network tcpdump commands

ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-98/network-tcpdump-show.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

network tcpdump commands . . . 1
- network tcpdump show . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- network tcpdump start . . . 1
  - Description . . . 2
  - Parameters . . . 2
  - Examples . . . 2
- network tcpdump stop . . . 2
  - Description . . . 2
  - Parameters . . . 3
  - Examples . . . 3
- network tcpdump trace delete . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 3
- network tcpdump trace show . . . 3
  - Description . . . 4
  - Parameters . . . 4
  - Examples . . . 4

network tcpdump commands

network tcpdump show

Show running tcpdump instances

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `network tcpdump show` command shows currently running packet traces (via tcpdump) on a matching node.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node Name

Use this parameter optionally to show the details of running packet traces on a matching node.

[-port {<netport>|<ifgrp>}] - Port

Use this parameter optionally to show the details of running packet trace on a matching network interface.

Examples

The following example shows the details of running packet traces on nodes "node1" and "node2":

```
cluster1::> network tcpdump show
Node       Port
---------- --------
node1
           e0a
node2
           e0c
```

network tcpdump start

tcpdump start

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `network tcpdump start` command starts packet tracing (via tcpdump) with the given parameters.

Parameters

`-node {<nodename>|local}` - Node Name

Use this parameter to specify the node on which the packet trace should run.

`-port {<netport>|<ifgrp>}` - Port

Use this parameter to specify the network interface for packet tracing.

`[-address <IP Address>]` - IP Address

Use this parameter to optionally specify the address for packet tracing.

`[-protocol-port <integer>]` - Protocol Port Number

Use this parameter to optionally specify the protocol port number for packet tracing.

`[-buffer-size <integer>]` - Buffer Size in KB

Use this parameter to optionally specify the buffer size for packet tracing. The default buffer size is 4 KB.

`[-file-size <integer>]` - Trace File Size in MB

Use this parameter to optionally specify the trace file size for packet tracing. The default trace file size is 1 GB.

`[-rolling-traces <integer>]` - Number of Rolling Trace Files

Use this parameter to optionally specify the number of rolling trace files for packet tracing. The default number of rolling trace files is 2.

Examples

The following example starts packet tracing on node "node1" with address "10.98.16.164", network port "e0c", buffer size "10 KB", and protocol port number "10000":

```
cluster1::> network tcpdump start -node node1
    -address 10.98.16.164 -port e0c -buffer-size 10 -protocol-port 10000
```

network tcpdump stop

Stop an active tcpdump trace

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `network tcpdump stop` command stops a running packet trace (via tcpdump) on a given network interface. The trace files could be located in /mroot/etc/log/packet_traces/.

Parameters

`-node {<nodename>|local}` - Node Name

Use this parameter to specify the node on which the packet tracing must be stopped.

`-port {<netport>|<ifgrp>}` - Port

Use this parameter to specify the network interface on which the packet tracing must be stopped.

Examples

The following example stops a packet trace on network interface "e0a" from node "node1":

```
cluster1::> network tcpdump stop -node node1 -port e0a
```

network tcpdump trace delete

Delete a tcpdump tracefile

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `network tcpdump trace delete` command deletes the tcpdump trace file from a matching node.

Parameters

`-node {<nodename>|local}` - Node Name

Use this parameter to delete the tcpdump trace file from a matching node.

`-trace-file <text>` - Trace File

Use this parameter to specify the tcpdump trace file to be deleted.

Examples

The following example deletes the list of tcpdump trace files from node "node1" using wildcard pattern:

```
cluster1::> network tcpdump trace delete -node node1 -trace-file *
```

network tcpdump trace show

Show list of tcpdump trace files

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `network tcpdump trace show` command shows the list of tcpdump trace files located in /mroot/etc/log/packet_traces/ directory.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node Name

Use this parameter to show the list of traces files of a matching node.

[-trace-file <text>] - Trace File

Use this parameter optionally to show the list of trace files with a matching trace-file name.

Examples

The following example shows the list of trace files on nodes "node1" and "node2":

```
cluster1::> network tcpdump trace show
Node             Trace File
---------------- ------------------------------
node1
                 e0a_20170314_115624.trc0
node2
                 e0c_20170314_115624.trc0
```

Copyright information

Copyright © 2026 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.