Manage protocols S3 services

REST API reference

NetApp
February 06, 2026

Table of Contents

Manage protocols S3 services

Manage protocols S3 services

Overview

An S3 server is an object store server that is compatible with the Amazon S3 protocol. In the initial version, only a subset of the protocol features necessary to support Fabric Pool capacity tier usecases are implemented. S3 server allows you to store objects in ONTAP using Amazon S3 protocol. This feature can be used as a target object store server for ONTAP FabricPools.

Performance monitoring

Performance of the SVM can be monitored by the `metric.*` and `statistics.*` properties. These show the performance of the SVM in terms of IOPS, latency and throughput. The `metric.*` properties denote an average whereas `statistics.*` properties denote a real-time monotonically increasing value aggregated across all nodes.

Examples

Retrieving all of the S3 configurations

```
# The API:
/api/protocols/s3/services

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/services?fields=*&return_records=true&return_timeout=
15" -H "accept: application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "cf90b8f2-8071-11e9-8190-0050568eae21",
      "name": "vs2"
    },
    "name": "vs1",
    "comment": "S3 server",
    "enabled": false,
    "max_lock_retention_period": "none",
    "min_lock_retention_period": "none"
  },
  {
    "svm": {
      "uuid": "d7f1219c-7f8e-11e9-9124-0050568eae21",
      "name": "vs1"
    },
    "name": "Server-1",
    "comment": "S3 server",
    "enabled": true,
    "max_lock_retention_period": "none",
    "min_lock_retention_period": "none",
    "buckets": [
      {
        "uuid": "e08665af-8114-11e9-8190-0050568eae21",
        "name": "bucket-1",
        "volume": {
          "name": "fg_oss_1559026220",
          "uuid": "de146bff-8114-11e9-8190-0050568eae21"
        },
        "size": 107374182400,
        "logical_used_size": 157286400,
        "encryption": {
          "enabled": false
        },
        "comment": "s3 bucket"
      },
      {
        "uuid": "fb1912ef-8114-11e9-8190-0050568eae21",
        "name": "bucket-2",
        "volume": {
          "name": "fg_oss_1559026269",
          "uuid": "f9b1cdd0-8114-11e9-8190-0050568eae21"
        },
        "size": 107374182400,
        "logical_used_size": 78643200,
        "encryption": {
          "enabled": false
        },
        "comment": "s3 bucket"
      }
    ],
    "users": [
      {
        "name": "user-1",
        "comment": "S3 user",
        "access_key": "<AWS-ACCESS-KEY-ID>"
      },
      {
        "name": "user-2",
        "comment": "",
          "access_key": "<AWS-ACCESS-KEY-ID>"
        }
      ]
    }
  ],
  "num_records": 2
  }
```

Retrieving all S3 configurations for a particular SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/24c2567a-f269-
11e8-8852-0050568e5298?fields=*" -H "accept: application/json"

# The response:
{
"svm": {
  "uuid": "d7f1219c-7f8e-11e9-9124-0050568eae21",
  "name": "vs1"
},
"name": "Server-1",
"comment": "S3 server",
"enabled": true,
"max_lock_retention_period": "none",
"min_lock_retention_period": "none",
"buckets": [
  {
    "uuid": "e08665af-8114-11e9-8190-0050568eae21",
    "name": "bucket-1",
    "volume": {
      "name": "fg_oss_1559026220",
      "uuid": "de146bff-8114-11e9-8190-0050568eae21"
    },
    "size": 107374182400,
    "logical_used_size": 157286400,
    "encryption": {
      "enabled": false
    },
    "comment": "s3 bucket",
    "policy": {
      "statements": [
        {
          "effect": "deny",
          "actions": [
            "*Object"
          ],
          "principals": [
            "mike"
          ],
          "resources": [
            "bucket-1/policy-docs/*",
            "bucket-1/confidential-*"
          ],
          "sid": "DenyAccessToGetPutDeleteObjectForMike"
        },
        {
          "effect": "allow",
          "actions": [
            "GetObject"
          ],
          "principals": [
            "*"
          ],
          "resources": [
            "bucket-1/readme"
          ],
          "sid": "AccessToGetObjectForAnonymousUser"
        }
      ]
    },
    "cors": {
      "rules": [
        {
          "id": "string",
          "allowed_origins": [
            "http://www.example.com"
          ],
          "allowed_methods": [
            "PUT",
            "DELETE"
          ],
          "allowed_headers": [
            "x-amz-request-id"
          ],
          "expose_headers": [
            "http://www.example.com"
          ],
          "max_age_seconds": 1024
        }
      ]
    }
  },
  {
    "uuid": "fb1912ef-8114-11e9-8190-0050568eae21",
    "name": "bucket-2",
    "volume": {
      "name": "fg_oss_1559026269",
      "uuid": "f9b1cdd0-8114-11e9-8190-0050568eae21"
    },
    "size": 107374182400,
    "logical_used_size": 1075838976,
    "encryption": {
      "enabled": false
    },
    "comment": "s3 bucket"
  }
],
"users": [
  {
    "name": "user-1",
    "comment": "s3 user",
    "access_key": "<AWS-ACCESS-KEY-ID>"
  },
  {
    "name": "user-2",
    "comment": "",
    "access_key": "<AWS-ACCESS-KEY-ID>"
  }
]
}
```

Creating an S3 server, users, and buckets configurations with required fields specified

```
# The API:
/api/protocols/s3/services

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"buckets\": [ { \"name\": \"bucket-1\" }, { \"name\": \"bucket-2\" } ],
\"enabled\": true, \"name\": \"Server-1\", \"svm\": { \"uuid\":
\"d49ef663-7f8e-11e9-9b2c-0050568e4594\" }, \"users\": [ { \"name\":
\"user-1\" }, { \"name\": \"user-2\" } ]}"
```

```
# The response:
HTTP/1.1 201 Created
Date: Fri, 31 May 2019 08:44:16 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/
Content-Length: 623
Content-Type: application/hal+json
{
"num_records": 1,
"records": [
  {
    "users": [
      {
        "name": "user-1",
        "access_key": "<AWS-ACCESS-KEY-ID>",
        "secret_key": "<AWS-SECRET-ACCESS-KEY>"
      },
      {
        "name": "user-2",
        "access_key": "<AWS-ACCESS-KEY-ID>",
        "secret_key": "<AWS-SECRET-ACCESS-KEY>"
      }
    ],
    "job": {
      "uuid": "f51675dd-820a-11e9-a762-0050568e4594",
      "_links": {
        "self": {
          "href": "/api/cluster/jobs/f51675dd-820a-11e9-a762-0050568e4594"
        }
      }
    },
    "_links": {
      "self": {
        "href": "/api/protocols/s3/services/"
      }
    }
  }
]
}
```

Creating an S3 server, users, and buckets configurations

```
# The API:
/api/protocols/s3/services

# The call:

curl -X POST "https://<mgmt-ip>/api/protocols/s3/services" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"buckets\": [ { \"aggregates\": [ { \"name\": \"aggr1\", \"uuid\":
\"1cd8a442-86d1-11e0-ae1c-123478563412\" } ],
\"constituents_per_aggregate\": 4, \"name\": \"bucket-1\", \"size\":
\"107374182400\",  \"policy\": { \"statements\": [ { \"actions\": [ \"*\"
], \"conditions\": [ { \"operator\": \"ip_address\", \"source_ips\": [
\"1.1.1.1/23\", \"1.2.2.2/20\" ] } ], \"effect\": \"allow\",
\"resources\": [ \"bucket-1\", \"bucket-1*\" ], \"sid\":
\"fullAccessForAllPrincipalsToBucket\"} ] } }, { \"aggregates\": [ {
\"name\": \"aggr1\", \"uuid\": \"1cd8a442-86d1-11e0-ae1c-123478563412\" },
{ \"name\": \"aggr2\", \"uuid\": \"982fc4d0-d1a2-4da4-9c47-5b433f24757d\"}
], \"constituents_per_aggregate\": 4, \"name\": \"bucket-2\" } ],
\"enabled\": true, \"name\": \"Server-1\", \"max_lock_retention_period\":
\"P41Y\", \"max_lock_retention_period\": \"P1Y\", \"svm\": { \"name\":
\"vs1\", \"uuid\": \"d49ef663-7f8e-11e9-9b2c-0050568e4594\" }, \"users\":
[ { \"name\": \"user-1\" }, { \"name\": \"user-2\" } ]}"



# The response:
HTTP/1.1 201 Created
Date: Fri, 31 May 2019 08:44:16 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/
Content-Length: 623
Content-Type: application/hal+json
{
"num_records": 1,
"records": [
  {
    "users": [
      {
        "name": "user-1",
        "access_key": "<AWS-ACCESS-KEY-ID>",
        "secret_key": "<AWS-SECRET-ACCESS-KEY>"
      },
      {
        "name": "user-2",
    "access_key": "<AWS-ACCESS-KEY-ID>",
    "secret_key": "<AWS-SECRET-ACCESS-KEY>"
   }
  ],
  "job": {
   "uuid": "f51675dd-820a-11e9-a762-0050568e4594",
   "_links": {
    "self": {
     "href": "/api/cluster/jobs/f51675dd-820a-11e9-a762-0050568e4594"
    }
   }
  },
  "_links": {
   "self": {
    "href": "/api/protocols/s3/services/"
   }
  }
 }
]
}
```

Creating an S3 server configuration (HTTPS)

```
# The API:
/api/protocols/s3/services

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"comment\":
\"http S3 server\", \"enabled\": true, \"name\": \"Server-1\", \"svm\": {
\"name\": \"vs1\", \"uuid\": \"db2ec036-8375-11e9-99e1-0050568e3ed9\" },
\"is_https_enabled\": \"false\" }"
```

Creating an S3 server configuration (HTTP)

```
# The API:
/api/protocols/s3/services

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"comment\":
\"https S3 server\", \"enabled\": true, \"name\": \"Server-1\", \"svm\": {
\"name\": \"vs1\", \"uuid\": \"db2ec036-8375-11e9-99e1-0050568e3ed9\" },
\"certificate\": { \"uuid\": \"db2ec036-8375-11e9-99e1-0050568e3ed9\" }}"
```

Disable s3 server for the specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/03ce5c36-f269-
11e8-8852-0050568e5298" -H "accept: application/json" -H "Content-Type:
application/json" -d "{ \"enabled\": false }"
```

Deleting the S3 server for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/a425f10b-ad3b-
11e9-b559-0050568e8222?delete_all=false" -H  "accept: application/json"
HTTP/1.1 200 OK
Date: Wed, 14 Aug 2019 07:04:24 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 132
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "job": {
      "uuid": "bf74ba50-be61-11e9-bea8-0050568e8222"
    }
  }
]
}
```

Deleting all of the S3 server configuration for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/03ce5c36-f269-
11e8-8852-0050568e5298?delete_all=true" -H "accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Sat, 01 Jun 2019 15:46:39 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/hal+json
{
"job": {
  "uuid": "71eaaf02-8484-11e9-91f7-0050568ebc5f",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/71eaaf02-8484-11e9-91f7-0050568ebc5f"
    }
  }
}
}
```

Retrieve the S3 server configuration for all SVMs

GET `/protocols/s3/services`

Introduced In: 9.7

Retrieves the S3 server configuration for all SVMs. Note that in order to retrieve S3 bucket policy conditions, 'fields' option should be set to '**'.

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.

- `statistics.*`
- `metric.*`

Related ONTAP commands

- `vserver object-store-server show`

Learn more

- DOC /protocols/s3/services

Parameters

Name	Type	In	Required	Description
statistics.latency_raw.other	integer	query	False	Filter by statistics.latency_raw.other • Introduced in: 9.8
statistics.latency_raw.total	integer	query	False	Filter by statistics.latency_raw.total • Introduced in: 9.8
statistics.latency_raw.write	integer	query	False	Filter by statistics.latency_raw.write • Introduced in: 9.8
statistics.latency_raw.read	integer	query	False	Filter by statistics.latency_raw.read • Introduced in: 9.8
statistics.iops_raw.other	integer	query	False	Filter by statistics.iops_raw.other • Introduced in: 9.8

Name	Type	In	Required	Description
statistics.iops_raw.total	integer	query	False	Filter by statistics.iops_raw.total - Introduced in: 9.8
statistics.iops_raw.write	integer	query	False	Filter by statistics.iops_raw.write - Introduced in: 9.8
statistics.iops_raw.read	integer	query	False	Filter by statistics.iops_raw.read - Introduced in: 9.8
statistics.status	string	query	False	Filter by statistics.status - Introduced in: 9.8
statistics.throughput_raw.write	integer	query	False	Filter by statistics.throughput_raw.write - Introduced in: 9.8
statistics.throughput_raw.read	integer	query	False	Filter by statistics.throughput_raw.read - Introduced in: 9.8
statistics.throughput_raw.total	integer	query	False	Filter by statistics.throughput_raw.total - Introduced in: 9.8

Name	Type	In	Required	Description
statistics.timestamp	string	query	False	Filter by statistics.timestamp • Introduced in: 9.8
name	string	query	False	Filter by name • maxLength: 253 • minLength: 3
is_http_enabled	boolean	query	False	Filter by is_http_enabled • Introduced in: 9.8
users.comment	string	query	False	Filter by users.comment • maxLength: 256 • minLength: 0
users.key_time_to_live	string	query	False	Filter by users.key_time_to_live • Introduced in: 9.14
users.svm.name	string	query	False	Filter by users.svm.name
users.svm.uuid	string	query	False	Filter by users.svm.uuid
users.name	string	query	False	Filter by users.name • maxLength: 64 • minLength: 1
users.key_expiry_time	string	query	False	Filter by users.key_expiry_time • Introduced in: 9.14

Name	Type	In	Required	Description
users.access_key	string	query	False	Filter by users.access_key
enabled	boolean	query	False	Filter by enabled
metric.iops.other	integer	query	False	Filter by metric.iops.other • Introduced in: 9.8
metric.iops.total	integer	query	False	Filter by metric.iops.total • Introduced in: 9.8
metric.iops.write	integer	query	False	Filter by metric.iops.write • Introduced in: 9.8
metric.iops.read	integer	query	False	Filter by metric.iops.read • Introduced in: 9.8
metric.latency.other	integer	query	False	Filter by metric.latency.other • Introduced in: 9.8
metric.latency.total	integer	query	False	Filter by metric.latency.total • Introduced in: 9.8
metric.latency.write	integer	query	False	Filter by metric.latency.write • Introduced in: 9.8

Name	Type	In	Required	Description
metric.latency.read	integer	query	False	Filter by metric.latency.read - Introduced in: 9.8
metric.timestamp	string	query	False	Filter by metric.timestamp - Introduced in: 9.8
metric.throughput.write	integer	query	False	Filter by metric.throughput.write - Introduced in: 9.8
metric.throughput.read	integer	query	False	Filter by metric.throughput.read - Introduced in: 9.8
metric.throughput.total	integer	query	False	Filter by metric.throughput.total - Introduced in: 9.8
metric.status	string	query	False	Filter by metric.status - Introduced in: 9.8
metric.duration	string	query	False	Filter by metric.duration - Introduced in: 9.8

Name	Type	In	Required	Description
default_unix_user	string	query	False	Filter by default_unix_user - Introduced in: 9.12
port	integer	query	False	Filter by port - Introduced in: 9.8 - Max value: 65535 - Min value: 1
comment	string	query	False	Filter by comment - maxLength: 256 - minLength: 0
default_win_user	string	query	False	Filter by default_win_user - Introduced in: 9.12
max_key_time_to_live	string	query	False	Filter by max_key_time_to_live - Introduced in: 9.15
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
buckets.is_nas_path_mutable	boolean	query	False	Filter by buckets.is_nas_path_mutable - Introduced in: 9.17

Name	Type	In	Required	Description
buckets.nas_path	string	query	False	Filter by buckets.nas_path - Introduced in: 9.12
buckets.encryption.enabled	boolean	query	False	Filter by buckets.encryption.enabled
buckets.allowed	boolean	query	False	Filter by buckets.allowed - Introduced in: 9.12
buckets.protection_status.destination.is_ontap	boolean	query	False	Filter by buckets.protection_status.destination.is_ontap - Introduced in: 9.10
buckets.protection_status.destination.is_cloud	boolean	query	False	Filter by buckets.protection_status.destination.is_cloud - Introduced in: 9.10
buckets.protection_status.destination.is_external_cloud	boolean	query	False	Filter by buckets.protection_status.destination.is_external_cloud - Introduced in: 9.12
buckets.protection_status.is_protected	boolean	query	False	Filter by buckets.protection_status.is_protected - Introduced in: 9.10
buckets.svm.name	string	query	False	Filter by buckets.svm.name

Name	Type	In	Required	Description
buckets.svm.uuid	string	query	False	Filter by buckets.svm.uuid
buckets.retention.default_period	string	query	False	Filter by buckets.retention.default_period • Introduced in: 9.14
buckets.retention.mode	string	query	False	Filter by buckets.retention.mode • Introduced in: 9.14
buckets.role	string	query	False	Filter by buckets.role • Introduced in: 9.10
buckets.size	integer	query	False	Filter by buckets.size • Max value: 67553994410557440 • Min value: 107374182400
buckets.logical_used_size	integer	query	False	Filter by buckets.logical_used_size
buckets.uuid	string	query	False	Filter by buckets.uuid
buckets.volume.name	string	query	False	Filter by buckets.volume.name
buckets.volume.uuid	string	query	False	Filter by buckets.volume.uuid

Name	Type	In	Required	Description
buckets.comment	string	query	False	Filter by buckets.comment • maxLength: 256 • minLength: 0
buckets.qos_policy.min_throughput_mbps	integer	query	False	Filter by buckets.qos_policy.min_throughput_mbps • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
buckets.qos_policy.max_throughput_iops	integer	query	False	Filter by buckets.qos_policy.max_throughput_iops • Introduced in: 9.8 • Max value: 2147483647 • Min value: 0
buckets.qos_policy.max_throughput_mbps	integer	query	False	Filter by buckets.qos_policy.max_throughput_mbps • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
buckets.qos_policy.name	string	query	False	Filter by buckets.qos_policy.name • Introduced in: 9.8

Name	Type	In	Required	Description
buckets.qos_policy.min_throughput_iops	integer	query	False	Filter by buckets.qos_policy.min_throughput_iops • Introduced in: 9.8 • Max value: 2147483647 • Min value: 0
buckets.qos_policy.uuid	string	query	False	Filter by buckets.qos_policy.uuid • Introduced in: 9.8
buckets.qos_policy.max_throughput	string	query	False	Filter by buckets.qos_policy.max_throughput • Introduced in: 9.17
buckets.qos_policy.min_throughput	string	query	False	Filter by buckets.qos_policy.min_throughput • Introduced in: 9.17
buckets.versioning_state	string	query	False	Filter by buckets.versioning_state • Introduced in: 9.11
buckets.is_consistent_etag	boolean	query	False	Filter by buckets.is_consistent_etag • Introduced in: 9.17

Name	Type	In	Required	Description
buckets.audit_event_selector.permission	string	query	False	Filter by buckets.audit_event_selector.permission • Introduced in: 9.10
buckets.audit_event_selector.access	string	query	False	Filter by buckets.audit_event_selector.access • Introduced in: 9.10
buckets.type	string	query	False	Filter by buckets.type • Introduced in: 9.12
buckets.lifecycle_management.rules.bucket_name	string	query	False	Filter by buckets.lifecycle_management.rules.bucket_name • Introduced in: 9.14 • maxLength: 63 • minLength: 3
buckets.lifecycle_management.rules.non_current_version_expiration.non_current_days	integer	query	False	Filter by buckets.lifecycle_management.rules.non_current_version_expiration.non_current_days • Introduced in: 9.13
buckets.lifecycle_management.rules.non_current_version_expiration.new_non_current_versions	integer	query	False	Filter by buckets.lifecycle_management.rules.non_current_version_expiration.new_non_current_versions • Introduced in: 9.13

Name	Type	In	Required	Description
buckets.lifecycle_management.rules.uuid	string	query	False	Filter by buckets.lifecycle_management.rules.uuid • Introduced in: 9.14
buckets.lifecycle_management.rules.expiration.expired_object_delete_marker	boolean	query	False	Filter by buckets.lifecycle_management.rules.expiration.expired_object_delete_marker • Introduced in: 9.13
buckets.lifecycle_management.rules.expiration.object_expiry_date	string	query	False	Filter by buckets.lifecycle_management.rules.expiration.object_expiry_date • Introduced in: 9.13
buckets.lifecycle_management.rules.expiration.object_age_days	integer	query	False	Filter by buckets.lifecycle_management.rules.expiration.object_age_days • Introduced in: 9.13
buckets.lifecycle_management.rules.name	string	query	False	Filter by buckets.lifecycle_management.rules.name • Introduced in: 9.13 • maxLength: 256 • minLength: 0

Name	Type	In	Required	Description
buckets.lifecycle_management.rules.svm.name	string	query	False	Filter by buckets.lifecycle_management.rules.svm.name - Introduced in: 9.14
buckets.lifecycle_management.rules.svm.uuid	string	query	False	Filter by buckets.lifecycle_management.rules.svm.uuid - Introduced in: 9.14
buckets.lifecycle_management.rules.object_filter.prefix	string	query	False	Filter by buckets.lifecycle_management.rules.object_filter.prefix - Introduced in: 9.13
buckets.lifecycle_management.rules.object_filter.size_greater_than	integer	query	False	Filter by buckets.lifecycle_management.rules.object_filter.size_greater_than - Introduced in: 9.13
buckets.lifecycle_management.rules.object_filter.size_less_than	integer	query	False	Filter by buckets.lifecycle_management.rules.object_filter.size_less_than - Introduced in: 9.13
buckets.lifecycle_management.rules.object_filter.tags	string	query	False	Filter by buckets.lifecycle_management.rules.object_filter.tags - Introduced in: 9.13

Name	Type	In	Required	Description
buckets.lifecycle_management.rules.enabled	boolean	query	False	Filter by buckets.lifecycle_management.rules.enabled - Introduced in: 9.13
buckets.lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days	integer	query	False	Filter by buckets.lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days - Introduced in: 9.13
buckets.policy.statements.principals	string	query	False	Filter by buckets.policy.statements.principals - Introduced in: 9.8
buckets.policy.statements.sid	string	query	False	Filter by buckets.policy.statements.sid - Introduced in: 9.8 - maxLength: 256 - minLength: 0
buckets.policy.statements.resources	string	query	False	Filter by buckets.policy.statements.resources - Introduced in: 9.8
buckets.policy.statements.effect	string	query	False	Filter by buckets.policy.statements.effect - Introduced in: 9.8

Name	Type	In	Required	Description
buckets.policy.statements.actions	string	query	False	Filter by buckets.policy.statements.actions • Introduced in: 9.8
buckets.policy.statements.conditions.operator	string	query	False	Filter by buckets.policy.statements.conditions.operator • Introduced in: 9.8
buckets.policy.statements.conditions.delimiters	string	query	False	Filter by buckets.policy.statements.conditions.delimiters • Introduced in: 9.8
buckets.policy.statements.conditions.prefixes	string	query	False	Filter by buckets.policy.statements.conditions.prefixes • Introduced in: 9.8
buckets.policy.statements.conditions.usernames	string	query	False	Filter by buckets.policy.statements.conditions.usernames • Introduced in: 9.8
buckets.policy.statements.conditions.source_ips	string	query	False	Filter by buckets.policy.statements.conditions.source_ips • Introduced in: 9.8

Name	Type	In	Required	Description
buckets.policy.statements.conditions.max_keys	integer	query	False	Filter by buckets.policy.statements.conditions.max_keys • Introduced in: 9.8
buckets.name	string	query	False	Filter by buckets.name • maxLength: 63 • minLength: 3
buckets.snapshot_restore.objects_remaining	integer	query	False	Filter by buckets.snapshot_restore.objects_remaining • Introduced in: 9.18
buckets.snapshot_restore.state	string	query	False	Filter by buckets.snapshot_restore.state • Introduced in: 9.18
buckets.snapshot_restore.snapshot	string	query	False	Filter by buckets.snapshot_restore.snapshot • Introduced in: 9.18
buckets.snapshot_restore.progress	integer	query	False	Filter by buckets.snapshot_restore.progress • Introduced in: 9.18
buckets.snapshot_policy.uuid	string	query	False	Filter by buckets.snapshot_policy.uuid • Introduced in: 9.16

Name	Type	In	Required	Description
buckets.snapshot_policy.name	string	query	False	Filter by buckets.snapshot_policy.name - Introduced in: 9.16
buckets.cors.rules.allowed_headers	string	query	False	Filter by buckets.cors.rules.allowed_headers - Introduced in: 9.16
buckets.cors.rules.id	string	query	False	Filter by buckets.cors.rules.id - Introduced in: 9.16 - maxLength: 256 - minLength: 0
buckets.cors.rules.max_age_seconds	integer	query	False	Filter by buckets.cors.rules.max_age_seconds - Introduced in: 9.16
buckets.cors.rules.allowed_origins	string	query	False	Filter by buckets.cors.rules.allowed_origins - Introduced in: 9.16
buckets.cors.rules.expose_headers	string	query	False	Filter by buckets.cors.rules.expose_headers - Introduced in: 9.16
buckets.cors.rules.allowed_methods	string	query	False	Filter by buckets.cors.rules.allowed_methods - Introduced in: 9.16

Name	Type	In	Required	Description
min_lock_retention_period	string	query	False	Filter by min_lock_retention_period • Introduced in: 9.16
max_lock_retention_period	string	query	False	Filter by max_lock_retention_period • Introduced in: 9.16
secure_port	integer	query	False	Filter by secure_port • Introduced in: 9.8 • Max value: 65535 • Min value: 1
certificate.name	string	query	False	Filter by certificate.name • Introduced in: 9.8
certificate.uuid	string	query	False	Filter by certificate.uuid • Introduced in: 9.8
is_https_enabled	boolean	query	False	Filter by is_https_enabled • Introduced in: 9.8
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_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. • Max value: 120 • Min value: 0 • Default value: 15
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_service]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "buckets": [
        {
          "audit_event_selector": {
            "access": "string",
            "permission": "string"
          },
          "comment": "S3 bucket.",
          "cors": {
            "rules": [
              {
                "_links": {
                  "self": {
                    "href": "/api/resourcelink"
                  }
                },
                "allowed_headers": [
                  "x-amz-request-id"
                ],
                "allowed_methods": [
                  "PUT",
                  "DELETE"
                ],
                "allowed_origins": [
                  "http://www.example.com"
                ],
                "expose_headers": [
                  "x-amz-date"
                ],
                "id": "string",
                "max_age_seconds": 1024
              }
            ]
          },
          "lifecycle_management": {
            "rules": [
              {
                "_links": {
                  "self": {
                    "href": "/api/resourcelink"
                  }
                },
                "abort_incomplete_multipart_upload": {
                  "_links": {
                    "self": {
                      "href": "/api/resourcelink"
                    }
                  }
                },
                "bucket_name": "bucket1",
                "expiration": {
                  "_links": {
                    "self": {
                      "href": "/api/resourcelink"
                    }
                  },
                  "object_age_days": 100,
                  "object_expiry_date": "2039-09-23 00:00:00 +0000"
                },
                "name": "string",
                "non_current_version_expiration": {
                  "_links": {
                    "self": {
                      "href": "/api/resourcelink"
                    }
                  }
                },
                "object_filter": {
                  "_links": {
                    "self": {
                      "href": "/api/resourcelink"
                    }
                  },
                  "prefix": "/logs",
            "size_greater_than": 10240,
            "size_less_than": 10485760,
            "tags": [
              "project1=projA",
              "project2=projB"
            ]
          },
          "svm": {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "svm1",
            "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
          },
          "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
        }
      ]
    },
    "logical_used_size": 0,
    "name": "bucket1",
    "nas_path": "/",
    "policy": {
      "statements": [
        {
          "actions": [
            "GetObject",
            "PutObject",
            "DeleteObject",
            "ListBucket"
          ],
          "conditions": [
            {
              "delimiters": [
                "/"
              ],
              "max_keys": [
                1000
              ],
              "operator": "ip_address",
              "prefixes": [
                "pref"
              ],
              "source_ips": [
                "1.1.1.1",
                    "1.2.2.0/24"
                  ],
                  "usernames": [
                    "user1"
                  ]
                }
              ],
              "effect": "allow",
              "principals": [
                "user1",
                "group/grp1",
                "nasgroup/group1"
              ],
              "resources": [
                "bucket1",
                "bucket1/*"
              ],
              "sid": "Full_Access_To_User1!"
            }
          ]
        },
        "qos_policy": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "max_throughput": [
            "900KB/s",
            "500MB/s",
            "120GB/s",
            "5000IOPS",
            "5000IOPS,500KB/s",
            "2500IOPS,100MB/s",
            "1000IOPS,25MB/s"
          ],
          "max_throughput_iops": 10000,
          "max_throughput_mbps": 500,
          "min_throughput": [
            "900KB/s",
            "500MB/s",
            "120GB/s",
            "5000IOPS",
            "5000IOPS,500KB/s",
            "2500IOPS,100MB/s",
            "1000IOPS,25MB/s"
          ],
          "min_throughput_iops": 2000,
          "min_throughput_mbps": 500,
          "name": "performance",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "retention": {
          "default_period": "P10Y",
          "mode": "governance"
        },
        "role": "string",
        "size": 214748364800,
        "snapshot_policy": {
          "name": "default-1weekly",
          "uuid": "3675af31-431c-12fa-114a-20675afebc12"
        },
        "snapshot_restore": {
          "snapshot": "string",
          "state": "string"
        },
        "svm": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "svm1",
          "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        },
        "type": "s3",
        "use_mirrored_aggregates": true,
        "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
        "versioning_state": "enabled",
        "volume": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "volume1",
          "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
        }
      }
    ],
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "comment": "S3 server",
    "default_unix_user": "string",
    "default_win_user": "string",
    "max_key_time_to_live": "PT6H3M",
    "max_lock_retention_period": "P10Y",
    "metric": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "duration": "PT15S",
      "iops": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 11:20:13 +0000"
    },
    "min_lock_retention_period": "P10Y",
    "name": "Server-1",
    "port": 80,
    "secure_port": 443,
    "statistics": {
      "iops_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 11:20:13 +0000"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "users": [
      {
        "access_key": "<AWS-ACCESS-KEY-ID>",
        "comment": "S3 user",
        "key_expiry_time": "2024-01-01 00:00:00 +0000",
        "key_time_to_live": "PT6H3M",
        "name": "user-1",
        "svm": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "svm1",
          "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        }
      }
    ]
  }
]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_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	

collection_links

Name	Type	Description
next	href	
self	href	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.

Name	Type	Description
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form {tag} or {tag=value}.

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The SID length can range from 1 to 256 characters.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance &dash; A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance &dash; An administrator can delete a Governance bucket. no_lock &dash; Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

snapshot_restore

Specifies information regarding a snapshot restore operation on the bucket

Name	Type	Description
objects_remaining	integer	Remaining objects to be restored for the bucket
progress	integer	Snapshot restore progress in percent
snapshot	string	Name of the snapshot being restored for the bucket
state	string	Snapshot restore state of the bucket

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.

Name	Type	Description
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 100GB to 60PB.

Name	Type	Description
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
snapshot_restore	snapshot_restore	Specifies information regarding a snapshot restore operation on the bucket
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3"and "nas".
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
_links	_links	
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_ delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.

Name	Type	Description
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won’t expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".","@", and "-".
svm	svm	SVM, applies only to SVM-scoped objects.

s3_service

Specifies the S3 server configuration.

Name	Type	Description
_links	self_link	
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

Name	Type	Description
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
metric	metric	Performance numbers, such as IOPS latency and throughput, for SVM protocols.
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

Name	Type	Description
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
statistics	statistics	These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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 S3 server, users, and buckets configurations

POST `/protocols/s3/services`

Introduced In: 9.7

Creates an S3 server, users, and buckets configurations.

Important notes

- Each SVM can have one S3 server configuration.
- By default, HTTPS is enabled on the S3 server, so a valid certificate must be provided when creating a S3 Server for the SVM.
- One or more buckets and users can also be created using this end-point.
- If creating a user configuration fails, buckets are not created either and already created users are not saved.
- If creating a bucket configuration fails, all buckets already created are saved with no new buckets created.

Required properties

- `svm.uuid` - Existing SVM in which to create an S3 server configuration.

Recommended optional properties

- `enabled` - Specifies the state of the server created.
- `comment` - Any information related to the server created.

Default property values

- `comment` - ""
- `enabled` - *true*
- `is_https_enabled` - *true*

Related ONTAP commands

- `vserver object-store-server create`
- `vserver object-store-server bucket create`
- `vserver object-store-server bucket policy statement create`
- `vserver object-store-server bucket policy-statement-condition create`
- `vserver object-store-server bucket cors-rule create`
- `vserver object-store-server user create`

Learn more

- DOC /protocols/s3/services

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
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.

Name	Type	Description
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>

Name	Type	Description
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

Example request

```
{
  "buckets": [
    {
      "aggregates": [
        {
          "name": "aggr1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      ],
      "audit_event_selector": {
        "access": "string",
        "permission": "string"
      },
      "comment": "S3 bucket.",
      "constituents_per_aggregate": 4,
      "cors": {
        "rules": [
          {
            "allowed_headers": [
              "x-amz-request-id"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ],
            "allowed_origins": [
              "http://www.example.com"
            ],
            "expose_headers": [
              "x-amz-date"
            ],
            "id": "string",
            "max_age_seconds": 1024
          }
        ]
      },
      "lifecycle_management": {
        "rules": [
          {
            "bucket_name": "bucket1",
            "expiration": {
              "object_age_days": 100,
              "object_expiry_date": "2039-09-23 00:00:00 +0000"
            },
            "name": "string",
            "object_filter": {
              "prefix": "/logs",
              "size_greater_than": 10240,
              "size_less_than": 10485760,
              "tags": [
                "project1=projA",
                "project2=projB"
              ]
            },
            "svm": {
              "name": "svm1",
              "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
            },
            "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
          }
        ]
      },
      "logical_used_size": 0,
      "name": "bucket1",
      "nas_path": "/",
      "policy": {
        "statements": [
          {
            "actions": [
              "GetObject",
              "PutObject",
              "DeleteObject",
              "ListBucket"
            ],
            "conditions": [
              {
                "delimiters": [
                  "/"
                ],
                "max_keys": [
                  1000
                ],
                "operator": "ip_address",
                "prefixes": [
                  "pref"
                ],
                "source_ips": [
                  "1.1.1.1",
                  "1.2.2.0/24"
                ],
                "usernames": [
                  "user1"
                ]
              }
            ],
            "effect": "allow",
            "principals": [
              "user1",
              "group/grp1",
              "nasgroup/group1"
            ],
            "resources": [
              "bucket1",
              "bucket1/*"
            ],
            "sid": "Full_Access_To_User1!"
          }
        ]
      },
      "qos_policy": {
        "max_throughput": [
          "900KB/s",
          "500MB/s",
          "120GB/s",
          "5000IOPS",
          "5000IOPS,500KB/s",
          "2500IOPS,100MB/s",
          "1000IOPS,25MB/s"
        ],
        "max_throughput_iops": 10000,
        "max_throughput_mbps": 500,
        "min_throughput": [
          "900KB/s",
          "500MB/s",
          "120GB/s",
          "5000IOPS",
          "5000IOPS,500KB/s",
          "2500IOPS,100MB/s",
          "1000IOPS,25MB/s"
        ],
        "min_throughput_iops": 2000,
        "min_throughput_mbps": 500,
        "name": "performance",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "retention": {
        "default_period": "P10Y",
        "mode": "governance"
      },
      "role": "string",
      "size": 214748364800,
      "snapshot_policy": {
        "name": "default-1weekly",
        "uuid": "3675af31-431c-12fa-114a-20675afebc12"
      },
      "snapshot_restore": {
        "snapshot": "string",
        "state": "string"
      },
      "storage_service_level": "value",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "type": "s3",
      "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
      "versioning_state": "enabled",
      "volume": {
        "name": "volume1",
        "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
      }
    }
  ],
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "comment": "S3 server",
  "default_unix_user": "string",
  "default_win_user": "string",
  "max_key_time_to_live": "PT6H3M",
  "max_lock_retention_period": "P10Y",
  "min_lock_retention_period": "P10Y",
  "name": "Server-1",
  "port": 80,
  "secure_port": 443,
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    {
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "comment": "S3 user",
      "key_expiry_time": "2024-01-01 00:00:00 +0000",
      "key_time_to_live": "PT6H3M",
      "name": "user-1",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Response

```
Status: 201, Created
```

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

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "job": {
        "uuid": "string"
      },
      "users": [
        {
          "access_key": "<AWS-ACCESS-KEY-ID>",
          "key_expiry_time": "2024-01-01 00:00:00 +0000",
          "name": "user-1",
          "secret_key": "<AWS-SECRET-ACCESS-KEY>"
        }
      ]
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1115127	The cluster lacks a valid S3 license.
2621706	The specified "{svm.uuid}" and "{svm.name}" refer to different SVMs.
92405789	The specified object server name contains invalid characters or not a fully qualified domain name. Valid characters for an object store server name are 0-9, A-Z, a-z, ".", and "-".

Error Code	Description
92405790	Object store server names must have between 3 and 253 characters.
92405839	Creating an object store server requires an effective cluster version of data ONTAP 9.7.0 or later. Upgrade all the nodes to 9.7.0 or later and try the operation again.
92405853	Failed to create the object store server because Cloud Volumes ONTAP does not support object store servers.
92405863	An error occurs when creating an S3 user or bucket. The reason for failure is detailed in the error message. Follow the error codes specified for the user or bucket endpoints to see details for the failure.
92405863	Failed to create bucket "{bucket name}". Reason: "Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: Bucket name "{bucket name}" contains invalid characters or invalid character combinations. Valid characters for a bucket name are 0-9, a-z, ".", and "-". Invalid character combinations are ".-", "-.", and "..". ". Resolve all the issues and retry the operation.
92405863	Failed to create bucket "{bucket name}". Reason: "Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: Invalid QoS policy group specified "{qos policy}". The specified QoS policy group has a min-throughput value set, and the workload being assigned resides on a platform that does not support min-throughput or the cluster is in a mixed version state and the effective cluster version of ONTAP does not support min-throughput on this platform. Resolve all the issues and retry the operation.
92405863	Failed to create bucket "{bucket name}". Reason: "User(s) "{user name(s)}" specified in the principal list do not exist for SVM "{svm.name}". Use the "object-store-server user create" command to create a user.". Resolve all the issues and retry the operation.
92405863	Failed to create user "{user name}". Reason: "SVM "Cluster" is not a data SVM. Specify a data SVM.". Resolve all the issues and retry the operation.
92405884	An object store server can only be created on a data SVM. An object store server can also be created on a system SVM on a mixed platform cluster.
92405903	Failed to configure HTTPS on an object store server for SVM "{svm.name}". Reason: {Reason of failure}.
92405900	Certificate not found for SVM "{svm.name}".

Error Code	Description
92405917	The specified certificate name and UUID do not refer to the same certificate.
92406020	Only certificates of type "server" are supported.
92406044	Failed to set default UNIX user for SVM "{svm.name}". Reason: UNIX user can only be created on a Data SVM.
92406071	S3 protocol is not present in the allowed protocol list for SVM "{svm.name}".
92406196	The specified value for the "key_time_to_live" field cannot be greater than the maximum limit specified for the "max_key_time_to_live" field in the object store server.
92406197	Object store user "user-2" must have a non-zero value for the "key_time_to_live" field because the maximum limit specified for the "max_key_time_to_live" field in the object store server is not zero.
92406230	The value for "retention.default_period" parameter for object store bucket "{bucket}" cannot be greater than the maximum lock retention period set in the object store server for SVM "{SVM}". Check the maximum allowed lock retention period present in the object store server for SVM "{SVM}" and try the operation again.
92406231	One or more object store buckets exist with a default retention period greater than the "max_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.
92406236	The value for "retention.default_period" parameter for object store bucket "{bucket}" cannot be less than the minimum lock retention period set in the object store server for SVM "{SVM}". Check the minimum allowed lock retention period present in the object store server for SVM "{SVM}" and try the operation again.
92406237	One or more object store buckets exist with a default retention period less than the "min_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.
92406238	The value for the "min_lock_retention_period" parameter cannot be greater than the "max_lock_retention_period" parameter for the object store server for SVM "vs1".
92406217	The specified "-allowed-headers" in not valid because it contains more than one wild card ("__") character.;

Error Code	Description
92406224	A Cross-Origin Resource Sharing (CORS) rule must have an origin and HTTP method specified.;
92406211	The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and POST.;
92405863	Failed to create CORS rules for bucket "bb1". Reason: "Field "index" cannot be specified for this operation.". Resolve all the issues and retry the operation.;
92406228	Cannot exceed the maximum limit of 100 Cross-Origin Resource Sharing (CORS) rules per S3 bucket "{bucket}" in SVM "{SVM}".;
92405968	Subnet "{condition.source_ips}" is not a valid IP subnet because it contains non-zero values in the host component of the address. Subnet address "{valid source ips subnet}" identifies a valid subnet for the given mask length. Example: "10.0.1.0/24" is a valid subnet while as"10.0.1.1/24" is invalid.";

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form {tag} or {tag=value}.

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.

Name	Type	Description
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

Name	Type	Description
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The SID length can range from 1 to 256 characters.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance &dash; A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance &dash; An administrator can delete a Governance bucket. no_lock &dash; Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

snapshot_restore

Specifies information regarding a snapshot restore operation on the bucket

Name	Type	Description
objects_remaining	integer	Remaining objects to be restored for the bucket
progress	integer	Snapshot restore progress in percent
snapshot	string	Name of the snapshot being restored for the bucket
state	string	Snapshot restore state of the bucket

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.

Name	Type	Description
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
aggregates	array[aggregates]	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume.
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.

Name	Type	Description
constituents_per_aggregate	integer	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 100GB to 60PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
snapshot_restore	snapshot_restore	Specifies information regarding a snapshot restore operation on the bucket
storage_service_level	string	Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme".
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	Specifies the bucket type. Valid values are "s3"and "nas".
use_mirrored_aggregates	boolean	Specifies whether mirrored aggregates are selected when provisioning a FlexGroup. Only mirrored aggregates are used if this parameter is set to "true" and only unmirrored aggregates are used if this parameter is set to "false". The default value is "true" for a MetroCluster configuration and is "false" for a non-MetroCluster configuration.
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_ delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.

Name	Type	Description
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won’t expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".","@", and "-".
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

s3_service

Specifies the S3 server configuration.

Name	Type	Description
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

Name	Type	Description
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

Name	Type	Description
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

collection_links

job_link

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

s3_service_user_post_response

Name	Type	Description
access_key	string	Specifies the access key for the user.
key_expiry_time	string	Specifies the date and time after which the keys expire and are no longer valid.
name	string	The name of the user.
secret_key	string	Specifies the secret key for the user.

warning

Specifies a warning message sent from the S3 server during a POST or PATCH operation.

Name	Type	Description
code	integer	Warning code of the warning encountered.

Name	Type	Description
message	string	Details of the warning sent from the S3 server.

records

Name	Type	Description
job	job_link	
users	array[s3_service_user_post_response]	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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 the S3 server configuration for an SVM

DELETE `/protocols/s3/services/{svm.uuid}`

Introduced In: 9.7

Deletes the S3 server configuration of an SVM. If the 'delete_all' parameter is set to false, only the S3 server is deleted. Otherwise S3 users and buckets present on the SVM are also deleted. Note that only empty buckets can be deleted. This endpoint returns the S3 server delete job-uuid in response. To monitor the job status follow /api/cluster/jobs/<job-uuid>.</job-uuid>

Related ONTAP commands

- `vserver object-store-server delete`

Learn more

- DOC /protocols/s3/services

Parameters

Name	Type	In	Required	Description
delete_all	boolean	query	False	Delete S3 server and associated users and empty buckets. • Default value: 1
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: 0 • Max value: 120 • Min value: 0

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
92405864	An error occurs when deleting an S3 user or bucket. The reason for failure is detailed in the error message. Follow the error codes specified for the user or bucket endpoints to see details for the failure.

Name	Type	Description
error	returned_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	

job_link

Name	Type	Description
_links	_links	
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

returned_error

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

Retrieve the S3 server configuration for an SVM

GET `/protocols/s3/services/{svm.uuid}`

Introduced In: 9.7

Retrieves the S3 Server configuration of an SVM. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to '**'.

Related ONTAP commands

- `vserver object-store-server show`

Learn more

- DOC /protocols/s3/services

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	self_link	
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.

Name	Type	Description
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
metric	metric	Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
statistics	statistics	These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "buckets": [
    {
      "audit_event_selector": {
        "access": "string",
        "permission": "string"
      },
      "comment": "S3 bucket.",
      "cors": {
        "rules": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "allowed_headers": [
              "x-amz-request-id"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ],
            "allowed_origins": [
              "http://www.example.com"
            ],
            "expose_headers": [
              "x-amz-date"
            ],
            "id": "string",
            "max_age_seconds": 1024
          }
        ]
      },
      "lifecycle_management": {
        "rules": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "abort_incomplete_multipart_upload": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              }
            },
            "bucket_name": "bucket1",
            "expiration": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              },
              "object_age_days": 100,
              "object_expiry_date": "2039-09-23 00:00:00 +0000"
            },
            "name": "string",
            "non_current_version_expiration": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              }
            },
            "object_filter": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              },
              "prefix": "/logs",
              "size_greater_than": 10240,
              "size_less_than": 10485760,
              "tags": [
                "project1=projA",
                "project2=projB"
              ]
            },
            "svm": {
              "_links": {
                "self": {
                  "href": "/api/resourcelink"
                }
              },
              "name": "svm1",
              "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
            },
            "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
          }
        ]
      },
      "logical_used_size": 0,
      "name": "bucket1",
      "nas_path": "/",
      "policy": {
        "statements": [
          {
            "actions": [
              "GetObject",
              "PutObject",
              "DeleteObject",
              "ListBucket"
            ],
            "conditions": [
              {
                "delimiters": [
                  "/"
                ],
                "max_keys": [
                  1000
                ],
                "operator": "ip_address",
                "prefixes": [
                  "pref"
                ],
                "source_ips": [
                  "1.1.1.1",
                  "1.2.2.0/24"
                ],
                "usernames": [
                  "user1"
                ]
              }
            ],
            "effect": "allow",
            "principals": [
              "user1",
              "group/grp1",
                "nasgroup/group1"
              ],
              "resources": [
                "bucket1",
                "bucket1/*"
              ],
              "sid": "Full_Access_To_User1!"
            }
          ]
        },
        "qos_policy": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "max_throughput": [
            "900KB/s",
            "500MB/s",
            "120GB/s",
            "5000IOPS",
            "5000IOPS,500KB/s",
            "2500IOPS,100MB/s",
            "1000IOPS,25MB/s"
          ],
          "max_throughput_iops": 10000,
          "max_throughput_mbps": 500,
          "min_throughput": [
            "900KB/s",
            "500MB/s",
            "120GB/s",
            "5000IOPS",
            "5000IOPS,500KB/s",
            "2500IOPS,100MB/s",
            "1000IOPS,25MB/s"
          ],
          "min_throughput_iops": 2000,
          "min_throughput_mbps": 500,
          "name": "performance",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "retention": {
          "default_period": "P10Y",
          "mode": "governance"
        },
        "role": "string",
        "size": 214748364800,
        "snapshot_policy": {
          "name": "default-1weekly",
          "uuid": "3675af31-431c-12fa-114a-20675afebc12"
        },
        "snapshot_restore": {
          "snapshot": "string",
          "state": "string"
        },
        "svm": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "svm1",
          "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        },
        "type": "s3",
        "use_mirrored_aggregates": true,
        "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
        "versioning_state": "enabled",
        "volume": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "volume1",
          "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
        }
      }
    ],
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "comment": "S3 server",
    "default_unix_user": "string",
    "default_win_user": "string",
    "max_key_time_to_live": "PT6H3M",
    "max_lock_retention_period": "P10Y",
    "metric": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "duration": "PT15S",
      "iops": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 11:20:13 +0000"
    },
    "min_lock_retention_period": "P10Y",
    "name": "Server-1",
    "port": 80,
    "secure_port": 443,
    "statistics": {
      "iops_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 11:20:13 +0000"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "users": [
      {
        "access_key": "<AWS-ACCESS-KEY-ID>",
        "comment": "S3 user",
        "key_expiry_time": "2024-01-01 00:00:00 +0000",
        "key_time_to_live": "PT6H3M",
        "name": "user-1",
        "svm": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "svm1",
          "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        }
      }
    ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_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	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form {tag} or {tag=value}.

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The SID length can range from 1 to 256 characters.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance &dash; A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance &dash; An administrator can delete a Governance bucket. no_lock &dash; Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

snapshot_restore

Specifies information regarding a snapshot restore operation on the bucket

Name	Type	Description
objects_remaining	integer	Remaining objects to be restored for the bucket
progress	integer	Snapshot restore progress in percent
snapshot	string	Name of the snapshot being restored for the bucket
state	string	Snapshot restore state of the bucket

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.

Name	Type	Description
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 100GB to 60PB.

Name	Type	Description
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
snapshot_restore	snapshot_restore	Specifies information regarding a snapshot restore operation on the bucket
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3"and "nas".
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
_links	_links	
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.

Name	Type	Description
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won’t expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".","@", and "-".
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Update the S3 server configuration for an SVM

PATCH `/protocols/s3/services/{svm.uuid}`

Introduced In: 9.7

Updates the S3 Server configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server modify`

Learn more

- DOC /protocols/s3/services

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.

Name	Type	Description
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>

Name	Type	Description
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.

Example request

```
{
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "comment": "S3 server",
  "default_unix_user": "string",
  "default_win_user": "string",
  "max_key_time_to_live": "PT6H3M",
  "max_lock_retention_period": "P10Y",
  "min_lock_retention_period": "P10Y",
  "name": "Server-1",
  "port": 80,
  "secure_port": 443
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
92405789	The name "{object server name}" is not valid. A valid object server name must be a fully qualified domain name.
92405790	Object store server name is not valid. Object store server names must have between 3 and 253 characters.
92405900	Certificate not found for SVM "{svm.name}".
92405917	The specified certificate name and UUID do not refer to the same certificate.
92406020	Only certificates of type "server" are supported.
	92406153

Error Code	Description
Set the enabled field of the server to "down" before modifying following fields: {field name}	92406231
One or more object store buckets exist with a default retention period greater than the "max_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.	92406237
One or more object store buckets exist with a default retention period less than the "min_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.	92406238

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form {tag} or {tag=value}.

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The SID length can range from 1 to 256 characters.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method. • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

snapshot_restore

Specifies information regarding a snapshot restore operation on the bucket

Name	Type	Description
objects_remaining	integer	Remaining objects to be restored for the bucket
progress	integer	Snapshot restore progress in percent
snapshot	string	Name of the snapshot being restored for the bucket

Name	Type	Description
state	string	Snapshot restore state of the bucket

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 100GB to 60PB.

Name	Type	Description
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
snapshot_restore	snapshot_restore	Specifies information regarding a snapshot restore operation on the bucket
type	string	Specifies the bucket type. Valid values are "s3"and "nas".
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_ delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

s3_service

Specifies the S3 server configuration.

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.

Name	Type	Description
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property. • Valid format is: 'PnDTnHnMnS|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

Name	Type	Description
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters':' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

Name	Type	Description
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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

Trademark information