Configure LDAP or NIS server access

ONTAP 9

NetApp
June 02, 2023

This PDF was generated from https://docs.netapp.com/us-en/ontap/authentication/enable-nis-ldap-users-access-cluster-task.html on June 02, 2023. Always check docs.netapp.com for the latest.

Table of Contents

Configure LDAP or NIS server access . . . 1
Configure LDAP or NIS server access overview . . . 1
Configure LDAP server access . . . 1
Configure NIS server access . . . 2
Create a name service switch . . . 3

Configure LDAP or NIS server access

Configure LDAP or NIS server access overview

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

Configure LDAP server access

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

What you'll need

- You must have installed a CA-signed server digital certificate on the SVM.
- You must be a cluster or SVM administrator to perform this task.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see the following documents.

- NFS configuration
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP

Steps

1. Create an LDAP client configuration on an SVM: `vserver services name-service ldap client create -vserver SVM_name -client-config client_configuration -servers LDAP_server_IPs -schema schema -use-start-tls true|false`

   Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

   For complete command syntax, see the worksheet.

   The following command creates an LDAP client configuration named `corp` on the SVM`engData`. The client makes anonymous binds to the LDAP servers with the IP addresses `172.160.0.100` and

`172.16.0.101`. The client uses the `RFC-2307` schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.

```
cluster1::>vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

2. Associate the LDAP client configuration with the SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

   For complete command syntax, see the worksheet.

   The following command associates the LDAP client configuration `corp` with the SVM`engData`, and enables the LDAP client on the SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

   Beginning with ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

3. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                  |
| Client Configuration Name: c1                                 |
| LDAP Status: up                                               |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

   The name service check command is available beginning with ONTAP 9.2.

Configure NIS server access

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create`

command to create an NIS domain configuration on an SVM.

What you'll need

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

About this task

You can create multiple NIS domains. Only one NIS domain can be set to `active` at a time.

Step

1. Create an NIS domain configuration on an SVM: `vserver services name-service nis-domain create -vserver SVM_name -domain client_configuration -active true|false -nis-servers NIS_server_IPs`

   For complete command syntax, see the worksheet.

   > Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

   The following command creates an NIS domain configuration on the SVM `engData`. The NIS domain `nisdomain` is active on creation and communicates with an NIS server with the IP address `192.0.2.180`.

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
   ```

Create a name service switch

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

What you'll need

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

Step

1. Specify the lookup order for name service sources:

   `vserver services name-service ns-switch modify -vserver SVM_name -database name_service_switch_database -sources name_service_source_order`

   For complete command syntax, see the worksheet.

   The following command specifies the lookup order of the LDAP and NIS name service sources for the `passwd` database on the `engData`SVM.

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

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.