



Forward audit logs to syslog/splunk servers

ONTAP 9.13.1 REST API reference

NetApp
August 29, 2024

Table of Contents

- Forward audit logs to syslog/splunk servers 1
 - Security audit destinations endpoint overview 1
 - Define a remote syslog or splunk server to receive audit information 4
 - Define the remote syslog or splunk server information 11
 - Delete the remote syslog or splunk server information 19
 - Retrieve the remote syslog or splunk server information 21
 - Update the remote syslog or splunk server information 24

Forward audit logs to syslog/splunk servers

Security audit destinations endpoint overview

Overview

This API controls the forwarding of audit log information to remote syslog/splunk servers. Multiple destinations can be configured and all audit records are forwarded to all destinations.

A GET operation retrieves information about remote syslog/splunk server destinations. A POST operation creates a remote syslog/splunk server destination. A GET operation on `/security/audit/destinations/{address}/{port}` retrieves information about the syslog/splunk server destination given its address and port number. A PATCH operation on `/security/audit/destinations/{address}/{port}` updates information about the syslog/splunk server destination given its address and port number. A DELETE operation on `/security/audit/destinations/{address}/{port}` deletes a syslog/splunk server destination given its address and port number.

Overview of fields used for creating a remote syslog/splunk destination

The fields used for creating a remote syslog/splunk destination fall into the following categories

Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- `address`

Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- `port`
- `ipspace`
- `protocol`
- `facility`
- `verify_server`
- `message_format` (Can be either "legacy_netapp" or "rfc_5424")
- `timestamp_format_override` (Can be either "no_override", "rfc_3164", "iso_8601_utc" or "iso_8601_local_time")
- `hostname_format_override` (Can be either "no_override", "fqdn" or "hostname_only") +

Examples

Retrieving remote syslog/splunk server destinations

The following example shows remote syslog/splunk server destinations

```
# The API:
/api/security/audit/destinations

# The call:
curl -X GET "https://<cluster-ip>/api/security/audit/destinations"

# The response:
{
  "records": [
    {
      "address": "1.1.1.1",
      "port": 514,
      "_links": {
        "self": {
          "href": "/api/security/audit/destinations/1.1.1.1/514"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/audit/destinations"
    }
  }
}
```

Creating remote syslog/splunk server destinations

The following example creates remote syslog/splunk server destinations.

```
# The API:
/api/security/audit/destinations

# The call:
curl -X POST "https://<cluster-
ip>/api/security/audit/destinations?force=true" -d '{ "address":
"1.1.1.1", "port": 514, "protocol": "udp_unencrypted", "facility":
"kern"}'
```

Retrieving a remote syslog/splunk server destination given its destination address and port number

The following example retrieves a remote syslog/splunk server destination given its destination address and port number.

```
# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X GET "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514"

# The response:
{
  "address": "1.1.1.1",
  "port": 514,
  "ipspace": {
    "name": "Default",
    "uuid": "a97a3549-f7ae-11ec-b6bc-005056a7c8ff"
  },
  "protocol": "udp_unencrypted",
  "facility": "kern",
  "verify_server": false,
  "message_format": "legacy_netapp",
  "timestamp_format_override": "no_override",
  "hostname_format_override": "no_override",
  "_links": {
    "self": {
      "href": "/api/security/audit/destinations/1.1.1.1/514"
    }
  }
}
```

Updating a remote syslog/splunk server destination given its destination address and port number

The following example updates a remote syslog/splunk server destination configuration given its destination address and port number.

```
# The API:
/api/security/audit/destinations/{address}/{port}
```

```
# The call:
curl -X PATCH "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514" -d '{"facility":
"user"}'
```

Deleting a remote syslog/splunk server destination given its destination address and port number

The following example deletes a remote syslog/splunk server destination configuration given its destination address and port number.

```
# The API:
/api/security/audit/destinations/{address}/{port}
```

```
# The call:
curl -X DELETE "https://<cluster-
ip>/api/security/audit/destinations/1.1.1.1/514"
```

Define a remote syslog or splunk server to receive audit information

GET /security/audit/destinations

Introduced In: 9.6

Defines a remote syslog/splunk server for sending audit information to.

Parameters

| Name | Type | In | Required | Description |
|---------|--------|-------|----------|-------------------|
| address | string | query | False | Filter by address |

| Name | Type | In | Required | Description |
|--|---------------|---------------|----------|--|
| timestamp_format_override | string | query | False | Filter by timestamp_format_override • Introduced in: 9.13 |
| verify_server | boolean | query | False | Filter by verify_server |
| hostname_format_override | string | query | False | Filter by hostname_format_override • Introduced in: 9.13 |
| facility | string | query | False | Filter by facility |
| port | integer | query | False | Filter by port |
| protocol | string | query | False | Filter by protocol |
| ipSPACE.name | string | query | False | Filter by ipSPACE.name • Introduced in: 9.12 |
| ipSPACE.uuid | string | query | False | Filter by ipSPACE.uuid • Introduced in: 9.12 |
| message_format | string | query | False | Filter by message_format • Introduced in: 9.13 |
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |
| desc] direction. Default direction is 'asc' for ascending. | fields | array[string] | query | False |

| Name | Type | In | Required | Description |
|--|----------------|---------|----------|-------------|
| Specify the fields to return. | max_records | integer | query | False |
| Limit the number of records returned. | return_timeout | integer | query | False |
| <p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0 | return_records | boolean | query | False |

Response

Status: 200, Ok

| Name | Type | Description |
|-------------|---|-------------------|
| _links | _links | |
| num_records | integer | Number of records |
| records | array[security_audit_log_forward] | |

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "address": "string",
      "facility": "string",
      "hostname_format_override": "string",
      "ipspace": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "name": "exchange",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    {
      "message_format": "string",
      "protocol": "string",
      "timestamp_format_override": "string"
    }
  ]
}
```

Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| next | href | |
| self | href | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

ipospace

| Name | Type | Description |
|--------|------------------------|--------------|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

security_audit_log_forward

| Name | Type | Description |
|--------------------------|--------------------------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipospace | ipospace | |

| Name | Type | Description |
|---------------------------|---------|--|
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|-------------------|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |

| Name | Type | Description |
|--------|--------|---|
| target | string | The target parameter that caused the error. |

Define the remote syslog or splunk server information

POST /security/audit/destinations

Introduced In: 9.6

Configures remote syslog/splunk server information.

Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- address

Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- port
- ipspace
- protocol
- facility
- verify_server (Can only be "true" when protocol is "tcp_encrypted")
- message_format (Can be either "legacy-netapp" or "rfc-5424")
- timestamp_format_override (Can be either "no-override", "rfc-3164", "iso-8601-utc" or "iso-8601-local-time")
- hostname_format_override (Can be either "no-override", "fqdn" or "hostname-only")

Parameters

| Name | Type | In | Required | Description |
|-------|---------|-------|----------|---|
| force | boolean | query | False | Skip the Connectivity Test <ul style="list-style-type: none"> • Default value: |

| Name | Type | In | Required | Description |
|----------------|---------|-------|----------|--|
| return_timeout | integer | query | False | <p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0 |
| return_records | boolean | query | False | <p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value: |

Request Body

| Name | Type | Description |
|---------|--------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |

| Name | Type | Description |
|---------------------------|---------|--|
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipspace | ipspace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

Example request

```
{
  "address": "string",
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "exchange",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "protocol": "string",
  "timestamp_format_override": "string"
}
```

Response

Status: 202, Accepted

| Name | Type | Description |
|------------------------|---|-------------------|
| _links | _links | |
| num_records | integer | Number of records |
| records | array[security_audit_log_forward] | |

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "address": "string",
      "facility": "string",
      "hostname_format_override": "string",
      "ipspace": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "name": "exchange",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    {
      "message_format": "string",
      "protocol": "string",
      "timestamp_format_override": "string"
    }
  ]
}
```

Headers

| Name | Description | Type |
|----------|---|--------|
| Location | Useful for tracking the resource location | string |

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 15661 | The object specified could not be found |
| 13114 | Internal error |
| 13115 | Invalid input |
| 4522285 | Server verification cannot be enabled because it requires a protocol with encryption. Encryption can be selected using the protocol field. |
| 9240603 | Cannot ping destination host. Verify connectivity to desired host or skip the connectivity check with the -force parameter. |
| 327698 | Failed to create RPC client to destination host |
| 9240609 | Cannot connect to destination host. |
| 9240604 | Cannot resolve the destination host. |

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

ipospace

| Name | Type | Description |
|--------|------------------------|--------------|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

security_audit_log_forward

| Name | Type | Description |
|--------------------------|--------------------------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipospace | ipospace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |

| Name | Type | Description |
|---------------------------|---------|--|
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| next | href | |
| self | href | |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|-------------------|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |

| Name | Type | Description |
|--------|--------|---|
| target | string | The target parameter that caused the error. |

Delete the remote syslog or splunk server information

DELETE /security/audit/destinations/{address}/{port}

Introduced In: 9.6

Deletes remote syslog/splunk server information.

Parameters

| Name | Type | In | Required | Description |
|---------|---------|------|----------|---|
| address | string | path | True | IP address of remote syslog/splunk server. |
| port | integer | path | True | Port number of remote syslog/splunk server. |

Response

Status: 200, Ok

Error

Status: Default, Error

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Retrieve the remote syslog or splunk server information

GET /security/audit/destinations/{address}/{port}

Introduced In: 9.6

Defines a remote syslog/splunk server for sending audit information to.

Parameters

| Name | Type | In | Required | Description |
|---------|---------------|-------|----------|---|
| address | string | path | True | IP address of remote syslog/splunk server. |
| port | integer | path | True | Port number of remote syslog/splunk server. |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| Name | Type | Description |
|--------------------------|-------------------------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipspace | ipspace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |

| Name | Type | Description |
|---------------------------|---------|--|
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

Example response

```
{
  "address": "string",
  "facility": "string",
  "hostname_format_override": "string",
  "ipospace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "name": "exchange",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"message_format": "string",
"protocol": "string",
"timestamp_format_override": "string"
}
```


Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

ipspace

| Name | Type | Description |
|--------|------------------------|--------------|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Update the remote syslog or splunk server information

PATCH /security/audit/destinations/{address}/{port}

Introduced In: 9.6

Updates remote syslog/splunk server information.

Parameters

| Name | Type | In | Required | Description |
|---------|---------|------|----------|---|
| address | string | path | True | IP address of remote syslog/splunk server. |
| port | integer | path | True | Port number of remote syslog/splunk server. |

Request Body

| Name | Type | Description |
|--------------------------|-------------------------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipspace | ipspace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |

| Name | Type | Description |
|---------------------------|---------|--|
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

Example request

```
{
  "address": "string",
  "facility": "string",
  "hostname_format_override": "string",
  "ipospace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "name": "exchange",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"message_format": "string",
"protocol": "string",
"timestamp_format_override": "string"
}
```

Response

Status: 200, Ok

| Name | Type | Description |
|---------------------------|---------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipspace | ipspace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

Example response

```
{
  "address": "string",
  "facility": "string",
  "hostname_format_override": "string",
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "exchange",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "message_format": "string",
  "protocol": "string",
  "timestamp_format_override": "string"
}
```

Error

Status: Default, Default

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

ipospace

| Name | Type | Description |
|--------|------------------------|--------------|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

security_audit_log_forward

| Name | Type | Description |
|--------------------------|--------------------------|--|
| address | string | Destination syslog splunk host to forward audit records to. This can be an IP address (IPv4 IPv6) or a hostname. |
| facility | string | This is the standard Syslog Facility value that is used when sending audit records to a remote server. |
| hostname_format_override | string | Syslog Hostname Format Override |
| ipospace | ipospace | |
| message_format | string | Syslog message format to be used. legacy_netapp format (variation of RFC-3164) is default message format. |

| Name | Type | Description |
|---------------------------|---------|--|
| port | integer | Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514. |
| protocol | string | Log forwarding protocol |
| timestamp_format_override | string | Syslog Timestamp Format Override. |
| verify_server | boolean | This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Copyright information

Copyright © 2024 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.