Monitor SMB activity

ONTAP 9

NetApp
November 30, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/smb-admin/display-session-task.html on November 30, 2022. Always check docs.netapp.com for the latest.
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:

<table>
<thead>
<tr>
<th>If you want to display SMB session information...</th>
<th>Enter the following command...</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>
<tr>
<td>If you want to display SMB session information...</td>
<td>Enter the following command...</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>From a specified Windows user</td>
<td><code>vserver cifs session show -vserver vserver_name -windows-user domain_name\user_name</code></td>
</tr>
<tr>
<td>With a specified authentication mechanism</td>
<td>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</td>
</tr>
<tr>
<td>With a specified protocol version</td>
<td>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</td>
</tr>
<tr>
<td>With a specified level of continuously available protection</td>
<td>`vserver cifs session show -vserver vserver_name -continuously-available {No</td>
</tr>
<tr>
<td>With a specified SMB signing session status</td>
<td>`vserver cifs session show -vserver vserver_name -is-session-signed {true</td>
</tr>
</tbody>
</table>

**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.

```
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.
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:

<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>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name</td>
</tr>
<tr>
<td>On a specified node</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -node</td>
</tr>
<tr>
<td></td>
<td>{node_name</td>
</tr>
<tr>
<td>On a specified file ID</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -file-id</td>
</tr>
<tr>
<td></td>
<td>integer</td>
</tr>
<tr>
<td>On a specified SMB connection ID</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -connection-id</td>
</tr>
<tr>
<td></td>
<td>integer</td>
</tr>
<tr>
<td>On a specified SMB session ID</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -session-id</td>
</tr>
<tr>
<td></td>
<td>integer</td>
</tr>
<tr>
<td>On the specified hosting aggregate</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -hosting</td>
</tr>
<tr>
<td></td>
<td>-aggregate aggregate_name</td>
</tr>
<tr>
<td>On the specified volume</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -hosting-volume</td>
</tr>
<tr>
<td></td>
<td>volume_name</td>
</tr>
<tr>
<td>On the specified SMB share</td>
<td>vserver cifs session file show</td>
</tr>
<tr>
<td></td>
<td>-vserver vserver_name -share</td>
</tr>
<tr>
<td></td>
<td>share_name</td>
</tr>
</tbody>
</table>
If you want to display open SMB files... | Enter the following command...
---|---
On the specified SMB path | `vserver cifs session file show -vserver vserver_name -path path`
With the specified level of continuously available protection | `vserver cifs session file show -vserver vserver_name -continuously_available {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 {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. See the man page for more information.

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

```bash
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:

<table>
<thead>
<tr>
<th>If you want to determine...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which objects are available</td>
<td>statistics catalog object show</td>
</tr>
<tr>
<td>Specific objects that are available</td>
<td>statistics catalog object show object object_name</td>
</tr>
<tr>
<td>Which counters are available</td>
<td>statistics catalog counter show object object_name</td>
</tr>
</tbody>
</table>

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

[...]
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:

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

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