Decide where to provision the new volume

System Manager Classic

NetApp
June 22, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-system-manager-classic/nas-multiprotocol-config/task_creating_new_svm.html on June 22, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Decide where to provision the new volume . . . 1
Procedure . . . 1
Create a basic SVM . . . 1
Add CIFS and NFS access to an existing SVM . . . 5
Open the export policy of the SVM root volume (Create a new NFS-enabled SVM) . . . 7
Map the SMB server on the DNS server . . . 8
Configure LDAP (Create a new NFS-enabled SVM) . . . 9
Map UNIX and Windows user names . . . 11

Decide where to provision the new volume

Before you create a new multiprotocol volume, you must decide whether to place the volume in an existing storage virtual machine (SVM), and, if so, how much configuration the SVM requires. This decision determines your workflow.

Procedure

- If you want to provision a volume on a new SVM, create a basic SVM.

  Creating a basic SVM

  You must choose this option if CIFS and NFS are not already enabled on an existing SVM.

- If you want to provision a volume on an existing SVM that has both CIFS and NFS enabled but not configured, add CIFS and NFS access on the existing SVM.

  Adding CIFS and NFS access on an existing SVM

- If you want to provision a volume on an existing SVM that is fully configured for CIFS and NFS multiprotocol access, you can directly create and configure the volume.

  Creating and configuring a volume

Create a basic SVM

You can use a wizard that guides you through the process of creating a new storage virtual machine (SVM), configuring Domain Name System (DNS), creating a data logical interface (LIF), configuring a CIFS server, enabling NFS, and optionally configuring NIS.

Before you begin

- Your network must be configured and the relevant physical ports must be connected to the network.
- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
  - NIS information, if your site uses NIS for name services or name mapping
- The subnet must be routable to all external servers required for services such as Network Information Service (NIS), Lightweight Directory Access Protocol (LDAP), Active Directory (AD), and DNS.
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized to within five minutes of each other.

About this task

When you are creating an SVM for multiprotocol access, you should not use the provisioning sections of the

Storage Virtual Machine (SVM) Setup window, which creates two volumes—not a single volume with multiprotocol access. You can provision the volume later in the workflow.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create.**
3. In the **Storage Virtual Machine (SVM) Setup** dialog box, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.

   c. Keep the default language setting, C.UTF-8.

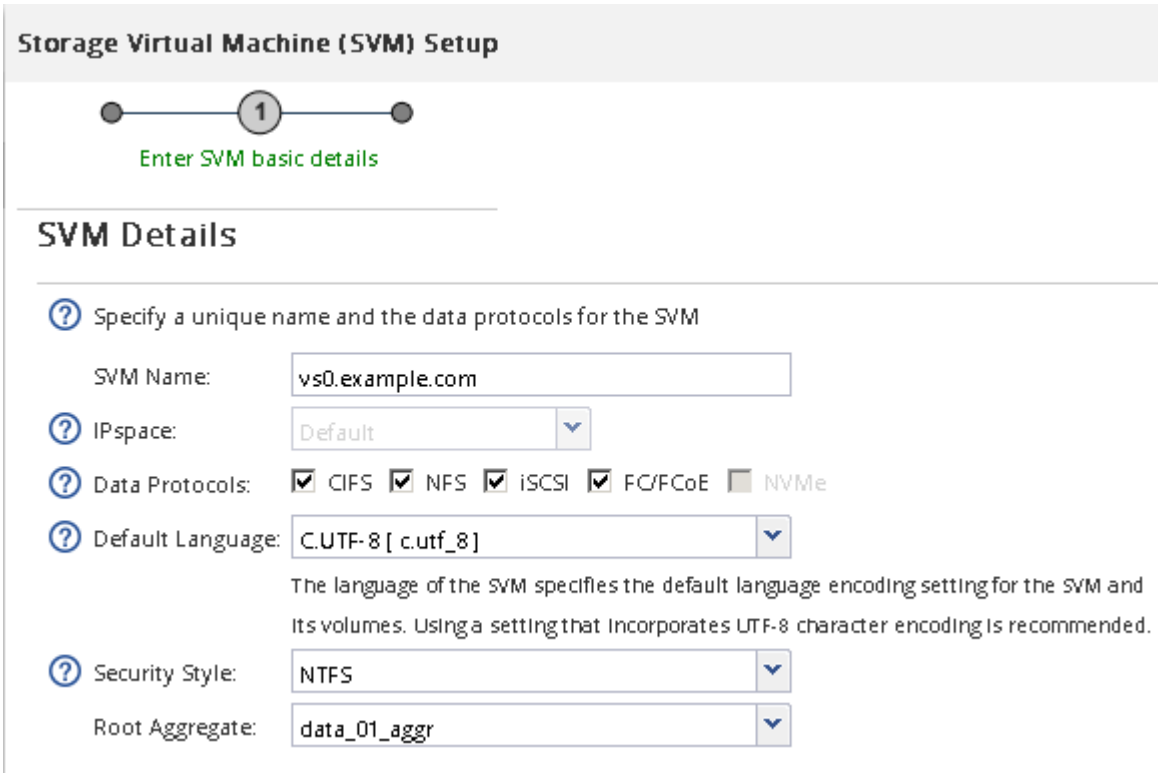
      If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

   d. **Optional**: Make sure that the security style is set to your preference.

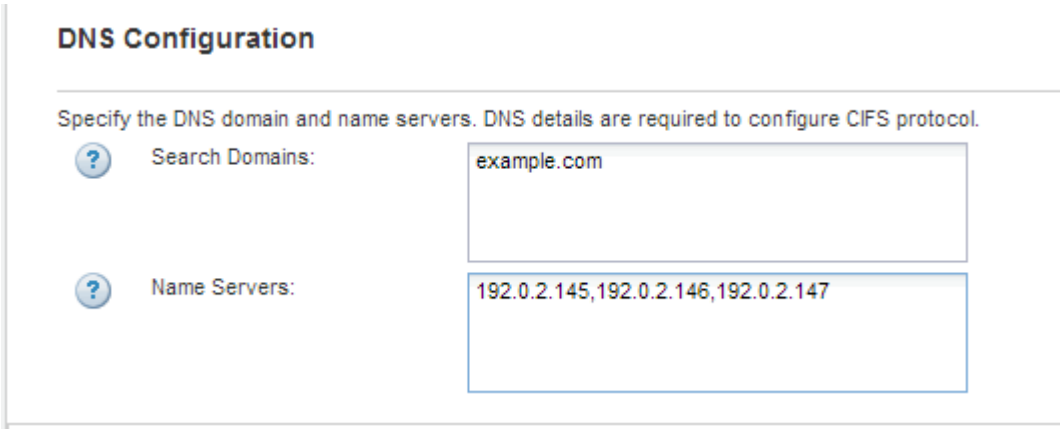
      Selecting the CIFS protocol sets the security style to NTFS by default.

   e. **Optional**: Select the root aggregate to contain the SVM root volume.

      The aggregate that you select for the root volume does not determine the location of the data volume. The aggregate for the data volume is selected separately in a later step.



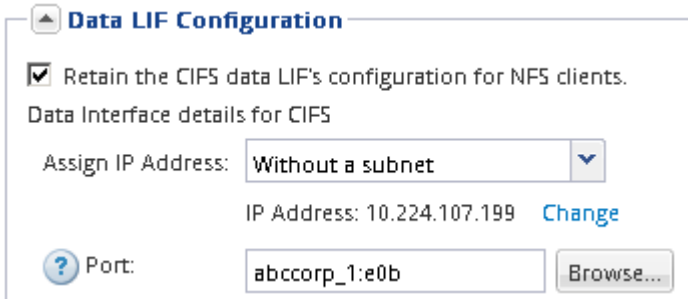
f. **Optional**: In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



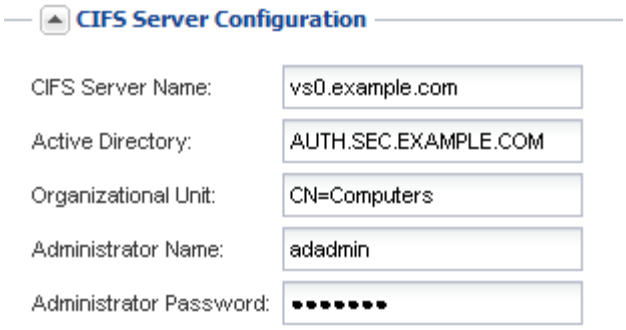
g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

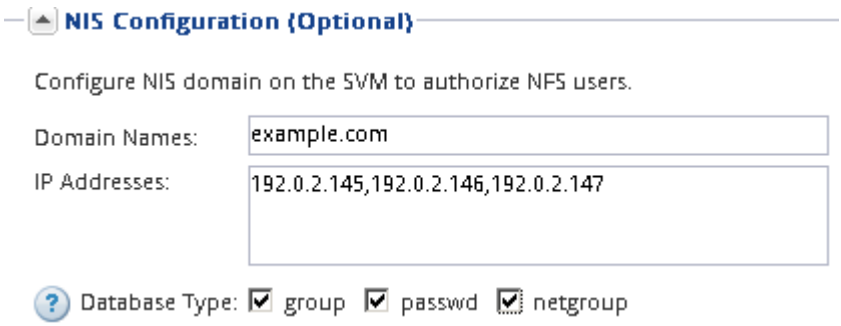
4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



5. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:
   a. Specify a name for the CIFS server that is unique in the AD domain.
   b. Specify the FQDN of the AD domain that the CIFS server can join.
   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.
   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.
   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.



6. Skip the **Provision a volume for CIFS Storage** area because it provisions a volume for only CIFS access—not for multiprotocol access.
7. If the **NIS Configuration** area is collapsed, expand it.
8. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers.



9. Skip the **Provision a volume for NFS Storage** area because it provisions a volume for NFS access only—not for multiprotocol access.
10. Click **Submit & Continue**.

    The following objects are created:

    - A data LIF named after the SVM with the suffix "_cifs_nfs_lif1"
    - A CIFS server that is part of the AD domain
    - An NFS server
11. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
12. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
    - Click **Skip** and configure an administrator later if required.
    - Enter the requested information and then click **Submit & Continue**.
13. Review the **Summary** page, record any information you might require later and then click **OK**.

    The DNS administrator needs to know the CIFS server name and the IP address of the data LIF. Windows clients need to know the name of the CIFS server. NFS clients need to know the IP address of the data LIF.

Results

A new SVM is created that has a CIFS server and an NFS server accessible through the same data LIF.

What to do next

You must now open the export policy of the SVM root volume.

Related information

Opening the export policy of the SVM root volume (Creating a new NFS-enabled SVM)

Add CIFS and NFS access to an existing SVM

Adding both CIFS/SMB and NFS access to an existing SVM involves creating a data LIF, configuring a CIFS server, enabling NFS, and optionally configuring NIS.

Before you begin

- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - The Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
  - NIS information if your site uses NIS for name services or name mapping
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized within five minutes of each other.
- The CIFS and NFS protocols must be allowed on the SVM.

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

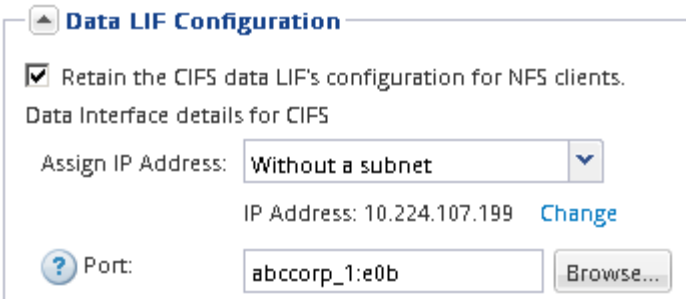
About this task

The order in which you configure CIFS and NFS affects the dialog boxes that are displayed. In this procedure, you must configure CIFS first and NFS second.

Steps

1. Navigate to the area where you can configure the protocols of the SVM:
   a. Select the SVM that you want to configure.
   b. In the **Details** pane, next to **Protocols**, click **CIFS**.

2. In the **Data LIF Configuration** section of the **Configure CIFS protocol** dialog box, create a data LIF for the SVM:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



3. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:

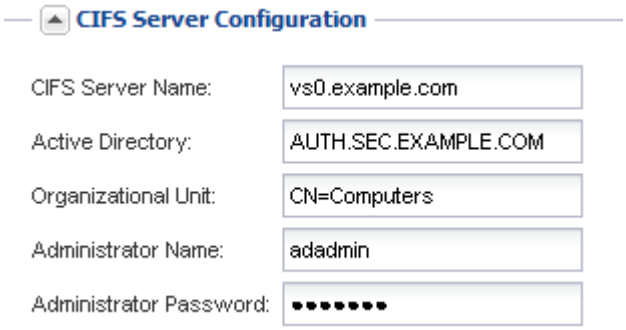
   a. Specify a name for the CIFS server that is unique in the AD domain.

   b. Specify the FQDN of the AD domain that the CIFS server can join.

   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.

   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.

   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.

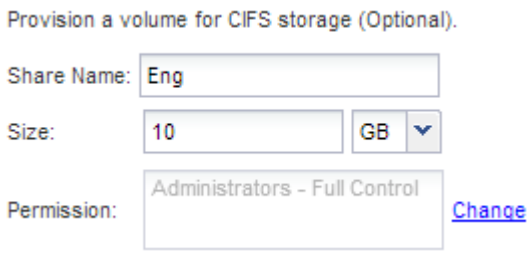


4. Create a volume for CIFS/SMB access and provision a share on it:

   a. Name the share that CIFS/SMB clients will use to access the volume.

      The name you enter for the share will also be used as the volume name.

   b. Specify a size for the volume.

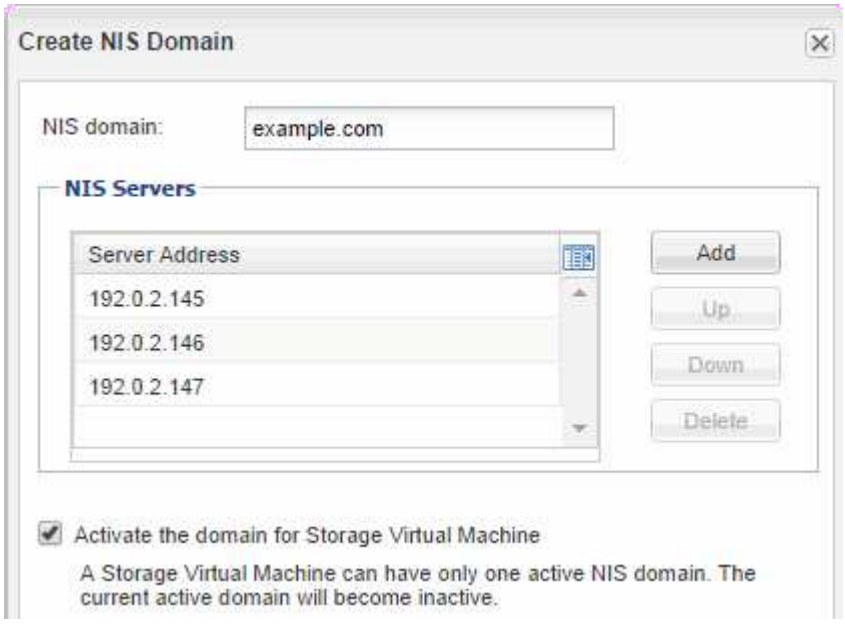


   You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

5. Skip the **Provision a volume for CIFS Storage** area, because it provisions a volume for only CIFS

access—not for multiprotocol access.

6. Click **Submit & Close**, and then click **OK**.
7. Enable NFS:
   a. From the SVMs tab, select the SVM for which you want to enable NFS and click **Manage**.
   b. In the **Protocols** pane, click **NFS** and then click **Enable**.
8. If your site uses NIS for name services or name mapping, configure NIS:
   a. In the **Services** window, click **NIS**.
   b. In the **NIS** window, click **Create**.
   c. Specify the domain of the NIS servers.
   d. Add the IP addresses of the NIS servers.
   e. Select **Activate the domain for Storage Virtual Machine**, and then click **Create**.



What to do next

Open the export policy of the SVM root volume.

Open the export policy of the SVM root volume (Create a new NFS-enabled SVM)

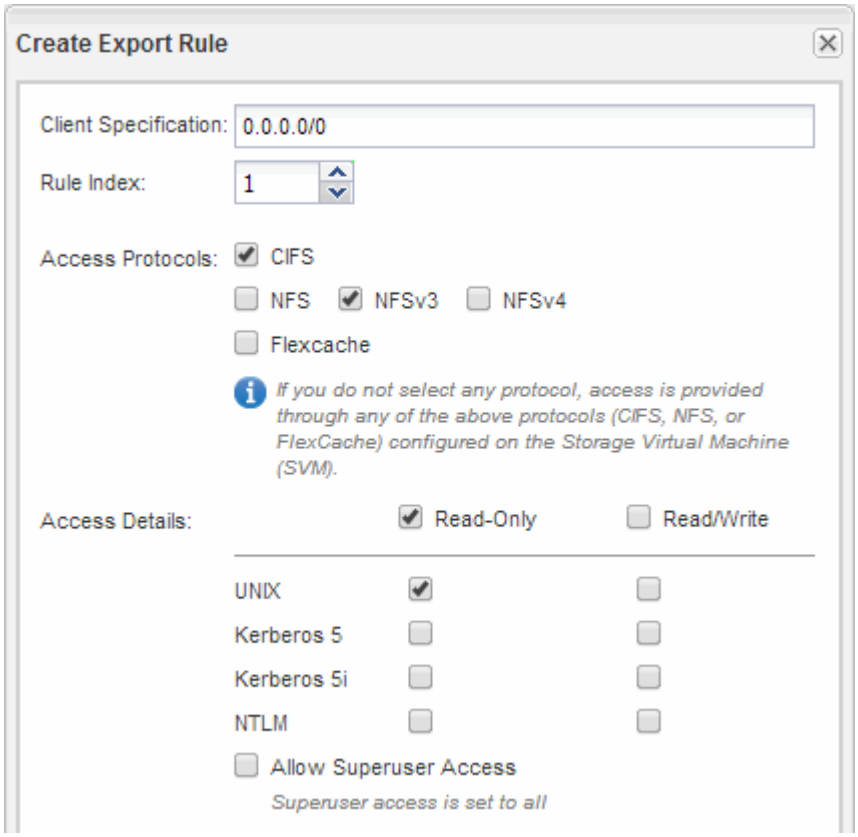
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

About this task

You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy named **default**, which is applied to the SVM root volume.
5. In the lower pane, click **Add**.
6. In the **Create Export Rule** dialog box, create a rule that opens access to all clients for NFS clients:
   a. In the **Client Specification** field, enter `0.0.0.0/0` so that the rule applies to all clients.
   b. Retain the default value as **1** for the rule index.
   c. Select **NFSv3**.
   d. Clear all the check boxes except the **UNIX** check box under **Read-Only**.
   e. Click **OK**.



Results

NFSv3 clients can now access any volumes created on the SVM.

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. 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 LIF.
3. 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 LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Configure LDAP (Create a new NFS-enabled SVM)

If you want the storage virtual machine (SVM) to get user information from Active Directory-based Lightweight Directory Access Protocol (LDAP), you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

- The LDAP configuration must be using Active Directory (AD).

  If you use another type of LDAP, you must use the command-line interface (CLI) and other documentation to configure LDAP.

  NetApp Technical Report 4067: NFS in NetApp ONTAP

  NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory

  NetApp Technical Report 4835: How to Configure LDAP in ONTAP

- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:

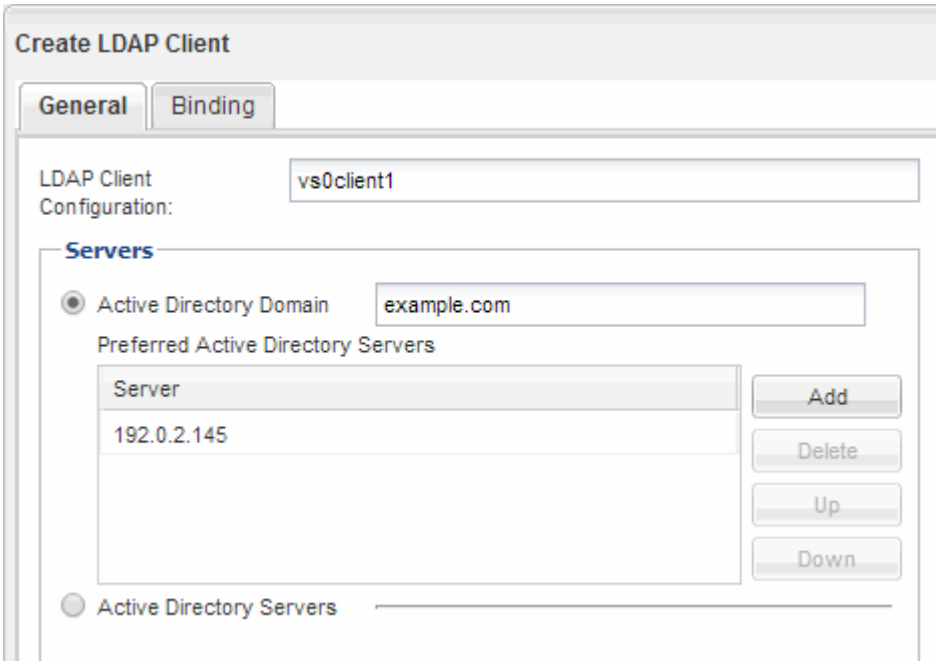
   a. In the **Services** pane, click **LDAP Client**.

   b. In the **LDAP Client Configuration** window, click **Add**.

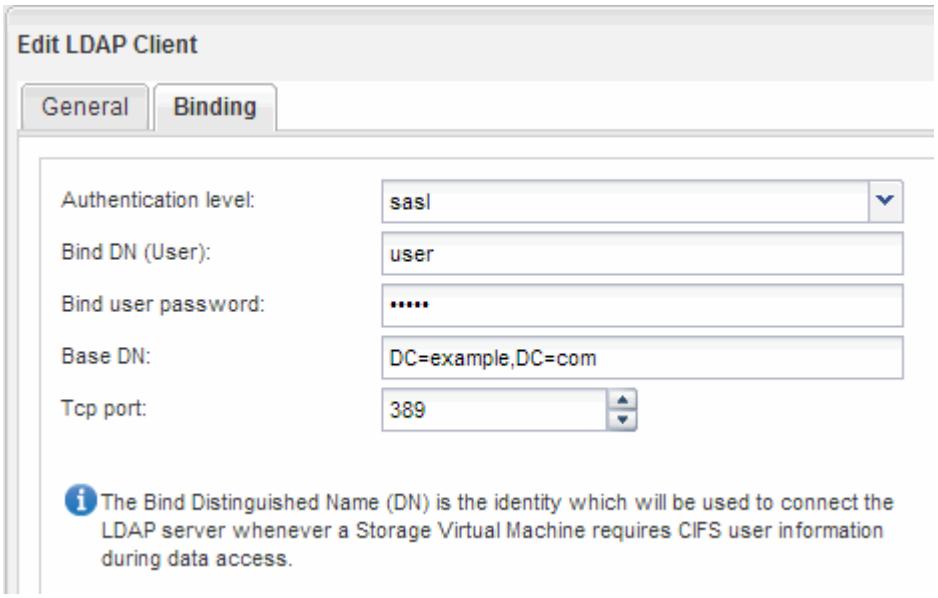
   c. In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration,

such as `vs0client1`.

d. Add either the AD domain or the AD servers.



e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.



f. Click **Save and Close**.

A new client is created and available for the SVM to use.

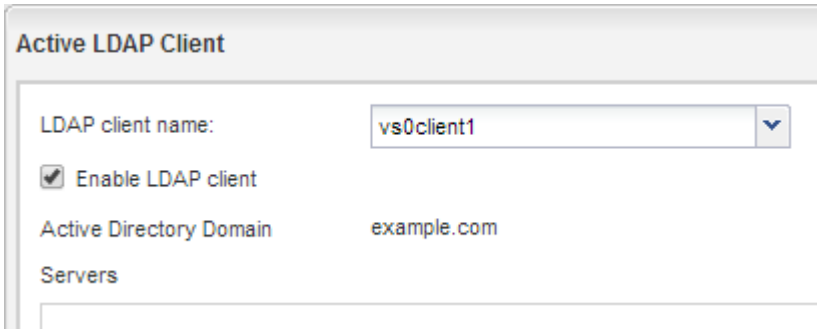
5. Enable the new LDAP client for the SVM:

a. In the navigation pane, click **LDAP Configuration**.

b. Click **Edit**.

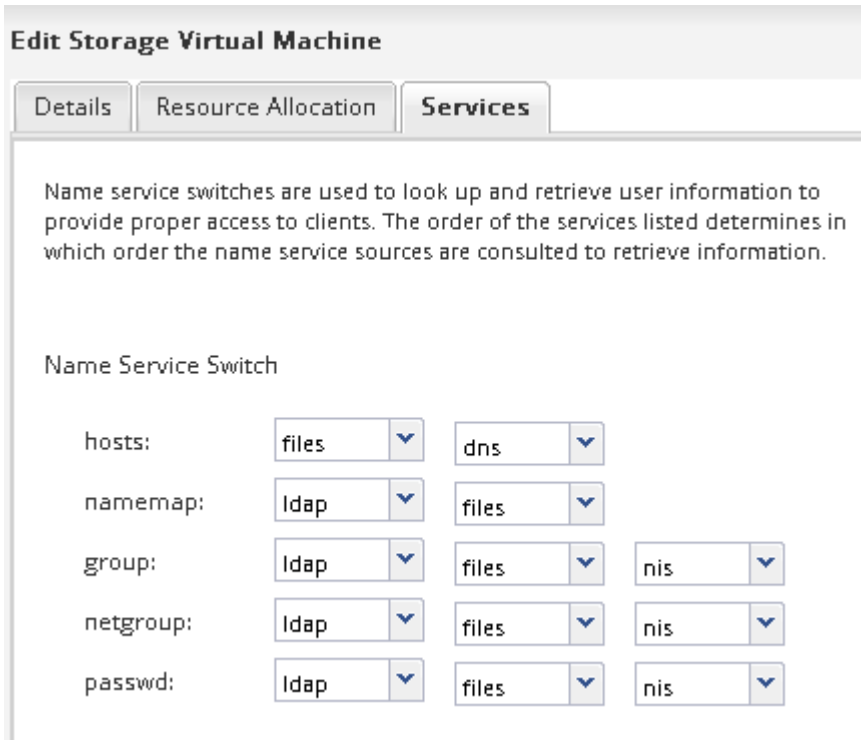
c. Ensure that the client you just created is selected in **LDAP client name**.

d. Select **Enable LDAP client**, and click **OK**.



The SVM uses the new LDAP client.

6. Give LDAP priority over other sources of user information, such as Network Information Service (NIS) and local users and groups:
   a. Navigate to the **SVMs** window.
   b. Select the SVM and click **Edit**.
   c. Click the **Services** tab.
   d. Under **Name Service Switch**, specify **LDAP** as the preferred name service switch source for the database types.
   e. Click **Save and Close**.



LDAP is the primary source of user information for name services and name mapping on this SVM.

Map UNIX and Windows user names

If your site has both Windows and UNIX user accounts, you should use name mapping to

ensure that Windows users can access files with UNIX file permissions and to ensure that UNIX users can access files with NTFS file permissions. Name mapping can involve any combination of implicit mapping, conversion rules, and default users.

About this task

You should use this procedure 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. This can be done using NIS, LDAP, or local users. If you have two sets of users that do not match, you should configure name mapping.

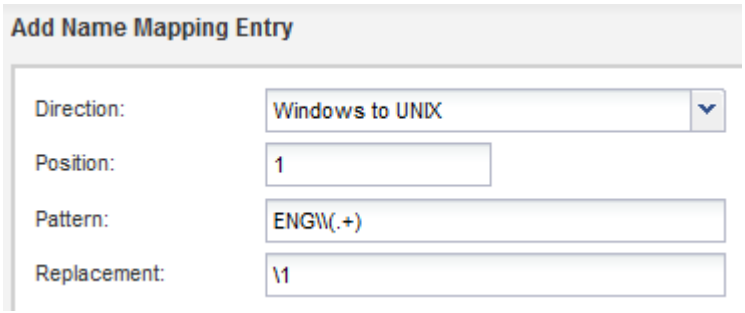
Steps

1. Decide on a method of name mapping—name mapping conversion rules, default user mappings, or both—by considering the following factors:
   - Conversion rules use regular expressions to convert one user name to another, which is useful if you want to control or track access at an individual level.

     For example, you can map UNIX users to Windows users in a domain, and vice versa.
   - Default users enable you to assign a user name to all users who are not mapped by implicit mappings or name mapping conversion rules.

     Each SVM has a default UNIX user named “pcuser” but does not have a default Windows user.
2. Navigate to the **SVMs** window.
3. Select the SVM that you want to configure.
4. Click the **SVM Settings** tab.
5. **Optional**: Create a name mapping that converts UNIX user accounts to Windows user accounts, and vice versa:
   a. In the **Host Users and Groups** pane, click **Name Mapping**.
   b. Click **Add**, retain the default **Windows to UNIX** direction, and then create a regular expression that produces a UNIX credential when a Windows user tries to access a file that uses UNIX file permissions.

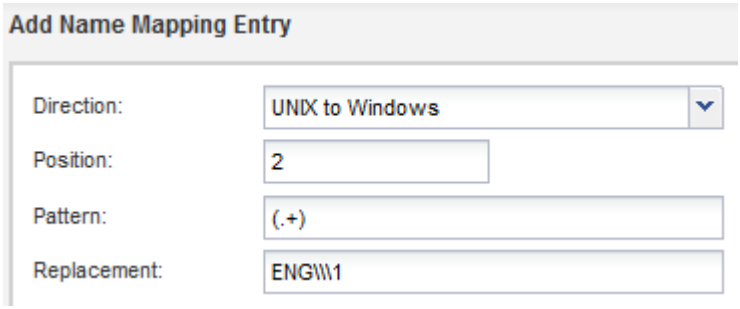
      Use the following entry to convert any Windows user in the ENG domain into a UNIX user of the same name. The pattern `ENG\\(.+)` finds any Windows user name with the prefix `ENG\\`, and the replacement `\1` creates the UNIX version by removing everything except the user name.

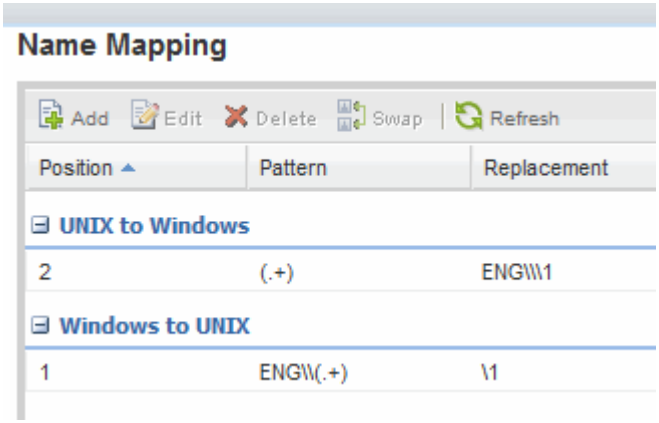
   c. Click**Add**, select the **UNIX to Windows** direction, and then create the corresponding mapping that produces a Windows credential when a UNIX user tries to access a file that has NTFS file permissions.

      Use the following entry to convert every UNIX user into a Windows user of the same name in the ENG

domain. The pattern `(.+)` finds any UNIX name, and the replacement `ENG\\\1` creates the Windows version by inserting `ENG\\` before the user name.



d. Because the position of each rule determines the order in which the rules are applied, you should review the result and confirm that the order matches your expectations.



e. Repeat steps 5b to 5d to map all of the domains and names on the SVM.

6. **Optional**: Create a default Windows user:

   a. Create a Windows user account in LDAP, NIS, or the local users of the SVM.

      If you use local users, you can create an account under **Windows** in the Host Users and Groups pane.

   b. Set the default Windows user by selecting **NFS** > **Edit** in the **Protocols** pane, and entering the user name.

   You can create a local Windows user named “unixusers” and set it as the default Windows user.

7. **Optional**: Configure the default UNIX user if you want a user different from the default value, which is the “pcuser” user.

   a. Create a UNIX user account in LDAP, NIS, or the local users of the SVM.

      If you use local users, you can create an account under **UNIX** in the Host Users and Groups pane.

   b. Set the default UNIX user by selecting **CIFS** > **Options** in the **Protocols** pane, and entering the user name.

   You can create a local UNIX user named “winusers” and set it as the default UNIX user.

What to do next

If you configured default users, when you configure file permissions later in the workflow, you should set permissions for the default Windows user and the default UNIX user.

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.