



# **Monitor SMB activity**

## **ONTAP 9**

NetApp  
February 03, 2023

# Table of Contents

- Monitor SMB activity . . . . . 1
  - Display SMB session information . . . . . 1
  - Display information about open SMB files . . . . . 4
  - Determine which statistics objects and counters are available . . . . . 7
  - Display statistics . . . . . 11

# Monitor SMB activity

## 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 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.

### Step

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 vserver_name</code>                                 |
| On a specified connection ID                      | <code>vserver cifs session show -vserver vserver_name -connection-id integer</code>          |
| From a specified workstation IP address           | <code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code> |
| On a specified LIF IP address                     | <code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>     |
| On a specified node                               | <code>vserver cifs session show -vserver vserver_name -node {node_name local}</code>         |

| If you want to display SMB session information...           | Enter the following command...  |
|---|---|
| From a specified Windows user                               | <pre>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</pre>   |
| With a specified authentication mechanism                   | <pre>vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1 NTLMv2 Kerberos Anonymous}</pre>   |
| With a specified protocol version                           | <pre>vserver cifs session show -vserver vserver_name -protocol-version {SMB1 SMB2 SMB2_1 SMB3 SMB3_1}</pre> <div data-bbox="873 751 928 810" data-label="Image"></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>  |
| With a specified level of continuously available protection | <pre>vserver cifs session show -vserver vserver_name -continuously-available {No Yes Partial}</pre> <div data-bbox="873 1291 928 1350" data-label="Image"></div> <p>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.</p> |
| 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::> vsriver 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::> vsriver 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
```

## Related information

[Displaying information about open SMB files](#)

# 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 display information about a file's continuously available protection level, 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.

## Step

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

| If you want to display open SMB files...                      | Enter the following command...  |
|---|---|
| On the specified SMB path                                     | <pre>vserver cifs session file show -vserver vserver_name -path path</pre>  |
| With the specified level of continuously available protection | <pre>vserver cifs session file show -vserver vserver_name -continuously -available {No Yes}</pre> <div data-bbox="873 541 928 604">  </div> <div data-bbox="987 436 1448 709"> <p>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.</p> </div>   |
| With the specified reconnected state                          | <pre>vserver cifs session file show -vserver vserver_name -reconnected {No Yes}</pre> <div data-bbox="873 1066 928 1129">  </div> <div data-bbox="987 930 1448 1266"> <p>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.</p> </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
```

## Related information

[Displaying SMB session information](#)

## Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`

2. Perform one of the following actions:

| If you want to determine...         | Enter...  |
|-------------------------------------|---|
| Which objects are available         | <code>statistics catalog object show</code>                         |
| Specific objects that are available | <code>statistics catalog object show object<br/>object_name</code>  |
| Which counters are available        | <code>statistics catalog counter show object<br/>object_name</code> |

See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level: `set -privilege admin`

### Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs       The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1              These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2              These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd             The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:



This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

| Counter              | Description  |
|----------------------|--|
| active_searches      | Number of active searches over SMB and SMB2                                  |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth  | Average number of directories crossed by SMB and SMB2 path-based commands    |
| ...                  | ...  |

```
cluster2::> statistics start -object client -sample-id
```

Object: client

| Counter              | Value                   |
|----------------------|-------------------------|
| cifs_ops             | 0                       |
| cifs_read_ops        | 0                       |
| cifs_read_recv_ops   | 0                       |
| cifs_read_recv_size  | 0B                      |
| cifs_read_size       | 0B                      |
| cifs_write_ops       | 0                       |
| cifs_write_recv_ops  | 0                       |
| cifs_write_recv_size | 0B                      |
| cifs_write_size      | 0B                      |
| instance_name        | vserver_1:10.72.205.179 |
| instance_uuid        | 2:10.72.205.179         |
| local_ops            | 0                       |
| mount_ops            | 0                       |

[...]

## Related information

[Displaying statistics](#)

# Display statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

## Before you begin

You must have collected data samples by using the `statistics start` and `statistics stop` commands before you can display information about objects.

## Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

| If you want to display statistics for... | Enter...   |
|--|--|
| All versions of SMB                      | <code>statistics show -object cifs</code>        |
| SMB 1.0                                  | <code>statistics show -object smb1</code>        |
| SMB 2.x and SMB 3.0                      | <code>statistics show -object smb2</code>        |
| CIFS subsystem of the node               | <code>statistics show -object nblade_cifs</code> |
| Multiprotocol audit                      | <code>statistics show -object audit_ng</code>    |
| BranchCache hash service                 | <code>statistics show -object hashd</code>       |
| Dynamic DNS                              | <code>statistics show -object ddns_update</code> |

See the man page for each command for more information.

3. Return to the admin privilege level: `set -privilege admin`

## Related information

[Determining which statistics objects and counters are available](#)

[Monitoring SMB signed session statistics](#)

[Displaying BranchCache statistics](#)

[Using statistics to monitor automatic node referral activity](#)

[SMB configuration for Microsoft Hyper-V and SQL Server](#)

[Performance monitoring setup](#)

## 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.