



Compuverde  
**REST API Management**

Version 1.7.1.1  
November 19, 2018



# Introduction

This document describes the Compuverde Management REST API, the types of operations it supports as well as how authentication and authorization are handled.

Copyright 2018 Compuverde. All rights reserved.

The information in this paper is provided "as is". It has been thoroughly checked for errors and believed to be accurate at the time it was written. Compuverde makes no warranties of any kind with respect to the content of this paper. It is subject to change without notice for clarification or product development and improvements.

All trademarks referred to in this document are the property of their respective owners.

# Contents

<b>Overview.....</b>	<b>6</b>
Getting started .....	6
Authentication.....	6
Access control.....	6
Current Working Directory .....	8
<b>File system Management.....</b>	<b>9</b>
Directories and Files .....	9
The Inode object.....	9
Create Directory .....	10
Modify Directory.....	11
Delete Directory .....	12
Head Inode.....	12
Get Inode / Statistics.....	13
Get Path Info.....	14
List Directories and Files .....	15
<b>Policy Management.....</b>	<b>16</b>
File Policies.....	16
The File Policy object.....	16
Create File Policy .....	18
Modify File Policy.....	19
Delete File Policy.....	20
Get File Policy.....	20
List File Policies .....	21
Quota Policies.....	23
The Quota Policy object.....	23
Create Quota Policy .....	23
Modify Quota Policy.....	24
Delete Quota Policy.....	24
Get Quota Policy.....	25
List Quota Policies .....	25
Snapshot Policies .....	26
The Snapshot Schedule object .....	26
The Snapshot Policy object .....	27
Create Snapshot Policy.....	27
Modify Snapshot Policy .....	28
Delete Snapshot Policy .....	29
Get Snapshot Policy .....	29
List Snapshot Policies .....	30
Antivirus Policies .....	31
The Antivirus Policy object .....	31
Create Antivirus Policy.....	33
Modify Antivirus Policy .....	34
Delete Antivirus Policy .....	35
Get Antivirus Policy .....	36
List Antivirus Policies .....	37
<b>Share Management .....</b>	<b>38</b>
Shares.....	38
The Share object.....	38
Create Share .....	41
Modify Share.....	42

Delete Share .....	43
Get Share.....	43
List Shares.....	44
<b>ISCSI Management.....</b>	<b>46</b>
iSCSI Targets .....	46
The Target object .....	46
Create Target .....	47
Modify Target.....	47
Delete Target .....	48
Get Target.....	48
List Targets.....	49
iSCSI LUNs.....	50
The LUN object .....	50
Create LUN.....	50
Modify LUN .....	51
Resize LUN .....	52
Delete LUN .....	52
iSCSI Initiator Groups .....	53
The iSCSI Initiator Group Object.....	53
Create Initiator Group .....	53
Modify Initiator Group.....	54
Delete Initiator Group.....	54
Get Initiator Group.....	55
List Initiator Groups .....	55
<b>User &amp; Group Management.....</b>	<b>56</b>
Users.....	56
The User object.....	56
Create User .....	58
Modify User.....	59
Delete User .....	59
Get User.....	60
List Users.....	61
Groups.....	62
The Group object.....	62
Create Group .....	63
Modify Group.....	63
Delete Group .....	64
Get Group.....	65
List Groups.....	66
<b>Actions .....</b>	<b>67</b>
Take Snapshot.....	67
<b>Reports .....</b>	<b>68</b>
The Report .....	68
System reports .....	68
Performance System report .....	68
Audit System report.....	70
Filesystem reports .....	71
Audit Filesystem report .....	71
DiskUsage Filesystem report .....	72
<b>Appendix .....</b>	<b>76</b>
Common Request Headers .....	76
Errors.....	76
File encodings.....	78
Tiers .....	78



## Overview

The Management REST API makes it possible to programmatically manage a Compuverde file system. The API supports administration of file shares, users, groups, iSCSI targets and LUNs, and policies; it also supports manual snapshots. Requests are executed in the context of a single domain / file system.

## Getting started

The storage cluster must have at least one file system configured. Before the REST API can be used, you will need to do the following in the Management tool (<domain> is the name of the domain / file system you want to configure):

1. Go to the **cluster > File System tab > <domain>** and enable **REST API**.
2. Go to the **cluster > File System tab > <domain> > Users** and create a user.
3. Go to a **node > Config tab > Gateway** and enable **REST API** (you will find this under *protocols*). Do this for any node that is going to be used for API communication.

Once the Web management service has been enabled and a user has been created, you are ready to start using the REST API. API requests are sent by using the HTTP protocol on port 81. Note that requests should be sent to a public IP address of the file system, or a DNS name that resolves to a public IP address. The user must also be defined in the same file system.

Example with Curl on a Linux machine (replace <username>, <password> and <node> with your own values):

```
$ CV_AUTH="$(echo -n <username>:<password> | base64)"
$ curl --head --header "Authorization: Basic $CV_AUTH" http://<node>:81/api/v1
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 09:52:42 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: ce1efac3-20ea-4a36-93f1-f0941ee2a650
```

In this example, a simple HEAD request is sent to the root URI. This is useful for checking that you are able to reach the REST API and that the user was successfully authenticated. No special permissions are needed for this request.

## Authentication

Compuverde uses HTTP Basic authentication. To authenticate as a user, you must first generate a base64 encoding of the string <username>:<password> (replace <username> and <password> with one of your users). Note that ':' must be included in the string. Once you have the base64 encoded string, you set the HTTP Authorization header in the following way:

```
Authorization: Basic <base64_encoded_string>
```

## Access control

There are two types of permissions to control access: management permissions on users and groups, and permissions on directories and files. User and group permissions determine the operations a user is allowed to perform – they are always checked before directory and file permissions. Directory and file permissions, or Access Control List (ACL), determine the operations a user is allowed to perform on a particular file system object.

### User and group permissions

The following screenshot shows the user and group permissions. They can be found in the Management Tool: cluster > File System tab > <domain> > Users/Groups > <User/Group name>.

- Management permissions
- Create/modify/delete directories and shares
  - Get/list directories and shares
  - Create/modify/delete snapshot, file, quota and antivirus policies
  - Get/list snapshot, file, quota and antivirus policies
  - Take manual snapshot
  - Create/modify/delete users and groups
  - Get/list users and groups
  - Create/modify/delete iSCSI targets and LUNs
  - Get/list iSCSI targets and LUNs
  - Get System reports
  - Get Filesystem reports

A user's effective management permissions is a combination of its own permissions and the permissions of all the groups it's a member of. If a user does not have the correct management permissions, then it will be denied access.

### ACL permissions

ACL is checked for all requests that operate on the file system tree. I.e., iSCSI, user and group operations are only verified using the user's management permissions. For all other operations, the ACL is checked before granting access. ACL can be modified using any of the supported protocols, or by specifying a new mode with the Modify Directory operation.

The following table lists the ACL permissions required by the operations. The Linux Mode column shows what the permissions correspond to in Linux. The Parent column means that the check is performed using the parent directory's ACL.

<i>Operation</i>	<i>ACL Permissions</i>	<i>Linux Mode</i>	<i>Parent</i>
<b>Create Directory</b>	<ul style="list-style-type: none"> <li>• Add subdirectory</li> </ul>	2 (w)	Yes
<b>Modify Directory</b>	<ul style="list-style-type: none"> <li>• Only owner is able to change mode</li> <li>• Read extended attributes on source parent directory</li> <li>• Add subdirectory on target parent directory</li> </ul> <p>Source parent directory and target parent directory are checked when renaming the directory.</p>	4 (r) on source and 2 (w) on target	-
<b>Delete Directory</b>	<ul style="list-style-type: none"> <li>• Delete subdirectory</li> </ul>	2 (w)	Yes
<b>Head Inode</b>	<ul style="list-style-type: none"> <li>• Read extended attributes</li> </ul>	2 (r)	Yes
<b>Get Inode</b>	<ul style="list-style-type: none"> <li>• Read extended attributes</li> </ul>	2 (r)	Yes
<b>List Directories and Files</b>	<ul style="list-style-type: none"> <li>• List directory</li> <li>• Read extended attributes</li> </ul>	2 (r)	No
<b>Create Policy</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No
<b>Modify Policy</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No
<b>Delete Policy</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No
<b>Get Policy</b>	<ul style="list-style-type: none"> <li>• Read extended attributes</li> </ul>	4 (r)	No
<b>List Policies</b>	<ul style="list-style-type: none"> <li>• Read extended attributes on file system root</li> </ul>	4 (r)	-
<b>Create Share</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No
<b>Modify Share</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No
<b>Delete Share</b>	<ul style="list-style-type: none"> <li>• Write extended attributes</li> </ul>	2 (w)	No

<b>Get Share</b>	<ul style="list-style-type: none"><li>• Read extended attributes</li></ul>	2 (r)	No
<b>List Shares</b>	<ul style="list-style-type: none"><li>• Read extended attributes on file system root</li></ul>	2 (r)	-
<b>Take Snapshot</b>	<ul style="list-style-type: none"><li>• Write extended attributes</li></ul>	2 (w)	No
<b>Get System reports</b>	-	-	-
<b>Get Filesystem reports</b>	-	-	-



**Note:** Administrator, and members of the Administrators group, are exempted from the ACL check.

## Current Working Directory

Every operation that takes a path as an argument, either in the path part of the URI, or in the request body, is executed relative to a current working directory (cwd). You specify a cwd by using a directory's unique ID in the x-cv-cwd-id header. The x-cv-cwd-id header is optional and the request is executed relative to the file system root if it's omitted. You can retrieve the unique ID of a directory by using the Head Inode operation or the Get Inode operation. The ID is also included in the result for an entry in the List Directories and Files operation.

Note that when the path is part of the request body, it's relative to the cwd only if it doesn't begin with a '/'. If it begins with a '/', the path is relative to the file system root. Paths that are included in the URI are always relative to the cwd.

## File system Management

Operations for file system management. Create, rename and delete a directory; get an inode, and list files and directories.

### Directories and Files

#### The Inode object

```
{
  "id": "8e82ba51-0000-0000-1956-56df2b153a43",
  "type": "directory",
  "name": "mydirectory",
  "createDate": "2016-10-14 12:44:21",
  "modifyDate": "2016-10-14 12:44:21",
  "accessDate": "2016-10-14 12:44:21",
  "metadataDate": "2016-10-14 12:44:21",
  "scanDate": "2016-10-14 12:44:21",
  "backupDate": "2000-01-01 00:00:00",
  "snapshotDate": "2016-10-14 12:44:21",
  "mode": "777",
  "size": 0,
  "usedSize": 0,
  "diskSize": 0,
  "directoryCount": 0,
  "fileCount": 0,
  "readBytes": 0,
  "writeBytes": 0,
  "readOperations": 0,
  "writeOperations": 0
}
```

#### Attribute Definitions

Name	Type	Description
<b>id</b>	String	The unique ID of the file / directory.
<b>type</b>	String	The type of inode. Valid values: directory, file, symlink, link
<b>name</b>	String	The name of the file / directory.
<b>createDate</b>	String	The date and time the file / directory was created.
<b>modifyDate</b>	String	The date and time the file / directory was last modified.
<b>accessDate</b>	String	The date and time the file / directory was last accessed.
<b>metadataDate</b>	String	The date and time the file / directory metadata was last modified.
<b>scanDate</b>	String	The date and time the file / directory was last scanned by the antivirus. Note: The value "2000-01-01 00:00:00" indicates that the item has never been scanned.
<b>backupDate</b>	String	The date and time the file / directory last had a backup taken. Note: The value "2000-01-01 00:00:00" indicates that the item has never been backed up.
<b>snapshotDate</b>	String	The date and time the file / directory last had a snapshot taken. Note: The value "2000-01-01 00:00:00" indicates that a snapshot has never been taken on the item.
<b>mode</b>	String	The Linux permissions of the file / directory.
<b>size</b>	Integer	For a file, this attribute indicates the total size, in bytes, of the file. For a directory, this attribute indicates the sum of the "size" values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the "size" of the .snapshot subfolder is not included in the value of this attribute.

<b>usedSize</b>	Integer	For a file, this attribute indicates the actual size, in bytes, of the data in the file (not-written areas in the file excluded). For a directory, this attribute indicates the sum of the "usedSize" values for each file in the directory and all its subdirectories. Note: due to thin-provisioning, "usedSize" is usually less than "size". If the directory has a .snapshot subfolder, the "usedSize" of the .snapshot subfolder is not included in the value of this attribute.
<b>diskSize</b>	Integer	For a file, this attribute indicates the actual size, in bytes, of the file (not-written areas in the file excluded, erasure coding data included) and of the metadata associated with the file, as stored on the storage disk. For a directory, this attribute indicates the sum of the "diskSize" values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the "diskSize" of the .snapshot subfolder is not included in the value of this attribute.
<b>directoryCount</b>	Integer	The number of subdirectory entries in a directory, including the directory itself. A directory without any subdirectories has the value 1 for this attribute. If the inode is a file, the value of the attribute is 0.
<b>fileCount</b>	Integer	The number of file entries in the directory. If the inode is a file, the value of the attribute is 0.
<b>readBytes</b>	Integer	The number of bytes that have been read from the file / directory (including all its contents, subdirectories and files), since its creation.
<b>writeBytes</b>	Integer	The number of bytes that have been written to the file / directory (including all its contents, subdirectories and files), since its creation.
<b>readOperations</b>	Integer	The number of read operations on the file / directory (including all its contents, subdirectories and files), since its creation.
<b>writeOperations</b>	Integer	The number of write operations on the file / directory (including all its contents, subdirectories and files), since its creation.

## Create Directory

POST `/api/v1/fs?type=directory`

Create a directory at the path specified in the request body.

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-inode-id</b>	The ID of the newly created directory.
<b>x-cv-parent-id</b>	The ID of the parent directory.

### Request Body

<i>Name</i>	<i>Type</i>	<i>Description</i>	<i>Status</i>
<b>createParents</b>	Bool	If true, parent directories in the path are created as needed. If false, only the last part of the path is created.	Optional, default false.
<b>path</b>	String	The path to the new directory, relative to the current working directory.	Required
<b>mode</b>	String	The Linux permissions. This can be used to restrict access to directories. If createParents is true, all directories will be created with the same mode.	Optional, default "775".

## Sample Request

```
POST /api/v1/fs?type=directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "createParents": true,
  "path": "/path/to/directory",
  "mode": "744"
}
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 10:51:57 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/fs/path/to/directory
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43
x-cv-inode-id: 3e4a8ed1-0000-0000-1956-56df2b153a43
```

## Modify Directory

**PUT** */api/v1/fs/<path>?type=directory*

Change name or mode of a directory. Only the owner of the directory is allowed to change mode.

### Path Parameters

<b>path</b>	The path of the directory, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-inode-id</b>	The ID of the directory.
<b>x-cv-parent-id</b>	The ID of the parent directory.

### Request Body

Same as for Create Directory, except createParents is not used.

## Sample Request

```
PUT /api/v1/fs/path/to/directory?type=directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "path": "new_name",
  "mode": "700"
}
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 11:50:56 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43
x-cv-inode-id: 3e4a8ed1-0000-0000-1956-56df2b153a43
```

## Delete Directory

**DELETE** */api/v1/fs/<path>?type=directory*

Delete a directory. The directory must be empty for this operation to succeed.

### Path Parameters

<b>path</b>	The path of the directory, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-parent-id</b>	The ID of the parent directory.
-----------------------	---------------------------------

## Sample Request

```
DELETE /api/v1/fs/path/to/directory?type=directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43
```

## Head Inode

**HEAD** */api/v1/fs/<path>*

Check the existence of a file or directory.

### Path Parameters

<b>path</b>	The path of the directory / file, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-inode-id</b>	The ID of the inode.
<b>x-cv-inode-type</b>	The type of the inode.
<b>x-cv-parent-id</b>	The ID of the parent directory.

## Sample Request

```
HEAD /api/v1/fs/path/to/directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:05:32 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: c69a0b0c-236c-4372-8fc6-2caaf85551b8
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43
x-cv-inode-id: 3e4a8ed1-0000-0000-1956-56df2b153a43
x-cv-inode-type: directory
```

## Get Inode / Statistics

**GET** */api/v1/fs/<path>*

Retrieve inode attributes.

### Path Parameters

<b>path</b>	The path of the directory / file, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-parent-id</b>	The ID of the parent directory.
-----------------------	---------------------------------

### Response Body

The [Inode object](#).

## Sample Request

```
GET /api/v1/fs/path/to/directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:05:32 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: c69a0b0c-236c-4372-8fc6-2caaf85551b8
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43

{
  "id": "8e82ba51-0000-0000-1956-56df2b153a43",
  "type": "directory",
  "name": "mydirectory",
  "createDate": "2016-10-14 12:44:21",
  "modifyDate": "2016-10-14 12:44:21",
  "accessDate": "2016-10-14 12:44:21",
  "metadataDate": "2016-10-14 12:44:21",
  "scanDate": "2016-10-14 12:44:21",
  "backupDate": "2016-10-14 12:44:21",
  "snapshotDate": "2016-10-14 12:44:21",
  "mode": "777",
  "size": 0,
  "usedSize": 0,
  "diskSize": 0,
  "directoryCount": 0,
  "fileCount": 0,
  "readBytes": 0,
  "writeBytes": 0,
  "readOperations": 0,
  "writeOperations": 0
}
```

## Get Path Info

GET */api/v1/fs?inode=<inode\_id>*

Retrieve the absolute path of the inode.

### Path Parameters

inode_id	The unique inode id of the directory / file.
----------	--

### Response Body

The path of the inode.

### Sample Request

```
GET /api/v1/fs?inode=4c210000-0000-0000-705d-4557b1a9ee4a HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:05:32 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: c69a0b0c-236c-4372-8fc6-2caaf85551b8

{
  "path": "/path/to/inode"
}
```

## List Directories and Files

GET */api/v1/fs/<path>?list*

List the content of a directory.

### Path Parameters

<b>path</b>	The path of the directory, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Headers

<b>x-cv-inode-id</b>	The ID of the directory.
<b>x-cv-parent-id</b>	The ID of the parent directory.
<b>x-cv-directory-count</b>	The number of entries in the directory.

### Response Body

A JSON array of **Inode objects**. Optional attributes are not included.

### Sample Request

```
GET /api/v1/fs/path/to/directory?list HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:05:32 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: c69a0b0c-236c-4372-8fc6-2caaf85551b8
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43
x-cv-inode-id: 3e4a8ed1-0000-0000-1956-56df2b153a43
x-cv-directory-count: 5

[
  {
    "id": "8e82ba51-0000-0000-1956-56df2b153a43",
    "type": "directory",
    "name": "mydirectory",
    "createDate": "2016-10-14 12:44:21",
    "modifyDate": "2016-10-14 12:44:21",
    "accessDate": "2016-10-14 12:44:21",
    "metadataDate": "2016-10-14 12:44:21",
    "scanDate": "2016-10-14 12:44:21",
    "backupDate": "2016-10-14 12:44:21",
    "snapshotDate": "2016-10-14 12:44:21",
    "mode": "777",
    "size": 0,
    "usedSize": 0,
    "diskSize": 0
  },
  ...
]
```

# Policy Management

Operations for policy management. Create, modify, delete, and get a file/quota/snapshot policy; list file/quota/snapshot policies. A policy is created by configuring an existing directory.

## File Policies

### The File Policy object

```
{
  "filters": {
    "pattern": {
      "enable": true,
      "value": "*.doc"
    },
    "age": {
      "enable": true,
      "count": 2,
      "type": "months"
    }
  },
  "actions": {
    "fileCoding": {
      "enable": true,
      "value": "ERASURE_2_1"
    },
    "tier": {
      "enable": true,
      "value": "TIER_0"
    },
    "encryption": {
      "enable": true
    },
    "retention": {
      "enable": true,
      "modifiedAgo": {
        "count": 2,
        "type": "days"
      },
      "accessedAgo": {
        "count": 1,
        "type": "days"
      }
    },
    "worm": {
      "enable": true,
      "count": 2,
      "type": "hours"
    }
  }
}
```

### Attribute Definitions

Name	Type	Description
<b>filters</b>	Object	A set of criteria that determine which files will be affected by the actions.
<b>filters.pattern</b>	Object	A filter for one or several file name patterns.
<b>filters.pattern.enable</b>	Bool	Flag that signals if the pattern filter is enabled (true) or disabled (false).

<b>filters.pattern.value</b>	String	The file name patterns, separated by semicolon, which determine which files will be affected by the actions (Ex: *.jpg; *.gif).
<b>filters.age</b>	Object	A filter for the files that are older than the specified age.
<b>filters.age.enable</b>	Bool	Flag that signals if the age filter is enabled (true) or disabled (false).
<b>filters.age.count</b>	Integer	The unit count for the age filter. Valid values: 1-30.
<b>filters.age.type</b>	String	The unit type for the age filter. Valid values: "days", "weeks", "months", "years"
<b>actions</b>	Object	A set of events triggered on files that match all enabled filters.
<b>actions.fileCoding</b>	Object	An action that will apply a certain file encoding to the files that match all enabled filters.
<b>actions.fileCoding.enable</b>	Bool	Flag that signals if the file encoding action is enabled (true) or disabled (false).
<b>actions.fileCoding.value</b>	String	The file encoding argument (Ex: COPIES_3, ERASURE_2_1 etc.). See the appendix "File encodings" for all valid values.
<b>actions.tier</b>	Object	An action that will move files that match all enabled filters to nodes belonging to a certain tier (tiers define different importance levels of the data).
<b>actions.tier.enable</b>	Bool	Flag that signals if the tier action is enabled (true) or disabled (false).
<b>actions.tier.value</b>	String	The tier argument (Ex: TIER_0, TIER_1 etc.). See the appendix "Tiers" for all valid file encodings.
<b>actions.encryption</b>	Object	An action that will encrypt files that match all enabled filters.
<b>actions.encryption.enable</b>	Bool	Flag that signals if the encryption action is enabled (true) or disabled (false).
<b>actions.retention</b>	Object	An action that will delete files that have not been accessed / modified in the retention period. Files that have been modified / accessed at least once since the specified time (for example, in the last 2 months) are kept; the remaining files are deleted. At least one of modifiedAgo and accessedAgo must be specified (have a positive value). If both are specified, only files that do not match any of the two retention periods will be deleted.
<b>actions.retention.enable</b>	Bool	Flag that signals if the retention action is enabled (true) or disabled (false).
<b>actions.retention.modifiedAgo</b>	Object	An attribute for the retention action. Once given a value, only files that have been modified since the specified time are retained, and the rest are deleted (unless they are retained by a different retention attribute, i.e. "accessedAgo").
<b>actions.retention.modifiedAgo.count</b>	Integer	The unit count for the modifiedAgo attribute. Valid values: 0-30. A value of 0 means the modifiedAgo attribute is disabled.
<b>actions.retention.modifiedAgo.type</b>	String	The unit type for the modifiedAgo attribute. Valid values: "days", "weeks", "months", "years"
<b>actions.retention.accessedAgo</b>	Object	An attribute for the retention action. Once given a value, only files that have been accessed since the specified time are retained, and the rest are deleted (unless they are retained by a different retention attribute, i.e. "modifiedAgo").
<b>actions.retention.accessedAgo.count</b>	Integer	The unit count for the accessedAgo attribute. Valid values: 0-30. A value of 0 means the accessedAgo attribute is disabled.
<b>actions.retention.accessedAgo.type</b>	String	The unit type for the accessedAgo attribute. Valid values: "days", "weeks", "months", "years"
<b>actions.worm</b>	Object	An action (name stands for Write Once Read Many) that will permanently mark as read-only the files that are older than the specified period.
<b>actions.worm.enable</b>	Bool	Flag that signals if the worm action is enabled (true) or disabled (false).
<b>actions.worm.count</b>	Integer	The unit count for the worm period. Valid values: > 0
<b>actions.worm.type</b>	String	The unit type for the worm period. Valid values: "seconds", "minutes", "hours", "days", "weeks", "months", "years"

## Create File Policy

POST `/api/v1/fs/<path>?policy=file`

Add a file policy to a directory.

### Path Parameters

<b>path</b>	The path of the directory the policy should be added to, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The **File Policy object**. At least one action must be specified.

### Sample Request

```
POST /api/v1/fs/path/to/directory?policy=file HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>
```

```
{
  "filters": {
    "pattern": {
      "enable": true,
      "value": "*.doc"
    },
    "age": {
      "enable": true,
      "count": 2,
      "type": "months"
    }
  },
  "actions": {
    "fileCoding": {
      "enable": true,
      "value": "ERASURE_2_1"
    },
    "tier": {
      "enable": true,
      "value": "TIER_0"
    },
    "encryption": {
      "enable": true
    },
    "retention": {
      "enable": true,
      "modifiedAgo": {
        "count": 2,
        "type": "days"
      },
      "accessedAgo": {
        "count": 1,
        "type": "days"
      }
    },
    "worm": {
      "enable": true,
      "count": 2,
      "type": "hours"
    }
  }
}
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Modify File Policy

PUT /api/v1/fs/<path>?policy=file

Modify a directory's file policy.

### Path Parameters

<b>path</b>	The path of the directory that has the file policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The **File Policy object**. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/fs/path/to/directory?policy=file HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "filters": {
    "pattern": {
      "value": "*.jpg"
    }
  },
  "actions": {
    "retention": {
      "enable": false
    },
    "worm": {
      "enable": false
    }
  }
}
```

This sample request changes the pattern from \*.doc to \*.jpg, and disables the retention and worm action. The other file policy configuration remains unchanged.

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete File Policy

**DELETE**      */api/v1/fs/<path>?policy=file*

Delete a directory's file policy.

### Path Parameters

<b>path</b>	The path of the directory that has the file policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Sample Request

```
DELETE /api/v1/fs/path/to/directory?policy=file HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get File Policy

**GET**      */api/v1/fs/<path>?policy=file*

Retrieve a directory's file policy configuration.

### Path Parameters

<b>path</b>	The path of the directory that has the file policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Body

The [File Policy object](#).

### Sample Request

```
GET /api/v1/fs/path/to/directory?policy=file HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```

HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "filters": {
    "pattern": {
      "enable": true,
      "value": "*.doc"
    },
    "age": {
      "enable": true,
      "count": 2,
      "type": "months"
    }
  },
  "actions": {
    "fileCoding": {
      "enable": true,
      "value": "ERASURE_2_1"
    },
    "tier": {
      "enable": true,
      "value": "TIER_0"
    },
    "encryption": {
      "enable": true
    },
    "retention": {
      "enable": true,
      "modifiedAgo": {
        "count": 2,
        "type": "days"
      },
      "accessedAgo": {
        "count": 1,
        "type": "days"
      }
    },
    "worm": {
      "enable": true,
      "count": 2,
      "type": "hours"
    }
  }
}

```

## List File Policies

GET `/api/v1/fs?policy=file&list`

List all file policies in the file system.

### Response Body

Name	Type	Description
<b>path</b>	String	The path of the directory that has the file policy.
<b>filePolicy</b>	Object	<a href="#">The File Policy object.</a>

## Sample Request

```
GET /api/v1/fs?policy=file&list HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

```
[
  {
    "path": "/path/to/directory",
    "filePolicy": {
      "filters": {
        "pattern": {
          "enable": true,
          "value": "*.doc"
        },
        "age": {
          "enable": true,
          "count": 2,
          "type": "months"
        }
      },
      "actions": {
        "fileCoding": {
          "enable": true,
          "value": "ERASURE_2_1"
        },
        "tier": {
          "enable": true,
          "value": "TIER_0"
        },
        "encryption": {
          "enable": true
        },
        "retention": {
          "enable": true,
          "modifiedAgo": {
            "count": 2,
            "type": "days"
          },
          "accessedAgo": {
            "count": 1,
            "type": "days"
          }
        },
        "worm": {
          "enable": true,
          "count": 2,
          "type": "hours"
        }
      }
    },
    ...
  ]
```

## Quota Policies

### The Quota Policy object

```
{
  "limit": {
    "count": 2,
    "type": "GB"
  }
}
```

### Attribute Definitions

Name	Type	Description
<b>limit</b>	Object	The quota limit for the directory (including all subdirectories and files). The total size of the data contained in the directory cannot normally surpass this limit; however, in case of multithreaded parallel write operations, there is a theoretical possibility that the limit is slightly exceeded due to the delay required by the system to compute the total size of the parallel write operations. As soon as the system has realized that the limit has been reached, no more write operations will be allowed on the directory (until some data is deleted and the directory size goes below the quota limit).  Note: It is a valid operation to apply a quota limit on a directory that already contains more data than the applied limit. Any new write attempt to the directory will however be denied, until the total size of the data in the directory goes below the quota limit (by deleting some of the already existing data).
<b>limit.count</b>	String	The unit count for the limit. Valid values: 1-999.
<b>limit.type</b>	String	The unit type for the limit. Valid values: "GB", "TB", "PB"

### Create Quota Policy

POST `/api/v1/fs/<path>?policy=quota`

Add a quota policy to a directory.

#### Path Parameters

<b>path</b>	The path of the directory the policy should be added to, relative to the current working directory.
-------------	---

#### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

#### Request Body

The Quota Policy object.

#### Sample Request

```
POST /api/v1/fs/path/to/directory?policy=quota HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "limit": {
    "count": 2,
    "type": "GB"
  }
}
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Modify Quota Policy

**PUT** */api/v1/fs/<path>?policy=quota*

Modify a directory's quota policy.

### Path Parameters

<b>path</b>	The path of the directory that has the quota policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The **Quota Policy object**. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/fs/path/to/directory?policy=quota HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "limit": {
    "count": 5,
    "type": "TB"
  }
}
```

This sample request changes the quota limit from 2 GB to 5 TB. The other quota policy configuration remains unchanged.

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Quota Policy

**DELETE** */api/v1/fs/<path>?policy=quota*

Delete a directory's quota policy.

### Path Parameters

<b>path</b>	The path of the directory that has the quota policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

## Sample Request

```
DELETE /api/v1/fs/path/to/directory?policy=quota HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Quota Policy

GET */api/v1/fs/<path>?policy=quota*

Retrieve a directory's quota policy configuration.

### Path Parameters

<b>path</b>	The path of the directory that has the quota policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Body

The Quota Policy object.

## Sample Request

```
GET /api/v1/fs/path/to/directory?policy=quota HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "limit": {
    "count": 2,
    "type": "GB"
  }
}
```

## List Quota Policies

GET */api/v1/fs?policy=quota&list*

List all quota policies in the file system.

### Response Body

Name	Type	Description
<b>path</b>	String	The path of the directory that has the quota policy.
<b>quotaPolicy</b>	Object	The Quota Policy object.

## Sample Request

```
GET /api/v1/fs?policy=quota&list HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

[
  {
    "path": "/path/to/directory",
    "quotaPolicy": {
      "limit": {
        "count": 2,
        "type": "GB"
      }
    }
  },
  ...
]
```

## Snapshot Policies

### The Snapshot Schedule object

```
{
  "type": "weekly",
  "numberOfCopies": 5,
  "timeOfDay": "13:56",
  "dayOfWeek": "monday",
  "hoursOfDay": [1, 12, 23]
}
```

### Attribute Definitions

Name	Type	Description
<b>type</b>	String	The type of snapshot schedule. The type determines how the numberOfCopies, timeOfDay, dayOfWeek and hoursOfDay attributes are used. Note that the schedule type "manually" is not required for snapshots to be triggered manually. See actions: <a href="#">Take Snapshot</a> . Valid values: "manually", "hourly", "daily", "weekly". The type "manually" uses numberOfCopies. The type "hourly" uses numberOfCopies and hoursOfDay. The type "daily" uses numberOfCopies and timeOfDay. The type "weekly" uses numberOfCopies, timeOfDay and dayOfWeek.
<b>numberOfCopies</b>	Integer	The maximum number of snapshots copies that can be retained at any point in time. For example, if numberOfCopies is 5, the sixth snapshot copy will overwrite the oldest of the previous five, thus keeping the total number of snapshots copies at a maximum of 5. The total maximum allowed number of copies for all Snapshot Schedules that belong to the same Snapshot Policy is 253.

<b>timeOfDay</b>	Integer	The time of the day the snapshot will be performed. Time is interpreted as UTC offset +00. Format: "hh:mm". "hh" must be in the range 00 – 23 and "mm" must be in the range 00 – 59.
<b>dayOfWeek</b>	String	The day of the week the snapshot should be performed. Valid values: "monday", "tuesday", "wednesday", "thursday", "friday", "saturday", "sunday"
<b>hoursOfDay</b>	Array of integers	The hours of the day a snapshot should be performed. Hours are interpreted as UTC offset +00. Format: [h1, h2, h3, ...]. Valid values: Each entry must be in the range 0 – 23. Duplicates are ignored.

## The Snapshot Policy object

An array of [Snapshot Schedule objects](#), each having a distinct type (i.e. weekly, hourly, daily or manually). The sum of all numberOfCopies values of a Snapshot Policy cannot exceed 253.

```
[
  {
    "type": "weekly",
    "numberOfCopies": 5,
    "timeOfDay": "00:00",
    "dayOfWeek": "monday",
  },
  {
    "type": "daily",
    "numberOfCopies": 7,
    "timeOfDay": "13:56",
  },
  {
    "type": "hourly",
    "numberOfCopies": 10,
    "hoursOfDay": [1,13]
  },
  ...
]
```

## Create Snapshot Policy

POST `/api/v1/fs/<path>?policy=snapshot`

Add a snapshot policy to a directory.

### Path Parameters

<b>path</b>	The path of the directory the policy should be added to, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

[The Snapshot Policy object](#).

## Sample Request

```
POST /api/v1/fs/path/to/directory?policy=snapshot HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

[
  {
    "type": "weekly",
    "numberOfCopies": 8,
    "timeOfDay": "18:00",
    "dayOfWeek": "friday"
  },
  {
    "type": "hourly",
    "numberOfCopies": 10,
    "hoursOfDay": [1,13]
  }
]
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

## Modify Snapshot Policy

**PUT** */api/v1/fs/<path>?policy=snapshot*

Modify a directory's snapshot policy. If, as a consequence of the modification, the sum of all numberOfCopies of the Snapshot Policy would exceed 253, the modification request will be denied.

### Path Parameters

<b>path</b>	The path of the directory that has the snapshot policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The **Snapshot Policy object**. Any snapshot schedule or snapshot schedule parameter not provided, remains unchanged.

## Sample Request

```
PUT /api/v1/fs/path/to/directory?policy=snapshot HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

[
  {
    "type": "hourly",
    "numberOfCopies": 20
  }
]
```

This sample request changes number of copies for the hourly schedule to 20. The other snapshot policy configuration remains unchanged.

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Snapshot Policy

**DELETE** */api/v1/fs/<path>?policy=snapshot*

Delete a directory's snapshot policy.

### Path Parameters

<b>path</b>	The path of the directory that has the snapshot policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Sample Request

```
DELETE /api/v1/fs/path/to/directory?policy=snapshot HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Snapshot Policy

**GET** */api/v1/fs/<path>?policy=snapshot*

Retrieve a directory's snapshot policy configuration.

### Path Parameters

<b>path</b>	The path of the directory that has the snapshot policy, relative to the current working directory.
-------------	--

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Body

The Snapshot Policy object.

### Sample Request

```
GET /api/v1/fs/path/to/directory?policy=snapshot HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```

HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

[
  {
    "type": "weekly",
    "numberOfCopies": 8,
    "timeOfDay": "18:00",
    "dayOfWeek": "friday"
  },
  {
    "type": "hourly",
    "numberOfCopies": 20,
    "hoursOfDay": [1,13]
  }
]

```

## List Snapshot Policies

GET */api/v1/fs?policy=snapshot&list*

List all snapshot policies in the file system.

### Response Body

Name	Type	Description
<b>path</b>	String	The path of the directory that has the snapshot policy.
<b>snapshotPolicy</b>	Object	<a href="#">The Snapshot Policy object.</a>

### Sample Request

```

GET /api/v1/fs?policy=snapshot&list HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>

```

### Sample Response

```

HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

[
  {
    "path": "/path/to/directory",
    "snapshotPolicy": [
      {
        "type": "weekly",
        "numberOfCopies": 5,
        "timeOfDay": "13:56",
        "dayOfWeek": "monday"
      },
      ...
    ]
  },
  ...
]

```

## Antivirus Policies

### The Antivirus Policy object

```

{
  "includePattern": "*",
  "excludePattern": "*.zip;*.exe;*.pdf",
  "maxFileSize": {
    "count": 2,
    "type": "GB"
  },
  "alerts": {
    "alertOnWarnings": true,
    "email": true,
    "snmp": true
  },
  "options": {
    "deleteInfectedFiles": false
  },
  "backgroundScan": {
    "enable": true,
    "maxFileSize": {
      "count": 10,
      "type": "GB"
    },
    "interval": {
      "type": "weekly",
      "timeOfDay": "14:00",
      "dayOfWeek": "monday",
      "hoursOfDay": [1, 12, 23]
    }
  }
}

```

### Attribute Definitions

Name	Type	Description
<b>includePattern</b>	String	The file name patterns, semicolon separated, for files that will be included in live scanning (at read time) and background scanning (example, "*.exe; *.zip"). If includePattern is empty, all file patterns are included.
<b>excludePattern</b>	String	The file name patterns, semicolon separated, for files that will be excluded from live scanning (at read time) and background scanning (E.g. "*.zip; *.pdf").
<b>maxFileSize</b>	Object	Files having this maximum size will be included in the live scanning (scanning at read time).
<b>maxFileSize.count</b>	Integer	The unit count for the maximum size of files that will be included in the live scanning (scanning at read time). Valid values: 1-999
<b>maxFileSize.type</b>	String	The unit type for the maximum size of files that will be included in the live scanning (scanning at read time). Valid values: "KB", "MB", "GB"
<b>alerts</b>	Object	A feature that alerts the user via email and/or SNMP traps on various antivirus-related events, e.g. when infected files are found (critical-level event), or when suspicious content is found (warning-level event). Note: the warning-level events must be separately enabled, see the "alerts.alertOnWarnings" attribute below.

<b>alerts.alertOnWarnings</b>	Bool	A feature that alerts the user even on warning-level events, e.g. suspicious content. If this attribute is disabled, and at least one of "alerts.email" or "alerts.snmp" is enabled, alerts will be sent only on critical-level events, i.e. when infected files are found.
<b>alerts.email</b>	Bool	Flag that signals if the email alerts are enabled (true) or disabled (false).
<b>alerts.snmp</b>	Bool	Flag that signals if the SNMP trap alerts are enabled (true) or disabled (false).
<b>options.deleteInfectedFiles</b>	Bool	If enabled, files will be automatically deleted if found infected. <b>Warning:</b> By using this option, there is a risk of unintentional loss of data.
<b>backgroundScan</b>	Object	A feature that does background antivirus scanning.
<b>backgroundScan.enable</b>	Bool	Flag that signals if the background scanning is enabled (true) or disabled (false).
<b>backgroundScan.maxFileSize</b>	Object	Files having this maximum size will be included in the background scanning.
<b>backgroundScan.maxFileSize.count</b>	Integer	The unit count for the maximum size of files that will be included in the background scanning. Valid values: 1-999.
<b>backgroundScan.maxFileSize.type</b>	String	The unit type for the maximum size of files that will be included in the background scanning. Valid values: "KB", "MB", "GB"
<b>backgroundScan.interval</b>	Object	Attributes to define intervals at which the background scanning is performed. If backgroundScan.enable is true, then this interval must be included.
<b>backgroundScan.interval.type</b>	String	The type of interval for the background scanning. The type determines how the timeOfDay, dayOfWeek and hoursOfDay attributes are used.  Valid values: "hourly", "daily", "weekly"  The type "hourly" uses hoursOfDay. The type "daily" uses timeOfDay. The type "weekly" uses timeOfDay and dayOfWeek.
<b>backgroundScan.interval.timeOfDay</b>	Integer	The time of day the background scan should be performed. Time is interpreted as UTC offset +00.  Format: "hh:00". hh must be in the range 00 – 23.
<b>backgroundScan.interval.dayOfWeek</b>	String	The day of the week the background scan should be performed.  Valid values: "monday", "tuesday", "wednesday", "thursday", "friday", "saturday", "sunday"
<b>backgroundScan.interval.hoursOfDay</b>	Array of integers	The hours of the day a background scan should be performed. Hours are interpreted as UTC offset +00.  Format: [h1, h2, h3, ...]. Valid values: Each entry must be in the range 0 – 23. Duplicates are ignored.

## Create Antivirus Policy

POST /api/v1/fs/<path>?policy=antivirus

Add an antivirus policy to a directory.

### Path Parameters

<b>path</b>	The path of the directory the policy should be added to, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The Antivirus Policy object.

### Sample Request

```
POST /api/v1/fs/path/to/directory?policy=antivirus HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "includePattern": "*",
  "excludePattern": "*.zip;*.exe;*.pdf",
  "maxFileSize": {
    "count": 2,
    "type": "GB"
  },
  "alerts": {
    "alertOnWarnings": true,
    "email": true,
    "snmp": true
  },
  "options": {
    "deleteInfectedFiles": false
  },
  "backgroundScan": {
    "enable": true,
    "maxFileSize": {
      "count": 10,
      "type": "GB"
    },
    "interval": {
      "type": "weekly",
      "timeOfDay": "14:00",
      "dayOfWeek": "monday",
      "hoursOfDay": [1, 12, 23]
    }
  }
}
```

### Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

## Modify Antivirus Policy

PUT /api/v1/fs/<path>?policy=antivirus

Modify a directory's antivirus policy.

### Path Parameters

<b>path</b>	The path of the directory that has the antivirus policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Request Body

The **Antivirus Policy object**. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/fs/path/to/directory?policy=antivirus HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "alerts": {
    "alertOnWarnings": false,
  }
}
```

This sample request changes the antivirus warnings to false. The other antivirus policy configuration remains unchanged.

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Antivirus Policy

**DELETE** /api/v1/fs/<path>?policy=antivirus

Delete a directory's antivirus policy.

### Path Parameters

<b>path</b>	The path of the directory that has the antivirus policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Sample Request

```
DELETE /api/v1/fs/path/to/directory?policy=antivirus HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Antivirus Policy

GET /api/v1/fs/<path>?policy=antivirus

Retrieve a directory's antivirus policy configuration.

### Path Parameters

<b>path</b>	The path of the directory that has the antivirus policy, relative to the current working directory.
-------------	---

### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path is relative to.
--------------------	--

### Response Body

The Antivirus Policy object.

### Sample Request

```
GET /api/v1/fs/path/to/directory?policy=antivirus HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "includePattern": "*",
  "excludePattern": "*.zip;*.exe;*.pdf",
  "maxFileSize": {
    "count": 2,
    "type": "GB"
  },
  "alerts": {
    "alertOnWarnings": true,
    "email": true,
    "snmp": true
  },
  "options": {
    "deleteInfectedFiles": false
  },
  "backgroundScan": {
    "enable": true,
    "maxFileSize": {
      "count": 10,
      "type": "GB"
    },
    "interval": {
      "type": "weekly",
      "timeOfDay": "14:00",
      "dayOfWeek": "monday",
      "hoursOfDay": [1, 12, 23]
    }
  }
}
```

## List Antivirus Policies

GET /api/v1/fs?policy=antivirus&list

List all antivirus policies in the file system.

### Response Body

Name	Type	Description
<b>path</b>	String	The path of the directory that has the antivirus policy.
<b>antivirusPolicy</b>	Object	<a href="#">The Antivirus Policy object.</a>

### Sample Request

```
GET /api/v1/fs?policy=antivirus&list HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e

[
  {
    "path": "/path/to/directory",
    "antivirusPolicy": {
      "includePattern": "*",
      "excludePattern": "*.zip;*.exe;*.pdf",
      "maxFileSize": {
        "count": 2,
        "type": "GB"
      },
      "alerts": {
        "alertOnWarnings": true,
        "email": true,
        "snmp": true
      },
      "options": {
        "deleteInfectedFiles": false
      },
      "backgroundScan": {
        "enable": true,
        "maxFileSize": {
          "count": 10,
          "type": "GB"
        },
        "interval": {
          "type": "weekly",
          "timeOfDay": "14:00",
          "dayOfWeek": "monday",
          "hoursOfDay": [1, 12, 23]
        }
      }
    }
  },
  ...
]
```

# Share Management

Operations for share management. Create, modify, delete, and get a file share; list file shares. A share is created by configuring an existing directory.

## Shares

### The Share object

```
{
  "name": "myshare",
  "path": "/path/to/directory",
  "smb": {
    "enable": true,
    "options": {
      "ALLOW_GUEST_ACCESS": true,
      "DISABLE_CLIENT_WRITE_CACHE": true,
      "ENCRYPTION": true,
      "SCALE_OUT": true,
      "ALLOW_OFFLINE_FILE_SUPPORT": true,
      "ACCESS_BASED_ENUMERATION": true,
      "DISTRIBUTED_FILESYSTEM": true
    },
    "ipFilter": "172.16.0.0/16"
  },
  "nfs": {
    "enable": true,
    "options": {
      "ALLOW_ROOT_ACCESS": true,
      "ALLOW_GUEST_ACCESS": true,
      "USE_32BIT_INODES": true,
      "DISABLE_SHARE_MODE_CHECK": true,
      "DISABLE_RW_DELEGATION": true
    },
    "authentication": {
      "sys": true,
      "krb5": true,
      "krb5i": true,
      "krb5p": true
    },
    "ipFilter": "192.168.1.0/24 192.168.2.0/24"
  },
  "amazonS3": {
    "enable": true,
    "account": "myaccount",
    "apiEndpoint": "api.endpoint",
    "websiteEndpoint": "website.endpoint",
    "websiteBucketDomains": "mydomain.com"
  },
  "openStack": {
    "enable": true
  },
  "nntp": {
    "enable": true
  }
}
```

## Attribute Definitions

<i>Name</i>	<i>Type</i>	<i>Description</i>
<b>name</b>	String	The name of the new share.
<b>path</b>	String	The path to the directory that should be enabled as a Compuverde file share. The path is relative to the current working directory. If the path starts with "/", it is absolute (starts at the file system root).
<b>smb</b>	Object	Configuration for the SMB protocol.
<b>smb.enable</b>	Bool	Flag that signals if the new share will be accessible via the SMB protocol.
<b>smb.options</b>	Object	<p>A set of attributes with Boolean values that configure the SMB-access on the new share.</p> <p>Valid attributes are:</p> <ul style="list-style-type: none"> <li>* ALLOW_GUEST_ACCESS (if true, enables the user to access the file share without user credentials)</li> <li>* DISABLE_CLIENT_WRITE_CACHE (if true, disables write caching on the client side and enables read only cache)</li> <li>* ENCRYPTION (if true, adds additional encryption on the data being sent to a client)</li> <li>* SCALE_OUT (if true, enables support for failover between nodes)</li> <li>* ALLOW_OFFLINE_FILE_SUPPORT (if true, enables the user to modify files in the file share even when the network is disconnected and merges the file changes when the network is available again)</li> <li>* ACCESS_BASED_ENUMERATION (if true, enables user access control based on the criteria present in the "User" section of the Management Tool)</li> <li>* DISTRIBUTED_FILESYSTEM (if true, enables DFS – Distributed file system)</li> </ul>
<b>smb.ipFilter</b>	String	If present, only clients having the IP specified by this attribute will be able to connect to the SMB share. Both individual IP addresses and IP+subnet mask combinations can be used. (E.g. a value of 172.16.0.0/16 means that only clients with the IP in the range 172.16.0.0 – 172.16.255.255 will be able to connect to the share). Several IP filters can be included, separated by space.
<b>nfs</b>	Object	Configuration for the NFS protocol.
<b>nfs.enable</b>	Bool	Flag that signals if the new share will be accessible via the NFS protocol.
<b>nfs.options</b>	Object	<p>A set of attributes with Boolean values that configure the NFS-access on the new share.</p> <p>Valid attributes are:</p> <ul style="list-style-type: none"> <li>* ALLOW_ROOT_ACCESS (if true, remote root users are able to access and change any file on the shared file system. This corresponds to no_root_squash. If false, the remote root user will become anonymous (uid -2, gid -2) and is either allowed or denied depending on the setting of "Allow Guest Access" - see below)</li> <li>* ALLOW_GUEST_ACCESS (if true, enables users that do not provide valid NFS credentials to access the file share. The user becomes anonymous - uid -2, gid -2)</li> <li>* USE_32BIT_INODES (if true, forces Compuverde to use 32-bit inodes internally instead of 64-bit inodes)</li> <li>* DISABLE_SHARE_MODE_CHECK (attribute for Mac only. If true, disables share mode check because Mac will always check if the file is open for read).</li> <li>* DISABLE_RW_DELEGATION (if true, disables read/write delegation, which allows clients to cache data locally for faster updates using less network traffic and improving response time. When enabled, can result in unwanted latency).</li> </ul>

<b>nfs.authentication</b>	Object	A set of attributes with Boolean values that enable and control various authentication methods to the NFS share.  Valid attributes are: sys (Unix uid), krb5 (Kerberos login), krb5i (Kerberos integrity), krb5p (Kerberos privacy / encryption of all traffic between the client and the server)
<b>nfs.ipFilter</b>	String	If present, only clients having the IP specified by this attribute will be able to connect to the NFS share. Both individual IP addresses and IP+subnet mask combinations can be used. (E.g. a value of 172.16.0.0/16 means that only clients with the IP in the range 172.16.0.0 – 172.16.255.255 will be able to connect to the share). Several IP filters can be included, separated by space.
<b>amazonS3</b>	Object	Configuration for the Amazon S3 protocol.
<b>amazonS3.enable</b>	Bool	Flag that signals if the new share will be accessible via the Amazon S3 protocol.
<b>amazonS3.account</b>	String	The user group that the S3 share is accessible to. If this attribute is not used, all users will have access.
<b>amazonS3.apiEndpoint</b>	String	The endpoint used to access the Amazon S3 REST API. For more details, see the Management Manual (File System > Additional protocol properties > Additional properties for Amazon S3 > API endpoint)
<b>amazonS3.websiteEndpoint</b>	String	The endpoint used to access static websites. For more details, see the Management Manual (File System > Additional protocol properties > Additional properties for Amazon S3 > Website endpoint).
<b>amazonS3.websiteBucketDomains</b>	String	The names of buckets that have a corresponding DNS record. For more details, see the Management Manual (File System > Additional protocol properties > Additional properties for Amazon S3 > Website bucket domains).
<b>openStack</b>	Object	Configuration for the OpenStack Swift protocol.
<b>openStack.enable</b>	Bool	Flag that signals if the new share will be accessible via the Open Stack protocol.
<b>nntp</b>	Object	Configuration for the NNTP protocol.
<b>nntp.enable</b>	Bool	Flag that signals if the new share will be accessible via the NNTP protocol.

## Create Share

POST /api/v1/shares

Create a new Compuverde file share. Note that the directory specified in the path in the request body must already exist.

---

**x-cv-cwd-id** Optional. The ID of the directory the path in the request body is relative to.

---

### Request Body

The **Share object**. Name and path are required.

### Sample Request

```
POST /api/v1/shares HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "myshare",
  "path": "/path/to/directory",
  "smb": {
    "enable": true,
    "options": {
      "ALLOW_GUEST_ACCESS": true,
      "DISABLE_CLIENT_WRITE_CACHE": true,
      "ENCRYPTION": true,
      "SCALE_OUT": true,
      "ALLOW_OFFLINE_FILE_SUPPORT": true,
      "ACCESS_BASED_ENUMERATION": true,
      "DISTRIBUTED_FILESYSTEM": true
    },
    "ipFilter": "172.16.0.0/16"
  },
  "nfs": {
    "enable": true,
    "options": {
      "ALLOW_ROOT_ACCESS": true,
      "ALLOW_GUEST_ACCESS": true,
      "USE_32BIT_INODES": true,
      "DISABLE_SHARE_MODE_CHECK": true,
      "DISABLE_RW_DELEGATION": true
    },
    "authentication": {
      "sys": true,
      "krb5": true,
      "krb5i": true,
      "krb5p": true
    },
    "ipFilter": "192.168.1.0/24 192.168.2.0/24"
  },
  "amazonS3": {
    "enable": true,
    "account": "myaccount",
    "apiEndpoint": "api.endpoint",
    "websiteEndpoint": "website.endpoint",
    "websiteBucketDomains": "mydomain.com"
  },
  "openStack": {
    "enable": true
  },
  "nntp": {
    "enable": true
  }
}
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 14:15:12 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/shares/myshare
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Modify Share

**PUT** `/api/v1/shares/<share>`

Modify a file share. Enable or disable a protocol, change protocol settings, and/or change the name of the share.

### Path Parameters

<b>share</b>	The name of the share.
--------------	------------------------

### Request Body

**The Share object.** Path is ignored and Name is optional. The name attribute is the new name of the share. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/shares/myshare HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "nfs": {
    "authentication": {
      "sys": false
    }
  },
  "openStack": {
    "enable": false
  }
}
```

This sample request disables sys as a security flavor for NFS and disables the OpenStack Swift protocol. The other share and protocol configuration remains unchanged.

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 14:17:33 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Share

**DELETE**            */api/v1/shares/<share>*

Delete a file share. Note that the directory is not deleted.

### Path Parameters

---

**share**                    The name of the share.

---

### Sample Request

```
DELETE /api/v1/shares/myshare HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Share

**GET**                    */api/v1/shares/<share>*

Retrieve the configuration for a file share.

### Path Parameters

---

**share**                    The name of the share.

---

### Response Body

The [Share object](#).

### Sample Request

```
GET /api/v1/shares/myshare HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "name": "myshare",
  "path": "/path/to/directory",
  "smb": {
    "enable": true,
    "options": {
      "ALLOW_GUEST_ACCESS": true,
      "DISABLE_CLIENT_WRITE_CACHE": true,
      "ENCRYPTION": true,
      "SCALE_OUT": true,
      "ALLOW_OFFLINE_FILE_SUPPORT": true,
      "ACCESS_BASED_ENUMERATION": true,
      "DISTRIBUTED_FILESYSTEM": true
    },
    "ipFilter": "172.16.0.0/16"
  },
  "nfs": {
    "enable": true,
    "options": {
      "ALLOW_ROOT_ACCESS": true,
      "ALLOW_GUEST_ACCESS": true,
      "USE_32BIT_INODES": true,
      "DISABLE_SHARE_MODE_CHECK": true,
      "DISABLE_RW_DELEGATION": true
    },
    "authentication": {
      "sys": true,
      "krb5": true,
      "krb5i": true,
      "krb5p": true
    },
    "ipFilter": "192.168.1.0/24 192.168.2.0/24"
  },
  "amazonS3": {
    "enable": true,
    "account": "myaccount",
    "apiEndpoint": "api.endpoint",
    "websiteEndpoint": "website.endpoint",
    "websiteBucketDomains": "mydomain.com"
  },
  "openStack": {
    "enable": true
  },
  "nntp": {
    "enable": true
  }
}
```

## List Shares

**GET** */api/v1/shares*

List all file shares in the file system.

### Response Body

AJSON array of [Share objects](#).

## Sample Request

```
GET /api/v1/shares HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

```
[
  {
    "name": "myshare",
    "path": "/path/to/directory",
    "smb": {
      "enable": true,
      "options": {
        "ALLOW_GUEST_ACCESS": true,
        "DISABLE_CLIENT_WRITE_CACHE": true,
        "ENCRYPTION": true,
        "SCALE_OUT": true,
        "ALLOW_OFFLINE_FILE_SUPPORT": true,
        "ACCESS_BASED_ENUMERATION": true,
        "DISTRIBUTED_FILESYSTEM": true
      },
      "ipFilter": "172.16.0.0/16"
    },
    "nfs": {
      "enable": true,
      "options": {
        "ALLOW_ROOT_ACCESS": true,
        "ALLOW_GUEST_ACCESS": true,
        "USE_32BIT_INODES": true,
        "DISABLE_SHARE_MODE_CHECK": true,
        "DISABLE_RW_DELEGATION": true
      },
      "authentication": {
        "sys": true,
        "krb5": true,
        "krb5i": true,
        "krb5p": true
      },
      "ipFilter": "192.168.1.0/24 192.168.2.0/24"
    },
    "amazonS3": {
      "enable": true,
      "account": "myaccount",
      "apiEndpoint": "api.endpoint",
      "websiteEndpoint": "website.endpoint",
      "websiteBucketDomains": "mydomain.com"
    },
    "openStack": {
      "enable": true
    },
    "nntp": {
      "enable": true
    }
  },
  ...
]
```

## ISCSI Management

Operations for iSCSI management. Create, modify, delete, and get an iSCSI target; list iSCSI targets. Create, modify, resize, and delete an iSCSI LUN.

### iSCSI Targets

#### The Target object

```
{
  "name": "mytarget",
  "fileCoding": "DEFAULT",
  "tier": "ANY",
  "allowAnonymous": false,
  "allowMPIO" : true,
  "initiatorGroup": "igroup1",
  "luns": [
    {
      "id": 1,
      "size": 1,
      "comment": "my lun"
    }
  ]
}
```

#### Attribute Definitions

Name	Type	Description
<b>name</b>	String	The name of the iSCSI target.
<b>fileCoding</b>	String	The file coding to apply to the target and its LUNs (Ex: DEFAULT, COPIES_3, ERASURE_2_1 etc.). "DEFAULT" uses the file encoding of the file system. See the appendix "File encodings" for all valid values.
<b>Tier</b>	String	The tier to use for the target and its LUNs (Ex: TIER_0, TIER_1 etc.). Tiers define different importance levels of the data. See the appendix "Tiers" for all valid file encodings.
<b>allowAnonymous</b>	Bool	If true, unauthenticated initiators can access the target's LUNs. If false, all initiators must authenticate by providing valid Compuverde credentials via the CHAP protocol.
<b>allowMPIO</b>	Bool	If true, iSCSI Multipath IO (MPIO) is enabled on the iSCSI Target, meaning that a discovery request sent to one of the storage nodes will get as response a list with the IP addresses of all nodes in the cluster (including the address of the node that got the discovery request), for that particular iSCSI Target. The client that made the request is thus informed that the iSCSI Target can be reached via multiple paths (via any of the IP addresses in the list). If false, iSCSI MPIO is disabled on the iSCSI Target, meaning that a discovery request sent to one of the storage nodes will get as response only the IP address of the node that got the request, for that particular iSCSI Target. The client that made the request is thus informed that the iSCSI Target can be reached only via the IP address of the node that got the discovery request.
<b>initiatorGroup</b>	String	If present, associates the existing iSCSI Initiator Group having this name to the target (only initiators coming from IPs white-listed by the Initiator Group will be able to log on to the target). If missing, or if the value is the empty string (""), the target is not associated to an Initiator Group (the effect is that any Initiator can log on to the target).

---

<b>luns</b>	Array	An array of LUN Objects. See section "iSCSI LUNs > The LUN object" below for details.
-------------	-------	---

---

## Create Target

**POST** */api/v1/iscsi/targets*

Create a target, as well as an optional set of LUNs. You can create a target without any LUNs and then use the Create LUN operation to manually create each LUN, or you can create a target and specify the LUNs in the same request.

### Request Body

The **Target object**. Name is required.

### Sample Request

```
POST /api/v1/iscsi/targets HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "mytarget",
  "fileCoding": "DEFAULT",
  "tier": "ANY",
  "allowAnonymous": false,
  "allowMPIO": true,
  "initiatorGroup": "",
  "luns": [
    {
      "id": 1,
      "size": 1,
      "comment": "my lun"
    }
  ]
}
```

### Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/iscsi/targets/mytarget
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

## Modify Target

**PUT** */api/v1/iscsi/targets/<target>*

Modify a target.

### Path Parameters

---

<b>target</b>	The name of the target.
---------------	-------------------------

---

### Request Body

The **Target object**. Name is optional — the name of the target is changed if it's specified. The LUNs array is ignored, i.e. you cannot use this operation to modify LUNs. Any parameters not provided remain unchanged.

## Sample Request

```
PUT /api/v1/iscsi/targets/mytarget HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "allowAnonymous": true
}
```

This sample request modifies the target to allow anonymous access. The other target configuration remains unchanged.

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Target

**DELETE** */api/v1/iscsi/targets/<target>*

Delete a target together with all its corresponding LUNs and data.



**Warning:** This operation may delete data and should be used with caution.

## Path Parameters

<b>target</b>	The name of the target.
---------------	-------------------------

## Sample Request

```
DELETE /api/v1/iscsi/targets/mytarget HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Target

**GET** */api/v1/iscsi/targets/<target>*

Retrieve information about a target and its LUNs.

## Path Parameters

<b>target</b>	The name of the target.
---------------	-------------------------

## Response Body

The Target object.

### Sample Request

```
GET /api/v1/iscsi/targets/mytarget HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "name": "mytarget",
  "fileCoding": "DEFAULT",
  "tier": "ANY",
  "allowAnonymous": false,
  "allowMPIO" : true,
  "initiatorGroup": "igroup1",
  "luns": [
    {
      "id": 1,
      "size": 1,
      "comment": "my lun"
    }
  ]
}
```

### List Targets

GET /api/v1/iscsi/targets

List all iSCSI targets and LUNs.

#### Response Body

A JSON array of [Target objects](#).

#### Sample Request

```
GET /api/v1/iscsi/targets HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e

[
  {
    "name": "mytarget",
    "fileCoding": "DEFAULT",
    "tier": "ANY",
    "allowAnonymous": false,
    "allowMPIO" : true,
    "initiatorGroup": "igroup1",
    "luns": [
      {
        "id": 1,
        "size": 1,
        "comment": "my lun"
      }
    ]
  },
  ...
]
```

## iSCSI LUNs

### The LUN object

```
{
  "id": 1,
  "size": 1,
  "comment": "my lun"
}
```

### Attribute Definitions

Name	Type	Description
<b>id</b>	Integer	The ID of the LUN. Must be unique within a target.
<b>size</b>	Integer	The size of the LUN, in GB.
<b>comment</b>	String	A short comment / description of the LUN.

### Create LUN

**POST** `/api/v1/iscsi/targets/<target>`

Create a LUN under the specified target.

### Path Parameters

<b>target</b>	The name of the target the LUN should be created for.
---------------	---

### Request Body

The **LUN object**. ID and size are required.

## Sample Request

```
POST /api/v1/iscsi/targets/mytarget HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "id": 1,
  "size": 1,
  "comment": "my lun"
}
```

## Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/iscsi/targets/mytarget/1
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

## Modify LUN

PUT */api/v1/iscsi/targets/<target>/<lun>*

Change the ID or comment of the LUN. To change the size of a LUN you must use the Resize LUN operation.

### Path Parameters

<b>target</b>	The name of the target that has the LUN.
<b>lun</b>	The ID of the LUN.

### Request Body

**The LUN object.** ID and comment are optional; ID is the new ID of the LUN. Size is ignored. Any parameters not provided remain unchanged.

## Sample Request

```
PUT /api/v1/iscsi/targets/mytarget/1 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "id": 2
}
```

This sample request changes the ID of the LUN from 1 to 2. The other LUN configuration remains unchanged.

## Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

## Resize LUN

**PUT** `/api/v1/iscsi/targets/<target>/<lun>?resize=<size>`

Change the size of a LUN. Reducing the LUN size is not supported.



**Warning:** Never attempt to reduce the size of an existing LUN; it would potentially result in data loss or data corruption.

### Path Parameters

<b>target</b>	The name of the target that has the LUN.
<b>lun</b>	The ID of the LUN.

### Query Parameters

<b>resize</b>	Required. The new size of the LUN, specified in GB.
---------------	---

### Sample Request

```
PUT /api/v1/iscsi/targets/mytarget/1?resize=2 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

This sample request changes the size of the LUN to 2 GB.

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete LUN

**DELETE** `/api/v1/iscsi/targets/<target>/<lun>`

Delete a LUN, together with all its content.



**Warning:** This operation will delete existing data and should be used with caution.

### Path Parameters

<b>target</b>	The name of the target that has the LUN.
<b>lun</b>	The ID of the LUN.

### Sample Request

```
DELETE /api/v1/iscsi/targets/mytarget/1 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## iSCSI Initiator Groups

### The iSCSI Initiator Group Object

```
{
  "name": "myInitiatorGroup",
  "accessFilter": "192.168.1.1/16 172.16.0.0/24"
}
```

### Attribute Definitions

Name	Type	Description
<b>name</b>	String	The name of the iSCSI Initiator Group.
<b>accessFilter</b>	String	All the IP addresses (optionally, subnet masks can be added) that belong to this Initiator Group, separated by spaces. If an iSCSI Target is associated with this Initiator Group, only Initiators having the IP address in this Initiator Group will be able to log on to the iSCSI Target. If an IP matches any of the entries in the filter, it is considered a part of the Initiator Group. Example: "172.16.2.24 192.168.1.0/24 172.16.0.0/16" Only initiators having the IP address either 172.16.2.24 or of the form 192.168.1.* (subnet mask 255.255.255.0) or of the form 172.16.*.* (subnet mask 255.255.0.0) will be able to log on to an iSCSI Target that is associated with this Initiator Group.

### Create Initiator Group

POST */api/v1/iscsi/initiatorgroups*

Create a new Initiator Group.

#### Request Body

**The iSCSI Initiator Group object.** The "name" parameter is required. A missing "accessFilter", or a value of "0.0.0.0/0", or a value of "" (empty string), are all equivalent and have the effect that the Initiator Group does not impose any restrictions on IP addresses (all clients will be able to log on to a Target that is associated with the Initiator Group).

#### Sample Request

```
POST /api/v1/iscsi/initiatorgroups HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "myInitiatorGroup",
  "accessFilter": "172.16.0.0/16"
}
```

#### Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/iscsi/initiatorgroups/myInitiatorGroup
x-cv-request-id: 880c0b32-9ad0-4f8e-b338-3e48bacdd75e
```

## Modify Initiator Group

PUT /api/v1/iscsi/initiatorgroups/<initiator group>

Modify an existing Initiator Group.

### Path Parameters

<b>initiator group</b>	The name of the Initiator Group to be modified.
------------------------	---

### Request Body

The **iSCSI Initiator Group object**. Both "name" and "accessFilter" parameters are optional. Any parameters not provided remain unchanged.

### Sample Request

```
PUT /api/v1/iscsi/initiatorgroups/myInitiatorGroup HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "myInitiatorGroup2",
  "accessFilter": "172.16.0.0/16"
}
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete Initiator Group

DELETE /api/v1/iscsi/initiatorgroups/<initiator group>

Delete an existing Initiator Group.

### Path Parameters

<b>initiator group</b>	The name of the Initiator Group to be deleted.
------------------------	--

### Sample Request

```
DELETE /api/v1/iscsi/initiatorgroups/myInitiatorGroup HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Initiator Group

GET /api/v1/iscsi/initiatorgroups/<initiator group>

Retrieve information about an existing Initiator Group.

### Path Parameters

<b>initiator group</b>	The name of the Initiator Group.
------------------------	----------------------------------

### Response Body

The [iSCSI Initiator Group object](#).

### Sample Request

```
GET /api/v1/iscsi/initiatorgroups/myInitiatorGroup HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 59
Content-Type: application/json; charset=UTF-8
x-cv-request-id: f90960f9-148f-478c-bd55-c94ed545170d
{
  "name": "myInitiatorGroup",
  "accessFilter": "192.168.1.1/16"
}
```

## List Initiator Groups

GET /api/v1/iscsi/initiatorgroups

List all existing Initiator Groups.

### Response Body

A JSON array of [iSCSI Initiator Group objects](#).

### Sample Request

```
GET /api/v1/iscsi/initiatorgroups/ HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 118
Content-Type: application/json; charset=UTF-8
x-cv-request-id: b7ddc00c-4124-47e0-92c7-47d1a4979264
[
  {
    "name": "myInitiatorGroup2",
    "accessFilter": "0.0.0.0/0"
  },
  {
    "name": "myInitiatorGroup3",
    "accessFilter": "172.16.14.0/24"
  }
]
```

## User & Group Management

Operations for user and group management. Create, modify, delete, and get a user; list existing users.  
Create, modify, delete, and get a group; list existing groups.

### Permissions

<i>Name</i>	<i>Type</i>	<i>Description</i>	<i>Status</i>
<b>SET_SHARE</b>	Bool	Create/modify/delete directories and shares.	Optional, default false
<b>GET_SHARE</b>	Bool	Get/list directories and shares.	Optional, default false
<b>SET_POLICY</b>	Bool	Create/modify/delete snapshot, file and quota policies.	Optional, default false
<b>GET_POLICY</b>	Bool	Get/list snapshot, file and quota policies.	Optional, default false
<b>TAKE_SNAPSHOT</b>	Bool	Take manual snapshot.	Optional, default false
<b>SET_USER_GROUP</b>	Bool	Create/modify/delete users and groups	Optional, default false
<b>GET_USER_GROUP</b>	Bool	Get/list users and groups.	Optional, default false
<b>SET_ISCSI</b>	Bool	Create/modify/delete iSCSI targets and LUNs	Optional, default false
<b>GET_ISCSI</b>	Bool	Get/list iSCSI targets and LUNs.	Optional, default false

## Users

### The User object

```
{
  "name": "myuser",
  "password": "mypassword",
  "enable": true,
  "linuxUID": 1000,
  "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
  "mainGroup": "Administrators",
  "additionalGroups": ["users"],
  "s3SecretKey": "secretkey",
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

## Attribute Definitions

<i>Name</i>	<i>Type</i>	<i>Description</i>
<b>name</b>	String	The name of the user. Must be unique in the scope of the file system.
<b>password</b>	String	The password of the user.
<b>enable</b>	Bool	If true, the user is allowed to login.
<b>linuxUID</b>	Integer	The Linux user ID.
<b>windowsSID</b>	String	The Windows Security Identifier.
<b>mainGroup</b>	String	The name of the user's primary group.
<b>additionalGroups</b>	Array	A list of groups the user is a member of.
<b>s3SecretKey</b>	String	The user's S3 secret key, used for accessing the Amazon S3 file share.
<b>permissions</b>	Object	A set of attributes with Boolean values that configure the user's access permissions on the file system.

Valid attributes are:

- \* SET\_SHARE (create/modify/delete directories and shares)
- \* GET\_SHARE (get / list directories and shares)
- \* SET\_POLICY (create/modify/delete snapshot, file, quota and antivirus policies)
- \* GET\_POLICY (get/list snapshot, file, quota and antivirus policies)
- \* TAKE\_SNAPSHOT (take manual snapshot)
- \* SET\_USER\_GROUP (create/modify/delete users and groups)
- \* GET\_USER\_GROUP (get/list users and groups)
- \* SET\_ISCSI (create/modify/delete iSCSI targets and LUNs)
- \* GET\_ISCSI (get/list iSCSI targets and LUNs)
- \* GET\_SYSTEM\_REPORTS (get System performance and audit reports)
- \* GET\_FILESYSTEM\_REPORTS (get Filesystem audit reports)

## Create User

POST */api/v1/users*

Create a user.

### Request Body

The **User object**. Name, password and mainGroup are required. WindowsSID is ignored.

### Sample Request

```
POST /api/v1/users HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "myuser",
  "password": "mypassword",
  "enable": true,
  "linuxUID": 1000,
  "mainGroup": "Administrators",
  "additionalGroups": ["users"],
  "s3SecretKey": "secretkey",
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

### Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/users/myuser
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Modify User

PUT */api/v1/users/<user>*

Modify an existing user.

### Path Parameters

<b>user</b>	The name of the user.
-------------	-----------------------

### Request Body

The **User object**. Name, password and mainGroup are optional. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/users/myuser HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "myuser2",
  "password": "mypassword2"
}
```

This sample request renames the user from myuser to myuser2, and changes the password from mypassword to mypassword2. The other user configuration remains unchanged.

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Delete User

DELETE */api/v1/users/<user>*

Delete a user.

### Path Parameters

<b>user</b>	The name of the user.
-------------	-----------------------

### Sample Request

```
DELETE /api/v1/users/myuser HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get User

GET */api/v1/users/<user>*

Retrieve a user.

### Path Parameters

<b>user</b>	The name of the user.
-------------	-----------------------

### Response Body

The User object.

### Sample Request

```
GET /api/v1/users/myuser HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "name": "myuser",
  "password": "mypassword",
  "enable": true,
  "linuxUID": 1000,
  "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
  "mainGroup": "Administrators",
  "additionalGroups": ["users"],
  "s3SecretKey": "secretkey",
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

## List Users

GET */api/v1/users*

List all users.

### Response Body

A JSON array of [User objects](#).

### Sample Request

```
GET /api/v1/users HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

[
  {
    "name": "myuser",
    "password": "mypassword",
    "enable": true,
    "linuxUID": 1000,
    "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
    "mainGroup": "Administrators",
    "additionalGroups": ["users"],
    "s3SecretKey": "secretkey",
    "permissions": {
      "SET_SHARE": true,
      "GET_SHARE": true,
      "SET_POLICY": true,
      "GET_POLICY": true,
      "TAKE_SNAPSHOT": true,
      "SET_USER_GROUP": true,
      "GET_USER_GROUP": true,
      "SET_ISCSI": true,
      "GET_ISCSI": true,
      "GET_SYSTEM_REPORTS": true,
      "GET_FILESYSTEM_REPORTS": true
    }
  },
  ...
]
```

## Groups

### The Group object

```
{
  "name": "users",
  "linuxGID": 1000,
  "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

### Attribute Definitions

Name	Type	Description
<b>name</b>	String	The name of the group. Must be unique in the scope of the file system.
<b>linuxGID</b>	Integer	The Linux group ID.
<b>windowsSID</b>	String	The Windows Security Identifier.
<b>permissions</b>	Object	A set of attributes with Boolean values that configure the group's access permissions on the file system.

Valid attributes are:

- \* SET\_SHARE (create/modify/delete directories and shares)
- \* GET\_SHARE (get / list directories and shares)
- \* SET\_POLICY (create/modify/delete snapshot, file, quota and antivirus policies)
- \* GET\_POLICY (get/list snapshot, file, quota and antivirus policies)
- \* TAKE\_SNAPSHOT (take manual snapshot)
- \* SET\_USER\_GROUP (create/modify/delete users and groups)
- \* GET\_USER\_GROUP (get/list users and groups)
- \* SET\_ISCSI (create/modify/delete iSCSI targets and LUNs)
- \* GET\_ISCSI (get/list iSCSI targets and LUNs)
- \* GET\_SYSTEM\_REPORTS (get System reports via the Rest-API)
- \* GET\_FILESYSTEM\_REPORTS (get Filesystem reports via the Rest-API)

## Create Group

POST /api/v1/groups

Create a group.

### Request Body

The **Group object**. Name is required. WindowsSID is ignored.

### Sample Request

```
POST /api/v1/groups HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "users",
  "linuxGID": 1000,
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

### Sample Response

```
HTTP/1.1 201 Created
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
Location: http://<node>:81/api/v1/groups/users
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Modify Group

PUT /api/v1/groups/<group>

Modify an existing user.

### Path Parameters

<b>group</b>	The name of the group.
--------------	------------------------

### Request Body

The **Group object**. Name is optional. Any parameters not provided remains unchanged.

### Sample Request

```
PUT /api/v1/groups/users HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "name": "users2"
}
```

This sample request renames the group from users to users2. The other user configuration remains unchanged.

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

### Delete Group

**DELETE** */api/v1/groups/<group>*

Delete a group.

### Path Parameters

---

<b>group</b>	The name of the group.
--------------	------------------------

---

### Sample Request

```
DELETE /api/v1/groups/users HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e
```

## Get Group

GET /api/v1/groups/<group>

Retrieve a group.

### Path Parameters

<b>group</b>	The name of the group.
--------------	------------------------

### Response Body

The Group object.

### Sample Request

```
GET /api/v1/groups/users HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

{
  "name": "users",
  "linuxGID": 1000,
  "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
  "permissions": {
    "SET_SHARE": true,
    "GET_SHARE": true,
    "SET_POLICY": true,
    "GET_POLICY": true,
    "TAKE_SNAPSHOT": true,
    "SET_USER_GROUP": true,
    "GET_USER_GROUP": true,
    "SET_ISCSI": true,
    "GET_ISCSI": true,
    "GET_SYSTEM_REPORTS": true,
    "GET_FILESYSTEM_REPORTS": true
  }
}
```

## List Groups

GET /api/v1/groups

List all groups.

### Response Body

A JSON array of [Group objects](#).

### Sample Request

```
GET /api/v1/groups HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: 880c0b32-9ad0-4fbe-b338-3e48bacdd75e

[
  {
    "name": "users",
    "linuxGID": 1000,
    "windowsSID": "S-1-5-21-1634518050-1170479241-3746985662-1000",
    "permissions": {
      "SET_SHARE": true,
      "GET_SHARE": true,
      "SET_POLICY": true,
      "GET_POLICY": true,
      "TAKE_SNAPSHOT": true,
      "SET_USER_GROUP": true,
      "GET_USER_GROUP": true,
      "SET_ISCSI": true,
      "GET_ISCSI": true,
      "GET_SYSTEM_REPORTS": true,
      "GET_FILESYSTEM_REPORTS": true
    }
  },
  ...
]
```

## Actions

### Take Snapshot

POST `/api/v1/actions/snapshot`

Take a manual snapshot of a directory. Note that the directory must have been configured with a snapshot policy, however it is not required that the schedule type “manually” is included.

#### Request Headers

<b>x-cv-cwd-id</b>	Optional. The ID of the directory the path in the request body is relative to.
--------------------	--

#### Request Body

Name	Type	Description	Status
<b>path</b>	String	The path of the directory the snapshot should be applied to, relative to the current working directory.	Required
<b>expireDate</b>	String	When the snapshot will expire, as UTC time (ex. 2016-10-31 00:00:00). After the snapshot expires, it is removed.	Required

#### Sample Request

```
POST /api/v1/actions/snapshot HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
Content-Length: <length>

{
  "path": "path/to/directory",
  "expireDate": "2016-10-31 00:00:00"
}
```

#### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:01:37 GMT
Server: Compuverde Management
Content-Length: 0
x-cv-request-id: 880c0b32-9ad0-4fbc-b338-3e48bacdd75e
```

# Reports

## The Report

A report is a collection of text data, describing the state of a Compuverde system (storage node) or of a Compuverde filesystem, at a certain date.

Each report is generated by a specific storage node in the Compuverde cluster (the one that the REST-API request is directed to), and contains information generated by that node only.

There are two categories of reports:

- **System report** - contains information relevant only to the node that sends the report, e.g. the amount of free memory on the node, or the fact that a storage disk of the node was brought offline.
- **Filesystem report** - contains information relevant to a filesystem, e.g. a file share was created, or a quota policy on a folder was modified. All nodes in the cluster have the same view of this type of information.

## System reports

A System report is a collection of CSV-formatted text data that describes the state of a Compuverde system (storage node), at a certain date.

The report contains an initial header line and a number of rows. The values are delimited by the comma character (',').

The report is produced from the log files generated by each Compuverde storage node. Note that deleting the log files for a specific date from the storage node will result in reports for that date becoming permanently unavailable.

There are two sub-types of System reports: Performance and Audit.

### Performance System report

A Performance System report describes the performance state of a Compuverde system (storage node), at a certain date. Each row in the report shows the performance state of the system at a certain time, e.g. the instant CPU usage on the node, or the number of Read/Write operations performed since the previous row in the report was generated. The Compuverde logging system generates every 5 minutes a new row that describes the current performance state of the node.

**GET** `/api/v1/reports/system/performance/<date>`

Retrieve the Performance System report for the respective date.

### Path Parameters

<b>date</b>	The date of the report, in the format: yyyyMMdd
-------------	---

### Response Body

The Performance System report.

### Sample Request

```
GET /api/v1/reports/system/performance/20180115 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```



<b>Write Ops</b>	The amount of write operations that were performed via all active protocols (e.g. SMB, NFS), since the previous row had been generated
<b>Write Data (MB)</b>	The amount of data, in MB, that was transferred as a result of write operations via all active protocols (e.g. SMB, NFS), since the previous row had been generated
<b>Writes/sec</b>	The amount of write operations per second that were performed via all active protocols (e.g. SMB, NFS), since the previous row had been generated
<b>Write Avg Latency (ms)</b>	The average response time, in milliseconds, of all write operations that were performed via all active protocols (e.g. SMB, NFS), since the previous row had been generated
<b>Write Max Latency (ms)</b>	The maximum response time, in milliseconds, of all write operations that were performed via all active protocols (e.g. SMB, NFS), since the previous row had been generated
<b>NFS Ops</b>	The amount of operations that were performed via the NFS protocol, since the previous row had been generated
<b>NFS Ops/sec</b>	The amount of operations per second that were performed via the NFS protocol, since the previous row had been generated
<b>NFS Avg Latency (ms)</b>	The average response time, in milliseconds, of all operations that were performed via the NFS protocol, since the previous row had been generated
<b>NFS Max Latency (ms)</b>	The maximum response time, in milliseconds, of all operations that were performed via the NFS protocol, since the previous row had been generated
<b>SMB Ops</b>	The amount of operations that were performed via the SMB protocol, since the previous row had been generated
<b>SMB Ops/sec</b>	The amount of operations per second that were performed via the SMB protocol, since the previous row had been generated
<b>SMB Avg Latency (ms)</b>	The average response time, in milliseconds, of all operations that were performed via the SMB protocol, since the previous row had been generated
<b>SMB Max Latency (ms)</b>	The maximum response time, in milliseconds, of all operations that were performed via the SMB protocol, since the previous row had been generated
<b>iSCSI Ops</b>	The amount of operations that were performed via the iSCSI protocol, since the previous row had been generated
<b>iSCSI Ops/sec</b>	The amount of operations per second that were performed via the iSCSI protocol, since the previous row had been generated
<b>iSCSI Avg Latency (ms)</b>	The average response time, in milliseconds, of all operations that were performed via the iSCSI protocol, since the previous row had been generated
<b>iSCSI Max Latency (ms)</b>	The maximum response time, in milliseconds, of all operations that were performed via the iSCSI protocol, since the previous row had been generated

## Audit System report

An Audit System report describes administrative events that occurred on the Compuverde system (storage node), at a certain date. Each row in the report is an administrative event (e.g. a node was taken online/offline, a disk was taken online/offline). The Compuverde logging system generates a new row when the respective event occurs.

**GET** `/api/v1/reports/system/audit/<date>`

Retrieve the Audit System report for the respective date.

### Path Parameters

<b>date</b>	The date of the report, in the format: yyyyMMdd
-------------	---

### Response Body

The Audit System report.

## Sample Request

```
GET /api/v1/reports/system/audit/20180115 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

## Sample Response

```
Date,Time,Private IP,Event
2018-01-15,08:38,172.16.1.129,A request to take the node offline was received from 172.16.0.42
(grace period 00:30:00).
2018-01-15,08:41,172.16.1.129,A request to take the node online was received from 172.16.0.42.
2018-01-15,15:11,172.16.1.129,A request to take online the storage disk in slot 1 was received
from 172.16.0.42.
```

The significance of each column in the Audit System report is described in the following table.

<i>Name</i>	<i>Description</i>
<b>Date</b>	The date of the report
<b>Time</b>	The time when the row was generated by the storage node
<b>Private IP</b>	The Private IP address of the storage node that generated the report
<b>Event</b>	The administrative event that occurred on the storage node

### *Audit System report Events*

---

**Node was taken offline**

---

**Node was taken online**

---

**Disk was taken offline**

---

**Disk was taken online**

---

**Disk was retired**

## Filesystem reports

A Filesystem report describes the state of a Compuverde filesystem, at a certain date.

There are two types of Filesystem reports, the Audit Filesystem report and the DiskUsage Filesystem report.

### Audit Filesystem report

An Audit Filesystem report is a collection of CSV-formatted text data that describes administrative events that occurred on the Compuverde filesystem, at a certain date.

The report contains an initial header line and a number of rows. The values are delimited by the comma character (`,`).

Each row represents an administrative event (creation, modification or deletion of file shares, file/quota/snapshot/antivirus policies, iSCSI Targets/LUNs/Initiator Groups, users, user groups).

The report is produced from the log files generated by each Compuverde storage node. Note that deleting the log files for a specific date from the storage node will result in reports for that date becoming permanently unavailable.

```
GET /api/v1/reports/filesystem/audit/<date>
```

Retrieve the Audit Filesystem report for the respective date.

### Path Parameters

<b>date</b>	The date of the report, in the format: yyyyMMdd
-------------	---

## Response Body

The Audit Filesystem report.

### Sample Request

```
GET /api/v1/reports/filesystem/audit/20180115 HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

### Sample Response

```
Date,Time,Private IP,Event
2018-01-15,10:20,172.16.1.129,Administrator 'user' from 192.168.4.42 created share 'share1'.
Protocols: 'SMB, OpenStack, NNTP'. Absolute path: '/rest-shares/share1'
2018-01-15,10:21,172.16.1.129,Administrator from 172.16.0.42 created iSCSI Target 'target1'
2018-01-15,10:24,172.16.1.129,Administrator from 172.16.0.42 deleted file policy on folder
'subfolder1' at absolute path '/rest-shares/share1/subfolder1'
```

The significance of each column in the Audit Filesystem report is described in the following table.

<i>Name</i>	<i>Description</i>
<b>Date</b>	The date of the report
<b>Time</b>	The time when the row was generated by the storage node
<b>Private IP</b>	The Private IP address of the storage node that generated the report
<b>Event</b>	The administrative event that occurred on the filesystem

#### *Audit Filesystem report Event Summary*

**File share was created/modified/deleted**

**File/Quota/Snapshot/Antivirus policy was created/modified/deleted**

**iSCSI Target/LUN/InitiatorGroup was created/modified/deleted**

**User was created/modified/deleted**

**User Group was created/modified/deleted**

## DiskUsage Filesystem report

A DiskUsage Filesystem report gives information about the disk space occupied by a folder protected with a snapshot policy in the Compuverde filesystem.

### The Snapshot DiskUsage object

```
{
  "ordinal": 1,
  "name": "days.0",
  "createDate": "2018-02-12 09:34:02",
  "expireDate": "2018-03-19 09:34:00",
  "diskSize": 1404,
  "status": "complete"
}
```

## Attribute Definitions

<i>Name</i>	<i>Type</i>	<i>Description</i>
<b>ordinal</b>	Integer	A numerical label of the snapshot copy. Among all snapshot copies taken for a folder, the one with the smallest ordinal is the most recent.
<b>name</b>	String	The name of the folder where the snapshot copy can be accessed.
<b>createDate</b>	String	When the snapshot was created, as UTC time (ex. 2016-10-31 00:00:00).
<b>expireDate</b>	String	When the snapshot will expire, as UTC time (ex. 2016-10-31 00:00:00). After the snapshot expires, it is removed.
<b>diskSize</b>	Integer	<p>For a file, this attribute indicates the actual size, in bytes, of the file (not-written areas in the file excluded, erasure coding data included) and of the metadata associated with the file, as stored on the storage disk.</p> <p>For a directory, this attribute indicates the sum of the "diskSize" values for each file in the directory and all its subdirectories.</p> <p>Note: This attribute refers to a subdirectory under the .snapshot directory and indicates the total "diskSize" used by the respective subdirectory in order to store the required snapshot data.</p> <p>Note: Each snapshot is differential (only stores the data that differs from the previous snapshot).</p>
<b>status</b>	String	An attribute that describes the current status of the snapshot. Possible values are "complete" and "inprogress". A snapshot that is in progress is currently being built and cannot yet be used for reverting data.

## The Folder DiskUsage object

```
{
  "path": "/path/to/directory",
  "size": 4145493381,
  "usedSize": 4145493360,
  "diskSize": 6368710686,
  "snapshotsDiskSize": 1695,
  "totalDiskSize": 6368712381,
  "snapshots": [
    {
      "ordinal": 1,
      "name": "days.0",
      "createDate": "2018-02-12 09:34:02",
      "expireDate": "2018-03-19 09:34:00",
      "diskSize": 1404,
      "status": "complete"
    },
    {
      "ordinal": 2,
      "name": "days.1",
      "createDate": "2018-02-11 08:11:01",
      "expireDate": "2018-03-12 09:34:00",
      "diskSize": 291,
      "status": "complete"
    }
  ]
}
```

**Attribute Definitions**

<i>Name</i>	<i>Type</i>	<i>Description</i>
<b>path</b>	String	The path to the directory that is protected by the snapshot policy. The path is relative to the current working directory. If the path starts with "/", it is absolute (starts at the file system root).
<b>size</b>	Integer	For a file, this attribute indicates the total size, in bytes, of the file. For a directory, this attribute indicates the sum of the "size" values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the "size" of the .snapshot subfolder is not included in the value of this attribute.
<b>usedSize</b>	Integer	For a file, this attribute indicates the actual size, in bytes, of the data in the file (not-written areas in the file excluded). For a directory, this attribute indicates the sum of the "usedSize" values for each file in the directory and all its subdirectories. Note: due to thin-provisioning, "usedSize" is usually less than "size". If the directory has a .snapshot subfolder, the "usedSize" of the .snapshot subfolder is not included in the value of this attribute.
<b>diskSize</b>	Integer	For a file, this attribute indicates the actual size, in bytes, of the file (not-written areas in the file excluded, erasure coding data included) and of the metadata associated with the file, as stored on the storage disk. For a directory, this attribute indicates the sum of the "diskSize" values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the "diskSize" of the .snapshot subfolder is not included in the value of this attribute.
<b>snapshotsDiskSize</b>	Integer	The sum of the "diskSize" values for each existent snapshot (each snapshot is a subfolder of the .snapshot folder).
<b>totalDiskSize</b>	Integer	The sum of the "diskSize" and the "snapshotsDiskSize" for the folder.
<b>snapshots</b>	Array	An array of <a href="#">Snapshot DiskUsage objects</a> . Each element of the array represents an existent snapshot (a subfolder of the .snapshot folder).

**GET** /api/v1/reports/filesystem/diskusage/<path>

Retrieve the DiskUsage Filesystem report for the respective folder.

#### Path Parameters

<b>path</b>	The path of the directory protected with a snapshot policy, relative to the current working directory.
-------------	--

#### Response Body

The Folder DiskUsage object.

#### Sample Request

```
GET /api/v1/reports/filesystem/diskusage/path/to/directory HTTP/1.1
Host: <node>
Authorization: Basic <base64_encoded_string>
```

#### Sample Response

```
HTTP/1.1 200 OK
Date: Fri, 14 Oct 2016 12:05:32 GMT
Server: Compuverde Management
Content-Length: <length>
x-cv-request-id: c69a0b0c-236c-4372-8fc6-2caaf85551b8
x-cv-parent-id: 3b100000-0000-0000-1956-56df2b153a43

{
  "size": 4145493381,
  "usedSize": 4145493360,
  "diskSize": 6368710686,
  "snapshotsDiskSize": 1695,
  "totalDiskSize": 6368712381,
  "snapshots": [
    {
      "ordinal": 1,
      "name": "days.0",
      "createDate": "2018-02-12 09:34:02",
      "expireDate": "2018-03-19 09:34:00",
      "diskSize": 1404,
      "status": "complete"
    },
    {
      "ordinal": 1,
      "name": "days.0",
      "createDate": "2018-02-11 08:11:01",
      "expireDate": "2018-03-12 09:34:00",
      "diskSize": 291,
      "status": "complete"
    }
  ]
}
```

# Appendix

## Common Request Headers

---

<b>x-cv-request-id</b>	The unique ID of the request. Used for troubleshooting.
------------------------	---

---

## Errors

Any response with a 4xx or 5xx HTTP status code includes an Error object in the response.

### The Error object

```
{
  "code": 72,
  "error": "UserNotFound",
  "message": "UserNotFound"
}
```

## Attribute Definitions

<i>Name</i>	<i>Type</i>	<i>Description</i>
<b>code</b>	Integer	Uniquely identifies the error.
<b>error</b>	String	Human readable string of the numerical code.
<b>message</b>	String	Description of the error. For some errors, this has the same value as the error attribute.

---

The following table is a list of the errors:

<i>Code</i>	<i>Error</i>	<i>Description</i>	<i>HTTP Status Code</i>
<b>53</b>	AccessDenied	Access denied. The user doesn't have the required permissions, or the ID in the x-cv-cwd-id header is not valid for the current domain / tenant.	403 Forbidden
<b>11</b>	DirectoryNotEmpty	The specified directory is not empty.	409 Conflict
<b>101 or 102</b>	GroupAlreadyExists	A group with the specified name / GID already exists.	409 Conflict
<b>100</b>	GroupNotFound	The group does not exist.	404 Not Found
<b>Depends</b>	InternalServerError	An internal server error occurred. The code varies, depending on the type of server error.	500 Internal Server Error
<b>5</b>	InvalidArgument	The request contains invalid arguments. Malformed JSON document, JSON attributes that doesn't conform to the specification, or invalid query parameters.	400 Bad Request
<b>17</b>	InvalidCredentials	User authentication failed.	403 Forbidden
<b>15</b>	InvalidMessage	There isn't an operation that matches the request, e.g. the combination of HTTP method and request URI is invalid.	400 Bad Request
<b>132</b>	IscsiTargetAlreadyExists	A target with the specified name already exists.	409 Conflict
<b>131</b>	IscsiTargetNotFound	The target does not exist.	404 Not Found
<b>134</b>	IscsiLunAlreadyExists	A LUN with the specified ID already exists for that target.	409 Conflict
<b>133</b>	IscsiLunNotFound	The LUN does not exist.	404 Not Found
<b>51</b>	PathAlreadyExists	A directory already exists at the specified path.	409 Conflict
<b>50</b>	PathNotFound	The directory does not exist.	404 Not Found
<b>91</b>	PolicyAlreadyExists	The directory already has a configuration for the specified policy.	409 Conflict
<b>90</b>	PolicyNotFound	The directory does not have a configuration for the specified policy.	404 Not Found
<b>10</b>	RequestBodyTooLarge	The size of the request body is larger than what is allowed.	400 Bad Request
<b>81</b>	ShareAlreadyExists	A file share with the specified name already exists.	409 Conflict
<b>80</b>	ShareNotFound	The file share does not exist.	404 Not Found
<b>73 or 74</b>	UserAlreadyExists	A user with the specified name / UID already exists.	409 Conflict
<b>72</b>	UserNotFound	The user does not exist.	404 Not Found

## File encodings

DEFAULT
COPIES_3
COPIES_5
ERASURE_2_1
ERASURE_2_2
ERASURE_3_1
ERASURE_3_2
ERASURE_4_1
ERASURE_4_2
ERASURE_5_1
ERASURE_5_2
ERASURE_6_1
ERASURE_6_2
ERASURE_8_1
ERASURE_8_2
METRO_COPIES_3
METRO_ERASURE_2_1
METRO_ERASURE_2_2
METRO_ERASURE_3_1
METRO_ERASURE_3_2
METRO_ERASURE_4_1
METRO_ERASURE_4_2
METRO_ERASURE_5_1
METRO_ERASURE_5_2
METRO_ERASURE_6_1
METRO_ERASURE_6_2

## Tiers

ANY
DEFAULT
TIER_0
TIER_1
TIER_2
TIER_3
TIER_4