cluster log-forwarding commands

ONTAP 9.13.1 commands

NetApp
August 29, 2024

Table of Contents

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
```