In organizations today, it's critical that storage be treated as a pivotal part of planning and execution. Understanding the growth of users and data in an organization needs to be reflected in storage planning.

Using a Drobo® as primary storage for an organization is a cost-effective solution—and as a bonus—Drobo is easy to deploy and manage. Drobo BeyondRAID™ technology and Drobo Dashboard minimize the time and effort it usually takes to manage, monitor, and maintain a storage solution.

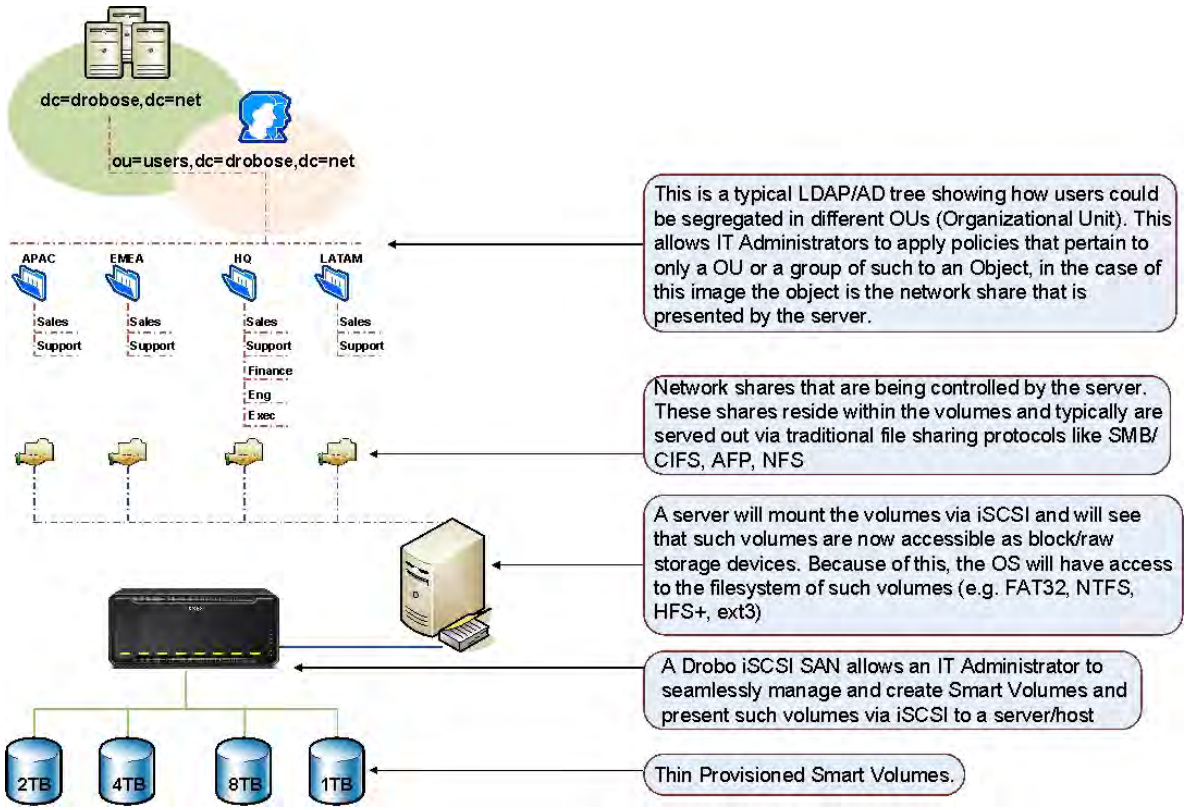
This document describes how easy it is to use a Drobo iSCSI SAN as backend storage for an organization's file servers: provisioning shares onto which Access Control List can be applied using Microsoft Windows Active Directory.

Topics

- Setup checklist and general information
- Provisioning shares using the File Server wizard

What You Will Need

- Drobo iSCSI SAN either model B800i or model B1200i
- Drobo Dashboard management software (latest version)
- Enterprise-grade 7200 RPM SATA disk drives recommended
- Windows Server Edition 2003 and above (2008 R2 used in this procedure)



Setup Checklist and General Information

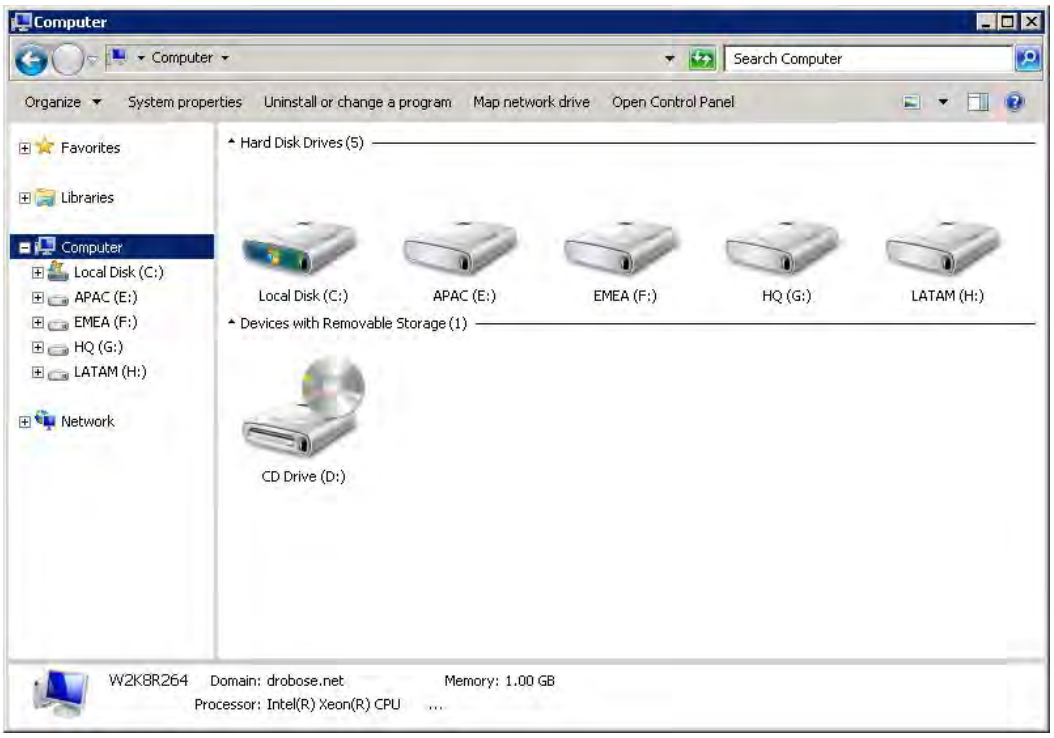
In this procedure, multiple volumes are created using a Drobo iSCSI SAN model B800i. The procedure also applies to the Drobo Pro with a USB, FireWire, or iSCSI connection (iSCSI recommended).

To learn more about Drobo and iSCSI, visit: http://www.drobo.com/resources/iscsi.php

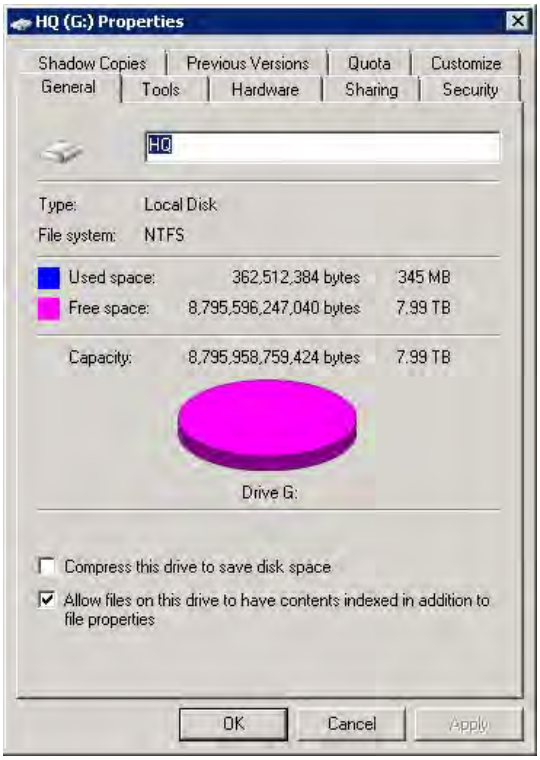
Follow the directions in the Drobo Online User Guide to configure the Drobo: http://www.drobo.com/support/documentation.php

To give you a better idea of how Drobo iSCSI SAN can be used as the backend storage for your file servers, multiple volumes are created, allowing user data to be stored on different volumes by department, function, region, and so on.

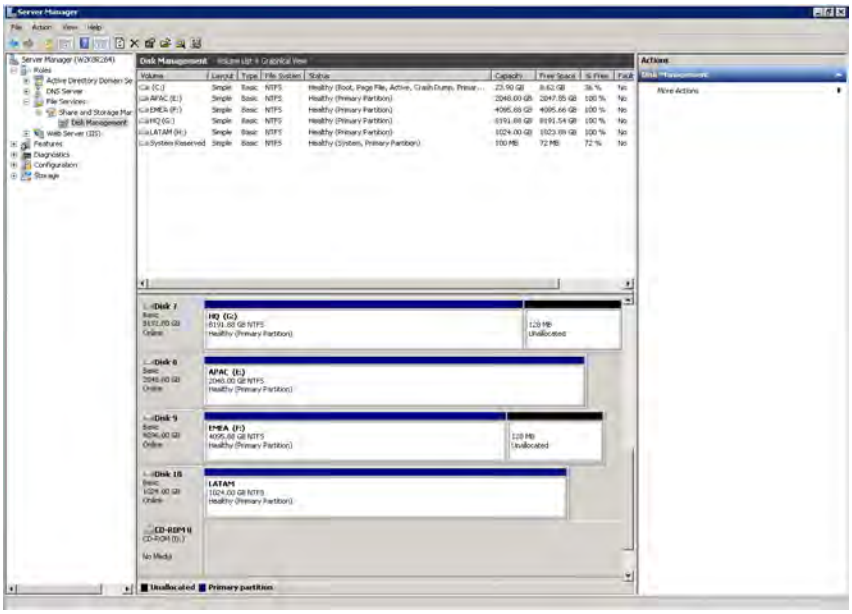
Once the volumes are mounted on the host, they appear as raw/block devices.



Looking at the properties of one of these volumes, notice that the operating systems sees them as just another hard drive. The volume shown below, for example, is formatted as an NTFS drive, allowing the operating system to take advantage of its file system features such as user access control.



STEP 1



Start by launching Server Manager in Windows Server 2008 R2. In the left navigation, go to **File Services > Share And Storage Management > Disk Management**.

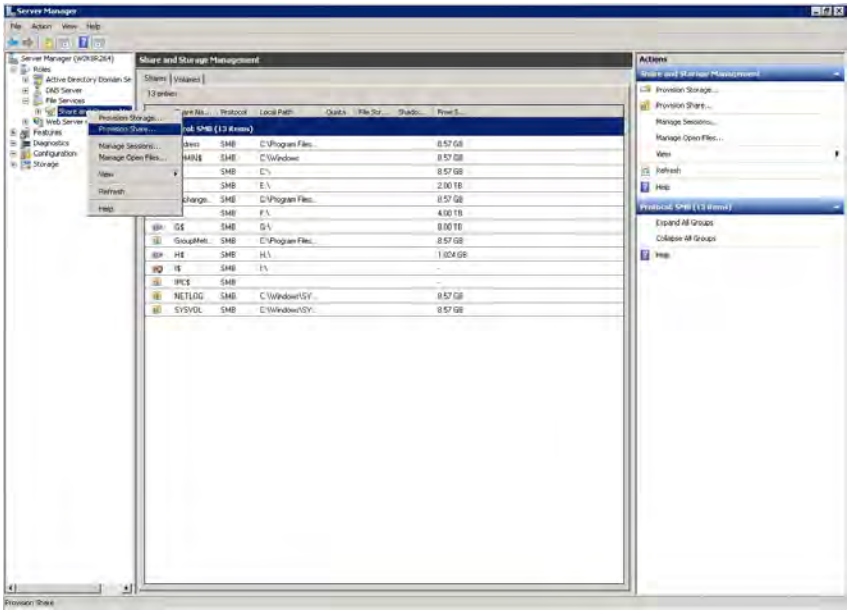
In this section you can see how the operating system sees the Drobo as a raw/block device. You can apply network restrictions/access control lists to the shares based on Active Directory usernames, groups, and so on

The additional unallocated space on volumes larger than 2 TB, in this case 128 MB, is the Microsoft Reserved Partition. Therefore each volume larger than 2 TB will show this unallocated space.

Provisioning Shares Using The Wizard

NOTE: This document focuses on creating a network share using the "Provision a Share Folder Wizard." It does not describe the most basic way to create a directory and share it from within Windows Explorer.

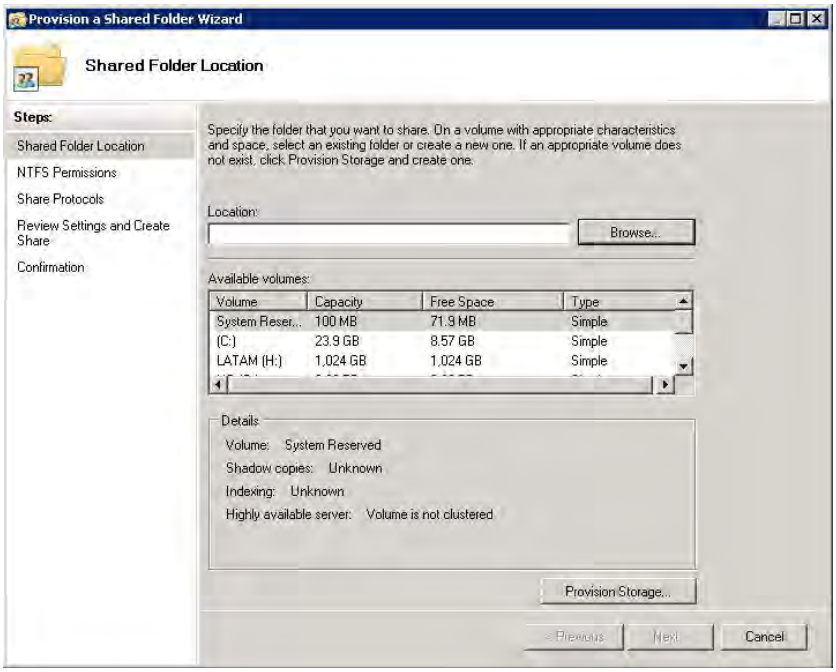
STEP 1



In the left navigation, select **Roles > File Services,** right-click Share and Storage Management, and select **Provision Share**.

Take a quick look at the available options for provisioning storage, which allow IT administrators to create, size, and format a partition. While it is possible to format and partition iSCSI LUNs using this wizard, to create and format LUNs, use Drobo Dashboard instead.

STEP 2

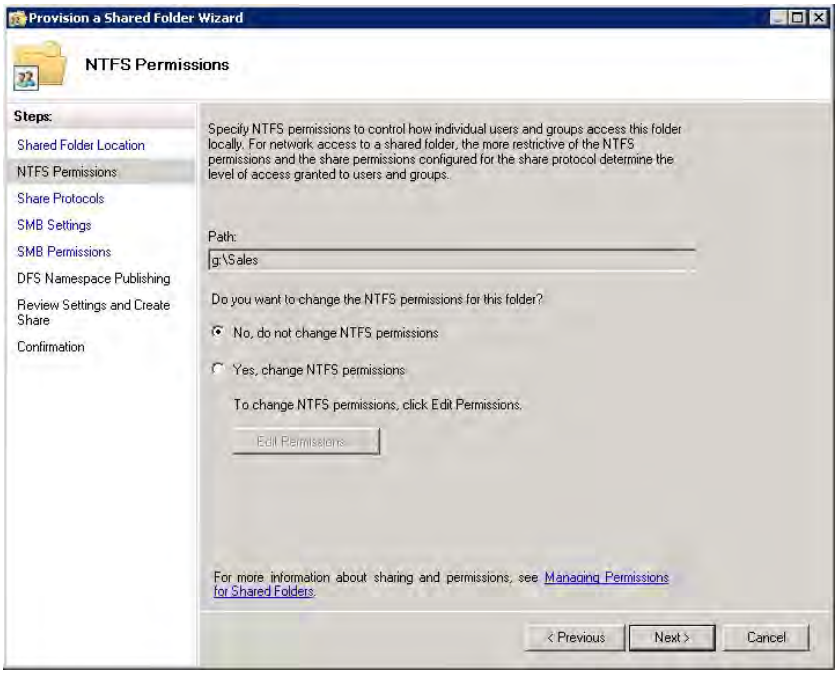


The first screen in the process prompts you to select the destination for the directory to be shared. Click **Browse**.

STEP 3

A window prompts you to select a folder. In this example, select a folder that resides on one of the Drobo volumes.

STEP 4

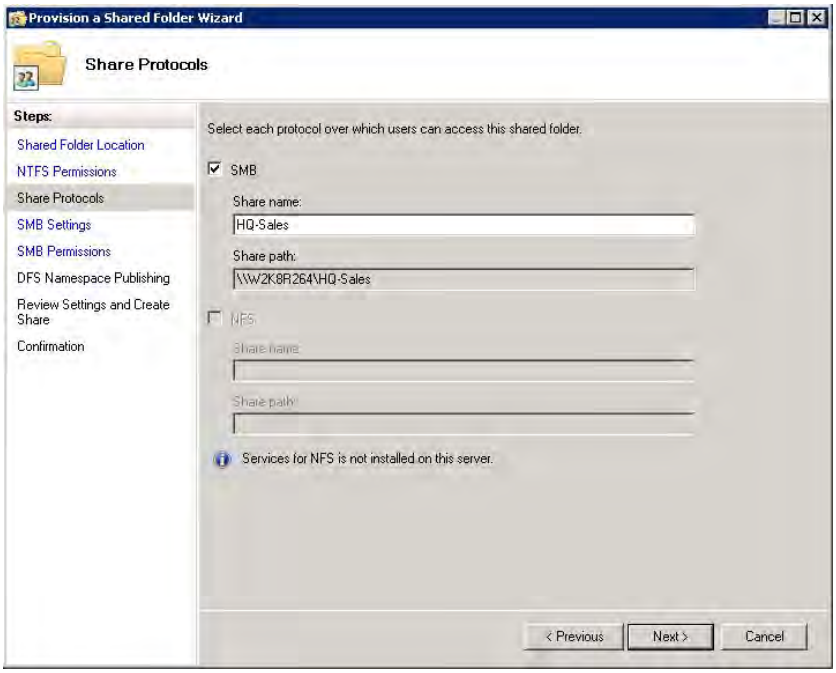


To change NTFS permissions on the share, click one of the radio buttons after the question in the right pane.

In this example, select "No, do not change NTFS permissions" and click **Next**.

NTFS permissions are applied to a directory or file for controlled access whether local or remote. *Share permissions* apply only to access to the folders across the network. In this document, you will see how to set network shares and IT access controls. For more information on key differences between NTFS vs. share-level permissions, refer to: http://technet.microsoft.com/en-us/library/cc754178.aspx.

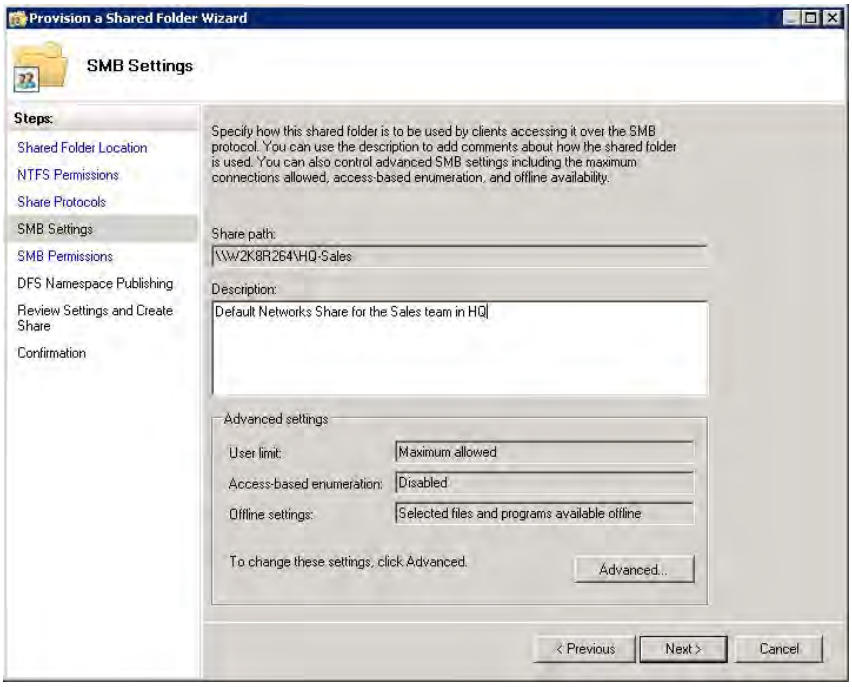
STEP 5



Enter the name of the share that will be exported to the network and the protocol to be used.

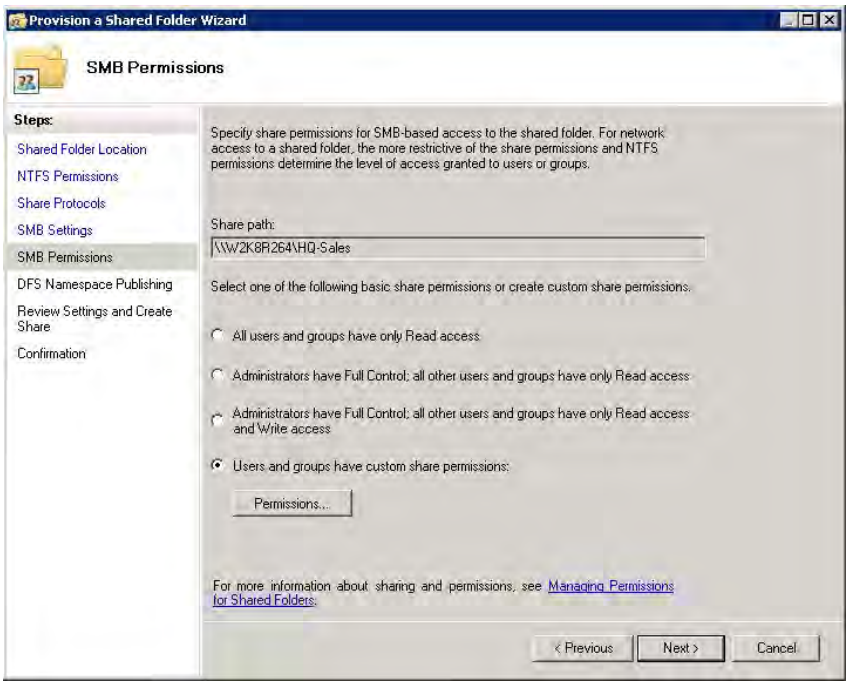
While both protocols can be used to present the share across the network, only SMB is documented in this example.

STEP 6



Enter a description for this share.

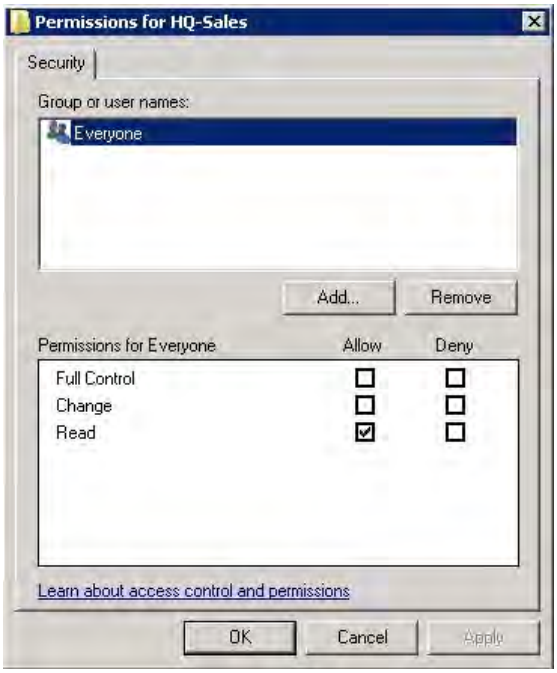
STEP 7



You are now ready to define the users and groups that will have access to the share.

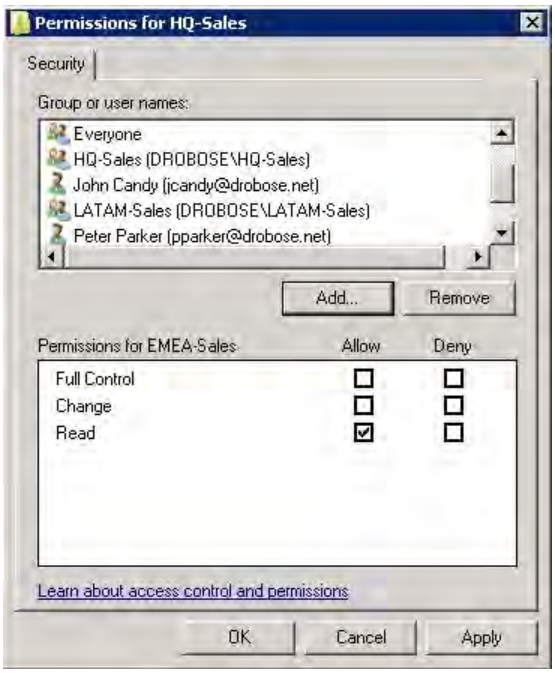
Select "Users and groups have custom share permissions" and click **Permissions**.

STEP 8



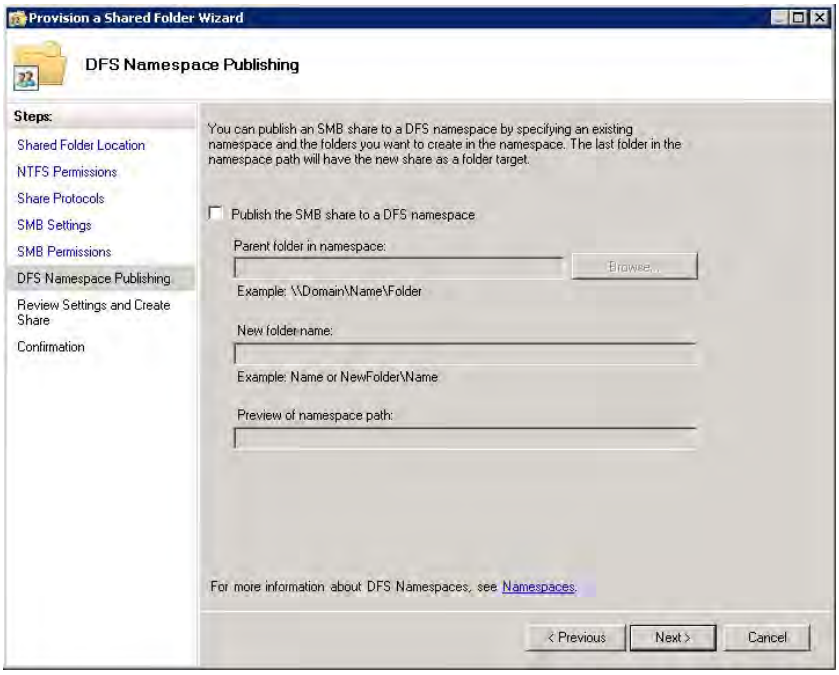
"Read" is the default setting for all users and groups. Click **Add** to specify which users and/or groups you want to have access to this network share.

STEP 9



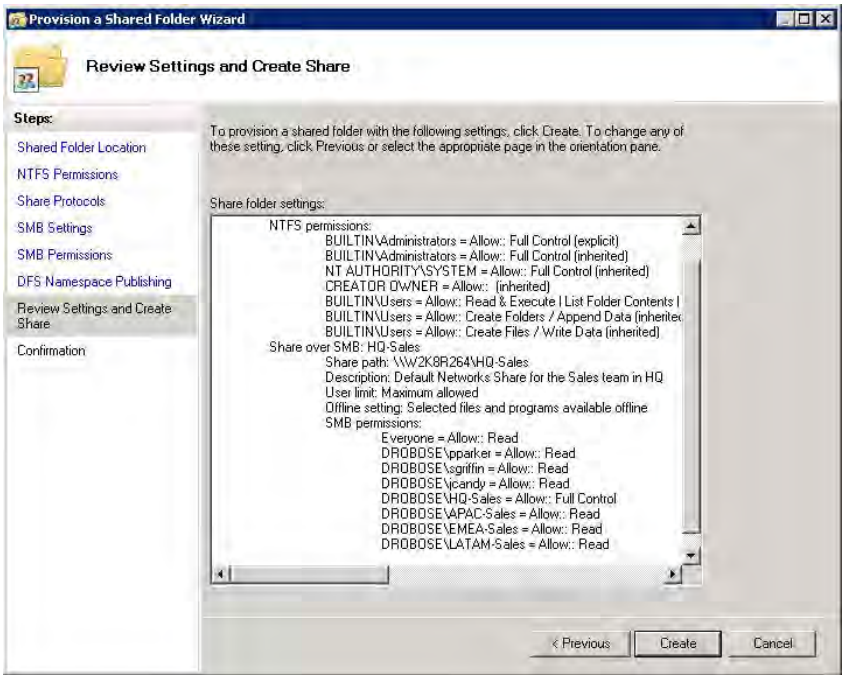
Once the Active Directory users and/or groups have been selected and permissions specified, click **Apply**.

STEP 10



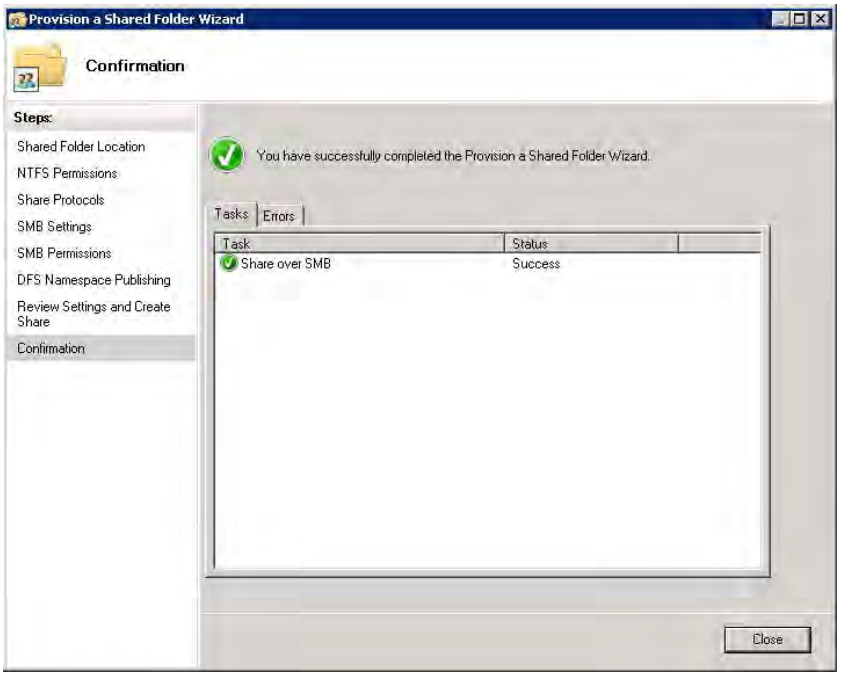
Since in this example, DFS is not covered, click **Next** to continue.

STEP 11



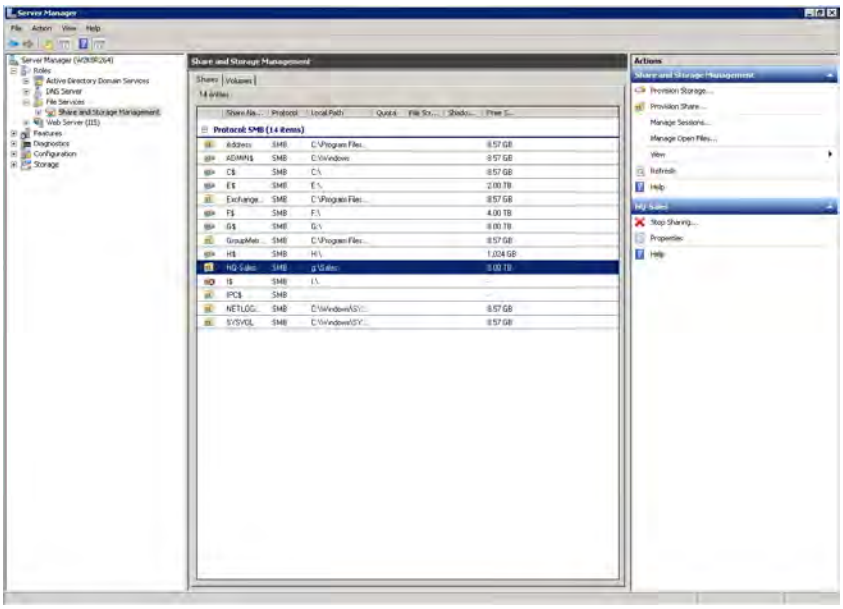
Review the settings to apply to this share and click **Create**.

STEP 12



Once the process is complete, the status changes to Success.

Click **Close** to complete the procedure.



The share that now resides on one of the volumes of the Drobo is created and published as a network share.