cluster log-forwarding commands

ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-9131/cluster-log-forwarding-create.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

cluster log-forwarding commands . . . 1
- cluster log-forwarding create . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 2
  - Related Links . . . 3
- cluster log-forwarding delete . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 3
- cluster log-forwarding modify . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 4
  - Related Links . . . 4
- cluster log-forwarding show . . . 5
  - Description . . . 5
  - Parameters . . . 5
  - Examples . . . 6

cluster log-forwarding commands

cluster log-forwarding create

Create a log forwarding destination

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

Description

The `cluster log-forwarding create` command creates log forwarding destinations for remote logging.

Parameters

`-destination <Remote InetAddress>` - Destination Host

Host name or IPv4 or IPv6 address of the server to forward the logs to.

`[-port <integer>]` - Destination Port

The port that the destination server listen on.

`[-protocol {udp-unencrypted|tcp-unencrypted|tcp-encrypted}]` - Log Forwarding Protocol

The protocols are used for sending messages to the destination. The protocols can be one of the following values:

- _ `udp-unencrypted` _ - User Datagram Protocol with no security
- _ `tcp-unencrypted` _ - Transmission Control Protocol with no security
- _ `tcp-encrypted` _ - Transmission Control Protocol with Transport Layer Security (TLS)

`[-ipspace <IPspace>]` - IPspace of Destination

The IPspace of the destination server.

`[-verify-server {true|false}]` - Verify Destination Server Identity

When this parameter is set to `true` , the identity of the log forwarding destination is verified by validating its certificate. The value can be set to `true` only when the *`tcp-encrypted`* value is selected in the protocol field. When this value is `true` the remote server might be validated by OCSP. The OCSP validation for cluster logs is controlled with the security config ocsp enable -app audit_log and security config ocsp disable -app audit_log .

`[-facility <Syslog Facility>]` - Syslog Facility

The Syslog facility to use for the forwarded logs.

`[-force <true>]` - Skip the Connectivity Test

Normally, the `cluster log-forwarding create` command checks that the destination is reachable via an ICMP ping, and fails if it is not reachable. Setting this value to `true` bypasses the ping check so that the destination can be configured when it is unreachable.

[-message-format {legacy-netapp|rfc-5424}] - Syslog Message Format

Use this parameter to specify the message format to be used for Syslog messages.

The `message-format` can be one of the following values:

- *`legacy-netapp`* - A variation of the RFC-3164 Syslog format (format: <PRIVAL>TIMESTAMP HOSTNAME: MSG)
- *`rfc-5424`* - Syslog format as per RFC-5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME: MSG)

Refer to the respective RFCs for detailed information regarding the Syslog message formats. + The default message format is *`legacy-netapp`* .

[-timestamp-format-override {no-override|rfc-3164|iso-8601-utc|iso-8601-local-time}] - Syslog Timestamp Format Override

Use this parameter to override the default timestamp format (based on the `message-format` parameter) used for Syslog messages.

The `timestamp-format-override` can be one of the following values:

- *`no-override`* - Timestamp format based on the `message-format` parameter (*`rfc-3164`* if the message format is *`legacy-netapp`* , *`iso-8601-local-time`* if message format is *`rfc-5424`*)
- *`rfc-3164`* - Timestamp format as per RFC-3164 (format: Mmm dd hh:mm:ss)
- *`iso-8601-utc`* - Timestamp format as per ISO-8601 in UTC (format: YYYY-MM-DDThh:mm:ssZ)
- *`iso-8601-local-time`* - Timestamp format as per ISO-8601 in local time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm)

The default value is *`no-override`* . When this parameter is modified, its value persists even when `message-format` is updated. +

[-hostname-format-override {no-override|fqdn|hostname-only}] - Syslog Hostname Format Override

Use this parameter to override the default hostname format (based on the `message-format` parameter) used for Syslog messages.

The `hostname-format-override` can be one of the following values:

- *`no-override`* - Hostname format based on the `message-format` parameter (*`fqdn`* if the message format is *`rfc-5424`* , *`hostname-only`* if message format is *`legacy-netapp`*)
- *`fqdn`* - Fully Qualified Domain Name (e.g., myhost.example.com)
- *`hostname-only`* - Hostname only, without the domain name (e.g., myhost)

The default value is *`no-override`* . When this parameter is modified, its value persists even when `message-format` is updated. +

Examples

This example causes audit logs to be forwarded to a server at address 192.168.0.1, port 514 with USER facility.

```
cluster1::> cluster log-forwarding create -destination 192.168.0.1 -port
514 -facility user
```

Related Links

- security config ocsp enable
- security config ocsp disable

cluster log-forwarding delete

Delete a log forwarding destination

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

Description

The `cluster log-forwarding delete` command deletes log forwarding destinations for remote logging.

Parameters

`-destination <Remote InetAddress>` - Destination Host

Host name or IPv4 or IPv6 address of the server to delete the forwarding entry for.

`-port <integer>` - Destination Port

The port that the destination server listen on.

Examples

This example deletes the forwarding of all logs to the server at address 1.1.1.1, port 514.

```
cluster1::> cluster log-forwarding delete -destination 1.1.1.1 -port 514
```

cluster log-forwarding modify

Modify log forwarding destination settings

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

Description

The `cluster log-forwarding modify` command modifies log forwarding destinations for remote logging.

Parameters

-destination <Remote InetAddress> - Destination Host

The host name or IPv4 or IPv6 address of the server to be modified.

-port <integer> - Destination Port

The port that the destinations servers listen on.

[-ipspace <IPspace>] - IPspace of Destination

The IPspace of the destination server.

[-verify-server {true|false}] - Verify Destination Server Identity

When this parameter is set to `true` , the identity of the log forwarding destination is verified by validating its certificate. The value can be set to `true` only when the *`tcp-encrypted`* value is selected in the protocol field. When this value is `true` the remote server might be validated by OCSP. The OCSP validation for cluster logs is controlled with the security config ocsp enable -app audit_log and security config ocsp disable -app audit_log .

[-facility <Syslog Facility>] - Syslog Facility

The Syslog facility to use for the forwarded logs.

[-message-format {legacy-netapp|rfc-5424}] - Syslog Message Format

Use this parameter to specify a new Syslog message format to replace the current message format.

[-timestamp-format-override {no-override|rfc-3164|iso-8601-utc|iso-8601-local-time}] - Syslog Timestamp Format Override

Use this parameter to override the default Syslog timestamp format (based on the `message-format` parameter).

[-hostname-format-override {no-override|fqdn|hostname-only}] - Syslog Hostname Format Override

Use this parameter to override the default Syslog hostname format (based on the `message-format` parameter).

Examples

This example modifies the facility of audit logs that are forwarded to the destination server at address 192.168.0.1, port 514.

```
cluster1::> cluster log-forwarding modify -destination 192.168.0.1 -port
514 -facility local1
```

Related Links

- security config ocsp enable
- security config ocsp disable

cluster log-forwarding show

Display log forwarding destinations

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

Description

The `cluster log-forwarding show` command displays log forwarding information:

- Destination (IPv4/IPv6/hostname)
- Port number
- List of log classes
- Facility

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.

[-destination <Remote InetAddress>] - Destination Host

If this optional parameter is specified, the command displays information about the forwarding destinations with the specified host name, IPv4 or IPv6 address.

[-port <integer>] - Destination Port

If this optional parameter is specified, the command displays information about the forwarding destinations with the specified ports.

[-protocol {udp-unencrypted|tcp-unencrypted|tcp-encrypted}] - Log Forwarding Protocol

If this optional parameter is specified, the command displays information about the forwarding destinations with the specified protocols.

[-ipspace <IPspace>] - IPspace of Destination

If this optional parameter is specified, the command displays information about the IPspace to which the forwarding destinations belong.

[-verify-server {true|false}] - Verify Destination Server Identity

If this optional parameter is specified, the command displays information about the forwarding destinations with the specified verify-server values.

[-facility <Syslog Facility>] - Syslog Facility

If this optional parameter is specified, the command displays information about the forwarding destinations with the specified facility.

[-message-format {legacy-netapp|rfc-5424}] - Syslog Message Format

Use this optional parameter to display information about the Syslog destination that has the specified Syslog message format.

[-timestamp-format-override {no-override|rfc-3164|iso-8601-utc|iso-8601-local-time}] - Syslog Timestamp Format Override

Use this optional parameter to display information about the Syslog destination that has the specified Syslog timestamp format override.

[-hostname-format-override {no-override|fqdn|hostname-only}] - Syslog Hostname Format Override

Use this optional parameter to display information about the Syslog destination that has the specified Syslog hostname format override.

Examples

```
The following example displays information about the log forwarding
cluster-1::> cluster log-forwarding show
Verify  Syslog
Destination Host         Port   Protocol        Server  Facility
------------------------ ------ --------------- ------  --------
192.168.0.1              514    udp-unencrypted false   user

cluster-1::> cluster log-forwarding show -instance
Destination Host: 192.168.0.1
                  Destination Port: 514
            Log Forwarding Protocol: udp-unencrypted
             IPspace of Destination: Default
 Verify Destination Server Identity: false
                    Syslog Facility: user
              Syslog Message Format: legacy-netapp
   Syslog Timestamp Format Override: no-override
    Syslog Hostname Format Override: no-override
```

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.