



Set up an SMB server in an Active Directory domain

ONTAP 9

NetApp
July 21, 2023

Table of Contents

- Set up an SMB server in an Active Directory domain 1
 - Configure time services 1
 - Commands for managing symmetric authentication on NTP servers 1
- Create an SMB server in an Active Directory domain 2
- Create keytab files for SMB authentication 5

Set up an SMB server in an Active Directory domain

Configure time services

Before creating an SMB server in an Active Domain controller, you must ensure that the cluster time and the time on the domain controllers of the domain to which the SMB server will belong matches to within five minutes.

About this task

You should configure cluster NTP services to use the same NTP servers for time synchronization that the Active Directory domain uses.

Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

Steps

1. Configure time services by using the `cluster time-service ntp server create` command.
 - To configure time services without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_ip_address`
 - To configure time services with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this...	Use this command...
Configure an NTP server without symmetric authentication	<code>cluster time-service ntp server create -server server_name</code>

To do this...	Use this command...
Configure an NTP server with symmetric authentication	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configure a shared NTP key	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</p> </div>
Configure an NTP server with an unknown key ID	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
Configure a server with a key ID not configured on the NTP server.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</p> </div>
Disable symmetric authentication	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Create an SMB server in an Active Directory domain

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the Active Directory (AD) domain to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM and to an AD domain controller of the domain to which you want to join the SMB server.

Any user who is authorized to create machine accounts in the AD domain to which you are joining the SMB server can create the SMB server on the SVM. This can include users from other domains.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

About this task

When creating an SMB server in an Activity Directory domain:

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default setting is to add the SMB server machine account to the Active Directory CN=Computer object.
- You can choose to add the SMB server to a different organizational unit (OU) by using the `-ou` option.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the SMB server.

Configuring NetBIOS aliases for an SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original servers' names.

The `vserver cifs` man pages contain additional optional parameters and naming requirements.



Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller (DC). Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default.

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted. ONTAP requires encryption for domain controller communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3. .

[SMB management](#) contains more information about SMB server configuration options.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

If it is not, contact your sales representative.

A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in an AD domain: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

When joining a domain, this command might take several minutes to finish.

The following command creates the SMB server “smb_server01” in the domain “example.com”:

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

The following command creates the SMB server “smb_server02” in the domain “mydomain.com” and authenticates the ONTAP administrator with a keytab file:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

In this example, the command output shows that an SMB server named “SMB_SERVER01” was created on SVM vs1.example.com, and was joined to the “example.com” domain.

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. If desired, enable encrypted communication with the domain controller (ONTAP 9.8 and later): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Examples

The following command creates a SMB server named “smb_server02” on SVM vs2.example.com in the “example.com” domain. The machine account is created in the “OU=eng,OU=corp,DC=example,DC=com” container. The SMB server is assigned a NetBIOS alias.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

The following command enables a user from a different domain, in this case an administrator of a trusted domain, to create a SMB server named “smb_server03” on SVM vs3.example.com. The `-domain` option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the SMB server. The `username` option specifies the administrator of the trusted domain.

- Home domain: example.com
- Trusted domain: trust.lab.com
- Username for the trusted domain: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com  
Password: . . .
```

Create keytab files for SMB authentication

Beginning with ONTAP 9.7, ONTAP supports SVM authentication with Active Directory (AD) servers using keytab files. AD administrators generate a keytab file and make it available to ONTAP administrators as a uniform resource identifier (URI), which is supplied when `vserver cifs` commands require Kerberos authentication with the AD domain.

AD administrators can create the keytab files using the standard Windows Server `ktpass` command. The command should be run on the primary domain where authentication is required. The `ktpass` command can be used to generate keytab files only for primary domain users; keys generated using trusted-domain users are not supported.

Keytab files are generated for specific ONTAP admin users. As long as the admin user’s password does not change, the keys generated for the specific encryption type and domain will not change. Therefore, a new keytab file is required whenever the admin user’s password is changed.

The following encryption types are supported:

- AES256-SHA1
- DES-CBC-MD5



ONTAP does not support DES-CBC-CRC encryption type.

- RC4-HMAC

AES256 is the highest encryption type and should be used if enabled on the ONTAP system.

Keytab files can be generated by specifying either the admin password or by using a randomly-generated password. However, at any given time only one password option can be used, because a private key specific to the admin user is needed at the AD server for decrypting the keys inside the keytab file. Any change in the private key for a specific admin will invalidate the keytab file.

Copyright information

Copyright © 2023 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.