■ NetApp

Monitor SMB activity

ONTAP 9

NetApp July 01, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/smb-admin/display-session-task.html on July 01, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Monito	r SMB activity
Disp	olay SMB session information
Disp	olay information about open SMB files
Dete	ermine which statistics objects and counters are available
Disp	olay statistics

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	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	<pre>vserver cifs session show -vserver vserver_name -address workstation_IP_address</pre>	
On a specified LIF IP address	vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address	
On a specified node	<pre>vserver cifs session show -vserver vserver_name -node {node_name local}</pre>	

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>
	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	<pre>vserver cifs session show -vserver vserver_name -continuously-available {No Yes Partial}</pre>
	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	<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
                                                Open
                                                           Idle
         ID
             Workstation
                                               Files
                                                           Time
                               Windows User
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
```

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 <code>-continuously-available</code> field in <code>vserver cifs session show command output</code> is <code>Partial</code>), 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	vserver cifs session file show -vserver vserver_name	
On a specified node	<pre>vserver cifs session file show -vserver vserver_name -node {node_name local}</pre>	
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	

If you want to display open SMB files		Enter the following command	
On the specified SMB path		cifs session file show er vserver_name -path path	
With the specified level of continuously available protection	-vserve	cifs session file show er vserver_name -continuously able {No Yes}	
	i	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		cifs session file show er vserver_name -reconnected s}	
	i	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
             Open Hosting
File File
                                    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	statistics catalog object show	
Specific objects that are available	statistics catalog object show object object_name	
Which counters are available	statistics catalog counter show object object_name	

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
                                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
                                These counters report activity from the
    smb1
SMB
                                revision of the protocol. For information
cluster1::*> statistics catalog object show -object smb2
                                These counters report activity from the
    smb2
                                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
   requests were made in rapid succession
  SMB
                            and SMB2 path-based commands
   . . .
                            . . .
cluster2::> statistics start -object client -sample-id
Object: client
   Counter
                                                       Value
   cifs ops
                                                           0
                                                           0
   cifs read ops
                                                           0
   cifs read recv ops
   cifs read recv size
                                                          0B
   cifs read size
                                                           0B
                                                           0
   cifs write ops
                                                           0
   cifs write recv ops
   cifs write recv size
                                                          0B
   cifs_write_size
                                                           0В
   instance name
                                        vserver 1:10.72.205.179
   instance uuid
                                               2:10.72.205.179
   local ops
                                                           0
                                                           0
   mount_ops
[...]
```

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	statistics show -object cifs
SMB 1.0	statistics show -object smb1
SMB 2.x and SMB 3.0	statistics show -object smb2
CIFS subsystem of the node	statistics show -object nblade_cifs
Multiprotocol audit	statistics show -object audit_ng
BranchCache hash service	statistics show -object hashd
Dynamic DNS	statistics show -object ddns_update

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 © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.