Overview

REST API reference

NetApp
February 07, 2026

Table of Contents

Overview

ONTAP REST API Application containers endpoints

Overview

Application containers provision one or more storage objects. Currently, only NAS volumes are supported. Application containers allow you to specify the policies and rules for enabling and managing client access to storage. FlexCache volumes can also be provisioned.

Examples

Creating a FlexVol with NAS (NFS and CIFS access) along with S3 NAS bucket with S3 access policies

```
# The API:
/api/application/containers

# The call:
curl -X POST 'https://<mgmt-ip>/api/application/containers' -d '{ "svm": {
"name": "vs0" }, "volumes": [ { "name": "vol1", "space": { "size": "100mb"
}, "scale_out": "false", "nas": { "path": "/vol1", "export_policy": {
"name": "vol1", "rules": [ { "clients": [ { "match": "0.0.0.0/0" } ],
"rw_rule": [ "any" ], "ro_rule": [ "any" ] } ] }, "cifs": { "shares": [ {
"name": "vol1", "acls": [ { "type": "windows", "permission":
"full_control", "user_or_group": "everyone" } ] } ] } }, "s3_bucket": {
"name": "vol1", "nas_path": "/vol1", "policy": { "statements": [ {
"actions": [ "ListBucket" ], "effect": "allow", "principals": [ "user1",
"group/grp1" ], "resources": [ "vol1", "vol1/*" ] } ] } } } ] }'

#### Response:
{
"job": {
  "uuid": "9c9cabf3-0a88-11ec-a449-005056bbcf9f",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/9c9cabf3-0a88-11ec-a449-005056bbcf9f"
    }
  }
}
}
```

= * post is not supported

POST `/application/containers`

Introduced In: 9.17

- POST is not supported

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
svm	svm	The SVM in which the container is located.
volumes	array[volumes]	A list of NAS volumes to provision.

Example request


```
{
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "volumes": [
    {
      "flexcache": {
        "origins": [
          {
            "svm": {
              "name": "svm1",
              "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
            },
            "volume": {
              "name": "volume1",
              "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
            }
          }
        ]
      },
      "name": "vol_cs_dept",
      "nas": {
        "cifs": {
          "shares": [
            {
              "acls": [
                {
                  "permission": "string",
                  "type": "string",
                  "user_or_group": "ENGDOMAIN\\ad_user"
                }
              ],
              "comment": "HR Department Share",
              "dir_umask": 18,
              "file_umask": 18,
              "name": "HR_SHARE",
              "offline_files": "string",
              "unix_symlink": "string",
              "vscan_profile": "string"
            }
          ]
        },
        "export_policy": {
```

```
      "id": 0,
      "name": "string",
      "rules": [
        {
          "anonymous_user": "string",
          "chown_mode": "string",
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
          ],
          "ntfs_unix_security": "string",
          "protocols": [
            "string"
          ],
          "ro_rule": [
            "string"
          ],
          "rw_rule": [
            "string"
          ],
          "superuser": [
            "string"
          ]
        }
      ]
    },
    "junction_parent": {
      "name": "vs1_root",
      "uuid": "75c9cfb0-3eb4-11eb-9fb4-005056bb088a"
    },
    "path": "/user/my_volume",
    "security_style": "string",
    "unix_permissions": 493
  },
  "qos": {
    "policy": {
      "name": "performance",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  },
  "s3_bucket": {
    "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"
            }
          ]
        }
      },
      "snaplock": {
        "append_mode_enabled": "",
        "autocommit_period": "P30M",
```

```
        "retention": {
          "default": "P30Y",
          "maximum": "P30Y",
          "minimum": "P30Y"
        },
        "type": "enterprise"
      },
      "snapshot_policy": {
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "space": {
        "size": 1073741824
      }
    }
  ]
}
```

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
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

The SVM in which the container is located.

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.

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

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

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

container_volume_flexcache_relationship

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.
volume	volume	

flexcache

The FlexCache origin volume.

Name	Type	Description
dr_cache	boolean	If set to true, a DR cache is created.
origins	array[container_volume_flexcache_relationship]	

acls

The permissions that users and groups have on a CIFS share.

Name	Type	Description
permission	string	Specifies the access rights that a user or group has on the defined CIFS Share. The following values are allowed: • no_access - User does not have CIFS share access • read - User has only read access • change - User has change access • full_control - User has full_control access
type	string	Specifies the type of the user or group to add to the access control list of a CIFS share. The following values are allowed: • windows - Windows user or group • unix_user - UNIX user • unix_group - UNIX group
user_or_group	string	Specifies the user or group name to add to the access control list of a CIFS share.

consistency_group_cifs_share

CIFS share is a named access point in a volume. Before users and applications can access data on the CIFS server over SMB, a CIFS share must be created with sufficient share permission. CIFS shares are tied to the CIFS server on the SVM. When a CIFS share is created, ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

Name	Type	Description
access_based_enumeration	boolean	Specifies whether all folders inside this share are visible to a user based on that individual user's access right; prevents the display of folders or other shared resources that the user does not have access to.
acls	array[acls]	

Name	Type	Description
allow_unencrypted_access	boolean	Specifies whether or not the SMB2 clients are allowed to access the encrypted share.
change_notify	boolean	Specifies whether CIFS clients can request for change notifications for directories on this share.
comment	string	Specify the CIFS share descriptions.
continuously_available	boolean	Specifies whether or not the clients connecting to this share can open files in a persistent manner. Files opened in this way are protected from disruptive events, such as, failover and giveback. If the Vscan ONTAP feature is used, it is not supported in continuous availability (CA) shares. • Default value: 1 • Introduced in: 9.12 • x-nullable: true
dir_umask	integer	Directory mode creation mask to be viewed as an octal number.
encryption	boolean	Specifies whether SMB encryption must be used when accessing this share. Clients that do not support encryption are not able to access this share.
file_umask	integer	File mode creation mask to be viewed as an octal number.

Name	Type	Description
home_directory	boolean	Specifies whether or not the share is a home directory share, where the share and path names are dynamic. ONTAP home directory functionality automatically offer each user a dynamic share to their home directory without creating an individual SMB share for each user. The ONTAP CIFS home directory feature enable us to configure a share that maps to different directories based on the user that connects to it. Instead of creating a separate shares for each user, a single share with a home directory parameters can be created. In a home directory share, ONTAP dynamically generates the share-name and share-path by substituting %w, %u, and %d variables with the corresponding Windows user name, UNIX user name, and domain name, respectively. • Default value: 1 • Introduced in: 9.12 • readCreate: 1 • x-nullable: true
name	string	Specifies the name of the CIFS share that you want to create. If this is a home directory share then the share name includes the pattern as %w (Windows user name), %u (UNIX user name) and %d (Windows domain name) variables in any combination with this parameter to generate shares dynamically.
namespace_caching	boolean	Specifies whether or not the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.

Name	Type	Description
no_strict_security	boolean	Specifies whether or not CIFS clients can follow Unix symlinks outside the share boundaries.
offline_files	string	Offline Files The supported values are: • none - Clients are not permitted to cache files for offline access. • manual - Clients may cache files that are explicitly selected by the user for offline access. • documents - Clients may automatically cache files that are used by the user for offline access. • programs - Clients may automatically cache files that are used by the user for offline access and may use those files in an offline mode even if the share is available.
oplocks	boolean	Specifies whether opportunistic locks are enabled on this share. "Oplocks" allow clients to lock files and cache content locally, which can increase performance for file operations.
show_snapshot	boolean	Specifies whether or not the snapshots can be viewed and traversed by clients.
unix_symlink	string	Controls the access of UNIX symbolic links to CIFS clients. The supported values are: • local - Enables only local symbolic links which is within the same CIFS share. • widelink - Enables both local symlinks and widelinks. • disable - Disables local symlinks and widelinks.

Name	Type	Description
vscan_profile	string	Vscan File-Operations Profile The supported values are: • no_scan - Virus scans are never triggered for accesses to this share. • standard - Virus scans can be triggered by open, close, and rename operations. • strict - Virus scans can be triggered by open, read, close, and rename operations. • writes_only - Virus scans can be triggered only when a file that has been modified is closed.

cifs

Name	Type	Description
shares	array[consistency_group_cifs_share]	

self_link

export_clients

Name	Type	Description
match	string	Client Match Hostname, IP Address, Netgroup, or Domain. You can specify the match as a string value in any of the following formats: • As a hostname; for instance, host1 • As an IPv4 address; for instance, 10.1.12.24 • As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1 • As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24 • As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64 • As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0 • As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng • As a domain name preceded by the . character; for instance, .example.com

export_rules

Name	Type	Description
allow_device_creation	boolean	Specifies whether or not device creation is allowed.
allow_suid	boolean	Specifies whether or not SetUID bits in SETATTR Op is to be honored.
anonymous_user	string	User ID To Which Anonymous Users Are Mapped.

Name	Type	Description
chown_mode	string	Specifies who is authorized to change the ownership mode of a file.
clients	array[export_clients]	Array of client matches
index	integer	Index of the rule within the export policy.
ntfs_unix_security	string	NTFS export UNIX security options.
protocols	array[string]	
ro_rule	array[string]	Authentication flavors that the read-only access rule governs
rw_rule	array[string]	Authentication flavors that the read/write access rule governs
superuser	array[string]	Authentication flavors that the superuser security type governs

export_policy

The policy associated with volumes to export them for protocol access.

Name	Type	Description
id	integer	Identifier for the export policy.
name	string	Name of the export policy.
rules	array[export_rules]	The set of rules that govern the export policy.

junction_parent

Name	Type	Description
name	string	The name of the parent volume that contains the junction inode of this volume. The junction parent volume must belong to the same SVM that owns this volume.

Name	Type	Description
uuid	string	Unique identifier for the parent volume.

nas

The CIFS share policy and export policies for this volume.

Name	Type	Description
cifs	cifs	
export_policy	export_policy	The policy associated with volumes to export them for protocol access.
gid	integer	The UNIX group ID of the volume. Valid in POST or PATCH.
junction_parent	junction_parent	
path	string	The fully-qualified path in the owning SVM’s namespace at which the volume is mounted. The path is case insensitive and must be unique within an SVM’s namespace. Path must begin with '/' and must not end with '/'. Only one volume can be mounted at any given junction path. An empty path in POST creates an unmounted volume. An empty path in PATCH deactivates and unmounts the volume. Taking a volume offline or restricted state removes its junction path. This attribute is reported in GET only when the volume is mounted.
security_style	string	Security style associated with the volume. Valid in POST or PATCH. mixed ‐ Mixed-style security ntfs ‐ NTFS/WIndows-style security unified ‐ Unified-style security, unified UNIX, NFS and CIFS permissions unix ‐ UNIX-style security.
uid	integer	The UNIX user ID of the volume. Valid in POST or PATCH.

Name	Type	Description
unix_permissions	integer	UNIX permissions to be viewed as an octal number, consisting of 4 digits derived by adding up bits 4 (read), 2 (write), and 1 (execute). First digit selects the set user ID (4), set group ID (2), and sticky (1) attributes. Second digit selects permission for the owner of the file. Third selects permissions for other users in the same group while the fourth selects permissions for other users not in the group. Valid in POST or PATCH. For security style "mixed" or "unix", the default setting is 0755 in octal (493 in decimal) and for security style "ntfs", the default setting is 0000. In cases where only owner, group, and other permissions are given (as in 755, representing the second, third and fourth digit), the first digit is assumed to be zero.

policy

The QoS policy

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.

qos

Name	Type	Description
policy	policy	The QoS 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.

statements

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 are 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[statements]	Specifies the bucket access policy statement.

s3_bucket

The S3 bucket

Name	Type	Description
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 "-".

Name	Type	Description
nas_path	string	Specifies the NAS path that corresponds with the NAS bucket.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies are 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.

retention

Name	Type	Description
default	string	Specifies the default retention period that is applied to files while committing them to the WORM state without an associated retention period. The retention value represents a duration and must be specified in the ISO-8601 duration format. The retention period can be in years, months, days, hours, and minutes. A duration specified for years, months, and days is represented in the ISO-8601 format as "P<num>Y", "P<num>M", "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. A duration in hours and minutes is represented by "PT<num>H" and "PT<num>M" respectively. The retention string must contain only a single time element that is, either years, months, days, hours, or minutes. A duration which combines different periods is not supported, for example "P1Y10M" is not supported. Apart from the duration specified in the ISO-8601 format, the duration field also accepts the string "infinite" to set an infinite retention period and the string "unspecified" to set an unspecified retention period.</num></num></num></num></num>

Name	Type	Description
maximum	string	Specifies the maximum allowed retention period for files committed to the WORM state on the volume. The retention value represents a duration and must be specified in the ISO-8601 duration format. The retention period can be in years, months, days, hours, and minutes. A duration specified for years, months, and days is represented in the ISO-8601 format as "P<num>Y", "P<num>M", "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. A duration in hours and minutes is represented by "PT<num>H" and "PT<num>M" respectively. The retention string must contain only a single time element that is, either years, months, days, hours, or minutes. A duration which combines different periods is not supported, for example "P1Y10M" is not supported. Apart from the duration specified in the ISO-8601 format, the duration field also accepts the string "infinite" to set an infinite retention period.</num></num></num></num></num>

Name	Type	Description
minimum	string	Specifies the minimum allowed retention period for files committed to the WORM state on the volume. The retention value represents a duration and must be specified in the ISO-8601 duration format. The retention period can be in years, months, days, hours, and minutes. A duration specified for years, month,s and days is represented in the ISO-8601 format as "P<num>Y", "P<num>M", "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. A duration in hours and minutes is represented by "PT<num>H" and "PT<num>M" respectively. The retention string must contain only a single time element that is, either years, months, days, hours, or minutes. A duration which combines different periods is not supported, for example "P1Y10M" is not supported. Apart from the duration specified in the ISO-8601 format, the duration field also accepts the string "infinite" to set an infinite retention period.</num></num></num></num></num>

snaplock

Name	Type	Description
append_mode_enabled	boolean	Specifies if the volume append mode is enabled or disabled. When it is enabled, all the files created with write permissions on the volume are, by default, WORM appendable files. The user can append the data to a WORM appendable file but cannot modify the existing contents of the file nor delete the file until it expires.

Name	Type	Description
autocommit_period	string	Specifies the autocommit period for SnapLock volume. All files which are not modified for a period greater than the autocommit period of the volume are committed to the WORM state. The autocommit period value represents a duration and must be specified in the ISO-8601 duration format. The autocommit period can be in years, months, days, hours, and minutes. A period specified for years, months, and days is represented in the ISO-8601 format as "P<num>Y", "P<num>M", "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. A duration in hours and minutes is represented by "PT<num>H" and "PT<num>M" respectively. The period string must contain only a single time element that is, either years, months, days, hours, or minutes. A duration which combines different periods is not supported, for example "P1Y10M" is not supported. Apart from the duration specified in the ISO-8601 format, the autocommit field also accepts the string "none".</num></num></num></num></num>
retention	retention	
type	string	The SnapLock type of the volume. compliance ‐ A SnapLock Compliance(SLC) volume provides the highest level of WORM protection and an administrator cannot destroy a SLC volume if it contains unexpired WORM files. enterprise ‐ An administrator can delete a SnapLock Enterprise(SLE) volume. non_snaplock ‐ Indicates the volume is non-snaplock.

snapshot_policy

This is a reference to the snapshot policy.

Name	Type	Description
name	string	
uuid	string	

space

Name	Type	Description
size	integer	The total provisioned size of the container, in bytes.

volumes

Name	Type	Description
flexcache	flexcache	The FlexCache origin volume.
name	string	Volume name. The name of volume must start with an alphabetic character (a to z or A to Z) or an underscore (_). The name must be 197 or fewer characters in length for FlexGroup volumes, and 203 or fewer characters in length for all other types of volumes. Volume names must be unique within an SVM. Required on POST.
nas	nas	The CIFS share policy and export policies for this volume.
qos	qos	
s3_bucket	s3_bucket	The S3 bucket
scale_out	boolean	Denotes a Flexgroup.
snaplock	snaplock	
snapshot_locking_enabled	boolean	Specifies whether or not snapshot copy locking is enabled on the volume.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.

Name	Type	Description
space	space	

container

Name	Type	Description
svm	svm	The SVM in which the container is located.
volumes	array[volumes]	A list of NAS volumes to provision.

job_link

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

Copyright information

Trademark information