



Verify that the configuration is capable of nondisruptive operations

ONTAP 9

NetApp
August 10, 2023

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:

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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is 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					

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 vs1 -lif lif1 -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 node1 -port e0d -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 vs1 -lif lif1
```

```
network interface revert -vserver vs1 -lif lif1
```


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

```
network interface show -vserver vs1
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
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	<code>vserver cifs session show -vserver <i>vserver_name</i></code>
On a specified connection ID	<code>vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer</code>
From a specified workstation IP address	<code>vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i></code>
On a specified LIF IP address	<code>vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i></code>
On a specified node	<code>vserver cifs session show -vserver <i>vserver_name</i> -node {<i>node_name</i> local}</code>
From a specified Windows user	<code>vserver cifs session show -vserver <i>vserver_name</i> -windows -user <i>user_name</i></code> The format for <i>user_name</i> is [domain]\user.
With a specified authentication mechanism	<code>vserver cifs session show -vserver <i>vserver_name</i> -auth -mechanism <i>authentication_mechanism</i></code> The value for <code>-auth-mechanism</code> can be one of the following: <ul style="list-style-type: none"> • NTLMv1 • NTLMv2 • Kerberos • Anonymous

If you want to display SMB session information...	Enter the following command...
With a specified protocol version	<pre>vserver cifs session show -vserver vserver_name -protocol -version protocol_version</pre> <p>The value for <code>-protocol-version</code> can be one of the following:</p> <ul style="list-style-type: none"> • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 <div>  <p>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.</p> </div>
With a specified level of continuously available protection	<pre>vserver cifs session show -vserver vserver_name -continuously-available continuously_available_protection_level</pre> <p>The value for <code>-continuously-available</code> can be one of the following:</p> <ul style="list-style-type: none"> • No • Yes • Partial <div>  <p>If the continuously available status is <code>Partial</code>, 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.</p> </div>
With a specified SMB signing session status	<pre>vserver cifs session show -vserver vserver_name -is -session-signed {true false}</pre>

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
ID        ID        Workstation      Windows User      Open      Idle
-----
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

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	<code>vserver cifs session file show -vserver vserver_name</code>
On a specified node	<code>vserver cifs session file show -vserver vserver_name -node {node_name local}</code>
On a specified file ID	<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>
On a specified SMB connection ID	<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>
On a specified SMB session ID	<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>
On the specified hosting aggregate	<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>
On the specified volume	<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>
On the specified SMB share	<code>vserver cifs session file show -vserver vserver_name -share share_name</code>
On the specified SMB path	<code>vserver cifs session file show -vserver vserver_name -path path</code>

If you want to display open SMB files...	Enter the following command...
With the specified level of continuously available protection	<div data-bbox="834 149 1495 315"><pre>vserver cifs session file show -vserver vserver_name -continuously -available continuously_available_status</pre></div> <div data-bbox="834 315 1495 409"><p>The value for <code>-continuously-available</code> can be one of the following:</p></div> <div data-bbox="834 409 1495 546"><ul style="list-style-type: none">• No• Yes</div> <div data-bbox="909 693 1495 892"><div data-bbox="909 693 990 766"></div><div data-bbox="990 546 1495 892"><p>If the continuously available status is <code>No</code>, 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.</p></div></div>
With the specified reconnected state	<div data-bbox="834 951 1495 1092"><pre>vserver cifs session file show -vserver vserver_name -reconnected reconnected_state</pre></div> <div data-bbox="834 1092 1495 1186"><p>The value for <code>-reconnected</code> can be one of the following:</p></div> <div data-bbox="834 1186 1495 1323"><ul style="list-style-type: none">• No• Yes</div> <div data-bbox="909 1491 1495 1732"><div data-bbox="909 1491 990 1564"></div><div data-bbox="990 1323 1495 1732"><p>If the reconnected state is <code>No</code>, 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 <code>Yes</code>, this means that the open file is successfully reconnected after a disconnection event.</p></div></div>

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       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

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.