Manage S3 buckets

REST API reference

NetApp
February 07, 2026

Table of Contents

Manage S3 buckets

Manage S3 buckets

Overview

An S3 bucket is a container of objects. Each bucket defines an object namespace. S3 server requests specify objects using a bucket-name and object-name pair. An object consists of data, along with optional metadata and access controls, that is accessible using a name. An object resides within a bucket. There can be more than one bucket in an S3 server. Buckets that are created for the server are associated with an S3 user that is created on the S3 server.

Examples

Retrieving all fields for all S3 buckets of a cluster

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

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

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
    "name": "bucket-2",
    "volume": {
      "name": "fg_oss_1558514455",
      "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
    },
    "size": 209715200,
    "logical_used_size": 157286400,
    "encryption": {
      "enabled": false
    },
    "comment": "S3 bucket.",
    "qos_policy": {
      "min_throughput_iops": 0,
      "min_throughput_mbps": 0,
      "max_throughput_iops": 1000,
      "max_throughput_mbps": 0,
      "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
      "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
    },
    "snapshot-policy": {
      "name": "default-1weekly",
      "uuid": "f9c5f090-4ac8-11ef-ba24-005056a7ceb6"
    },
  },
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "a8234aec-7e06-11e9-97e8-0050568ea123",
    "name": "bucket-1",
    "volume": {
      "name": "fg_oss_1558690256",
      "uuid": "a36a1ea7-7e06-11e9-97e8-0050568ea123"
    },
    "size": 1677721600,
    "logical_used_size": 0,
    "encryption": {
      "enabled": false
    },
    "comment": "bucket2",
    "qos_policy": {
      "min_throughput_iops": 0,
      "min_throughput_mbps": 0,
      "max_throughput_iops": 1000,
      "max_throughput_mbps": 0,
      "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
      "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
    }
  },
  {
    "svm": {
      "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
      "name": "vs2"
    },
    "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
    "name": "bucket-3",
    "volume": {
      "name": "fg_oss_1558690257",
      "uuid": "a46a1ea7-7e06-11e9-97e8-0050568ea123"
    },
    "size": 1677721600,
    "logical_used_size": 1075838976,
    "encryption": {
      "enabled": false
    },
    "comment": "bucket3",
    "qos_policy": {
      "min_throughput_iops": 0,
      "min_throughput_mbps": 0,
      "max_throughput_iops": 1000,
      "max_throughput_mbps": 0,
      "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
      "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
    },
    "policy": {
      "statements": [
        {
          "effect": "allow",
          "actions": [
            "*"
          ],
          "principals": [
            "Alice"
          ],
          "resources": [
            "bucket-3",
            "bucket-3/*"
          ],
          "sid": "fullAccessForAliceToBucket",
          "conditions": [
            {
              "operator": "ip_address",
              "source_ips": [
                "1.1.1.1/10"
              ]
            }
          ]
        }
      ]
    },
    "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
        }
      ]
    }
  }
],
"num_records": 3
}
```

Retrieving all S3 buckets of a cluster ordered by size

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

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/buckets?return_records=true&order_by=size" -H
"accept: application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "754389d0-7e13-11e9-bfdc-0050568ea123",
    "name": "bb1",
    "size": 838860800
  },
  {
    "svm": {
      "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
      "name": "vs2"
    },
    "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
    "name": "bb2",
    "size": 838860800
  },
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "a8234aec-7e06-11e9-97e8-0050568ea123",
    "name": "bucket-1",
    "size": 1677721600
  }
],
"num_records": 3
}
```

Retrieving all S3 buckets of a cluster with name "bb2"

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

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/buckets?name=bb2&return_records=true" -H "accept:
application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "087d940e-7e15-11e9-bfdc-0050568ea123",
    "name": "bb2"
  },
  {
    "svm": {
      "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
      "name": "vs2"
    },
    "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
    "name": "bb2"
  }
],
"num_records": 2
}
```

Retrieving the specified bucket associated with an SVM

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

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/buckets/12f3ba4c-7ae0-
11e9-8c06-0050568ea123/527812ab-7c6d-11e9-97e8-0050568ea123" -H "accept:
application/json"

# The response:
{
"svm": {
  "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
  "name": "vs1"
},
"uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
"name": "bucket-2",
"volume": {
  "name": "fg_oss_1558514455",
  "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
},
"size": 209715200,
"logical_used_size": 157286400,
"encryption": {
  "enabled": false
},
"comment": "S3 bucket.",
"qos_policy": {
  "min_throughput_iops": 0,
  "min_throughput_mbps": 0,
  "max_throughput_iops": 1000,
  "max_throughput_mbps": 0,
  "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
  "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
}
}
```

Creating an S3 bucket for an SVM

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

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"svm\": {
\"name\": \"vs1\" } }"



# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "name": "bucket-3",
    "comment": "S3 bucket."
  }
],
"job": {
  "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Creating an S3 bucket along with QoS policy for an SVM

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

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"comment\": \"S3 bucket.\", \"name\": \"bucket-3\", \"svm\": { \"name\":
\"vs1\" },  \"qos_policy\": { \"min_throughput_iops\": 0,
\"min_throughput_mbps\": 0, \"max_throughput_iops\": 1000000,
\"max_throughput_mbps\": 900000, \"uuid\": \"02d07a93-6177-11ea-b241-
000c293feac8\", \"name\":
\"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "name": "bucket-3",
    "comment": "S3 bucket."
  }
],
"job": {
  "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Creating an S3 bucket along with policies and conditions for an SVM

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

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"policy\": {
\"statements\": [ { \"actions\": [ \"GetObject\" ], \"conditions\": [ {
\"operator\": \"ip_address\", \"source_ips\": [ \"1.1.1.1/23\",
\"1.2.2.2/20\" ] } ], \"effect\": \"allow\", \"resources\": [ \"bucket-
3/policies/examples/*\" ], \"sid\": \"AccessToGetObjectForAllUsersofSVM\"
}, { \"actions\": [ \"*Object\" ], \"effect\": \"deny\", \"principals\": [
\"mike\" ], \"resources\": [ \"bucket-3/policy-docs/*\", \"bucket-
3/confidential-*\" ], \"sid\": \"DenyAccessToObjectForMike\" }, {
\"actions\": [ \"GetObject\" ], \"effect\": \"allow\", \"principals\": [
\"*\" ], \"resources\": [ \"bucket-3/readme\" ], \"sid\":
\"AnonymousAccessToGetObjectForUsers\" } ] }, \"svm\": { \"uuid\":
\"259b4e46-2d33-11ea-9145-005056bbbec1\" } }"



# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "name": "bucket-3",
    "comment": "S3 bucket."
  }
],
"job": {
  "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Creating an S3 bucket and CORS rules for an SVM

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

# The call:

curl -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"cors\": {
\"rules\": [{ \"allowed_headers\": [ \"x-amz-request-id\" ],
\"allowed_methods\": [ \"PUT\", \"DELETE\" ], \"allowed_origins\": [
\"http://www.example.com\" ], \"expose_headers\": [
\"http://www.example.com\" ], \"id\": \"id1\", \"max_age_seconds\": 1024
}]}, \"svm\": { \"uuid\": \"259b4e46-2d33-11ea-9145-005056bbbec1\" }}"



# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "name": "bucket-3",
    "comment": "S3 bucket."
  }
],
"job": {
  "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Creating an S3 bucket along with a bucket lifecycle management rule for an SVM

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

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-4\",
\"lifecycle_management\": { \"rules\": [ { \"name\": \"rule1\",
\"expiration\": { \"object_age_days\" : \"1000\" },
\"abort_incomplete_multipart_upload\" : { \"after_initiation_days\" : 200
}, \"object_filter\": { \"prefix\" : \"obj1*/\" ,  \"size_greater_than\" :
\"1000\" } }, { \"name\": \"rule2\", \"object_filter\": {
\"size_greater_than\" : \"50\" }, \"expiration\": { \"object_age_days\" :
\"5000\" } } ] } }"



# The response:
HTTP/1.1 202 Accepted
Date: Fri, 18 April 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-4
Content-Length: 353
Content-Type: application/json
{
"num_records": 1,
"records": [
  {
    "name": "bucket-4",
    "comment": "S3 bucket."
  }
],
"job": {
  "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Creating an S3 bucket with a snapshot-policy

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

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"comment\":
\"S3 snapshot policy bucket.\", \"snapshot_policy\": { \"name\":
\"default-1weekly\", \"uuid\": \"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" },
\"name\": \"bucket-7\", \"svm.uuid\": \"8c38f10b-4871-11ef-aab5-
005056a7ceb6\" }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 17:16:15 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/8c38f10b-4871-11ef-aab5-
005056a7ceb6/buckets/9f21f404-4aa4-11ef-ba24-005056a7ceb6
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "99978136-4aa9-11ef-ba24-005056a7ceb6",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/99978136-4aa9-11ef-ba24-005056a7ceb6"
    }
  }
}
}
```

Updating an S3 bucket for an SVM

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-
11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-
005056bb883a?return_records=true" -H "accept:
application/json?return_records=true" -H "Content-Type: application/json"
-d "{ \"comment\": \"Bucket modified.\", \"size\": 111111111111,
\"qos_policy\": { \"min_throughput_iops\": 0, \"min_throughput_mbps\": 0,
\"max_throughput_iops\": 1000000, \"max_throughput_mbps\": 900000,
\"uuid\": \"02d07a93-6177-11ea-b241-000c293feac8\", \"name\":
\"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\" }}"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Updating an S3 bucket policy for an SVM

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-
11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-
005056bb883a?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"policy\": { \"statements\": [ {
\"actions\": [ \"*\" ], \"conditions\": [ { \"operator\": \"ip_address\",
\"source_ips\": [ \"1.1.1.5/23\" ] } ], \"effect\": \"allow\",
\"resources\": [ \"*\" ], \"sid\": \"fullAccessForAllPrincipalsToBucket\"}
] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Updating an S3 bucket CORS configuration for an SVM

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-
11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-
005056bb883a?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"cors\": { \"rules\": [{
\"allowed_headers\": [ \"x-amz-request-id\" ], \"allowed_methods\": [
\"PUT\", \"DELETE\" ], \"allowed_origins\": [ \"http://www.example.com\"
], \"expose_headers\": [ \"http://www.example.com\" ], \"id\": \"id1\",
\"max_age_seconds\": 1024 } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Updating the snapshot-policy for an S3 bucket for an SVM

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

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/8c38f10b-4871-
11ef-aab5-005056a7ceb6/eec0d90e-4934-11ef-947d-005056a7ceb6" -H "accept:
application/json" -H "Content-Type: application/json" -d "{
\"snapshot_policy\": { \"name\": \"default-1weekly\", \"uuid\":
\"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 17:26:17 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "003a4cad-4aab-11ef-ba24-005056a7ceb6",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/003a4cad-4aab-11ef-ba24-005056a7ceb6"
    }
  }
}
}
```

Deleting an S3 bucket for a specified SVM

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

# The call:
curl -iku admin:<password> -X DELETE "https://<mgmt-
ip>/api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/98528221-2d52-11ea-892e-005056bbbec1?return_records=true" -H
"accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:40:17 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
"job": {
  "uuid": "b3af4a54-7e18-11e9-bfdc-0050568ea123",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/b3af4a54-7e18-11e9-bfdc-0050568ea123"
    }
  }
}
}
```

Retrieve all S3 buckets for all SVMs

GET `/protocols/s3/buckets`

Introduced In: 9.7

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

Related ONTAP commands

- `vserver object-store-server bucket show`
- `vserver object-store-server bucket policy statement show`
- `vserver object-store-server bucket policy-statement-condition show`
- `vserver object-store-server bucket lifecycle-management-rule show`
- `vserver object-store-server bucket cors-rule show`

Learn more

- DOC /protocols/s3/buckets

Parameters

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
lifecycle_management.rules.uuid	string	query	False	Filter by lifecycle_management.rules.uuid • Introduced in: 9.14
lifecycle_management.rules.name	string	query	False	Filter by lifecycle_management.rules.name • Introduced in: 9.13 • maxLength: 256 • minLength: 0
lifecycle_management.rules.bucket_name	string	query	False	Filter by lifecycle_management.rules.bucket_name • Introduced in: 9.14 • maxLength: 63 • minLength: 3
lifecycle_management.rules.non_current_version_expiration.new_non_current_versions	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.new_non_current_versions • Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.non_current_version_expiration.non_current_days	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.non_current_days - Introduced in: 9.13
lifecycle_management.rules.expiration.object_age_days	integer	query	False	Filter by lifecycle_management.rules.expiration.object_age_days - Introduced in: 9.13
lifecycle_management.rules.expiration.expired_object_delete_marker	boolean	query	False	Filter by lifecycle_management.rules.expiration.expired_object_delete_marker - Introduced in: 9.13
lifecycle_management.rules.expiration.object_expiry_date	string	query	False	Filter by lifecycle_management.rules.expiration.object_expiry_date - Introduced in: 9.13
lifecycle_management.rules.object_filter.tags	string	query	False	Filter by lifecycle_management.rules.object_filter.tags - Introduced in: 9.13
lifecycle_management.rules.object_filter.prefix	string	query	False	Filter by lifecycle_management.rules.object_filter.prefix - Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.object_filter.size_greater_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_greater_than • Introduced in: 9.13
lifecycle_management.rules.object_filter.size_less_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_less_than • Introduced in: 9.13
lifecycle_management.rules.enabled	boolean	query	False	Filter by lifecycle_management.rules.enabled • Introduced in: 9.13
lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days	integer	query	False	Filter by lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days • Introduced in: 9.13
lifecycle_management.rules.svm.name	string	query	False	Filter by lifecycle_management.rules.svm.name • Introduced in: 9.14
lifecycle_management.rules.svm.uuid	string	query	False	Filter by lifecycle_management.rules.svm.uuid • Introduced in: 9.14

Name	Type	In	Required	Description
comment	string	query	False	Filter by comment • maxLength: 256 • minLength: 0
encryption.enabled	boolean	query	False	Filter by encryption.enabled
policy.statements.resources	string	query	False	Filter by policy.statements.resources • Introduced in: 9.8
policy.statements.actions	string	query	False	Filter by policy.statements.actions • Introduced in: 9.8
policy.statements.effect	string	query	False	Filter by policy.statements.effect • Introduced in: 9.8
policy.statements.conditions.usernames	string	query	False	Filter by policy.statements.conditions.usernames • Introduced in: 9.8
policy.statements.conditions.source_ips	string	query	False	Filter by policy.statements.conditions.source_ips • Introduced in: 9.8
policy.statements.conditions.max_keys	integer	query	False	Filter by policy.statements.conditions.max_keys • Introduced in: 9.8

Name	Type	In	Required	Description
policy.statements.conditions.delimiters	string	query	False	Filter by policy.statements.conditions.delimiters - Introduced in: 9.8
policy.statements.conditions.operator	string	query	False	Filter by policy.statements.conditions.operator - Introduced in: 9.8
policy.statements.conditions.prefixes	string	query	False	Filter by policy.statements.conditions.prefixes - Introduced in: 9.8
policy.statements.principals	string	query	False	Filter by policy.statements.principals - Introduced in: 9.8
policy.statements.sid	string	query	False	Filter by policy.statements.sid - Introduced in: 9.8 - maxLength: 256 - minLength: 0
qos_policy.min_throughput_mbps	integer	query	False	Filter by qos_policy.min_throughput_mbps - Introduced in: 9.8 - Max value: 4194303 - Min value: 0

Name	Type	In	Required	Description
qos_policy.max_throughput_mbps	integer	query	False	Filter by qos_policy.max_throughput_mbps • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
qos_policy.name	string	query	False	Filter by qos_policy.name • Introduced in: 9.8
qos_policy.uuid	string	query	False	Filter by qos_policy.uuid • Introduced in: 9.8
qos_policy.max_throughput	string	query	False	Filter by qos_policy.max_throughput • Introduced in: 9.17
qos_policy.max_throughput_iops	integer	query	False	Filter by qos_policy.max_throughput_iops • Introduced in: 9.8 • Max value: 2147483647 • Min value: 0

Name	Type	In	Required	Description
qos_policy.min_throughput_iops	integer	query	False	Filter by qos_policy.min_throughput_iops - Introduced in: 9.8 - Max value: 2147483647 - Min value: 0
qos_policy.min_throughput	string	query	False	Filter by qos_policy.min_throughput - Introduced in: 9.17
role	string	query	False	Filter by role - Introduced in: 9.10
size	integer	query	False	Filter by size - Max value: 62672162783232000 - Min value: 199229440
is_nas_path_mutable	boolean	query	False	Filter by is_nas_path_mutable - Introduced in: 9.17
uuid	string	query	False	Filter by uuid
logical_used_size	integer	query	False	Filter by logical_used_size
allowed	boolean	query	False	Filter by allowed - Introduced in: 9.12

Name	Type	In	Required	Description
versioning_state	string	query	False	Filter by versioning_state • Introduced in: 9.11
cors.rules.expose_headers	string	query	False	Filter by cors.rules.expose_headers • Introduced in: 9.16
cors.rules.max_age_seconds	integer	query	False	Filter by cors.rules.max_age_seconds • Introduced in: 9.16
cors.rules.allowed_origins	string	query	False	Filter by cors.rules.allowed_origins • Introduced in: 9.16
cors.rules.allowed_methods	string	query	False	Filter by cors.rules.allowed_methods • Introduced in: 9.16
cors.rules.allowed_headers	string	query	False	Filter by cors.rules.allowed_headers • Introduced in: 9.16
cors.rules.id	string	query	False	Filter by cors.rules.id • Introduced in: 9.16 • maxLength: 256 • minLength: 0

Name	Type	In	Required	Description
nas_path	string	query	False	Filter by nas_path - Introduced in: 9.12
retention.mode	string	query	False	Filter by retention.mode - Introduced in: 9.14
retention.default_period	string	query	False	Filter by retention.default_period - Introduced in: 9.14
snapshot_policy.uuid	string	query	False	Filter by snapshot_policy.uuid - Introduced in: 9.16
snapshot_policy.name	string	query	False	Filter by snapshot_policy.name - Introduced in: 9.16
audit_event_selector.permission	string	query	False	Filter by audit_event_selector.permission - Introduced in: 9.10
audit_event_selector.access	string	query	False	Filter by audit_event_selector.access - Introduced in: 9.10

Name	Type	In	Required	Description
protection_status.is_protected	boolean	query	False	Filter by protection_status.is_protected - Introduced in: 9.10
protection_status.destination.is_ontap	boolean	query	False	Filter by protection_status.destination.is_ontap - Introduced in: 9.10
protection_status.destination.is_external_cloud	boolean	query	False	Filter by protection_status.destination.is_external_cloud - Introduced in: 9.12
protection_status.destination.is_cloud	boolean	query	False	Filter by protection_status.destination.is_cloud - Introduced in: 9.10
type	string	query	False	Filter by type - Introduced in: 9.12
volume.uuid	string	query	False	Filter by volume.uuid
volume.name	string	query	False	Filter by volume.name
is_consistent_etag	boolean	query	False	Filter by is_consistent_etag - Introduced in: 9.17

Name	Type	In	Required	Description
name	string	query	False	Filter by name • maxLength: 63 • minLength: 3
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • 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_bucket]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "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": "2039-09-22 20:00:00 -0400"
          },
          "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": "FullAccessToUser1"
          }
        ]
      },
      "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": 1677721600,
      "snapshot_policy": {
        "name": "default-1weekly",
        "uuid": "3675af31-431c-12fa-114a-20675afebc12"
      },
      "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"
      }
    }
  ]
}
```

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	

_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 &lt;tag=value&gt;.</tag>

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 and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

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: • 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: • 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.

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.
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.

Name	Type	Description
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.
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 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
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.

Name	Type	Description
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.

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 the S3 bucket configuration for an SVM

POST `/protocols/s3/buckets`

Introduced In: 9.8

Creates the S3 bucket configuration of an SVM.

Important notes

- Each SVM can have one or more bucket configurations.
- Aggregate lists should be specified explicitly. If not specified, then the bucket is auto-provisioned as a

FlexGroup volume.

- Constituents per aggregate specifies the number of components (or FlexVol volumes) per aggregate. Is specified only when an aggregate list is explicitly defined.
- An access policy can be created along with a bucket create. If creating an access policy fails, bucket configurations are saved and the access policy can be created using the PATCH endpoint.
- "qos_policy" can be specified if a bucket needs to be attached to a QoS group policy during creation time.
- "audit_event_selector" can be specified if a bucket needs to be specify access and permission type for auditing.
- A CORS configuration can be specified along with bucket creation.

Required properties

- `svm.uuid or svm.name` - Existing SVM in which to create the bucket configuration.
- `name` - Bucket name that is to be created.

Recommended optional properties

- `aggregates` - List of aggregates for the FlexGroup volume on which the bucket is hosted on.
- `constituents_per_aggregate` - Number of constituents per aggregate.
- `size` - Specifying the bucket size is recommended.
- `policy` - Specifying a policy enables users to perform operations on buckets; specifying the resource permissions is recommended.
- `qos_policy` - A QoS policy for buckets.
- `audit_event_selector` - Audit policy for buckets.
- `versioning_state` - Versioning state for buckets.
- `type` - Type of bucket.
- `nas_path` - NAS path to which the bucket corresponds to.
- `use_mirrored_aggregates` - Specifies whether mirrored aggregates are selected when provisioning a FlexGroup volume.
- `lifecycle_management` - Object store server lifecycle management policy.
- `retention.mode` - Object lock mode supported on the bucket.
- `retention.default_period` - Specifies the duration of default-retention applicable for objects on the object store bucket.
- `cors` - Specifying CORS rules enables the bucket to service the cross-origin requests.
- `snapshot_policy` - Snapshot policy for the bucket.
- `is_nas_path_mutable` - Specifies whether the NAS bucket mapping with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount.

Default property values

- `size` - 800MB
- `comment` - ""
- `aggregates` - No default value.
- `constituents_per_aggregate` - *4* , if an aggregates list is specified. Otherwise, no default value.
- `policy.statements.actions` - GetObject, PutObject, DeleteObject, ListBucket, ListBucketMultipartUploads, ListMultipartUploadParts, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketVersioning, PutBucketVersioning.
- `policy.statements.principals` - all S3 users and groups in the SVM or the NAS groups.
- `policy.statements.resources` - all objects in the bucket.
- `policy.statements.conditions` - list of bucket policy conditions.
- `versioning_state` - disabled.
- `use_mirrored_aggregates` - *true* for a MetroCluster configuration and *false* for a non-MetroCluster configuration.
- `type` - S3
- `retention.mode` - no_lock

Related ONTAP commands

- `vserver object-store-server bucket create`
- `vserver object-store-server bucket policy statement create`
- `vserver object-store-server bucket lifecycle-management-rule create`
- `vserver object-store-server bucket cors-rule create`

Learn more

- DOC /protocols/s3/buckets

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

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.
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	

Name	Type	Description
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 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.

Name	Type	Description
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.
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.

Example request

```
{
  "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": "2039-09-22 20:00:00 -0400"
        },
        "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": "FullAccessToUser1"
      }
    ]
  },
  "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": 1677721600,
  "snapshot_policy": {
    "name": "default-1weekly",
    "uuid": "3675af31-431c-12fa-114a-20675afebc12"
  },
  "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"
  }
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response

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

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error code	Message
92405777	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason of failure}. ";
92405785	"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 "..". ";
92405786	"Bucket name "{bucket name}" is not valid. Bucket names must have between 3 and 63 characters. ";
92405811	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405812	"Failed to create the object store volume. Reason: {Reason for failure}.";
92405819	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are SnapLock aggregates: {List of aggregates.name}.";
92405820	"Failed to check whether the aggregate "{aggregates.name}" is a FabricPool. Reason: {Reason for failure}.";
92405821	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are FabricPool: {List of aggregates.name}.";
92405827	"Internal Error. Unable to generate object store volume name.";
92405857	"One or more aggregates must be specified if "constituents_per_aggregate" is specified.";
92405858	"Failed to "create" the "bucket" because the operation is only supported on data SVMs.";
92405859	"The specified "aggregates.uuid" "{aggregates.uuid}" does not exist.";

Error code	Message
92405860	"The specified "aggregates.name" "{aggregates.name}" and "aggregates.uuid" "{aggregates.uuid}" refer to different aggregates.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405863	"An error occurs when creating an access policy. The reason for failure is detailed in the error message.";
92405863	"Failed to create lifecycle management rules for bucket "s3bucket1". Reason: {Reason of failure}. ";
92405891	The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/…/…. Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @,?, (,), single quote, *, !, - and $.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_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 &lt;tag=value&gt;.</tag>

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.

Name	Type	Description
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.

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 and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

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	

Name	Type	Description
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.

Name	Type	Description
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.
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	Type	Description
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>

Name	Type	Description
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.

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
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 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
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.
type	string	Specifies the bucket type. Valid values are "s3"and "nas".

Name	Type	Description
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.

job_link

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

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

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 bucket configuration for an SVM

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

Introduced In: 9.8

Deletes the S3 bucket configuration of an SVM. An access policy is also deleted on an S3 bucket "delete" command.

Related ONTAP commands

- `vserver object-store-server bucket delete`
- `vserver object-store-server bucket policy statement delete`
- `vserver object-store-server bucket policy-statement-condition delete`
- `vserver object-store-server bucket lifecycle-management-rule delete`
- `vserver object-store-server bucket cors-rule delete`

Learn more

- DOC /protocols/s3/buckets

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0
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	Message
92405811	"Failed to delete bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405858	"Failed to "delete" the "bucket" because the operation is only supported on data SVMs.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405779	"Failed to remove bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}. ";
92405813	"Failed to delete the object store volume. Reason: {Reason for failure}.";
92405864	"An error occurred when deleting an access policy. The reason for failure is detailed in the error message.";

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 bucket configuration for an SVM

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

Introduced In: 9.8

Retrieves the S3 bucket 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 bucket show`
- `vserver object-store-server bucket policy statement show`
- `vserver object-store-server bucket policy-statement-condition show`
- `vserver object-store-server bucket lifecycle-management-rule show`
- `vserver object-store-server bucket cors-rule show`

Learn more

- DOC /protocols/s3/buckets

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.
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
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.

Name	Type	Description
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.
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 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
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.

Name	Type	Description
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.

Example response

```
{
  "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": "2039-09-22 20:00:00 -0400"
        },
        "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": "FullAccessToUser1"
        }
      ]
    },
    "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": 1677721600,
    "snapshot_policy": {
      "name": "default-1weekly",
      "uuid": "3675af31-431c-12fa-114a-20675afebc12"
    },
    "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"
  }
}
```

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	

_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.

Name	Type	Description
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	

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
_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	
prefix	string	A prefix that is matched against object-names within a bucket.

Name	Type	Description
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 &lt;tag=value&gt;.</tag>

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 and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

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.

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.
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

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 bucket configuration for an SVM

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

Introduced In: 9.8

Updates the S3 bucket configuration of an SVM.

Important notes

- The following fields can be modified for a bucket:
  - `comment` - Any information related to the bucket.
  - `size` - Bucket size.
  - `policy` - An access policy for resources (buckets and objects) that defines their permissions. New policies are created after existing policies are deleted. To retain any of the existing policy statements, you need to specify those statements again. Also, policy conditions can be specified as part of a bucket policy.
  - `qos_policy` - A QoS policy for buckets.
  - `audit_event_selector` - Audit policy for buckets. None can be specified for both access and permission to remove an audit event selector.
  - `versioning-state` - Versioning state of the buckets.
  - `nas_path` - NAS path to which the bucket corresponds to.
  - `retention.default_period` - Specifies the duration of default-retention applicable for objects on the object store bucket.
  - `cors` - Specifying CORS rules enables the bucket to service the cross-origin requests. Note that the new CORS configuration specified will replace the existing one. If you need to retain any of the existing CORS rules, specify those rules again as part of the new CORS rules. To remove all the existing rules, specify an empty CORS configuration as input.
  - `snapshot_policy` - Snapshot policy for the bucket.

Related ONTAP commands

- `vserver object-store-server bucket modify`
- `vserver object-store-server bucket policy statement modify`

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

Learn more

- DOC /protocols/s3/buckets

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.
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.

Request Body

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.

Name	Type	Description
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.
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 190MB to 62PB.

Name	Type	Description
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
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.

Example request

```
{
  "audit_event_selector": {
    "access": "string",
    "permission": "string"
  },
  "comment": "S3 bucket.",
  "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
      }
    ]
  },
  "is_nas_path_mutable": true,
  "logical_used_size": 0,
  "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": "FullAccessToUser1"
      }
    ]
  },
  "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"
  },
  "role": "string",
  "size": 1677721600,
  "snapshot_policy": {
    "name": "default-1weekly",
    "uuid": "3675af31-431c-12fa-114a-20675afebc12"
  },
  "type": "s3",
  "use_mirrored_aggregates": true,
  "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
  "versioning_state": "enabled",
  "volume": {
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

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

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error code	Message
92405778	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}. ";
92405846	"Failed to modify the object store volume. Reason: {Reason for failure}.";
92405811	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405858	"Failed to "modify" the "bucket" because the operation is only supported on data SVMs.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405863	"An error occurs when creating an access policy. The reason for failure is detailed in the error message.";
92405864	"An error occurs when deleting an access policy. The reason for failure is detailed in the error message.";
92405891	The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/…/…. Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @,?, (,), single quote, *, !, - and $.
92405894	"Statements, principals and resources list can have a maximum of 10 entries.";

Error code	Message
92405897	The principals specified in the access policy are not in the correct format. User name must be in between 1 and 64 characters. Valid characters for a user name are 0-9, A-Z, a-z, _, +, =, comma, ., @, and - .
92405898	"The SID specified in the access policy is not valid. Valid characters for a SID are 0-9, A-Z and a-z.";
92406014	"Failed to modify event selector for bucket "{bucket name}". If the value of either access or permission is set to none, they both must be set to none.";
92733458	"[Job job number] Job failed: Failed to modify bucket "s3bucket1" for SVM "vs1". Reason: {Reason for failure}. ";
8454236	"Could not assign qtree "qtree1" to QoS policy group "group1". Invalid QoS policy group specified "group1". 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.";
8454323	"Policy group with UUID "23bwegew-8eqg-121r-bjad-0050e628wq732" does not exist."
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."; //end row //start row
92406236 //end row //start row	"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."; //end row //start row
92406217 //end row //start row	"The specified "allowed_headers" is not valid because it contains more than one wild card ("*") character."; //end row //start row
92406224 //end row //start row	"A Cross-Origin Resource Sharing (CORS) rule must have an origin and HTTP method specified."; //end row //start row

Error code	Message
92406222 //end row //start row	"Cannot specify Cross-Origin Resource Sharing (CORS) configuration for object store bucket "<bucket>" on SVM "<SVM>". Specifying such configuration is supported on object store volumes created in ONTAP 9.8 or later releases only."; //end row //start row
92406211 //end row //start row	"The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and POST."; //end row //start row
92405863 //end row //start row	"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."; //end row //start row
92406228 //end row //start row	"Cannot exceed the maximum limit of 100 Cross-Origin Resource Sharing (CORS) rules per S3 bucket "<bucket>" in SVM "<SVM>".";; //end row

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links [#aggregates] [.api-collapsible-fifth-title] aggregates

Aggregate

[cols=3*,options=header]

|Name |Type |Description

|name |string a|

|uuid |string a|

[#audit_event_selector] [.api-collapsible-fifth-title] audit_event_selector

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

[cols=3*,options=header]

|Name |Type |Description

|access |string a|Specifies read and write access types.

|permission |string a|Specifies allow and deny permission types.

[#rules] [.api-collapsible-fifth-title] rules

Information about the CORS rule of an S3 bucket.

[cols=3*,options=header]

|Name |Type |Description

|allowed_headers |array[string] a|An array of HTTP headers allowed in the cross-origin requests.

|allowed_methods |array[string] a|An array of HTTP methods allowed in the cross-origin requests.

|allowed_origins |array[string] a|List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

|expose_headers |array[string] a|List of extra headers sent in the response that customers can access from their applications.

|id |string a|Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.

|max_age_seconds |integer a|The time in seconds for your browser to cache the preflight response for the specified resource.

[#cors] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|rules |array[rules] a|Specifies an object store bucket CORS rule.

[#encryption] [.api-collapsible-fifth-title] encryption

[cols=3*,options=header]

|Name |Type |Description

|enabled |boolean a|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] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|after_initiation_days |integer a|Number of days of initiation after which uploads can be aborted.

[#expiration] [.api-collapsible-fifth-title] expiration

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

[cols=3*,options=header]

|Name |Type |Description

|expired_object_delete_marker |boolean a|Cleanup object delete markers.

|object_age_days |integer a|Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.

|object_expiry_date |string a|Specific date from when objects can expire. This cannot be used with object_age_days.

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

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

[cols=3*,options=header]

|Name |Type |Description

|new_non_current_versions |integer a|Number of latest non-current versions to be retained.

|non_current_days |integer a|Number of days after which non-current versions can be deleted.

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|prefix |string a|A prefix that is matched against object-names within a bucket.

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or &lt;tag=value&gt;.</tag>

[#svm] [.api-collapsible-fifth-title] svm

Specifies the name of the SVM where this bucket exists.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

[#rules] [.api-collapsible-fifth-title] rules

Information about the lifecycle management rule of a bucket.

[cols=3*,options=header]

|Name |Type |Description

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

|enabled |boolean a|Specifies whether or not the associated rule is enabled.

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

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

|svm |svm a|Specifies the name of the SVM where this bucket exists.

|uuid |string a|Specifies the unique identifier of the bucket.

[#lifecycle_management] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|rules |array[rules] a|Specifies an object store lifecycle management policy.

[#s3_bucket_policy_condition] [.api-collapsible-fifth-title] s3_bucket_policy_condition

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

[cols=3*,options=header]

|Name |Type |Description

|delimiters |array[string] a|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] a|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 a|Condition operator that is applied to the specified condition key.

|prefixes |array[string] a|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] a|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] a|An array of usernames that a current user in the context is evaluated against using the condition operators.

[#s3_bucket_policy_statement] [.api-collapsible-fifth-title] s3_bucket_policy_statement

Specifies information about a single access permission.

[cols=3*,options=header]

|Name |Type |Description

|actions |array[string] a|

|conditions |array[s3_bucket_policy_condition] a|Specifies bucket policy conditions.

|effect |string a|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] a|

|resources |array[string] a|

|sid |string a|Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

[#policy] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|statements |array[s3_bucket_policy_statement] a|Specifies bucket access policy statement.

[#destination] [.api-collapsible-fifth-title] destination

[cols=3*,options=header]

|Name |Type |Description

|is_cloud |boolean a|Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.

|is_external_cloud |boolean a|Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

|is_ontap |boolean a|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] [.api-collapsible-fifth-title] protection_status

Specifies attributes of bucket protection.

[cols=3*,options=header]

|Name |Type |Description

|destination |destination a|

|is_protected |boolean a|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] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|max_throughput |string a|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 a|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 a|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 a|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 a|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 a|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 a|The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.

|uuid |string a|The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

[#retention] [.api-collapsible-fifth-title] retention

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

[cols=3*,options=header]

|Name |Type |Description

|default_period |string a|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] [.api-collapsible-fifth-title] snapshot_policy

Specifies the bucket snapshot policy.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|Specifies the name of the snapshot policy.

|uuid |string a|Specifies the unique identifier of the snapshot policy.

[#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

[#volume] [.api-collapsible-fifth-title] volume

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

[cols=3*,options=header]

|Name |Type |Description

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

|uuid |string a|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] [.api-collapsible-fifth-title] 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.

[cols=3*,options=header]

|Name |Type |Description

|allowed |boolean a|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 a|Audit event selector allows you to specify access and permission types to audit.

|comment |string a|Can contain any additional information about the bucket being created or modified.

|cors |cors a|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 a|

|is_consistent_etag |boolean a|Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |policy a|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 a|Specifies attributes of bucket protection.

|qos_policy |qos_policy a|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 a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be specified using a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |snapshot_policy a|Specifies the bucket snapshot policy.

|type |string a|Specifies the bucket type. Valid values are "s3"and "nas".

|uuid |string a|Specifies the unique identifier of the bucket.

|versioning_state |string a|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 a|Specifies the FlexGroup volume name and UUID where the bucket is hosted.

```
[#job_link] [.api-collapsible-fifth-title] job_link

[cols=3*,options=header]
```

|Name |Type |Description

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

[#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

|Name |Type |Description

|code |string a|Argument code

|message |string a|Message argument

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

|Name |Type |Description

|arguments |array[error_arguments] a|Message arguments

|code |string a|Error code

|message |string a|Error message

|target |string a|The target parameter that caused the error.

====

:leveloffset: -1

:leveloffset: -1

<<< **Copyright information**

Trademark information