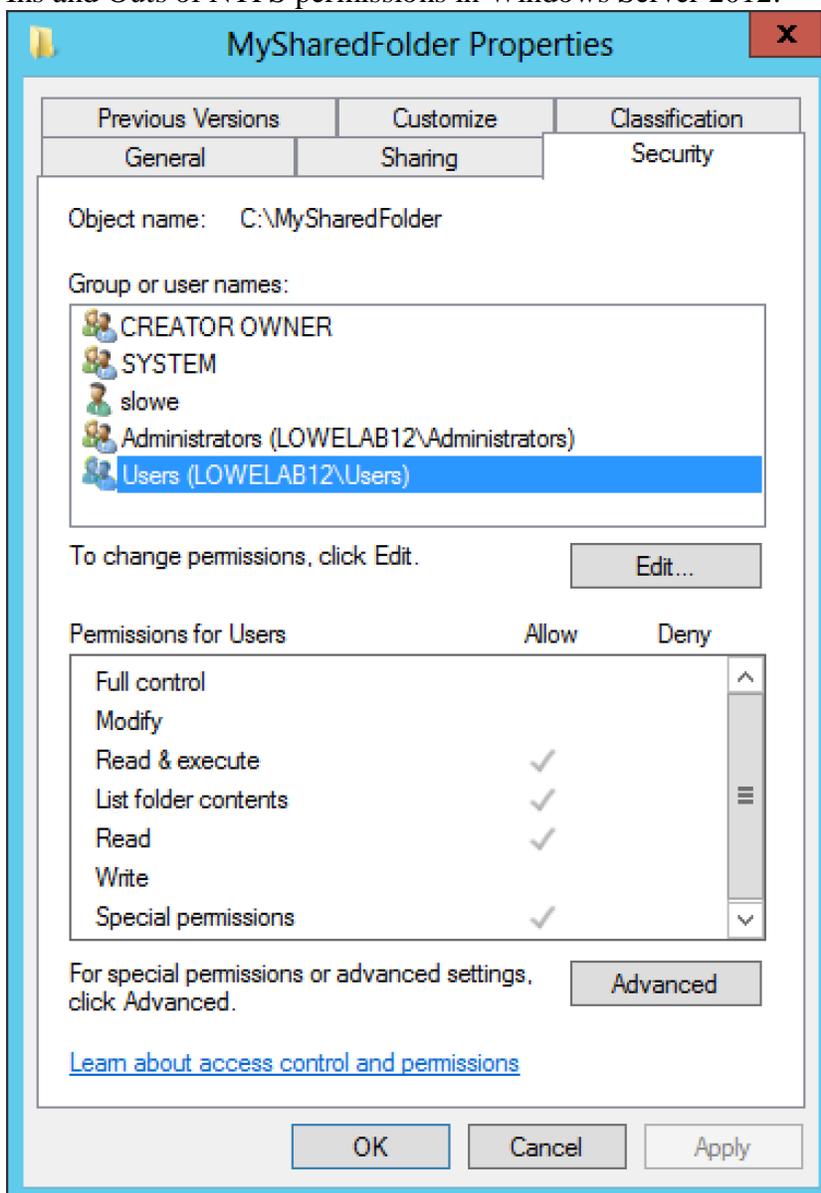


NTFS File and Folder Permissions

Windows Server 2012.

Microsoft have made lot of improvements in [Server 2012](#). One of the major changes is **Server Manager**. Server Manager is now linked with almost all the server roles. Server Manager allows you to easily setup shared folder in Windows Server 2012. **File Server** role must be installed prior to be able to share files and folder on the network. Shared folders on the network allows many users to access the files and folders. Remember, folders can be shared but individual files cannot. In Server 2012, the **File Server** role is installed by default allowing users to share files and folders. The **File Server** sub-role is found under **File and Storage Services** server role in server role installation wizard. **File Server** in Server 2012 uses [SMB 3.0](#) protocol.

Ins and Outs of NTFS permissions in Windows Server 2012.



The Security Tab

On this tab, you can see that there are a number of different permissions available for the selected user. Any changes you make will apply only to the selected user. If you want to make changes to multiple users, either add the user to a group and then apply permissions to the group or individually apply permissions to individual users one by one.

Permissions explained

I'll start with an explanation for what each permission means. Bear in mind that permissions can be set at both the folder and the file level. The table below outlines what each permission does for both folders and files.

Permission name	Description (folder)	Description (file)
Full control	The user has full control to the folder and can add, change, move and delete items. <i>The user can also add and remove permissions on the folder as well as for any subfolders.</i> The italicized sentence is very important to keep in mind. This permission level can be dangerous in the wrong hands.	The user has full control to the file and can change, move or delete it. <i>The user can also add and remove permissions on the file.</i>
Modify	A combination of Read and Write permissions. A user also has the ability to delete files within a folder that has the Modify permission. She can also view the contents of subfolders.	A user is able to modify the contents of the selected file.
Read & execute	Users are allowed to read the contents of files in the folder or execute programs inside the folder.	Users are allowed to read the contents of the file or execute the program.
List folder contents	Allows the user to view the contents of the selected folder. The user is not allowed to read a file's contents or execute a file.	This permission is not available at the file level
Read	The user can read the contents of a folder.	The user can read the contents of a file.
Write	A user can create files and	A user can create a file.

	folders. This does not grant a user with the ability to read any existing information.	
--	--	--

You will note that the permissions screen has both Allow and Deny columns. You are able to allow a user a particular set of rights or deny a user access rights to a particular file or folder.

As you create groups for permissions reasons, understand that the permissions that you assign are cumulative. So, perhaps you grant a user's account rights to read/execute the contents of a folder and you grant a group to which the user belongs the ability to write to a folder. The user will get all of those permissions because NTFS rights are cumulative.

When Deny permissions are involved, they *always override Allow permissions*. It's not considered a best practice to use Deny permissions a whole lot. Doing so can create administrative nightmares that are difficult to solve. That said, Deny can be useful when group permissions have been applied to a folder, but you still want a user in that group to be denied access to the folder.

Notes

- Permissions and Security are different things
- Permissions allow Users, or Groups access to Resources such as Files, Folders and Printers
- It is best to assign Permissions to Groups and not to Individual Users
- Share and NTFS Permissions are different
- Share Permissions only matter when Resources are being accessed over the network. If a User is Local the Permissions are ignored.
- NTFS Permissions are used whether Resources are access over the Network or Locally.
- Over the Network is there are both Share and NTFS permissions set on a Resource then the Most Restrictive Permission is the one that will be applied.
- In General it is best to set Share Permissions to a resource to Everyone with Full Control, and then use NTFS Permissions to grant or restrict access.
- Share Permissions allow you to access Resource through UNC (Universal naming Convention) \\SERVERNAME\SHARE
- The FAT, FAT 16 and FAT 32 file systems used in Windows 95 and 98 could only use Share Permissions.
- Inheritance means that Permissions set to parent Folders will be inherited by Child Resources
- Log in and Out for New Permissions to be applied
- By Default Creators of Resources are the Owners.
- Resource Owners can set permissions to Resources.

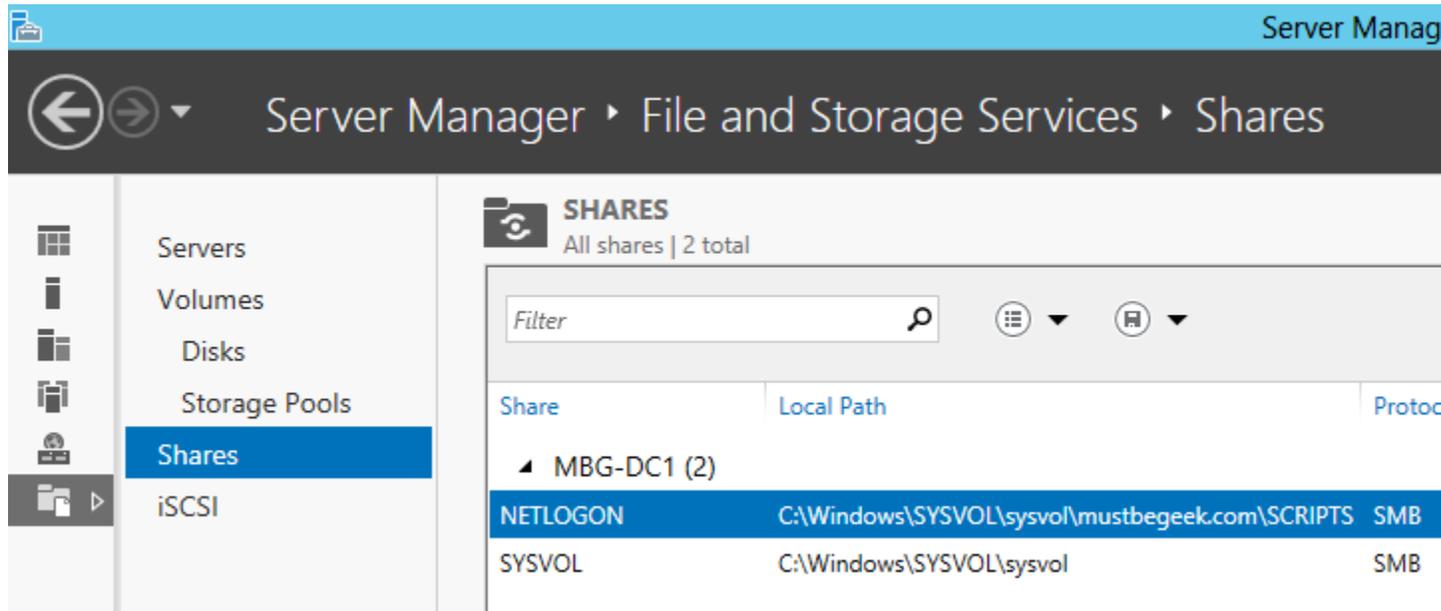
Setup Shared Folder in Windows Server 2012

Posted by [Bipin](#) on July 30, 2013

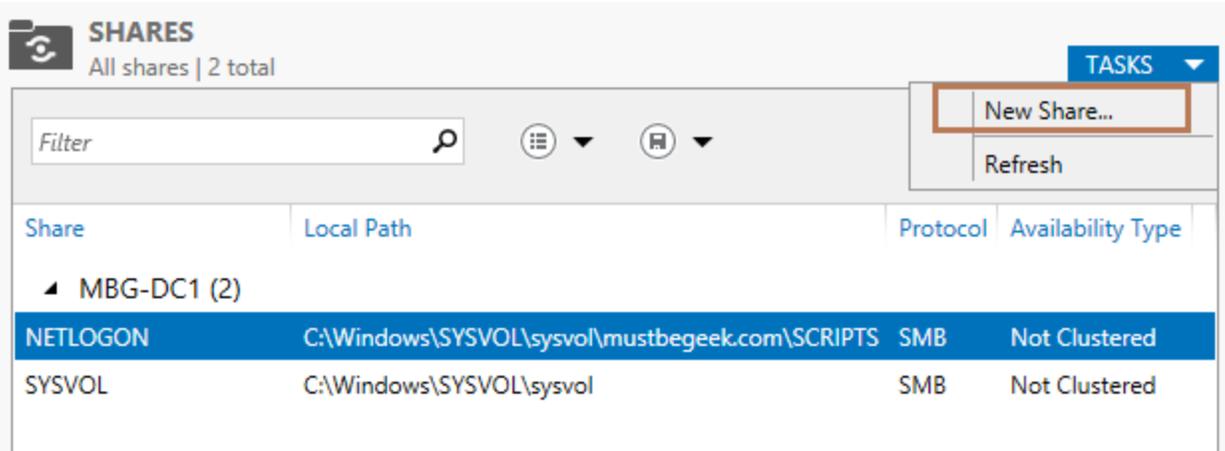
Microsoft have made lot of improvements in [Server 2012](#). One of the major changes is **Server Manager**. Server Manager is now linked with almost all the server roles. Server Manager allows you to easily setup shared folder in Windows Server 2012. **File Server** role must be installed prior to be able to share files and folder on the network. Shared folders on the network allows many users to access the files and folders. Remember, folders can be shared but individual files cannot. In Server 2012, the **File Server** role is installed by default allowing users to share files and folders. The **File Server** sub-role is found under **File and Storage Services** server role in server role installation wizard. **File Server** in Server 2012 uses [SMB 3.0](#) protocol.

Setup Shared Folder in Windows Server 2012

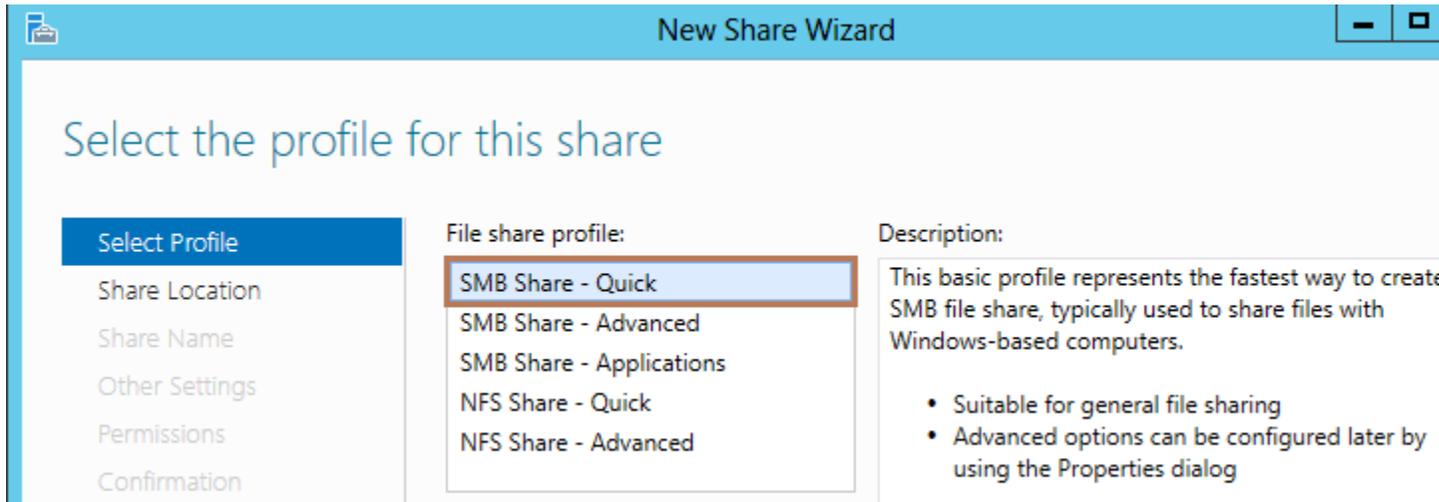
There are different ways to share a folder in Server 2012. Most efficient way is to use the **Server Manager**. Here, I will configure some shared folder from domain controller named **MBG-DC1**. So, let's setup some shared folders. To do so, open **Server Manager**. Click **File and Storage Services** on the left pane. Then click **Shares** from the list. You will see the list of shared folders on this server. As you can see below there are two folders, **netlogon** and **sysvol** shared by default. This is because the server is [AD DC](#).



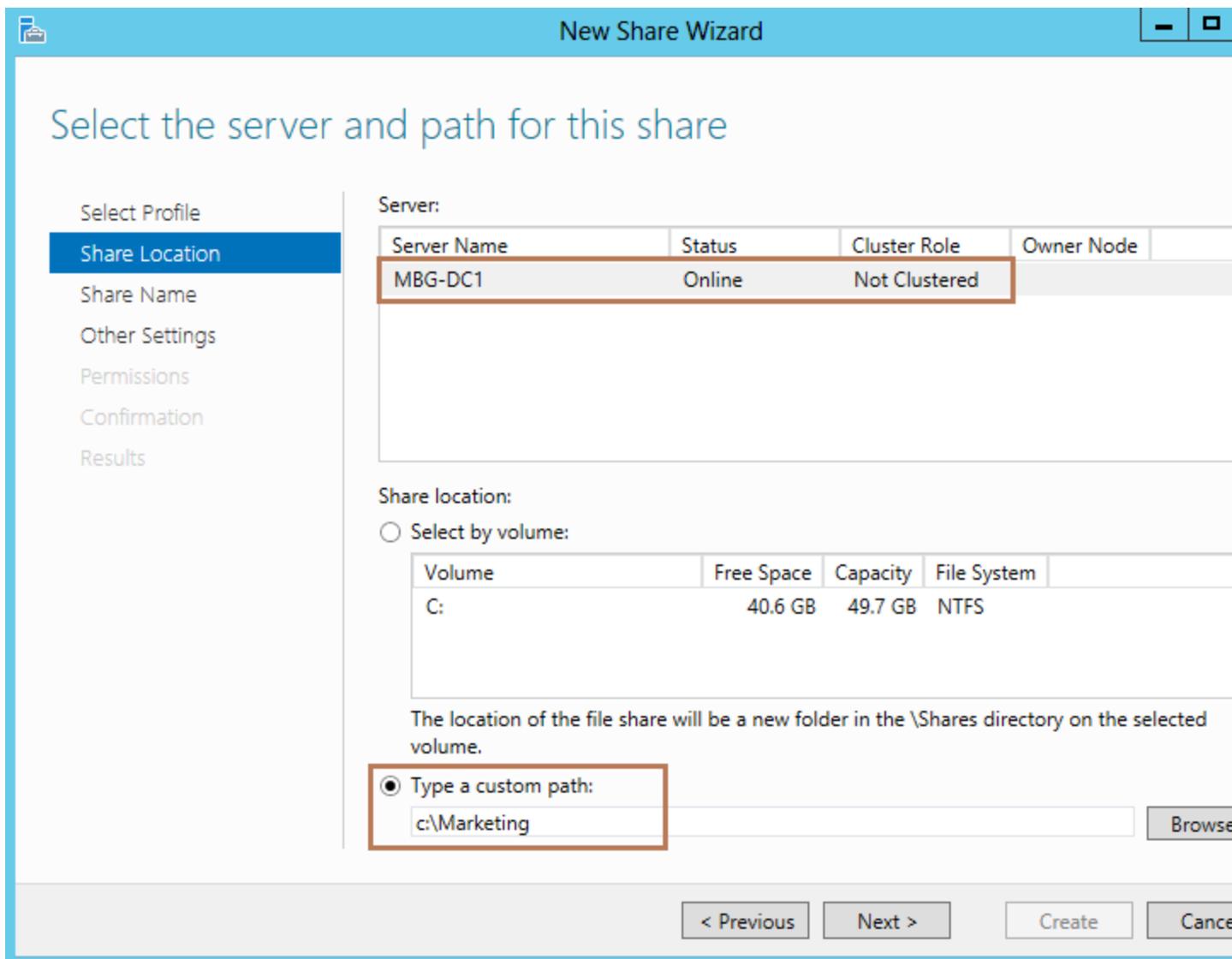
We have a scenario. We want to share a folder named **Marketing** to **Marketing users group**. We want only the marketing users to view and execute the contents of the folder. We already have Marketing users group set up and assigned users into the group. So, let's create the shared folder. To create a new shared folder, click **Tasks** and click **New share** in **Server Manager** console.



New **share wizard** pops up. There are number of share profiles by default. You can choose any of these share profiles as seen below. I will choose **SMB Share - Quick** and click **Next**.



Now you are asked to provide the share location of the folder that you want to share. I will choose custom location as C:\Marketing. Then click **Next**.



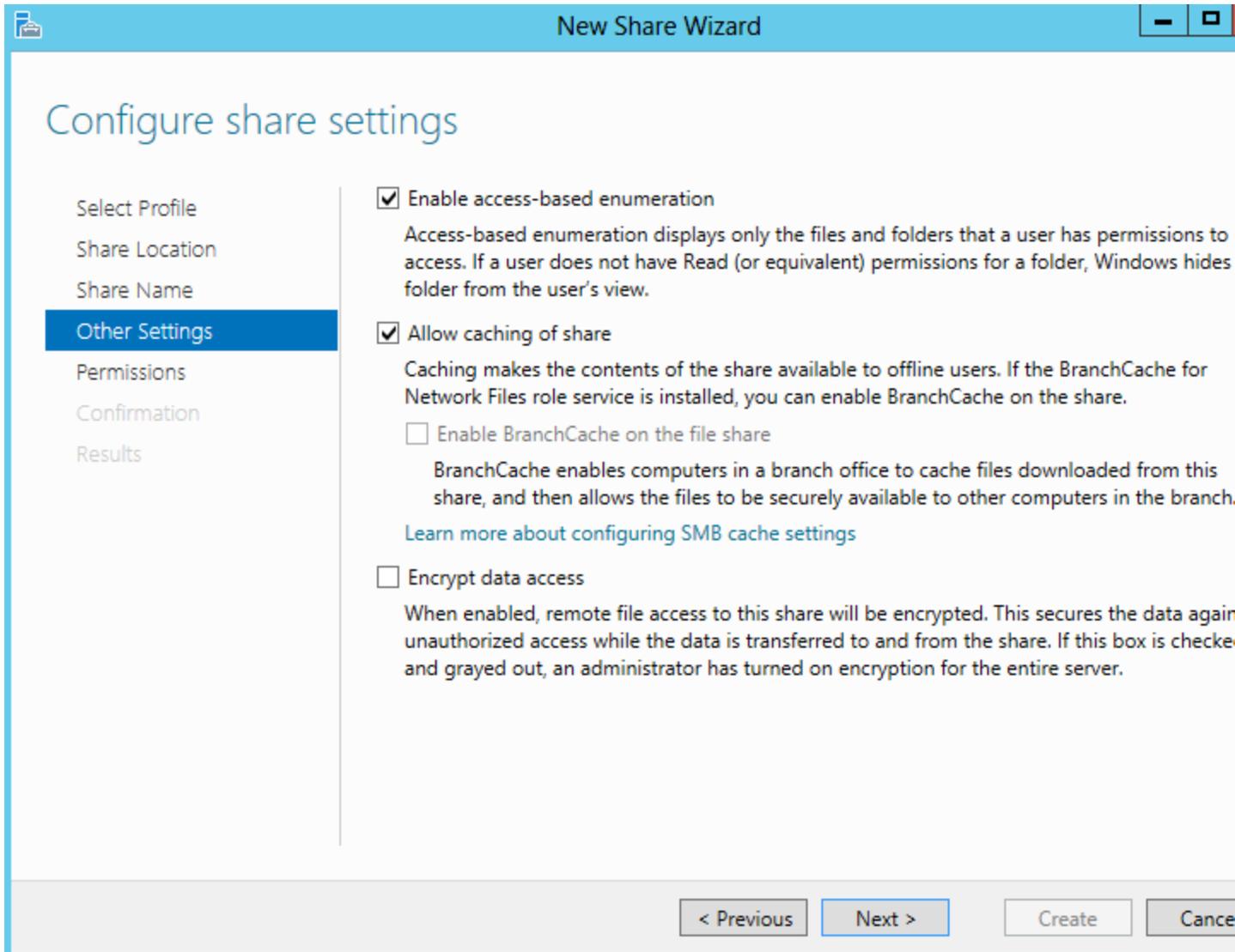
Type the share **name** and **description** of the shared folder. Then click **Next**. Click **OK** to create the new directory on path doesn't exist warning.

The screenshot shows the 'New Share Wizard' window with the 'Specify share name' step selected in the left-hand navigation pane. The main area contains the following fields:

- Share name:** A text box containing 'Marketing', which is highlighted with a red rectangular border.
- Share description:** A text box containing 'This folder is shared to Marketing Group only.'
- Local path to share:** A text box containing 'c:\Marketing'.
- Remote path to share:** A text box containing '\\MBG-DC1\Marketing'.

The left-hand navigation pane includes the following options: Select Profile, Share Location, Share Name (highlighted in blue), Other Settings, Permissions, Confirmation, and Results.

Now configure other settings. Here, I will check to enable **access-based enumeration**. This option makes the folder visible for users that have permission to access the folder otherwise the folder will be hidden. **Allow caching of share** option makes the folder to be accessed even when the user is offline. Click **Next**.



Here, configure the folder permission. The shared folder have **shared folder permission** and **NTFS permission**. These both permission work together to allow/deny users to access the shared folder. Microsoft recommends to allow full control for share permission and use NTFS permission to restrict and configure folder access. As you can see below, **Share permissions: Everyone Full Control**. The permission shown here, is the inherited NTFS permission from drive NTFS permission. To change the permission, click **Customize permission**.

New Share Wizard

Specify permissions to control access

- Select Profile
- Share Location
- Share Name
- Other Settings
- Permissions**
- Confirmation
- Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

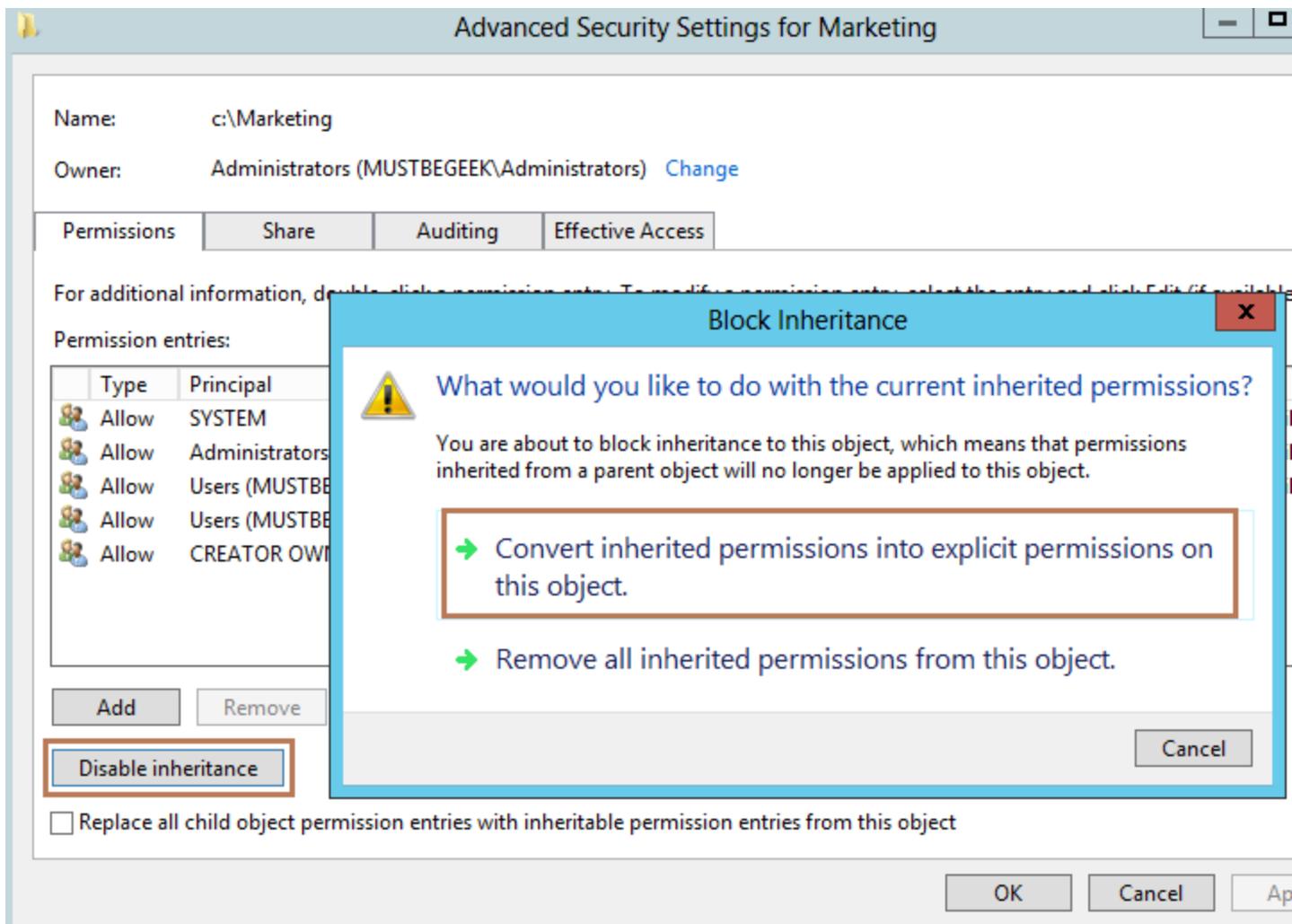
Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files

Customize permissions...

Click **disable inheritance**. Then select **convert inherited permission into explicit permissions on this object**.



You can see the changes below. Remove both **User groups** from the permission. This Users group contains all the users of the domain. We don't want all the users of the domain to access this shared folder so remove it. Click **Add** to add the marketing group. Click **Select a principal** and add **Marketing** group. Select the basic permissions and click **OK**.

Permission Entry for Marketing

Principal: Marketing (MUSTBEGEEK\Marketing) [Select a principal](#)

Type:

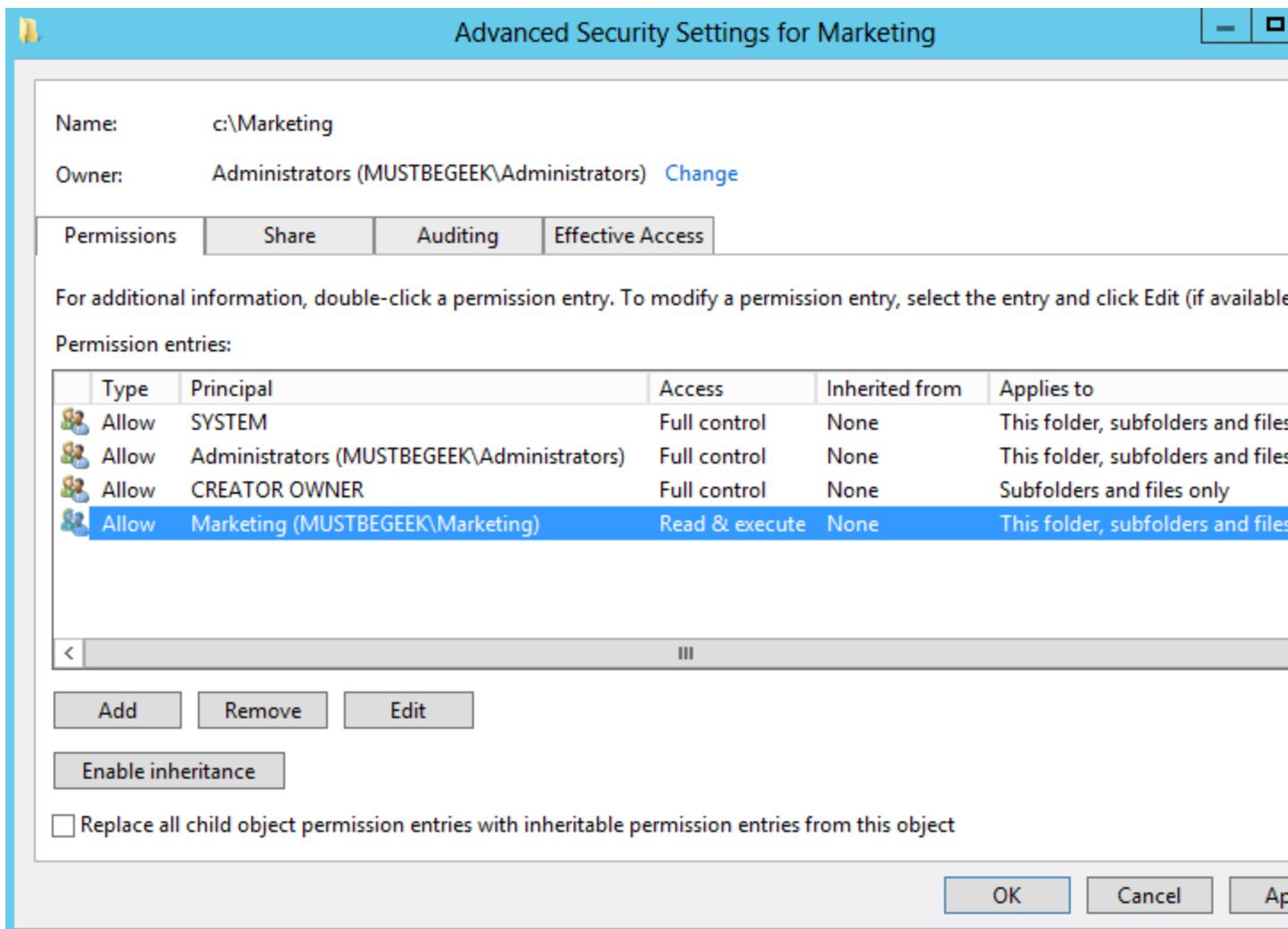
Applies to:

Basic permissions:

- Full control
- Modify
- Read & execute
- List folder contents
- Read
- Write
- Special permissions

Only apply these permissions to objects and/or containers within this container

Now the overall permission for the **Marketing** folder looks like this. Users of marketing group can only read the files of **Marketing** folder.



Now let's come back to the wizard. Click **Next**.

New Share Wizard

Specify permissions to control access

- Select Profile
- Share Location
- Share Name
- Other Settings
- Permissions**
- Confirmation
- Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

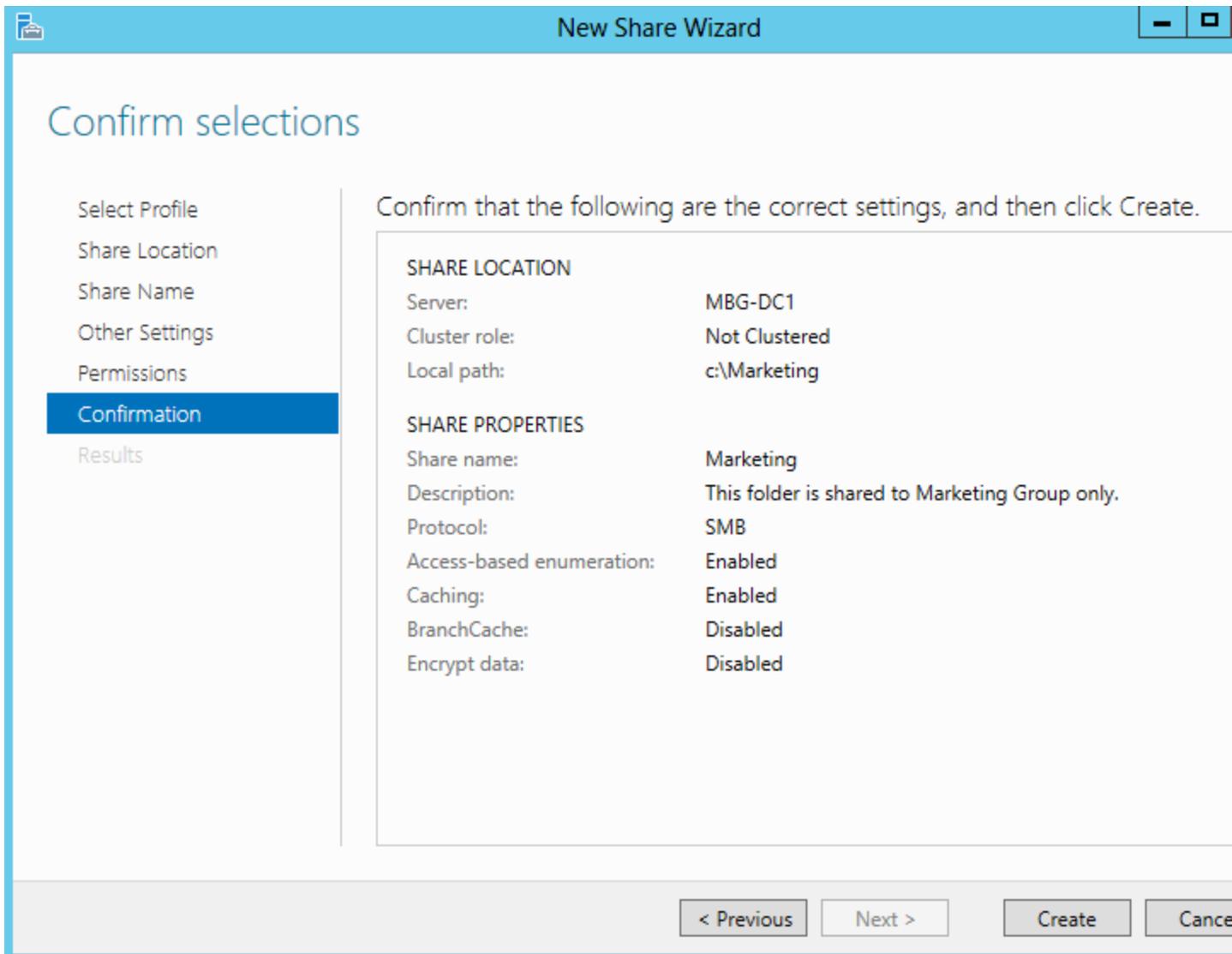
Share permissions: Everyone Full Control

Folder permissions:

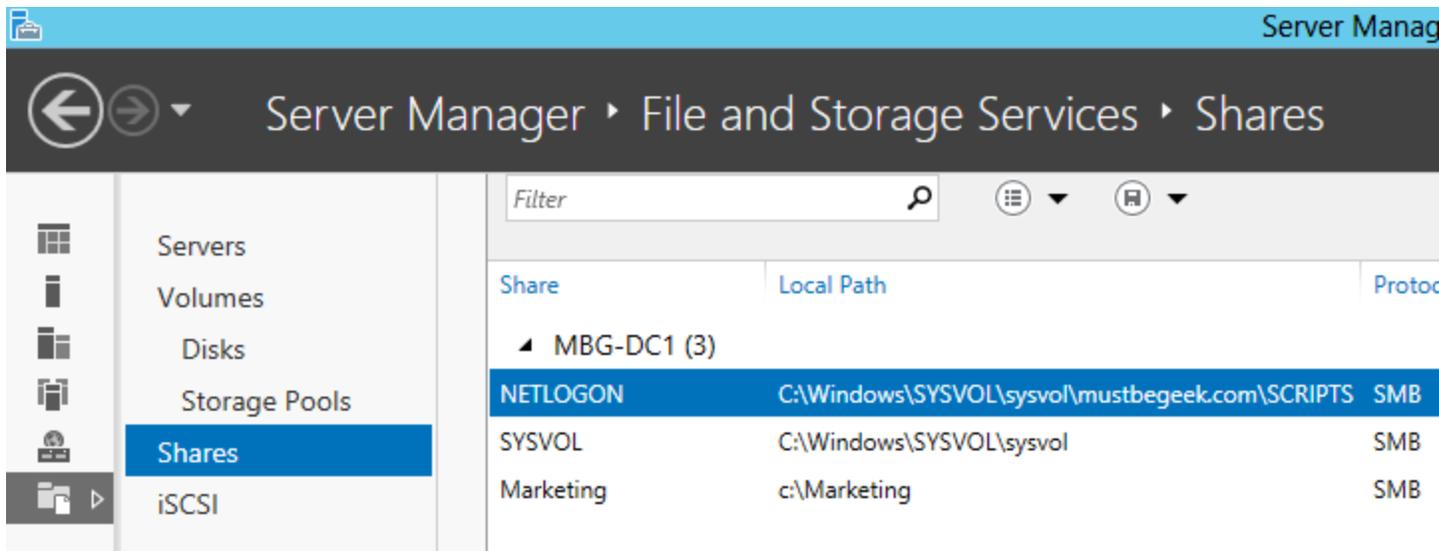
Type	Principal	Access	Applies To
Allow	MUSTBEGEEK\Marketing	Read & execute	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only

Customize permissions...

Review the settings and click **Create**.

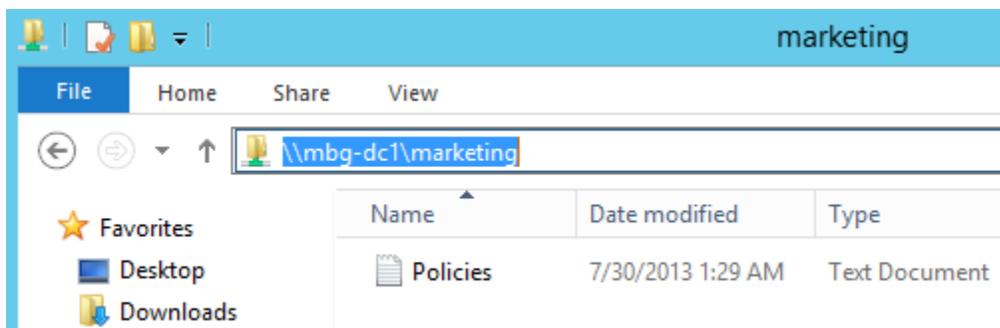


The shared folder is now created. You can view the shared folder in **Server Manager** console.



In this way you can configure shared folder using **Server Manager**. Remember, NTFS permissions and shared folder permissions are different. If NTFS permission and shared folder permission are conflicting, then the most restrictive permission is applied. For example, if you configure NTFS permission to **Full Control** and shared permission to **Read** on a folder then the permission applied will be **Read** only. Best practice to manage permissions for shared folder is, *configure full control permission for everyone* and restrict the folder access using *NTFS permission*.

Clients can now access the shared folder by typing the UNC (Universal Naming Convention) path of the shared folder in windows explorer. In our case, the **UNC** path is, **\\MBG-DC1\Marketing**.



In this way you can access the shared folder contents.

Read

Read is the default permission that is assigned to the Everyone group. Read allows:

- Viewing file names and subfolder names
- Viewing data in files
- Running program files

Change

Change is not a default permission for any group. The Change permission allows all Read permissions, plus:

- Adding files and subfolders
- Changing data in files
- Deleting subfolders and files

Full Control

Full Control is the default permission that is assigned to the Administrators group on the local computer. Full Control allows all Read and Change permissions, plus:

- Changing permissions (NTFS files and folders only)