Add a CIFS volume to a CIFS-enabled SVM

System Manager Classic

NetApp
April 09, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-sm-classic/smb-config/task_creating_configuring_volume.html on April 09, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Add a CIFS volume to a CIFS-enabled SVM . . . 1
- Create and configure a volume . . . 1
- Create a share and set its permissions . . . 2
- Verify SMB client access . . . 3
- Configure and verify CIFS client access . . . 3

Add a CIFS volume to a CIFS-enabled SVM

Adding a CIFS volume to a CIFS-enabled SVM involves creating and configuring a volume, creating a share and setting its permissions, and verifying access from a Windows administration host. You can then configure CIFS client access.

Before you begin

CIFS must be completely set up on the SVM.

Create and configure a volume

You must create a FlexVol volume to contain your data. You can optionally change the volume's default security style, which is inherited from the security style of the root volume. You can also optionally change the volume's default location in the namespace, which is at the root volume of the storage virtual machine (SVM).

Steps

1. Navigate to the **Volumes** window.
2. Click **Create** > **Create FlexVol**.

   The Create Volume dialog box is displayed.

3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

   Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. You use the junction path and the junction name when configuring CIFS shares.

7. **Optional**: If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:

   a. Navigate to the **Namespace** window.
   b. Select the **SVM** from the drop-down menu.
   c. Click **Mount**.
   d. In the **Mount Volume** dialog box, specify the volume, the name of its junction path, and the junction path on which you want the volume mounted.
   e. Verify the new junction path in the **Namespace** window.

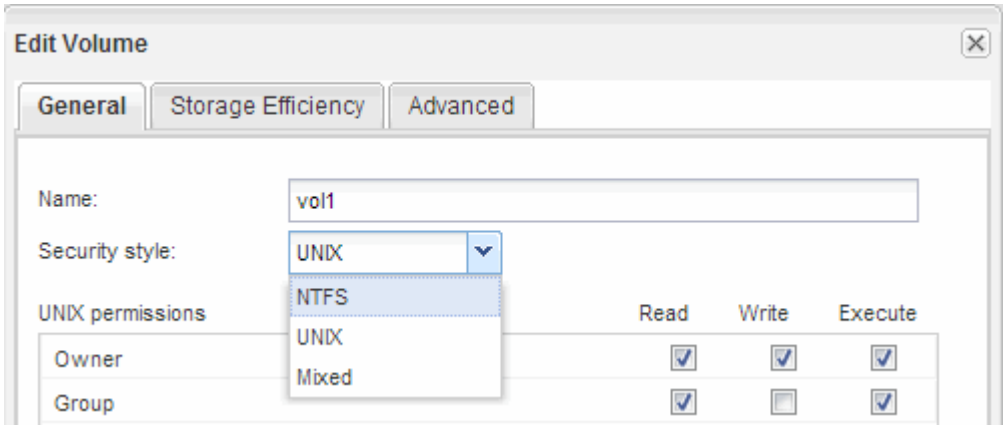
   If you want to organize certain volumes under a main volume named "data", you can move the new volume "vol1" from the root volume to the "data" volume.

8. Review the volume's security style and change it, if necessary:

   a. In the **Volume** window, select the volume you just created, and click **Edit**.

The Edit Volume dialog box is displayed, showing the volume's current security style, which is inherited from the security style of the SVM root volume.

b. Make sure the security style is NTFS.



Create a share and set its permissions

Before Windows users can access a volume, you must create a CIFS share on the volume and restrict access to the share by modifying the access control list (ACL) for the share.

About this task

For testing purposes, you should permit access only to administrators. Later, after you have verified that the volume is accessible, you can permit access to more clients.

Steps

1. Navigate to the **Shares** window.
2. Create a share so that SMB clients can access the volume:

   a. Click **Create Share**.

   b. In the **Create Share** dialog box, click **Browse**, expand the namespace hierarchy, and then select the volume that you created earlier.

   c. **Optional**: If you want the share name to be different from the volume name, change the share name.

   d. Click **Create**.

   The share is created with a default ACL set to Full Control for the Everyone group.

3. **Optional**: Restrict access to the share by modifying the share ACL:

   a. Select the share, and then click **Edit**.

   b. In the **Permissions** tab, select the **Everyone** group, and then click **Remove**.

   c. Click **Add**, and then enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.

   d. With the new administrator group selected, select all permissions for it.

   e. Click **Save and Close**.

   The updated share access permissions are listed in the Share Access Control pane.

What to do next

You should verify access as a Windows administrator.

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

   b. On the newly created drive, create a test file, and then delete the file.

   You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Configure and verify CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
   a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
   b. In Windows Explorer, right-click the drive, and then select **Properties**.
   c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the **Shares** window.
   b. Select the share, and click **Edit**.
   c. Select the **Permissions** tab, and give the users or groups access to the share.

4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.