

Manage domain controller connections

ONTAP 9

NetApp July 19, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/smb-admin/display-discovered-servers-task.html on July 19, 2022. Always check docs.netapp.com for the latest.

Table of Contents

VI	lanage domain controller connections	1
	Display information about discovered servers	1
	Reset and rediscover servers	1
	Manage domain controller discovery	_
	Add preferred domain controllers	-
	Commands for managing preferred domain controllers	1
	Enable SMB2 connections to domain controllers.	1
	Enable encrypted connections to domain controllers	-

Manage domain controller connections

Display information about discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

Step

1. To display information related to discovered servers, enter the following command: vserver cifs domain discovered-servers show

Example

The following example shows discovered servers for SVM vs1:

cluster1::> vserver cifs domain discovered-servers show					
Node: node1 Vserver: vs1					
Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com example.com	MS-LDAP MS-DC	adequate adequate	DC-2 DC-1	1.1.3.5	OK OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Related information

Resetting and rediscovering servers

Stopping or starting the CIFS server

Reset and rediscover servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

Steps

- 1. Enter the following command: vserver cifs domain discovered-servers reset-servers -vserver vserver name
- 2. Display information about the newly rediscovered servers: vserver cifs domain discovered-servers show -vserver vserver name

Example

The following example resets and rediscovers servers for storage virtual machine (SVM, formerly known as Vserver) vs1:

cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name	Туре	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Related information

Displaying information about discovered servers

Stopping or starting the CIFS server

Manage domain controller discovery

Beginning with ONTAP 9.3, you can modify the default process by which domain controllers (DCs) are discovered. This enables you to limit discovery to your site or to a pool of preferred DCs, which can lead to performance improvements depending on the environment.

About this task

By default, the dynamic discovery process discovers all available DCs, including any preferred DCs, all DCs in the local site, and all remote DCs. This configuration can lead to latency in authentication and accessing shares in certain environments. If you have already determined the pool of DCs that you want to use, or if the remote DCs are inadequate or inaccessible, you can change the discovery method.

In ONTAP 9.3 and later releases, the discovery-mode parameter of the cifs domain discovered-servers command enables you to select one of the following discovery options:

- · All DCs in the domain are discovered.
- · Only DCs in the local site are discovered.

The default-site parameter for the SMB server must be defined to use this mode.

• Server discovery is not performed, the SMB server configuration depends only on preferred DCs.

To use this mode, you must first define the preferred DCs for the SMB server.

Step

 Specify the desired discovery option: vserver cifs domain discovered-servers discoverymode modify -vserver vserver name -mode {all|site|none}

Options for the mode parameter:

 \circ all

Discover all available DCs (default).

° site

Limit DC discovery to your site.

° none

Use only preferred DCs and not perform discovery.

Add preferred domain controllers

ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

Step

1. To add to the list of preferred domain controllers, enter the following command:

```
vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name
-preferred-dc IP_address, ...+
```

-vserver vserver name specifies the storage virtual machine (SVM) name.

-domain domain_name specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.

-preferred-dc *IP_address*,... specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the SMB server on SVM vs1 uses to manage external access to the cifs.lab.example.com domain.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Commands for managing preferred domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

If you want to	Use this command
Add a preferred domain controller	vserver cifs domain preferred-dc add
Display preferred domain controllers	vserver cifs domain preferred-dc show
Remove a preferred domain controller	vserver cifs domain preferred-dc remove

See the man page for each command for more information.

Related information

Adding preferred domain controllers

Enable SMB2 connections to domain controllers

Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller. Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB2 is enabled by default.

About this task

The smb2-enabled-for-dc-connections command option enables the system default for the release of ONTAP you are using. The system default for ONTAP 9.1 is enabled for SMB 1.0 and disabled for SMB 2.0. The system default for ONTAP 9.2 is enabled for SMB 1.0 and enabled for SMB 2.0. If the domain controller cannot negotiate SMB 2.0 initially, it uses SMB 1.0.

SMB 1.0 can be disabled from ONTAP to a domain controller. In ONTAP 9.1, if SMB 1.0 has been disabled, SMB 2.0 must be enabled in order to communicate with a domain controller.



If -smb1-enabled-for-dc-connections is set to false while -smb1-enabled is set to true, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server. See the topic, *Enabling and disabling SMB versions* in this guide.

Steps

- 1. Before changing SMB security settings, verify which SMB versions are enabled: vserver cifs security show
- 2. Scroll down the list to see the SMB versions.
- 3. Perform the appropriate command, using the smb2-enabled-for-dc-connections option.

If you want SMB2 to be	Enter the command
Enabled	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre>

Related information

Supported SMB versions and functionality

Enable encrypted connections to domain controllers

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted.

About this task

ONTAP requires encryption for domain controller (DC) communications when the <code>-encryption-required</code> <code>-for-dc-connection</code> option is set to <code>true</code>; the default is <code>false</code>. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3.

When encrypted DC communications are required, the <code>-smb2-enabled-for-dc-connections</code> option is ignored, because ONTAP only negotiates SMB3 connections. If a DC doesn't support SMB3 and encryption, ONTAP will not connect with it.

Step

1. Enable encrypted communication with the DC: vserver cifs security modify -vserver svm name -encryption-required-for-dc-connection true

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.