Support

REST API reference

NetApp
September 12, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9131/support_overview.html on September 12, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Support . . . 1
- Support overview . . . 1
  - Overview . . . 1
- Manage an automatic update feature . . . 1
  - Support auto-update endpoint overview . . . 1
  - Retrieve the current status of an automatic update feature . . . 3
  - Update the current enabled status of an automatic update feature . . . 6
- Retrieve automatic update configuration . . . 9
  - Support auto-update configurations endpoint overview . . . 9
  - Retrieve the configuration for an automatic update . . . 10
- Manage automatic update configuration . . . 15
  - Support auto-update configurations UUID endpoint overview . . . 15
  - Retrieve a specific configuration for an automatic update . . . 17
  - Modify the configuration for an automatic update . . . 21
- Retrieve status for all automatic updates . . . 24
  - Support auto-update updates endpoint overview . . . 24
  - Retrieve all automatic update status . . . 26
- Manage automatic updates . . . 36
  - Support auto-update updates UUID endpoint overview . . . 36
  - Retrieve the status of an update . . . 38
  - Perform an action on the update . . . 45
- Manage AutoSupport configuration . . . 47
  - Support AutoSupport endpoint overview . . . 47
  - Retrieve the AutoSupport configuration . . . 53
  - Update AutoSupport configuration for an entire cluster . . . 59
- Manage AutoSupport messages . . . 67
  - Support AutoSupport messages endpoint overview . . . 67
  - Retrieve AutoSupport message history . . . 77
  - Create and send an AutoSupport message . . . 82
- Manage cluster configuration backup information . . . 88
  - Support configuration-backup endpoint overview . . . 88
  - Retrieve cluster configuration backup information . . . 89
  - Update cluster configuration backup information . . . 91
- Manage configuration backups . . . 95
  - Support configuration-backup backups endpoint overview . . . 95
  - Retrieve configuration backup files . . . 99
  - Create a configuration backup . . . 105
  - Delete a configuration backup . . . 111
  - Retrieve configuration backup file details . . . 113
- Manage core dumps . . . 118
  - Support coredump coredumps endpoint overview . . . 118
  - Retrieve core dumps . . . 122
  - Delete a core dump . . . 128

Retrieve a core dump . . . 131
Manage EMS configuration . . . 134
Support EMS endpoint overview . . . 135
Retrieve an EMS configuration . . . 137
Update an EMS configuration . . . 140
Manage application logs . . . 144
Support EMS application-logs endpoint overview . . . 144
Create an application log . . . 146
Manage event destinations . . . 150
Support EMS destinations endpoint overview . . . 150
Retrieve a collection of event destinations . . . 154
Create an event destination . . . 166
Manage an event destination instance . . . 178
Support EMS destinations name endpoint overview . . . 178
Delete an event destination . . . 181
Retrieve an event destination . . . 183
Update an event destination . . . 191
Retrieve events . . . 204
Support EMS events endpoint overview . . . 204
Retrieve observed events . . . 206
Create or retrieve event filters . . . 212
Support EMS filters endpoint overview . . . 212
Retrieve event filters . . . 215
Create an event filter . . . 223
Manage event filters . . . 230
Support EMS filters name endpoint overview . . . 230
Delete an event filter . . . 233
Retrieve an event filter . . . 235
Update an event filter . . . 241
Create or retrieve filter rules . . . 246
Support EMS filters name rules endpoint overview . . . 246
Retrieve event filter rules . . . 248
Create an event filter rule . . . 255
Manage event filter rules . . . 261
Support EMS filters name rules index endpoint overview . . . 261
Delete an event filter rule . . . 263
Retrieve an event filter rule . . . 265
Update an event filter rule . . . 270
Manage the EMS event catalog . . . 275
Support EMS messages endpoint overview . . . 275
Retrieve event catalog definitions . . . 276
View and create EMS role configurations . . . 282
Support EMS role-configs endpoint overview . . . 282
Retrieve EMS role-based configurations . . . 285
Create role configurations . . . 289

Manage EMS role configurations . . . 293
Support EMS role-configs access_control_role.name endpoint overview . . . 293
Delete EMS role-based configurations . . . 295
Retrieve EMS role-based configurations . . . 297
Update EMS role-based configurations . . . 301
Manage cluster-wide SNMP configuration . . . 304
Support SNMP endpoint overview . . . 304
Retrieve the cluster-wide SNMP configuration . . . 306
Update the cluster-wide SNMP configuration . . . 309
Create or retrieve SNMP traphosts . . . 313
Support SNMP traphosts endpoint overview . . . 313
Retrieve SNMP traphosts . . . 316
Create SNMP traphosts . . . 322
Manage individual SNMP traphosts . . . 327
Support SNMP traphosts host endpoint overview . . . 327
Delete an SNMP traphost . . . 329
Retrieve SNMP traphost details . . . 332
Retrieve and create SNMP users . . . 336
Support SNMP users endpoint overview . . . 336
Retrieve SNMP users on a cluster . . . 339
Create a cluster-scoped or an SVM-scoped SNMP user . . . 348
Manage individual SNMP users . . . 358
Support SNMP users engine_id name endpoint overview . . . 359
Delete an SNMP user . . . 360
Retrieve SNMP user details . . . 363
Update the comment parameter of an SNMP user . . . 370

Support

Support overview

Overview

You can use ONTAP support APIs to manage configuration backups, autosupport settings, and event handling.

Configuration backups

Configuration backups are copies of node and cluster settings saved to an external server. Single-node clusters must have configuration backups as protection against corruption of the configuration database. Multi-node clusters back up the configuration automatically between the nodes in the cluster.

Manage an automatic update feature

Support auto-update endpoint overview

Overview

The Automatic Update feature helps keep the ONTAP cluster current with the latest software component updates by automatically downloading and applying them to the cluster. By enabling this feature, you agree to the following terms:

AUTOMATIC UPDATE TERMS

These Automatic Update Terms ("Terms") set forth the terms and conditions between NetApp, Inc., NetApp B.V., or any of their affiliates ("NetApp") and End User Customer ("Customer") in connection with the feature enabling Customer to receive software patches, upgrades, and updates to NetApp Software automatically ("Automatic Update"). By agreeing to and accepting Automatic Updates, Customer agrees to be bound by these Terms, as well as NetApp's End User License Agreement and Support Terms available at https://www.netapp.com/how-to-buy/sales-terms-and-conditions/.

By enabling the Automatic Update feature, Customer agrees to receive Automatic Updates that NetApp may provide from time to time, without any additional notice, and NetApp will not be liable for any damages, loss of data or loss of functionalities arising from provision of Automatic Updates. Customer may revoke acceptance of these Terms and disable the receipt of Automatic Updates by setting the feature configuration to "Disabled" in ONTAP.

Important note: When the automatic update feature is disabled

- No new updates are shown to the user
- All automatic updates currently scheduled will have their schedules cancelled.
- All automatic updates currently waiting for user confirmation cannot be started until the feature is re-enabled.

Examples

Retrieving the current status of the automatic update feature

The following example shows how to retrieve the current status of the automatic update feature:

```
# The API:
GET /support/auto-update

# The call:
curl -X GET "https://<mgmt-ip>/api/support/auto-update"

# The response:
{
"enabled": true,
"eula": {
  "accepted": true,
  "accepted_timestamp": "2020-12-01T21:24:44-04:00",
  "user_id_accepted": "admin",
  "accepted_ip_address": "192.168.1.125"
},
"_links": {
  "self": {
    "href": "/api/support/auto-update"
  }
}
}
```

Updating the status of the automatic update feature

The following example shows how to update the status of the automatic update feature:

```
# The API:
PATCH /support/auto-update

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/auto-update" -H "accept:
application/hal+json" -d '{ "enabled" : "true" }'

# The response:
200 OK
```

Retrieve the current status of an automatic update feature

GET `/support/auto-update`

Introduced In: 9.10

Retrieves the current status of the automatic update feature and the End User License Agreement (EULA).

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
enabled	boolean	Flag indicating feature state.
eula	eula	

Example response


```
{
  "_links": {
    "self": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "enabled": 1,
  "eula": {
    "accepted": 1,
    "accepted_ip_address": "192.168.1.125",
    "accepted_timestamp": "2020-12-01 13:12:23 +0000",
    "user_id_accepted": "admin"
  }
}
```

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	

self

Name	Type	Description
self	href	

_links

Name	Type	Description
self	self	

eula

Name	Type	Description
accepted	boolean	Flag indicating the End User License Agreement (EULA) acceptance. When the feature is enabled, it is assumed that the EULA is accepted.
accepted_ip_address	string	IP Address from where the EULA was accepted.
accepted_timestamp	string	Date and time when the EULA was accepted.
user_id_accepted	string	User ID that provided the EULA acceptance.

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 current enabled status of an automatic update feature

PATCH `/support/auto-update`

Introduced In: 9.10

Updates the current enabled status of the automatic update feature and accepts the EULA.

Request Body

Name	Type	Description
_links	_links	
enabled	boolean	Flag indicating feature state.
eula	eula	

Example request

```
{
  "enabled": 1,
  "eula": {
    "accepted": 1,
    "accepted_ip_address": "192.168.1.125",
    "accepted_timestamp": "2020-12-01 13:12:23 +0000",
    "user_id_accepted": "admin"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262179	Unexpected argument.
131072216	Automatic update requires AutoSupport to be enabled.
131072217	Automatic update requires AutoSupport OnDemand to be enabled.
131072218	Automatic update requires AutoSupport to use the HTTPS transport.

Definitions

See Definitions

href

Name	Type	Description
href	string	

self

_links

Name	Type	Description
self	self	

eula

Name	Type	Description
accepted	boolean	Flag indicating the End User License Agreement (EULA) acceptance. When the feature is enabled, it is assumed that the EULA is accepted.
accepted_ip_address	string	IP Address from where the EULA was accepted.
accepted_timestamp	string	Date and time when the EULA was accepted.
user_id_accepted	string	User ID that provided the EULA acceptance.

auto_update_info

Name	Type	Description
_links	_links	
enabled	boolean	Flag indicating feature state.
eula	eula	

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
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 automatic update configuration

Support auto-update configurations endpoint overview

Overview

Use this API to query and retrieve all the configurations for automatic updates.

This API only supports GET calls.

Examples

Retrieving the configuration settings for automatic updates

The following example shows how to retrieve settings for all automatic updates:

```
# The API:
GET /support/auto-update/configurations/

# The call:
curl -X GET "https://<mgmt-ip>/api/support/auto-
update/configurations?fields=*"

# The response:
{
"records": [
  {
    "uuid": "440ae2e4-fd8f-4225-9bee-94e2da3f8d9d",
    "category": "firmware",
    "description": {
      "message": "SP/BMC Firmware",
      "code": "131072402"
    },
    "action": "confirm",
  }
],
"num_records": 1
}
```

Retrieve the configuration for an automatic update

GET `/support/auto-update/configurations`

Introduced In: 9.10

Retrieves the configuration for automatic updates.

Parameters

Name	Type	In	Required	Description
category	string	query	False	Filter by category
action	string	query	False	Filter by action
uuid	string	query	False	Filter by uuid
description.message	string	query	False	Filter by description.message
description.code	string	query	False	Filter by description.code

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[auto_update_configuration]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "action": "confirm",
      "category": "disk_fw",
      "description": {
        "code": "string",
        "message": "string"
      },
      "uuid": "572361f3-e769-439d-9c04-2ba48a08ff47"
    }
  ]
}
```


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	

description

Description of the configuration row. ONTAP Message Codes

Code	Description
131072401	Storage Firmware
131072402	SP/BMC Firmware
131072403	System Files

Name	Type	Description
code	string	Argument code
message	string	Message argument

auto_update_configuration

Name	Type	Description
_links	_links	
action	string	The action to be taken by the alert source as specified by the user.
category	string	Category for the configuration row.

Name	Type	Description
description	description	Description of the configuration row. ONTAP Message Codes Code — Description 131072401 — Storage Firmware 131072402 — SP/BMC Firmware 131072403 — System Files
uuid	string	Unique identifier for the configuration row.

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.

Manage automatic update configuration

Support auto-update configurations UUID endpoint overview

Overview

Use this API to query and retrieve a specific automatic package update configuration.

This API supports GET and PATCH calls. PATCH enables the `action` field to be updated for the specified

configuration.

Examples

Retrieving settings for a specific automatic update

The following example shows how to retrieve configuration settings for an automatic update category:

```
# The API:
/support/auto-update/configurations/{uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/auto-
update/configurations/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d"

# The response:
{
"uuid": "440ae2e4-fd8f-4225-9bee-94e2da3f8d9d",
"category": "firmware",
"description": {
  "message": "SP/BMC Firmware",
  "code": "131072402"
},
"action": "confirm",
}
```

Updating the settings for a specific automatic update

The following example shows how to modify configuration settings for an automatic update:

```
# The API:
/support/auto-update/configurations/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/auto-
update/configurations/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d" -H "accept:
application/hal+json" -d '{"action":"confirm"}'

# The response:
200 OK
```

Retrieve a specific configuration for an automatic update

GET `/support/auto-update/configurations/{uuid}`

Introduced In: 9.10

Retrieves the configuration for a specified automatic update.

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Unique identifier for configuration record.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
action	string	The action to be taken by the alert source as specified by the user.
category	string	Category for the configuration row.
description	description	Description of the configuration row. ONTAP Message Codes Code — Description 131072401 — Storage Firmware 131072402 — SP/BMC Firmware 131072403 — System Files
uuid	string	Unique identifier for the configuration row.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "action": "confirm",
  "category": "disk_fw",
  "description": {
    "code": "string",
    "message": "string"
  },
  "uuid": "572361f3-e769-439d-9c04-2ba48a08ff47"
}
```


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	

description

Description of the configuration row. ONTAP Message Codes

Code	Description
131072401	Storage Firmware
131072402	SP/BMC Firmware
131072403	System Files

Name	Type	Description
code	string	Argument code
message	string	Message argument

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.

Modify the configuration for an automatic update

PATCH `/support/auto-update/configurations/{uuid}`

Introduced In: 9.10

Updates the configuration for a specified automatic update.

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Unique identifier for configuration record.

Request Body

Name	Type	Description
_links	_links	
action	string	The action to be taken by the alert source as specified by the user.
category	string	Category for the configuration row.
description	description	Description of the configuration row. ONTAP Message Codes Code — Description 131072401 — Storage Firmware 131072402 — SP/BMC Firmware 131072403 — System Files
uuid	string	Unique identifier for the configuration row.

Example request


```
{
  "action": "confirm",
  "category": "disk_fw",
  "description": {
    "code": "string",
    "message": "string"
  },
  "uuid": "572361f3-e769-439d-9c04-2ba48a08ff47"
}
```


Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262179	Unexpected argument.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

description

Description of the configuration row. ONTAP Message Codes

Code	Description
131072401	Storage Firmware
131072402	SP/BMC Firmware
131072403	System Files

Name	Type	Description
code	string	Argument code
message	string	Message argument

auto_update_configuration

Name	Type	Description
_links	_links	
action	string	The action to be taken by the alert source as specified by the user.
category	string	Category for the configuration row.
description	description	Description of the configuration row. ONTAP Message Codes Code — Description 131072401 — Storage Firmware 131072402 — SP/BMC Firmware 131072403 — System Files

Name	Type	Description
uuid	string	Unique identifier for the configuration row.

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 status for all automatic updates

Support auto-update updates endpoint overview

Overview

Use this API to retrieve the status for all the automatic package updates.

This API only supports GET calls.

Examples

Retrieving the status of all package updates

The following example shows how to retrieve the status of all automatic updates:

```
# The API:
GET /support/auto-update/updates/
```

```
# The call:
curl -X GET "https://<mgmt-ip>/api/support/auto-update/updates?fields=*"

# The response:
{
"records": [
  {
    "uuid" : "440ae2e4-fd8f-4225-9bee-94e2da3f8d9d",
    "package_id" : "572361f3-e769-439d-9c04-2ba48a08ff47",
    "content_type" : "disk_fw",
    "content_category" : "firmware",
    "description" : "disk_fw version 3.0",
    "state" : "downloading",
    "creation_time" : "2020-12-01T09:12:03Z",
    "expiry_time" : "2021-06-01T09:12:03Z",
    "last_state_change_time" : "2020-12-01T09:12:23Z",
    "start_time": "2020-12-01T09:12:23Z",
    "percent_complete": 25,
    "remaining_time": "PT1M30S",
    "_links": {
      "self": {
        "href": "/support/auto-update/updates/440ae2e4-fd8f-4225-9bee-
94e2da3f8d9d"
      }
    }
  },
  {
    "uuid" : "440ae2e4-fd8f-4225-9bee-94e2da3f9d8d",
    "package_id" : "e2e12753-8501-11e8-a7c1-00505695c997",
    "content_type" : "disk_fw",
    "content_category" : "firmware",
    "description" : "disk_fw version 3.1",
    "state" : "pending_confirmation",
    "creation_time" : "2020-12-01T09:12:03Z",
    "expiry_time" : "2021-06-01T09:12:03Z",
    "last_state_change_time" : "2020-12-01T09:12:23Z",
    "start_time": "2020-12-01T09:12:23Z",
    "_links": {
      "self": {
        "href": "/support/auto-update/updates/440ae2e4-fd8f-4225-9bee-
94e2da3f8d9d"
      }
    }
  },
  {
    "uuid" : "440ae2e4-fd8f-4225-9aeb-94e2da3f8ef9",
```

```
    "package_id" : "e2e12753-8501-11e8-a7c1-00505695c997",
    "content_type" : "shelf_fw",
    "content_category" : "Firmware",
    "description" : "shelf_fw version 4.0",
    "state" : "applying",
    "creation_time" : "2020-12-01T09:11:53Z",
    "expiry_time" : "2021-06-01T09:12:03Z",
    "last_state_change_time" : "2020-12-01T09:12:13Z",
    "start_time": "2020-12-01T09:12:23Z",
    "percent_complete": 85,
    "remaining_time": "PT30S",
    "_links": {
      "self": {
        "href": "/support/auto-update/updates/440ae2e4-fd8f-4225-9aeb-
94e2da3f8ef9"
      }
    }
  }
],
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/support/auto-update/updates?fields=*"
  }
}
}
```


Retrieve all automatic update status

GET `/support/auto-update/updates`

Introduced In: 9.10

Retrieves the status of all updates.

Parameters

Name	Type	In	Required	Description
status.arguments.message	string	query	False	Filter by status.arguments.message
status.arguments.code	string	query	False	Filter by status.arguments.code

Name	Type	In	Required	Description
status.message	string	query	False	Filter by status.message
status.code	string	query	False	Filter by status.code
status.target	string	query	False	Filter by status.target
remaining_time	string	query	False	Filter by remaining_time
uuid	string	query	False	Filter by uuid
state	string	query	False	Filter by state
scheduled_time	string	query	False	Filter by scheduled_time
end_time	string	query	False	Filter by end_time
start_time	string	query	False	Filter by start_time
expiry_time	string	query	False	Filter by expiry_time
percent_complete	integer	query	False	Filter by percent_complete
description	string	query	False	Filter by description
creation_time	string	query	False	Filter by creation_time
content_type	string	query	False	Filter by content_type
package_id	string	query	False	Filter by package_id
last_state_change_time	string	query	False	Filter by last_state_change_time
content_category	string	query	False	Filter by content_category

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[auto_update_status]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "action": "schedule_now",
      "content_category": "Firmware",
      "content_type": "disk_fw",
      "creation_time": "2020-12-01 09:12:23 +0000",
      "description": "disk_fw version 3.0",
      "end_time": "2020-12-01 09:12:23 +0000",
      "expiry_time": "2021-06-01 09:12:23 +0000",
      "last_state_change_time": "2020-12-01 09:12:23 +0000",
      "package_id": "572361f3-e769-439d-9c04-2ba48a08ff47",
      "percent_complete": 85,
      "remaining_time": "PT1H45M13S",
      "schedule_time": "2020-12-20 21:00:00 +0000",
      "scheduled_time": "2020-12-05 09:12:23 +0000",
      "start_time": "2020-12-01 09:12:23 +0000",
      "state": "pending_confirmation",
      "status": {
        "arguments": [
          {
            "code": "string",
            "message": "string"
          }
        ],
        "code": "4",
        "message": "entry doesn't exist",
        "target": "uuid"
```

```
        },
        "uuid": "440ae2e4-fd8f-4225-9bee-94e2da3f9d8d"
      }
    ]
}
```


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	

self

Name	Type	Description
self	href	

_links

Name	Type	Description
self	self	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

status

Status of the update. ONTAP Message Codes

Code	Description
8650878	Get-url request to AutoSupport OnDemand Server failed.
131072105	Package installation successful.
131072106	Package installation failed.
131072107	Package installation is in progress.
131072108	An internal error occurred.
131072109	No errors found.
131072110	Failed to extract package.

Code	Description
131072111	Failed to create entry in status table.
131072209	Failed to download package.
131072210	Failed to obtain download links. Will be retried.
131072211	Installation cannot start because the following nodes are not up. Will be retried.
131072212	Automatic update cannot start. Will be retried.
131072213	Installation complete.
131072214	Installation in progress.
131072215	Scheduled to start.
131072301	Unable to create directory.
131072302	Update not required. It is already on the target firmware version.
131072303	Unable to move installable to installation location.
131072304	Successfully updated. All nodes already updated and skipped.
131072306	Firmware distribution starting.
131072307	Firmware distribution restarting.
131072308	Firmware distribution failed.
131072309	Firmware installation successful on node.
131072310	Firmware installable is corrupt on node.
131072311	Could not apply firmware update on nodes.
131072312	Firmware update operation failed.
131072313	Install failed to initiate on node.
131072314	Install initiated on node.
131072315	Install failed on node.
131072316	Update in progress on node.
131072317	Unexpected state occurred during firmware installation on node.
131072318	Successfully updated SP/BMC firmware.
131072319	Backup SP image is running. Firmware installation failed prematurely on node.
131072320	SP rebooted with an unexpected firmware version on node.
131072321	Waiting for shelf firmware to update.
131072322	Update complete.

Code	Description
131072323	Shelf update timed out.
131072324	Successfully updated shelves on nodes.
131072325	Waiting for disk firmware to update.
131072326	Disk update completed.
131072327	Disk update timed out.
131072328	Successfully updated disks on nodes.
131072329	Waiting for DQP firmware to update.
131072330	Successfully updated DQP on nodes.
131072331	DQP update timed out.
131072332	Failed to copy firmware.

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.

auto_update_status

Name	Type	Description
_links	_links	
action	string	Action to be applied to the automatic update.
content_category	string	Category of the update
content_type	string	Image or package type.
creation_time	string	The date and time at which the update request was received.
description	string	Description of the update.

Name	Type	Description
end_time	string	The date and time at which the update request processing ended.
expiry_time	string	The date and time at which the update request will expire.
last_state_change_time	string	The date and time at which the state of the update changed last.
package_id	string	Unique identifier provided by the back-end.
percent_complete	integer	Percentage of update completed
remaining_time	string	The time remaining for the update processing to complete in an ISO-8601 duration formatted string.
schedule_time	string	Date and time when an automatic update action is scheduled. This field is required when the action field is set to "schedule".
scheduled_time	string	The date and time at which the update request is currently scheduled for.
start_time	string	The date and time at which the update request processing started.
state	string	Current state of the update.

Name	Type	Description
status	status	Status of the update. ONTAP Message Codes Code — Description 8650878 — Get-url request to AutoSupport OnDemand Server failed. 131072105 — Package installation successful. 131072106 — Package installation failed. 131072107 — Package installation is in progress. 131072108 — An internal error occurred. 131072109 — No errors found. 131072110 — Failed to extract package. 131072111 — Failed to create entry in status table. 131072209 — Failed to download package. 131072210 — Failed to obtain download links. Will be retried. 131072211 — Installation cannot start because the following nodes are not up. Will be retried. 131072212 — Automatic update cannot start. Will be retried. 131072213 — Installation complete. 131072214 — Installation in progress. 131072215 — Scheduled to start. 131072301 — Unable to create directory. 131072302 — Update not required. It is already on the target firmware version.

Name	Type	Description
uuid	string	Unique identifier for this update.

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.

131072304 — Successfully updated. All nodes already

131072310 — Firmware installable is corrupt on node.

131072311 — Could not apply firmware update on nodes.

131072312 — Firmware update operation failed.

131072313 — Install failed to initiate on node.

131072314 — Install initiated on node.

131072315 — Install failed on node.

131072316 — Update in progress on node.

131072317 — Unexpected state occurred during firmware installation on node.

131072318 — Successfully updated SP/BMC firmware.

131072319 — Backup SP image is running. Firmware installation failed prematurely on node.

131072320 — SP rebooted with an unexpected firmware version on node.

131072321 — Waiting for shelf firmware to update.

Manage automatic updates

Support auto-update updates UUID endpoint overview

Overview

Use this API to retrieve the status for a specific automatic package update.

This API supports GET and PATCH calls. PATCH can be used to perform an action on an automatic update.

Examples

Retrieving the status of an update

The following example shows how to retrieve the status of an automatic update:

```
# The API:
GET /support/auto-update/updates/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d

# The call:
curl -X GET "https://<mgmt-ip>/api/support/auto-update/updates/440ae2e4-
fd8f-4225-9bee-94e2da3f8d9d"

# The response:
{
"uuid" : "440ae2e4-fd8f-4225-9bee-94e2da3f8d9d",
"package_id" : "572361f3-e769-439d-9c04-2ba48a08ff47",
"content_type" : "disk_fw",
"content_category" : "Firmware",
"description" : "disk_fw version 3.0",
"state" : "downloading",
"creation_time" : "2020-12-01T09:12:03Z",
"expiry_time" : "2021-06-01T09:12:03Z",
"last_state_change_time" : "2020-12-01T09:12:23Z",
"start_time" : "2020-12-01T09:12:23Z",
"percent_complete": 25,
"remaining_time": "PT1M30S",
"status": {
    "message": "Get-url request to AutoSupport OnDemand Server failed.
Error: Couldn't connect to server.",
    "code": "8650878"
},
"_links": {
  "self": {
    "href": "/support/auto-update/updates/440ae2e4-fd8f-4225-9bee-
94e2da3f8d9d"
  }
}
}
```

Updating the state of an automatic update

The following example shows how to trigger an automatic update that is waiting for user confirmation:

```
# The API:
PATCH /support/auto-update/updates/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/auto-update/updates/440ae2e4-
fd8f-4225-9bee-94e2da3f8d9d?action=schedule_now" -H "accept:
application/hal+json"

# The response:
200 OK
```

The following example shows how to dismiss an automatic update that is waiting for user confirmation:

```
# The API:
PATCH /support/auto-update/updates/440ae2e4-fd8f-4225-9bee-94e2da3f8d9d

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/auto-update/updates/440ae2e4-
fd8f-4225-9bee-94e2da3f8d9d?action=dismiss" -H "accept:
application/hal+json"

# Response
200 OK
```

Retrieve the status of an update

GET `/support/auto-update/updates/{uuid}`

Introduced In: 9.10

Retrieves the status of an update.

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Update identifier
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
action	string	Action to be applied to the automatic update.
content_category	string	Category of the update
content_type	string	Image or package type.
creation_time	string	The date and time at which the update request was received.
description	string	Description of the update.
end_time	string	The date and time at which the update request processing ended.
expiry_time	string	The date and time at which the update request will expire.
last_state_change_time	string	The date and time at which the state of the update changed last.
package_id	string	Unique identifier provided by the back-end.
percent_complete	integer	Percentage of update completed
remaining_time	string	The time remaining for the update processing to complete in an ISO-8601 duration formatted string.
schedule_time	string	Date and time when an automatic update action is scheduled. This field is required when the action field is set to "schedule".
scheduled_time	string	The date and time at which the update request is currently scheduled for.
start_time	string	The date and time at which the update request processing started.
state	string	Current state of the update.

Name	Type	Description
status	status	Status of the update. ONTAP Message Codes Code — Description 8650878 — Get-url request to AutoSupport OnDemand Server failed. 131072105 — Package installation successful. 131072106 — Package installation failed. 131072107 — Package installation is in progress. 131072108 — An internal error occurred. 131072109 — No errors found. 131072110 — Failed to extract package. 131072111 — Failed to create entry in status table. 131072209 — Failed to download package. 131072210 — Failed to obtain download links. Will be retried. 131072211 — Installation cannot start because the following nodes are not up. Will be retried. 131072212 — Automatic update cannot start. Will be retried. 131072213 — Installation complete. 131072214 — Installation in progress. 131072215 — Scheduled to start. 131072301 — Unable to create directory. 131072302 — Update not required. It is already on the target firmware version. 131072303 — Unable to move

Name	Type	Description
uuid	string	Unique identifier for this update.

131072304 — Successfully updated. All nodes already updated and skipped

Example response


```
{
  "_links": {
    "self": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "action": "schedule_now",
  "content_category": "Firmware",
  "content_type": "disk_fw",
  "creation_time": "2020-12-01 09:12:23 +0000",
  "description": "disk_fw version 3.0",
  "end_time": "2020-12-01 09:12:23 +0000",
  "expiry_time": "2021-06-01 09:12:23 +0000",
  "last_state_change_time": "2020-12-01 09:12:23 +0000",
  "package_id": "572361f3-e769-439d-9c04-2ba48a08ff47",
  "percent_complete": 85,
  "remaining_time": "PT1H45M13S",
  "schedule_time": "2020-12-20 21:00:00 +0000",
  "scheduled_time": "2020-12-05 09:12:23 +0000",
  "start_time": "2020-12-01 09:12:23 +0000",
  "state": "pending_confirmation",
  "status": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "uuid": "440ae2e4-fd8f-4225-9bee-94e2da3f9d8d"
}
```


unexpected firmware version on node.

131072321 — Waiting for shelf firmware to update.

131072322 — Update complete.

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	

self

Name	Type	Description
self	href	

_links

Name	Type	Description
self	self	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

status

Status of the update. ONTAP Message Codes

Code	Description
8650878	Get-url request to AutoSupport OnDemand Server failed.
131072105	Package installation successful.
131072106	Package installation failed.
131072107	Package installation is in progress.
131072108	An internal error occurred.
131072109	No errors found.
131072110	Failed to extract package.
131072111	Failed to create entry in status table.
131072209	Failed to download package.
131072210	Failed to obtain download links. Will be retried.
131072211	Installation cannot start because the following nodes are not up. Will be retried.

Code	Description
131072212	Automatic update cannot start. Will be retried.
131072213	Installation complete.
131072214	Installation in progress.
131072215	Scheduled to start.
131072301	Unable to create directory.
131072302	Update not required. It is already on the target firmware version.
131072303	Unable to move installable to installation location.
131072304	Successfully updated. All nodes already updated and skipped.
131072306	Firmware distribution starting.
131072307	Firmware distribution restarting.
131072308	Firmware distribution failed.
131072309	Firmware installation successful on node.
131072310	Firmware installable is corrupt on node.
131072311	Could not apply firmware update on nodes.
131072312	Firmware update operation failed.
131072313	Install failed to initiate on node.
131072314	Install initiated on node.
131072315	Install failed on node.
131072316	Update in progress on node.
131072317	Unexpected state occurred during firmware installation on node.
131072318	Successfully updated SP/BMC firmware.
131072319	Backup SP image is running. Firmware installation failed prematurely on node.
131072320	SP rebooted with an unexpected firmware version on node.
131072321	Waiting for shelf firmware to update.
131072322	Update complete.
131072323	Shelf update timed out.
131072324	Successfully updated shelves on nodes.
131072325	Waiting for disk firmware to update.
131072326	Disk update completed.
131072327	Disk update timed out.

Code	Description
131072328	Successfully updated disks on nodes.
131072329	Waiting for DQP firmware to update.
131072330	Successfully updated DQP on nodes.
131072331	DQP update timed out.
131072332	Failed to copy firmware.

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.

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.

Perform an action on the update

PATCH `/support/auto-update/updates/{uuid}`

Introduced In: 9.10

Perform an action on the update.

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Update identifier

Name	Type	In	Required	Description
action	string	query	True	Action to be performed on the update • enum: ["cancel_schedule", "dismiss", "schedule", "schedule_now", "abort", "undismiss"]
schedule_time	string	query	False	Date and Time for which update is to be scheduled. This parameter is required only when action is "schedule". It should be in the ISO-8601 Date and Time format. Example- "2020-12-05T09:12:23Z". • format: date-time

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
262248	Unexpected parameter missing a delimiter.
131072200	Invalid Automatic Update ID.
131072201	No schedule to cancel for automatic update ID.
131072202	Cannot abort an automatic update that is not in progress.
131072203	Cannot dismiss a non-pending automatic update.

Error Code	Description
131072204	Cannot reactivate an automatic update that has not been dismissed.
131072205	Cannot schedule a non-pending automatic update to start.
131072206	Cannot schedule an automatic update past its expiration date.
131072207	Cannot schedule an automatic update in the past.
131072208	Cannot schedule automatic update while the feature is disabled.

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.

Manage AutoSupport configuration

Support AutoSupport endpoint overview

Overview

AutoSupport is the NetApp *call home* mechanism. AutoSupport sends configuration details, status details, and error reporting details to NetApp.

This endpoint supports both GET and PATCH calls. GET is used to retrieve AutoSupport configuration details for the cluster and PATCH is used to modify the AutoSupport configuration of the cluster. You can also use GET calls to check AutoSupport connectivity.

Examples

Configuring 'to' addresses

The following example configures AutoSupport to send emails to 'to' addresses.

```
# The API:
PATCH /support/autosupport

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/autosupport" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"to\": [
\"abc@netapp.com\", \"xyz@netapp.com\" ]}"

# The response:
200 OK
{}
```

Configuring 'SMTP' transport

The following example configures AutoSupport to use 'SMTP' transport. The default transport is 'HTTPS'.

```
# The API:
PATCH /support/autosupport

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/autosupport" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"transport\": \"smtp\"}"

# The response:
200 OK
{}
```

Retrieving the AutoSupport configuration

The following example retrieves AutoSupport configuration for the cluster.

```
# The API:
GET /support/autosupport

# The call:
curl -X GET "https://<mgmt-ip>/api/support/autosupport" -H "accept:
application/hal+json"

# The response:
200 OK
{
"enabled": true,
"mail_hosts": [
  "mailhost"
],
"from": "Postmaster",
"to": [
  "abc@netapp.com",
  "xyz@netapp.com"
],
"contact_support": true,
"transport": "smtp",
"proxy_url": "",
"is_minimal": false,
"_links": {
  "self": {
    "href": "/api/support/autosupport"
  }
}
}
```

Retrieving AutoSupport connectivity issues

The following example retrieves AutoSupport connectivity issues for the cluster. The `fields=issues` parameter must be specified, for the response to return connectivity issues. The `corrective_action` section might contain commands which needs to be executed on the ONTAP CLI.

Note that the connectivity check can take up to 10 seconds to complete.

```
# The API:
GET /support/autosupport

# The call:
curl -X GET "https://<mgmt-ip>/api/support/autosupport?fields=issues" -H
"accept: application/hal+json"
```

```
# The response:
200 OK
{
"issues": [
  {
    "node": {
      "name": "node3",
      "uuid": "0ecfd0a6-f1b3-11e8-9d9f-005056bbaadc",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/0ecfd0a6-f1b3-11e8-9d9f-
005056bbaadc"
        }
      }
    },
    "issue": {
      "message": "SMTP connectivity check failed for destination:
mailhost. Error: Could not resolve host - 'mailhost'",
      "code": "53149746"
    },
    "corrective_action": {
      "message": "Check the hostname of the SMTP server",
      "code": "53149746"
    }
  },
  {
    "node": {
      "name": "node3",
      "uuid": "0ecfd0a6-f1b3-11e8-9d9f-005056bbaadc",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/0ecfd0a6-f1b3-11e8-9d9f-
005056bbaadc"
        }
      }
    },
    "issue": {
      "message": "AutoSupport OnDemand is disabled when \"-transport\" is
not set to \"https\".",
      "code": "53149740"
    },
    "corrective_action": {
      "message": "Run \"system node autosupport modify -transport https
-node <node name>\" to set \"-transport\" to \"https\".",
      "code": "53149740"
```

```
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport"
  }
}
}
```

Retrieving AutoSupport configuration and connectivity issues

The following example retrieves AutoSupport configuration and connectivity issues on the cluster. Use `fields=*,issues` parameter to return both configuration and connectivity issues.

```
# The API:
GET /support/autosupport

# The call:
curl -X GET "https://<mgmt-ip>/api/support/autosupport?fields=*%2Cissues"
-H "accept: application/hal+json"

# The response:
200 OK
{
"enabled": true,
"mail_hosts": [
  "mailhost"
],
"from": "Postmaster",
"to": [
  "abc@netapp.com",
  "xyz@netapp.com"
],
"contact_support": true,
"transport": "smtp",
"proxy_url": "",
"is_minimal": false,
"issues": [
  {
    "node": {
      "name": "node3",
      "uuid": "0ecfd0a6-f1b3-11e8-9d9f-005056bbaadc",
      "_links": {
```

```
        "self": {
          "href": "/api/cluster/nodes/0ecfd0a6-f1b3-11e8-9d9f-
005056bbaadc"
        }
      }
    },
    "issue": {
      "message": "SMTP connectivity check failed for destination:
mailhost. Error: Could not resolve host - 'mailhost'",
      "code": "53149746"
    },
    "corrective_action": {
      "message": "Check the hostname of the SMTP server",
      "code": "53149746"
    }
  },
  {
    "node": {
      "name": "node3",
      "uuid": "0ecfd0a6-f1b3-11e8-9d9f-005056bbaadc",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/0ecfd0a6-f1b3-11e8-9d9f-
005056bbaadc"
        }
      }
    },
    "issue": {
      "message": "AutoSupport OnDemand is disabled when \"-transport\" is
not set to \"https\".",
      "code": "53149740"
    },
    "corrective_action": {
      "message": "Run \"system node autosupport modify -transport https
-node <node name>\" to set \"-transport\" to \"https\".",
      "code": "53149740"
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport"
  }
}
}
```

Retrieve the AutoSupport configuration

GET `/support/autosupport`

Introduced In: 9.6

Retrieves the AutoSupport configuration of the cluster and if requested, returns connectivity issues with the AutoSupport configuration.

Important note:

- The **issues** field consists of a list of objects containing details of the node that has a connectivity issue, the issue description, and corrective action you can take to address the issue. When not empty, this indicates a connection issue to the **HTTP/S**, **SMTP**, or **AutoSupport On Demand** server.

Expensive properties

There is an added computational cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See Requesting specific fields to learn more.

- `issues`

Related ONTAP commands

- `system node autosupport show -instance`
- `system node autosupport check show-details`

Learn more

- DOC /support/autosupport

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
contact_support	boolean	Specifies whether to send the AutoSupport messages to vendor support.

Name	Type	Description
enabled	boolean	Specifies whether the AutoSupport daemon is enabled. When this setting is disabled, delivery of all AutoSupport messages is turned off.
from	string	The e-mail address from which the AutoSupport messages are sent. To generate node-specific 'from' addresses, enable '-node-specific-from' parameter via ONTAP CLI. • example: postmaster@example.com • format: email • Introduced in: 9.6 • x-nullable: true
is_minimal	boolean	Specifies whether the system information is collected in compliant form, to remove private data or in complete form, to enhance diagnostics.
issues	array[autosupport_issues]	A list of nodes in the cluster with connectivity issues to HTTP/SMTP/AOD AutoSupport destinations along with the corresponding error descriptions and corrective actions.
mail_hosts	array[string]	The names of the mail servers used to deliver AutoSupport messages via SMTP.
partner_addresses	array[string]	The list of partner addresses.
proxy_url	string	Proxy server for AutoSupport message delivery via HTTP/S. Optionally specify a username/password for authentication with the proxy server.
to	array[string]	The e-mail addresses to which the AutoSupport messages are sent.

Name	Type	Description
transport	string	The name of the transport protocol used to deliver AutoSupport messages. Support for 'http' transport has been deprecated and is no longer supported by AutoSupport servers.

Example response


```
{
  "contact_support": 1,
  "enabled": 1,
  "from": "<a href="
mailto:postmaster@example.com">postmaster@example.com</a>",
  "is_minimal": 1,
  "issues": [
    {
      "corrective_action": {
        "code": "53149746",
        "message": "Check the hostname of the SMTP server"
      },
      "issue": {
        "code": "53149746",
        "message": "SMTP connectivity check failed for destination:
mailhost. Error: Could not resolve host - 'mailhost'"
      },
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "mail_hosts": [
    "mailhost1.example.com",
    "mailhost2.example.com"
  ],
  "partner_addresses": [
    "<a href="mailto:user1@partner.com">user1@partner.com</a>",
    "<a href="mailto:user2@partner.com">user2@partner.com</a>"
  ],
  "proxy_url": "https://proxy.company.com",
  "to": [
    "<a href="mailto:user1@example.com">user1@example.com</a>",
    "<a href="mailto:user2@example.com">user2@example.com</a>"
  ],
  "transport": "smtp"
}
```

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

autosupport_connectivity_corrective_action

Name	Type	Description
code	string	Corrective action code
message	string	Corrective action message. The corrective action might contain commands which needs to be executed on the ONTAP CLI. • example: Check the hostname of the SMTP server • readOnly: 1 • Introduced in: 9.6 • x-nullable: true

autosupport_connectivity_issue

Name	Type	Description
code	string	Error code
message	string	Error message

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

autosupport_issues

Name	Type	Description
corrective_action	autosupport_connectivity_corrective_action	
issue	autosupport_connectivity_issue	
node	node	

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 AutoSupport configuration for an entire cluster

PATCH `/support/autosupport`

Introduced In: 9.6

Updates the AutoSupport configuration for the entire cluster.

Related ONTAP commands

- `system node autosupport modify`

Learn more

- DOC /support/autosupport

Request Body

Name	Type	Description
contact_support	boolean	Specifies whether to send the AutoSupport messages to vendor support.
enabled	boolean	Specifies whether the AutoSupport daemon is enabled. When this setting is disabled, delivery of all AutoSupport messages is turned off.
from	string	The e-mail address from which the AutoSupport messages are sent. To generate node-specific 'from' addresses, enable '-node-specific-from' parameter via ONTAP CLI. • example: postmaster@example.com • format: email • Introduced in: 9.6 • x-nullable: true
is_minimal	boolean	Specifies whether the system information is collected in compliant form, to remove private data or in complete form, to enhance diagnostics.
issues	array[autosupport_issues]	A list of nodes in the cluster with connectivity issues to HTTP/SMTP/AOD AutoSupport destinations along with the corresponding error descriptions and corrective actions.
mail_hosts	array[string]	The names of the mail servers used to deliver AutoSupport messages via SMTP.
partner_addresses	array[string]	The list of partner addresses.
proxy_url	string	Proxy server for AutoSupport message delivery via HTTP/S. Optionally specify a username/password for authentication with the proxy server.

Name	Type	Description
to	array[string]	The e-mail addresses to which the AutoSupport messages are sent.
transport	string	The name of the transport protocol used to deliver AutoSupport messages. Support for 'http' transport has been deprecated and is no longer supported by AutoSupport servers.

Example request


```
{
  "contact_support": 1,
  "enabled": 1,
  "from": "<a href="
mailto:postmaster@example.com">postmaster@example.com</a>",
  "is_minimal": 1,
  "issues": [
    {
      "corrective_action": {
        "code": "53149746",
        "message": "Check the hostname of the SMTP server"
      },
      "issue": {
        "code": "53149746",
        "message": "SMTP connectivity check failed for destination:
mailhost. Error: Could not resolve host - 'mailhost'"
      },
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ],
  "mail_hosts": [
    "mailhost1.example.com",
    "mailhost2.example.com"
  ],
  "partner_addresses": [
    "<a href="mailto:user1@partner.com">user1@partner.com</a>",
    "<a href="mailto:user2@partner.com">user2@partner.com</a>"
  ],
  "proxy_url": "https://proxy.company.com",
  "to": [
    "<a href="mailto:user1@example.com">user1@example.com</a>",
    "<a href="mailto:user2@example.com">user2@example.com</a>"
  ],
  "transport": "smtp"
}
```


Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
8650862	The SMTP mail host provided cannot be empty
8650863	A maximum of 5 SMTP mail hosts can be provided
8650864	A maximum of 5 email addresses can be provided
8650865	A maximum of 5 partner email addresses can be provided
8650880	Automatic update requires AutoSupport to be enabled.
8650881	Automatic update requires AutoSupport to use the HTTPS transport.
8650882	Automatic update requires AutoSupport OnDemand to be enabled.
53149727	The proxy URI provided is invalid
53149728	The mailhost URI provided is invalid

Definitions

See Definitions

autosupport_connectivity_corrective_action

Name	Type	Description
code	string	Corrective action code
message	string	Corrective action message. The corrective action might contain commands which needs to be executed on the ONTAP CLI. • example: Check the hostname of the SMTP server • readOnly: 1 • Introduced in: 9.6 • x-nullable: true

autosupport_connectivity_issue

Name	Type	Description
code	string	Error code
message	string	Error message

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

autosupport_issues

Name	Type	Description
corrective_action	autosupport_connectivity_corrective_action	

Name	Type	Description
issue	autosupport_connectivity_issue	
node	node	

autosupport

Name	Type	Description
contact_support	boolean	Specifies whether to send the AutoSupport messages to vendor support.
enabled	boolean	Specifies whether the AutoSupport daemon is enabled. When this setting is disabled, delivery of all AutoSupport messages is turned off.
from	string	The e-mail address from which the AutoSupport messages are sent. To generate node-specific 'from' addresses, enable '-node-specific-from' parameter via ONTAP CLI. • example: postmaster@example.com • format: email • Introduced in: 9.6 • x-nullable: true
is_minimal	boolean	Specifies whether the system information is collected in compliant form, to remove private data or in complete form, to enhance diagnostics.
issues	array[autosupport_issues]	A list of nodes in the cluster with connectivity issues to HTTP/SMTP/AOD AutoSupport destinations along with the corresponding error descriptions and corrective actions.
mail_hosts	array[string]	The names of the mail servers used to deliver AutoSupport messages via SMTP.

Name	Type	Description
partner_addresses	array[string]	The list of partner addresses.
proxy_url	string	Proxy server for AutoSupport message delivery via HTTP/S. Optionally specify a username/password for authentication with the proxy server.
to	array[string]	The e-mail addresses to which the AutoSupport messages are sent.
transport	string	The name of the transport protocol used to deliver AutoSupport messages. Support for 'http' transport has been deprecated and is no longer supported by AutoSupport servers.

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.

Manage AutoSupport messages

Support AutoSupport messages endpoint overview

Overview

Use this API to invoke and retrieve AutoSupport messages from the nodes in the cluster.

This API supports POST and GET calls. Use a POST call to invoke AutoSupport and a GET call to retrieve AutoSupport messages.

Examples

Invoking an AutoSupport on all nodes in the cluster

The following example invokes an AutoSupport on every node in the cluster. Note that AutoSupport is invoked on all nodes in the cluster if the `node` parameter is omitted. Also, note that the `subject` line is the same when invoking on all nodes.

By default, the response is an empty object. If `return_records=true` is passed in the request, the response includes information about the node and the index of the invoked AutoSupport message.

```
# The API:
POST /support/autosupport/messages

# The call:
curl -X POST "https://<mgmt-
ip>/api/support/autosupport/messages?return_records=true" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"
message\": \"test_msg\", \"type\": \"all\"}"

# The response:
201 CREATED
{
"num_records": 2,
"records": [
  {
    "index": 4,
    "node": {
      "name": "node1",
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
```

```
    },
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/4"
      }
    }
  },
  {
    "index": 2,
    "node": {
      "name": "node2",
      "uuid": "e47d2630-f250-11e8-b186-005056bb5cab",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/e47d2630-f250-11e8-b186-
005056bb5cab"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/e47d2630-f250-11e8-
b186-005056bb5cab/2"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport/messages/"
  }
}
}
```


Invoking an AutoSupport on a single node

The following examples invoke an AutoSupport on a single node in the cluster. Note that AutoSupport is invoked on all nodes in the cluster if the `node` parameter is omitted. You can specify the node-name with either `node` or `node.name` parameter. You can also specify UUID of the node with the `node.uuid` parameter.

By default, the response is an empty object. If `return_records=true` is passed in the request, the response includes information about the node and the index of the invoked AutoSupport message.

```
# The API:
POST /support/autosupport/messages

# The call:
curl -X POST "https://<mgmt-
ip>/api/support/autosupport/messages?return_records=true" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"message\": \"test_msg\", \"type\": \"test\", \"node\": { \"name\":
\"node1\" }}"

# The response:
201 CREATED
{
"num_records": 1,
"records": [
  {
    "index": 8,
    "node": {
      "name": "node1",
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/8"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport/messages/"
  }
}
}
```

```
# The call:
curl -X POST "https://<mgmt-
ip>/api/support/autosupport/messages?return_records=true" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"message\": \"test_msg\", \"type\": \"test\", \"node.name\":\"node2\"}"

# The response:
201 CREATED
{
"num_records": 1,
"records": [
  {
    "index": 4,
    "node": {
      "name": "node2",
      "uuid": "e47d2630-f250-11e8-b186-005056bb5cab",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/e47d2630-f250-11e8-b186-
005056bb5cab"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/e47d2630-f250-11e8-
b186-005056bb5cab/4"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport/messages/"
  }
}
}
```

```
# The call:
curl -X POST "https://<mgmt-
ip>/api/support/autosupport/messages?return_records=true" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"message\": \"test_msg\", \"type\": \"test\", \"node.uuid\":\"092e0298-
f250-11e8-9a05-005056bb6666\"}"

# The response:
201 CREATED
{
"num_records": 1,
"records": [
  {
    "index": 5,
    "node": {
      "name": "node1",
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/5"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/autosupport/messages/"
  }
}
}
```

Retrieving AutoSupport messages from all nodes in the cluster

The following example retrieves AutoSupport messages from every node in the cluster. Note that if the *fields=** parameter is not specified, only node, index, and destination fields are returned. Filters can be added on the fields to limit the results.

```
# The API:
GET /support/autosupport/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/support/autosupport/messages?fields=*&return_timeout=15" -H
"accept: application/hal+json"

# The response:
200 OK
{
"records": [
  {
    "node": {
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
    },
    "index": 1,
    "destination": "smtp",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "ignore",
    "generated_on": "2019-03-28T10:18:04-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/1/smtp"
      }
    }
  },
  {
    "node": {
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
```

```
    },
    "index": 1,
    "destination": "http",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "sent_successful",
    "generated_on": "2019-03-28T10:18:04-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/1/http"
      }
    }
  },
  {
    "node": {
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
    },
    "index": 1,
    "destination": "noteto",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "ignore",
    "generated_on": "2019-03-28T10:18:04-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/1/noteto"
      }
    }
  },
  {
    "node": {
      "uuid": "e47d2630-f250-11e8-b186-005056bb5cab",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/e47d2630-f250-11e8-b186-
005056bb5cab"
        }
      }
```

```
    },
    "index": 1,
    "destination": "smtp",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "ignore",
    "generated_on": "2019-03-28T10:18:06-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/e47d2630-f250-11e8-
b186-005056bb5cab/1/smtp"
      }
    }
  },
  {
    "node": {
      "uuid": "e47d2630-f250-11e8-b186-005056bb5cab",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/e47d2630-f250-11e8-b186-
005056bb5cab"
        }
      }
    },
    "index": 1,
    "destination": "http",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "sent_successful",
    "generated_on": "2019-03-28T10:18:06-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/e47d2630-f250-11e8-
b186-005056bb5cab/1/http"
      }
    }
  },
  {
    "node": {
      "uuid": "e47d2630-f250-11e8-b186-005056bb5cab",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/e47d2630-f250-11e8-b186-
005056bb5cab"
        }
      }
```

```
    },
    "index": 1,
    "destination": "noteto",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "ignore",
    "generated_on": "2019-03-28T10:18:06-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/e47d2630-f250-11e8-
b186-005056bb5cab/1/noteto"
      }
    }
  }
],
"num_records": 6,
"_links": {
  "self": {
    "href": "/api/support/autosupport/messages?fields=*&return_timeout=15"
  }
}
}
```


Retrieving AutoSupport messages from a specific node and has 'sent_successful' state

The following example retrieves AutoSupport messages from a specific node in the cluster. Note that if the `fields=*` parameter is not specified, only node, index, and destination fields are returned. This example uses a filter on the `node.name` and `state` fields. You can add filters to any fields in the response.

```
# The API:
GET /support/autosupport/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/support/autosupport/messages?node.name=node1&state=sent_successful
&fields=*&return_timeout=15" -H "accept: application/hal+json"

# The response:
200 OK
{
"records": [
  {
    "node": {
      "uuid": "092e0298-f250-11e8-9a05-005056bb6666",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/092e0298-f250-11e8-9a05-
005056bb6666"
        }
      }
    },
    "index": 1,
    "destination": "http",
    "subject": "USER_TRIGGERED (TEST:test_msg)",
    "state": "sent_successful",
    "generated_on": "2019-03-28T10:18:04-04:00",
    "_links": {
      "self": {
        "href": "/api/support/autosupport/messages/092e0298-f250-11e8-
9a05-005056bb6666/1/http"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href":
"/api/support/autosupport/messages?node.name=node1&state=sent_successful&f
ields=*&return_timeout=15"
  }
}
}
```

Retrieve AutoSupport message history

GET `/support/autosupport/messages`

Introduced In: 9.6

Retrieves AutoSupport message history from all nodes in the cluster.

There can be a short delay on invoked AutoSupport messages showing in history, dependent on processing of other AutoSupports in the queue.

Related ONTAP commands

- `system node autosupport history show`

Learn more

- DOC /support/autosupport/messages

Parameters

Name	Type	In	Required	Description
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
destination	string	query	False	Filter by destination
state	string	query	False	Filter by state
generated_on	string	query	False	Filter by generated_on
index	integer	query	False	Filter by index
subject	string	query	False	Filter by subject
error.message	string	query	False	Filter by error.message
error.code	integer	query	False	Filter by error.code
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
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
Specify the fields to return.	max_records	integer	query	False
Limit the number of records returned.	return_timeout	integer	query	False

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[autosupport_message]	List of messages invoked on the node

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "destination": "http",
      "error": {
        "code": "53149746",
        "message": "Could not resolve host: test.com"
      },
      "generated_on": "2019-03-25 21:30:04 +0000",
      "index": 9,
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "state": "sent_successful",
      "subject": "WEEKLY_LOG"
    }
  ]
}
```


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	

error

Last error during delivery attempt. Empty if "status=sent-successful".

Name	Type	Description
code	integer	Error code
message	string	Error message

_links

Name	Type	Description
self	href	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

autosupport_message

Name	Type	Description
destination	string	Destination for the AutoSupport
error	error	Last error during delivery attempt. Empty if "status=sent-successful".

Name	Type	Description
generated_on	string	Date and Time of AutoSupport generation in ISO-8601 format
index	integer	Sequence number of the AutoSupport
node	node	
state	string	State of AutoSupport delivery
subject	string	Subject line for the AutoSupport

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.

Create and send an AutoSupport message

POST `/support/autosupport/messages`

Introduced In: 9.6

Creates and sends an AutoSupport message with the provided input parameters.

Important note:

- By default, the response is an empty object. If `return_records=true` is passed in the request, the response includes information about the node and the index of the invoked AutoSupport message.

Recommended optional properties

- `message` - Message included in the AutoSupport subject. Use this to identify the generated AutoSupport message.

Default property values

If not specified in POST, the following are the default property values:

- `type` - *all*
- `node.name` or `node.uuid` - Not specifying these properties invokes AutoSupport on all nodes in the cluster.

Related ONTAP commands

- `system node autosupport invoke`

Learn more

- DOC /support/autosupport/messages

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
destination	string	Destination for the AutoSupport
error	error	Last error during delivery attempt. Empty if "status=sent-successful".
generated_on	string	Date and Time of AutoSupport generation in ISO-8601 format
index	integer	Sequence number of the AutoSupport
message	string	Message included in the AutoSupport subject
node	node	

Name	Type	Description
state	string	State of AutoSupport delivery
subject	string	Subject line for the AutoSupport
type	string	Type of AutoSupport collection to issue
uri	string	Alternate destination for the AutoSupport

Example request

```
{
  "destination": "http",
  "error": {
    "code": "53149746",
    "message": "Could not resolve host: test.com"
  },
  "generated_on": "2019-03-25 21:30:04 +0000",
  "index": 9,
  "message": "invoked_test_autosupport_rest",
  "node": {
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "state": "sent_successful",
  "subject": "WEEKLY_LOG",
  "type": "test",
  "uri": "http://1.2.3.4/delivery_uri"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "num_records": 3,
  "records": [
    {
      "index": 9,
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
8650866	The message parameter is not supported with performance AutoSupports
53149748	The destination URI provided for the invoked AutoSupport is invalid

Definitions

See Definitions

error

Last error during delivery attempt. Empty if "status=sent-successful".

Name	Type	Description
code	integer	Error code
message	string	Error message

href

Name	Type	Description
href	string	

_links

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

autosupport_message

Name	Type	Description
destination	string	Destination for the AutoSupport
error	error	Last error during delivery attempt. Empty if "status=sent-successful".
generated_on	string	Date and Time of AutoSupport generation in ISO-8601 format
index	integer	Sequence number of the AutoSupport
message	string	Message included in the AutoSupport subject
node	node	
state	string	State of AutoSupport delivery

Name	Type	Description
subject	string	Subject line for the AutoSupport
type	string	Type of AutoSupport collection to issue
uri	string	Alternate destination for the AutoSupport

node

Name	Type	Description
name	string	
uuid	string	

records

Name	Type	Description
index	integer	Sequence number of the generated AutoSupport
node	node	

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.

Manage cluster configuration backup information

Support configuration-backup endpoint overview

Overview

This API retrieves the current settings for the configuration and updates configuration backup settings. The GET operation retrieves the current settings for the configuration and the PATCH operation updates the configuration backup settings.

Examples

These examples show how to retrieve and update the configuration backup settings.

Retrieving the configuration backup settings

```
# The API:
/api/support/configuration-backup

# The call:
curl -X GET "https://<mgmt-ip>/api/support/configuration-backup" -H
"accept: application/hal+json"

# The response:
{
  "url": "http://10.224.65.198/backups",
  "username": "me",
  "_links": {
      "self": {
          "href": "/api/support/configuration-backup"
      }
  }
}
```

Updating the configuration backup settings

```
# The API:
/api/support/configuration-backup

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/configuration-backup" -H
"accept: application/hal+json"

# The body:
{
  "url": "https://10.224.65.198/new_backups",
  "username": "new_me",
  "password": "new_pass",
  "validate_certificate": "true"
}

# The response header:
HTTP/1.1 200 OK
Date: Tue, 05 Jun 2018 18:17:48 GMT
Server: libzapid-httpd
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 3
Content-Type: application/hal+json
```

Retrieve cluster configuration backup information

GET `/support/configuration-backup`

Introduced In: 9.6

Retrieves the cluster configuration backup information.

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
password	string	
url	string	An external backup location for the cluster configuration. This is mostly required for single node clusters where node and cluster configuration backups cannot be copied to other nodes in the cluster.
username	string	
validate_certificate	boolean	Use this parameter with the value "true" to validate the digital certificate of the remote server. Digital certificate validation is available only when the HTTPS protocol is used in the URL; it is disabled by default.

Example response


```
{
  "password": "yourpassword",
  "url": "http://10.224.65.198/backups",
  "username": "me"
}
```


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.

Update cluster configuration backup information

PATCH `/support/configuration-backup`

Introduced In: 9.6

Updates the cluster configuration backup information.

Request Body

Name	Type	Description
password	string	
url	string	An external backup location for the cluster configuration. This is mostly required for single node clusters where node and cluster configuration backups cannot be copied to other nodes in the cluster.
username	string	
validate_certificate	boolean	Use this parameter with the value "true" to validate the digital certificate of the remote server. Digital certificate validation is available only when the HTTPS protocol is used in the URL; it is disabled by default.

Example request

```
{
  "password": "yourpassword",
  "url": "http://10.224.65.198/backups",
  "username": "me"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
39387137	Invalid URL
39387138	Invalid URL Scheme
5963792	Using HTTPS for URL requires an effective cluster version of 9.7.0 or later.
5963794	Validating the certificate is supported for the HTTPS protocol only.

Definitions

See Definitions

configuration_backup

Name	Type	Description
password	string	
url	string	An external backup location for the cluster configuration. This is mostly required for single node clusters where node and cluster configuration backups cannot be copied to other nodes in the cluster.
username	string	
validate_certificate	boolean	Use this parameter with the value "true" to validate the digital certificate of the remote server. Digital certificate validation is available only when the HTTPS protocol is used in the URL; it is disabled by default.

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.

Manage configuration backups

Support configuration-backup backups endpoint overview

Overview

This API supports creating, deleting and retrieving configuration backup files. Configuration backups can be 'cluster' or 'node' type. A 'cluster' backup contains cluster-wide configuration in addition to the configuration of each node in the cluster. A 'node' backup contains only node-specific configuration such as configuration files on the root volume and the boot variables. For creating a cluster backup, a cluster-wide job is queued. For creating a node backup, a private job local to the node is queued. In addition to the backups created using this API, ONTAP creates configuration backups automatically based on job schedules. This API supports creating configuration backups on demand only. It supports deleting and retrieving configuration backups that are created automatically or on demand. For information on configuration backup settings for automatically created backups, see DOC /support/configuration-backup

Examples

Retrieving a list of configuration backup files

```
# The API:
/api/support/configuration-backup/backups

# The call:
curl -X GET "https://<mgmt-ip>/api/support/configuration-backup/backups"
-H "accept: application/hal+json"

# The response:
{
"records": [
  {
    "node": {
      "uuid": "5cafe0f6-499f-11e9-b644-005056bbcf93",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/5cafe0f6-499f-11e9-b644-
005056bbcf93"
        }
      }
    },
    "name": "backup1.7z",
    "_links": {
      "self": {
        "href": "/api/support/configuration-backup/backups/5cafe0f6-499f-
11e9-b644-005056bbcf93/backup1.7z"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/configuration-backup/backups"
  }
}
}
```

Retrieving details of the specified configuration backup file

```
# The API:
/api/support/configuration-backup/backups/{node.uuid}/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/configuration-
backup/backups/bc2f15d0-8b93-11e9-90e9-005056bb6a30/backup1.7z" -H
"accept: application/hal+json"

# The response:
{
"node": {
  "uuid": "bc2f15d0-8b93-11e9-90e9-005056bb6a30",
  "name": "node1",
  "_links": {
    "self": {
      "href": "/api/cluster/nodes/bc2f15d0-8b93-11e9-90e9-005056bb6a30"
    }
  }
},
"name": "backup1.7z",
"type": "cluster",
"time": "2019-06-10T13:35:06-04:00",
"size": 6058408,
"backup_nodes": [
  {
    "name": "node1"
  },
  {
    "name": "node2"
  }
],
"version": "9.7.0",
"auto": false,
"download_link": "https://10.224.66.113/backups/backup1.7z",
"_links": {
  "self": {
    "href": "/api/support/configuration-backup/backups/bc2f15d0-8b93-11e9-
90e9-005056bb6a30/backup1.7z"
  }
}
}
```

Creating a configuration backup file

```
# The API:
/api/support/configuration-backup/backups

# The call:
curl -X POST "https://<mgmt-ip>/api/support/configuration-backup/backups"
-H "accept: application/hal+json" -d "@create_backup.txt"
create_backup.txt:
{
"node":
  {
    "uuid": "ac13c636-4fc9-11e9-94c2-005056bb2516",
    "name": "node1"
  },
"name": "backup3.7z"
}

# The response header:
HTTP/1.1 202 Accepted
Date: Tue, 26 Mar 2019 14:26:24 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/support/configuration-backup/backups/ac13c636-4fc9-11e9-
94c2-005056bb2516/backup3.7z
Content-Length: 189
Content-Type: application/hal+json
{
"job": {
  "uuid": "22acfb68-4fd3-11e9-94c2-005056bb2516",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/22acfb68-4fd3-11e9-94c2-005056bb2516"
    }
  }
}
}
```

Deleting a configuration backup file

```
# The API:
/api/support/configuration-backup/backups/{node.uuid}/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/configuration-
backup/backups/5cafe0f6-499f-11e9-b644-005056bbcf93/backup1.7z" -H
"content-type: application/json"

# The response header:
HTTP/1.1 200 OK
Date: Tue, 26 Mar 2019 14:32:23 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 3
Content-Type: application/hal+json
```

Retrieve configuration backup files

GET `/support/configuration-backup/backups`

Introduced In: 9.7

Retrieves a list of configuration backup files.

Related ONTAP commands

- `system configuration backup show`

Parameters

Name	Type	In	Required	Description
type	string	query	False	Filter by type
backup_nodes.name	string	query	False	Filter by backup_nodes.name
download_link	string	query	False	Filter by download_link
size	integer	query	False	Filter by size
version	string	query	False	Filter by version

Name	Type	In	Required	Description
auto	boolean	query	False	Filter by auto
time	string	query	False	Filter by time
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
name	string	query	False	Filter by name
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
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

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[configuration_backup_file]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "backup_nodes": [
        {
          "name": "string"
        }
      ],
      "download_link": "https://10.224.65.198/backups/backup_file.7z",
      "name": "backup_file.7z",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "size": 4787563,
      "time": "2019-02-04 18:33:48 +0000",
      "type": "string",
      "version": "9.7.0"
    }
  ]
}
```


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	

backup_node

The node name in the backup.

Name	Type	Description
name	string	

_links

Name	Type	Description
self	href	

node

The node that owns the configuration backup.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

configuration_backup_file

The configuration backup file.

Name	Type	Description
auto	boolean	Indicates if the backup was created automatically.
backup_nodes	array[backup_node]	The list of nodes included in the backup.

Name	Type	Description
download_link	string	The link to download the backup file.
name	string	The backup name.
node	node	The node that owns the configuration backup.
size	integer	The size of the backup in bytes.
time	string	The backup creation time.
type	string	The backup type.
version	string	The software version.

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.

Create a configuration backup

POST `/support/configuration-backup/backups`

Introduced In: 9.7

Creates a configuration backup. The required backup file name must end with .7z extension.

Required properties

- `node.uuid` or `node.name` - The node UUID or node name on which the configuration backup will be created.
- `name` - The backup file name

Related ONTAP commands

- `system configuration backup create`

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
auto	boolean	Indicates if the backup was created automatically.
backup_nodes	array[backup_node]	The list of nodes included in the backup.
download_link	string	The link to download the backup file.
name	string	The backup name.
node	node	The node that owns the configuration backup.
size	integer	The size of the backup in bytes.
time	string	The backup creation time.
type	string	The backup type.
version	string	The software version.

Example request


```
{
  "backup_nodes": [
    {
      "name": "string"
    }
  ],
  "download_link": "https://10.224.65.198/backups/backup_file.7z",
  "name": "backup_file.7z",
  "node": {
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "size": 4787563,
  "time": "2019-02-04 18:33:48 +0000",
  "type": "string",
  "version": "9.7.0"
}
```


Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5963818	Failed to queue private job.
5963819	Failed to queue cluster job.
5963871	Requested backup name is missing .7z suffix.

Definitions

See Definitions

backup_node

The node name in the backup.

Name	Type	Description
name	string	

href

Name	Type	Description
href	string	

_links

node

The node that owns the configuration backup.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

configuration_backup_file

The configuration backup file.

Name	Type	Description
auto	boolean	Indicates if the backup was created automatically.
backup_nodes	array[backup_node]	The list of nodes included in the backup.
download_link	string	The link to download the backup file.
name	string	The backup name.
node	node	The node that owns the configuration backup.
size	integer	The size of the backup in bytes.

Name	Type	Description
time	string	The backup creation time.
type	string	The backup type.
version	string	The software version.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

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.

Delete a configuration backup

DELETE `/support/configuration-backup/backups/{node.uuid}/{name}`

Introduced In: 9.7

Deletes a configuration backup.

Related ONTAP commands

- `system configuration backup delete`

Parameters

Name	Type	In	Required	Description
node.uuid	string	path	True	UUID of the node that owns the configuration backup.
name	string	path	True	Name of the configuration backup to be deleted.

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5963826	Failed to delete backup file.

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 configuration backup file details

GET `/support/configuration-backup/backups/{node.uuid}/{name}`

Introduced In: 9.7

Retrieves details of the specified configuration backup file.

Related ONTAP commands

- `system configuration backup show`

Parameters

Name	Type	In	Required	Description
node.uuid	string	path	True	UUID of the node that owns the configuration backup.
name	string	path	True	Name of the configuration backup.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
auto	boolean	Indicates if the backup was created automatically.
backup_nodes	array[backup_node]	The list of nodes included in the backup.
download_link	string	The link to download the backup file.
name	string	The backup name.
node	node	The node that owns the configuration backup.
size	integer	The size of the backup in bytes.
time	string	The backup creation time.

Name	Type	Description
type	string	The backup type.
version	string	The software version.

Example response


```
{
  "backup_nodes": [
    {
      "name": "string"
    }
  ],
  "download_link": "https://10.224.65.198/backups/backup_file.7z",
  "name": "backup_file.7z",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "size": 4787563,
  "time": "2019-02-04 18:33:48 +0000",
  "type": "string",
  "version": "9.7.0"
}
```


Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5963777	Configuration backup file does not exist.

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

backup_node

The node name in the backup.

Name	Type	Description
name	string	

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

node

The node that owns the configuration backup.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

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.

Manage core dumps

Support coredump coredumps endpoint overview

Overview

The core dump GET API retrieves all of the core dumps on the cluster or a node. The core dump DELETE API deletes a specified core dump. Some fields are only populated for core dump type "kernel". Refer to the model for further information. Fields will not be displayed if they are not populated. A core can be deleted even if the core is in the process of being saved.

Examples

1) Retrieving a list of core dumps from the cluster

The following example returns a list of core dumps on the cluster:

```
# The API:
/api/support/coredump/coredumps

# The call:
curl -X GET "https://<mgmt-ip>/api/support/coredump/coredumps" -H "accept:
application/hal+json"

# The response:
{
"records": [
  {
    "node": {
      "uuid": "227683c1-e9c7-11eb-b995-005056bbbfb3",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/227683c1-e9c7-11eb-b995-
005056bbbfb3"
        }
      }
    },
    "type": "kernel",
    "name": "core.4136886422.2021-07-21.20_20_53.nz",
```

```
    "_links": {
      "self": {
        "href": "/api/support/coredump/coredumps/227683c1-e9c7-11eb-b995-
005056bbbfb3/core.4136886422.2021-07-21.20_20_53.nz"
      }
    }
  },
  {
    "node": {
      "uuid": "227683c1-e9c7-11eb-b995-005056bbbfb3",
      "name": "node2",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/227683c1-e9c7-11eb-b995-
005056bbbfb3"
        }
      }
    },
    "type": "application",
    "name": "mlogd.968.4136886422.2021-07-22.01_10_01.ucore.bz2",
    "_links": {
      "self": {
        "href": "/api/support/coredump/coredumps/227683c1-e9c7-11eb-b995-
005056bbbfb3/mlogd.968.4136886422.2021-07-22.01_10_01.ucore.bz2"
      }
    }
  },
  {
    "node": {
      "uuid": "d583d44e-e9c6-11eb-a270-005056bb47f9",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/d583d44e-e9c6-11eb-a270-
005056bb47f9"
        }
      }
    },
    "type": "kernel",
    "name": "core.4136886421.2021-07-21.17_57_02.nz",
    "_links": {
      "self": {
        "href": "/api/support/coredump/coredumps/d583d44e-e9c6-11eb-a270-
005056bb47f9/core.4136886421.2021-07-21.17_57_02.nz"
      }
    }
```

```
  },
  {
    "node": {
      "uuid": "d583d44e-e9c6-11eb-a270-005056bb47f9",
      "name": "node1",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/d583d44e-e9c6-11eb-a270-
005056bb47f9"
        }
      }
    },
    "type": "application",
    "name": "mlogd.979.4136886421.2021-07-22.01_11_37.ucore.bz2",
    "_links": {
      "self": {
        "href": "/api/support/coredump/coredumps/d583d44e-e9c6-11eb-a270-
005056bb47f9/mlogd.979.4136886421.2021-07-22.01_11_37.ucore.bz2"
      }
    }
  }
],
"num_records": 4,
"_links": {
  "self": {
    "href": "/api/support/coredump/coredumps"
  }
}
}
```

2) Retrieving a specific core dump

The following example returns the requested core dump. If there is no core dump with the requested node UUID and name, an error is returned.

```
# The API:
/api/support/coredump/coredumps/{node.uuid}/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/coredump/coredumps/d583d44e-
e9c6-11eb-a270-005056bb47f9/core.4136886421.2021-07-21.17_57_02.nz" -H
"accept: application/hal+json"

# The response:
{
"node": {
  "uuid": "d583d44e-e9c6-11eb-a270-005056bb47f9",
  "name": "node1",
  "_links": {
    "self": {
      "href": "/api/cluster/nodes/d583d44e-e9c6-11eb-a270-005056bb47f9"
    }
  }
},
"type": "kernel",
"name": "core.4136886421.2021-07-21.17_57_02.nz",
"panic_time": "2021-07-21T13:57:02-04:00",
"size": 945111148,
"md5_data_chksum": "611a6fa50d230a1af402f3724ab320af",
"is_saved": true,
"_links": {
  "self": {
    "href": "/api/support/coredump/coredumps/d583d44e-e9c6-11eb-a270-
005056bb47f9/core.4136886421.2021-07-21.17_57_02.nz"
  }
}
}
```

3) Deleting a core dump

The following example deletes the requested core dump. If there is no core dump with the requested node UUID and name to delete, an error is returned.

```
# The API:
/api/support/coredump/coredumps/{node.uuid}/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/coredump/coredumps/d583d44e-
e9c6-11eb-a270-005056bb47f9/mlogd.979.4136886421.2021-07-
22.01_11_37.ucore.bz2" -H "accept: application/hal+json"

# The response header:
HTTP/1.1 200 OK
Date: Thu, 22 Jul 2021 01:32:24 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 3
Content-Type: application/hal+json
```

Retrieve core dumps

GET `/support/coredump/coredumps`

Introduced In: 9.10

Retrieves a collection of coredumps.

Related ONTAP commands

- `system node coredump show`

Parameters

Name	Type	In	Required	Description
is_saved	boolean	query	False	Filter by is_saved
panic_time	string	query	False	Filter by panic_time
md5_data_checksum	string	query	False	Filter by md5_data_checksum
name	string	query	False	Filter by name
node.uuid	string	query	False	Filter by node.uuid

Name	Type	In	Required	Description
node.name	string	query	False	Filter by node.name
size	integer	query	False	Filter by size
type	string	query	False	Filter by type
is_partial	boolean	query	False	Filter by is_partial
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[coredump]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "md5_data_checksum": "5118488cc5065e33a16986001b1ffa48",
      "name": "core.4136886413.2021-03-01.22_09_11.nz",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "panic_time": "2021-03-01 22:09:11 +0000",
      "size": 1161629804,
      "type": "kernel"
    }
  ]
}
```


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	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

coredump

Name	Type	Description
_links	_links	
is_partial	boolean	Specifies whether or not the core is a partial core. Applicable only to kernel core dump type.
is_saved	boolean	Specifies whether or not the core file is saved.
md5_data_checksum	string	MD5 checksum of the compressed data of core. Applicable only to kernel core dump type.
name	string	Core name
node	node	

Name	Type	Description
panic_time	string	Time of panic that generated the core.
size	integer	Size of core, in bytes. Applicable only to kernel core dump type.
type	string	Core type, kernel or application

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.

Delete a core dump

DELETE `/support/coredump/coredumps/{node.uuid}/{name}`

Introduced In: 9.10

Deletes a core dump.

Related ONTAP commands

- `system node coredump delete`

Parameters

Name	Type	In	Required	Description
node.uuid	string	path	True	Node UUID
name	string	path	True	Core name
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

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 a core dump

GET `/support/coredump/coredumps/{node.uuid}/{name}`

Introduced In: 9.10

Retrieves a specific core dump.

Related ONTAP commands

- `system node coredump show`

Parameters

Name	Type	In	Required	Description
node.uuid	string	path	True	Node UUID
name	string	path	True	Core name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
is_partial	boolean	Specifies whether or not the core is a partial core. Applicable only to kernel core dump type.
is_saved	boolean	Specifies whether or not the core file is saved.
md5_data_checksum	string	MD5 checksum of the compressed data of core. Applicable only to kernel core dump type.
name	string	Core name
node	node	
panic_time	string	Time of panic that generated the core.

Name	Type	Description
size	integer	Size of core, in bytes. Applicable only to kernel core dump type.
type	string	Core type, kernel or application

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "md5_data_checksum": "5118488cc5065e33a16986001b1ffa48",
  "name": "core.4136886413.2021-03-01.22_09_11.nz",
  "node": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "panic_time": "2021-03-01 22:09:11 +0000",
  "size": 1161629804,
  "type": "kernel"
}
```


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	

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

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.

Manage EMS configuration

Support EMS endpoint overview

Overview

The Event Management System (EMS) collects and processes events, and sends notification of the events through various reporting mechanisms. The following endpoints defined under '/support/ems', allow you to query a list of observed events, and configure which events you handle and how you are notified:

- /support/ems
- /support/ems/events
- /support/ems/messages
- /support/ems/filters
- /support/ems/filters/{name}/rules
- /support/ems/filters/{name}/rules/{index}
- /support/ems/destinations
- /support/ems/destinations/{name}

Examples

Configuring an email destination

The following example configures EMS to send a support email when a WAFL event is observed with an error severity.

Configure the system-wide email parameters

```
# The API:
PATCH /support/ems

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/ems" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_config_patch.txt"
test_ems_config_patch.txt(body):
{
"mail_from": "administrator@mycompany.com",
"mail_server": "smtp@mycompany.com"
}

# The response:
200 OK
```

Configuring a filter with an enclosed rule

```
# The API:
POST /support/ems/filters

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/filters" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filters_post.txt"
test_ems_filters_post.txt(body):
{
"name": "critical-wafl",
"rules": [
  {
    "index": 1,
    "type": "include",
    "message_criteria": {
      "name_pattern": "wafl.*",
      "severities": "emergency,error,alert"
    }
  }
]
}

# The response:
201 Created
```

Setting up an email destination

```
# The API:
POST /support/ems/destinations

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/destinations" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_dest_post.txt"
test_ems_dest_post.txt(body):
{
"name": "Technician_Email",
"type": "email",
"destination": "technician@mycompany.com",
"filters": [
  { "name" : "critical-wafl" }
]
}

# The response:
201 Created
```

Retrieve an EMS configuration

GET `/support/ems`

Introduced In: 9.6

Retrieves the EMS configuration.

Related ONTAP commands

- `event config show`

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	

Name	Type	Description
mail_from	string	Mail from
mail_server	string	Mail server (SMTP)
proxy_password	string	Password for HTTP/HTTPS proxy
proxy_url	string	HTTP/HTTPS proxy URL
proxy_user	string	User name for HTTP/HTTPS proxy
pubsub_enabled	boolean	Is Publish/Subscribe Messaging Enabled?

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "mail_from": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
  "mail_server": "mail.mycompany.com",
  "proxy_password": "password",
  "proxy_url": "https://proxyserver.mycompany.com",
  "proxy_user": "proxy_user",
  "pubsub_enabled": 1
}
```


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	

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 an EMS configuration

PATCH `/support/ems`

Introduced In: 9.6

Updates the EMS configuration.

Related ONTAP commands

- `event config modify`

Request Body

Name	Type	Description
mail_from	string	Mail from
mail_server	string	Mail server (SMTP)
proxy_password	string	Password for HTTP/HTTPS proxy
proxy_url	string	HTTP/HTTPS proxy URL
proxy_user	string	User name for HTTP/HTTPS proxy
pubsub_enabled	boolean	Is Publish/Subscribe Messaging Enabled?

Example request

```
{
  "mail_from": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
  "mail_server": "mail.mycompany.com",
  "proxy_password": "password",
  "proxy_url": "https://proxyserver.mycompany.com",
  "proxy_user": "proxy_user",
  "pubsub_enabled": 1
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983123	The validation of the mail server provided failed

Error Code	Description
983136	The proxy URL cannot contain a username or password
983137	The proxy URL provided is invalid
983139	The IPv6 proxy URL provided is invalid
983140	The proxy URL provided contains an invalid scheme. The only supported scheme is 'http'
983160	The provided parameter requires an effective cluster version of ONTAP 9.9.1 or later

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ems_config

Name	Type	Description
mail_from	string	Mail from
mail_server	string	Mail server (SMTP)
proxy_password	string	Password for HTTP/HTTPS proxy
proxy_url	string	HTTP/HTTPS proxy URL
proxy_user	string	User name for HTTP/HTTPS proxy
pubsub_enabled	boolean	Is Publish/Subscribe Messaging Enabled?

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.

Manage application logs

Support EMS application-logs endpoint overview

Overview

A POST request allows a standalone application to log its events on the ONTAP system as EMS events and optionally generate AutoSupports. This event information is encapsulated in an app.log.x event, or callhome.client.app.x event in case AutoSupport generation is required, based on the event's severity.

This API only supports POST. Generated events can be retrieved using the /api/support/ems/events API.

Examples

Creating a new app.log.* event

The following example generates an app.log.error event.

```
# The API:
POST /api/support/ems/application-logs

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/application-logs" -H
"accept: application/hal+json" -H "Content-Type: application/json" -d "{
\"computer_name\": \"W12-R2-DC\", \"event_source\": \"SnapCenter
Software\", \"app_version\": \"3.0.0.2373\", \"event_id\": 10001,
\"category\": \"error\", \"event_description\": \"Clone split job
failed\", \"severity\": \"error\", \"autosupport_required\": false}"

# The response:
201 CREATED
{}
```

Retrieving a list of events generated by this API

The following example retrieves all app.log.* events.

```
# The API:
GET /api/support/ems/events

# The call:
curl -X GET "https://<mgmt-
ip>/api/support/ems/events?message.name=app.log.*" -H "accept:
application/hal+json"

# The response:
200 OK
{
"records": [
  {
    "node": {
      "name": "node1",
      "uuid": "d96d5d8d-118a-11ec-aad8-005056bb974c",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/d96d5d8d-118a-11ec-aad8-
005056bb974c"
        }
      }
    },
    "index": 7865,
    "time": "2021-09-17T09:36:28-04:00",
    "message": {
      "severity": "emergency",
      "name": "app.log.emerg"
    },
    "log_message": "app.log.emerg: iMac: iPad ipad3: (10001) handheld:
TestLine1",
    "_links": {
      "self": {
        "href": "/api/support/ems/events/node1/7865"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/ems/events?message.name=app.log.*"
  }
}
}
```

Create an application log

POST `/support/ems/application-logs`

Introduced In: 9.11

Creates an app.log.* event. Setting the "autosupport_required" flag causes callhome.client.app.* events also to be generated, which in turn triggers AutoSupports.

Required properties

- `computer_name` - Client computer connected to the cluster.
- `event_source` - Client application that generated this event.
- `app_version` - Client application version.
- `event_id` - Application eventID.
- `category` - Event category.
- `event_description` - Event description.
- `severity` - Severity of the event.
- `autosupport_required` - Indicates whether AutoSupport generation is required.

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
app_version	string	Client application version.
autosupport_required	boolean	Indicates whether AutoSupport generation is required.
category	string	Event category.
computer_name	string	Client computer connected to the cluster.

Name	Type	Description
event_description	string	Event description, which corresponds to the subject parameter in the generated event.
event_id	integer	Application eventID.
event_source	string	Client application that generated this event.
severity	string	Severity

Example request

```
{
  "app_version": "3.0.0.2373",
  "autosupport_required": "",
  "category": "Error",
  "computer_name": "W12-R2-DC",
  "event_description": "Clone split job failed",
  "event_id": 10001,
  "event_source": "SnapCenter Software",
  "severity": "error"
}
```

Response

```
Status: 201, Created
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983146	Invalid value specified for the field "severity".
983173	Application log event generation failed.

Definitions

See Definitions

ems_application_log

Input for generation of app.log.x and callhome.client.app.x events.

Name	Type	Description
app_version	string	Client application version.
autosupport_required	boolean	Indicates whether AutoSupport generation is required.
category	string	Event category.
computer_name	string	Client computer connected to the cluster.
event_description	string	Event description, which corresponds to the subject parameter in the generated event.
event_id	integer	Application eventID.
event_source	string	Client application that generated this event.
severity	string	Severity

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.

Manage event destinations

Support EMS destinations endpoint overview

Overview

Manages the list of destinations. A destination is defined by a type and a place to which an event's information is transmitted.

Destination Types

An EMS destination is defined by a single type, which is one of the following:

- email
- syslog
- rest_api
- snmp

Email

The 'email' type allows you to define a mailbox where information about an observed event is sent by SMTP. Enter the address in the destination field in a valid format. For example: administrator@mycompany.com

Syslog

The 'syslog' type allows you to specify a remote syslog server that can receive information about an observed event. Enter the hostname or IP address in the destination field. For example: syslog.mycompany.com, 192.168.1.1

You can optionally specify the port and transport protocol to be used. The supported transport protocols are:

- udp_unencrypted
- tcp_unencrypted
- tcp_encrypted

#

If transport is specified and the port is not specified, the default port for each transport is automatically selected. The default port for udp_unencrypted is 514, for tcp_unencrypted 601, and for tcp_encrypted 6514. The default transport protocol is udp_unencrypted.

#

The message format to be used can also be optionally specified. The supported message formats are:

- legacy_netapp (format: <PRIVAL>TIMESTAMP [HOSTNAME:Event-name:Event-severity]: MSG)
- rfc_5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME Event-source - Event-name - MSG)

#

If the default timestamp or hostname formats in the message format needs to be overridden, use timestamp_override and hostname_override properties.

The supported timestamp formats are:

- no_override (timestamp format based on the syslog.format.message property i.e. rfc_3164 if syslog.format.message is legacy_netapp, iso_8601_local_time if syslog.format.message is rfc_5424)
- rfc_3164 (format: Mmm dd hh:mm:ss)
- iso_8601_local_time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm)
- iso_8601_utc (format: YYYY-MM-DDThh:mm:ssZ)

#

The supported hostname formats are:

- no_override (hostname format based on the syslog.format.message property i.e. fqdn if syslog.format.message is rfc_5424, hostname_only if syslog.format.message is legacy_netapp)
- fqdn (Fully Qualified Domain Name)
- hostname_only

Rest API

The 'rest_api' type allows you to define a URL where information about an observed event is sent using the REST protocol. Enter the URL in the destination field. The URL must contain a valid transmission schema which can be one of the following:

- http
- https

#

Using the *https* schema, you can configure a client-side certificate for mutual authentication. A client-side certificate is specified by the `ca` and `serial_number` fields in the `certificate` object. The `name` field of the `certificate` object is read-only and cannot be used to configure a client-side certificate.

For example: http://rest.mycompany.com, https://192.168.1.1

SNMP

The 'snmp' type describes addresses where information about an observed event is sent using SNMP traps. The system defines a default instance of this type and it is restricted to read-only. This type has the following limitations:

- Cannot create new destinations of type 'snmp'
- Cannot modify the default 'snmp' destination

SNMP trap host details need to be configured through one of the following:

Type	Command / API
CLI	'system snmp traphost'
ZAPI	'snmp-traphost-add' / 'snmp-traphost-delete'

Examples

Retrieving the list of active destinations

```
# The API:
GET /api/support/ems/destinations

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/destinations" -H "accept:
application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "name": "snmp-traphost",
    "_links": {
      "self": {
        "href": "/api/support/ems/destinations/snmp-traphost"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/ems/destinations"
  }
}
}
```

Creating a new 'email' destination

```
# The API:
POST /support/ems/destinations

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/destinations" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_destinations_post.txt"
test_ems_destinations_post.txt(body):

# JSON Body
{
"name": "Technician_Email",
"type": "email",
"destination": "technician@mycompany.com",
"filters": [
  { "name" : "critical-wafl" }
]
}

# The response:
201 Created
```

Creating a new 'syslog' destination

```
# The API:
POST /support/ems/destinations

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/destinations" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_destinations_syslog_post.txt"
test_ems_destinations_syslog_post.txt(body):

# JSON Body
{
"name": "Syslog_dest",
"type": "syslog",
"destination": "syslog.mycompany.com",
"syslog": {
  "port": 601,
  "transport": "tcp_unencrypted",
  "format": {
    "message": "rfc_5424",
    "hostname_override": "fqdn",
    "timestamp_override": "iso_8601_local_time"
  }
},
"filters": [
  { "name" : "critical-wafl" }
]
}

# The response:
201 Created
```

Retrieve a collection of event destinations

GET `/support/ems/destinations`

Introduced In: 9.6

Retrieves a collection of event destinations.

Related ONTAP commands

- `event notification destination show`
- `event notification show`

Parameters

Name	Type	In	Required	Description
type	string	query	False	Filter by type
connectivity.errors.node.uuid	string	query	False	Filter by connectivity.errors.node.uuid • Introduced in: 9.11
connectivity.errors.node.name	string	query	False	Filter by connectivity.errors.node.name • Introduced in: 9.11
connectivity.errors.message.code	string	query	False	Filter by connectivity.errors.message.code • Introduced in: 9.11
connectivity.errors.message.message	string	query	False	Filter by connectivity.errors.message.message • Introduced in: 9.11
connectivity.errors.message.arguments.message	string	query	False	Filter by connectivity.errors.message.arguments.message • Introduced in: 9.11
connectivity.errors.message.arguments.code	string	query	False	Filter by connectivity.errors.message.arguments.code • Introduced in: 9.11

Name	Type	In	Required	Description
connectivity.state	string	query	False	Filter by connectivity.state • Introduced in: 9.11
filters.name	string	query	False	Filter by filters.name
access_control_role.name	string	query	False	Filter by access_control_role.name • Introduced in: 9.13
certificate.ca	string	query	False	Filter by certificate.ca • maxLength: 256 • minLength: 1
certificate.name	string	query	False	Filter by certificate.name • Introduced in: 9.11
certificate.serial_number	string	query	False	Filter by certificate.serial_number • maxLength: 40 • minLength: 1
syslog.port	integer	query	False	Filter by syslog.port • Introduced in: 9.12
syslog.transport	string	query	False	Filter by syslog.transport • Introduced in: 9.12

Name	Type	In	Required	Description
syslog.format.timestamp_override	string	query	False	Filter by syslog.format.timestamp_override • Introduced in: 9.12
syslog.format.message	string	query	False	Filter by syslog.format.message • Introduced in: 9.12
syslog.format.hostname_override	string	query	False	Filter by syslog.format.hostname_override • Introduced in: 9.12
name	string	query	False	Filter by name
destination	string	query	False	Filter by destination
system_defined	boolean	query	False	Filter by system_defined • Introduced in: 9.10
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_control_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "certificate": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "ca": "VeriSign",
        "name": "cert1",
        "serial_number": 1234567890
      },
      "connectivity": {
        "errors": [
          {
            "message": {
              "arguments": [
                {
                  "code": "string",
                  "message": "string"
                }
```

```
            ],
            "code": "4",
            "message": "entry doesn't exist"
          },
          "node": {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          }
        }
      ],
      "state": "fail"
    },
    "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
    "filters": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "important-events"
      }
    ],
    "name": "Admin_Email",
    "syslog": {
      "format": {
        "hostname_override": "string",
        "message": "string",
        "timestamp_override": "string"
      },
      "port": 514,
      "transport": "string"
    },
    "system_defined": 1,
    "type": "email"
  }
 ]
}
```

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	

access_control_role

Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

certificate

Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate.

Name	Type	Description
_links	_links	
ca	string	Client certificate issuing CA
name	string	Certificate name
serial_number	string	Client certificate serial number

arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

message

Name	Type	Description
arguments	array[arguments]	Message arguments
code	string	Unique message code.
message	string	User message.

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

errors

Error object included in the event of connectivity failure.

Name	Type	Description
message	message	
node	node	

connectivity

Name	Type	Description
errors	array[errors]	A list of errors encountered during connectivity checks.
state	string	Current connectivity state.

filters

Name	Type	Description
_links	_links	
name	string	

format

Name	Type	Description
hostname_override	string	Syslog Hostname Format Override. The supported hostname formats are no_override (hostname format based on the syslog.format.message property i.e. fqdn if syslog.format.message is rfc_5424, hostname_only if syslog.format.message is legacy_netapp), fqdn (Fully Qualified Domain Name) and hostname_only.
message	string	Syslog Message Format. The supported message formats are legacy_netapp (format: <PRIVAL>TIMESTAMP [HOSTNAME:Event-name:Event-severity]: MSG) and rfc_5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME Event-source - Event-name - MSG).
timestamp_override	string	Syslog Timestamp Format Override. The supported timestamp formats are no_override (timestamp format based on the syslog.format.message property i.e. rfc_3164 if syslog.format.message is legacy_netapp, iso_8601_local_time if syslog.format.message is rfc_5424), rfc_3164 (format: Mmm dd hh:mm:ss), iso_8601_local_time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm) and iso_8601_utc (format: YYYY-MM-DDThh:mm:ssZ).

syslog

Name	Type	Description
format	format	

Name	Type	Description
port	integer	Syslog Port.
transport	string	Syslog Transport Protocol.

records

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
name	string	Destination name. Valid in POST.
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.
type	string	Type of destination. Valid in POST.

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.

Create an event destination

POST `/support/ems/destinations`

Introduced In: 9.6

Creates an event destination.

Required properties

- `name` - String that uniquely identifies the destination.
- `type` - Type of destination that is to be created.
- `destination` - String that identifies the destination. The contents of this property changes depending on type.

Recommended optional properties

- `filters.name` - List of filter names that should direct to this destination.
- `certificate` - When specifying a rest api destination, a client certificate can be provided.
- `syslog` - When specifying a syslog destination, a port, transport protocol, message format, timestamp format and hostname format can be provided.

Related ONTAP commands

- `event notification destination create`

- `event notification create`

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
name	string	Destination name. Valid in POST.
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.
type	string	Type of destination. Valid in POST.

Example request


```
{
  "certificate": {
    "ca": "VeriSign",
    "name": "cert1",
    "serial_number": 1234567890
  },
  "connectivity": {
    "errors": [
      {
        "message": {
          "arguments": [
            {
              "code": "string",
              "message": "string"
            }
          ],
          "code": "4",
          "message": "entry doesn't exist"
        },
        "node": {
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      }
    ],
    "state": "fail"
  },
  "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
  "filters": [
    {
      "name": "important-events"
    }
  ],
  "name": "Admin_Email",
  "syslog": {
    "format": {
      "hostname_override": "string",
      "message": "string",
      "timestamp_override": "string"
    },
    "port": 514,
    "transport": "string"
  },
```

```
  "system_defined": 1,
  "type": "email"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "certificate": {
        "ca": "VeriSign",
        "name": "cert1",
        "serial_number": 1234567890
      },
      "connectivity": {
        "errors": [
          {
            "message": {
              "arguments": [
                {
                  "code": "string",
                  "message": "string"
                }
              ],
              "code": "4",
              "message": "entry doesn't exist"
            },
            "node": {
              "name": "node1",
              "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
            }
          }
        ],
        "state": "fail"
      },
      "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
      "filters": [
        {
          "name": "important-events"
        }
      ],
      "name": "Admin_Email",
      "syslog": {
        "format": {
          "hostname_override": "string",
          "message": "string",
          "timestamp_override": "string"
        },
```

```
        "port": 514,
        "transport": "string"
      },
      "system_defined": 1,
      "type": "email"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983104	The syslog destination provided is invalid
983107	A provided filter does not exist
983116	The number of notifications has reached maximum capacity
983117	The number of destinations has reached maximum capacity
983129	The rest-api destination provided must contain a valid scheme, such as http// or https//
983130	The rest-api destination provided contains an invalid URL
983131	The rest-api destination provided contains an invalid IPv6 URL
983144	The security certificate information provided is incomplete. Provide the certificate and serial number
983145	The rest-api destination provided has an 'http://' scheme. It is invalid to provide certificate information
983149	New SNMP destinations cannot be created
983152	Default destinations cannot be modified or removed
983153	The security certificate provided does not exist

Error Code	Description
983154	The necessary private key is not installed on the system
983170	Connectivity check is not supported for the specified destination type on the node
983171	Connectivity check failed for the specified destination on the node
983176	Connectivity check is only supported for TCP-based syslog destinations
983179	The value for the destination field cannot be empty
983180	The destination name provided cannot be empty
983181	The destination name provided cannot contain spaces
983182	The destination name provided is invalid. The destination name must contain between 2 and 64 characters and start and end with an alphanumeric symbol or _(underscore). The allowed special characters are _(underscore) and -(hyphen)
983184	A provided property cannot be configured on the requested destination type
983200	Access control role compatibility issue with provided filters

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

certificate

Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate.

Name	Type	Description
_links	_links	
ca	string	Client certificate issuing CA
name	string	Certificate name
serial_number	string	Client certificate serial number

arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

message

Name	Type	Description
arguments	array[arguments]	Message arguments
code	string	Unique message code.
message	string	User message.

node

Name	Type	Description
name	string	
uuid	string	

errors

Error object included in the event of connectivity failure.

Name	Type	Description
message	message	
node	node	

connectivity

Name	Type	Description
errors	array[errors]	A list of errors encountered during connectivity checks.
state	string	Current connectivity state.

filters

Name	Type	Description
name	string	

format

Name	Type	Description
hostname_override	string	Syslog Hostname Format Override. The supported hostname formats are no_override (hostname format based on the syslog.format.message property i.e. fqdn if syslog.format.message is rfc_5424, hostname_only if syslog.format.message is legacy_netapp), fqdn (Fully Qualified Domain Name) and hostname_only.
message	string	Syslog Message Format. The supported message formats are legacy_netapp (format: <PRIVAL>TIMESTAMP [HOSTNAME:Event-name:Event-severity]: MSG) and rfc_5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME Event-source - Event-name - MSG).
timestamp_override	string	Syslog Timestamp Format Override. The supported timestamp formats are no_override (timestamp format based on the syslog.format.message property i.e. rfc_3164 if syslog.format.message is legacy_netapp, iso_8601_local_time if syslog.format.message is rfc_5424), rfc_3164 (format: Mmm dd hh:mm:ss), iso_8601_local_time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm) and iso_8601_utc (format: YYYY-MM-DDThh:mm:ssZ).

syslog

Name	Type	Description
format	format	
port	integer	Syslog Port.

Name	Type	Description
transport	string	Syslog Transport Protocol.

ems_destination

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
name	string	Destination name. Valid in POST.
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.
type	string	Type of destination. Valid in POST.

access_control_role

Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
name	string	Role name

records

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
name	string	Destination name. Valid in POST.
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.
type	string	Type of destination. Valid in POST.

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

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Manage an event destination instance

Support EMS destinations name endpoint overview

Overview

Manages a specific instance of a destination. There are limits to the information that you can modify after a destination is created. For example, you cannot change a destination's type, but you can modify the underlying details of the type.

The system defines default destinations that cannot be removed or modified. These destinations are specified by setting the "system_defined" field to "true".

See the documentation for /support/ems/destinations for details on the various properties in a destination.

Connectivity Test

Optionally, you can request the connectivity object by specifically requesting the object in the fields query. This will perform an additional test to determine the state of the destination. The state response can include one of the following values:

- success
- fail
- not_supported

success

If the connectivity object indicates a state of 'success', then the destination check passed.

Currently, only the 'rest_api' destination type is supported. A successful result indicates that the server received the event.

fail

If the connectivity object indicates a state of 'fail', then the destination check has not passed. The object will contain a 'error' object with additional information regarding the failure.

not_supported

If the connectivity object indicates a state of 'not_supported', then the destination check is not available for the indicated destination type. This is not considered a failure condition.

Currently, only the 'rest_api' destination type is supported for connectivity testing.

Examples

Retrieving a specific destination instance

```
# The API:
GET /api/support/ems/destinations/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/destinations/snmp-traphost"
-H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"name": "snmp-traphost",
"type": "snmp",
"destination": "",
"filters": [
  {
    "name": "default-trap-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/default-trap-events"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/ems/destinations/snmp-traphost"
  }
}
}
```

Check whether a destination passes connectivity tests

```
# The API:
GET /api/support/ems/destinations/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/destinations/rest-api-
destination?fields=name,connectivity.*" -H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"name": "rest-api-destination",
"connectivity": {
  "state": "fail",
  "errors": [
    {
      "message": {
        "message": "Cannot reach host mail@mail.com.",
        "code": "4",
        "arguments": [
          {
            "code": "5",
            "message": "mail@mail.com"
          }
        ],
      },
      "node": {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    }
  ]
},
"_links": {
  "self": {
    "href": "/api/support/ems/destinations/rest-api-
destination?fields=name,connectivity.*"
  }
}
}
```

Updating an existing destination (change of email address)

```
# The API:
PATCH /api/support/ems/destinations/{name}

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/destinations/test-
destination" -H "accept: application/hal+json" -H "Content-Type:
application/json" -d "@test_ems_destinations_patch.txt"
test_ems_destinations_patch.txt(body):
{
"destination": "support@mycompany.com"
}

# The response:
200 OK
```

Deleting an existing destination

```
# The API:
DELETE /api/support/ems/destinations/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/ems/destinations/test-
destination" -H "accept: application/hal+json"

# The response:
200 OK
```

Delete an event destination

DELETE `/support/ems/destinations/{name}`

Introduced In: 9.6

Deletes an event destination.

Related ONTAP commands

- `event notification destination delete`
- `event notification delete`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Destination name

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983152	Default destinations cannot be modified or removed

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 an event destination

GET `/support/ems/destinations/{name}`

Introduced In: 9.6

Retrieves event destinations.

Expensive properties

There is an added computational cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter.

- `connectivity.*`

Related ONTAP commands

- `event notification destination show`
- `event notification show`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Destination name

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
name	string	Destination name. Valid in POST.
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.
type	string	Type of destination. Valid in POST.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "ca": "VeriSign",
    "name": "cert1",
    "serial_number": 1234567890
  },
  "connectivity": {
    "errors": [
      {
        "message": {
          "arguments": [
            {
              "code": "string",
              "message": "string"
            }
          ],
          "code": "4",
          "message": "entry doesn't exist"
        },
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "node1",
```

```
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          }
        }
      ],
      "state": "fail"
    },
    "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
    "filters": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "important-events"
      }
    ],
    "name": "Admin_Email",
    "syslog": {
      "format": {
        "hostname_override": "string",
        "message": "string",
        "timestamp_override": "string"
      },
      "port": 514,
      "transport": "string"
    },
    "system_defined": 1,
    "type": "email"
}
```


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	

access_control_role

Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

certificate

Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate.

Name	Type	Description
_links	_links	
ca	string	Client certificate issuing CA
name	string	Certificate name
serial_number	string	Client certificate serial number

arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

message

Name	Type	Description
arguments	array[arguments]	Message arguments
code	string	Unique message code.
message	string	User message.

node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

errors

Error object included in the event of connectivity failure.

Name	Type	Description
message	message	
node	node	

connectivity

Name	Type	Description
errors	array[errors]	A list of errors encountered during connectivity checks.
state	string	Current connectivity state.

filters

Name	Type	Description
_links	_links	
name	string	

format

Name	Type	Description
hostname_override	string	Syslog Hostname Format Override. The supported hostname formats are no_override (hostname format based on the syslog.format.message property i.e. fqdn if syslog.format.message is rfc_5424, hostname_only if syslog.format.message is legacy_netapp), fqdn (Fully Qualified Domain Name) and hostname_only.
message	string	Syslog Message Format. The supported message formats are legacy_netapp (format: <PRIVAL>TIMESTAMP [HOSTNAME:Event-name:Event-severity]: MSG) and rfc_5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME Event-source - Event-name - MSG).
timestamp_override	string	Syslog Timestamp Format Override. The supported timestamp formats are no_override (timestamp format based on the syslog.format.message property i.e. rfc_3164 if syslog.format.message is legacy_netapp, iso_8601_local_time if syslog.format.message is rfc_5424), rfc_3164 (format: Mmm dd hh:mm:ss), iso_8601_local_time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm) and iso_8601_utc (format: YYYY-MM-DDThh:mm:ssZ).

syslog

Name	Type	Description
format	format	
port	integer	Syslog Port.

Name	Type	Description
transport	string	Syslog Transport Protocol.

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 an event destination

PATCH `/support/ems/destinations/{name}`

Introduced In: 9.6

Updates an event destination.

Recommended optional properties

- `filters.name` - New list of filters that should direct to this destination. The existing list is discarded.
- `certificate` - New certificate parameters when the destination type is `rest api`.

Related ONTAP commands

- `event notification destination modify`
- `event notification modify`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Destination name

Request Body

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.

Example request

```
{
  "certificate": {
    "ca": "VeriSign",
    "name": "cert1",
    "serial_number": 1234567890
  },
  "connectivity": {
    "errors": [
      {
        "message": {
          "arguments": [
            {
              "code": "string",
              "message": "string"
            }
          ],
          "code": "4",
          "message": "entry doesn't exist"
        },
        "node": {
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      }
    ],
    "state": "fail"
  },
  "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
  "filters": [
    {
      "name": "important-events"
    }
  ],
  "syslog": {
    "format": {
      "hostname_override": "string",
      "message": "string",
      "timestamp_override": "string"
    },
    "port": 514,
    "transport": "string"
  },
  "system_defined": 1
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.

Example response

```
{
  "certificate": {
    "ca": "VeriSign",
    "name": "cert1",
    "serial_number": 1234567890
  },
  "connectivity": {
    "errors": [
      {
        "message": {
          "arguments": [
            {
              "code": "string",
              "message": "string"
            }
          ],
          "code": "4",
          "message": "entry doesn't exist"
        },
        "node": {
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      }
    ],
    "state": "fail"
  },
  "destination": "<a href="
mailto:administrator@mycompany.com">administrator@mycompany.com</a>",
  "filters": [
    {
      "name": "important-events"
    }
  ],
  "syslog": {
    "format": {
      "hostname_override": "string",
      "message": "string",
      "timestamp_override": "string"
    },
    "port": 514,
    "transport": "string"
  },
  "system_defined": 1
}
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983088	The destination name provided cannot be empty
983089	The destination name provided cannot contain spaces
983094	The destination name provided is invalid. The destination name must contain between 2 and 64 characters and start and end with an alphanumeric symbol or _(underscore). The allowed special characters are _(underscore) and -(hyphen)
983104	The syslog destination provided is invalid
983107	A provided filter does not exist
983116	The number of notifications has reached maximum capacity
983117	The number of destinations has reached maximum capacity
983129	The rest-api destination must contain a valid scheme, such as http// or https//
983130	The rest-api destination provided contains an invalid URL
983131	The rest-api destination provided contains an invalid IPv6 URL
983142	The security certificate provided does not exist
983143	The private security key provided does not exist
983144	The security certificate information provided is incomplete. Provide the certificate and serial number
983145	The rest-api destination provided has an 'http://' scheme. It is invalid to provide certificate information
983150	The type of an existing destination cannot be changed
983152	Default destinations cannot be modified or removed
983184	A provided property cannot be configured on the requested destination type
983200	Access control role compatibility issue with provided filters

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Indicates the access control role that created the event destination and is used to control access to the destination based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

certificate

Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate.

Name	Type	Description
_links	_links	
ca	string	Client certificate issuing CA
name	string	Certificate name
serial_number	string	Client certificate serial number

arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

message

Name	Type	Description
arguments	array[arguments]	Message arguments
code	string	Unique message code.
message	string	User message.

node

Name	Type	Description
name	string	
uuid	string	

errors

Error object included in the event of connectivity failure.

Name	Type	Description
message	message	
node	node	

connectivity

Name	Type	Description
errors	array[errors]	A list of errors encountered during connectivity checks.
state	string	Current connectivity state.

filters

Name	Type	Description
name	string	

format

Name	Type	Description
hostname_override	string	Syslog Hostname Format Override. The supported hostname formats are no_override (hostname format based on the syslog.format.message property i.e. fqdn if syslog.format.message is rfc_5424, hostname_only if syslog.format.message is legacy_netapp), fqdn (Fully Qualified Domain Name) and hostname_only.
message	string	Syslog Message Format. The supported message formats are legacy_netapp (format: <PRIVAL>TIMESTAMP [HOSTNAME:Event-name:Event-severity]: MSG) and rfc_5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME Event-source - Event-name - MSG).
timestamp_override	string	Syslog Timestamp Format Override. The supported timestamp formats are no_override (timestamp format based on the syslog.format.message property i.e. rfc_3164 if syslog.format.message is legacy_netapp, iso_8601_local_time if syslog.format.message is rfc_5424), rfc_3164 (format: Mmm dd hh:mm:ss), iso_8601_local_time (format: YYYY-MM-DDThh:mm:ss+/-hh:mm) and iso_8601_utc (format: YYYY-MM-DDThh:mm:ssZ).

syslog

Name	Type	Description
format	format	
port	integer	Syslog Port.

Name	Type	Description
transport	string	Syslog Transport Protocol.

ems_destination

Name	Type	Description
certificate	certificate	Specifies the client-side certificate used by the ONTAP system when mutual authentication is required. This object is only applicable for **rest_api** type destinations. Both the `ca` and `serial_number` fields must be specified when configuring a certificate in a PATCH or POST request. The `name` field is read-only and cannot be used to configure a client-side certificate. • Introduced in: 9.6
connectivity	connectivity	
destination	string	Event destination
filters	array[filters]	
syslog	syslog	
system_defined	boolean	Flag indicating system-defined destinations.

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

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve events

Support EMS events endpoint overview

Overview

Queries a live collection of observed events on the system. Note: The `filter.name` parameter is used to pass a filter to be applied to the event collection returned. To retrieve the list of available filters, refer to /support/ems/filters

Example

Querying for the latest event received by EMS

```
# The API:
GET /api/support/ems/events

# The call:
curl -X GET "https://<mgmt-
ip>/api/support/ems/events?fields=message.name&max_records=1" -H "accept:
application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "node": {
      "name": "node1",
      "uuid": "f087b8e3-99ac-11e8-b5a5-005056bb4ec7",
      "_links": {
        "self": {
          "href": "/api/cluster/nodes/f087b8e3-99ac-11e8-b5a5-
005056bb4ec7"
        }
      }
    },
    "index": 661,
    "message": {
      "name": "raid.aggr.log.CP.count"
    },
    "_links": {
      "self": {
        "href": "/api/support/ems/events/node1/661"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/ems/events?fields=message.name&max_records=1"
  },
}
}
```

Retrieve observed events

GET `/support/ems/events`

Introduced In: 9.6

Retrieves a collection of observed events.

Related ONTAP commands

- `event log show`

Parameters

Name	Type	In	Required	Description
index	integer	query	False	Filter by index
parameters.value	string	query	False	Filter by parameters.value
parameters.name	string	query	False	Filter by parameters.name
time	string	query	False	Filter by time
source	string	query	False	Filter by source
message.severity	string	query	False	Filter by message.severity
message.name	string	query	False	Filter by message.name
log_message	string	query	False	Filter by log_message
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
filter.name	string	query	False	Filter the collection returned using an event filter • Introduced in: 9.8

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "log_message": "string",
      "message": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "callhome.spares.low",
        "severity": "emergency"
      },
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "parameters": [
        {
          "name": "numOps",
          "value": 123
        }
      ],
      "source": "string",
```

```
      "time": "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	

self

Name	Type	Description
href	string	

_links

Name	Type	Description
self	self	

_links

Name	Type	Description
self	href	

message

Name	Type	Description
_links	_links	
name	string	Message name of the event. Returned by default.
severity	string	Severity of the event. Returned by default.

node

Name	Type	Description
_links	_links	
name	string	

Name	Type	Description
uuid	string	

parameters

Name	Type	Description
name	string	Name of parameter
value	string	Value of parameter

records

Name	Type	Description
_links	_links	
index	integer	Index of the event. Returned by default.
log_message	string	A formatted text string populated with parameter details. Returned by default.
message	message	
node	node	
parameters	array[parameters]	A list of parameters provided with the EMS event.
source	string	Source
time	string	Timestamp of the event. Returned by default.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create or retrieve event filters

Support EMS filters endpoint overview

Overview

Manages the list of available filters. A filter is a named collection of rules that enable the system to identify events that require additional handling. A filter is linked with a destination to which the system sends specific events.

When EMS processes an event, each filter is evaluated for a match. More than one filter can handle a single event.

The system defines default filters that cannot be removed or modified. These filters are specified by setting the "system_defined" field to "true".

Filter rule position

A filter's rules are evaluated sequentially, according to their position index. When a rule is added or modified, the position can be set to customize the filter's logic. If no position is specified, a new rule is appended to the end of the list.

Filter rule types

A filter rule can be one of two types: 'include' or 'exclude'. If an event matches the criteria of the rule, the type dictates whether it should be forwarded to the destination or ignored.

Filter rule matching criteria

A valid filter rule must contain at least one set of criteria.

Name pattern

A name pattern is matched against an event's name. Multiple characters can be matched using the wildcard character '*'.

Severity

The severity pattern is matched against an event's severity. Multiple severities can be specified in a comma separated list. A single wildcard '*' will match all severities. Valid values are:

- emergency
- alert
- error
- notice
- informational
- debug

SNMP trap type

The SNMP trap type pattern is matched against an event’s trap type. Multiple trap types can be specified in a comma separated list. A single wildcard '*' matches all trap types. Valid values are:

- standard
- built_in
- severity_based

Parameter criteria

A parameter criterion is matched against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.

Examples

Retrieving a list of filters whose names contain a hyphen

```
# The API:
GET /api/support/ems/filters

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/filters?name=*-*" -H
"accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "name": "default-trap-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/default-trap-events"
      }
    }
  },
  {
    "name": "important-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/important-events"
      }
    }
  },
  {
    "name": "no-info-debug-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/no-info-debug-events"
      }
    }
  }
],
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/support/ems/filters?name=*-*"
  }
}
}
```

Creating a new filter using various matching criteria

```
# The API:
POST /api/support/ems/filters

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/filters" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filters_post.txt"
test_ems_filters_post.txt(body):
{
"name": "test-filter",
"rules": [
  {
    "index": 1,
    "type": "include",
    "message_criteria": {
      "name_pattern": "LUN.*",
      "severities": "alert,error",
      "snmp_trap_types": "severity_based"
    },
    "parameter_criteria": [
      {
        "name_pattern": "type",
        "value_pattern": "volume"
      },
      {
        "name_pattern": "vol",
        "value_pattern": "cloud*"
      }
    ]
  }
]
}

# The response:
201 Created
```

Retrieve event filters

GET `/support/ems/filters`

Introduced In: 9.6

Retrieves a collection of event filters.

Related ONTAP commands

- `event filter show`

Parameters

Name	Type	In	Required	Description
rules.type	string	query	False	Filter by rules.type
rules.message_criteria.name_pattern	string	query	False	Filter by rules.message_criteria.name_pattern
rules.message_criteria.snmp_trap_types	string	query	False	Filter by rules.message_criteria.snmp_trap_types
rules.message_criteria.severities	string	query	False	Filter by rules.message_criteria.severities
rules.index	integer	query	False	Filter by rules.index
rules.parameter_criteria.name_pattern	string	query	False	Filter by rules.parameter_criteria.name_pattern • Introduced in: 9.13
rules.parameter_criteria.value_pattern	string	query	False	Filter by rules.parameter_criteria.value_pattern • Introduced in: 9.13
name	string	query	False	Filter by name
access_control_role.name	string	query	False	Filter by access_control_role.name • Introduced in: 9.13

Name	Type	In	Required	Description
system_defined	boolean	query	False	Filter by system_defined • Introduced in: 9.10
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_control_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "name": "snmp-traphost",
      "rules": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "index": 1,
          "message_criteria": {
            "_links": {
              "related": {
                "href": "/api/resourcelink"
              }
            },
            "name_pattern": "callhome.*",
            "severities": "error,informational",
            "snmp_trap_types": "standard|built_in"
          },
```

```
          "parameter_criteria": [
            {
              "name_pattern": "vol",
              "value_pattern": "cloud*"
            }
          ],
          "type": "include"
        }
      ],
      "system_defined": 1
    }
  ]
}
```


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	

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.

Name	Type	Description
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

records

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

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.

Create an event filter

POST `/support/ems/filters`

Introduced In: 9.6

Creates an event filter.

Required properties

- `name` - String that uniquely identifies the filter.

Recommended optional properties

- `rules` - List of criteria which is used to match a filter with an event.

Related ONTAP commands

- `event filter create`

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

Example request

```
{
  "name": "snmp-traphost",
  "rules": [
    {
      "index": 1,
      "message_criteria": {
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ],
  "system_defined": 1
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "name": "snmp-traphost",
      "rules": [
        {
          "index": 1,
          "message_criteria": {
            "name_pattern": "callhome.*",
            "severities": "error,informational",
            "snmp_trap_types": "standard|built_in"
          },
          "parameter_criteria": [
            {
              "name_pattern": "vol",
              "value_pattern": "cloud*"
            }
          ],
          "type": "include"
        }
      ],
      "system_defined": 1
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983088	The filter name provided is empty

Error Code	Description
983089	The filter name provided cannot contain spaces
983092	The index of the rule provided is outside the allowed range for the filter provided
983094	The filter name provided is invalid. The filter name must contain between 2 and 64 characters and start and end with an alphanumeric symbol or (underscore). The allowed special characters are (underscore) and -(hyphen)
983095	The rule index provided is invalid for the filter provided
983101	No event is matched by the rule provided
983113	Default filters cannot be modified or removed
983114	The maximum number of filters is reached
983115	The maximum number of filter rules is reached
983126	A rule requires at least one name_pattern, severities, snmp_trap_types, or parameter pattern to be defined
983127	A property cannot contain a combination of the wildcard character and other values
983128	An invalid value is provided for the property 'snmp_trap_types'
983146	An invalid value is provided for the property 'severities'
983147	The severities provided are not supported
983155	The provided severities property does not match that of the name_pattern
983156	The provided snmp_trap_types property does not match that of the name_pattern
983157	The provided severities and snmp_trap_types properties do not match those of the name_pattern
983158	The name_pattern provided does not exist
983195	Empty field in parameter_criteria. Both name and value patterns must be specified
983196	name_pattern and value_pattern fields in parameter_criteria are empty
983211	Parameter criteria based filtering is not supported in this version of ONTAP

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
name	string	Role name

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

ems_filter

Name	Type	Description
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

records

Name	Type	Description
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

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.

Manage event filters

Support EMS filters name endpoint overview

Overview

Manages a specific filter instance. See the documentation for /support/ems/filters for details on the various properties.

Examples

Retrieving a specific filter instance

```
# The API:
GET /api/support/ems/filters/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/filters/aggregate-events"
-H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
```

```
"name": "aggregate-events",
"rules": [
  {
    "index": 1,
    "type": "include",
    "message_criteria": {
      "name_pattern": "*",
      "severities": "emergency,alert,error,notice",
      "snmp_trap_types": "*",
      "_links": {
        "related": {
          "href":
"/api/support/ems/messages?name=*&severity=emergency,alert,error,notice&sn
mp_trap_type=*"
        }
      }
    },
    "parameter_criteria": [
      {
        "name_pattern": "type",
        "value_pattern": "aggregate"
      }
    ],
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/aggregate-events/rules/1"
      }
    }
  },
  {
    "index": 2,
    "type": "exclude",
    "message_criteria": {
      "name_pattern": "*",
      "severities": "*",
      "snmp_trap_types": "*",
      "_links": {
        "related": {
          "href":
"/api/support/ems/messages?name=*&severity=*&snmp_trap_type=*"
        }
      }
    },
    "parameter_criteria": [
      {
        "name_pattern": "*",
```

```
        "value_pattern": "*"
      }
    ],
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/aggregate-events/rules/2"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/support/ems/filters/aggregate-events"
  }
}
}
```

Updating an existing filter with a new rule

```
# The API:
PATCH /api/support/ems/filters/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/ems/filters/test-filter" -H
"accept: application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filters_patch.txt"
test_ems_filters_patch.txt(body):
{
"rules": [
  {
    "type": "include",
    "message_criteria": {
      "name_pattern": "wafl.*",
      "severities": "error"
    }
  }
]
}

# The response:
200 OK
```

Deleting an existing filter

```
# The API:
DELETE /api/support/ems/filters/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/ems/filters/test-filter" -H
"accept: application/hal+json"

# The response:
200 OK
```

Delete an event filter

DELETE `/support/ems/filters/{name}`

Introduced In: 9.6

Deletes an event filter.

Related ONTAP commands

- `event filter delete`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983113	Default filters cannot be modified or removed
983124	Filter is being referenced by a destination
983204	Filter is being used for role-based operations

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 an event filter

GET `/support/ems/filters/{name}`

Introduced In: 9.6

Retrieves an event filter.

Related ONTAP commands

- `event filter show`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "name": "snmp-traphost",
  "rules": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "message_criteria": {
        "_links": {
          "related": {
            "href": "/api/resourcelink"
          }
        },
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ],
  "system_defined": 1
}
```

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	

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

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 an event filter

PATCH `/support/ems/filters/{name}`

Introduced In: 9.6

Updates an event filter.

Recommended optional properties

- `new_name` - New string that uniquely identifies a filter.
- `rules` - New list of criteria used to match the filter with an event. The existing list is discarded.

Related ONTAP commands

- `event filter rename`
- `event filter rule add`
- `event filter rule delete`
- `event filter rule reorder`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
new_name	string	query	False	New filter name for renames. Valid in PATCH.

Request Body

Name	Type	Description
name	string	Filter name

Name	Type	Description
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

Example request

```
{
  "name": "snmp-traphost",
  "rules": [
    {
      "index": 1,
      "message_criteria": {
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ],
  "system_defined": 1
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983088	The filter name provided is empty
983089	The filter name provided cannot contain spaces
983092	The index of the rule provided is outside the allowed range for the filter provided
983094	The filter name provided is invalid. The filter name must contain between 2 and 64 characters and start and end with an alphanumeric symbol or (underscore). The allowed special characters are (underscore) and -(hyphen)
983095	The rule index provided is invalid for the filter provided
983101	No event is matched by the rule provided
983113	Default filters cannot be modified or removed
983114	The maximum number of filters is reached
983115	The maximum number of filter rules is reached
983126	A rule requires at least one name_pattern, severities, snmp_trap_types, or parameter pattern to be defined
983127	A property cannot contain a combination of the wildcard characters and other values
983128	An invalid value is provided for the property 'snmp_trap_types'
983146	An invalid value is provided for the property 'severities'
983147	The severities provided are not supported
983155	The provided severities property does not match that of the name_pattern
983156	The provided snmp_trap_types property does not match that of the name_pattern
983157	The provided severities and snmp_trap_types properties do not match those of the name_pattern
983158	The name_pattern provided does not exist
983195	Empty field in parameter_criteria. Both name and value patterns must be specified
983196	name_pattern and value_pattern fields in parameter_criteria are empty
983211	Parameter criteria based filtering is not supported in this version of ONTAP

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
name	string	Role name

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

ems_filter

Name	Type	Description
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

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.

Create or retrieve filter rules

Support EMS filters name rules endpoint overview

Overview

Manages the list of rules associated with a specific filter. A filter contains a list of rules that are evaluated to determine whether an event matches the filter. When a rule matches an event, the filter is considered a match. See the documentation for /support/ems/filters for details on the various properties in a rule.

Examples

Retrieving the collection of rules connected to a filter

```
# The API:
GET /api/support/ems/filters/{name}/rules

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/filters/no-info-debug-
events/rules" -H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "index": 1,
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/no-info-debug-events/rules/1"
      }
    }
  },
  {
    "index": 2,
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/no-info-debug-events/rules/2"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/support/ems/filters/no-info-debug-events/rules"
  }
}
}
```

Creating a new rule under an existing filter

The absence of a position index appends the rule to the end of the list.

```
# The API:
POST /api/support/ems/filters/{name}/rules

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/filters/test-filter/rules"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filter_rules_post.txt"
test_ems_filter_rules_post.txt(body):

# JSON Body
{
"type": "include",
"message_criteria": {
  "name_pattern": "wafl.*",
  "severities": "error,informational"
}
}

# The response:
201 Created
```

Retrieve event filter rules

GET `/support/ems/filters/{name}/rules`

Introduced In: 9.6

Retrieves event filter rules.

Related ONTAP commands

- `event filter show`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter Name
type	string	query	False	Filter by type
message_criteria.name_pattern	string	query	False	Filter by message_criteria.name_pattern

Name	Type	In	Required	Description
message_criteria.snmp_trap_types	string	query	False	Filter by message_criteria.snmp_trap_types
message_criteria.severities	string	query	False	Filter by message_criteria.severities
index	integer	query	False	Filter by index
parameter_criteria.name_pattern	string	query	False	Filter by parameter_criteria.name_pattern • Introduced in: 9.13
parameter_criteria.value_pattern	string	query	False	Filter by parameter_criteria.value_pattern • Introduced in: 9.13
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "message_criteria": {
        "_links": {
          "related": {
            "href": "/api/resourcelink"
          }
        },
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ]
}
```


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	

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

records

Rule for an event filter

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

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.

Create an event filter rule

POST `/support/ems/filters/{name}/rules`

Introduced In: 9.6

Creates an event filter rule.

Required properties

- `type` - Enumeration indicating whether the rule is for include or exclude.
- `message_criteria` - Message criteria used by a rule to match an event.
- `parameter_criteria` - Parameter criteria used by a rule to match an event. Note: At least one pattern needs to be provided for message_criteria and / or parameter_criteria.

Recommended optional properties

- `index` - One-based position index of the new rule.

Related ONTAP commands

- `event filter rule add`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

Example request

```
{
  "index": 1,
  "message_criteria": {
    "name_pattern": "callhome.*",
    "severities": "error,informational",
    "snmp_trap_types": "standard|built_in"
  },
  "parameter_criteria": [
    {
      "name_pattern": "vol",
      "value_pattern": "cloud*"
    }
  ],
  "type": "include"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "index": 1,
      "message_criteria": {
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983092	The index of the rule provided is outside the allowed range for the filter provided
983095	The rule index provided is invalid for the filter provided
983113	Default filters cannot be modified or removed
983115	The maximum number of filter rules is reached
983126	A rule requires at least one name_pattern, severities, snmp_trap_types, or parameter pattern to be defined
983127	A property cannot contain a combination of the wildcard characters and other values
983128	An invalid value is provided for the property 'snmp_trap_types'
983146	An invalid value is provided for the property 'severities'
983147	The severities provided are not supported
983155	The provided severities property does not match that of the name_pattern
983156	The provided snmp_trap_types property does not match that of the name_pattern
983157	The provided severities and snmp_trap_types properties do not match those of the name_pattern
983158	The name_pattern provided does not exist
983195	Empty field in parameter_criteria. Both name and value patterns must be specified
983196	name_pattern and value_pattern fields in parameter_criteria are empty
983211	Parameter criteria based filtering is not supported in this version of ONTAP

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

ems_filter_rule

Rule for an event filter

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.

Name	Type	Description
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

records

Rule for an event filter

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

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.

Manage event filter rules

Support EMS filters name rules index endpoint overview

Overview

Manages a specific instance of a rule within a filter. See the documentation for /support/ems/filters for details on the various properties in a rule.

Examples

Retrieving a single instance of a rule

```
# The API:
GET /api/support/ems/filters/{name}/rules/{index}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/filters/no-info-debug-
events/rules/1" -H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"name": "no-info-debug-events",
"index": 1,
"type": "include",
"message_criteria": {
  "name_pattern": "*",
  "severities": "emergency,alert,error,notice",
  "snmp_trap_types": "*",
  "_links": {
    "self": {
      "href":
"/api/support/ems/messages?name=*&severity=emergency,alert,error,notice&sn
mp_trap_type=*"
    }
  }
},
"parameter_criteria": [
  {
    "name_pattern": "*",
    "value_pattern": "*"
  }
],
"_links": {
  "self": {
    "href": "/api/support/ems/filters/no-info-debug-events/rules/1"
  }
}
}
```

Updating an existing rule to use severity emergency

```
# The API:
PATCH /api/support/ems/filters/{name}/rules/{index}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/ems/filters/test-
filter/rules/1" -H "accept: application/hal+json" -H "Content-Type:
application/json" -d "@test_ems_filter_rules_patch.txt"
test_ems_filter_rules_patch.txt(body):
{
"message_criteria": {
  "severities": "emergency"
}
}

# The response:
200 OK
```

Deleting a rule from an existing filter

```
# The API:
DELETE /api/support/ems/filters/{name}/rules/{index}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/ems/filters/test-
filter/rules/1" -H "accept: application/hal+json"

# The response:
200 OK
```

Delete an event filter rule

DELETE `/support/ems/filters/{name}/rules/{index}`

Introduced In: 9.6

Deletes an event filter rule.

Related ONTAP commands

- `event filter rule delete`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
index	string	path	True	Filter rule index

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983091	A default rule cannot be removed
983092	The index of the rule provided is outside the allowed range for the filter provided
983095	The rule index provided is invalid for the filter provided
983110	There are no user defined rules in the filter provided
983113	Default filters cannot be modified or removed

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 an event filter rule

GET `/support/ems/filters/{name}/rules/{index}`

Introduced In: 9.6

Retrieves an event filter rule.

Related ONTAP commands

- `event filter show`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
index	string	path	True	Filter rule index
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "index": 1,
  "message_criteria": {
    "_links": {
      "related": {
        "href": "/api/resourcelink"
      }
    },
    "name_pattern": "callhome.*",
    "severities": "error,informational",
    "snmp_trap_types": "standard|built_in"
  },
  "parameter_criteria": [
    {
      "name_pattern": "vol",
      "value_pattern": "cloud*"
    }
  ],
  "type": "include"
}
```


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	

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

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 an event filter rule

PATCH `/support/ems/filters/{name}/rules/{index}`

Introduced In: 9.6

Updates an event filter rule.

Recommended optional properties

- `message_criteria` - Message criteria used by a rule to match an event.
- `parameter_criteria` - Parameter criteria used by a rule to match an event.

Related ONTAP commands

- `event filter rule add`
- `event filter rule delete`

Parameters

Name	Type	In	Required	Description
name	string	path	True	Filter name
index	string	path	True	Filter rule index

Name	Type	In	Required	Description
new_index	integer	query	False	New position for the filter rule index

Request Body

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

Example request

```
{
  "index": 1,
  "message_criteria": {
    "name_pattern": "callhome.*",
    "severities": "error,informational",
    "snmp_trap_types": "standard|built_in"
  },
  "parameter_criteria": [
    {
      "name_pattern": "vol",
      "value_pattern": "cloud*"
    }
  ],
  "type": "include"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983092	The index of the rule provided is outside the allowed range for the filter provided
983095	The rule index provided is invalid for the filter provided
983113	Default filters cannot be modified or removed
983126	A rule requires at least one name_pattern, severities, snmp_trap_types, or parameter pattern to be defined
983127	A property cannot contain a combination of the wildcard characters and other values.
983128	An invalid value is provided for the property 'snmp_trap_types'
983146	An invalid value is provided for the property 'severities'

Error Code	Description
983147	The severities provided are not supported
983155	The provided severities property does not match that of the name_pattern
983156	The provided snmp_trap_types property does not match that of the name_pattern
983157	The provided severities and snmp_trap_types properties do not match those of the name_pattern
983158	The name_pattern provided does not exist
983195	Empty field in parameter_criteria. Both name and value patterns must be specified
983196	name_pattern and value_pattern fields in parameter_criteria are empty
983211	Parameter criteria based filtering is not supported in this version of ONTAP

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

ems_filter_rule

Rule for an event filter

Name	Type	Description
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.

Name	Type	Description
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

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.

Manage the EMS event catalog

Support EMS messages endpoint overview

Overview

Allows access to the EMS event catalog. The catalog contains a list of all events supported by the system and their corresponding descriptions, the reason for an event occurrence, and how to correct issues related to the

event.

Example

Querying for the first event that has a message name beginning with 'C'

```
# The API:
GET /api/support/ems/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/support/ems/messages?fields=name&max_records=1&name=C*" -H
"accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "name": "CR.Data.File.Inaccessible",
    "_links": {
      "self": {
        "href": "/api/support/ems/messages/CR.Data.File.Inaccessible"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/ems/messages?fields=name&max_records=1&name=C*"
  },
}
}
```

Retrieve event catalog definitions

GET `/support/ems/messages`

Introduced In: 9.6

Retrieves the event catalog definitions.

Related ONTAP commands

- `event catalog show`

Parameters

Name	Type	In	Required	Description
severity	string	query	False	Filter by severity
corrective_action	string	query	False	Filter by corrective_action
deprecated	boolean	query	False	Filter by deprecated
name	string	query	False	Filter by name
snmp_trap_type	string	query	False	Filter by snmp_trap_type
description	string	query	False	Filter by description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "corrective_action": "string",
      "deprecated": 1,
      "description": "string",
      "name": "callhome.spares.low",
      "severity": "error",
      "snmp_trap_type": "standard"
    }
  ]
}
```


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	

records

Name	Type	Description
_links	_links	
corrective_action	string	Corrective action
deprecated	boolean	Is deprecated?
description	string	Description of the event.
name	string	Name of the event.
severity	string	Severity
snmp_trap_type	string	SNMP trap type

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.

View and create EMS role configurations

Support EMS role-configs endpoint overview

Overview

Manages the list of access control roles that have limited access to the EMS events and configurations. Access to the EMS events and configurations are controlled by the EMS role-based configuration, which has the following two properties:

- `event_filter`
- `limit_access_to_global_configs`

Role-based event filter

A role-based event filter is a filter assigned to an access control role that limits what events users of that role have access to. It is applied transparently when a user of that role performs GET requests on the following endpoints:

- `/support/ems/events`
- `/support/ems/messages`

It is also applied when events are forwarded as notifications to destinations created by users of that role. To those destinations, only events that match the role-based filter in addition to the filters configured on the destinations are forwarded.

Limiting access to the global EMS configurations

The APIs at the `/api/support/ems` endpoint expose several configuration properties that affect how EMS handles events. The following properties are always accessible by all roles that have access to the `/api/support/ems` APIs.

- `mail_from`
- `mail_server`
- `proxy_url`
- `proxy_user`

- `proxy_password`

Access to the following property by an access control role can be restricted:

- `pubsub_enabled`

Limiting access to EMS events and configurations is typically applied for an access control role that is designed to have limited administrative capabilities. For example, when the cluster is physically managed by a service provider and the services are managed by the customer.

Examples

Retrieving the list of EMS role-based configurations

```
# The API:
GET /api/support/ems/role-configs

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/role-configs" -H "accept:
application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "access_control_role": {
      "name": "storage-admin",
      "_links": {
        "self": {
          "href": "/api/security/roles/0b2580c8-de36-4213-bfca-
88cdaaaf3ae6/storage-admin"
        }
      }
    },
    "event_filter": {
      "name": "storage-admin-events",
      "_links": {
        "self": {
          "href": "/api/support/ems/filters/storage-admin-events"
        }
      }
    },
    "limit_access_to_global_configs": true,
    "_links": {
      "self": {
```

```
        "href": "/api/support/ems/role-configs/storage-admin"
      }
    }
  },
  {
    "access_control_role": {
      "name": "network-admin",
      "_links": {
        "self": {
          "href": "/api/security/roles/0b2580c8-de36-4213-bfca-
88cdaaaf3ae6/network-admin"
        }
      }
    },
    "filter_filter": {
      "name": "network-admin-events",
      "_links": {
        "self": {
          "href": "/api/support/ems/filters/network-admin-events"
        }
      }
    },
    "limit_access_to_global_configs": true,
    "_links": {
      "self": {
        "href": "/api/support/ems/role-configs/network-admin"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/support/ems/role-configs"
  }
}
}
```


Creating an EMS role-based configuration for an access control role

```
# The API:
POST /api/support/ems/role-configs

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/role-configs" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@role_configs_post.txt"
role_configs_post.txt(body):
{
"access_control_role": {
  "name": "storage-admin"
},
"event_filter": {
  "name": "storage-admin-events"
},
"limit_access_to_global_configs": true
}

# The response:
201 Created
```

Retrieve EMS role-based configurations

GET `/support/ems/role-configs/{access_control_role.name}`

Introduced In: 9.13

Retrieves the EMS role-based configuration of the access control role.

Related ONTAP commands

- `event role-config show`

Parameters

Name	Type	In	Required	Description
access_control_role.name	string	path	True	Access control role name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Access control role that the event filter is assigned to.
event_filter	event_filter	Event filter that is assigned to the access control role.
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "event_filter": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "important-events"
  }
}
```

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	

access_control_role

Access control role that the event filter is assigned to.

Name	Type	Description
_links	_links	
name	string	Role name

event_filter

Event filter that is assigned to the access control role.

Name	Type	Description
_links	_links	
name	string	

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.

Create role configurations

POST `/support/ems/role-configs`

Introduced In: 9.13

Creates an EMS role-based configuration for an access control role.

Required properties

- `access_control_role` - Uniquely identifies the access control role.

Recommended optional properties

- `event_filter` - Identifies the event filter.
- `limit_access_to_global_configs` - Indicates whether the access control role has limited access to global EMS configurations.

Related ONTAP commands

- `event role-config create`

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
access_control_role	access_control_role	Access control role that the event filter is assigned to.
event_filter	event_filter	Event filter that is assigned to the access control role.

Name	Type	Description
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

Example request

```
{
  "access_control_role": {
    "name": "admin"
  },
  "event_filter": {
    "name": "important-events"
  }
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[records]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "access_control_role": {
        "name": "admin"
      },
      "event_filter": {
        "name": "important-events"
      }
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983198	The event filter provided does not exist.
983199	The access control role provided does not exist.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Access control role that the event filter is assigned to.

Name	Type	Description
name	string	Role name

event_filter

Event filter that is assigned to the access control role.

Name	Type	Description
name	string	

ems_role_config

Name	Type	Description
access_control_role	access_control_role	Access control role that the event filter is assigned to.
event_filter	event_filter	Event filter that is assigned to the access control role.
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

records

Name	Type	Description
access_control_role	access_control_role	Access control role that the event filter is assigned to.
event_filter	event_filter	Event filter that is assigned to the access control role.

Name	Type	Description
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

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.

Manage EMS role configurations

Support EMS role-configs access_control_role.name endpoint overview

Overview

Manages the EMS role-based configuration of a specific access control role.

See the documentation for /support/ems/role-configs for details on the various properties.

Examples

Retrieving the EMS role-based configuration of an access control role

```
# The API:
GET /api/support/ems/role-configs/{access_control_role.name}

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/role-configs/storage-admin"
-H "accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"access_control_role": {
  "name": "storage-admin",
  "_links": {
    "self": {
      "href": "/api/security/roles/0b2580c8-de36-4213-bfca-
88cdaaaf3ae6/storage-admin"
    }
  }
},
"event_filter": {
  "name": "storage-admin-events",
  "_links": {
    "self": {
      "href": "/api/support/ems/filters/storage-admin-events"
    }
  },
  "limit_access_to_global_configs": true
},
"_links": {
  "self": {
    "href": "/api/support/ems/role-configs/storage-admin"
  }
}
}
```

Updating the EMS role-based configuration of an access control role

```
# The API:
PATCH /api/support/ems/event-configs/{access_control_role.name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/ems/role-configs/storage-
admin" -H "accept: application/hal+json" -H "Content-Type:
application/json" -d "@role_configs_patch.txt"
role_configs_patch.txt(body):
{
"event_filter": {
  "name": "new-storage-admin-events"
},
"limit_access_to_global_configs": false
}

# The response:
200 OK
```

Removing the EMS role-based configuration of an access control role

```
# The API:
DELETE /api/support/ems/role-configs/{access_control_role.name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/ems/role-configs/storage-
admin" -H "accept: application/hal+json"

# The response:
200 OK
```

Delete EMS role-based configurations

DELETE `/support/ems/role-configs/{access_control_role.name}`

Introduced In: 9.13

Removes the EMS role-based configuration of the access control role.

Related ONTAP commands

- `event role-config delete`

Parameters

Name	Type	In	Required	Description
access_control_role.name	string	path	True	Access control role name

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 EMS role-based configurations

GET `/support/ems/role-configs/{access_control_role.name}`

Introduced In: 9.13

Retrieves the EMS role-based configuration of the access control role.

Related ONTAP commands

- `event role-config show`

Parameters

Name	Type	In	Required	Description
access_control_role.name	string	path	True	Access control role name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Access control role that the event filter is assigned to.
event_filter	event_filter	Event filter that is assigned to the access control role.
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "event_filter": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "important-events"
  }
}
```

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	

access_control_role

Access control role that the event filter is assigned to.

Name	Type	Description
_links	_links	
name	string	Role name

event_filter

Event filter that is assigned to the access control role.

Name	Type	Description
_links	_links	
name	string	

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.

Update EMS role-based configurations

PATCH `/support/ems/role-configs/{access_control_role.name}`

Introduced In: 9.13

Updates the EMS role-based configuration of the access control role.

Recommended optional properties

- `event_filter` - Identifies the event filter.
- `limit_access_to_global_configs` - Indicates whether the access control role has limited access to global EMS configurations.

Related ONTAP commands

- `event role-config modify`

Parameters

Name	Type	In	Required	Description
access_control_role.name	string	path	True	Access control role name

Request Body

Name	Type	Description
event_filter	event_filter	Event filter that is assigned to the access control role.
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

Example request

```
{
  "event_filter": {
    "name": "important-events"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983197	The event filter provided is the same as the currently assigned filter.
983198	The event filter provided does not exist.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

access_control_role

Access control role that the event filter is assigned to.

Name	Type	Description
name	string	Role name

event_filter

Event filter that is assigned to the access control role.

Name	Type	Description
name	string	

ems_role_config

Name	Type	Description
event_filter	event_filter	Event filter that is assigned to the access control role.
limit_access_to_global_configs	boolean	Indicates whether the access control has limited access to global EMS configurations.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage cluster-wide SNMP configuration

Support SNMP endpoint overview

Overview

Cluster wide SNMP configuration. You can configure or retrieve the following SNMP parameters using this endpoint:

- enable or disable SNMP
- enable or disable SNMP authentication traps
- enable or disable SNMP traps

This endpoint can also be used to trigger an SNMP test trap.

Examples

Disables SNMP protocol in the cluster.

```
# The API:
PATCH "/api/support/snmp"

# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d '{"enabled":"false"}'

# The response
200 OK
{}
```

Enables SNMP authentication traps in the cluster.

```
# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d
'{"auth_traps_enabled":"true"}'

# The response
200 OK
{}
```

Enables SNMP protocol and SNMP authentication traps in the cluster.

```
# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d '{"enabled":"true",
"auth_traps_enabled":"true"}'

# The response
200 OK
{}
```

Disables the SNMP trap subsystem in the cluster. Once the SNMP trap subsystem is disabled, the cluster stops sending SNMP traps.

```
# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d '{"traps_enabled":"false"}'

# The response
200 OK
{}
```

Triggers an SNMP test trap.

```
# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d
'{"trigger_test_trap":"true"}'

#The response
200 OK
{}
```

Enables the SNMP protocol in the cluster, SNMP traps, and triggers an SNMP test trap.

```
# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-ip>/api/support/snmp" -d '{"enabled":"true",
"traps_enabled":"true", "trigger_test_trap":"true"}'

# The response
200 OK
{}
```

Retrieve the cluster-wide SNMP configuration

GET `/support/snmp`

Introduced In: 9.7

Retrieves the cluster wide SNMP configuration.

Related ONTAP commands

- `options snmp.enable`
- `system snmp show`

Learn more

- DOC /support/snmp

Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
auth_traps_enabled	boolean	Specifies whether to enable or disable SNMP authentication traps.
enabled	boolean	Specifies whether to enable or disable SNMP.
traps_enabled	boolean	Specifies whether to enable or disable SNMP traps.
trigger_test_trap	boolean	Trigger a test SNMP trap.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "auth_traps_enabled": 1,
  "enabled": 1,
  "traps_enabled": 1,
  "trigger_test_trap": 1
}
```


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	

self_link

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

Update the cluster-wide SNMP configuration

PATCH `/support/snmp`

Introduced In: 9.7

Updates the cluster wide SNMP configuration, such as, enabling or disabling SNMP, enabling or disabling SNMP traps, and enabling or disabling authentication traps. It can also be used to trigger an SNMP test trap.

Related ONTAP commands

- `options snmp.enable`
- `system snmp authtrap`

- `system snmp init`

Learn more

- DOC /support/snmp

Request Body

Name	Type	Description
auth_traps_enabled	boolean	Specifies whether to enable or disable SNMP authentication traps.
enabled	boolean	Specifies whether to enable or disable SNMP.
traps_enabled	boolean	Specifies whether to enable or disable SNMP traps.
trigger_test_trap	boolean	Trigger a test SNMP trap.

Example request

```
{
  "auth_traps_enabled": 1,
  "enabled": 1,
  "traps_enabled": 1,
  "trigger_test_trap": 1
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1179738	Cluster identification not available for modification since a cluster has not been created.

Error Code	Description
1179739	Cluster identification modification is not available in maintenance mode or other boot modes.

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

snmp

Cluster-wide SNMP configuration.

Name	Type	Description
auth_traps_enabled	boolean	Specifies whether to enable or disable SNMP authentication traps.
enabled	boolean	Specifies whether to enable or disable SNMP.
traps_enabled	boolean	Specifies whether to enable or disable SNMP traps.
trigger_test_trap	boolean	Trigger a test SNMP trap.

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.

Create or retrieve SNMP traphosts

Support SNMP traphosts endpoint overview

Overview

This SNMP endpoint is used to retrieve, configure and reconfigure SNMP traphosts. An SNMP traphost is a host machine that is configured to receive SNMP traps from ONTAP. An SNMP traphost can be an SNMPv1/SNMPv2c traphost or an SNMPv3 traphost. ONTAP sends SNMPv1/SNMPv2c traps to an SNMPv1/SNMPv2c traphost over the SNMPv1/SNMPv2c protocol. Similarly, it sends SNMPv3 traps to an SNMPv3 traphost over the SNMPv3 protocol.

Examples

Retrieves a list of SNMP traphosts in the cluster, sorted by IP address

```
# The API:
GET "/api/support/snmp/traphosts"

# The call:
curl -H "accept: application/hal+json" -X GET "https://<mgmt-
ip>/api/support/snmp/traphosts?order_by=ip_address"

# The response:
{
"records": [
  {
    "host": "scspr0651011001.gdl.englab.netapp.com",
    "ip_address": "10.235.36.62",
    "_links": {
      "self": {
        "href":
"/api/support/snmp/traphosts/scspr0651011001.gdl.englab.netapp.com"
      }
    }
  },
  {
    "host": "scspr0647726006.gdl.englab.netapp.com",
    "ip_address": "10.235.36.139",
    "_links": {
      "self": {
        "href":
"/api/support/snmp/traphosts/scspr0647726006.gdl.englab.netapp.com"
      }
    }
  },
  {
```

```
    "host": "scspr0651055012.gdl.englab.netapp.com",
    "ip_address": "10.237.245.106",
    "_links": {
      "self": {
        "href":
"/api/support/snmp/traphosts/scspr0651055012.gdl.englab.netapp.com"
      }
    }
  }
],
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/support/snmp/traphosts?order_by=ip_address"
  }
}
}
```

Retrieves a list of SNMP traphosts in the cluster for which SNMP user is 'snmpv3user1'

```
# The call:
curl -H "accept: application/hal+json" -X GET "https://<mgmt-
ip>/api/support/snmp/traphosts?name=snmpv3user1"

# The response:
{
"records": [
  {
    "host": "scspr0653246020.gdl.englab.netapp.com",
    "user": {
      "name": "snmpv3user1",
      "_links": {
        "self": {
          "href":
"/api/support/snmp/users/800003150558b57e8dbd9ce9119d82005056a7b4e5/snmpv3
user1"
        }
      }
    },
    "_links": {
      "self": {
        "href":
"/api/support/snmp/traphosts/scspr0653246020.gdl.englab.netapp.com"
      }
    }
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/support/snmp/traphosts?user.name=snmpv3user1"
  }
}
}
```

Adds an SNMPv1 or SNMPv2c traphost

```
# The API:
POST "/api/support/snmp/traphosts"

# The call:
curl -H "accept: application/json" -H "Content-Type: application/json" -X
POST "https://<mgmt-ip>/api/support/snmp/traphosts" -d
'{"host":"10.140.128.48"}'

# The response:
201 Created
{}
```

Adds an SNMPv3 traphost

```
# The API:
POST "/api/support/snmp/traphosts"

# The call:
curl -H "accept: application/json" -H "Content-Type: application/json" -X
POST "https://<mgmt-ip>/api/support/snmp/traphosts" -d '{"host":"fd-
geoycpi-uno.gycpi.b.yahoodns.net", "user":{"name":"snmpv3user1"}}'

# The response:
201 Created
{}
```

Retrieve SNMP traphosts

GET `/support/snmp/traphosts`

Introduced In: 9.7

Retrieves the list of SNMP traphosts along with the SNMP users configured for those traphosts.

Related ONTAP commands

- `system snmp traphost show`

Learn more

- DOC /support/snmp/traphosts

Parameters

Name	Type	In	Required	Description
ip_address	string	query	False	Filter by ip_address
host	string	query	False	Filter by host
user.name	string	query	False	Filter by user.name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records.
records	array[snmp_traphost]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "host": "traphost.example.com",
      "ip_address": "10.10.10.7",
      "user": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "snmpv3user3"
      }
    }
  ]
}
```


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	

user

Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

Name	Type	Description
_links	_links	

Name	Type	Description
name	string	Optional SNMPv1/SNMPv2c or SNMPv3 user name. For an SNMPv3 traphost, this object refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this object refers to an SNMP community. For an SNMPv3 traphost, this object is mandatory and refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, ONTAP automatically uses "public", if the same is configured, or any other configured community as user. So, for an SNMPv1 or SNMPv2c traphost, this property should not be provided in the "POST" method. However, the configured community for the SNMPv1/SNMPv2c traphost is returned by the "GET" method. • example: snmpv3user3 • Introduced in: 9.7 • x-nullable: true

snmp_traphost

SNMP manager or host machine that receives SNMP traps from ONTAP.

Name	Type	Description
_links	_links	
host	string	Fully qualified domain name (FQDN), IPv4 address or IPv6 address of SNMP traphost.
ip_address	string	IPv4 or IPv6 address

Name	Type	Description
user	user	Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

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.

Create SNMP traphosts

POST `/support/snmp/traphosts`

Introduced In: 9.7

Creates SNMP traphosts. While adding an SNMPv3 traphost, an SNMPv3 user configured in ONTAP must be specified. ONTAP uses this user's credentials to authenticate and/or encrypt traps sent to this SNMPv3 traphost. While adding an SNMPv1/SNMPv2c traphost, SNMPv1/SNMPv2c user or community need not be specified.

Required properties

- `host` - Fully Qualified Domain Name (FQDN), IPv4 address or IPv6 address of SNMP traphost.

Recommended optional properties

- If `host` refers to an SNMPv3 traphost, the following field is required:
  - `user` - SNMPv3 or User-based Security Model (USM) user.
- For an SNMPv1/SNMPv2c traphost, ONTAP automatically uses 'public' if 'public' is configured or no community is configured. Otherwise, ONTAP uses the first configured community.

Related ONTAP commands

- `system snmp traphost add`

Learn more

- DOC /support/snmp/traphosts

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
host	string	Fully qualified domain name (FQDN), IPv4 address or IPv6 address of SNMP traphost.
user	user	Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

Example request

```
{
  "host": "traphost.example.com",
  "user": {
    "name": "snmpv3user3"
  }
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records.
records	array[snmp_traphost]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "host": "traphost.example.com",
      "user": {
        "name": "snmpv3user3"
      }
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
8847365	Unknown host.
9043969	Duplicate traphost entry.
9043980	IPv6 support is disabled.
9043991	Not a USM user.
9043993	Current cluster version does not support SNMPv3 traps.
9044001	Failed to create SNMPv1 traphost.
9044002	Failed to create SNMPv3 traphost.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

user

Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

Name	Type	Description
name	string	Optional SNMPv1/SNMPv2c or SNMPv3 user name. For an SNMPv3 traphost, this object refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this object refers to an SNMP community. For an SNMPv3 traphost, this object is mandatory and refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, ONTAP automatically uses "public", if the same is configured, or any other configured community as user. So, for an SNMPv1 or SNMPv2c traphost, this property should not be provided in the "POST" method. However, the configured community for the SNMPv1/SNMPv2c traphost is returned by the "GET" method. • example: snmpv3user3 • Introduced in: 9.7 • x-nullable: true

snmp_traphost

SNMP manager or host machine that receives SNMP traps from ONTAP.

Name	Type	Description
host	string	Fully qualified domain name (FQDN), IPv4 address or IPv6 address of SNMP traphost.
user	user	Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

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.

Manage individual SNMP traphosts

Support SNMP traphosts host endpoint overview

Overview

Defines, retrieves or deletes an individual SNMP traphost.

Examples

Retrieves an individual traphost in the cluster

```
# The API:
GET "/api/support/snmp/traphosts/{host}"

# The call
curl -H "accept: application/hal+json" -X GET "https://<mgmt-
ip>/api/support/snmp/traphosts/10.235.36.62"

# The response
{
"host": "scspr0651011001.gdl.englab.netapp.com",
"ip_address": "10.235.36.62",
"user": {
  "name": "public",
  "_links": {
    "self": {
      "href":
"/api/support/snmp/users/800003150558b57e8dbd9ce9119d82005056a7b4e5/public
"
    }
  }
},
"_links": {
  "self": {
    "href": "/api/support/snmp/traphosts/10.235.36.62"
  }
}
}
```

Deletes an individual traphost in the cluster

```
# The API:
DELETE "/api/support/snmp/traphosts/{host}"

# The call:
curl -H "accept: application/json" -H "Content-Type: application/json" -X
DELETE "https://<mgmt-
ip>/api/support/snmp/traphosts/3ffe:ffff:100:f102::1"

# The response:
200 OK
{}
```

Delete an SNMP traphost

DELETE `/support/snmp/traphosts/{host}`

Introduced In: 9.7

Deletes an SNMP traphost.

Learn more

- DOC /support/snmp/traphosts/{host}

Parameters

Name	Type	In	Required	Description
host	string	path	True	Fully Qualified Domain Name (FQDN), IPv4 address or IPv6 address of SNMP traphost.

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
9043970	Traphost entry does not exist.

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 SNMP traphost details

GET `/support/snmp/traphosts/{host}`

Introduced In: 9.7

Retrieves the details of an SNMP traphost along with the SNMP user configured for that traphost.

Learn more

- DOC /support/snmp/traphosts/{host}

Parameters

Name	Type	In	Required	Description
host	string	path	True	Fully Qualified Domain Name (FQDN), IPv4 address or IPv6 address of SNMP traphost.
fields	array[string]	query	False	Specify the fields to return.
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
host	string	Fully qualified domain name (FQDN), IPv4 address or IPv6 address of SNMP traphost.
ip_address	string	IPv4 or IPv6 address
user	user	Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "host": "traphost.example.com",
  "ip_address": "10.10.10.7",
  "user": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "snmpv3user3"
  }
}
```


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	

user

Optional SNMP user parameter. For an SNMPv3 traphost, this property refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this property refers to an SNMP community.

Name	Type	Description
_links	_links	
name	string	Optional SNMPv1/SNMPv2c or SNMPv3 user name. For an SNMPv3 traphost, this object refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, this object refers to an SNMP community. For an SNMPv3 traphost, this object is mandatory and refers to an SNMPv3 or User-based Security Model (USM) user. For an SNMPv1 or SNMPv2c traphost, ONTAP automatically uses "public", if the same is configured, or any other configured community as user. So, for an SNMPv1 or SNMPv2c traphost, this property should not be provided in the "POST" method. However, the configured community for the SNMPv1/SNMPv2c traphost is returned by the "GET" method. • example: snmpv3user3 • Introduced in: 9.7 • x-nullable: true

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 and create SNMP users

Support SNMP users endpoint overview

Overview

Defines, retrieves and adds new SNMP users. An SNMP user can be an SNMPv1/SNMPv2c user or an SNMPv3 user. SNMPv1/SNMPv2c user is also called a "community" user. Use a "community" user to query ONTAP SNMP server over SNMPv1/SNMPv2c protocol. An SNMPv3 user, also called a User-based Security Model (USM) user, can be a local SNMPv3 user or a remote SNMPv3 user. Use a local SNMPv3 user to query ONTAP SNMP server over SNMPv3 and/or to send SNMPv3 traps. A remote SNMPv3 user is configured in ONTAP as well as on a remote switch. ONTAP SNMP client uses a remote SNMPv3 user to query the switch over SNMPv3.

Examples

Retrieves a list of SNMP users in the cluster, sorted by SVM UUID

```
# The API:
GET "/api/support/snmp/users"

# The call:
curl -H "accept: application/hal+json" -X GET "https://<mgmt-
ip>/api/support/snmp/users?order_by=owner.uuid"

# The response:
```

```
{
"records": [
  {
    "engine_id": "80000315052d7d2c4410b8e911bc9f005056bb942e",
    "name": "snmpv1user1",
    "owner": {
      "uuid": "442c7d2d-b810-11e9-bc9f-005056bb942e"
    },
    "_links": {
      "self": {
        "href":
"/api/support/snmp/users/80000315052d7d2c4410b8e911bc9f005056bb942e/snmpv1
user1"
      }
    }
  },
  {
    "engine_id": "80000315058e02057c0fb8e911bc9f005056bb942e",
    "name": "snmpv3user1",
    "owner": {
      "uuid": "7c05028e-b80f-11e9-bc9f-005056bb942e"
    },
    "_links": {
      "self": {
        "href":
"/api/support/snmp/users/80000315058e02057c0fb8e911bc9f005056bb942e/snmpv3
user1"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/support/snmp/users?order_by=owner.uuid"
  }
}
}
```


Creates an SNMPv1 or SNMPv2c community user

```
# The API:
POST "/api/support/snmp/users"

# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
POST "https://<mgmt-ip>/api/support/snmp/users" -d
'{"owner":{"uuid":"02c9e252-41be-11e9-81d5-00a0986138f7",
"name":"cluster1"}, "name":"public", "authentication_method":"community"}'

# The response:
201 Created
{}
```

Creates a local SNMPv3 user

```
# The API:
POST "/api/support/snmp/users"

# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
POST "https://<mgmt-ip>/api/support/snmp/users" -d
'{"owner":{"uuid":"02c9e252-41be-11e9-81d5-00a0986138f7",
"name":"cluster1"}, "name":"snmpv3u1", "authentication_method":"usm",
"snmpv3":{"authentication_protocol":"sha",
"authentication_password":"jelly22fi$h", "privacy_protocol":"aes",
"privacy_password":"a11Black$"}}'

# The response:
201 Created
{}
```

Creates a remote SNMPv3 user

```
# The API:
POST "/api/support/snmp/users"

# The call
curl -H "accept: application/json" -H "Content-Type: application/json" -X
POST "https://<mgmt-ip>/api/support/snmp/users" -d
'{"owner":{"uuid":"02c9e252-41be-11e9-81d5-00a0986138f7",
"name":"cluster1"},
"engine_id":"8000031505b67667a26975e9118a480050568e6f74",
"name":"switchuser1", "authentication_method":"usm",
"switch_address":"fdf8:f53b:82e4::53",
"snmpv3":{"authentication_protocol":"md5",
"authentication_password":"TfhIeliw601lS.Rw$3pm"}}'

# The response:
201 Created
{}
```

Retrieve SNMP users on a cluster

GET `/support/snmp/users`

Introduced In: 9.7

Retrieves the list of SNMP users on the cluster.

Related ONTAP commands

- `security snmpusers`
- `security login show -application snmp`

Learn more

- DOC /support/snmp/users

Parameters

Name	Type	In	Required	Description
owner.uuid	string	query	False	Filter by owner.uuid
owner.name	string	query	False	Filter by owner.name

Name	Type	In	Required	Description
comment	string	query	False	Filter by comment • maxLength: 128 • minLength: 0
snmpv3.privacy_protocol	string	query	False	Filter by snmpv3.privacy_protocol
snmpv3.authentication_protocol	string	query	False	Filter by snmpv3.authentication_protocol
name	string	query	False	Filter by name • maxLength: 32
switch_address	string	query	False	Filter by switch_address
scope	string	query	False	Filter by scope
authentication_method	string	query	False	Filter by authentication_method
engine_id	string	query	False	Filter by engine_id
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records.
records	array[snmp_user]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "authentication_method": "usm",
      "comment": "This is a comment.",
      "engine_id": "80000315055415ab26d4aae811ac4d005056bb792e",
      "name": "snmpv3user2",
      "owner": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "scope": "svm",
      "snmpv3": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "authentication_protocol": "sha2_256",
        "privacy_protocol": "aes128"
      },
      "switch_address": "10.23.34.45"
    }
  ]
}
```

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	

owner

Optional name and UUID of owning Storage Virtual Machine (SVM).

Name	Type	Description
_links	_links	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

snmpv3

Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
_links	_links	
authentication_protocol	string	Authentication protocol.
privacy_protocol	string	Privacy protocol.

snmp_user

An SNMP user can be an SNMPv1/SNMPv2c user or an SNMPv3 user. SNMPv1/SNMPv2c user is also called a "community" user. An SNMPv3 user, also called a User-based Security Model (USM) user, can be a local SNMPv3 user or a remote SNMPv3 user. A local SNMPv3 user can be used for querying ONTAP SNMP server over SNMPv3 and/or for sending SNMPv3 traps. The local SNMPv3 user used for

sending SNMPv3 traps must be configured with the same authentication and privacy credentials on the traphost receiver as well. A remote SNMPv3 user is also configured on a remote switch and used by ONTAP SNMP client functionality to query the remote switch over SNMPv3. An SNMP user is scoped to its owning Storage Virtual Machine (SVM). Owning SVM could be a data SVM or the administrative SVM.

Name	Type	Description
_links	_links	
authentication_method	string	Optional authentication method.
comment	string	Optional comment text.
engine_id	string	Optional SNMPv3 engine identifier. For a local SNMP user belonging to the administrative Storage Virtual Machine (SVM), the default value of this parameter is the SNMPv3 engine identifier for the administrative SVM. For a local SNMP user belonging to a data SVM, the default value of this parameter is the SNMPv3 engine identifier for that data SVM. For an SNMPv1/SNMPv2c community, this parameter should not be specified in "POST" method. For a remote switch SNMPv3 user, this parameter specifies the SNMPv3 engine identifier for the remote switch. This parameter can also optionally specify a custom engine identifier.
name	string	SNMP user name.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).
scope	string	Set to "svm" for data Storage Virtual Machine (SVM) SNMP users and to "cluster" for administrative SVM SNMP users.

Name	Type	Description
snmpv3	snmpv3	Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.
switch_address	string	Optional remote switch address. It can be an IPv4 address or an IPv6 address. A remote switch can be queried over SNMPv3 using ONTAP SNMP client functionality. Querying such a switch requires an SNMPv3 user (remote switch user) to be configured on the switch. Since ONTAP requires remote switch user's SNMPv3 credentials (to query it), this user must be configured in ONTAP as well. This parameter is specified when configuring such a user. • example: 10.23.34.45 • Introduced in: 9.7 • readCreate: 1 • x-nullable: true

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.

Create a cluster-scoped or an SVM-scoped SNMP user

POST `/support/snmp/users`

Introduced In: 9.7

Creates either a cluster-scoped or an SVM-scoped SNMP user. This user can be an SNMPv1 or SNMPv2c community user or an SNMPv3 user. An SNMPv3 user can be a local SNMPv3 user or a remote SNMPv3 user.

Required properties

- `owner` - Name and UUID of owning SVM.
- `engine_id` - Engine ID of owning SVM or remote switch.
- `name` - SNMP user name
- `authentication_method` - Authentication method

Optional properties

- `switch_address` - Optional remote switch address
- `snmpv3` - SNMPv3-specific credentials
- `comment` - Comment text

Default property values

- `snmpv3.authentication_protocol` - none
- `snmpv3.privacy_protocol` - none

Related ONTAP commands

- `security login create`
- `system snmp community add`

Learn more

- DOC /support/snmp/users

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
authentication_method	string	Optional authentication method.
comment	string	Optional comment text.

Name	Type	Description
engine_id	string	Optional SNMPv3 engine identifier. For a local SNMP user belonging to the administrative Storage Virtual Machine (SVM), the default value of this parameter is the SNMPv3 engine identifier for the administrative SVM. For a local SNMP user belonging to a data SVM, the default value of this parameter is the SNMPv3 engine identifier for that data SVM. For an SNMPv1/SNMPv2c community, this parameter should not be specified in "POST" method. For a remote switch SNMPv3 user, this parameter specifies the SNMPv3 engine identifier for the remote switch. This parameter can also optionally specify a custom engine identifier.
name	string	SNMP user name.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).
snmpv3	snmpv3	Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
switch_address	string	Optional remote switch address. It can be an IPv4 address or an IPv6 address. A remote switch can be queried over SNMPv3 using ONTAP SNMP client functionality. Querying such a switch requires an SNMPv3 user (remote switch user) to be configured on the switch. Since ONTAP requires remote switch user's SNMPv3 credentials (to query it), this user must be configured in ONTAP as well. This parameter is specified when configuring such a user. • example: 10.23.34.45 • Introduced in: 9.7 • readCreate: 1 • x-nullable: true

Example request

```
{
  "authentication_method": "usm",
  "comment": "This is a comment.",
  "engine_id": "80000315055415ab26d4aae811ac4d005056bb792e",
  "name": "snmpv3user2",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "snmpv3": {
    "authentication_password": "humTdumt*@t0nAwa11",
    "authentication_protocol": "sha2_256",
    "privacy_password": "p@**GOandCLCt*200",
    "privacy_protocol": "aes128"
  },
  "switch_address": "10.23.34.45"
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
authentication_method	string	Optional authentication method.
comment	string	Optional comment text.
engine_id	string	Optional SNMPv3 engine identifier. For a local SNMP user belonging to the administrative Storage Virtual Machine (SVM), the default value of this parameter is the SNMPv3 engine identifier for the administrative SVM. For a local SNMP user belonging to a data SVM, the default value of this parameter is the SNMPv3 engine identifier for that data SVM. For an SNMPv1/SNMPv2c community, this parameter should not be specified in "POST" method. For a remote switch SNMPv3 user, this parameter specifies the SNMPv3 engine identifier for the remote switch. This parameter can also optionally specify a custom engine identifier.
name	string	SNMP user name.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).
snmpv3	snmpv3	Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
switch_address	string	Optional remote switch address. It can be an IPv4 address or an IPv6 address. A remote switch can be queried over SNMPv3 using ONTAP SNMP client functionality. Querying such a switch requires an SNMPv3 user (remote switch user) to be configured on the switch. Since ONTAP requires remote switch user's SNMPv3 credentials (to query it), this user must be configured in ONTAP as well. This parameter is specified when configuring such a user. • example: 10.23.34.45 • Introduced in: 9.7 • readCreate: 1 • x-nullable: true

Example response


```
{
  "authentication_method": "usm",
  "comment": "This is a comment.",
  "engine_id": "80000315055415ab26d4aae811ac4d005056bb792e",
  "name": "snmpv3user2",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "snmpv3": {
    "authentication_password": "humTdumt*@t0nAwa11",
    "authentication_protocol": "sha2_256",
    "privacy_password": "p@**GOandCLCt*200",
    "privacy_protocol": "aes128"
  },
  "switch_address": "10.23.34.45"
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2621475	This operation is not allowed on a node SVM.
2621601	This operation is not permitted on a system SVM.
5636101	One role for all applications and authentication methods is recommended for a user account.
5636106	Engine ID starting with first bit set as 1 in first octet should have a minimum of 5 or maximum of 32 octets.
5636107	Engine ID specified is based on an IP address, and must therefore be 9 octets in length.
5636108	Engine ID specified is based on an IPv6 address, and must therefore be 21 octets in length.
5636109	Engine ID specified is based on a MAC address, and must therefore be 11 octets in length.
5636110	Engine ID starting with first bit set as 0 in the first octet needs to be 12 octets in length.
5636111	Engine ID cannot have all zeroes.
5636112	Invalid Engine ID specified.
5636113	Cannot enable SNMP user capability for data SVM.
5636116	Cannot read SNMP user capability for data SVM.
5636121	User account name is reserved for use by the system.
5636123	Cannot create an SNMP user with a role other than readonly, none, or admin.
5636124	Cannot create an SNMP user with a role other than vsadmin-readonly, none, or vsadmin.
5636126	Cannot create a user with the user name, group name, or role "autosupport" because it is reserved by the system.
5636148	Failed to discover SNMPv3 engine ID of remote SNMP agent.

Error Code	Description
5636150	The switch_address parameter can be specified only for administrative SVMs.
5636152	0.0.0.0 cannot be specified as the IP Address for the switch_address parameter.
5636153	Engine ID is already associated with user.
5832711	The only application permitted for user "diag" is "console."
7077897	Invalid character in username. Valid characters":" A-Z, a-z, 0-9, ".", "_", and "-". Note that the user name cannot start with "-".
7077898	The username must contain both letters and numbers.
7077899	Username does not meet length requirements.
7077906	Cannot use given role with this SVM because a role with that name has not been defined for the SVM.
9043995	Failed to create SNMP community. Reason":" SNMPv1 and SNMPv2c are not supported when cluster FIPS mode is enabled.
9043999	ONTAP failed to create an SNMPv3 user because SNMPv3 is disabled in the cluster.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

Optional name and UUID of owning Storage Virtual Machine (SVM).

Name	Type	Description
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

snmpv3

Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
authentication_password	string	Authentication protocol password.
authentication_protocol	string	Authentication protocol.
privacy_password	string	Privacy protocol password.
privacy_protocol	string	Privacy protocol.

snmp_user

An SNMP user can be an SNMPv1/SNMPv2c user or an SNMPv3 user. SNMPv1/SNMPv2c user is also called a "community" user. An SNMPv3 user, also called a User-based Security Model (USM) user, can be a local SNMPv3 user or a remote SNMPv3 user. A local SNMPv3 user can be used for querying ONTAP SNMP server over SNMPv3 and/or for sending SNMPv3 traps. The local SNMPv3 user used for sending SNMPv3 traps must be configured with the same authentication and privacy credentials on the traphost receiver as well. A remote SNMPv3 user is also configured on a remote switch and used by ONTAP SNMP client functionality to query the remote switch over SNMPv3. An SNMP user is scoped to its owning Storage Virtual Machine (SVM). Owning SVM could be a data SVM or the administrative SVM.

Name	Type	Description
authentication_method	string	Optional authentication method.

Name	Type	Description
comment	string	Optional comment text.
engine_id	string	Optional SNMPv3 engine identifier. For a local SNMP user belonging to the administrative Storage Virtual Machine (SVM), the default value of this parameter is the SNMPv3 engine identifier for the administrative SVM. For a local SNMP user belonging to a data SVM, the default value of this parameter is the SNMPv3 engine identifier for that data SVM. For an SNMPv1/SNMPv2c community, this parameter should not be specified in "POST" method. For a remote switch SNMPv3 user, this parameter specifies the SNMPv3 engine identifier for the remote switch. This parameter can also optionally specify a custom engine identifier.
name	string	SNMP user name.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).
snmpv3	snmpv3	Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
switch_address	string	Optional remote switch address. It can be an IPv4 address or an IPv6 address. A remote switch can be queried over SNMPv3 using ONTAP SNMP client functionality. Querying such a switch requires an SNMPv3 user (remote switch user) to be configured on the switch. Since ONTAP requires remote switch user's SNMPv3 credentials (to query it), this user must be configured in ONTAP as well. This parameter is specified when configuring such a user. • example: 10.23.34.45 • Introduced in: 9.7 • readCreate: 1 • x-nullable: true

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.

Manage individual SNMP users

Support SNMP users engine_id name endpoint overview

Overview

Defines, retrieves, updates and deletes an individual SNMP user.

Examples

Retrieves the details of an SNMP user

```
# The API:
GET "/api/support/snmp/users/{engine_id}/{name}"

# The call:
curl -H "accept: application/hal+json" -X GET "https://<mgmt-
ip>/api/support/snmp/users/80000315056622e52625a9e911a981005056bb1dcb/snmp
v1user2"

# The response:
{
"engine_id": "80000315056622e52625a9e911a981005056bb1dcb",
"name": "snmpv1user2",
"scope": "cluster",
"owner": {
  "name": "cluster-1",
  "uuid": "26e52266-a925-11e9-a981-005056bb1dcb"
},
"authentication_method": "community",
"_links": {
  "self": {
    "href":
"/api/support/snmp/users/80000315056622e52625a9e911a981005056bb1dcb/snmpv1
user2"
  }
}
}
```

Updates the comment parameter for an individual SNMP user

```
# The API:
PATCH "/api/support/snmp/users/{engine_id}/{name}"

# The call:
curl -H "accept: application/json" -H "Content-Type: application/json" -X
PATCH "https://<mgmt-
ip>/api/support/snmp/users/8000031505b67667a26975e9118a480050568e6f74/publ
ic" -d '{"comment":"Default SNMP community"}'

# The response:
200 OK
{}
```

Deletes an individual SNMP user in the cluster

```
# The API:
DELETE "/api/support/snmp/users/{engine_id}/{name}"

# The call:
curl -H "accept: application/json" -H "Content-Type: application/json" -X
DELETE "https://<mgmt-
ip>/api/support/snmp/users/8000031505b67667a26975e9118a480050568e6f74/snmp
user"

# The response:
200 OK
{}
```

Delete an SNMP user

DELETE `/support/snmp/users/{engine_id}/{name}`

Introduced In: 9.7

Deletes an SNMP user. The engine ID can be the engine ID of the administrative SVM or a data SVM. It can also be the SNMPv3 engine ID of a remote switch.

Related ONTAP commands

- `security login delete`
- `system snmp community delete`

Learn more

- DOC /support/snmp/users/{engine_id}/{name}

Parameters

Name	Type	In	Required	Description
engine_id	string	path	True	Engine ID of owning SVM or remote switch.
name	string	path	True	SNMP user name.
fields	array[string]	query	False	Specify the fields to return.
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2621475	This operation is not allowed on a node SVM.
2621699	This operation is not allowed on a system SVM.
5636123	Cannot create an SNMP user with a role other than readonly, none, or admin.
5636124	Cannot create an SNMP user with a role other than vsadmin-readonly, none, or vsadmin.
5832712	Cannot modify attributes for user "diag."
7077906	Cannot use given role with this SVM because a role with that name has not been defined for the SVM.
9043999	ONTAP failed to create an SNMPv3 user because SNMPv3 is disabled in the cluster.

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 SNMP user details

GET `/support/snmp/users/{engine_id}/{name}`

Introduced In: 9.7

Retrieves the details of an SNMP user. The engine ID can be the engine ID of the administrative SVM or a data SVM. It can also be the SNMPv3 engine ID of a remote switch.

Related ONTAP commands

- `security snmpusers -vserver <SVM Name> -username <User Name>`
- `security login show -application snmp -vserver <SVM Name> -user-or-group-name <User Name>`

Learn more

- DOC /support/snmp/users/{engine_id}/{name}

Parameters

Name	Type	In	Required	Description
engine_id	string	path	True	Engine ID of owning SVM or remote switch.
name	string	path	True	SNMP user name.
fields	array[string]	query	False	Specify the fields to return.
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
authentication_method	string	Optional authentication method.
comment	string	Optional comment text.

Name	Type	Description
engine_id	string	Optional SNMPv3 engine identifier. For a local SNMP user belonging to the administrative Storage Virtual Machine (SVM), the default value of this parameter is the SNMPv3 engine identifier for the administrative SVM. For a local SNMP user belonging to a data SVM, the default value of this parameter is the SNMPv3 engine identifier for that data SVM. For an SNMPv1/SNMPv2c community, this parameter should not be specified in "POST" method. For a remote switch SNMPv3 user, this parameter specifies the SNMPv3 engine identifier for the remote switch. This parameter can also optionally specify a custom engine identifier.
name	string	SNMP user name.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).
scope	string	Set to "svm" for data Storage Virtual Machine (SVM) SNMP users and to "cluster" for administrative SVM SNMP users.
snmpv3	snmpv3	Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
switch_address	string	Optional remote switch address. It can be an IPv4 address or an IPv6 address. A remote switch can be queried over SNMPv3 using ONTAP SNMP client functionality. Querying such a switch requires an SNMPv3 user (remote switch user) to be configured on the switch. Since ONTAP requires remote switch user's SNMPv3 credentials (to query it), this user must be configured in ONTAP as well. This parameter is specified when configuring such a user. • example: 10.23.34.45 • Introduced in: 9.7 • readCreate: 1 • x-nullable: true

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "authentication_method": "usm",
  "comment": "This is a comment.",
  "engine_id": "80000315055415ab26d4aae811ac4d005056bb792e",
  "name": "snmpv3user2",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "svm",
  "snmpv3": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "authentication_protocol": "sha2_256",
    "privacy_protocol": "aes128"
  },
  "switch_address": "10.23.34.45"
}
```


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	

owner

Optional name and UUID of owning Storage Virtual Machine (SVM).

Name	Type	Description
_links	_links	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

snmpv3

Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
_links	_links	
authentication_protocol	string	Authentication protocol.
privacy_protocol	string	Privacy protocol.

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 comment parameter of an SNMP user

PATCH `/support/snmp/users/{engine_id}/{name}`

Introduced In: 9.7

Updates the comment parameter of an SNMP user.

Optional properties

- `comment` - Comment text.

Related ONTAP commands

- `security login modify`

Learn more

- DOC /support/snmp/users/{engine_id}/{name}

Parameters

Name	Type	In	Required	Description
engine_id	string	path	True	Engine ID of owning SVM or remote switch.
name	string	path	True	SNMP user name.

Name	Type	In	Required	Description
return_timeout	integer	query	False	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. • Default value: 1 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
comment	string	Optional comment text.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).

Example request

```
{
  "comment": "This is a comment.",
  "owner": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
2621475	This operation is not allowed on a node SVM.
2621699	This operation is not allowed on a system SVM.
5636123	Cannot create an SNMP user with a role other than readonly, none, or admin.
5636124	Cannot create an SNMP user with a role other than vsadmin-readonly, none, or vsadmin.
5832712	Cannot modify attributes for user "diag."
7077906	Cannot use given role with this SVM because a role with that name has not been defined for the SVM.
9043999	ONTAP failed to create an SNMPv3 user because SNMPv3 is disabled in the cluster.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

owner

Optional name and UUID of owning Storage Virtual Machine (SVM).

Name	Type	Description
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

snmpv3

Optional parameter that can be specified only for an SNMPv3 user i.e. when 'authentication_method' is either 'usm' or 'both'. This parameter defines the SNMPv3 credentials for an SNMPv3 user.

Name	Type	Description
authentication_protocol	string	Authentication protocol.
privacy_protocol	string	Privacy protocol.

snmp_user

An SNMP user can be an SNMPv1/SNMPv2c user or an SNMPv3 user. SNMPv1/SNMPv2c user is also called a "community" user. An SNMPv3 user, also called a User-based Security Model (USM) user, can be a local SNMPv3 user or a remote SNMPv3 user. A local SNMPv3 user can be used for querying ONTAP SNMP server over SNMPv3 and/or for sending SNMPv3 traps. The local SNMPv3 user used for sending SNMPv3 traps must be configured with the same authentication and privacy credentials on the traphost receiver as well. A remote SNMPv3 user is also configured on a remote switch and used by ONTAP SNMP client functionality to query the remote switch over SNMPv3. An SNMP user is scoped to its owning Storage Virtual Machine (SVM). Owning SVM could be a data SVM or the administrative SVM.

Name	Type	Description
comment	string	Optional comment text.
owner	owner	Optional name and UUID of owning Storage Virtual Machine (SVM).

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 © 2025 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.