



Manage an event destination instance

ONTAP 9.12.1 REST API reference

NetApp

February 13, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9121/ontap/support_ems_destinations_name_endpoint_overview.html on February 13, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Manage an event destination instance 1
 - Support EMS destinations name endpoint overview 1
 - Delete an event destination 4
 - Retrieve an event destination 6
 - Update an event destination 14

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 |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| Name | Type | Description |
|----------------|----------------------------------|---|
| _links | _links | |
| 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 <code>ca</code> and <code>serial_number</code> fields must be specified when configuring a certificate in a PATCH or POST request. The <code>name</code> field is read-only and cannot be used to configure a client-side certificate. <ul style="list-style-type: none"> 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"
    }
  },
  "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-aelc-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": "no_override",
    "message": "legacy_netapp",
    "timestamp_override": "no_override"
  },
  "port": 514,
  "transport": "udp_unencrypted"
},
"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 | |

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. |

| Name | Type | Description |
|--------------------|--------|--|
| 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. |
| 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 |
|---------------------|------------------------|-------------|
| <code>_links</code> | _links | |

| 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 <code>ca</code> and <code>serial_number</code> fields must be specified when configuring a certificate in a PATCH or POST request. The <code>name</code> field is read-only and cannot be used to configure a client-side certificate. <ul style="list-style-type: none"> 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

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "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-aelc-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": "no_override",
    "message": "legacy_netapp",
    "timestamp_override": "no_override"
  },
  "port": 514,
  "transport": "udp_unencrypted"
},
"system_defined": 1,
"type": "email"
}

```

Response

Status: 200, Ok

| Name | Type | Description |
|--------------|----------------------------------|---|
| _links | _links | |
| 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 <code>ca</code> and <code>serial_number</code> fields must be specified when configuring a certificate in a PATCH or POST request. The <code>name</code> field is read-only and cannot be used to configure a client-side certificate. <ul style="list-style-type: none"> Introduced in: 9.6 |
| connectivity | connectivity | |
| destination | string | Event destination |
| filters | array[filters] | |
| name | string | Destination name. Valid in POST. |

| Name | Type | Description |
|----------------|------------------------|--|
| 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"
    }
  },
  "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-aelc-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": "no_override",
    "message": "legacy_netapp",
    "timestamp_override": "no_override"
  },
  "port": 514,
  "transport": "udp_unencrypted"
},
"system_defined": 1,
"type": "email"
}

```

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 |
| 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 |

| Error Code | Description |
|------------|---|
| 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 |

| 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 | |

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. |

| Name | Type | Description |
|--------------------|--------|--|
| 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. |
| transport | string | Syslog Transport Protocol. |

ems_destination

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| 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 <code>ca</code> and <code>serial_number</code> fields must be specified when configuring a certificate in a PATCH or POST request. The <code>name</code> field is read-only and cannot be used to configure a client-side certificate. <ul style="list-style-type: none"> 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. |

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.