Manage domain controller connections
ONTAP 9
NetApp
November 28, 2022
# Table of Contents

Manage domain controller connections .......................................................... 1  
   Display information about discovered servers ........................................... 1  
   Reset and rediscover servers .................................................................. 1  
   Manage domain controller discovery ......................................................... 2  
Add preferred domain controllers ................................................................. 3  
Commands for managing preferred domain controllers ................................. 4  
Enable SMB2 connections to domain controllers .......................................... 4  
Enable encrypted connections to domain controllers .................................... 5
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

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
</tbody>
</table>
```

**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

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
</tbody>
</table>
```

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

1. Specify the desired discovery option: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}

Options for the `mode` parameter:

- **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:

   ```bash
   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.

```bash
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.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a preferred domain controller</td>
<td>vserver cifs domain preferred-dc add</td>
</tr>
<tr>
<td>Display preferred domain controllers</td>
<td>vserver cifs domain preferred-dc show</td>
</tr>
<tr>
<td>Remove a preferred domain controller</td>
<td>vserver cifs domain preferred-dc remove</td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

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 | `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true`

Disabled | `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false`

**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 `-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.

When encrypted DC communications are required, the `-smb2-enabled-for-dc-connections` 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`