Exercise 1 - Configuring Shared Folders and NTFS Permissions.

Share permissions are used by the Windows operating system to advertise the availability of resources such as files and printers to users on a network. This is true regardless of whether the server is part of a workgroup or a domain.

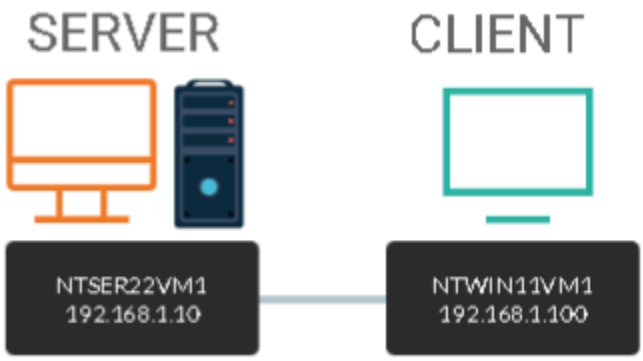
Members of the Domain Admins or Server Operators groups in a Windows Active Directory domain have the ability to create shared folders. Users who are members of the Administrators or Power Users groups on non-domain joined Windows machines can establish shared folders.

Administrators configure NTFS security by providing groups with the appropriate rights to folders that need to be accessible via a network to safeguard a server's file system.

In this exercise,

1. We will use different methods to configure share permissions using Windows Server 2019 and Windows 10 computers.

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: Create a New Folder Share

Files can be shared among devices on a network via shared folders. On a Windows Server or Windows 10 device, you can create a shared folder with File Explorer, Computer Management, net.exe, or Windows PowerShell.

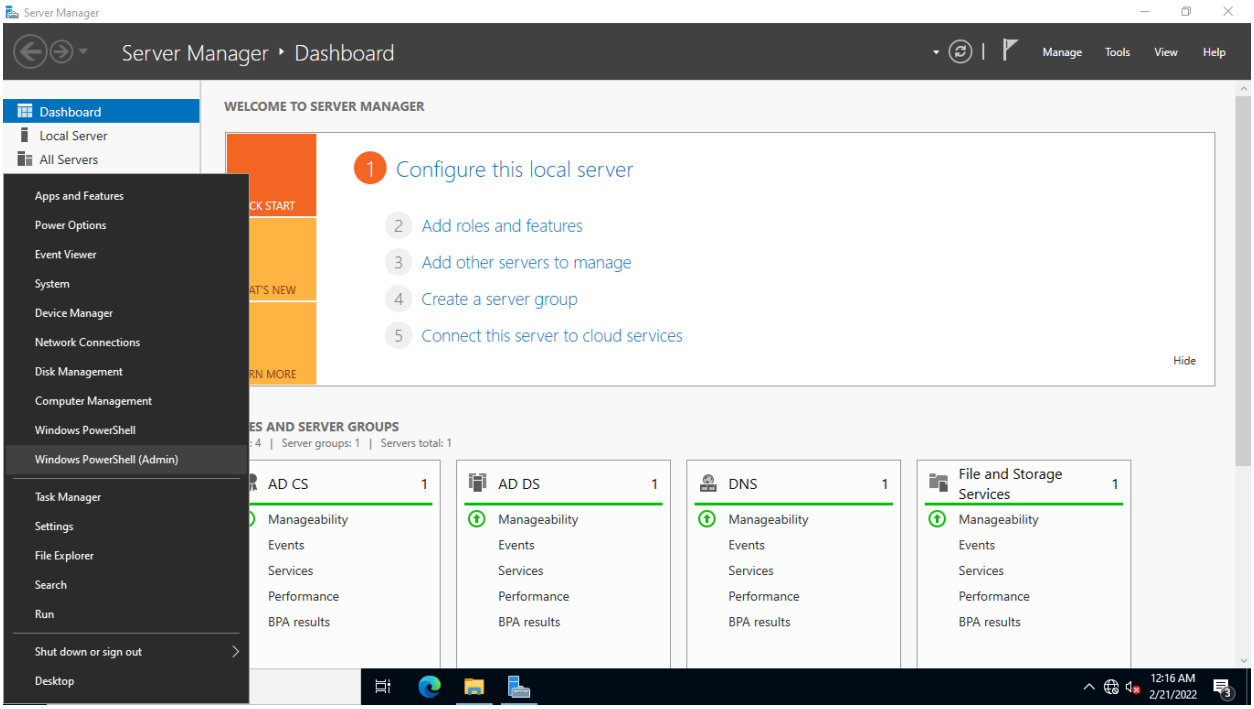
In this task, we will create a new folder share using Windows PowerShell and the Computer Management.

Step 1:

Make sure all of the devices listed in the exercise introduction are turned on.

Right now, let’s work with the NTSER22VM1

Right-click the **Start** icon and select **Windows PowerShell.**

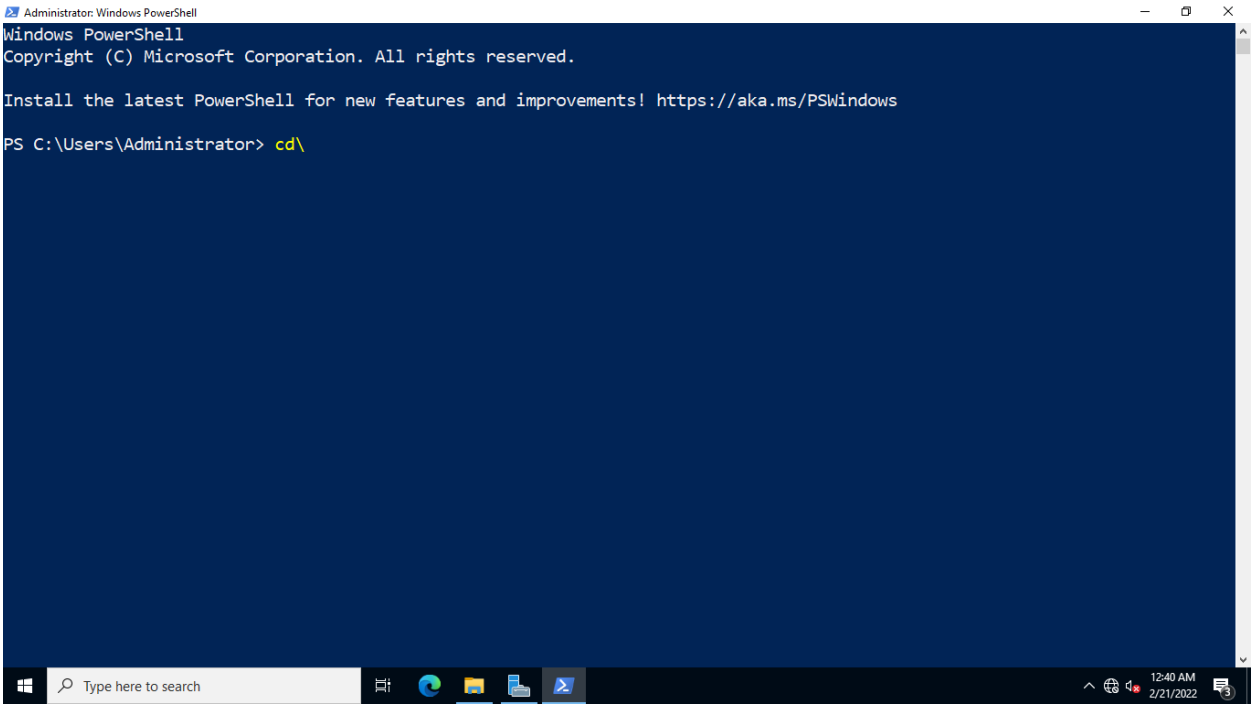


Step 2:

On the Windows **PowerShell window**, type the following:

```
cd\
```

Press **Enter.**

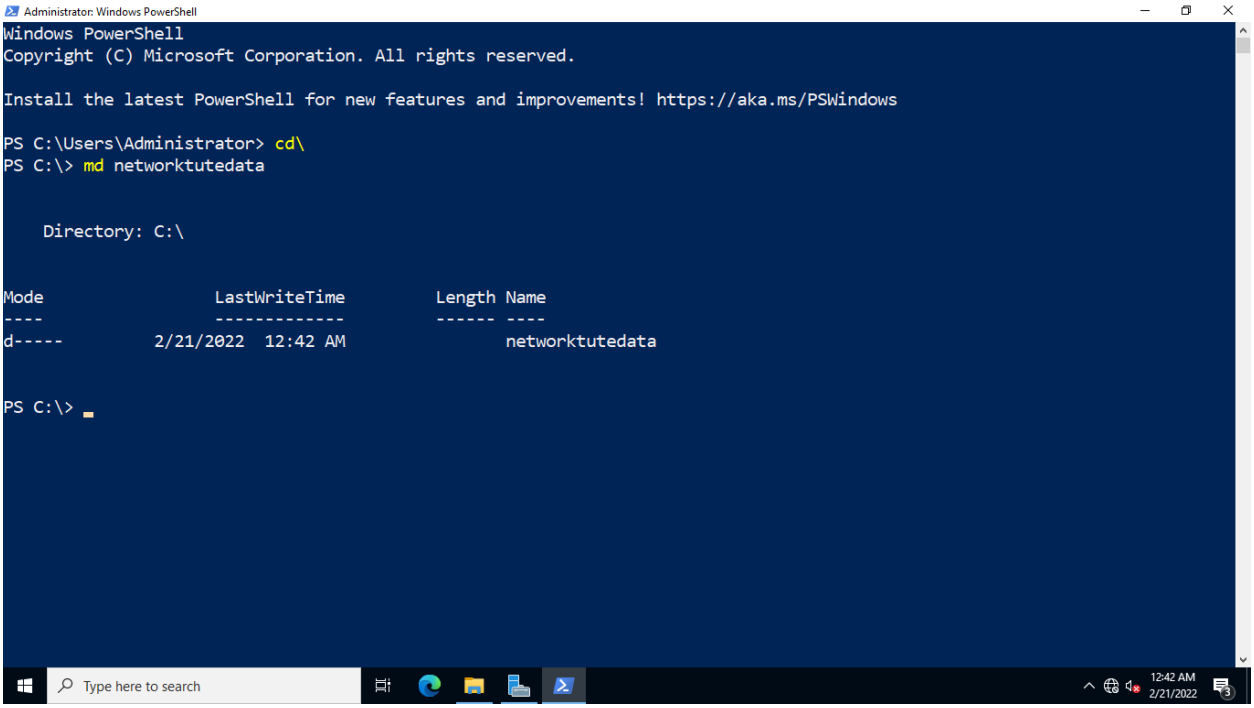


Step 3:

On the next prompt, create a folder by typing the following:

```
md networktutedata
```

Press **Enter.**

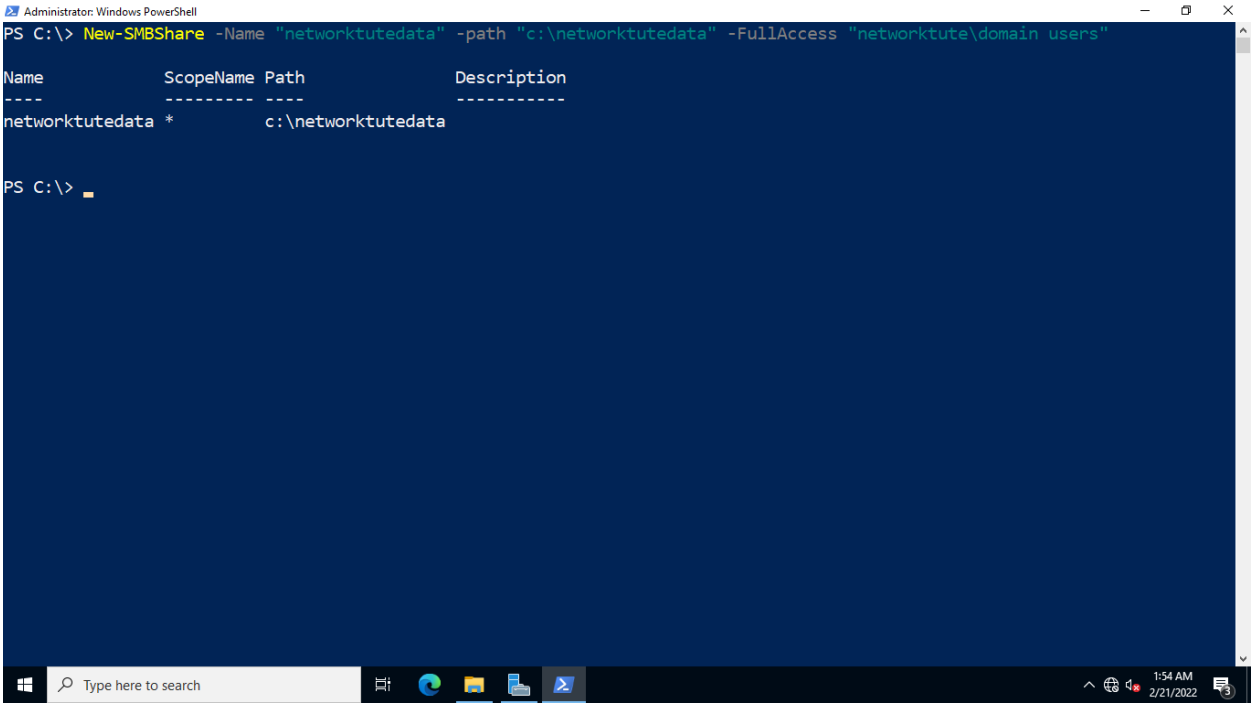


Step 4:

After creating the **networktute** data folder, type the following to create a shared folder:

```
New-SMBShare -Name “networktutedata” -path “c:\networktutedata” -FullAccess “networktute\domain users”
```

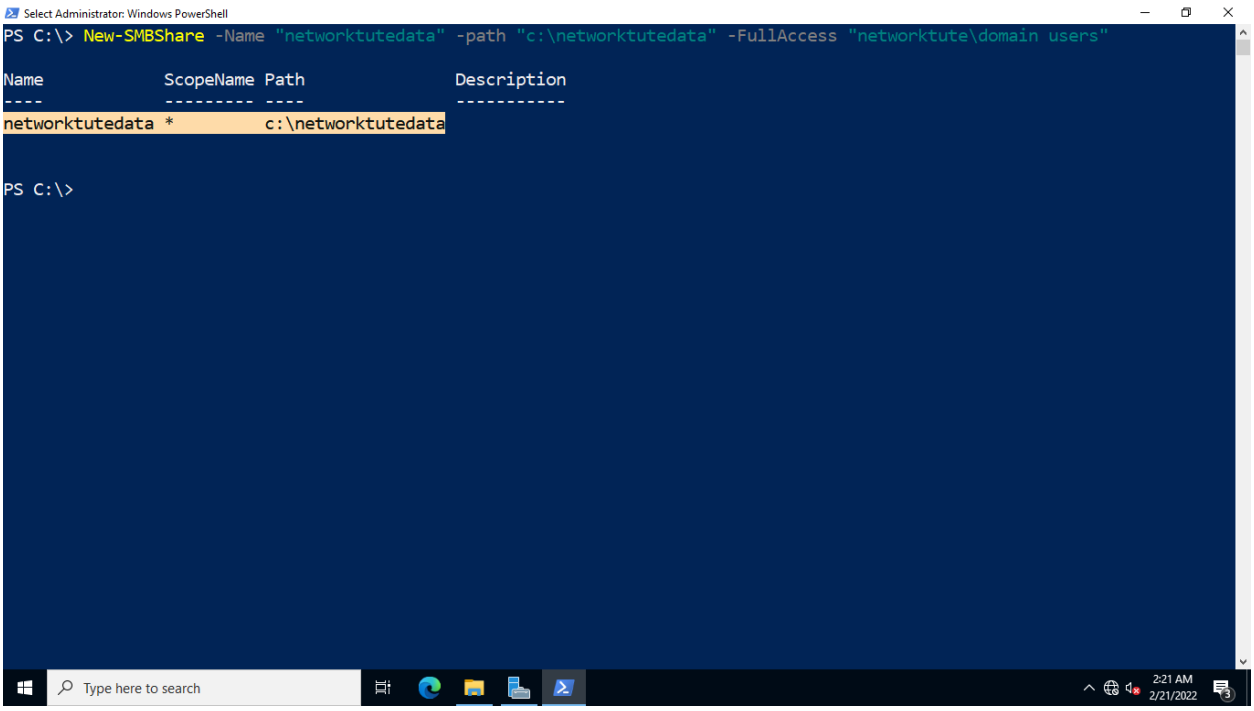
Press **Enter.**



Step 5:

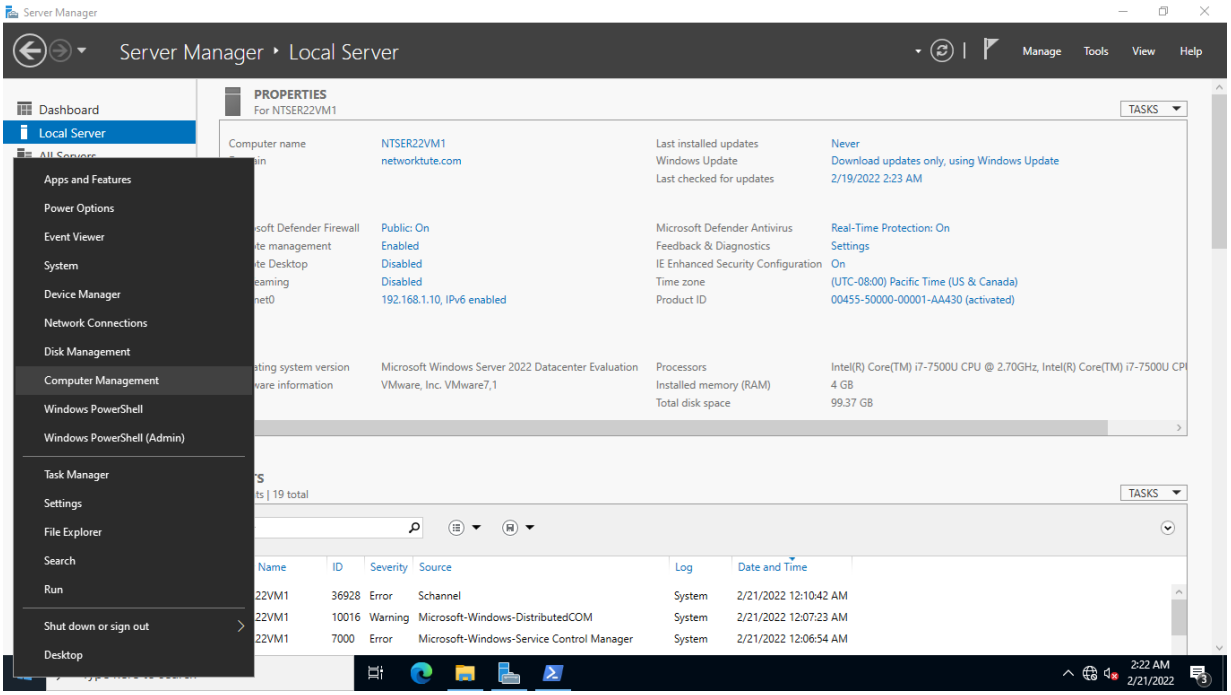
The **networktute** shared folder is successfully created.

Close the **Windows PowerShell** window.



Step 6:

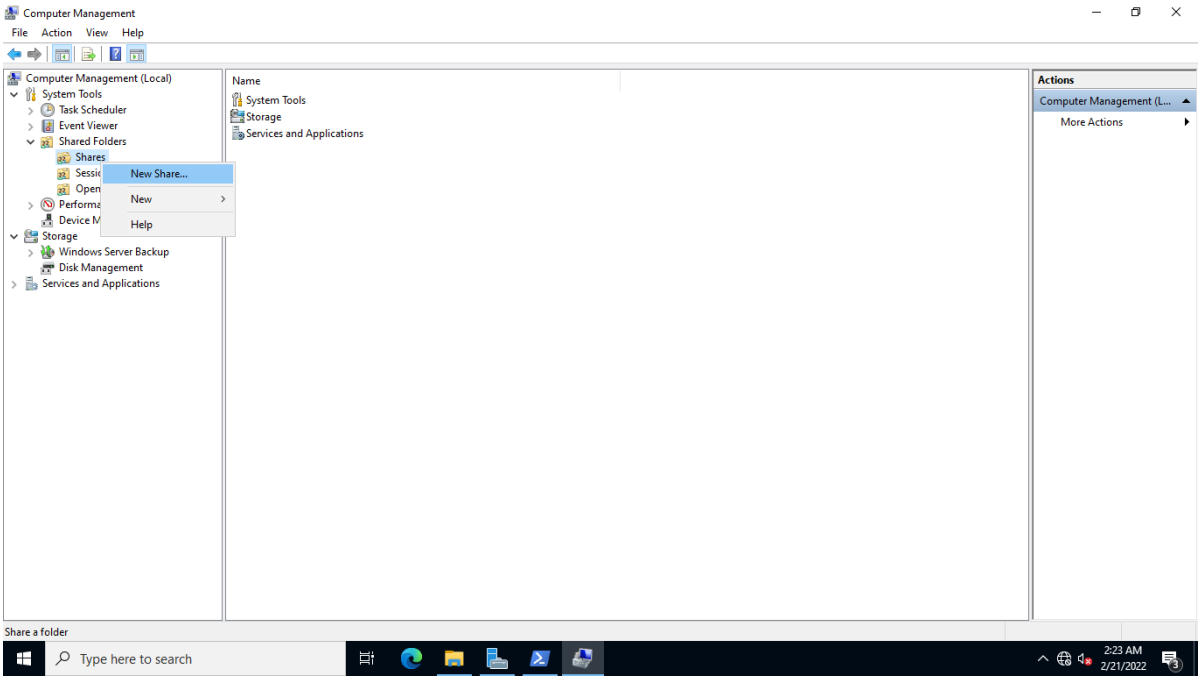
Right-click the **Start** icon and select **Computer Management**.



Step 7:

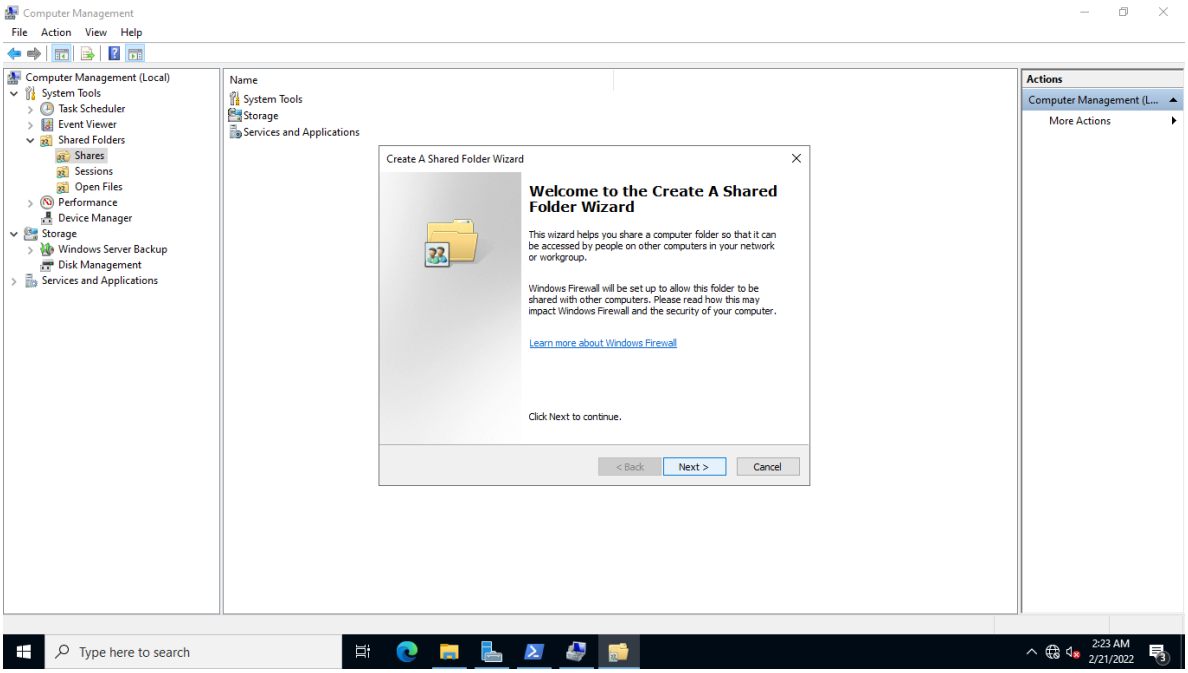
On the **Computer Management** window, expand **Shared Folders.**

Then right-click **Shares** then click **New Share….**



Step 8:

On the **Create A Shared Folder Wizard - Welcome to the Create a Shared Folder Wizard** window, click **Next**

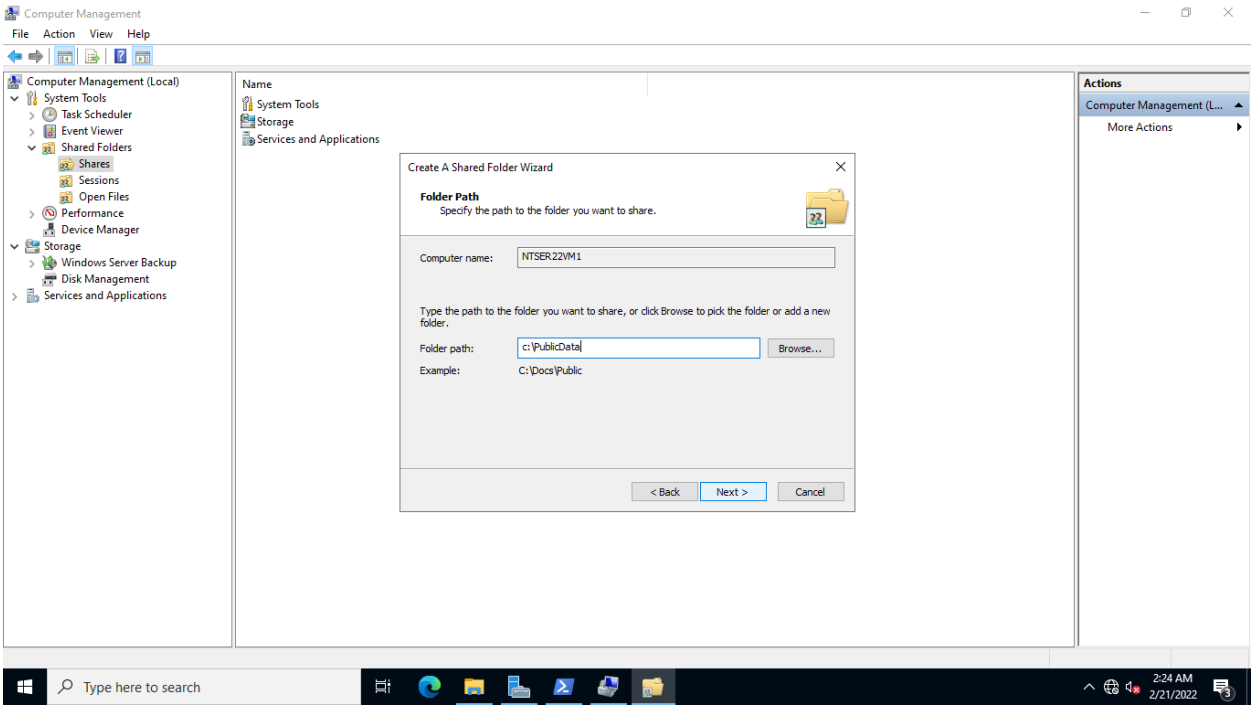


Step 9:

On the **Folder Path** page, click in the **Folder path** textbox and type:

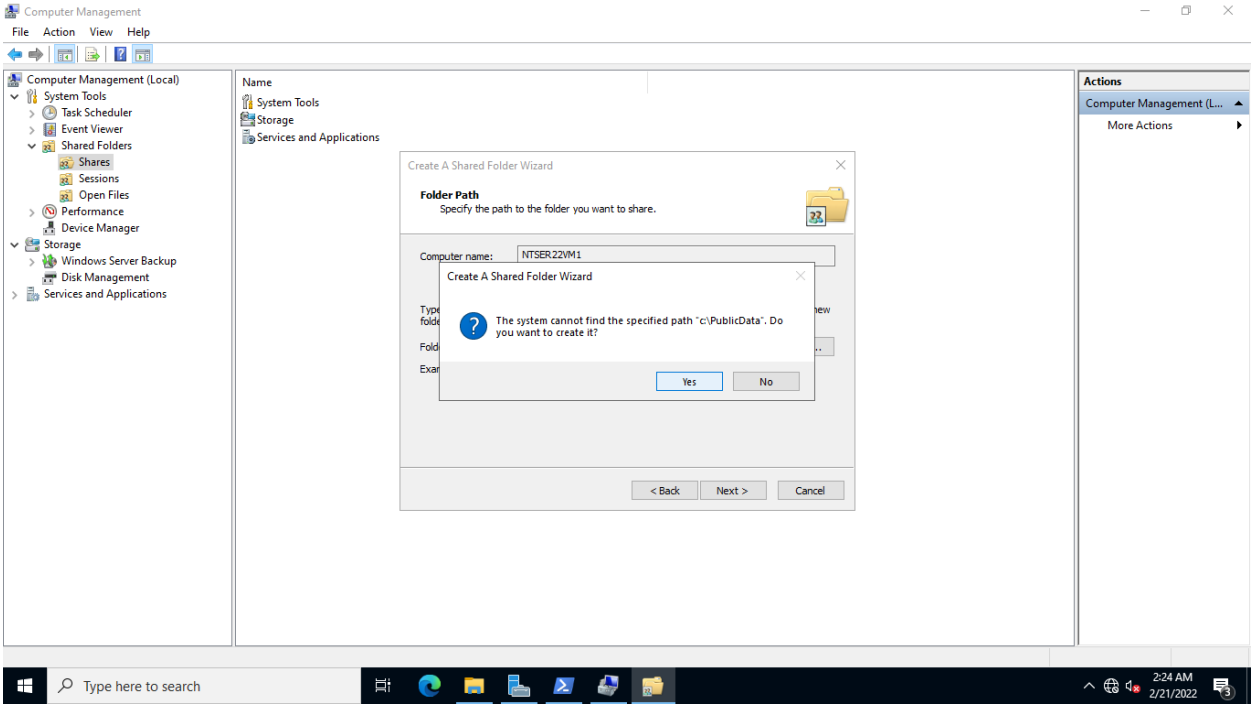
c:\PublicData

Click **Next**.



Step 10:

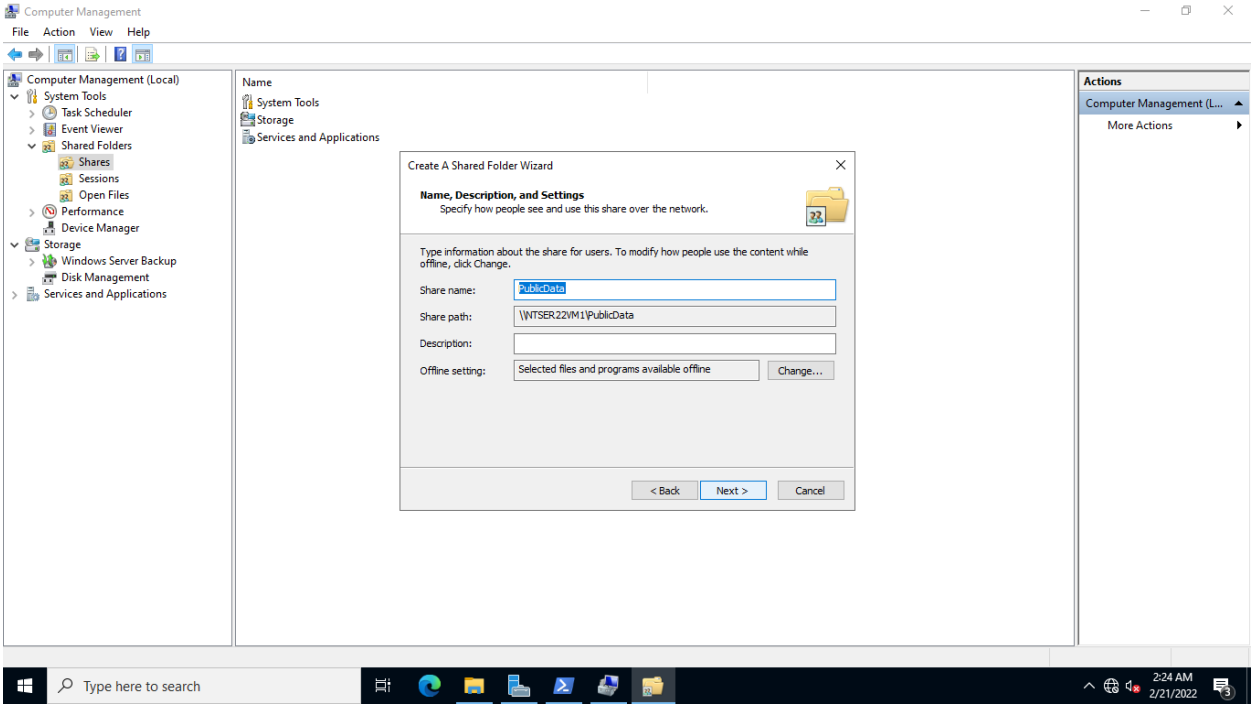
Click **Yes** on the **Create A Shared Folder Wizard** message box to create the folder.



Step 11:

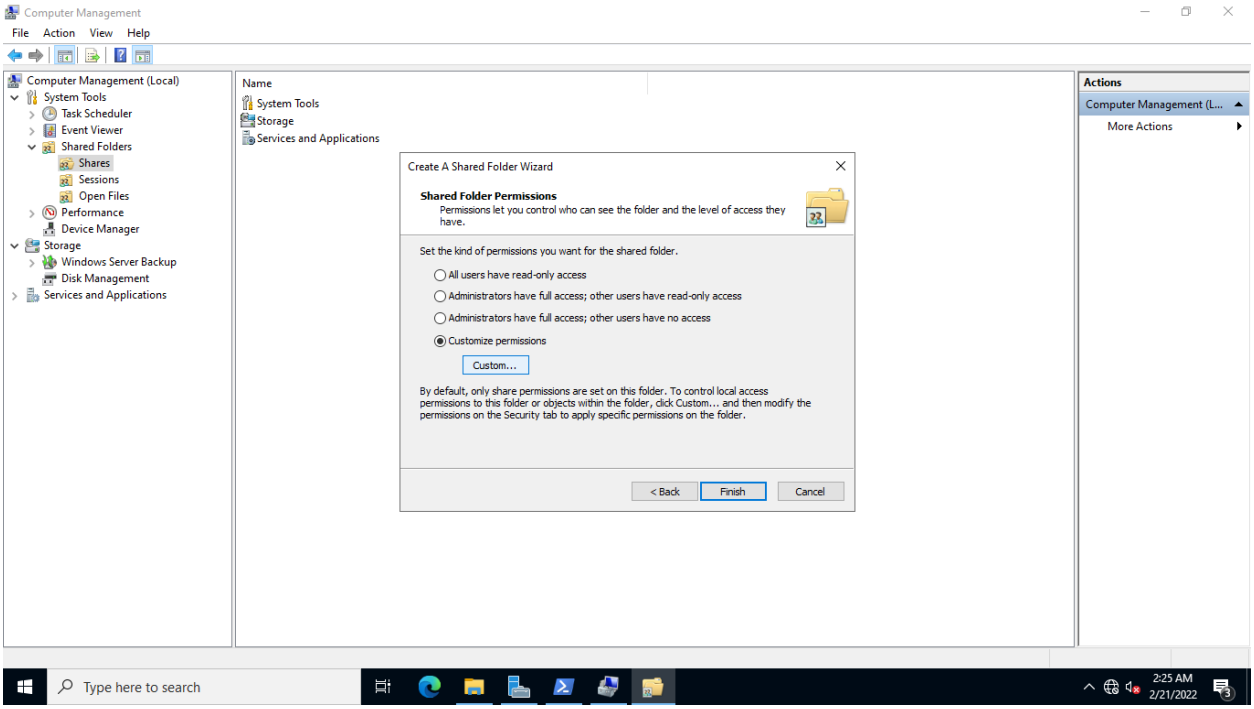
On the **Name, Description and Settings** page, information about the new shared folder is displayed.

Click **Next**.



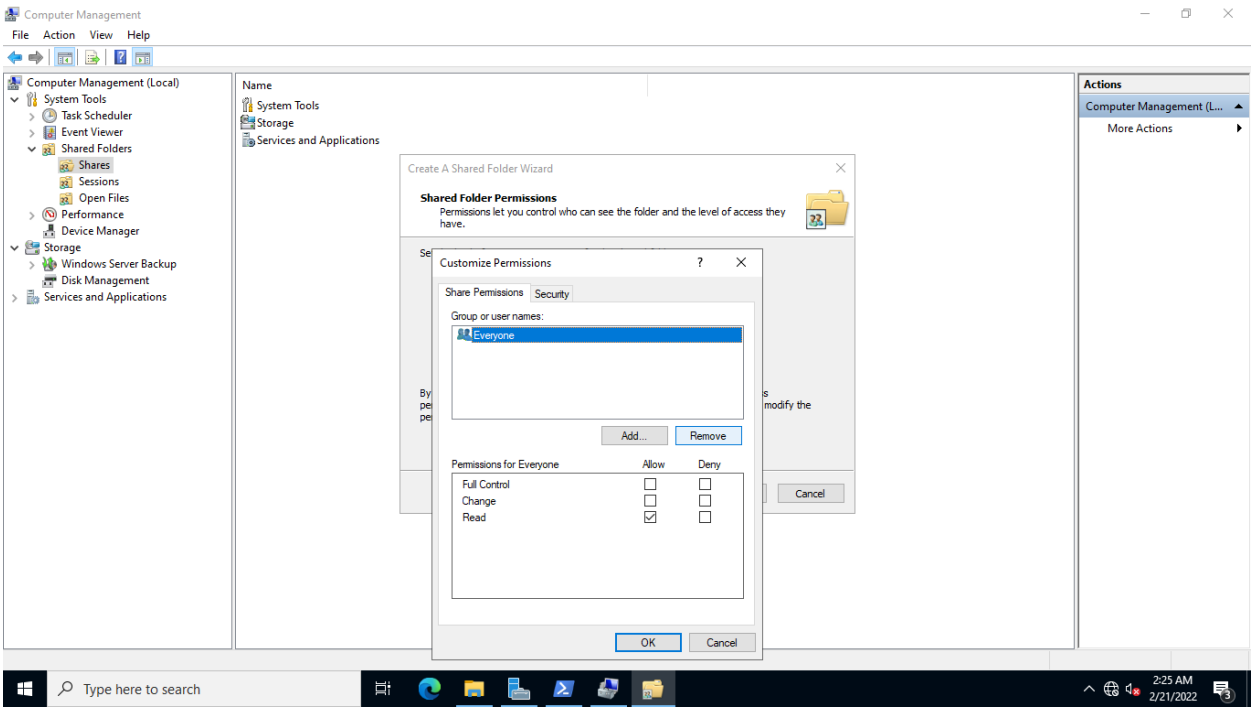
Step 12:

On the **Shared Folder Permissions** page, select **Customize permissions**, then click **Custom**…



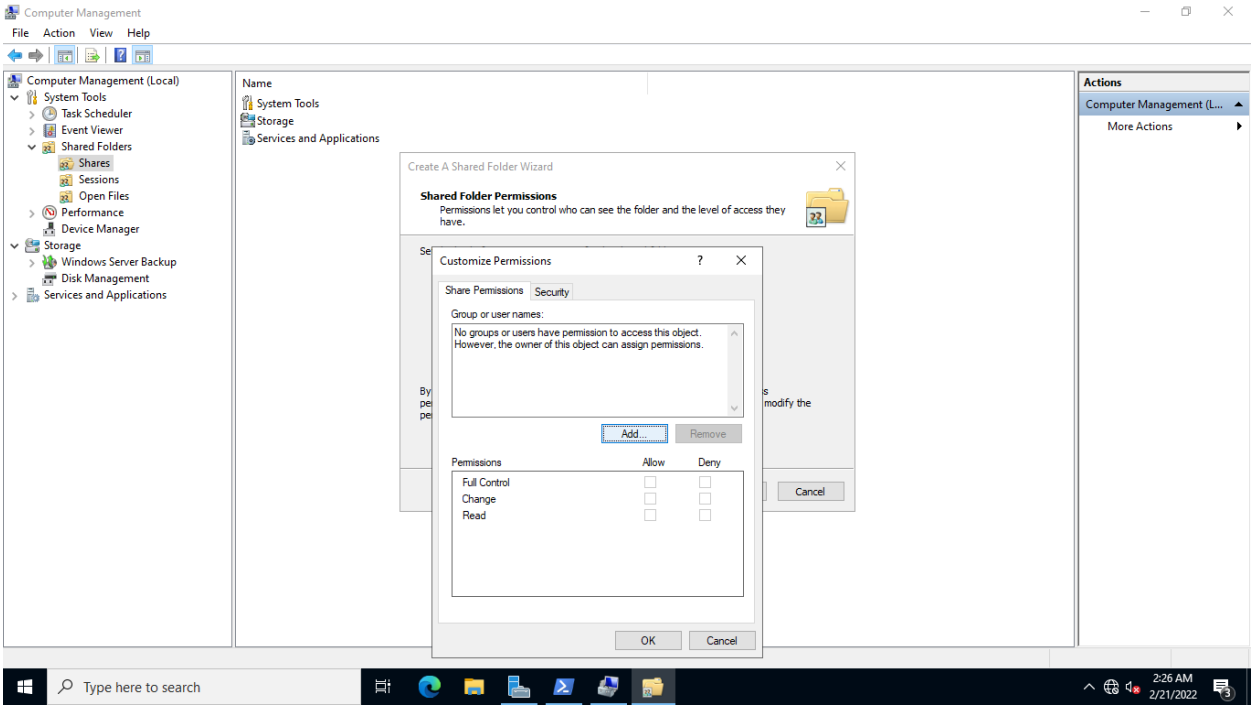
Step 13:

On the **Customize Permissions** dialog box, select **Everyone** and click **Remove**.



Step 14:

Still on the **Customize Permissions** dialog box, click **Add**



Step 15:

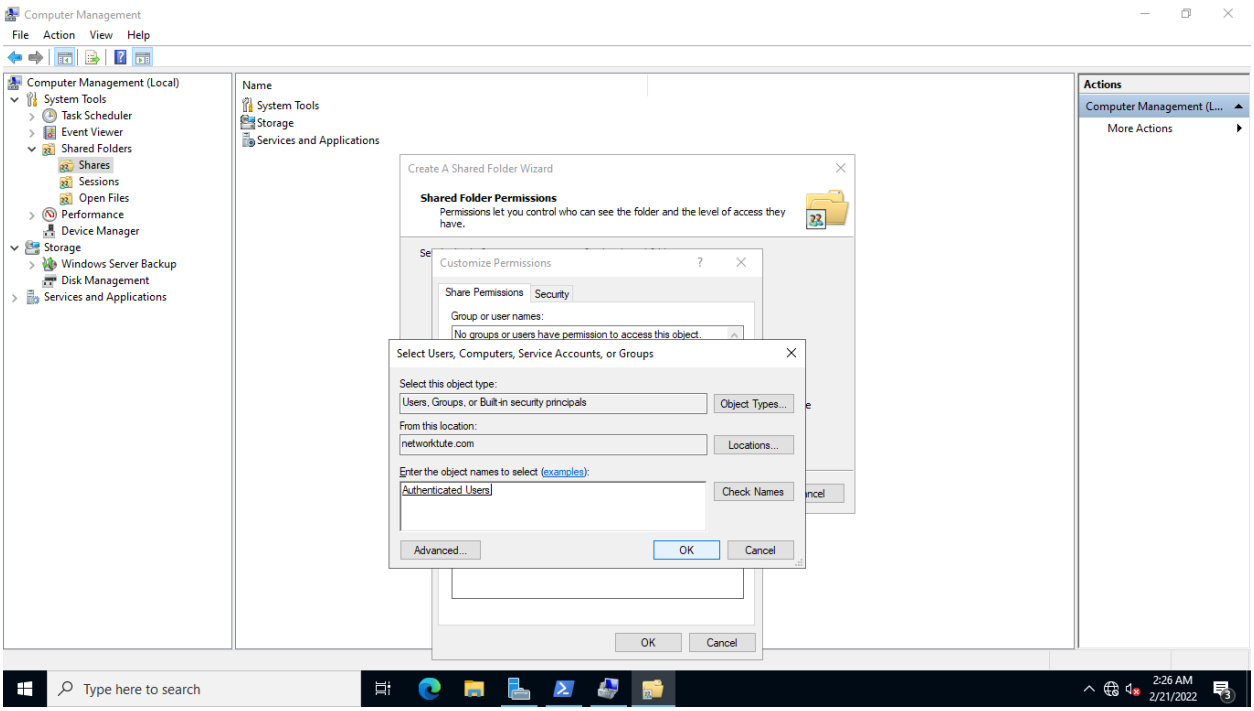
In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** textbox, type:

authenticated users

Note: Authenticated Users is a unique security group that does not include any user accounts. When a user account successfully authenticates with a Windows server or Active Directory domain, it is added to this group.

Click **Check Names** to verify you have typed in a valid group name.

Click **OK.**



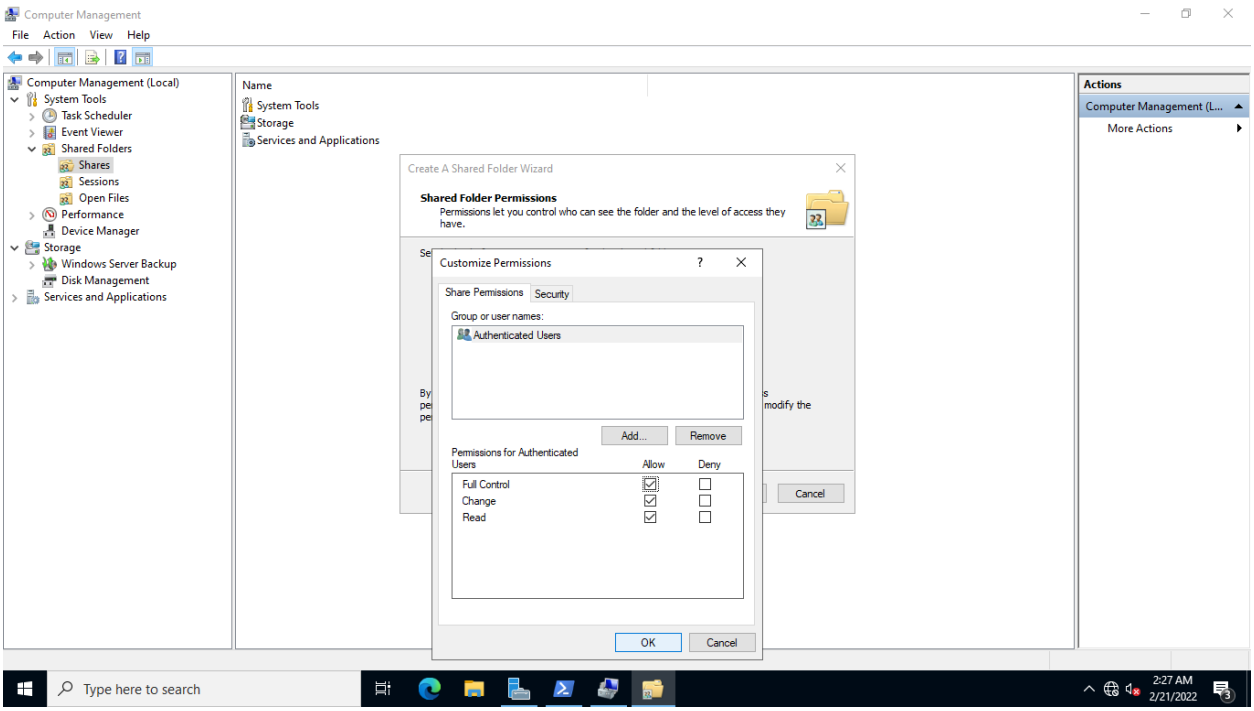
Step 16:

Back on the **Customize Permissions** dialog box, select **Authenticated Users**.

Then in the **Permissions for Authenticated Users** section, in the **Allow** column, tick the **Full Control** checkbox.

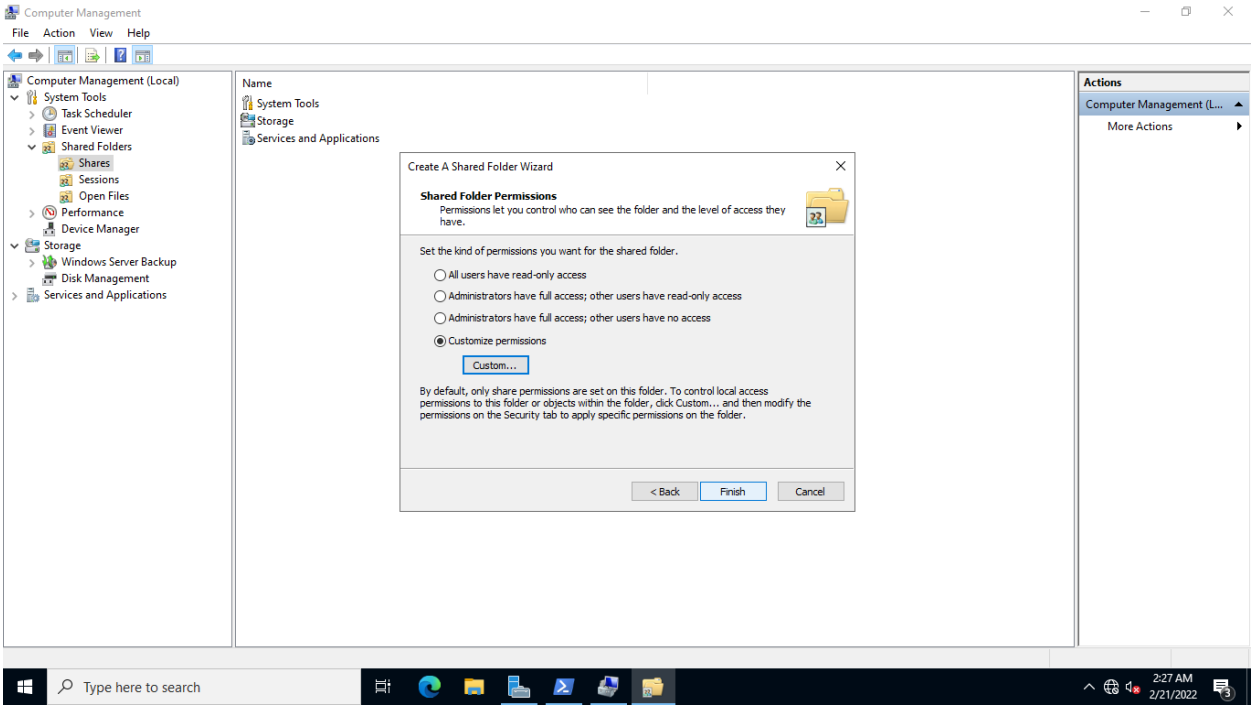
Note: NTFS permissions will be used later to limit the users or security groups who will have access to the PublicData shared folder, despite the fact that Authenticated Users was given Allow - Full Control.

Click **OK.**



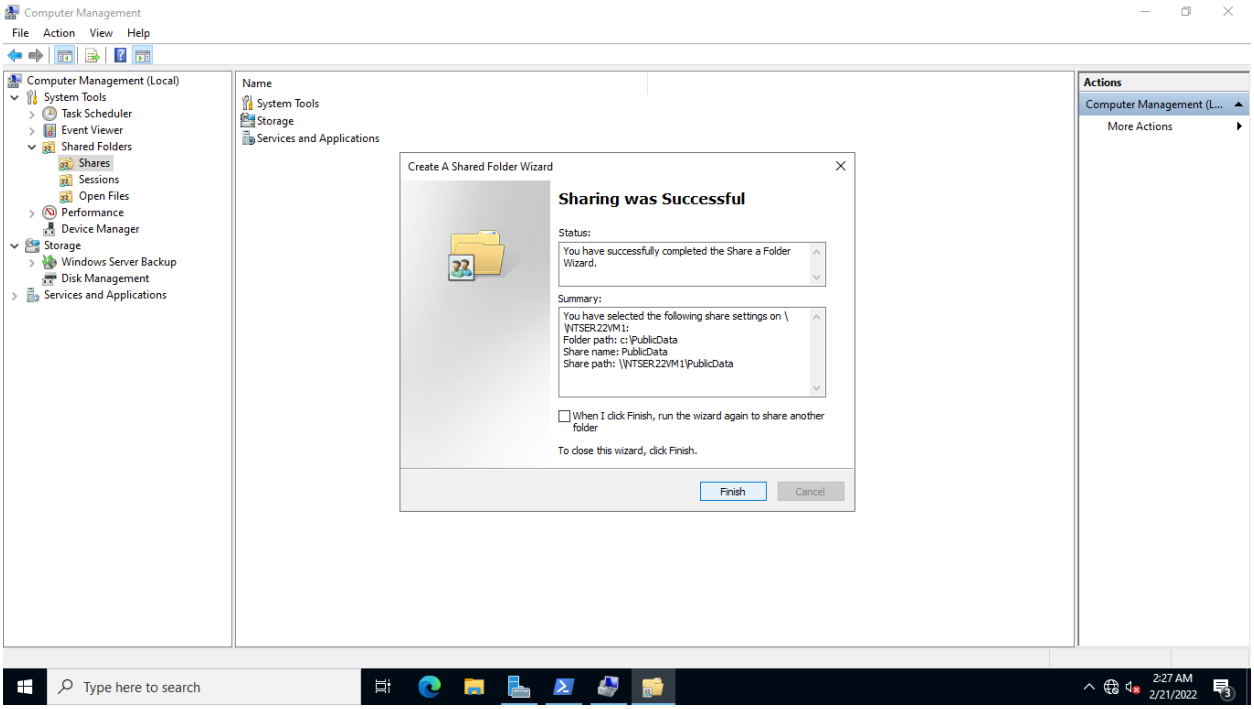
Step 17:

On the **Shared Folder Permissions** page, click **Finish**.



Step 18:

On the **Sharing was Successful** page, click **Finish**.



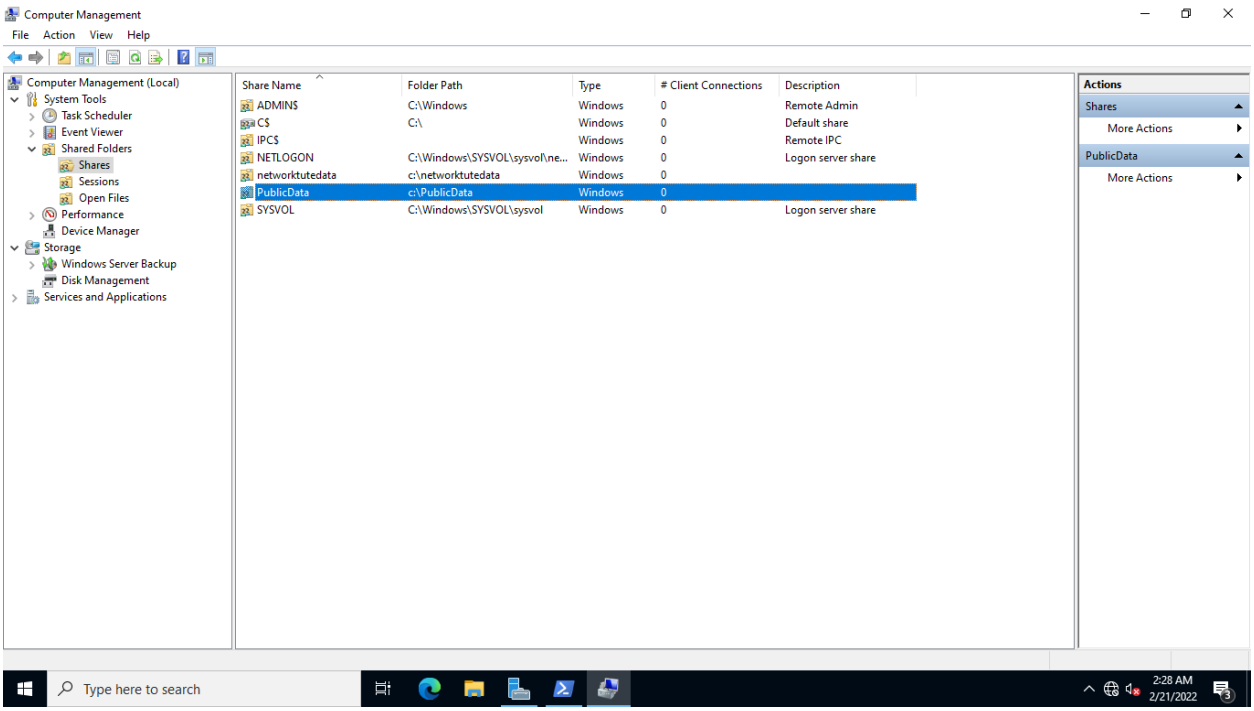
Step 19:

Ensure the **Computer Management** window is open.

Under **Shared Folders**, click **Shares.**

Notice the **PublicData** shared folder is now available in the middle pane.

Close the **Computer Management** window.



Task 2: Modify NTFS Permissions

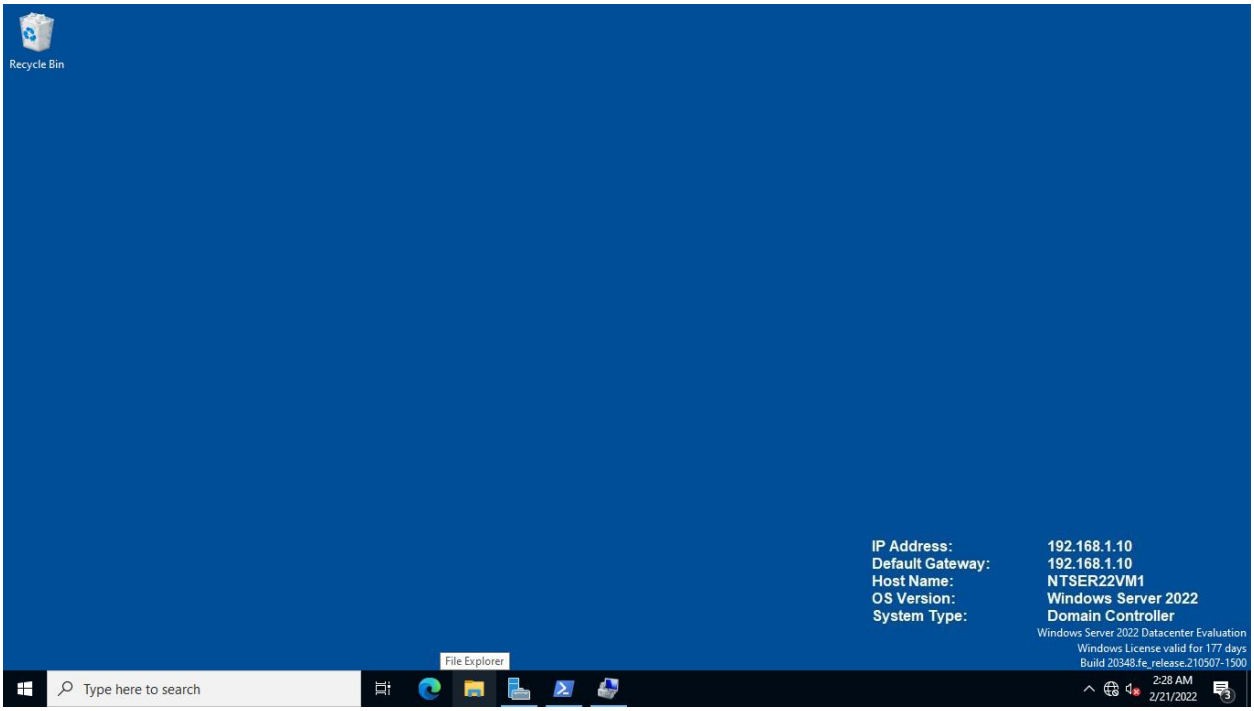
After a folder is shared, the NTFS permissions for that folder must be specified to define which security groups will have access to it.

In this task, we will examine the NTFS permissions set on a folder in NTSER22VM1then change the folder inheritance settings.

Step 1:

Make sure you turn on **NTSER22VM1.**

Click **File Explorer** on the **Taskbar**.

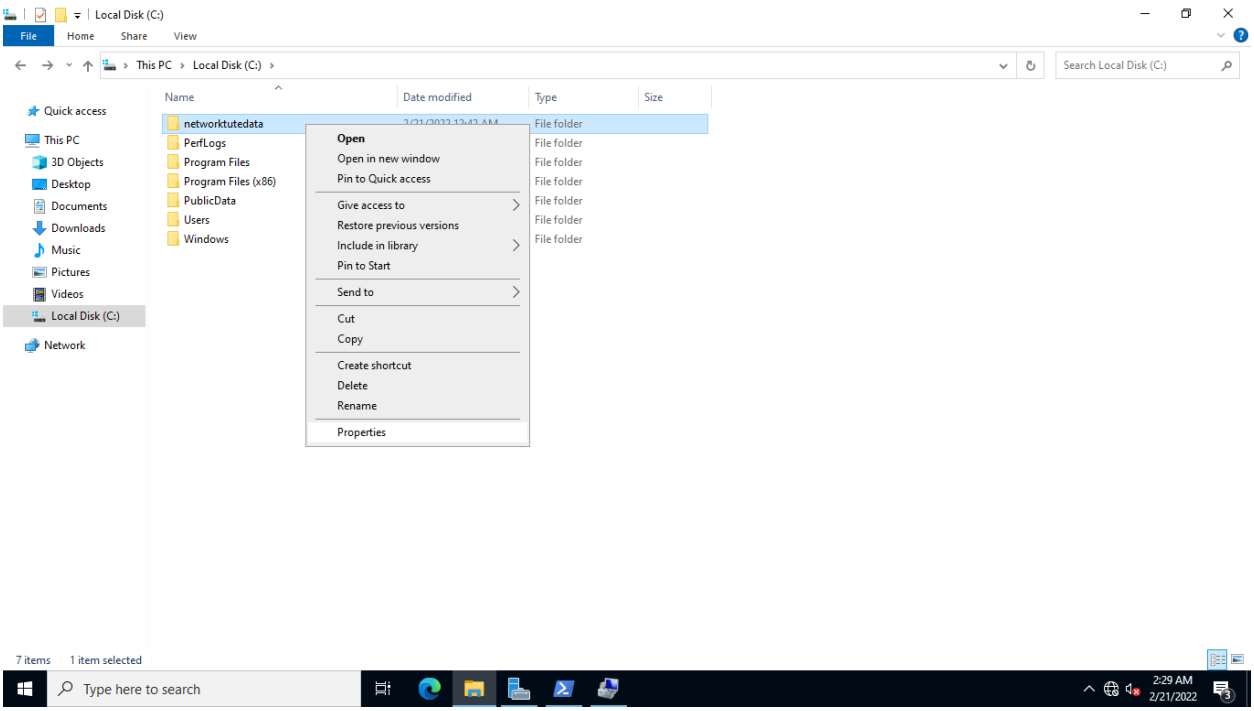


Step 2:

On the **File Explorer** window, expand **This PC** and **Local Disk (C:).**

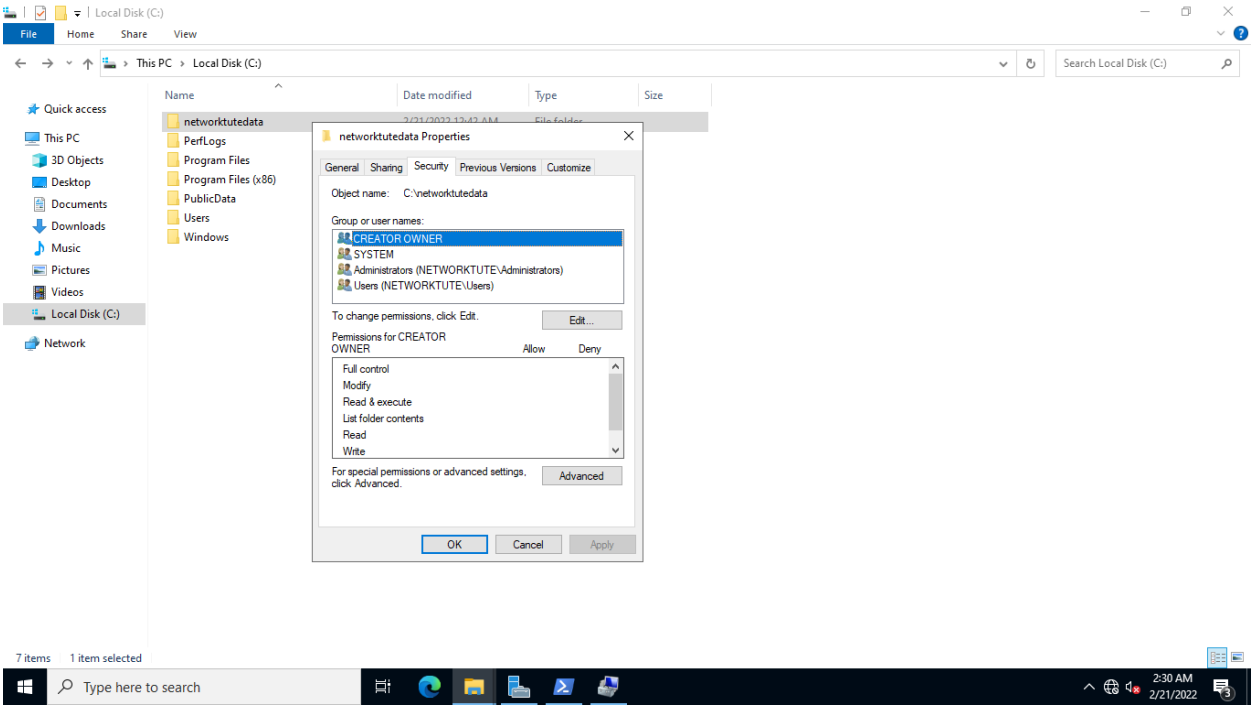
Right-click the **networktutedata** folder and select **Properties.**

Note: Recall that in an earlier task, the **networktutedata** folder was shared using Windows PowerShell.



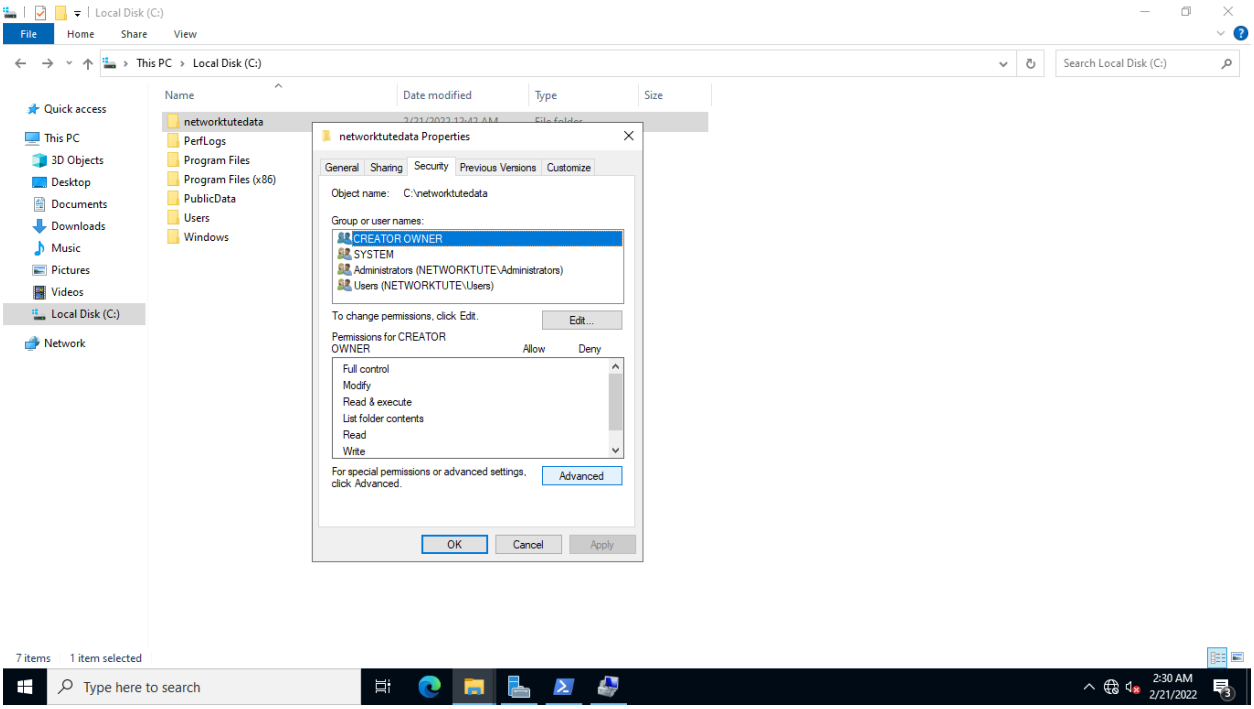
Step 3:

On the **networktutedata Properties** dialog box, click the **Security** tab.



Step 4:

From the **Security** tab, click **Advanced**.



Step 5:

On the **Advanced Security Settings for networktutedata** dialog box, notice that the permissions were inherited from drive **C:** as indicated in the **Inherited from** column.

Notice the different assigned permissions in the **Access** column:

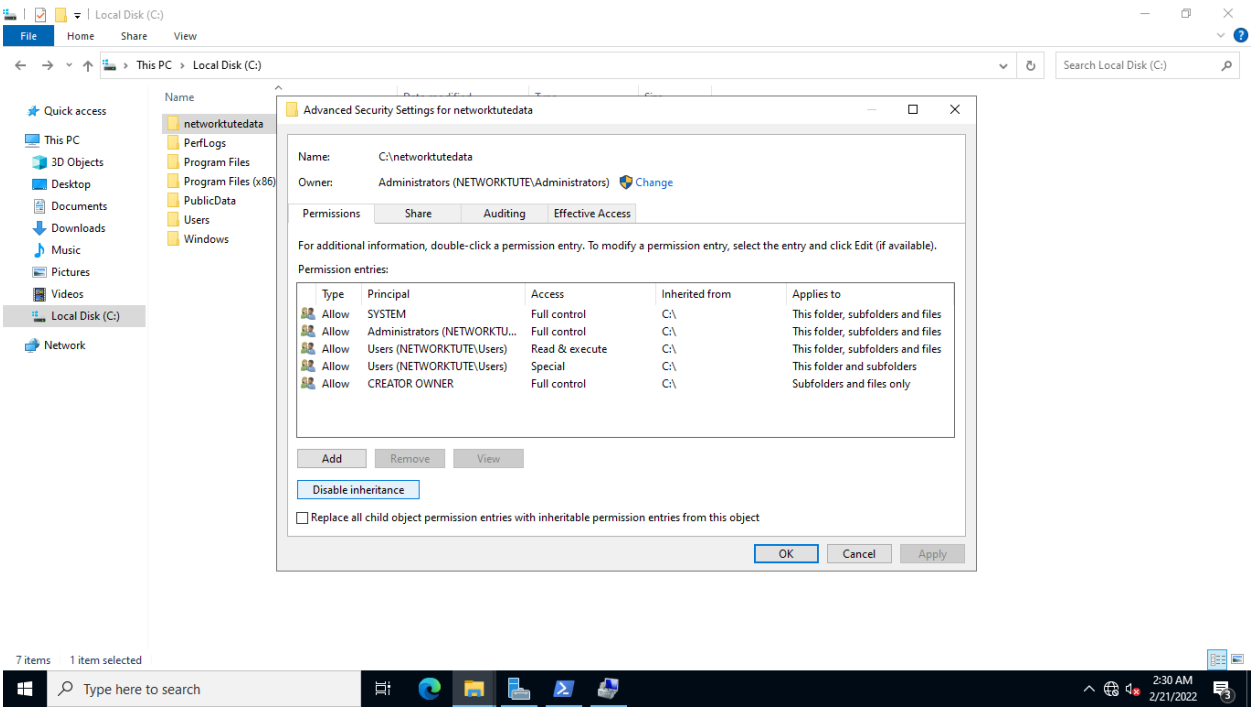
Read & execute: Users will only be able to view files and execute programs.

Full control: Users/groups will have full control over selected files/folders.

Special: Special advanced permission sets which are defined by the Administrator.

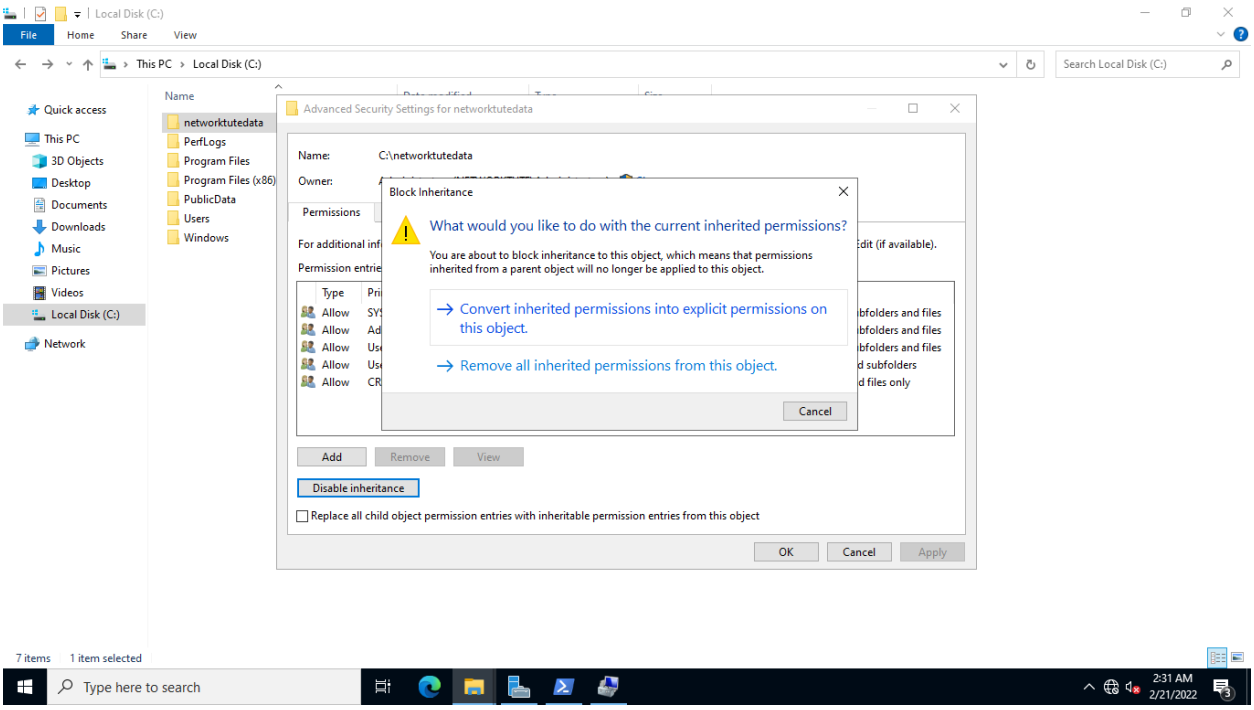
NOTE: CREATOR OWNER is a unique identifier for anyone who creates a folder or file. **Full Control** must be provided to the **CREATOR OWNER** in order for the person who created the folder or file to have total control over it. said the object

Click **Disable Inheritance.**



Step 6:

On the **Block Inheritance** message box, click **Convert inherited permissions into explicit permissions on this object.**

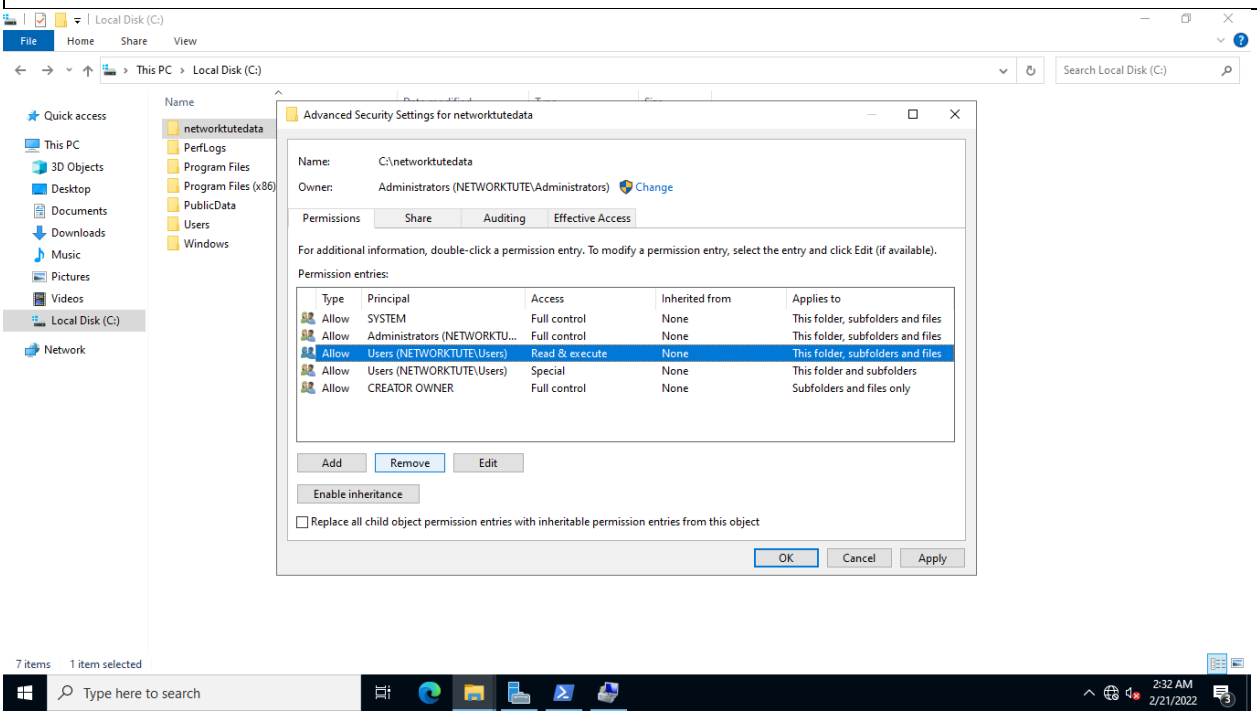


Step 7:

On the **Advanced Security Settings for networktutedata** dialog box, select the first of the two instances of **Users (NTWIN11VM1\Users)** and click **Remove**.

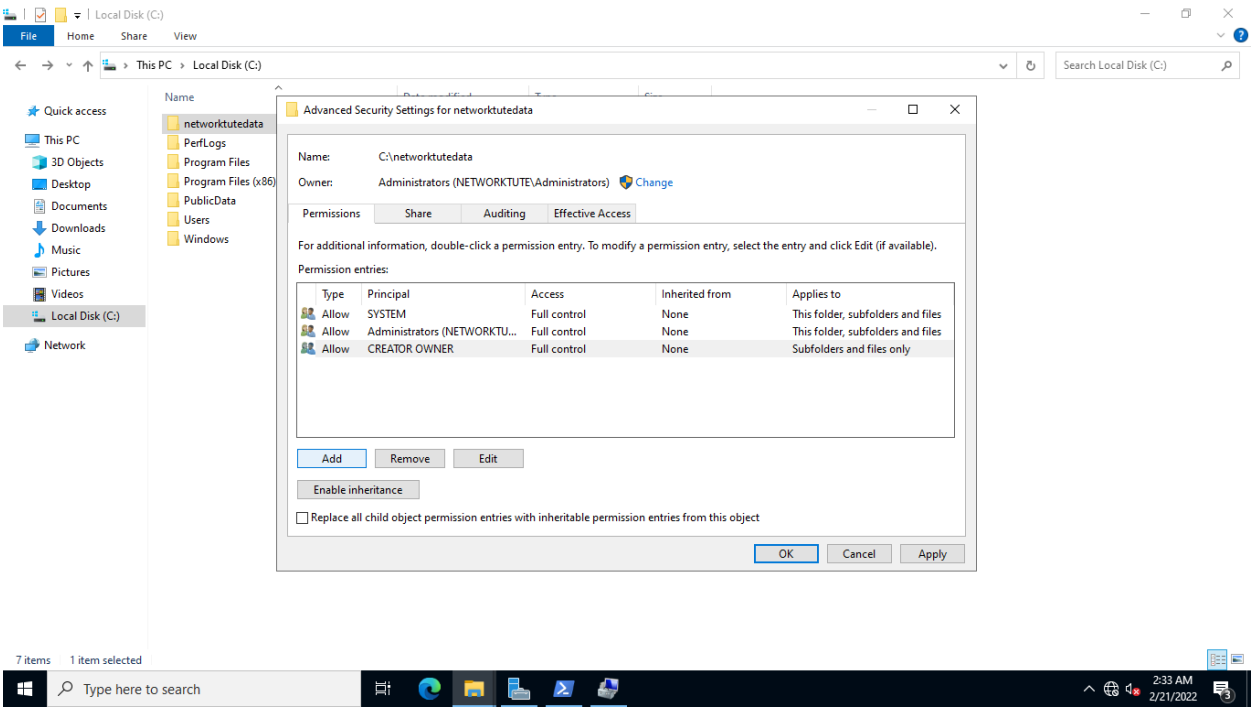
Select the second instance of Users **Users (NTWIN11VM1\Users)** and click **Remove** again.

Note: that you will not be able to remove the two instances of **Users (NTWIN11VM1\Users)** in one go



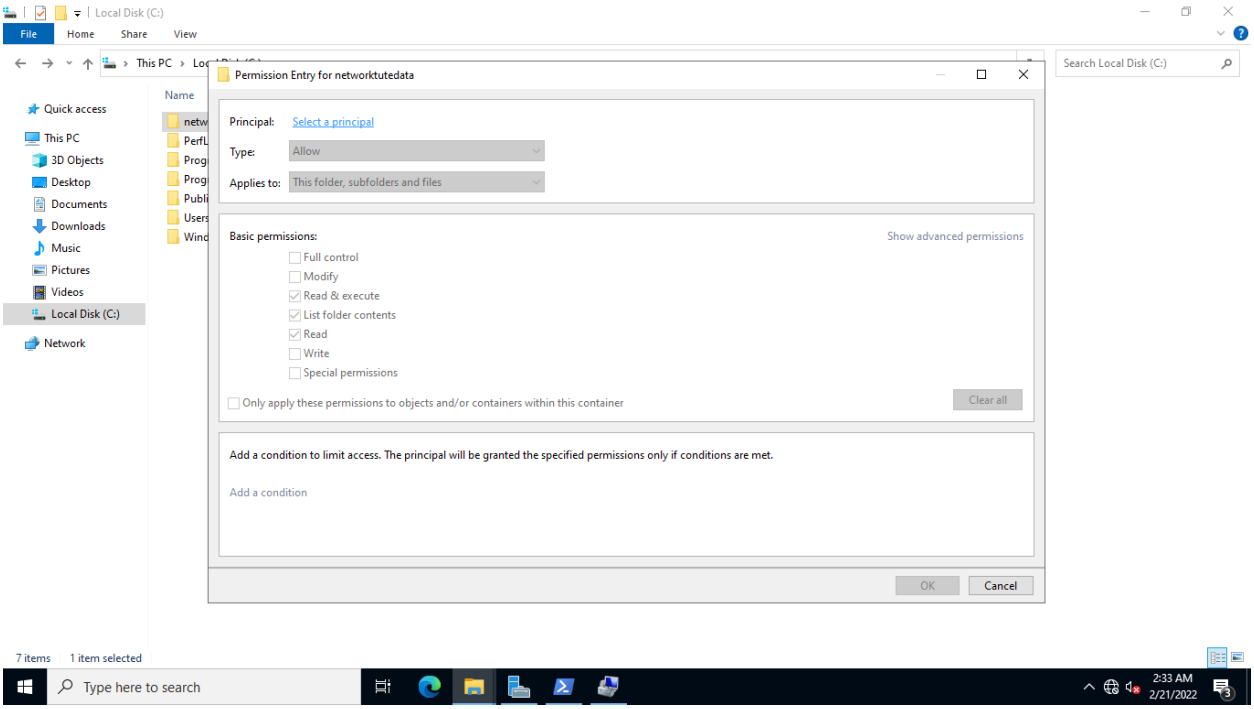
Step 8:

On the **Advanced Security Settings for networktutedata** dialog box, click **Add**.



Step 9:

On the **Permission Entry for networktutedata** dialog box, click the **Select a principal** web link



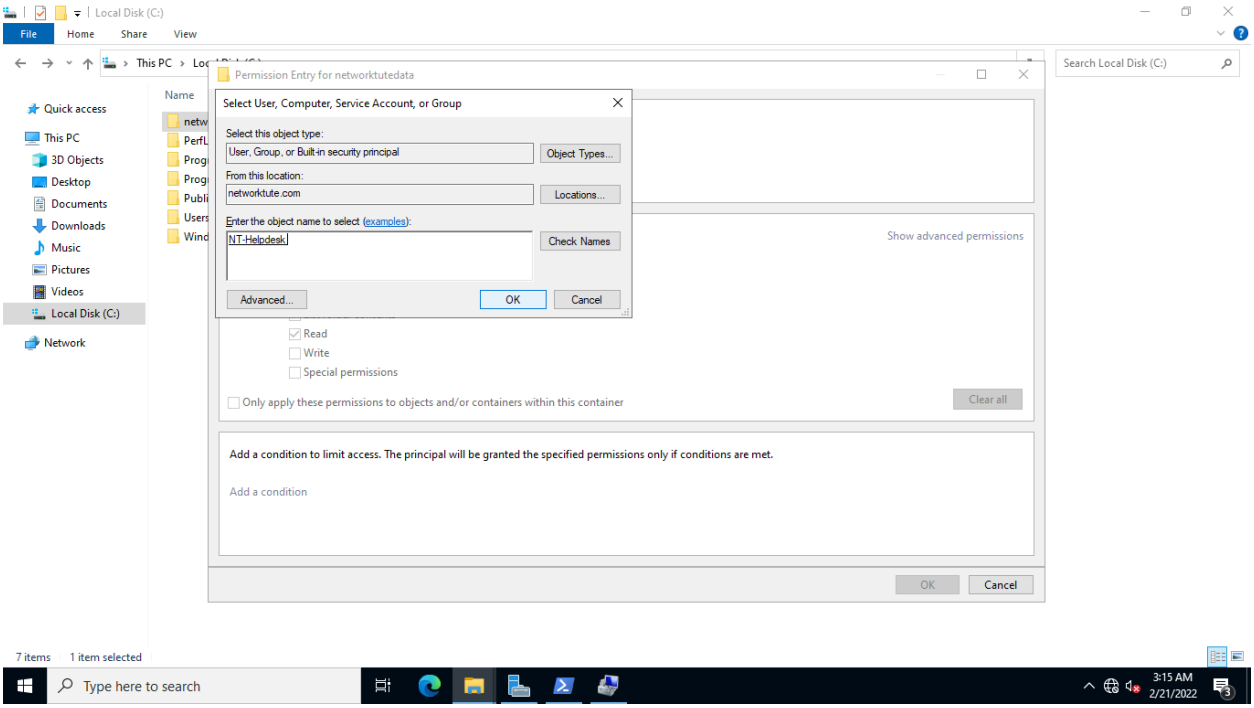
Step 10:

On the **Select User, Computer, Service Account or Group** dialog box, click in the **Enter the objective name to select** textbox and type:

nt-helpdesk

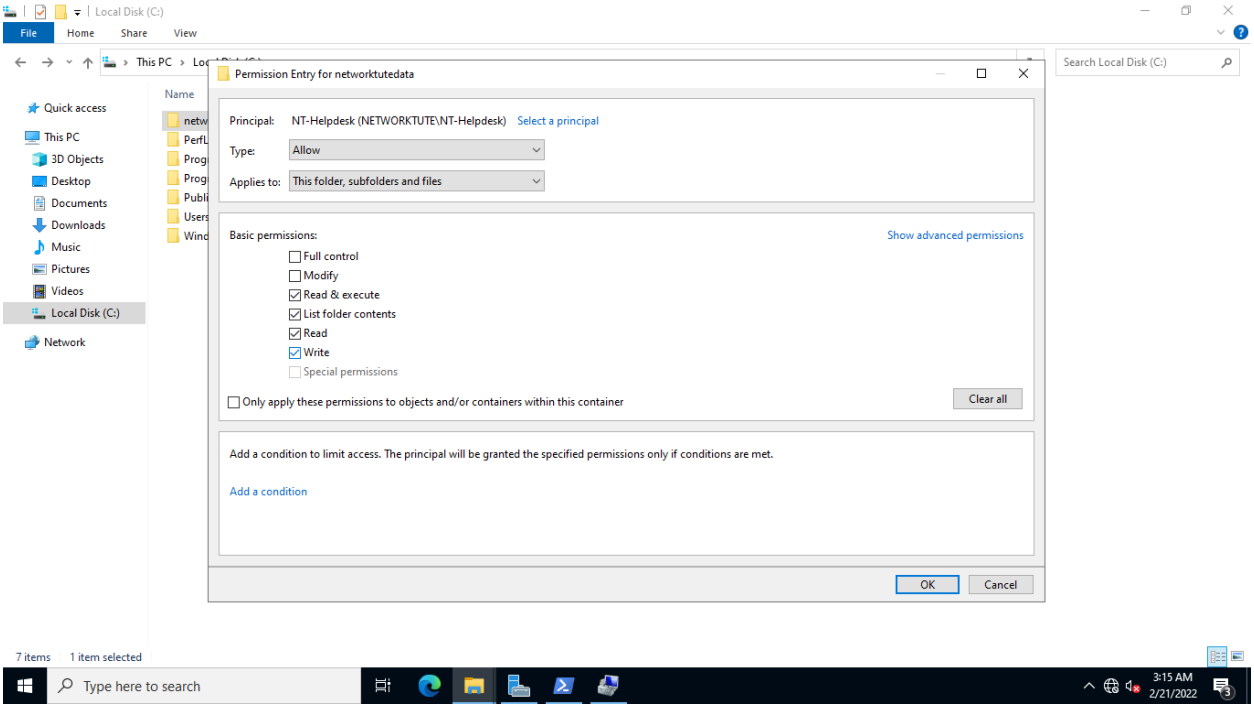
Click **Check Names** to verify you have typed in a valid group name.

Click **OK.**



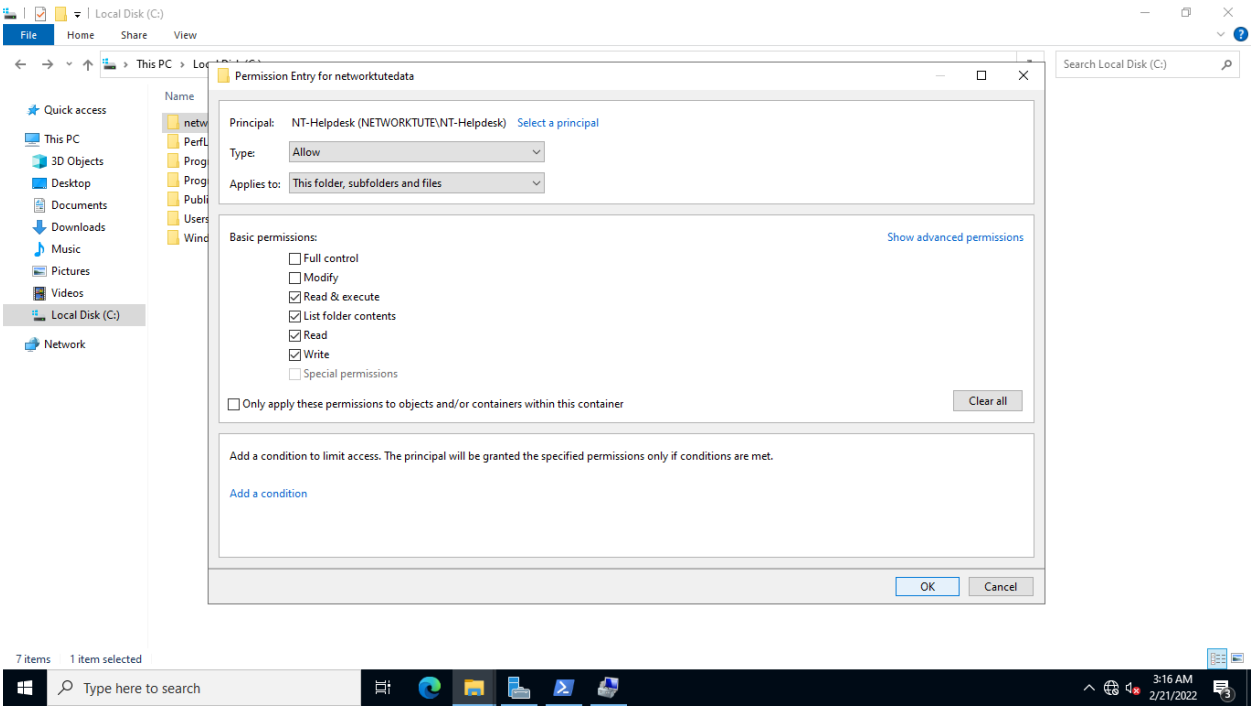
Step 11:

On the **Permission Entry for networktutedata** dialog box, under the **Basic permissions** section, tick the **Write** checkbox



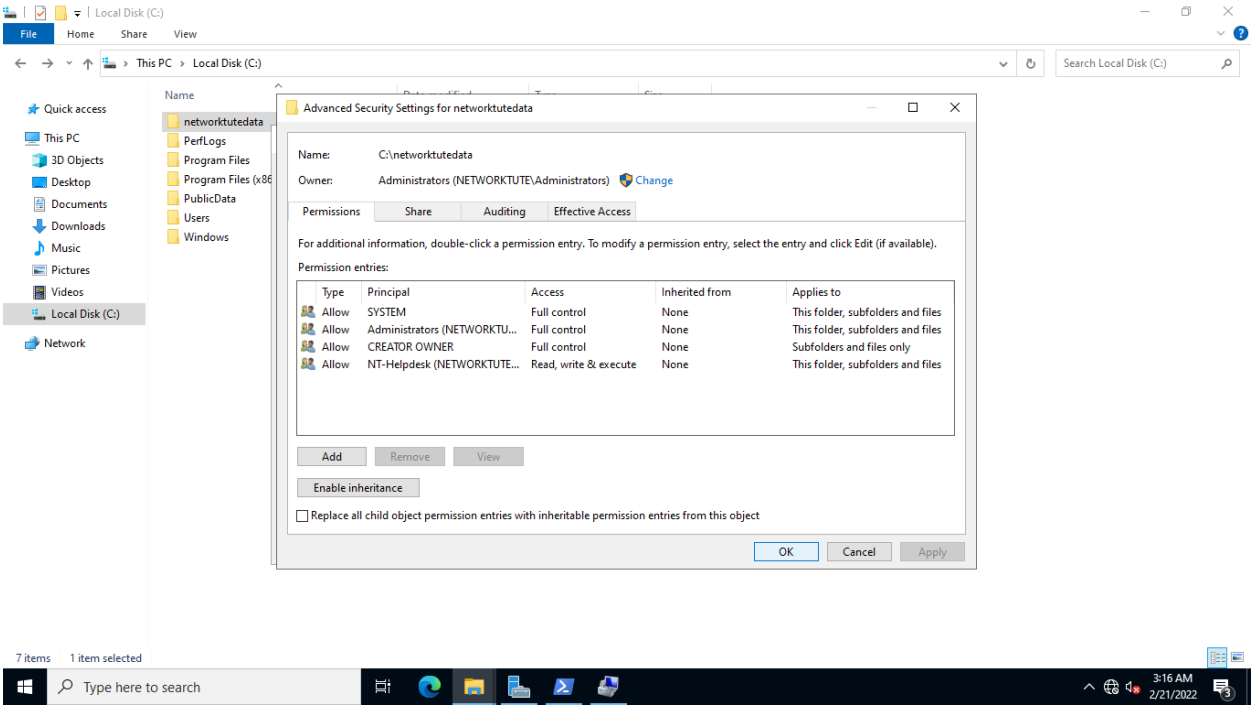
Step 12:

On the **Permission Entry for networktutedata** dialog box, click **OK.**

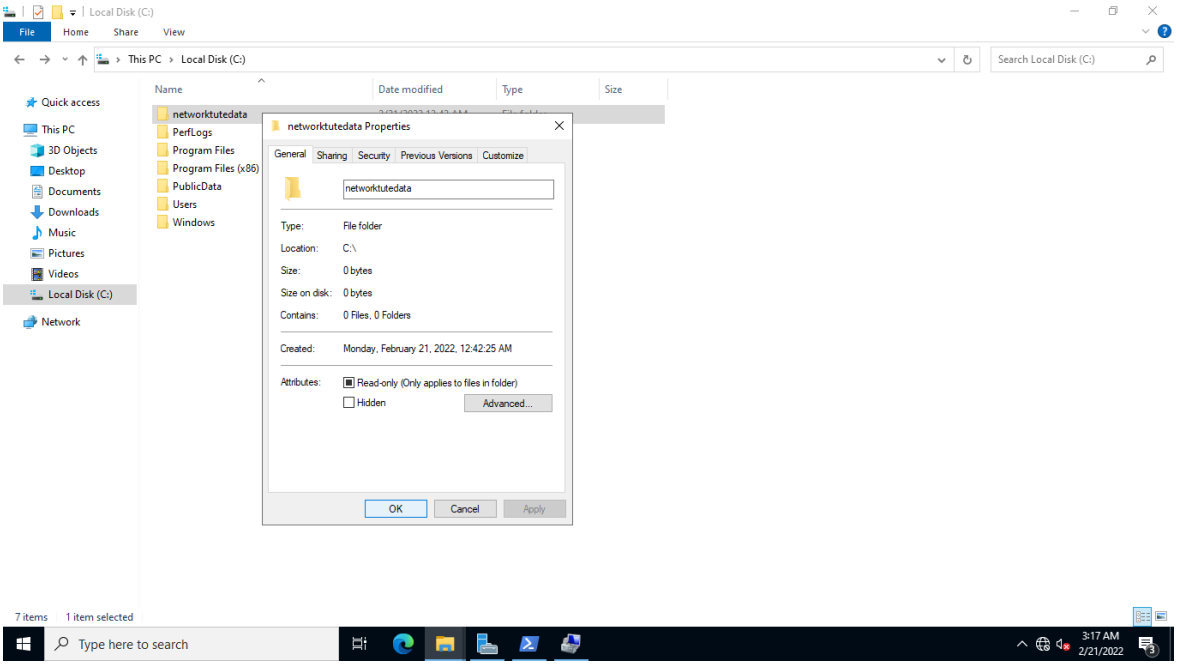


Step 13:

On the **Advanced Security Settings for networktutedata** dialog box, click **OK**.



Similarly, click **OK** to close **networktutedata Properties.**



Step 14:

Close the **File Explorer** window.