



# **Enable NAS storage**

## **ONTAP 9**

NetApp  
June 04, 2024

# Table of Contents

- Enable NAS storage. . . . . 1
  - Enable NAS storage for Linux servers using NFS . . . . . 1
  - Enable NAS storage for Windows servers using SMB. . . . . 2
  - Enable NAS storage for both Windows and Linux using both NFS and SMB . . . . . 3

# Enable NAS storage

## Enable NAS storage for Linux servers using NFS

Create or modify storage VMs to enable NFS servers for serving data to Linux clients.





Enable a new or existing storage VM for the NFS protocol using this procedure.



### Before you begin

Ensure that you have noted the configuration details for any networking, authentication, or security services required in your environment.

### Steps

1. Enable NFS on a storage VM.
  - For new storage VMs: Click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable NFS**.
    - i. Confirm the default language.
    - ii. Add network interfaces.
    - iii. Update storage VM administrator account information (optional).
  - For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = 0.0.0.0/0
    - Access protocols = NFS
    - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
4. Configure name services as required.
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click for  LDAP or NIS.
  - b. Click  in the Name Services Switch tile to include any changes.
5. Configure encryption if required:

### Configure TLS for NFS clients



NFS over TLS is available in ONTAP 9.15.1 as a public preview. As a preview offering, NFS over TLS is not supported for production workloads in ONTAP 9.15.1.

#### Steps

- a. Refer to the [requirements](#) for NFS over TLS before you begin.
- b. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- c. In the **NFS** tile, click **NFS over TLS settings**.
- d. In the **NFS over TLS settings** area, select an NFS network interface for which you want to enable TLS.
- e. Click the for that interface.
- f. Click **Enable**.
- g. In the **Network interface TLS configuration** dialog, include a certificate for use with TLS by selecting one of the following options:
  - **Installed certificate**: Choose a previously installed certificate from the drop-down list.
  - **New certificate**: Choose a common name for the certificate.
  - **External CA-signed certificate**: Follow the instructions to paste the contents of your certificate and private key into the boxes.
- h. Click **Save**.

### Configure Kerberos

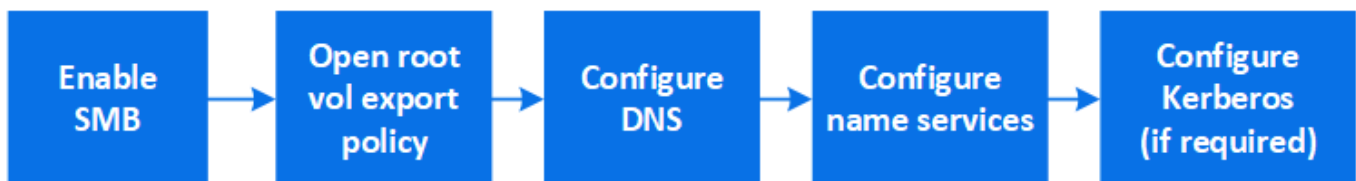
#### Steps

- a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- b. Click in the Kerberos tile and then click **Add**.

## Enable NAS storage for Windows servers using SMB






Create or modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables a new or existing storage VM for the SMB protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



#### Steps

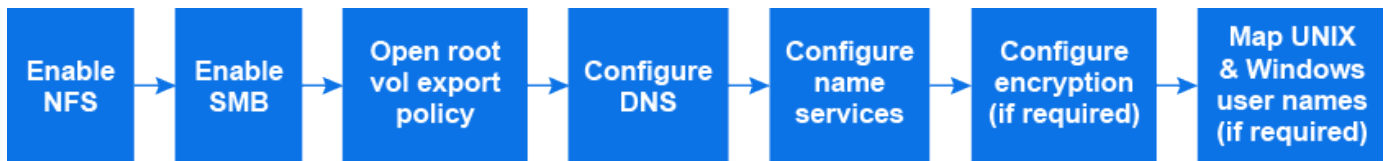
1. Enable SMB on a storage VM.
  - a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS**.
    - Enter the following information:

- Administrator name and password
  - Server name
  - Active directory domain
  - Confirm the Organizational Unit.
  - Confirm the DNS values.
  - Confirm the default language.
  - Add network interfaces.
  - Update storage VM administrator account information (optional).
- b. For existing storage VMs:: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **SMB**.
2. Open the export policy of the storage VM root volume:
- a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
- b. Click **Add** to add a rule.
- Client specification = 0 . 0 . 0 . 0 / 0
  - Access protocols = SMB
  - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
- a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
- b. Switch to the DNS server and map the SMB server.
- Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
  - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required
- a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **LDAP** or **NIS**.
- b. Include any changes in the name services switch file: click  under **Name Services Switch**.
5. Configure Kerberos if required:
- a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- b. Click  under **Kerberos** and then click **Add**.

## Enable NAS storage for both Windows and Linux using both NFS and SMB

Create or modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.




Enable a new or existing storage VM to serve both NFS and SMB protocols using this procedure.





### Before you begin

Ensure that you have noted the configuration details for any networking, authentication, or security services required in your environment.

### Steps

1. Enable NFS and SMB on a storage VM.
  - a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS** and **Enable NFS**.
  - b. Enter the following information:
    - Administrator name and password
    - Server name
    - Active directory domain
  - c. Confirm the Organizational Unit.
  - d. Confirm the DNS values.
  - e. Confirm the default language.
  - f. Add network interfaces.
  - g. Update storage VM administrator account information (optional).
  - h. For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, and then click **Settings**. Complete the following sub-steps if NFS or SMB is not already enabled.
    - Click  under **NFS**.
    - Click  under **SMB**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = 0.0.0.0/0
    - Access protocols = NFS
    - Access details = NFS Read-Only
3. Configure DNS for host-name resolution:
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required:


- a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  for LDAP or NIS.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
5. Configure authentication and encryption if required:

#### Configure TLS for NFS clients




NFS over TLS is available in ONTAP 9.15.1 as a public preview. As a preview offering, NFS over TLS is not supported for production workloads in ONTAP 9.15.1.


#### Steps

- a. Refer to the [requirements](#) for NFS over TLS before you begin.
- b. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- c. In the **NFS** tile, click **NFS over TLS settings**.
- d. In the **NFS over TLS settings** area, select an NFS network interface for which you want to enable TLS.
- e. Click the  for that interface.
- f. Click **Enable**.
- g. In the **Network interface TLS configuration** dialog, include a certificate for use with TLS by selecting one of the following options:
  - **Installed certificate**: Choose a previously installed certificate from the drop-down list.
  - **New certificate**: Choose a common name for the certificate.
  - **External CA-signed certificate**: Follow the instructions to paste the contents of your certificate and private key into the boxes.
- h. Click **Save**.

#### Configure Kerberos

##### Steps

- a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- b. Click  in the Kerberos tile and then click **Add**.

6. Map UNIX and Windows user names if required: click  under **Name Mapping** and then click **Add**.

You should do this only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. You can map user names using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

## 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.