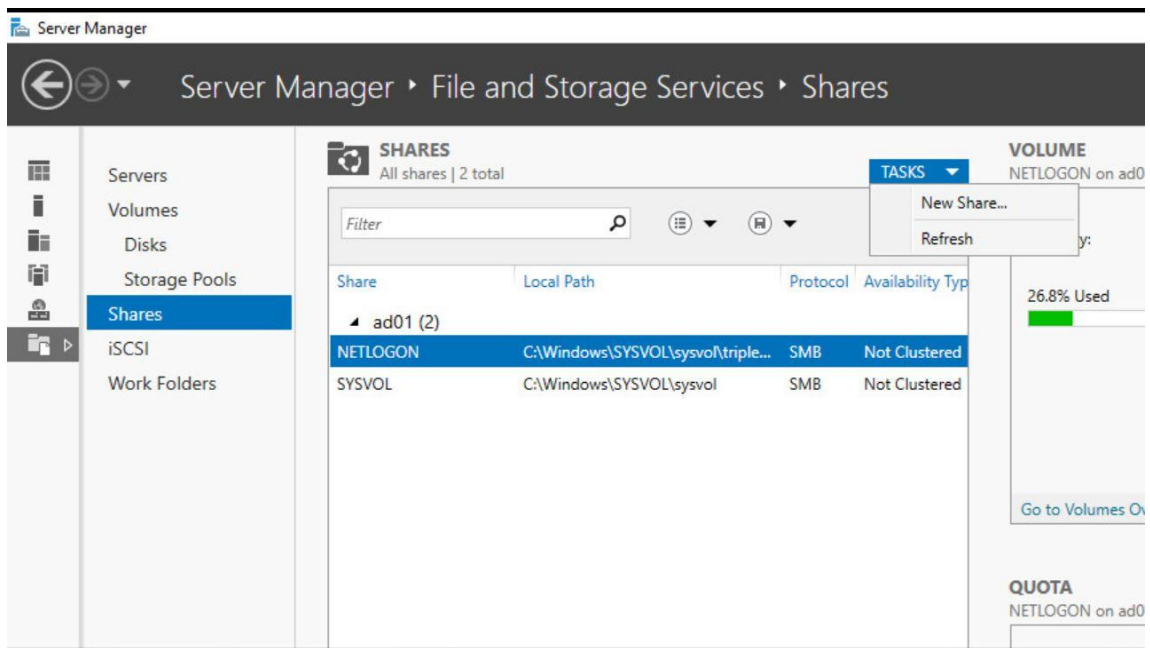# Create an NFS file share with Server Manager
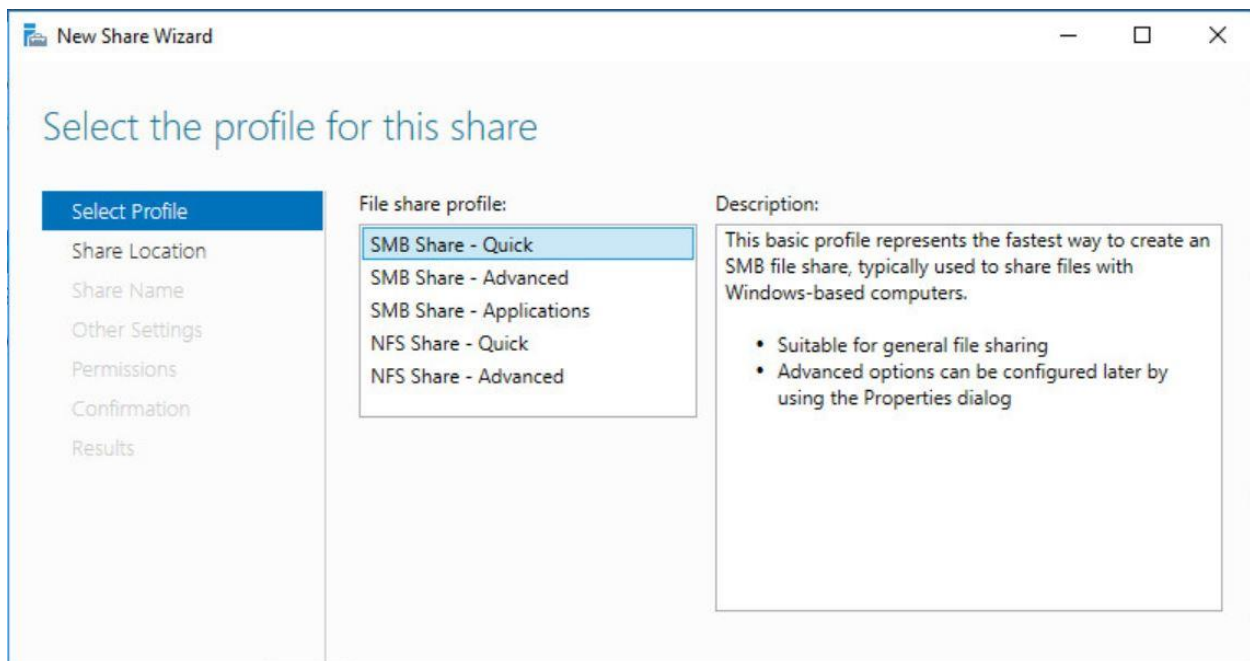
1. Server Manager will start automatically.

2. On the left, select File and Storage Services, and then select Shares.
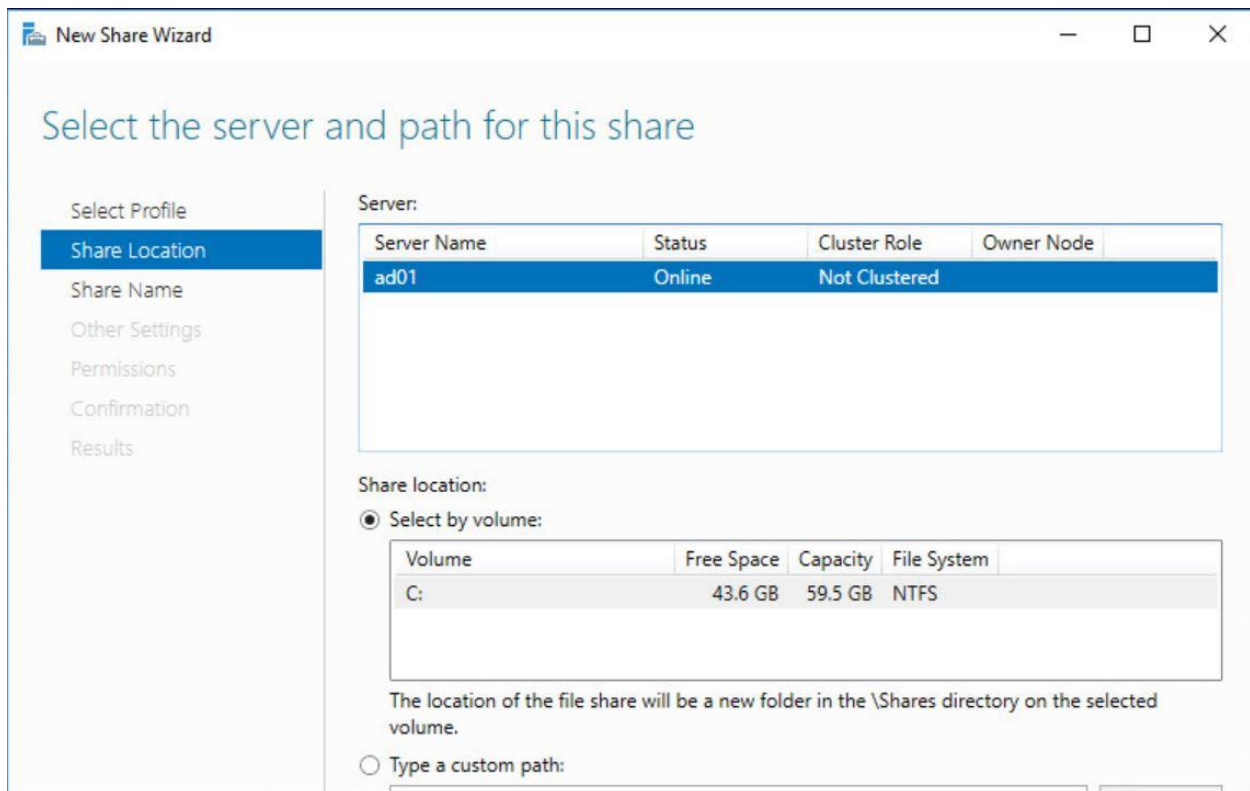
3. Select Tasks then New Share.

4. Select NFS Share – Quick.

5. Select a server and a volume, and click next.
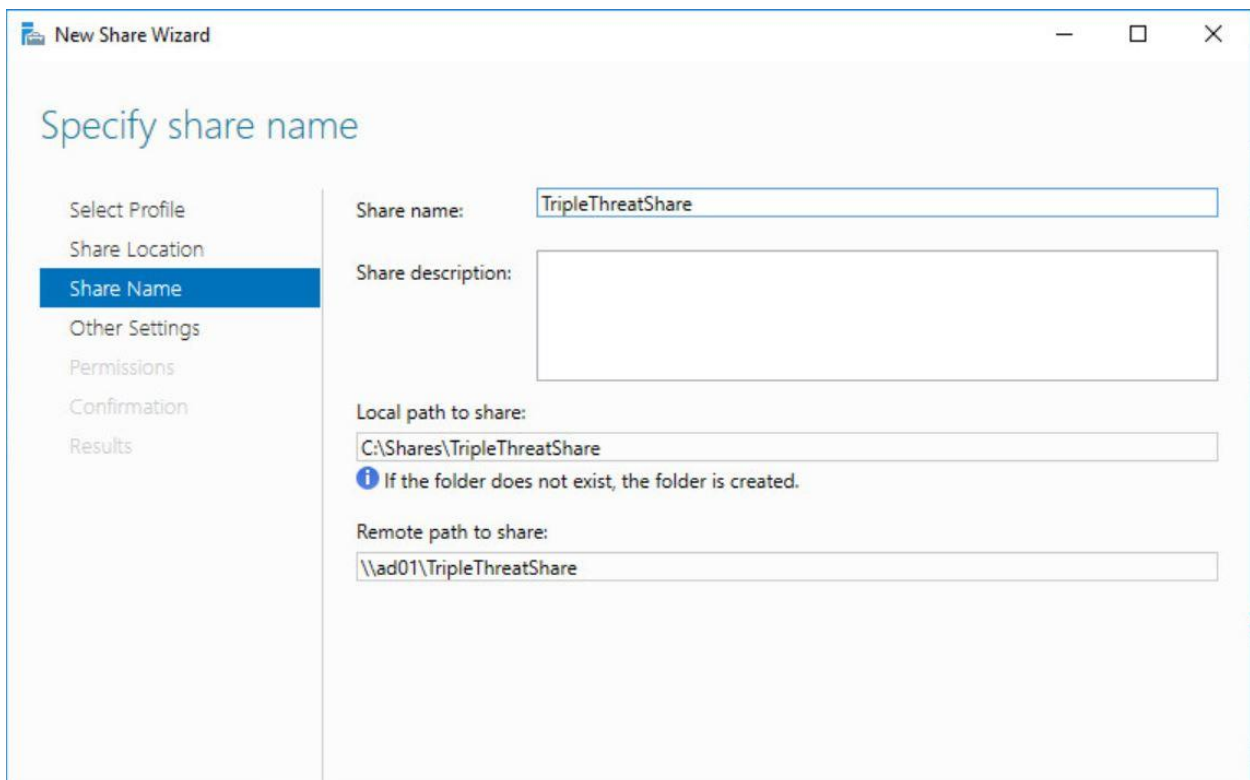
6. Create a name for the new share, and click next.

7. Specify the authentication method you want to use for this share.

8. Click Customize Permissons, and then specify the host, client group or netgroup you want to grant permission to the share.

9. In **Permissions**, configure the type of access control you want the users to have, and select **OK**.
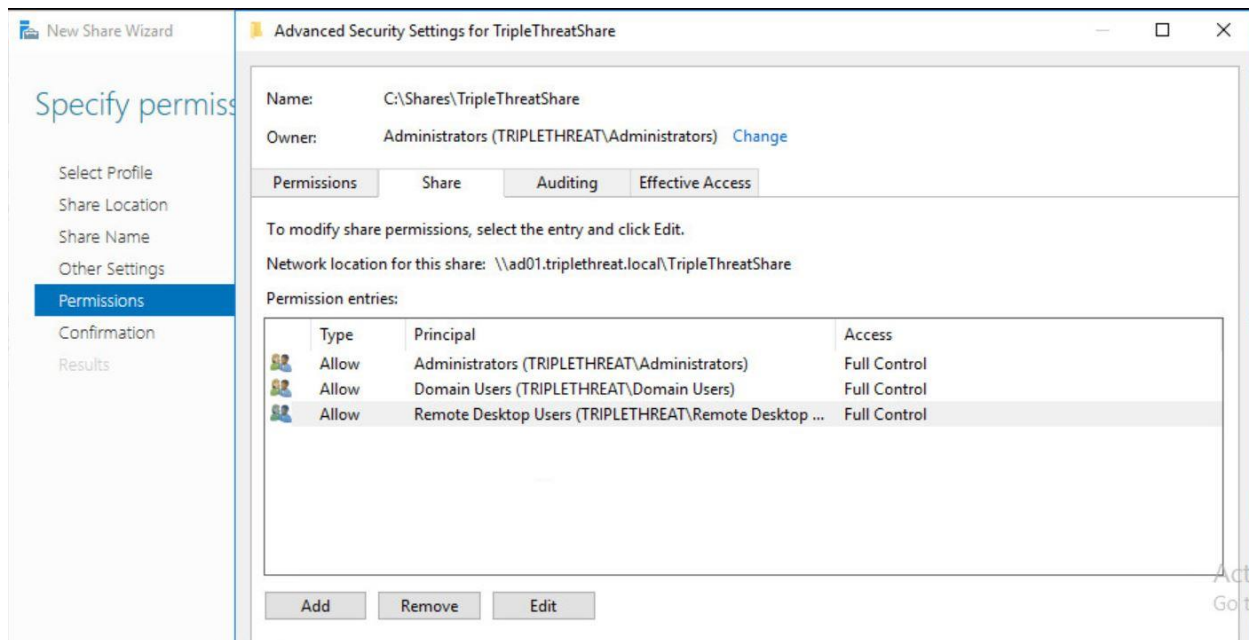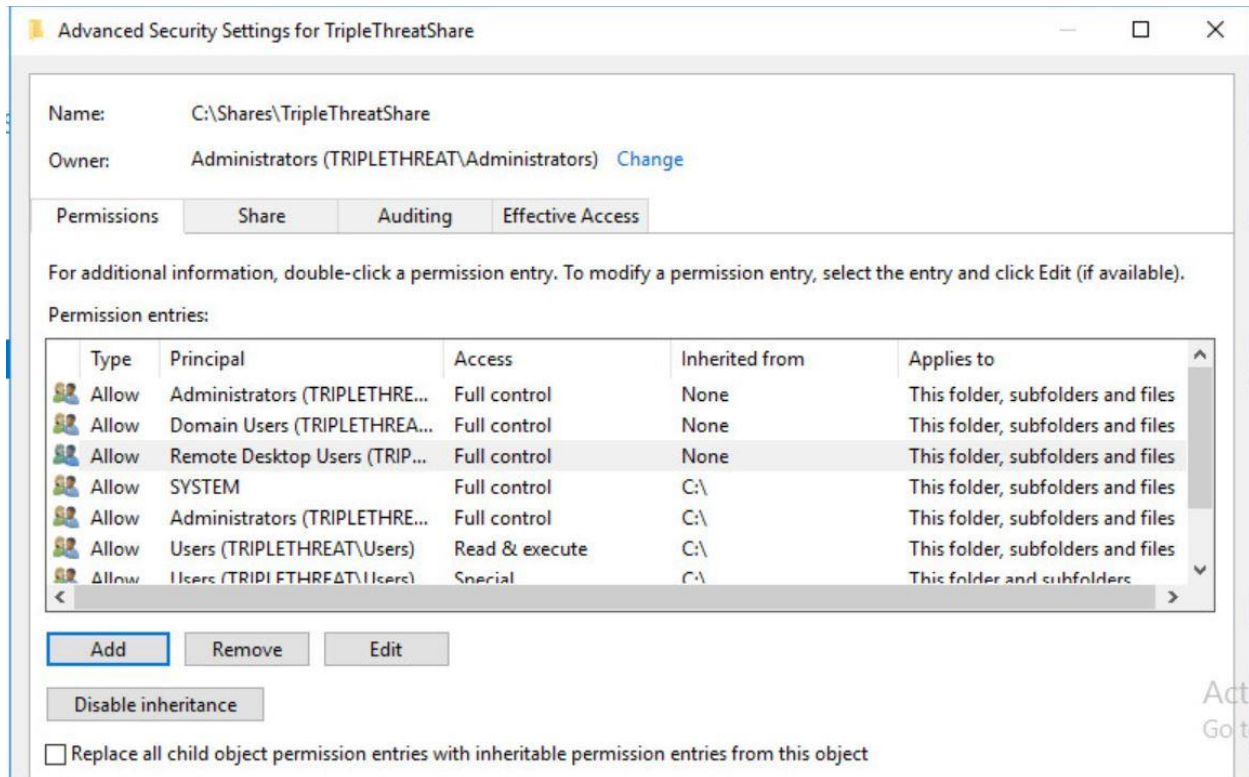
Advanced Security Settings for TripleThreatShare

Name: C:\Shares\TripleThreatShare

Owner: Administrators (TRIPLETHREAT\Administrators)   Change

Permissions | **Share** | **Auditing** | **Effective Access**

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

	Type	Principal	Access	Inherited from	Applies to
🔓	Succ...	Administrators (TRIPLETHREA...	Full control	None	This folder, subfolders and files
🔓	Succ...	Domain Users (TRIPLETHREA...	Full control	None	This folder, subfolders and files
🔓	Succ...	Remote Desktop Users (TRIPL...	Full control	None	This folder, subfolders and files

[Add]   [Remove]   [Edit]

[Disable inheritance]

☐ Replace all child object auditing entries with inheritable auditing entries from this object

---

Advanced Security Settings for TripleThreatShare

Name: C:\Shares\TripleThreatShare

Owner: Administrators (TRIPLETHREAT\Administrators)   Change

Permissions | **Share** | **Auditing** | **Effective Access**

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

User/ Group: Select a user

                Include group membership   Click Add items ▾   Add items

Device: Select a device

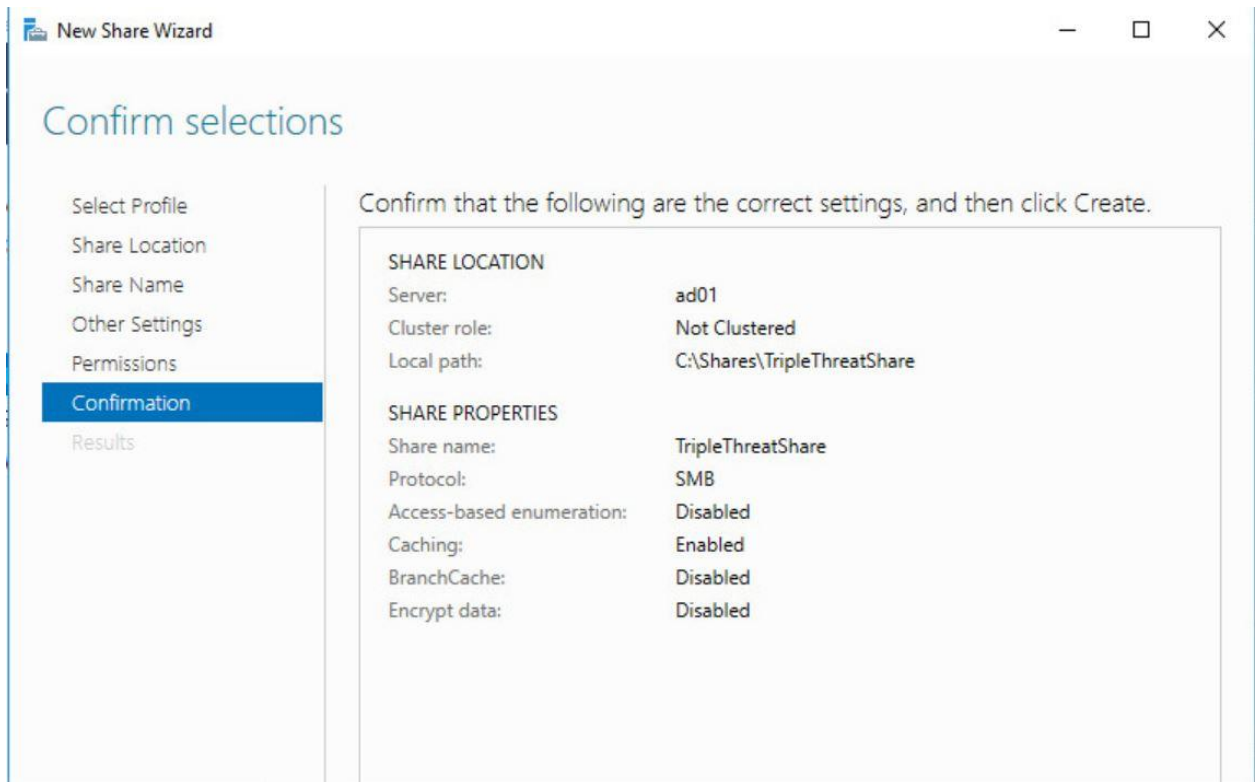   Include group membership   Click Add items ▾   Add items

                Include a user claim
                Include a device claim

[View effective access]

10. Review configuration, and select Create.

11. The share was created.