Verify that the configuration is capable of nondisruptive operations

ONTAP 9

NetApp
January 08, 2026

Table of Contents

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:

Alert ID	Severity	Condition
`HaNotReadyCifsNdo_Alert`	Major	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.
`NoStandbyLifCifsNdo_Alert`	Minor	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.

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:

If you want to display…	Enter the command…
The health status of the system, which reflects the overall status of individual health monitors	**system health status show**
Information about the health status of the CIFS-NDO subsystem	**system health subsystem show -subsystem CIFS-NDO -instance**

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

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

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:

```
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):

```
cluster1::> vserver cifs share 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
```

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    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

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`

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Learn more about `network interface show` in the ONTAP command reference.

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`.

      Learn more about `network port show` in the ONTAP command reference.

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. Learn more about `up` in the ONTAP command reference.
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

Learn more about `network interface revert` in the ONTAP command reference.

5. Verify that each node in the cluster has an active LIF for the SVM:

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

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…
For all sessions on the SVM in summary form	**vserver cifs session show -vserver *vserver_name***
On a specified connection ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
From a specified workstation IP address	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
On a specified LIF IP address	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
On a specified node	**vserver cifs session show -vserver *vserver_name* -node {node_name|local}**
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…
With a specified protocol version	**vserver cifs session show -vserver *vserver_name* -protocol -version protocol_version** The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` 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.
With a specified level of continuously available protection	**vserver cifs session show -vserver *vserver_name* -continuously-available *continuously_available_protection_level*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` • `Partial` 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 `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
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:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

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.

```
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 in ONTAP

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:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	**vserver cifs session file show -vserver *vserver_name***
On a specified node	**vserver cifs session file show -vserver *vserver_name* -node {node_name|local}**
On a specified file ID	**vserver cifs session file show -vserver *vserver_name* -file-id integer**
On a specified SMB connection ID	**vserver cifs session file show -vserver *vserver_name* -connection-id integer**
On a specified SMB session ID	**vserver cifs session file show -vserver *vserver_name* -session-id integer**
On the specified hosting aggregate	**vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name***
On the specified volume	**vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name***
On the specified SMB share	**vserver cifs session file show -vserver *vserver_name* -share *share_name***
On the specified SMB path	**vserver cifs session file show -vserver *vserver_name* -path *path***

If you want to display open SMB files…	Enter the following command…
With the specified level of continuously available protection	**vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` 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*** The value for `-reconnected` can be one of the following: • `No` • `Yes` 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. Learn more about the commands described in this procedure in the ONTAP command reference.

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    File      Open Hosting              Continuously
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
```

Copyright information

Trademark information