



Manage CIFS shares

ONTAP 9.11.1 REST API reference

NetApp
May 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9111/ontap/protocols_cifs_shares_endpoint_overview.html on May 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Manage CIFS shares 1
 - Protocols CIFS shares endpoint overview 1
 - Retrieve CIFS shares 9
 - Create a CIFS share 22
 - Delete a CIFS share 38
 - Retrieve a CIFS share 40
 - Update a CIFS share 50

Manage CIFS shares

Protocols CIFS shares endpoint overview

Overview

Before any users or applications can access data on the CIFS server over SMB, a CIFS share must be created with sufficient share permissions. CIFS share is a named access point in a volume which is tied to the CIFS server on the SVM. Before creating a CIFS share make sure that the path is valid within the scope of the SVM and that it is reachable.

Permissions can be assigned to this newly created share by specifying the 'acls' field. When a CIFS share is created, ONTAP creates a default ACL for this share with 'Full-Control' permissions for an 'Everyone' user.

Examples

Creating a CIFS share

To create a CIFS share for a CIFS server, use the following API. Note the *return_records=true* query parameter used to obtain the newly created entry in the response.

```
# The API:
POST /api/protocols/cifs/shares

# The call:
curl -X POST "https://<mgmt-
ip>/api/protocols/cifs/shares?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{
  \"access_based_enumeration\": false, \"acls\": [ { \"permission\":
  \"no_access\", \"type\": \"unix_user\", \"user_or_group\": \"root\" } ],
  \"change_notify\": true, \"comment\": \"HR Department Share\",
  \"encryption\": false, \"home_directory\": false, \"name\": \"TEST\",
  \"oplocks\": true, \"no_strict_security\": true, \"path\": \"/\", \"svm\":
  { \"name\": \"vs1\", \"uuid\": \"6d8e8870-8753-11eb-8d86-0050568ea61a\" },
  \"unix_symlink\": \"local\", \"show_snapshot\": \"true\",
  \"continuously_available\": \"false\", \"namespace_caching\": \"true\",
  \"allow_unencrypted_access\": \"false\", \"file_umask\": \"025\",
  \"dir_umask\": \"026\", \"offline_files\": \"documents\",
  \"vscan_profile\": \"standard\", \"force_group_for_create\": \"root\"}"

# The response:
{
  "num_records": 1,
  "records": [
    {
```

```

"svm": {
  "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
  "name": "vs1"
},
"name": "TEST",
"path": "/",
"comment": "HR Department Share",
"home_directory": false,
"oplocks": true,
"access_based_enumeration": false,
"change_notify": true,
"encryption": false,
"unix_symlink": "local",
"acls": [
  {
    "user_or_group": "root",
    "type": "unix_user",
    "permission": "no_access",
    "winsid_unixId": "0"
  }
],
"no_strict_security": true,
"show_snapshot": true,
"continuously_available": false,
"namespace_caching": true,
"allow_unencrypted_access": false,
"file_umask": 25,
"dir_umask": 26,
"offline_files": "documents",
"vscan_profile": "standard",
"force_group_for_create": "root"
}
]
}

```

Retrieving CIFS Shares for all SVMs in the cluster

```

# The API:
GET /api/protocols/cifs/shares

# The call:
curl -X GET "https://<mgmt-

```

```

ip>/api/protocols/cifs/shares?fields=*&return_records=true&return_timeout=
15" -H "accept application/hal+json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
        "name": "vs1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/6d8e8870-8753-11eb-8d86-0050568ea61a"
          }
        }
      },
      "name": "c$",
      "path": "/",
      "home_directory": false,
      "oplocks": true,
      "access_based_enumeration": false,
      "change_notify": true,
      "encryption": false,
      "unix_symlink": "local",
      "acls": [
        {
          "user_or_group": "BUILTIN\\Administrators",
          "type": "windows",
          "permission": "full_control"
        }
      ],
      "volume": {
        "name": "vol1",
        "uuid": "6f4fb33a-8753-11eb-8d86-0050568ea61a"
      },
      "show_snapshot": false,
      "cache_attribute": false,
      "continuously_available": false,
      "namespace_caching": false,
      "allow_unencrypted_access": true,
      "vscan_profile": "standard",
      "_links": {
        "self": {
          "href": "/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/c%24"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "svm": {
      "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
      "name": "vs1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/6d8e8870-8753-11eb-8d86-0050568ea61a"
        }
      }
    },
    "name": "ipc$",
    "path": "/",
    "home_directory": false,
    "oplocks": false,
    "access_based_enumeration": false,
    "change_notify": false,
    "encryption": false,
    "volume": {
      "name": "vol1",
      "uuid": "6f4fb33a-8753-11eb-8d86-0050568ea61a"
    },
    "show_snapshot": false,
    "cache_attribute": false,
    "continuously_available": false,
    "namespace_caching": false,
    "allow_unencrypted_access": false,
    "vscan_profile": "standard",
    "_links": {
      "self": {
        "href": "/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/ipc%24"
      }
    }
  },
  {
    "svm": {
      "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
      "name": "vs1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/6d8e8870-8753-11eb-8d86-0050568ea61a"
        }
      }
    }
  },

```

```

"name": "TEST",
"path": "/",
"comment": "HR Department Share",
"home_directory": false,
"oplocks": true,
"access_based_enumeration": false,
"change_notify": true,
"encryption": false,
"unix_symlink": "local",
"acls": [
  {
    "user_or_group": "Everyone",
    "type": "windows",
    "permission": "full_control"
  },
  {
    "user_or_group": "root",
    "type": "unix_user",
    "permission": "no_access"
  }
],
"volume": {
  "name": "vol1",
  "uuid": "6f4fb33a-8753-11eb-8d86-0050568ea61a"
},
"no_strict_security": true,
"show_snapshot": true,
"cache_attribute": true,
"continuously_available": false,
"namespace_caching": true,
"allow_unencrypted_access": true,
"file_umask": 25,
"dir_umask": 26,
"offline_files": "documents",
"vscan_profile": "standard",
"force_group_for_create": "root",
"_links": {
  "self": {
    "href": "/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/TEST"
  }
}
},
"num_records": 3,
"_links": {

```

```
"self": {
  "href":
"/api/protocols/cifs/shares?fields=*&return_records=true&return_timeout=15
"
}
}
}
```

Retrieving all CIFS Shares for all SVMs in the cluster for which the acls are configured for a "root" user

```
# The API:
GET /api/protocols/cifs/shares

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/cifs/shares?acls.user_or_group=root&fields=*&return_reco
rds=true&return_timeout=15" -H "accept: application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
      "name": "vs1"
    },
    "name": "TEST",
    "path": "/",
    "comment": "HR Department Share",
    "home_directory": false,
    "oplocks": true,
    "access_based_enumeration": false,
    "change_notify": true,
    "encryption": false,
    "unix_symlink": "local",
    "acls": [
      {
        "user_or_group": "Everyone",
        "type": "windows",
        "permission": "full_control"
      },
      {
```



```

        "user_or_group": "root",
        "type": "unix_user",
        "permission": "no_access"
    }
],
"volume": {
    "name": "vol1",
    "uuid": "6f4fb33a-8753-11eb-8d86-0050568ea61a"
},
"no_strict_security": true,
"show_snapshot": true,
"cache_attribute": true,
"continuously_available": false,
"namespace_caching": true,
"allow_unencrypted_access": true,
"file_umask": 25,
"dir_umask": 26,
"offline_files": "documents",
"vscan_profile": "standard",
"force_group_for_create": "root"
}
],
"num_records": 1
}

```

Retrieving a specific CIFS share configuration for an SVM

The configuration being returned is identified by the UUID of its SVM and the name of the share.

```

# The API:
GET /api/protocols/cifs/shares/{svm.uuid}/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/TEST" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "6d8e8870-8753-11eb-8d86-0050568ea61a",
    "name": "vs1"
  },
  "name": "TEST",
  "path": "/",
  "comment": "HR Department Share",
  "home_directory": false,

```

```

"oplocks": true,
"access_based_enumeration": false,
"change_notify": true,
"encryption": false,
"unix_symlink": "local",
"acls": [
  {
    "user_or_group": "Everyone",
    "type": "windows",
    "permission": "full_control"
  },
  {
    "user_or_group": "root",
    "type": "unix_user",
    "permission": "no_access"
  }
],
"volume": {
  "name": "vol1",
  "uuid": "6f4fb33a-8753-11eb-8d86-0050568ea61a"
},
"no_strict_security": true,
"show_snapshot": true,
"cache_attribute": true,
"continuously_available": false,
"namespace_caching": true,
"allow_unencrypted_access": true,
"file_umask": 25,
"dir_umask": 26,
"offline_files": "documents",
"vscan_profile": "standard",
"force_group_for_create": "root"
}

```

Updating a specific CIFS share for an SVM

The CIFS share being modified is identified by the UUID of its SVM and the CIFS share name. The CIFS share ACLs cannot be modified with this API.

```
# The API:
PATCH /api/protocols/cifs/shares/{svm.uuid}/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/TEST" -H "accept: application/json" -H "Content-Type: application/json" -d '{"access_based_enumeration": true, "change_notify": true, "comment": "HR Department Share", "encryption": false, "oplocks": true, "no_strict_security": true, "path": "/", "unix_symlink": "widelink", "show_snapshot": "false", "continuously_available": "true", "namespace_caching": "false", "allow_unencrypted_access": "true", "file_umask": "022", "dir_umask": "022", "offline_files": "programs", "vscan_profile": "no_scan", "force_group_for_create": "root"}'
```

Removing a specific CIFS share for an SVM

The CIFS share being removed is identified by the UUID of its SVM and the CIFS share name.

```
# The API:
DELETE /api/protocols/cifs/shares/{svm.uuid}/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/cifs/shares/6d8e8870-8753-11eb-8d86-0050568ea61a/test" -H "accept: application/json"
```

Retrieve CIFS shares

GET /protocols/cifs/shares

Introduced In: 9.6

Retrieves CIFS shares.

Related ONTAP commands

- `vserver cifs share show`
- `vserver cifs share properties show`

Learn more

- [DOC /protocols/cifs/shares](#)

Parameters

| Name | Type | In | Required | Description |
|--------------------------|---------|-------|----------|--|
| offline_files | string | query | False | Filter by offline_files <ul style="list-style-type: none">Introduced in: 9.10 |
| force_group_for_create | string | query | False | Filter by force_group_for_create <ul style="list-style-type: none">Introduced in: 9.10 |
| allow_unencrypted_access | boolean | query | False | Filter by allow_unencrypted_access <ul style="list-style-type: none">Introduced in: 9.11 |
| namespace_caching | boolean | query | False | Filter by namespace_caching <ul style="list-style-type: none">Introduced in: 9.10 |
| file_umask | integer | query | False | Filter by file_umask <ul style="list-style-type: none">Introduced in: 9.10 |
| vscan_profile | string | query | False | Filter by vscan_profile <ul style="list-style-type: none">Introduced in: 9.10 |
| name | string | query | False | Filter by name <ul style="list-style-type: none">maxLength: 80minLength: 1 |
| comment | string | query | False | Filter by comment <ul style="list-style-type: none">maxLength: 256minLength: 1 |

| Name | Type | In | Required | Description |
|--------------------------|---------|-------|----------|---|
| path | string | query | False | Filter by path <ul style="list-style-type: none"> • maxLength: 256 • minLength: 1 |
| oplocks | boolean | query | False | Filter by oplocks |
| dir_umask | integer | query | False | Filter by dir_umask <ul style="list-style-type: none"> • Introduced in: 9.10 |
| acls.permission | string | query | False | Filter by acls.permission |
| acls.type | string | query | False | Filter by acls.type |
| acls.user_or_group | string | query | False | Filter by acls.user_or_group |
| svm.uuid | string | query | False | Filter by svm.uuid |
| svm.name | string | query | False | Filter by svm.name |
| home_directory | boolean | query | False | Filter by home_directory |
| no_strict_security | boolean | query | False | Filter by no_strict_security <ul style="list-style-type: none"> • Introduced in: 9.9 |
| access_based_enumeration | boolean | query | False | Filter by access_based_enumeration |
| show_snapshot | boolean | query | False | Filter by show_snapshot <ul style="list-style-type: none"> • Introduced in: 9.10 |
| encryption | boolean | query | False | Filter by encryption |

| Name | Type | In | Required | Description |
|------------------------|---------------|-------|----------|---|
| continuously_available | boolean | query | False | Filter by continuously_available • Introduced in: 9.10 |
| volume.name | string | query | False | Filter by volume.name |
| volume.uuid | string | query | False | Filter by volume.uuid |
| unix_symlink | string | query | False | Filter by unix_symlink |
| change_notify | boolean | query | False | Filter by change_notify |
| fields | array[string] | query | False | Specify the fields to return. |
| max_records | integer | query | False | Limit the number of records returned. |
| return_records | boolean | query | False | The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1 |

| Name | Type | In | Required | Description |
|----------------|---------------|-------|----------|--|
| return_timeout | integer | query | False | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0 |
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |

Response

Status: 200, Ok

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

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "acls": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "permission": "no_access",
      "type": "windows",
      "user_or_group": "ENGDOMAIN\\ad_user"
    },
    "comment": "HR Department Share",
    "dir_umask": 22,
    "file_umask": 22,
    "name": "HR_SHARE",
    "offline_files": "none",
    "path": "/volume_1/eng_vol/",
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "unix_symlink": "local",
    "volume": {
      "_links": {
        "self": {
```



```

        "href": "/api/resourcelink"
      },
    ],
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  },
  "vscan_profile": "no_scan"
}

```

Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| next | href | |
| self | href | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

acls

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

| Name | Type | Description |
|------------|------------------------|--|
| _links | _links | |
| permission | string | <p>Specifies the access rights that a user or group has on the defined CIFS Share. The following values are allowed:</p> <ul style="list-style-type: none">• 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 |

| Name | Type | Description |
|---------------|--------|--|
| 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: <ul style="list-style-type: none"> • 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. |

svm

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

volume

| Name | Type | Description |
|------------------------|------------------------|---|
| _links | _links | |
| name | string | The name of the volume. |
| 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. <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 |

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 |
|--------------------------|------------------------------|--|
| _links | _links | |
| access_based_enumeration | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| acls | array [acls] | |
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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 |
|------------------------|---------|--|
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: • Introduced in: 9.6 • readCreate: 1 |

| Name | Type | Description |
|--------------------|---------|--|
| 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. |
| no_strict_security | boolean | Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries. |
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | Specify 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. |

| Name | Type | Description |
|---------------|------------------------|---|
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |

| Name | Type | Description |
|---------------|--------|---|
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> • 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. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Create a CIFS share

POST /protocols/cifs/shares

Introduced In: 9.6

Creates a CIFS share.

Required properties

- `svm.uuid` or `svm.name` - Existing SVM in which to create the CIFS share.
- `name` - Name of the CIFS share.
- `path` - Path in the owning SVM namespace that is shared through this share.

Recommended optional properties

- `comment` - Optionally choose to add a text comment of up to 256 characters about the CIFS share.
- `acls` - Optionally choose to add share permissions that users and groups have on the CIFS share.

Default property values

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

- `home_directory` - *false*
- `oplocks` - *true*
- `access_based_enumeration` - *false*
- `change_notify` - *true*
- `encryption` - *false*
- `unix_symlink` - *local*

Related ONTAP commands

- `vserver cifs share create`
- `vserver cifs share properties add`
- `vserver cifs share access-control create`

Learn more

- [DOC /protocols/cifs/shares](#)

Parameters

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

Request Body

| Name | Type | Description |
|--------------------------|------------------------------|--|
| _links | _links | |
| access_based_enumeration | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| acls | array [acls] | |
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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 |
|------------------------|---------|--|
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Introduced in: 9.6 • readCreate: 1 |
| 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. |

| Name | Type | Description |
|--------------------|---------|--|
| 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. |
| no_strict_security | boolean | Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries. |
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | <p>Specify 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.</p> |

| Name | Type | Description |
|---------------|------------------------|---|
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |

| Name | Type | Description |
|---------------|--------|---|
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> • 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. |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "acls": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "permission": "no_access",
    "type": "windows",
    "user_or_group": "ENGDOMAIN\\ad_user"
  },
  "comment": "HR Department Share",
  "dir_umask": 22,
  "file_umask": 22,
  "name": "HR_SHARE",
  "offline_files": "none",
  "path": "/volume_1/eng_vol/",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "unix_symlink": "local",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  },
  "vscan_profile": "no_scan"
}
```

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 655628 | CIFS Share Creation with property 'SMB_ENCRYPTION' failed because the CIFS server does not support SMB3.0 |
| 655551 | CIFS Share Creation failed because the specified path does not exist |
| 655577 | The CIFS share name cannot be more than 80 characters long |
| 655399 | Failed to create CIFS share. The CIFS server does not exist for specified SVM |
| 656422 | Failed to create the home directory share because the directory shares must specify a path relative to one or more home directory search paths |
| 656423 | Failed to create CIFS share. The Shares must define an absolute share path |
| 656424 | Failed to create CIFS the administrator share 'c\$' because you are not permitted to created any admin shares |
| 655625 | Failed to create CIFS share. The Shares path is not a valid file-type for CIFS share |
| 656426 | CIFS Share Creation failed because the share name is invalid |
| 655655 | no-strict-security should be set to true only if unix_symlink is configured as "local" or "widelink" |
| 655394 | Failed to create CIFS share because share cannot be made continuously available unless running SMB3 or later. |
| 4849678 | Failed to create CIFS share because the specified UNIX group does not exist |

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

acls

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

| Name | Type | Description |
|---------------|------------------------|--|
| _links | _links | |
| permission | string | <p>Specifies the access rights that a user or group has on the defined CIFS Share. The following values are allowed:</p> <ul style="list-style-type: none">• 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 | <p>Specifies the type of the user or group to add to the access control list of a CIFS share. The following values are allowed:</p> <ul style="list-style-type: none">• windows - Windows user or group• unix_user - UNIX user• unix_group - UNIX group |
| user_or_group | string | <p>Specifies the user or group name to add to the access control list of a CIFS share.</p> |

svm

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

volume

| Name | Type | Description |
|--------|------------------------|--|
| _links | _links | |
| name | string | The name of the volume. |
| uuid | string | <p>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.</p> <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 |

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 |
|--------------------------|------------------------------|--|
| _links | _links | |
| access_based_enumeration | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| acls | array [acls] | |
| allow_unencrypted_access | boolean | Specifies whether or not the SMB2 clients are allowed to access the encrypted share. |

| Name | Type | Description |
|------------------------|---------|--|
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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. |
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |

| Name | Type | Description |
|-------------------|---------|--|
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Introduced in: 9.6 • readCreate: 1 |
| name | string | <p>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.</p> |
| namespace_caching | boolean | <p>Specifies whether or not the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.</p> |

| Name | Type | Description |
|--------------------|---------|--|
| no_strict_security | boolean | Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries. |
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | Specify 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. |

| Name | Type | Description |
|---------------|------------------------|---|
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |

| Name | Type | Description |
|---------------|--------|---|
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> 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. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Delete a CIFS share

DELETE /protocols/cifs/shares/{svm.uuid}/{name}

Introduced In: 9.6

Deletes a CIFS share.

Related ONTAP commands

- `vserver cifs share delete`

Learn more

- [DOC /protocols/cifs/shares](#)

Parameters

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

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|---|
| 655393 | Standard admin shares cannot be removed |

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Retrieve a CIFS share

GET /protocols/cifs/shares/{svm.uuid}/{name}

Introduced In: 9.6

Retrieves a CIFS share.

Related ONTAP commands

- `vserver cifs share show`
- `vserver cifs share properties show`

Learn more

- [DOC /protocols/cifs/shares](#)

Parameters

| Name | Type | In | Required | Description |
|----------|---------------|-------|----------|---|
| name | string | path | True | Share Name |
| 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 |
|---------------------------------------|------------------------------|--|
| <code>_links</code> | _links | |
| <code>access_based_enumeration</code> | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| <code>acls</code> | array [acls] | |
| <code>allow_unencrypted_access</code> | boolean | Specifies whether or not the SMB2 clients are allowed to access the encrypted share. |
| <code>change_notify</code> | boolean | Specifies whether CIFS clients can request for change notifications for directories on this share. |

| Name | Type | Description |
|------------------------|---------|--|
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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. |
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |

| Name | Type | Description |
|--------------------|---------|--|
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Introduced in: 9.6 • readCreate: 1 |
| name | string | <p>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.</p> |
| namespace_caching | boolean | <p>Specifies whether or not the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.</p> |
| no_strict_security | boolean | <p>Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries.</p> |

| Name | Type | Description |
|---------------|---------|---|
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | <p>Specify 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.</p> |
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |

| Name | Type | Description |
|---------------|------------------------|---|
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> • 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. |

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "acls": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "permission": "no_access",
    "type": "windows",
    "user_or_group": "ENGDOMAIN\\ad_user"
  },
  "comment": "HR Department Share",
  "dir_umask": 22,
  "file_umask": 22,
  "name": "HR_SHARE",
  "offline_files": "none",
  "path": "/volume_1/eng_vol/",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "unix_symlink": "local",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  },
  "vscan_profile": "no_scan"
}
```


Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

acls

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

| Name | Type | Description |
|---------------|------------------------|--|
| _links | _links | |
| permission | string | <p>Specifies the access rights that a user or group has on the defined CIFS Share. The following values are allowed:</p> <ul style="list-style-type: none">• 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 | <p>Specifies the type of the user or group to add to the access control list of a CIFS share. The following values are allowed:</p> <ul style="list-style-type: none">• windows - Windows user or group• unix_user - UNIX user• unix_group - UNIX group |
| user_or_group | string | <p>Specifies the user or group name to add to the access control list of a CIFS share.</p> |

svm

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

volume

| Name | Type | Description |
|--------|------------------------|--|
| _links | _links | |
| name | string | The name of the volume. |
| uuid | string | <p>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.</p> <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Update a CIFS share

PATCH /protocols/cifs/shares/{svm.uuid}/{name}

Introduced In: 9.6

Updates a CIFS share.

Related ONTAP commands

- `vserver cifs share modify`
- `vserver cifs share properties add`
- `vserver cifs share properties remove`

Learn more

- [DOC /protocols/cifs/shares](#)

Parameters

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

Request Body

| Name | Type | Description |
|--------------------------|------------------------------|--|
| _links | _links | |
| access_based_enumeration | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| acls | array [acls] | |
| allow_unencrypted_access | boolean | Specifies whether or not the SMB2 clients are allowed to access the encrypted share. |

| Name | Type | Description |
|------------------------|---------|--|
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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. |
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |

| Name | Type | Description |
|--------------------|---------|--|
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Introduced in: 9.6 • readCreate: 1 |
| name | string | <p>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.</p> |
| namespace_caching | boolean | <p>Specifies whether or not the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.</p> |
| no_strict_security | boolean | <p>Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries.</p> |

| Name | Type | Description |
|---------------|---------|---|
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | <p>Specify 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.</p> |
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |

| Name | Type | Description |
|---------------|------------------------|---|
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> • 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. |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "acls": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "permission": "no_access",
    "type": "windows",
    "user_or_group": "ENGDOMAIN\\ad_user"
  },
  "comment": "HR Department Share",
  "dir_umask": 22,
  "file_umask": 22,
  "name": "HR_SHARE",
  "offline_files": "none",
  "path": "/volume_1/eng_vol/",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "unix_symlink": "local",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  },
  "vscan_profile": "no_scan"
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 655628 | 'SMB_ENCRYPTION' property cannot be set on CIFS share because the CIFS server does not support SMB3.0 |
| 655551 | CIFS Share modification failed because the specified path does not exist |
| 655620 | Cannot set symlink properties for admin shares |
| 656420 | Cannot modify the standard share ipc\$ |
| 656421 | Cannot modify the standard share admin\$ |
| 656422 | Failed to modify the home directory share because the directory shares must specify a path relative to one or more home directory search paths |
| 656423 | Failed to modify CIFS share. The Shares must define an absolute share path |
| 656425 | Failed to modify the CIFS share because the path for an administrative share cannot be modified |
| 655395 | Failed to modify the CIFS share because share cannot be made continuously available unless running SMB3 or later. |
| 4849678 | Failed to modify the CIFS share because the specified UNIX group does not exist |

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

acls

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

| Name | Type | Description |
|---------------|------------------------|--|
| _links | _links | |
| permission | string | <p>Specifies the access rights that a user or group has on the defined CIFS Share. The following values are allowed:</p> <ul style="list-style-type: none">• 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 | <p>Specifies the type of the user or group to add to the access control list of a CIFS share. The following values are allowed:</p> <ul style="list-style-type: none">• windows - Windows user or group• unix_user - UNIX user• unix_group - UNIX group |
| user_or_group | string | <p>Specifies the user or group name to add to the access control list of a CIFS share.</p> |

svm

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

volume

| Name | Type | Description |
|--------|------------------------|--|
| _links | _links | |
| name | string | The name of the volume. |
| uuid | string | <p>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.</p> <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 |

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 |
|--------------------------|------------------------------|--|
| _links | _links | |
| access_based_enumeration | boolean | If enabled, all folders inside this share are visible to a user based on that individual user access right; prevents the display of folders or other shared resources that the user does not have access to. |
| acls | array [acls] | |
| allow_unencrypted_access | boolean | Specifies whether or not the SMB2 clients are allowed to access the encrypted share. |

| Name | Type | Description |
|------------------------|---------|--|
| 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. |
| dir_umask | integer | Directory Mode Creation Mask to be viewed as an octal number. |
| encryption | boolean | Specifies that 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. |
| force_group_for_create | string | Specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. |

| Name | Type | Description |
|-------------------|---------|--|
| home_directory | boolean | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Introduced in: 9.6 • readCreate: 1 |
| name | string | <p>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.</p> |
| namespace_caching | boolean | <p>Specifies whether or not the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.</p> |

| Name | Type | Description |
|--------------------|---------|--|
| no_strict_security | boolean | Specifies whether or not CIFS clients can follow a unix symlinks outside the share boundaries. |
| offline_files | string | <p>Offline Files The supported values are:</p> <ul style="list-style-type: none"> • 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 | Specify 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. |

| Name | Type | Description |
|---------------|------------------------|---|
| path | string | <p>The fully-qualified pathname in the owning SVM namespace that is shared through this share. If this is a home directory share then the path should be dynamic by specifying the pattern %w (Windows user name), %u (UNIX user name), or %d (domain name) variables in any combination. ONTAP generates the path dynamically for the connected user and this path is appended to each search path to find the full Home Directory path.</p> <ul style="list-style-type: none"> • example: /volume_1/eng_vol/ • maxLength: 256 • minLength: 1 • Introduced in: 9.6 |
| show_snapshot | boolean | Specifies whether or not the Snapshot copies can be viewed and traversed by clients. |
| svm | svm | |
| unix_symlink | string | <p>Controls the access of UNIX symbolic links to CIFS clients. The supported values are:</p> <ul style="list-style-type: none"> • 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. |
| volume | volume | |

| Name | Type | Description |
|---------------|--------|---|
| vscan_profile | string | <p>Vscan File-Operations Profile The supported values are:</p> <ul style="list-style-type: none"> • 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. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Copyright information

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

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

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

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

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

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

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

Trademark information

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