Verify that the configuration is capable of nondisruptive operations

ONTAP 9

NetApp

March 08, 2024
Table of Contents

Verify that the configuration is capable of nondisruptive operations ........................................ 1
  Use health monitoring to determine whether nondisruptive operation status is healthy .......... 1
  Display nondisruptive operation status by using system health monitoring ......................... 1
  Verify the continuously available SMB share configuration ................................................. 3
  Verify LIF status .................................................................................................................. 5
  Determine whether SMB sessions are continuously available ............................................... 7
Verify that the configuration is capable of nondisruptive operations

Use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Severity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HaNotReadyCifsNdo_Alert</td>
<td>Major</td>
<td>One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.</td>
</tr>
<tr>
<td>NoStandbyLifCifsNdo_Alert</td>
<td>Minor</td>
<td>The storage virtual machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.</td>
</tr>
</tbody>
</table>

Display nondisruptive operation status by using system health monitoring

You can use the system health commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

Steps
1. Monitor health status by performing the appropriate action:

<table>
<thead>
<tr>
<th>If you want to display...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The health status of the system, which reflects the overall status of individual health monitors</td>
<td>system health status show</td>
</tr>
<tr>
<td>Information about the health status of the CIFS-NDO subsystem</td>
<td>system health subsystem show -subsystem CIFS-NDO -instance</td>
</tr>
</tbody>
</table>

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

<table>
<thead>
<tr>
<th>If you want to display information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status</td>
<td>system health config show -subsystem CIFS-NDO</td>
</tr>
<tr>
<td>The CIFS-NDO alerts that a health monitor can potentially generate</td>
<td>system health alert definition show -subsystem CIFS-NDO</td>
</tr>
<tr>
<td>CIFS-NDO health monitor policies, which determine when alerts are raised</td>
<td>system health policy definition show -monitor node-connect</td>
</tr>
</tbody>
</table>

Use the `-instance` parameter to display detailed information.

Examples
The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```bash
cluster1::> system health status show
Status
---------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

  Subsystem: CIFS-NDO
  Health: ok
  Initialization State: initialized
  Number of Outstanding Alerts: 0
  Number of Suppressed Alerts: 0
    Node: node2
  Subsystem Refresh Interval: 5m
```
The following output shows detailed information about the configuration and status of the health monitor of the CIFS-NDO subsystem:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0
```

**Verify the continuously available SMB share configuration**

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to provide seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.
About this task
You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`
- Symlinks must be disabled.

For proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps
1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:

   `vserver cifs shares show -vserver vserver_name`

2. Verify that the SMB shares are configured for continuous availability:

   `vserver cifs shares properties show -vserver vserver_name`

Examples
The following example displays the share setting for a share named “share1” on storage virtual machine (SVM, formerly known as Vserver) vs1. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the `Symlink Properties` field output):
The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name share1
Vserver: vs1
Share: share1
CIFS Server NetBIOS Name: VS1
Path: /data/share1
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

**Verify LIF status**

Even if you configure storage virtual machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

**About this task**

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

**Steps**

1. Display information about configured LIFs for the SVM:

   ```
   network interface show -vserver vserver_name
   ```

   In this example, “lif1” is not located on the home port.
network interface show -vserver vs1

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>10.0.0.128/24</td>
<td>node2</td>
<td>e0d</td>
</tr>
<tr>
<td>false</td>
<td>lif2</td>
<td>up/up</td>
<td>10.0.0.129/24</td>
<td>node2</td>
<td>e0d</td>
</tr>
</tbody>
</table>

2. If some of the LIFs are not on their home ports, perform the following steps:
   a. For each LIF, determine what the LIF’s home port is:

```
   network interface show -vserver vserver_name -lif lif_name -fields home-node,home-port
   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
   vserver lif home-node home-port
   ------- ---- ---------- ----------
   vs1     lif1 node1      e0d
```

b. For each LIF, determine whether the LIF’s home port is up:

```
   network port show -node node_name -port port -fields port,link
   network port show -node node1 -port e0d -fields port,link
```

```
   node       port link
   ---------- ---- ----
   node1      e0d   up
```

   In this example, “lif1” should be migrated back to its home port, node1:e0d.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the up state, resolve the problem so that these interfaces are up.

4. If needed, revert the LIFs to their home ports:

```
   network interface revert -vserver vserver_name -lif lif_name
   network interface revert -vserver vs1 -lif lif1
```
5. Verify that each node in the cluster has an active LIF for the SVM:

```bash
network interface show -vserver vserver_name

network interface show -vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical</th>
<th>Status</th>
<th>Network</th>
<th>Current</th>
<th>Current Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>--------</td>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>10.0.0.128/24</td>
<td>node1</td>
<td>e0d</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>10.0.0.129/24</td>
<td>node2</td>
<td>e0d</td>
</tr>
</tbody>
</table>

Determine whether SMB sessions are continuously available

Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session’s SMB protocol version and continuously available protection level, which helps you to identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.
  
  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.

- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:
| If you want to display SMB session information... | Enter the following command...
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For all sessions on the SVM in summary form</td>
<td><code>vserver cifs session show -vserver vserver_name</code></td>
</tr>
<tr>
<td>On a specified connection ID</td>
<td><code>vserver cifs session show -vserver vserver_name -connection-id integer</code></td>
</tr>
<tr>
<td>From a specified workstation IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code></td>
</tr>
<tr>
<td>On a specified LIF IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address</code></td>
</tr>
<tr>
<td>On a specified node</td>
<td>`vserver cifs session show -vserver vserver_name -node {node_name</td>
</tr>
</tbody>
</table>
| From a specified Windows user | `vserver cifs session show -vserver vserver_name -windows -user user_name`  
  The format for user_name is [domain]\user. |
| With a specified authentication mechanism | `vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism`  
  The value for -auth-mechanism can be one of the following:  
  * NTLMv1  
  * NTLMv2  
  * Kerberos  
  * Anonymous |
If you want to display SMB session information…

Enter the following command…

<table>
<thead>
<tr>
<th>With a specified protocol version</th>
<th>vserver cifs session show -vserver vserver_name -protocol -version protocol_version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The value for <code>-protocol-version</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• SMB1</td>
</tr>
<tr>
<td></td>
<td>• SMB2</td>
</tr>
<tr>
<td></td>
<td>• SMB2_1</td>
</tr>
<tr>
<td></td>
<td>• SMB3</td>
</tr>
<tr>
<td></td>
<td>• SMB3_1</td>
</tr>
<tr>
<td></td>
<td>Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to SMB3 or later.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>With a specified level of continuously available protection</th>
<th>vserver cifs session show -vserver vserver_name -continuously-available continuously_available_protection_level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The value for <code>-continuously-available</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Partial</td>
</tr>
<tr>
<td></td>
<td>If the continuously available status is Partial, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the <code>vserver cifs sessions file show</code> command to determine which files on the established session are not open with continuously available protection.</td>
</tr>
</tbody>
</table>

| With a specified SMB signing session status | vserver cifs session show -vserver vserver_name -is -session-signed {true|false} |

**Examples**

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:
The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```bash
cluster1::> vserver cifs session show -instance -continuously-available
Yes
```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.
cluster1::> vserver cifs session show -instance -protocol-version SMB3

  Node: node1
  Vserver: vs1
  Session ID: 1
  **Connection IDs: 3151272607,31512726078,3151272609**
  Connection Count: 3**
  Incoming Data LIF IP Address: 10.2.1.2
  Workstation IP address: 10.1.1.3
  Authentication Mechanism: NTLMv2
    Windows User: DOMAIN\administrator
    UNIX User: pcuser
  Open Shares: 1
  Open Files: 0
  Open Other: 0
  Connected Time: 6m 22s
  Idle Time: 5m 42s
  Protocol Version: SMB3
  Continuously Available: No
  Is Session Signed: false
  User Authenticated as: domain-user
  NetBIOS Name: -
  SMB Encryption Status: Unencrypted

Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can also display information about the continuously available protection level of a file, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the -continuously-available field in vserver cifs session show command output is Partial), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the vserver cifs session file show command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.
• You can use the optional `-fields` parameter to display output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.

• You can use the `-instance` parameter to display detailed information about open SMB files. You can use this parameter either alone or in combination with other optional parameters.

**Steps**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display open SMB files…</th>
<th>Enter the following command…</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the SVM in summary form</td>
<td><code>vserver cifs session file show -vserver vserver_name</code></td>
</tr>
<tr>
<td>On a specified node</td>
<td>`vserver cifs session file show -vserver vserver_name -node {node_name</td>
</tr>
<tr>
<td>On a specified file ID</td>
<td><code>vserver cifs session file show -vserver vserver_name -file-id integer</code></td>
</tr>
<tr>
<td>On a specified SMB connection ID</td>
<td><code>vserver cifs session file show -vserver vserver_name -connection-id integer</code></td>
</tr>
<tr>
<td>On a specified SMB session ID</td>
<td><code>vserver cifs session file show -vserver vserver_name -session-id integer</code></td>
</tr>
<tr>
<td>On the specified hosting aggregate</td>
<td><code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code></td>
</tr>
<tr>
<td>On the specified volume</td>
<td><code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code></td>
</tr>
<tr>
<td>On the specified SMB share</td>
<td><code>vserver cifs session file show -vserver vserver_name -share share_name</code></td>
</tr>
<tr>
<td>On the specified SMB path</td>
<td><code>vserver cifs session file show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>If you want to display open SMB files...</td>
<td>Enter the following command...</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>With the specified level of continuously available protection</td>
<td>vserver cifs session file show -vserver vserver_name -continuously-available continuously_available_status</td>
</tr>
<tr>
<td></td>
<td>The value for <code>--continuously-available</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
</tbody>
</table>

If the continuously available status is No, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.

With the specified reconnected state | vserver cifs session file show -vserver vserver_name -reconnected reconnected_state |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The value for <code>--reconnected</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
</tbody>
</table>

If the reconnected state is No, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is Yes, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples
The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node: node1
Vserver: vs1
Connection: 3151274158
Session: 1
File ID Type Mode Volume Share Available
------- --------- ---- --------- ----------- ------------
41 Regular r data data Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -instance

Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```