

# Dell EMC OneFS

Version 8.2.0

## API Reference

Copyright © 2001-2019 All rights reserved.

Published April 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.  
Published in the USA.

Dell EMC  
Hopkinton, Massachusetts 01748-9103  
1-508-435-1000 In North America 1-866-464-7381  
[www.DellEMC.com](http://www.DellEMC.com)

# CONTENTS

<b>Tables</b>		<b>5</b>
<b>Chapter 1</b>	<b>Introduction to this guide</b>	<b>7</b>
	About this guide.....	8
	About the Isilon SDK.....	8
	Isilon scale-out NAS overview.....	9
	Where to go for support.....	9
<b>Chapter 2</b>	<b>Introduction to the OneFS API</b>	<b>11</b>
	OneFS API overview.....	12
	OneFS API architecture.....	12
	OneFS API terminology .....	14
	OneFS API access.....	14
	HTTP methods.....	15
	OneFS API authentication.....	16
	HTTP Basic Authentication.....	16
	Session cookies.....	17
<b>Chapter 3</b>	<b>System configuration API</b>	<b>21</b>
	System configuration API overview.....	22
	Collection patterns.....	22
	API versions in OneFS.....	25
	API directory and browsing URIs.....	26
	OneFS API self-documentation.....	28
	System configuration API resources.....	30
	Authentication and access control.....	30
	Auditing.....	54
	Access zones.....	58
	NFS.....	60
	SMB.....	69
	FTP.....	73
	HTTP and HTTPS.....	73
	HDFS.....	74
	Isilon Swift.....	79
	Networking.....	80
	System jobs.....	86
	Cluster statistics.....	91
	FSA.....	94
	Events and alerts.....	97
	Snapshots.....	101
	NDMP backup and recovery.....	106
	SynclQ backup and recovery.....	111
	SmartLock.....	127
	Deduplication.....	129
	General cluster configuration.....	131
	Licensing.....	146
	Security hardening.....	148
	Upgrading OneFS.....	149

Cluster date and time.....	155
Managing SNMP settings.....	156
Hardware.....	157
File pools.....	159
Storage pools.....	162
CloudPools.....	168
SmartQuotas.....	173
Antivirus.....	177
Performance.....	180
Code samples for file system configuration.....	182

<b>Chapter 4</b>	<b>File system access API</b>	<b>183</b>
	File system access API overview.....	184
	Common response headers.....	184
	Common request headers.....	184
	Common namespace attributes.....	185
	Troubleshooting.....	186
	File system access operations.....	188
	Access points.....	188
	Directory operations.....	195
	File operations.....	210
	Access control lists.....	224
	Query operations.....	249
	SmartLock settings.....	254
	Code samples for file system access.....	257

# TABLES

1	Isilon SDK documentation and resources.....	8
2	Isilon SDK code samples.....	8

## TABLES

# CHAPTER 1

## Introduction to this guide

This is a reference guide to the OneFS API.

This guide provides an introduction to the OneFS API, and documents the system configuration API resource handlers and the file system API.

- [About this guide](#)..... 8
- [About the Isilon SDK](#)..... 8
- [Isilon scale-out NAS overview](#)..... 9
- [Where to go for support](#)..... 9

## About this guide

This guide describes how the Isilon OneFS application programming interface (API) provides access to cluster configuration and access to cluster data. This guide also provides a list of all available API resource URLs, HTTP methods, and parameter and object descriptions.

Your suggestions help us to improve the accuracy, organization, and overall quality of the documentation. Send your feedback to <https://www.research.net/s/isi-docfeedback>. If you cannot provide feedback through the URL, send an email message to [docfeedback@isilon.com](mailto:docfeedback@isilon.com).

## About the Isilon SDK

Information about the Isilon SDK documentation and resources.

The Isilon software development kit (Isilon SDK) is a collection of documentation, resources, tools, and code samples that allows the creation of applications for the Isilon family of products.

**Table 1** Isilon SDK documentation and resources

Resource	Location
EMC {code}	<a href="http://emccode.com/">http://emccode.com/</a>
EMC {code} blog	<a href="https://blog.emccode.com/">https://blog.emccode.com/</a>
EMC {code} CodeCommunity Slack channel, #isilon	<a href="http://community.emccode.com/">http://community.emccode.com/</a>
EMC Isilon community on ECN	<a href="http://community.emc.com/community/products/isilon">http://community.emc.com/community/products/isilon</a>
GitHub repository for the Isilon SDK	<a href="https://github.com/isilon">https://github.com/isilon</a>
Isilon SDK Info Hub	<a href="https://community.emc.com/docs/DOC-52521">https://community.emc.com/docs/DOC-52521</a>
Isilon space on EMC {code}	<a href="http://emccode.com/isilon">http://emccode.com/isilon</a>

**Table 2** Isilon SDK code samples

Resource	Location
Python Language Bindings for OneFS 7.2	<a href="https://github.com/Isilon/isilon_sdk_7_2_python">https://github.com/Isilon/isilon_sdk_7_2_python</a>
Stat Browser	<a href="https://github.com/Isilon/isilon_stat_browser%20">https://github.com/Isilon/isilon_stat_browser%20</a>

## Isilon scale-out NAS overview

The Isilon scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. Powered by the OneFS operating system, a cluster delivers a scalable pool of storage with a global namespace.

The unified software platform provides centralized web-based and command-line administration to manage the following features:

- A cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

## Where to go for support

If you have any questions about Isilon products, contact Isilon Technical Support.

Online Support	<ul style="list-style-type: none"> <li>• <a href="#">Live Chat</a></li> <li>• <a href="#">Create a Service Request</a></li> </ul>
Telephone Support	<ul style="list-style-type: none"> <li>• United States: 1-800-SVC-4EMC (1-800-782-4362)</li> <li>• Canada: 1-800-543-4782</li> <li>• Worldwide: 1-508-497-7901</li> <li>• Local phone numbers for a specific country are available at <a href="#">EMC Customer Support Centers</a>.</li> </ul>
Support registration or access	For questions about accessing <a href="#">EMC Customer Support</a> , email <a href="mailto:support@emc.com">support@emc.com</a> .
Isilon Info Hubs	For the list of Isilon info hubs, see the <a href="#">Isilon Info Hubs</a> page on the Isilon Community Network. Isilon info hubs organize Isilon documentation, videos, blogs, and user-contributed content into topic areas, making it easy to find content about subjects that interest you.

### Support for IsilonSD Edge

If you are running a free version of IsilonSD Edge, support is available through the [Isilon Community Network](#). If you purchased one or more IsilonSD Edge licenses, support is available through Isilon Technical Support, provided you have a valid support contract for the product.



# CHAPTER 2

## Introduction to the OneFS API

The OneFS application programming interface (API) is divided into two functional areas: One area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster.

- [OneFS API overview](#)..... 12
- [OneFS API access](#)..... 14
- [OneFS API authentication](#)..... 16

## OneFS API overview

The OneFS application programming interface (API) is divided into two functional areas: One area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster. You can send requests to the OneFS API through a Representational State Transfer (REST) interface, which is accessed through resource URIs and standard HTTP methods.

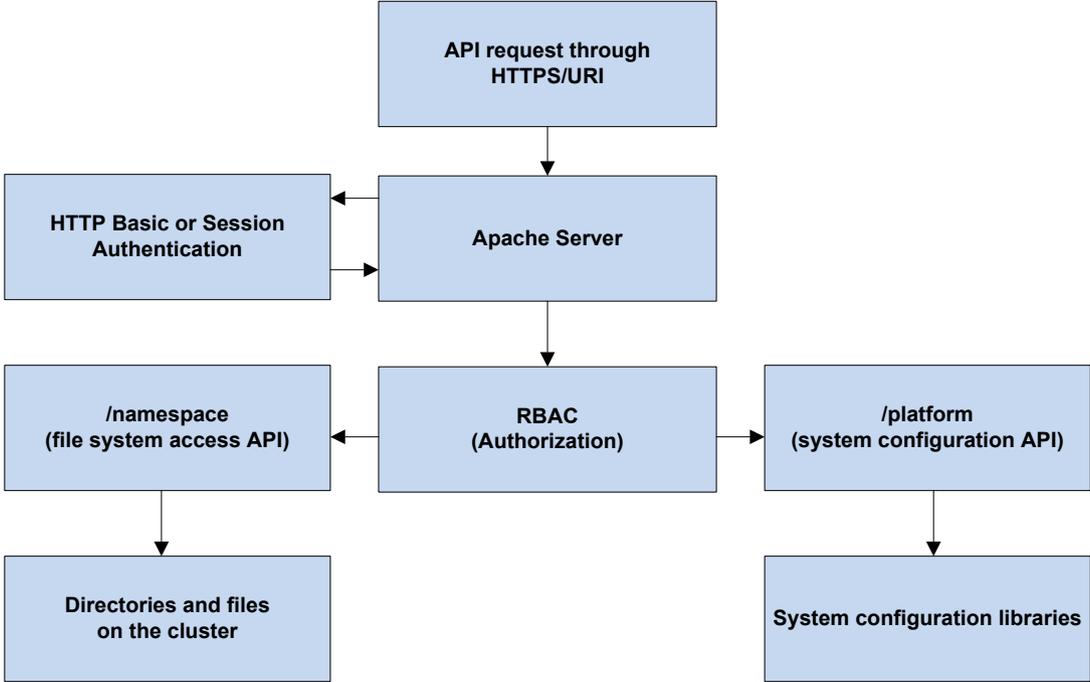
When an API request is sent over HTTPS to a cluster IP address or hostname, that request is authenticated and then authorized through role-based access control (RBAC). After the request is approved, access is provided to either file system configuration libraries or directories and files on the cluster.

## OneFS API architecture

When you send an HTTP request through the OneFS API, your request is sent to an Apache server. The Apache server verifies your username and password, either through HTTP Basic Authentication for single requests or through an established session to a single node for multiple requests over a period of time.

After the user account is authenticated, the privileges associated with the user account that generated the request are verified by role-based access control (RBAC). If the user account has the required privileges, the request enables access to files and directories on the cluster or to system configuration libraries, based on the resource URL provided in the request.

The following simplified diagram shows the basic flow of the two types of OneFS API requests:



## OneFS API terminology

The following terms are relevant to understanding the OneFS API.

Term	Definition
Access point	Root path of the URL to the file system. You can define an access point for any directory in the file system.
Collection	Group of objects of a similar type. For example, all of the user-defined quotas in the system make up a collection of quotas.
Data object	An object that contains content data, such as a file on the system.
Namespace	The file system structure on the cluster.
Object	Containers or data objects.  This term can refer to system configuration data that is created by users, or to a global setting on the system.  For example, a user-created object can be a file system snapshot, quota, share, export, logical unit, or synchronization policy.  An object can also be global settings on the system, such as default share settings, HTTP server settings, snapshot subsystem settings, and so on.
Resource	An object, collection, or function that you can access by a URI.

## OneFS API access

By applying standard HTTP methods to resource URIs, you can modify file system settings or access content on any node in a cluster through the OneFS API. When making multiple changes through the OneFS API, it is recommended that you send all requests to a single node to avoid configuration collisions.

OneFS API resource URIs are composed of the following components.

Component	Definition
my_cluster	The IPv4 or IPv6 address or hostname for the cluster
obj_port	The number of the port. The default setting is 8080
access_point	The name of the access point, such as <code>/ifs</code>
resource_path	The file path to the directory that you want to access
api_version	The version of the OneFS API

Component	Definition
collection_pattern	The namespace, collection name, and object ID of the resource that you want to configure

In both types of API requests, you can append query parameters to the end of resource URIs to refine your request. For example, you can revise a GET request to return only a set number of entries. In the following example, a maximum of 1,000 SMB shares are returned:

```
GET https://192.168.1.100:8080/platform/1/protocols/smb/shares&limit="1000"
```

### File system configuration API requests

For file system configuration API requests, the resource URI is composed of the following components:

```
https://<my_cluster>:<obj_port>/<api-version>/<collection_pattern>
```

For example, you can send a GET request to the following URI to retrieve all SMB shares on a cluster, where protocols is the namespace, smb is the collection name, and shares is the object ID:

```
GET https://192.168.1.100:8080/platform/1/protocols/smb/shares
```

### File system access API requests

For file system access APIs requests, the resource URI is composed of the following components:

```
https://<my_cluster>:<obj_port>/namespace/<access_point>/<resource_path>
```

For example, you can send a GET request to the following URI to view files that are stored in the folder at /ifs/users/folder1:

```
GET https://192.168.0.25:8080/namespace/ifs/users/folder1
```

Additionally, in file system access API requests, you can indicate a special operation in your request by appending a predefined keyword to the end of the resource URI. These keywords must be placed first in the argument list and must not contain any value. If these keywords are placed in any other position in the argument list, the keywords are ignored. Predefined keywords are `acl`, `metadata`, `worm`, and `query`. For example:

```
GET https://192.168.0.25:8080/namespace/ifs/users/folder1?acl
```

## HTTP methods

You can apply certain HTTP methods to resource URIs through the OneFS API to modify file system settings or to access file system content.

The following conditions apply to the HTTP methods available for the OneFS API:



Privileges are granted to the user on login to a cluster through the OneFS API, the web administration interface, SSH, or a console session. A token is generated for the user, which includes a list of all privileges granted to the user. Each URI, web-administration interface page, and command requires a specific privilege to view or modify the information available through any of these interfaces.

In some cases, privileges cannot be granted or there are privilege limitations.

- Privileges are not granted to users that do not connect to the System Zone during login or to users that connect through the deprecated Telnet service, even if they are members of a role.
- Privileges do not provide administrative access to configuration paths outside of the OneFS API. For example, the `ISI_PRIV_SMB` privilege does not grant a user the right to configure SMB shares using the Microsoft Management Console (MMC).
- Privileges do not provide administrative access to all log files. Most log files require root access.

## Session cookies

Establish a session by creating a session cookie through the session resource.

You can create a session cookie by sending credentials to a session service resource, which responds with a Set-Cookie header. The Set-Cookie header contains an authentication token that can then be sent with subsequent requests to provide immediate authentication.

### Session resource overview

You can set a session cookie that provides extended authentication to a single node.

#### Object properties

Property	Type	Description
username	String	Specifies the username for the account requesting access to the cluster.
password	String	Specifies the password for the username requesting access to the cluster.
services	Array	Specifies a list of services to obtain access to.
timeout_absolute	Integer	Retrieves the number of seconds before the session expires in a GET request.
timeout_inactive	Integer	Retrieves the number of seconds of inactivity before the session expires in a GET request.

#### Create a session

You can authenticate to a OneFS API resource URI by creating a session cookie and a session. When you create a session, you extend your authentication to a node for multiple requests over a period of time.

Session cookies are specific to a single node; all requests must be made to the same node from which the session cookie is obtained.

**Procedure**

1. Send a POST request to `/session/1/session` by specifying the JSON content-type in the request header and by specifying your username, password, and the service that you want to access in the request body. In the `services` property, specify `platform` for system configuration or `namespace` for file system access.

```
Content-type: application/json
Body:
{
  "username": "<string>",
  "password": "<string>",
  "services": ["platform" | "namespace"]
}
```

If the server validates your username and password, a Set-Cookie header is returned.

2. Obtain the `isid` value from the Set-Cookie header.

```
201 Created
Content-Length:104
Content-Type:application/json
Date:Fri, 22 Feb 2013 19:08:36 GMT
Set-Cookie:isid=12345678-abcd-1234-abcd-1234567890ab;
path=/;
HttpOnly; Secure
Response Body:
{
  "services": [
    "platform",
    "namespace"
  ],
  "timeout_absolute":14400,
  "timeout_inactive":900,
  "username":"user123"
}
```

This value will authenticate the session when you send a request through a session cookie.

**Results**

A session is created on the node on which the POST request was executed.

**Send a request for access through a session cookie**

Authenticate to a session through a session cookie.

**Before you begin**

Create a session and obtain an `isid` value from the Set-Cookie header.

You do not need to specify a WWW-AUTHENTICATE header.

**Procedure**

- Send a GET request to any API resource by typing the `isid` value in the Cookie request header.

If the server validates your username and password, access is granted.

**Results**

Authentication is granted for future requests on the specified node.

## Request example

```
GET 10.10.111.120:8080/platform/1/quotas
Cookie: isisessid=12345678-abcd-1234-abcd-1234567890ab
```

## Response example

```
200 OK
Content-Type:application/json
{
//JSON content
}
```

## Get information about the current session

You can send a GET request to obtain information about the current session. If the server validates your session cookie, the system returns a JSON document that contains information about the session. If the server does not validate the session ID contained in the cookie, the server returns an error message.

### Request syntax

```
GET /session/1/session
Cookie: isisessid=12345678-abcd-1234-abcd-1234567890ab
```

### Response body

If authorization is successful:

```
"username": <string>
"services": [<string>, ...]
"timeout_absolute": <integer>,
"timeout_inactive": <integer>

{
  "services":[
    "platform",
    "namespace"
  ],
  "timeout_absolute":14396,
  "timeout_inactive":900,
  "username":"user123"
}
```

If authorization fails:

```
401 Unauthorized
Content-Type: application/json
{
  "errors":[
    {
      "message":"authorization required"
    }
  ]
}
```

```
]
}
```

## Log out of a session

If you no longer need to stay authenticated to a node, you can log out of a session by deleting the session cookie. Session cookies are configured to expire automatically in 15 minutes after a period of inactivity or in 4 hours after an absolute period of time.

### Request syntax

```
DELETE /session/1/session
Cookie: isisessid=12345678-abcd-1234-abcd-1234567890ab
```

### Response body

If authorization is successful:

```
204 No Content
Set-Cookie:isisessid=deleted; path=/; Expires=Thu, 01-Jan-1970
00:00:01 GMT; HttpOnly; Secure
Content-Length: 0
```

If authorization fails:

```
401 Unauthorized
Content-Type: application/json
{
  "errors": [
    {
      "message": "authorization required"
    }
  ]
}
```

# CHAPTER 3

## System configuration API

You can access cluster configuration, status information, and file system content through objects and collections of objects. These objects and collections are exposed as resource URIs, which are represented as JavaScript Object Notation (JSON) formatted documents.

- [System configuration API overview](#).....22
- [System configuration API resources](#)..... 30
- [Code samples for file system configuration](#)..... 182

## System configuration API overview

You can access cluster configuration, status information, and file system content through objects and collections of objects. These objects and collections are exposed as resource URIs, which are represented as JavaScript Object Notation (JSON) formatted documents.

### Collection patterns

You can configure the file system on your cluster through the OneFS API by applying HTTP methods to resource URIs according to a set of collection patterns.

---

#### Note

The OneFS API supports a maximum URI length of 8,198 characters.

---

### Read a system object

You can read a system object that has a unique identifier through the GET method; the identifier is the name or system-generated id for that object.

Request pattern:

```
GET https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<object-id>
```

Response:

```
Content-Type: application/json
{
  "<object>": {
    "<property>": <value>,
    ...
  }
}
```

### Modify a system object

You can modify an object by sending one or more of the object properties through the PUT method. Only the specified properties are modified on the resource, which leaves all other properties in their current state.

Request pattern:

```
PUT https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<object-id>
Content-Type: application/json
{
  "<property>": <value>
  ...
}
```

**Response:**

```
{Standard JSON success or error response}
```

**Read an entire collection**

You can read all of the objects in a collection through the GET method.

**Request pattern:**

```
GET https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>
```

**Response:**

```
Content-Type: application/json
{
  "<collection>": [
    "<property>": <value>
    ...
  ]
}
```

**Read an object from a collection**

You can read an object in a collection through the GET method.

**Request pattern:**

```
GET https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>/<object-id>
```

**Response:**

```
Content-Type: application/json
{
  "<collection>": [
    "<property>": <value>
    ...
  ]
}
```

**Create an object in a collection**

You can create a user object in a collection through the POST method. The system responds with the final URI where the new object is located.

**Request pattern:**

```
POST https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>
Content-Type: application/json
{
  "<property>": <value>,
  ...
}
```

**Response:**

```
Location: https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>/<new-object-id>

Content-Type: application/json

{Standard JSON success or error response}
```

**Modify an object in a collection**

You can modify an object in a collection through the PUT method.

**Request pattern:**

```
PUT https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>/<object-id>

Content-Type: application/json
{
    "parameter_name": <value>
    ...
}
```

**Response:**

```
{Standard JSON success or error response}
```

**Delete an object from a collection**

You can delete a user object from a collection through the DELETE method.

**Request pattern:**

```
DELETE https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>/<object-id>
```

**Response:**

```
{Standard JSON success or error response}
```

**Filter a collection**

You can apply a filter to a collection to retrieve user objects that match some common criteria.

**Request pattern:**

```
GET https://<cluster-ip-or-host-name>:<port>/<api-version>/
<namespace>/<collection-name>?<parameter_name>=<match-pattern>&...
```

**Response:**

```
Content-Type: application/json
{
    "count": <integer>,
```

```
"<collection-name>": [
  {
    "<parameter-name>":
    <matched-value>,
    ...
  },
  ...
]
```

## API versions in OneFS

OneFS provides version control of API resources.

To use the latest API version, retrieve the latest API version at the URI `/platform/latest`. In OneFS 8.2, the API version is 7.

In OneFS 8.2, you can access the latest version of any configuration API resource at:

```
/platform/7/<path-to-resource>
```

Where resources have older versions, the older versions can be accessed at:

```
/platform/<version>/<path-to-resource>
```

The functionality of each resource is preserved, even with subsequent API versions. For example, if `/resource/x` is introduced in API version 1, updated in API version 3, and then updated again in API version 7, the following URI-to-resource mapping applies:

```
/platform/1/resource/x -> resource from API version 1
/platform/2/resource/x -> resource from API version 1
/platform/3/resource/x -> resource from API version 3
/platform/4/resource/x -> resource from API version 3
/platform/5/resource/x -> resource from API version 5
/platform/7/resource/x -> resource from API version 7
```

You are guaranteed that when you write code to a specific resource version, that behavior continues to function even if subsequent API versions are released.

These are the OneFS API versions and their corresponding releases:

OneFS version	API version
8.2	7
8.1.1	6
8.1	5
8.0.1	4
8.0	3
7.2.1	2
7.2	1

In future OneFS releases, when the configuration API version is incremented, the `/platform/latest` URI returns the latest version number. You are guaranteed to

access to the latest version of any resource by using the applicable version number in the resource URI.

Older versions of certain resources might be deprecated in the future. Large changes in the underlying OneFS system and configuration can cause certain fields or sets of fields to no longer be applicable. Isilon only deprecates resources when necessary. If an old version of a resource can function, it is accessible at its original API version number URI.

## API directory and browsing URIs

There are special URIs that you can use to get more information about system configuration API resources and their versions.

### List all API URIs

You can list all URIs for the system configuration API.

To retrieve a list of all system configuration API URIs:

```
https://<cluster-ip>:<port>/platform/?describe&list
```

The example above retrieves a separate listing for every update of each resource. For example, the resource for `/cluster/config` was introduced in API version 1 and updated in version 3, so `/platform/?describe&list` lists both:

```
"/1/cluster/config"
"/3/cluster/config"
```

---

#### Note

`/2/cluster/config` is also a valid URI, and will forward to the same resource as `/1/cluster/config`, because there were no updates to the resource in API version 2.

---

### List all URIs for a specific API version

You can list all the URIs for a specific version of the system configuration API.

To retrieve a list of all URIs available for the specified API version:

```
https://<cluster-ip>:<port>/platform/<version>/?describe&list
```

For example, the following retrieves all URIs available for API version 3:

```
https://<cluster-ip>:<port>/platform/3/?describe&list
```

This is an example of the output generated by the above query:

```
{
  "directory" :
  [
    "/3/antivirus/policies",
    "/3/antivirus/policies/<NAME>",
```

```

"/3/antivirus/quarantine/<PATH+>",
.
.
.
"/3/zones-summary",
"/3/zones-summary/<ZONE>",
"/3/zones/<ZONE>"
]
}

```

## List all URIs changed in a specific API version

You can list all the URIs that changed in a specific version of the system configuration API.

To retrieve a list of changed URIs that were updated for a specific API version:

```
https://<cluster-ip>:<port>/platform/changed/<version>
```

The previous example also returns a list of any removed URIs that were originally introduced or updated at the specified version, but that now have been permanently deprecated and can no longer be accessed.

---

### Note

In most cases there will be at least one new resource that provides the current functionality to replace any deprecated resources.

For example, to list all URIs that changed in API version 3:

```
https://<cluster-ip>:<port>/platform/changed/3
```

This is an example of the output generated by the above query:

```

{
  "changed" :
  [
    "/3/antivirus/policies",
    "/3/antivirus/policies/<NAME>",
    "/3/antivirus/quarantine/<PATH+>",
    .
    .
    .
    "/3/upgrade/cluster/upgrade",
    "/3/zones",
    "/3/zones/<ZONE>"
  ],
  "removed" : []
}

```

## List URI introduction or update version

You can retrieve a list of URIs detailing when a resource was introduced or updated in the system configuration API.

To retrieve a list of URIs representing the API versions in which a specified resource was introduced or updated:

```
https://<cluster-ip>:<port>/platform/updated/<path-to-resource>
```

For example, to retrieve information about when the API resource for OneFS audit settings was introduced or updated:

```
https://<cluster-ip>:<port>/platform/updated/audit/settings
```

This is an example of the output generated by the above query:

```
{
  "removed" : [],
  "updated" : [ "/1/audit/settings", "/3/audit/settings" ]
}
```

## List API resource versions

You can list all of the versions in which a resource exists.

To retrieve a list of URIs representing all API versions in which the specified resource exists as a valid resource in any form, including versions in which the resource was not updated, but excluding versions before the resource existed:

```
https://<cluster-ip>:<port>/platform/versions/<path-to-resource>
```

For example, to list the versions of the resource for NFS NLM sessions:

```
https://<cluster-ip>:<port>/platform/versions/protocols/nfs/nlm/sessions
```

This is an example of the output generated by the above query:

```
{
  "versions" :
  [
    "/1/protocols/nfs/nlm/sessions",
    "/2/protocols/nfs/nlm/sessions",
    "/3/protocols/nfs/nlm/sessions"
  ]
}
```

## OneFS API self-documentation

The system configuration API is completely self-documenting. You can access detailed information about each URI by appending the `?describe` query parameter. This self-

documentation includes URI descriptions, query arguments, allowable HTTP methods, and the request and response JSON representation structures.

To access the OneFS API self-documentation through any `/platform` resource URI, append the `?describe` query parameter as follows:

```
https://<cluster-ip>:<port>/platform/<version>/<path-to-resource>?describe
```

For example, the following will retrieve the API version 3 JSON schema documentation for upgrading nodes on a OneFS cluster:

```
https://<cluster-ip>:<port>/platform/3/upgrade/cluster/nodes?describe
```

This is an example of the output generated by the above query:

```
Resource URL: /platform/3/upgrade/cluster/nodes
  Overview: View information about nodes during an upgrade,
            rollback, or pre-upgrade assessment.
  Methods: GET
*****
Method GET: View information about nodes during an upgrade,
            rollback,
            or pre-upgrade assessment.
  URL: GET /platform/3/upgrade/cluster/nodes
There are no query arguments for this method.
GET response body schema:
{
  "type": "object",
  "description": "View information about nodes during an upgrade,
                rollback, or pre-upgrade assessment.",
  "properties": {
    "nodes": {
      .
      .
      .
    }
  }
}
```

You can retrieve a list of all of the resources for a feature by appending the `describe`, `list`, and `all` query parameters. The content is returned as mime-type `text/plain`. For example, to return a list of all resource URIs for snapshots, type the following URL:

```
https://<cluster-ip-or-host-name>:<port>/platform/3/snapshot/snapshots?describe&list&all
```

You can retrieve a list of all of the resource URIs on your cluster by typing the following URL:

```
https://<cluster-ip-or-host-name>:<port>/platform?describe&list
```

You can retrieve the JSON-formatted documents that are included in the self-documentation through any resource URI by appending the query parameters `describe` and `json`. This content is returned as mime-type `application/json`.

For example, to obtain the JSON-formatted document for the quotas resource, type the following URL:

```
https://<cluster-ip-or-host-name>:<port>/platform/1/quota/quotas?describe&json
```

If you include any values for either the `describe` or `json` parameters, the values are ignored.

## System configuration API resources

You can make requests through the OneFS API to access system configuration resources.

### Authentication and access control overview

OneFS supports several methods for ensuring that your cluster remains secure, including UNIX- and Windows-style permissions for data-level access control, access zones for data isolation, and role-based administration control access to system configuration settings.

OneFS is designed for a mixed environment that allows you to configure both Access Control Lists (ACLs) and standard UNIX permissions on the cluster file system.

---

#### Note

In most situations, the default settings are sufficient. You can configure additional access zones, custom roles, and permissions policies as necessary for your particular environment.

---

### Authentication classes

Authentication classes define values for the object properties in authentication resources.

#### <persona-id>

The <persona-id> class must be set in the following format: `"["user", "group", "SID", "UID", "GID"] : [<string>"]`, such as: `"GID:2003"` or `"user:johndoe"`.

#### <persona>

The <persona> class must be set with either the <persona-id> or the <type> and <name> parameters, as follows:

Property	Type	Description
id	<persona-id>	Specifies the serialized form of the persona.
type	String	Specifies the type of persona, which must be combined with a name. The type of the persona can be set to <code>user</code> , <code>group</code> , or <code>wellknown</code> .

Property	Type	Description
name	String	Specifies the persona name, which must be combined with a type.

**<user-id>**

The <user-id> class must be set in the following format: "["user", "SID", "UID"] : [<string>]", such as "UID:2283" or "user:john DOE".

**<user>**

The <user> class contains the following properties:

Property	Type	Description
dn	String	Specifies the distinguished name for the user.
dns_domain	String	Specifies the DNS domain.
domain	String	Specifies the domain the object is part of.
email	String	Specifies an email address.
enabled	Boolean	True if the user is enabled.
expired	Boolean	True if the password for the user has expired.
expiry	Integer	Specifies the Unix Epoch time at which the user account will expire.
gecos	String	Specifies the GECOS value, which is usually the full name.
generated_gid	Boolean	Indicates if the GID was generated.
generated_uid	Boolean	Indicates if the UID was generated.
gid	<persona>	Specifies the group ID.
home_directory	String	Specifies the home directory for the user.
id	String	Specifies the system ID given to the user or group. In a POST request, this value is the ID that refers to the item in the collection item resource path.
locked	Boolean	Specifies if the account is locked.
max_password_age	Integer	Specifies the maximum age in seconds allowed for the password before the password expires.
member_of	Array of [<persona>]	Specifies groups that this user or group are members of.
name	String	Specifies a user or group name.
password_expired	Boolean	Specifies whether the password has expired.
password_expires	Boolean	Specifies whether the password is allowed to expire.

Property	Type	Description
password_last_set	Integer	Specifies the last time the password was set.
primary_group_sid	<persona>	Specifies the security ID of the primary group for the user.
prompt_password_change	Boolean	Prompts a password change for the user at the next log in.
provider	String	Specifies the authentication provider the object belongs to.
sam_account_name	String	Specifies a user or group name.
shell	String	Specifies the path to the shell for the user.
sid	<persona>	Specifies the security identifier.
type	String	Indicates the object type.
uid	<persona>	Specifies the user ID.
upn	String	Specifies the principal name for the user.
user_can_change_password	Boolean	Specifies whether the user can change their own password.

**<group-id>**

The <group-id> class must be set in the following format: "["group", "SID", "GID"] : [<string>]", such as: "GID:2003" or "group:admins".

**<group>**

The <group> class contains the following properties:

Property	Type	Type	Property of
dn	String	Specifies the distinguished name for the group or object.	groups
dns_domain	String	Specifies the DNS domain for the object.	groups
domain	String	Specifies the domain of the group.	groups
generated_gid	Boolean	Indicates if the GID was generated.	groups
gid	<persona>	Specifies properties for the persona.	groups
id	String	Specifies the system ID given to the user or group. In a POST request, this value refers to the item in the collection item resource path.	groups
member_of	Array of [<persona>]	Specifies properties for groups that this user or group are members of.	groups
name	String	Specifies a user or group name.	groups
provider	String	Specifies an authentication provider.	groups
sam_account_name	String	Specifies a user or group name.	groups

Property	Type	Type	Property of
sid	<persona>	Specifies properties for the security identifier.	groups
type	String	Indicates the object type.	groups

**<privilege>**

The <privilege> class must be set as follows:

Property	Type	Description
id	String	Specifies the formal name of the privilege.
name	String	Specifies the name of the privilege.
read-only	Boolean	Determines if the privilege is specified as read-only.

**Authentication resources**

You can retrieve, create, modify, or delete authentication providers, users, groups, and other configurations and settings through authentication resource URIs.

**Auth access token resource**

Retrieve information about the access token for the authenticated user.

Operation	Method and URI
Get the security token for the currently authenticated user	GET <cluster-ip:port>/platform/1/auth/id
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/id?describe

**Auth user access resource**

Retrieve the access rights that a specified user has for a file.

Operation	Method and URI
Get the access rights that a user has for a specified file	GET <cluster-ip:port>/platform/1/auth/access/<user-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/access/<user-id>?describe

**Security objects cache resource**

Flush the security objects cache.

Operation	Method and URI
Flush objects from the security objects cache.	POST <cluster-ip:port>/platform/4/auth/cache

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/auth/cache?describe

### Auth user password resource

Enable users to change their password on a local authentication provider.

Operation	Method and URI
Change the password for a user	PUT <cluster-ip:port>/platform/1/auth/users/<user-id>/change_password
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/users/<user-id>/change_password?describe

### Auth users resource

Create, modify, delete, or retrieve information about users who are authenticated through a local authentication provider. Remote users are restricted to read-only operations.

Operation	Method and URI
Get all users	GET <cluster-ip:port>/platform/7/auth/users
Get one user	GET <cluster-ip:port>/platform/7/auth/users/<user-id>
Modify a user	PUT <cluster-ip:port>/platform/7/auth/users/<user-id>
Create a user	POST <cluster-ip:port>/platform/7/auth/users
Flush the users cache	DELETE <cluster-ip:port>/platform/7/auth/users
Delete a user	DELETE <cluster-ip:port>/platform/7/auth/users/<user-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/users?describe

### Auth users member of resource

Create, retrieve, or remove group membership for a user who is authenticated through a local authentication provider. Remote users are restricted to read-only operations.

Operation	Method and URI
Get the groups that a user is a member of	GET <cluster-ip:port>/platform/1/auth/users/<user-id>/member_of
Add a group membership for a user	POST <cluster-ip:port>/platform/1/auth/users/<user-id>/member_of

Operation	Method and URI
Remove a group membership from a user	DELETE <cluster-ip:port>/platform/1/auth/users/<user-id>/member_of/<group-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/users/<user-id>/member_of?describe

## Auth groups resource

Create, modify, delete, or retrieve information about groups that are authenticated through a local or remote authentication provider.

Operation	Method and URI
Get all groups	GET <cluster-ip:port>/platform/1/auth/groups
Flush the groups cache	DELETE <cluster-ip:port>/platform/1/auth/groups
Get a group	GET <cluster-ip:port>/platform/1/auth/groups/<group-id>
Create a group	POST <cluster-ip:port>/platform/1/auth/groups
Modify a group	PUT <cluster-ip:port>/platform/1/auth/groups/<group-id>
Delete a group	DELETE <cluster-ip:port>/platform/1/auth/groups/<group-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/groups?describe

## Auth groups members resource

Add, remove, or retrieve information about the members of a group who are authenticated through a local or remote authentication provider.

Operation	Method and URI
Get the members of a group	GET <cluster-ip:port>/platform/1/auth/groups/<group-id>/members
Add a member to a group	POST <cluster-ip:port>/platform/1/auth/groups/<group-id>/members
Remove a member from a group	DELETE <cluster-ip:port>/platform/1/auth/groups/<group-id>/members/<persona-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/groups/<group-id>/members?describe

## Auth netgroups resource

Retrieve information about the members of a netgroup that are specified through a local or remote authentication provider.

Operation	Method and URI
Get the members of a netgroup	GET <cluster-ip:port>/platform/1/auth/netgroups/<netgroup>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/netgroups/<netgroup>?describe

## Auth settings mapping resource

Modify or retrieve information about identity mapping settings.

Operation	Method and URI
Retrieve default identity mapping settings	GET <cluster-ip:port>/platform/1/auth/settings/mapping/defaults
Modify the default identity mapping settings	PUT <cluster-ip:port>/platform/1/auth/settings/mapping/defaults
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/settings/mapping/defaults?describe

## Auth mapping identities resource

Set, modify, delete, or retrieve information about identity mappings.

Operation	Method and URI
Retrieve identity mapping (UID, GID, SID, and on-disk) for the specified source persona	GET <cluster-ip:port>/platform/1/auth/mapping/identities/<identity>
Flush the identity mappings cache	DELETE <cluster-ip:port>/platform/1/auth/mapping/identities?remove=true
Flush the identity mapping	DELETE <cluster-ip:port>/platform/1/auth/mapping/identities/<identity>?remove=true
Manually set or modify the mapping between two personae	POST <cluster-ip:port>/platform/1/auth/mapping/identities
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/mapping/identities?describe
	GET <cluster-ip:port>/platform/1/auth/mapping/identities/<identity>?describe

## Auth mapping users rules resource

Retrieve the rules for user mapping. User mapping rules define how access tokens are created during authentication.

Operation	Method and URI
Get the user mapping rules	GET <cluster-ip:port>/platform/1/auth/mapping/users/rules
Replace all user mapping rules	PUT <cluster-ip:port>/platform/1/auth/mapping/users/rules
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/mapping/users/rules?describe

## Auth mapping users lookup resource

Retrieve the access token for any authenticated user.

Operation	Method and URI
Lookup a user through the user mapper	GET <cluster-ip:port>/platform/1/auth/mapping/users/lookup
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/mapping/users/lookup?describe

## Auth providers summary resource

Retrieve a summary of all of the authentication providers that are configured on the cluster.

Operation	Method and URI
Get a summary of authentication providers	GET <cluster-ip:port>/platform/3/auth/providers/summary
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/auth/providers/summary?describe

## Auth Kerberos providers resource

Create, modify, delete or retrieve information about Kerberos authentication providers.

Operation	Method and URI
Retrieve all Kerberos providers	GET <cluster-ip:port>/platform/7/auth/providers/krb5
Retrieve a Kerberos provider	GET <cluster-ip:port>/platform/7/auth/providers/krb5/<provider-id>
Create a new Kerberos provider	POST <cluster-ip:port>/platform/7/auth/providers/krb5

Operation	Method and URI
Modify a Kerberos provider	PUT <cluster-ip:port>/platform/7/auth/providers/krb5/<provider-id>
Delete a Kerberos provider	DELETE <cluster-ip:port>/platform/7/auth/providers/krb5/<provider-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/krb5?describe
	GET <cluster-ip:port>/platform/7/auth/providers/krb5/<provider-id>?describe

### Auth settings krb5 defaults resource

Retrieve or modify default Kerberos authentication settings.

Operation	Method and URI
Retrieve default Kerberos authentication settings	GET <cluster-ip:port>/platform/1/auth/settings/krb5/default
Modify the default Kerberos authentication settings	PUT <cluster-ip:port>/platform/1/auth/settings/krb5/default
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/settings/krb5/default?describe

### Auth settings krb5 realms resource

Create, modify, delete, or retrieve information about a Kerberos authentication realm.

Operation	Method and URI
Retrieve Kerberos authentication settings for realm	GET <cluster-ip:port>/platform/1/auth/settings/krb5/realms
Retrieve Kerberos authentication settings for a specific realm	GET <cluster-ip:port>/platform/1/auth/settings/krb5/realms/<realm name or ID>
Create a new Kerberos authentication realm	POST <cluster-ip:port>/platform/1/auth/settings/krb5/realms
Modify Kerberos authentication realm settings	PUT <cluster-ip:port>/platform/1/auth/settings/krb5/realms/<realm name or ID>
Delete a Kerberos authentication realm	DELETE <cluster-ip:port>/platform/1/auth/settings/krb5/realms/<realm name or ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/settings/krb5/realms?describe
	GET <cluster-ip:port>/platform/1/auth/settings/krb5/realms/<realm name or ID>?describe

## Auth settings krb5 domains resource

Create, modify, delete, or retrieve information about a Kerberos authentication domain.

Operation	Method and URI
Retrieve Kerberos authentication settings for domains	GET <cluster-ip:port>/platform/1/auth/settings/krb5/domains
Retrieve Kerberos authentication settings for a specific domains	GET <cluster-ip:port>/platform/1/auth/settings/krb5/domains/<domain name or ID>
Create a new Kerberos authentication domain	POST <cluster-ip:port>/platform/1/auth/settings/krb5/domains
Modify Kerberos authentication domain settings	PUT <cluster-ip:port>/platform/1/auth/settings/krb5/domains/<domain name or ID>
Delete a Kerberos authentication domain	DELETE <cluster-ip:port>/platform/1/auth/settings/krb5/domains/<domain name or ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/settings/krb5/domains?describe
	GET <cluster-ip:port>/platform/1/auth/settings/krb5/domains/<domain name or ID>?describe

## LDAP provider template resources

Retrieve a list of all LDAP provider templates.

Operation	Method and URI
Retrieve a list of all LDAP provider templates.	GET <cluster-ip:port>/platform/7/auth/ldap-templates
Retrieve a specific LDAP provider template.	GET <cluster-ip:port>/platform/7/auth/ldap-templates/<user-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/ldap-templates?describe

## Auth ADS providers domains resource

Retrieve information about the trusted domains of configured ADS providers.

Operation	Method and URI
List all trusted domains of ADS providers	GET <cluster-ip:port>/platform/7/auth/providers/ads/<id>/domains
View the trusted domains of a single ADS provider	GET <cluster-ip:port>/platform/7/auth/providers/ads/<id>/domains/<ads-domain>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/ads/<id>/domains?describe

Operation	Method and URI
	GET <cluster-ip:port>/platform/7/auth/providers/ads/<id>/domains/<ads-domain?describe

### Auth ADS providers resource

View, modify, create, or delete ADS providers.

Operation	Method and URI
List all ADS providers	GET <cluster-ip:port>/platform/7/auth/providers/ads
View an ADS provider	GET <cluster-ip:port>/platform/7/auth/providers/ads/<provider-id>
Create a new ADS provider	POST <cluster-ip:port>/platform/7/auth/providers/ads
Modify an ADS provider	PUT <cluster-ip:port>/platform/7/auth/providers/ads/<provider-id>
Delete an ADS provider	DELETE <cluster-ip:port>/platform/7/auth/providers/ads/<provider-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/ads?describe
	GET <cluster-ip:port>/platform/7/auth/providers/ads/<provider-id>?describe

### Auth ADS providers controllers resource

Retrieve information about all of the domain controllers for a trusted ADS domain.

Operation	Method and URI
Get all domain controllers for a trusted ADS domain	GET <cluster-ip:port>/platform/7/auth/providers/ads/<domain-id>/controllers
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/ads/<domain-id>/controllers?describe

### Auth ADS providers search resource

Perform searches within Active Directory service (ADS) providers for users, groups, and computer accounts.

Operation	Method and URI
Get objects that are searchable in domains	GET <cluster-ip:port>/platform/1/auth/providers/ads/<object>/search
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/providers/ads/<object>/search?describe

## Auth Duo provider resource

View or modify the Duo provider settings.

Operation	Method and URI
View a Duo provider	GET <cluster-ip:port>/platform/7/auth/providers/duo
Modify a Duo provider	PUT <cluster-ip:port>/platform/7/auth/providers/duo
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/duo?describe

## Auth file providers resource

Create, modify, delete, or retrieve information about an authentication file provider.

Operation	Method and URI
Get all file providers	GET <cluster-ip:port>/platform/7/auth/providers/file
Get one file provider	GET <cluster-ip:port>/platform/7/auth/providers/file/<provider-id>
Create a file provider	POST <cluster-ip:port>/platform/7/auth/providers/file
Modify a file provider	PUT <cluster-ip:port>/platform/7/auth/providers/file/<provider-id>
Delete a file provider	DELETE <cluster-ip:port>/platform/7/auth/providers/file/<provider-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/file?describe

## Auth LDAP providers resource

Create, modify, delete, or retrieve information about a Lightweight Directory Access Protocol (LDAP) provider.

Operation	Method and URI
Get all LDAP providers	GET <cluster-ip:port>/platform/7/auth/providers/ldap
Get one LDAP provider	GET <cluster-ip:port>/platform/7/auth/providers/ldap/<provider-id>
Create an LDAP provider	POST <cluster-ip:port>/platform/7/auth/providers/ldap
Modify an LDAP provider	PUT <cluster-ip:port>/platform/7/auth/providers/ldap/<provider-id>

Operation	Method and URI
Delete an LDAP provider	DELETE <cluster-ip:port>/platform/7/auth/providers/ldap/<provider-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/ldap?describe
	GET <cluster-ip:port>/platform/7/auth/providers/ldap/<provider-id>?describe

## Auth local providers resource

Create, modify, delete, or retrieve information about a local authentication provider.

Operation	Method and URI
Get all local providers	GET <cluster-ip:port>/platform/7/auth/providers/local
Get one local provider	GET <cluster-ip:port>/platform/7/auth/providers/local/<provider-id>
Create a local provider	POST <cluster-ip:port>/platform/7/auth/providers/local
Modify a local provider	PUT <cluster-ip:port>/platform/7/auth/providers/local/<provider-id>
Delete a local provider	DELETE <cluster-ip:port>/platform/7/auth/providers/local/<provider-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/local?describe
	GET <cluster-ip:port>/platform/7/auth/providers/local/<provider-id>?describe

## Auth NIS providers resource

Create, modify, delete, or retrieve information about an Network Information Service (NIS) authentication provider.

Operation	Method and URI
Get all NIS providers	GET <cluster-ip:port>/platform/7/auth/providers/nis
Get one NIS provider	GET <cluster-ip:port>/platform/7/auth/providers/nis/<provider-id>
Create an NIS provider	POST <cluster-ip:port>/platform/7/auth/providers/nis
Modify an NIS provider	PUT <cluster-ip:port>/platform/7/auth/providers/nis/<provider-id>
Delete an NIS provider	DELETE <cluster-ip:port>/platform/7/auth/providers/nis/<provider-id>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/providers/nis?describe
	GET <cluster-ip:port>/platform/7/auth/providers/nis/<provider-id>?describe

## Authentication settings ACLs resource

View or modify ACL policy settings and preset configurations.

Operation	Method and URI
List ACL policy settings	GET <cluster-ip:port>/platform/7/auth/settings/acls
Modify ACL policy settings	PUT <cluster-ip:port>/platform/7/auth/settings/acls
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/settings/acls?describe

## Authentication privileges resource

List all privileges.

Operation	Method and URI
List authentication privileges	GET <cluster-ip:port>/platform/7/auth/privileges
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/privileges?describe

## Auth roles resource

Create, modify, delete, or retrieve information about roles that are assigned to authenticated users.

Operation	Method and URI
Get all roles	GET <cluster-ip:port>/platform/7/auth/roles
Get one role	GET <cluster-ip:port>/platform/7/auth/roles/<role-id>
Create a role	POST <cluster-ip:port>/platform/7/auth/roles
Modify a role	PUT <cluster-ip:port>/platform/7/auth/roles/<role-id>
Delete a role	DELETE <cluster-ip:port>/platform/7/auth/roles/<role-id>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/roles?describe

### Auth roles members resource

Add, modify, remove, or retrieve information about the members assigned to a role.

Operation	Method and URI
Get the members of a role	GET <cluster-ip:port>/platform/7/auth/roles/<role>/members
Add a member to a role	POST <cluster-ip:port>/platform/7/auth/roles/<role-id>/members
Remove a member from a role	DELETE <cluster-ip:port>/platform/7/auth/roles/<role-id>/members/<persona-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/roles/<role-id>/members?describe

### Auth roles privileges resource

Add, modify, remove, or retrieve information about the privileges that are assigned to a role.

Operation	Method and URI
Get the privileges of a role	GET <cluster-ip:port>/platform/7/auth/roles/<id>/privileges
Add a privilege to a role	POST <cluster-ip:port>/platform/7/auth/roles/<id>/privileges
Remove a privilege from a role	DELETE <cluster-ip:port>/platform/7/auth/roles/<id>/privileges/<privilege-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/roles/<id>/privileges?describe

### Auth global settings resource

Retrieve or modify the global authentication settings on the cluster.

Operation	Method and URI
Get global settings	GET <cluster-ip:port>/platform/1/auth/settings/global
Modify global settings	PUT <cluster-ip:port>/platform/1/auth/settings/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/settings/global?describe

## Auth shells resource

Retrieve a list of user shells that are supported on the cluster.

Operation	Method and URI
Get a list of user shells that are supported on the cluster	GET <cluster-ip:port>/platform/1/auth/shells
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/shells?describe

## Auth wellknowns resource

Retrieve wellknown personas from the cluster.

Operation	Method and URI
Get all wellknown personas	GET <cluster-ip:port>/platform/1/auth/wellknowns
Get a wellknown persona	GET <cluster-ip:port>/platform/1/auth/wellknowns/<wellknown>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/auth/wellknowns?describe

## Configured TLS certificate authority resource

View, import, modify or delete one or more TLS certificate authorities.

Operation	Method and URI
Retrieve a list of all configured TLS certificate authorities.	GET <cluster-ip:port>/platform/7/certificate/authority
Retrieve a single configured TLS certificate authority.	GET <cluster-ip:port>/platform/7/certificate/authority/<authority-id>
Modify a TLS certificate authority.	PUT <cluster-ip:port>/platform/7/certificate/authority/<authority-id>
Delete a TLS certificate authority.	DELETE <cluster-ip:port>/platform/7/certificate/authority/<authority-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/certificate/authority?describe
	GET <cluster-ip:port>/platform/7/certificate/authority/<authority-id>?describe

## Configured TLS server certificate resources

Retrieve a list of all configured TLS server certificates.

Operation	Method and URI
Retrieve a list of all configured TLS server certificates.	GET <cluster-ip:port>/platform/4/certificate/server

Operation	Method and URI
Retrieve a single TLS server certificate.	GET <cluster-ip:port>/platform/4/certificate/server/<certificate-id>
Modify a TLS server certificate.	PUT <cluster-ip:port>/platform/4/certificate/server/<certificate-id>
Delete an TLS server certificate.	DELETE <cluster-ip:port>/platform/4/certificate/server/<certificate-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/certificate/server?describe
	GET <cluster-ip:port>/platform/4/certificate/server/<certificate-id>?describe

### Configured TLS certificate settings resource

Retrieve and modify system-wide TLS certificate settings.

Operation	Method and URI
View a configured TLS certificate setting.	GET <cluster-ip:port>/platform/7/certificate/settings
Modify a configured TLS certificate setting.	PUT <cluster-ip:port>/platform/7/certificate/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/certificate/settings?describe

### Authentication error resource

View authentication error details.

Operation	Method and URI
View authentication error	GET <cluster-ip:port>/platform/7/auth/errors/<error-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/auth/errors/<error-id>?describe

### ID resolution domains resource

List domain to path mappings for one or more domains.

Operation	Method and URI
List domain to path mappings	GET <cluster-ip:port>/platform/7/id-resolution/domains
List a path mapping for a specific domain	GET <cluster-ip:port>/platform/7/id-resolution/domains/<domain-id>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/id-resolution/domains/<domain-id>?describe

## ID resolution LINS resource

List LIN to path mappings

Operation	Method and URI
List LIN to path mappings	GET <cluster-ip:port>/platform/7/id-resolution/lins
List a specific LIN to path mapping	GET <cluster-ip:port>/platform/7/id-resolution/lins/<lin-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/id-resolution/lins/<lin-id>?describe

## ID resolution zones resource

List zone ID to zone name mappings.

Operation	Method and URI
List zone ID to zone name mappings	GET <cluster-ip:port>/platform/7/id-resolution/zones
List a specific zone ID to zone name mapping	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>?describe

## ID resolution zone groups resource

List GIDs/GSIDs to group name mappings.

Operation	Method and URI
List GID/GSID mappings for a zone to a group name	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/groups
List a specific GID/GSID mapping for a zone to a group	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/groups/<group-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/groups?describe

## ID resolution zones users resource

List mappings between UIDs/SIDs and user names.

Operation	Method and URI
List mappings between UIDs/SIDs and user names	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/users
List mappings between UIDs/SIDs and a specific user name	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/users/<user-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/id-resolution/zones/<zone-id>/users?describe

## Authentication API examples

You can see examples for some authentication API requests.

### Change a user password

Change a user password.

#### Request example

Specify both the new and old password.

```
PUT /platform/1/auth/users/USER:johndoe/change_password
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"new_password":"ABC12345",
 "old_password":"12345ABC"}
```

#### Response example

```
204 No Content
Content-type: text/plain
```

### Create a local group

Create a local group.

#### Request example

```
POST /platform/1/auth/group
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"name": "mygroup", "type": "GROUP"}
```

#### Response example

```
201 Created
Content-type: application/json

{
```

```
"id" : "SID:S-1-5-21-4224731515-2571109568-2823010237-1003"
}
```

## Modify a local group

Modify a local group.

### Request example

You must include the `force` parameter when modifying an authentication group.

```
PUT /platform/1/auth/groups/GROUP:mygroup?force=true
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"gid": 2004}
```

### Response example

```
204 No Content
Content-type: text/plain
```

## Add a member to a local group

Add a member to a local group.

### Request example

```
POST /platform/1/auth/groups/GROUP:mygroup/members
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"id": "USER:user01"}
```

### Response example

```
201 Created
Content-type: application/json

{"id" : "SID:S-1-5-21-4224731515-2571109568-2823010237-1003"}
```

## Create a user

Create a user and add the user to a local group.

### Request example

Create the user "user123" through the following request:

```
POST /platform/1/auth/users
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"name": "user123", "type": "USER"}
```

### Response example

```
201 Created
Content-type: application/json
```

```
{
  "id" : "SID:S-1-5-21-4224731515-2571109568-2823010237-1005"
}
```

**Request example**

Then, add "user123" to a group called "administrators" through the following request:

```
POST /platform/1/auth/groups/administrators/members
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"name": "user123", "type": "USER"}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id" : "SID:S-7-6-25-4784731515-2575609568-2323010237-2005"
}
```

**Modify a user**

Modify the properties for a user.

**Request example**

In this example, an email address is added for the user.

```
PUT /platform/1/auth/users/USER:user123
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"email": "user1@company.com"}
```

**Response example**

```
204 No Content
Content-type: application/json
```

**Join a domain**

Join an Active Directory server domain.

**Request example**

```
POST /platform/3/auth/providers/ads
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"name": "server.company.com",
 "user": "Administrator",
 "password": "abc123"}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id" : "SERVER.COMPANY.COM"
}
```

**Modify an ADS provider**

Modify an Active Directory authentication provider.

**Request example**

```
PUT /platform/1/auth/providers/ads/server1.company.com
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"home_directory_template":"/ifs/home/ads"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Create an LDAP provider**

Create an LDAP provider.

**Request example**

```
POST /platform/3/auth/providers/ldap
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"name":"ldaptest",
 "server_uris":["ldap://ldaptest.company.com"],
 "base_dn":"dc=company,dc=com"}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id" : "ldaptest"
}
```

**Modify an LDAP provider**

Modify an LDAP provider.

**Request example**

```
PUT /platform/3/auth/providers/ldap/ldaptest
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"name":"ldaptest2",
```

```
"server_uris":["ldap://ldaptest.company.com"],
"base_dn":"dc=company,dc=com"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Modify a local provider**

Modify a local provider.

**Request example**

```
PUT /platform/3/auth/providers/local/zone1
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
{"home_directory_template" : "/ifs/home/%Z/%U"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Create an authentication role**

Create an authentication role.

**Request example**

```
POST /platform/1/auth/roles
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
{"name":"dba"}
```

**Response example**

```
201 Created
Content-type: application/json
{
  "id" : "dba"
}
```

**Modify an authentication role**

Modify an authentication role.

**Request example**

```
PUT /platform/1/auth/roles/dba
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
{"name":"dba2"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Modify global authentication settings**

Modify global authentication settings.

**Request example**

```
PUT /platform/1/auth/settings/global
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"send_ntlmv2":"true"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Create a krb5 realm**

Create a krb5 authentication realm.

**Request example**

```
POST /platform/1/auth/settings/krb5/realms
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{"realm":"test_realm"}
```

**Response example**

```
201 Created
Content-type: application/json

{"id" : "2024839292"}
```

**Create a krb5 domain**

Create a krb5 authentication domain.

**Request example**

```
POST /platform/1/auth/settings/krb5/domains
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "domain":"test_domain",
  "realm":"test_realm"
}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id" : "29274939282"
}
```

**Modify krb5 domains**

Modify a krb5 authentication domain

**Request example**

```
PUT /platform/1/auth/settings/krb5/domains/test_domain
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "domain":"test_domain2",
  "realm":"test_realm4"
}
```

**Response example**

```
204 No Content
Content-type: application/json
```

**Modify krb5 settings**

Modify default krb5 authentication settings.

**Request example**

```
PUT /platform/1/auth/settings/krb5/defaults
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "dns_lookup_realm":"true"
  "dns_lookup_kdc":"true"
}
```

**Response example**

```
204 No Content
Content-type: application/json
```

**Auditing overview**

You can audit system configuration changes and protocol activity on an Isilon cluster. All audit data is stored and protected in the cluster file system and organized by audit topics.

Auditing can detect many potential sources of data loss, including fraudulent activities, inappropriate entitlements, and unauthorized access attempts. Customers in industries such as financial services, health care, life sciences, and media and

entertainment, as well as in governmental agencies, must meet stringent regulatory requirements developed to protect against these sources of data loss.

System configuration auditing tracks and records all configuration events that are handled by the OneFS HTTP API. The process involves auditing the command-line interface (CLI), web administration interface, and OneFS APIs. When you enable system configuration auditing, no additional configuration is required. System configuration auditing events are stored in the `config` audit topic directories.

Protocol auditing tracks and stores activity performed through SMB, NFS, and HDFS protocol connections. You can enable and configure protocol auditing for one or more access zones in a cluster. If you enable protocol auditing for an access zone, file-access events through the SMB, NFS, and HDFS protocols are recorded in the protocol audit topic directories. You can specify which events to log in each access zone. For example, you might want to audit the default set of `protocol` events in the System access zone but audit only successful attempts to delete files in a different access zone.

The audit events are logged on the individual nodes where the SMB, NFS, or HDFS client initiated the activity. The events are then stored in a binary file under `/ifs/.ifsvvar/audit/logs`. The logs automatically roll over to a new file after the size reaches 1 GB. The logs are then compressed to reduce space.

The `protocol` audit log file is consumable by auditing applications that support the Common Event Enabler (CEE).

## Audit resources

You can retrieve and modify OneFS audit topics and settings.

### Audit settings resource

Modify or retrieve information about audit settings per access zone.

Operation	Method and URI
Get audit settings	GET <cluster-ip:port>/platform/7/audit/settings
Modify audit settings	PUT <cluster-ip:port>/platform/7/audit/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/audit/settings?describe

### Audit global settings resource

Modify or retrieve information about audit global settings.

Operation	Method and URI
Get audit global settings	GET <cluster-ip:port>/platform/7/audit/settings/global
Modify audit global settings	PUT <cluster-ip:port>/platform/7/audit/settings/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/audit/settings/global?describe

## Audit topic resource

Modify or retrieve information about audit topics.

Operation	Method and URI
Get all audit topics	GET <cluster-ip:port>/platform/1/audit/topics
Get an audit topic	GET <cluster-ip:port>/platform/1/audit/topics/<name>
Modify an audit topic	PUT <cluster-ip:port>/platform/1/audit/topics/<name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/audit/topics?describe

## Audit progress resource

View the current audit log time.

Operation	Method and URI
Retrieve the current audit log time by node	GET <cluster-ip:port>/platform/4/audit/progress
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/audit/progress?describe

## Audit progress global resource

View the global audit log time.

Operation	Method and URI
Retrieve the current global audit log time	GET <cluster-ip:port>/platform/4/audit/progress/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/audit/progress/global?describe

## Audit API examples

You can see examples for some audit API calls.

## Enable protocol auditing

You can enable SMB protocol auditing on the system for specified zones.

### Request example

In the following example, protocol auditing is enabled for the "myZone" and "System" zones.

```
PUT /platform/1/audit/settings
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'audited_zones': ['myZone', 'System'],
  'protocol_auditing_enabled': True
}
```

### Response example

In the following example, the request was successful, and protocol auditing is enabled on the system for the specified zones. No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Enable configuration auditing

You can enable configuration auditing on the system.

### Request example

```
PUT /platform/1/audit/settings
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'config_auditing_enabled': True
}
```

### Response example

No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Modify an audit topic

You can modify an audit topic on the system.

### Request example

```
PUT /1/audit/topics/protocol
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "max_cached_messages": 1000
}
```

**Response example**

No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Access zones overview

Although the default view of an Isilon cluster is that of one physical machine, you can partition a cluster into multiple virtual containers called access zones. Access zones allow you to isolate data and control who can access data in each zone.

Access zones support configuration settings for authentication and identity management services on a cluster, so you can configure authentication providers and provision protocol directories such as SMB shares and NFS exports on a zone-by-zone basis. When you create an access zone, a local provider is automatically created, which allows you to configure each access zone with a list of local users and groups. You can also authenticate through a different authentication provider in each access zone.

To control data access, you associate the access zone with a groupnet, which is a top-level networking container that manages DNS client connection settings and contains subnets and IP address pools. When you create an access zone, you must specify a groupnet. If a groupnet is not specified, the access zone will reference the default groupnet. Multiple access zones can reference a single groupnet. You can direct incoming connections to the access zone through a specific IP address pool in the groupnet. Associating an access zone with an IP address pool restricts authentication to the associated access zone and reduces the number of available and accessible SMB shares and NFS exports.

An advantage to multiple access zones is the ability to configure audit protocol access for individual access zones. You can modify the default list of successful and failed protocol audit events and then generate reports through a third-party tool for an individual access zone.

A cluster includes a built-in access zone named System where you manage all aspects of a cluster and other access zones. By default, all cluster IP addresses connect to the System zone. Role-based access, which primarily allows configuration actions, is available through only the System zone. All administrators, including those given privileges by a role, must connect to the System zone to configure a cluster. The System zone is automatically configured to reference the default groupnet on the cluster, which is groupnet0.

Configuration management of a non-System access zone is not permitted through SSH, the OneFS API, or the web administration interface. However, you can create and delete SMB shares in an access zone through the Microsoft Management Console (MMC).

## Access zone resources

Retrieve, create, modify, or delete access zone configurations and settings.

## Access zones resource

Create, modify, delete, or retrieve information about the access zones on a cluster.

Operation	Method and URI
Get all access zones	GET <cluster-ip:port>/platform/3/zones
Get one access zone	GET <cluster-ip:port>/platform/3/zones/<zone-id>
Create an access zone	POST <cluster-ip:port>/platform/3/zones
Modify an access zone	PUT <cluster-ip:port>/platform/3/zones/<zone-id>
Delete an access zone	DELETE <cluster-ip:port>/platform/3/zones/<zone-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/zones?describe
	GET <cluster-ip:port>/platform/3/zones/<zone-id>?describe

## Access zones summary resource

Retrieve summary information about the access zones on a cluster.

Operation	Method and URI
Get information about all access zones	GET <cluster-ip:port>/platform/1/zones-summary
Get non-privileged information about a specific access zone.	GET <cluster-ip:port>/platform/1/zones-summary/<ZONE>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/zones-summary?describe
	GET <cluster-ip:port>/platform/1/zones-summary/<ZONE>?describe

## Access zone API examples

You can see examples for some access zone API calls.

### Create an access zone

Create an access zone on the cluster.

#### Request example

```
POST /platform/1/zones
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{"name": "MyZone", "path": "/ifs/data/myzone"}
```

**Response example**

```
201 Created
Content-type: application/json

{"id": "MyZone"}
```

**Modify an access zone**

Modify the properties for an access zone on the cluster.

**Request example**

In the following example, the `name` for ZoneA is changed to ZoneB.

```
PUT /platform/1/zones/ZoneA
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{"name": "ZoneB"}
```

**Response example**

```
204 No Content
Content-type: 'text/plain'
```

## NFS

OneFS provides an NFS server so you can share files on your cluster with NFS clients that adhere to the RFC1813 (NFSv3) and RFC3530 (NFSv4) specifications.

In OneFS, the NFS server is fully optimized as a multi-threaded service running in user space instead of the kernel. This architecture load balances the NFS service across all nodes of the cluster, providing the stability and scalability necessary to manage up to thousands of connections across multiple NFS clients.

NFS mounts execute and refresh quickly, and the server constantly monitors fluctuating demands on NFS services and makes adjustments across all nodes to ensure continuous, reliable performance. Using a built-in process scheduler, OneFS helps ensure fair allocation of node resources so that no client can seize more than its fair share of NFS services.

The NFS server also supports access zones defined in OneFS, so that clients can access only the exports appropriate to their zone. For example, if NFS exports are specified for Zone 2, only clients assigned to Zone 2 can access these exports.

To simplify client connections, especially for exports with large path names, the NFS server also supports aliases, which are shortcuts to mount points that clients can specify directly.

For secure NFS file sharing, OneFS supports NIS and LDAP authentication providers.

## NFS classes

NFS classes define values for the object properties in NFS resources.

**<user-mapping>**

The `<user-mapping>` class must be set as follows:

Property	Type	Description
enabled	Boolean	True if the user mapping is applied.
user	<persona>	Specifies the name of the privilege.
primary_group	<persona>	Specifies persona properties for the primary user group. A persona consists of either a type and name, or an ID.
secondary_group	Array of <persona>	Specifies persona properties for the secondary user group. A persona consists of either a type and name, or an ID.

**<persona>**

The <persona> class must be set with either the <persona-id> or the <type> and <name> parameters, as follows:

Property	Type	Description
id	<persona-id>	Specifies the serialized form of the persona.
type	String	Specifies the type of persona, which must be combined with a name. The type of the persona can be set to <code>user</code> , <code>group</code> , or <code>wellknown</code> .
name	String	Specifies the persona name, which must be combined with a type.

**<persona-id>**

The <persona-id> class must be set in the following format: `"["user", "group", "SID", "UID", "GID"] : [<string>]"`, such as: `"GID:2003"` or `"user:johndoe"`.

## NFS resources

You can retrieve, create, modify, or delete NFS export configurations and settings.

### NFS exports summary resource

Retrieve summary information for NFS exports.

Operations	Method and URI
Get the NFS exports summary	GET <cluster-ip:port>/platform/2/protocols/nfs/exports-summary
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/exports-summary?describe

## NFS exports resource

Create, modify, delete, or retrieve information about NFS exports.

Operation	Method and URI
Retrieve all NFS exports	GET <cluster-ip:port>/platform/4/protocols/nfs/exports
Retrieve one NFS export	GET <cluster-ip:port>/platform/4/protocols/nfs/exports/<export-id>
Create an NFS export	POST <cluster-ip:port>/platform/4/protocols/nfs/exports
Modify an NFS export	PUT <cluster-ip:port>/platform/4/protocols/nfs/exports/<export-id>
Delete an NFS export	DELETE <cluster-ip:port>/platform/4/protocols/nfs/exports/<export-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/protocols/nfs/exports?describe
	GET <cluster-ip:port>/platform/4/protocols/nfs/exports/<export-id>?describe

## NFS aliases resource

Create, modify, delete, or retrieve information about NFS aliases. Aliases are names for physical paths in the file system. Note that you are retrieving, deleting, or modifying aliases with forward slashes "/" in their names, you will need to substitute the URI encoding. For example, if the alias name is /username, you must substitute %2fusername in the call.

Operation	Method and URI
Get all NFS aliases	GET <cluster-ip:port>/platform/2/protocols/nfs/aliases
Get an NFS aliases	GET <cluster-ip:port>/platform/2/protocols/nfs/aliases/<alias id>
Create a new NFS alias	POST <cluster-ip:port>/platform/2/protocols/nfs/aliases
Modify an NFS alias	PUT <cluster-ip:port>/platform/2/protocols/nfs/aliases/<alias id>
Delete an NFS alias	DELETE <cluster-ip:port>/platform/2/protocols/nfs/aliases/<alias id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/aliases?describe
	GET <cluster-ip:port>/platform/2/protocols/nfs/aliases/<alias id>?describe

## NFS NLM locks resource

Retrieve information about NFS Network Lock Manager (NLM) advisory locks.

Operation	Method and URI
Get a list of NFS advisory locks	GET <cluster-ip:port>/platform/2/protocols/nfs/nlm/locks
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/nlm/locks?describe

## NFS NLM lock waiters resource

Retrieve information about NFS Network Lock Manager (NLM) lock waiters.

Operation	Method and URI
Get a list of NLM lock waiters on NFS	GET <cluster-ip:port>/platform/2/protocols/nfs/nlm/waiters
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/nlm/waiters?describe

## NFS NLM sessions resource

Delete or retrieve information about NFS Network Lock Manager (NLM) sessions.

Operation	Method and URI
Get all NFS NLM sessions	GET <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions
Retrieve all lock states for a specific NFS NLM session	GET <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions/<session-id>
Delete all lock states for a specific NFS NLM session	DELETE <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions/<session-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions?describe
	GET <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions/<session-id>?describe

## NFS NLM sessions check resource

Perform an active scan for lost NFSv3 locks.

Operation	Method and URI
Scan for lost NFSv3 locks	POST <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions-check
View the detailed JSON schema for this resource, which has	GET <cluster-ip:port>/platform/3/protocols/nfs/nlm/sessions-check?describe

Operation	Method and URI
information about query parameters and object properties.	

### NFS log level resource

Retrieve or set the current NFS logging level.

Operation	Method and URI
Retrieve the current NFS logging level	GET <cluster-ip:port>/platform/3/protocols/nfs/log-level
Set the NFS logging level	PUT <cluster-ip:port>/platform/3/protocols/nfs/log-level
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/nfs/log-level?describe

### NFS netgroup resource

Get or modify the current NFS netgroup cache settings.

Operation	Method and URI
Retrieve the current NFS netgroup cache settings	GET <cluster-ip:port>/platform/3/protocols/nfs/netgroup
Modify the current NFS netgroup cache settings	PUT <cluster-ip:port>/platform/3/protocols/nfs/netgroup
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/nfs/netgroup?describe

### NFS netgroup check resource

Update the NFS netgroups in the cache.

Operation	Method and URI
Update the NFS netgroups	POST <cluster-ip:port>/platform/3/protocols/nfs/netgroup/check
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/nfs/netgroup/check?describe

### NFS netgroup flush resource

Flush the NFS netgroups in the cache.

Operation	Method and URI
Flush the NFS netgroups	POST <cluster-ip:port>/platform/3/protocols/nfs/netgroup/flush

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/nfs/netgroup/flush?describe

### NFS default export settings resource

Modify or retrieve information about the default NFS export settings.

Operation	Method and URI
Get default NFS export settings	GET <cluster-ip:port>/platform/2/protocols/nfs/settings/export
Modify default NFS export settings	PUT <cluster-ip:port>/platform/2/protocols/nfs/settings/export
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/settings/export?describe

### NFS global settings resource

Retrieve or modify global configuration settings for NFS exports.

Operation	Method and URI
Get default NFS export settings	GET <cluster-ip:port>/platform/7/protocols/nfs/settings/global
Modify default NFS export settings	PUT <cluster-ip:port>/platform/7/protocols/nfs/settings/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/nfs/settings/global?describe

### NFS exports configuration check resource

Retrieve information on the status and validity of current NFS exports. Each export with an error is reported along with the first error encountered during the check.

Operation	Method and URI
Check NFS exports for configuration errors	GET <cluster-ip:port>/platform/2/protocols/nfs/check
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/check?describe

## NFS zone settings resource

Retrieve or modify zone configuration settings for NFS exports.

Operation	Method and URI
Get NFS server settings for a zone	GET <cluster-ip:port>/platform/2/protocols/nfs/settings/zone
Modify NFS server settings for a zone	PUT <cluster-ip:port>/platform/2/protocols/nfs/settings/zone
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/settings/zone?describe

## NFS reload resource

Reload cached export information. The netgroup cache is updated against the remote provider and hosts are updated against the DNS if the time to live (TTL) has expired. Netgroups are automatically refreshed on an interval specified by the netgroup expiration option. DNS hosts are intermittently refreshed. Local export information, such as options specified with exports create or exports modify, is updated immediately following the action.

Operation	Method and URI
Reload NFS exports	POST <cluster-ip:port>/platform/2/protocols/nfs/reload
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/protocols/nfs/reload?describe

## NFS API examples

You can see examples for some NFS API requests.

### Create NFS alias

Create an NFS alias.

#### Request example

```
POST /platform/2/protocols/nfs/aliases
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  "name": "nfs_alias_01",
  "path": "/ifs/nfs/aliases"
}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id": "204"
}
```

**Modify NFS alias**

Modify an NFS alias.

**Request example**

```
PUT /platform/2/protocols/nfs/aliases/204
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"name": "nfs_alias_02"}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Create NFS export**

Create an NFS export.

**Request example**

```
POST /platform/2/protocols/nfs/exports
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  "paths": [
    exports/test",
    "/ifs/nfs/exports/test2"
  ]
}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id": 24
}
```

## Modify NFS export

Modify an NFS export.

### Request example

```
PUT /platform/2/protocols/nfs/exports/24
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "write_transfer_max_size":1024,
  "write_transfer_multiple":512
}
```

### Response example

```
204 No Content
Content-type: text/plain
```

## Modify default NFS settings

Modify the default NFS settings on the cluster.

### Request example

```
PUT /platform/2/protocols/nfs/settings/export
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "block_size":512,
  "can_set_time":true,
  "case_insensitive":false
}
```

### Response example

```
204 No Content
Content-type: text/plain
```

## Modify global NFS settings

Modify the global NFS settings on the cluster.

### Request example

```
PUT /platform/2/protocols/nfs/settings/global
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  "nfsv3_enabled":true
}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Modify NFS zone settings**

Modify the settings for an NFS access zone.

**Request example**

```
PUT /platform/2/protocols/nfs/settings/zone
Authorization: Basic QWxhZGRpbjpvGVuIHNlc2FtZQ==

{
  "nfsv4_allow_numeric_ids":true,
  "nfsv4_domain":"test_domain"
}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**SMB**

OneFS includes a configurable SMB service to create and manage SMB shares. SMB shares provide Windows clients network access to file system resources on the cluster. You can grant permissions to users and groups to carry out operations such as reading, writing, and setting access permissions on SMB shares.

The `/ifs` directory is configured as an SMB share and is enabled by default. OneFS supports both user and anonymous security modes. If the user security mode is enabled, users who connect to a share from an SMB client must provide a valid user name with proper credentials.

SMB shares act as checkpoints, and users must have access to a share in order to access objects in a file system on a share. If a user has access granted to a file system, but not to the share on which it resides, that user will not be able to access the file system regardless of privileges. For example, assume a share named `ABCDOcs` contains a file named `file1.txt` in a path such as: `/ifs/data/ABCDOcs/file1.txt`. If a user attempting to access `file1.txt` does not have share privileges on `ABCDOcs`, that user cannot access the file even if originally granted read and/or write privileges to the file.

The SMB protocol uses security identifiers (SIDs) for authorization data. All identities are converted to SIDs during retrieval and are converted back to their on-disk representation before they are stored on the cluster.

When a file or directory is created, OneFS checks the access control list (ACL) of its parent directory. If the ACL contains any inheritable access control entries (ACEs), a new ACL is generated from those ACEs. Otherwise, OneFS creates an ACL from the combined file and directory create mask and create mode settings.

OneFS supports the following SMB clients:

SMB version	Supported operating systems
3.0 - Multichannel only	Windows 8 or later Windows Server 2012 or later
2.1	Windows 7 or later Windows Server 2008 R2 or later
2.0	Windows Vista or later Windows Server 2008 or later Mac OS X 10.9 or later
1.0	Windows 2000 or later Windows XP or later Mac OS X 10.5 or later

## SMB resources

You can retrieve, create, modify, or delete SMB share configurations and settings.

### SMB shares summary resource

Retrieve summary information for SMB shares.

Operation	Method and URI
Get the SMB shares summary	GET <cluster-ip:port>/platform/1/protocols/smb/shares-summary
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/smb/shares-summary?describe

### SMB shares resource

Modify, delete, create, or retrieve information about SMB shares.

Operation	Method and URI
Retrieve a single SMB share	GET <cluster-ip:port>/platform/7/protocols/smb/shares/<share>
Retrieve a list of SMB shares	GET <cluster-ip:port>/platform/7/protocols/smb/shares
Create an SMB share	POST <cluster-ip:port>/platform/7/protocols/smb/shares
Modify an SMB share	PUT <cluster-ip:port>/platform/7/protocols/smb/shares/<share>
Delete an SMB share	DELETE <cluster-ip:port>/platform/7/protocols/smb/shares/<share>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/smb/shares?describe
	GET <cluster-ip:port>/platform/7/protocols/smb/shares/<share>?describe

## SMB share settings resource

Modify or retrieve information about default SMB share settings.

Operation	Method and URI
Get SMB share settings	GET <cluster-ip:port>/platform/7/protocols/smb/settings/share
Modify SMB share settings	PUT <cluster-ip:port>/platform/7/protocols/smb/settings/share
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/smb/settings/share?describe

## SMB global settings resource

Modify or retrieve information about global SMB share settings.

Operation	Method and URI
Get the global SMB settings	GET <cluster-ip:port>/platform/7/protocols/smb/settings/global
Modify the global SMB settings	PUT <cluster-ip:port>/platform/7/protocols/smb/settings/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/smb/settings/global?describe

## SMB open files resource

Retrieve a listing of all files that are currently open through SMB on the queried node or close an open file.

Operation	Method and URI
Get a list of files opened through SMB	GET <cluster-ip:port>/platform/1/protocols/smb/openfiles
Close a file opened through SMB	DELETE <cluster-ip:port>/platform/1/protocols/smb/openfiles/<file-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/smb/openfiles?describe
	GET <cluster-ip:port>/platform/1/protocols/smb/openfiles/<file-id>?describe

## SMB sessions resource

Close or retrieve a listing of all SMB user sessions that are currently open on the queried node.

Operation	Method and URI
Get a list of SMB sessions	GET <cluster-ip:port>/platform/1/protocols/smb/sessions

Operation	Method and URI
Close an SMB session user	DELETE <cluster-ip:port>/platform/1/protocols/smb/sessions/<computer>/<user>
Close an SMB session computer	DELETE <cluster-ip:port>/platform/1/protocols/smb/sessions/<computer>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/smb/sessions?describe
	GET <cluster-ip:port>/platform/1/protocols/smb/sessions/<computer>/<user>?describe
	GET <cluster-ip:port>/platform/1/protocols/smb/sessions/<computer>?describe

### SMB log level resource

List or modify the current SMB logging level.

Operation	Method and URI
List the current SMB logging level	GET <cluster-ip:port>/platform/3/protocols/smb/log-level
Modify the current SMB logging level	PUT <cluster-ip:port>/platform/3/protocols/smb/log-level
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/smb/log-level?describe

### SMB log level filters resource

Retrieve, add, or delete SMB logging level filter information.

Operation	Method and URI
View all SMB log filters	GET <cluster-ip:port>/platform/3/protocols/smb/log-level/filters
View a specific SMB log filter	GET <cluster-ip:port>/platform/3/protocols/smb/log-level/filters/<filter-id>
Add an SMB log filter	POST <cluster-ip:port>/platform/3/protocols/smb/log-level/filters
Delete existing SMB log filters	DELETE <cluster-ip:port>/platform/3/protocols/smb/log-level/filters
Delete a specific SMB log filter	DELETE <cluster-ip:port>/platform/3/protocols/smb/log-level/filters/<filter-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/smb/log-level/filters?describe
	GET <cluster-ip:port>/platform/3/protocols/smb/log-level/filters/<filter-id>?describe

## SMB zone settings resource

Modify or retrieve information about SMB share settings on a per-zone basis.

Operation	Method and URI
Get the SMB settings for an access zone	GET <cluster-ip:port>/platform/6/protocols/smb/settings/zone
Modify the SMB settings for an access zone	PUT <cluster-ip:port>/platform/6/protocols/smb/settings/zone
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/6/protocols/smb/settings/zone?describe

## FTP

OneFS includes a secure FTP service called vsftpd, which stands for Very Secure FTP Daemon, that you can configure for standard FTP and FTPS file transfers.

### FTP resources

You can retrieve or modify global FTP configuration settings.

### FTP settings resource

Retrieve and modify global FTP configuration settings.

Operation	Method and URI
Retrieve global FTP configuration settings	GET <cluster-ip:port>/platform/3/protocols/ftp/settings
Modify global FTP configuration settings	PUT <cluster-ip:port>/platform/3/protocols/ftp/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ftp/settings?describe

## HTTP and HTTPS

OneFS includes a configurable Hypertext Transfer Protocol (HTTP) service, which is used to request files that are stored on the cluster and to interact with the web administration interface.

OneFS supports both HTTP and its secure variant, HTTPS. Each node in the cluster runs an instance of the Apache HTTP Server to provide HTTP access. You can configure the HTTP service to run in different modes.

Both HTTP and HTTPS are supported for file transfer, but only HTTPS is supported for API calls. The HTTPS-only requirement includes the web administration interface. In addition, OneFS supports a form of the web-based DAV (WebDAV) protocol that enables users to modify and manage files on remote web servers. OneFS performs distributed authoring, but does not support versioning and does not perform security checks. You can enable DAV in the web administration interface.

## HTTP resources

You can retrieve and modify global HTTP configuration settings.

### HTTP settings resource

Retrieve and modify global HTTP configuration settings.

Operation	Method and URI
Retrieve global HTTP configuration settings	GET <cluster-ip:port>/platform/3/protocols/http/settings
Modify global HTTP configuration settings	PUT <cluster-ip:port>/platform/3/protocols/http/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/http/settings?describe

## About Hadoop

Hadoop is an open-source platform that runs analytics on large sets of data across a distributed file system.

In a Hadoop implementation on an Isilon cluster, OneFS acts as the distributed file system and HDFS is supported as a native protocol. Clients from a Hadoop cluster connect to the Isilon cluster through the HDFS protocol to manage and process data.

Hadoop support on the cluster requires you to activate an HDFS license. To obtain a license, contact your Isilon sales representative.

## HDFS resources

You can retrieve, create, modify, or delete HDFS configurations and settings.

### HDFS settings resource

Modify or retrieve information about global HDFS settings.

Operation	Method and URI
Retrieve the global HDFS settings	GET <cluster-ip:port>/platform/4/protocols/hdfs/settings
Modify the global HDFS settings	PUT <cluster-ip:port>/platform/4/protocols/hdfs/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/protocols/hdfs/settings?describe

### HDFS racks resource

Create, modify, delete, or retrieve information about HDFS racks.

Operation	Method and URI
Get all HDFS racks	GET <cluster-ip:port>/platform/1/protocols/hdfs/racks

Operation	Method and URI
Create an HDFS rack	POST <cluster-ip:port>/platform/1/protocols/hdfs/racks
Get an HDFS rack	GET <cluster-ip:port>/platform/1/protocols/hdfs/racks/<rack ID>
Modify an HDFS rack	PUT <cluster-ip:port>/platform/1/protocols/hdfs/racks/<rack ID>
Delete an HDFS rack	DELETE <cluster-ip:port>/platform/1/protocols/hdfs/racks/<rack ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/hdfs/racks?describe
	GET <cluster-ip:port>/platform/1/protocols/hdfs/racks/<rack ID>?describe

### HDFS proxyusers resource

Create, delete, or retrieve information about HDFS proxyusers.

Operation	Method and URI
Get all HDFS proxyusers	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers
Get an HDFS proxyuser	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>
Create an HDFS proxyuser	POST <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/ or PUT <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>
Delete an HDFS proxyuser	DELETE <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers?describe
	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>?describe

### HDFS proxyusers name members resource

Add, delete, or retrieve information about HDFS proxyuser members.

Operation	Method and URI
Get all members of the HDFS proxyusers	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>/members
Add a member to the HDFS proxyuser	POST <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>/members/ or

Operation	Method and URI
	PUT <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>/members/<MEMBER>
Remove a member from the HDFS proxyuser	DELETE <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>/members/<MEMBER>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/protocols/hdfs/proxyusers/<NAME>/members?describe

### HDFS log level resource

Retrieve or modify the HDFS service logging level for a node.

Operation	Method and URI
Retrieve the HDFS logging level	GET <cluster-ip:port>/platform/3/protocols/hdfs/log-level
Modify the HDFS logging level	PUT <cluster-ip:port>/platform/3/protocols/hdfs/log-level
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/hdfs/log-level?describe

### HDFS Apache Ranger plug-in settings resource

Retrieve and modify the HDFS Apache Ranger plug-in properties.

Operation	Method and URI
Retrieve the HDFS Range plug-in properties	GET <cluster-ip:port>/platform/4/protocols/hdfs/ranger-plugin/settings
Modify the HDFS Range plug-in properties	PUT <cluster-ip:port>/platform/4/protocols/hdfs/ranger-plugin/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/protocols/hdfs/ranger-plugin/settings?describe

### HDFS crypto settings resource

List or modify HDFS crypto settings.

Operation	Method and URI
List HDFS crypto settings	GET <cluster-ip:port>/platform/7/protocols/hdfs/crypto/settings
Modify HDFS crypto settings	PUT <cluster-ip:port>/platform/7/protocols/hdfs/crypto/settings

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/hdfs/crypto/settings?describe

## HDFS crypto encryption zones resource

List encryption zones, or turn an empty directory into an encryption zone.

Operation	Method and URI
List HDFS encryption zones	GET <cluster-ip:port>/platform/7/protocols/hdfs/crypto/encryption-zones
Create an HDFS encryption zone	POST <cluster-ip:port>/platform/7/protocols/hdfs/crypto/encryption-zones
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/hdfs/crypto/encryption-zones?describe

## HDFS API examples

You can see examples for some HDFS API requests.

### Create an HDFS rack

You can create an HDFS rack.

#### Request example

The rack name must be preceded by a forward slash (/).

```
POST /platform/1/protocols/hdfs/racks
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  "name": "/racktest"
}
```

#### Response example

```
201 Created
Content-type: application/json

{
  "id" : "1-5-21-4224731515-2571109568-2823010237-1003"
}
```

## Modify an HDFS rack

You can modify the properties for an HDFS rack.

### Request example

The rack name must be preceded by a forward slash (/). In the URL, you must replace the forward slash with the escape character %2F.

```
PUT /platform/1/protocols/hdfs/racks/%2Fracktest
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  "name":"/rack2test"
}
```

### Response example

No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Modify global HDFS settings

You can modify the properties for global HDFS settings.

### Request example

```
PUT /platform/1/protocols/hdfs/settings/
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  "default_checksum_type":"crc32"
}
```

### Response example

No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Create HDFS proxyusers

Create an HDFS proxyuser.

### Request example

```
POST /platform/1/protocols/hdfs/proxyusers
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"name":"proxy_user_test"}
```

**Response example**

```
201 Created
Content-type: application/json
```

You can also create an HDFS proxyuser through the PUT method.

**Request example**

```
PUT /platform/1/protocols/hdfs/proxyusers/proxy_user_test
Authorization: Basic QWxhZGRpbjpvvcGVuIHN1c2FtZQ==

{}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Create HDFS proxyuser member**

Create an HDFS proxyuser member.

**Request example**

```
POST /platform/1/protocols/hdfs/proxyusers/proxy_user_test/members
Authorization: Basic QWxhZGRpbjpvvcGVuIHN1c2FtZQ==

{"name":"proxy_user_member_test"}
```

**Response example**

```
201 Created
Content-type: application/json
```

You can also create an HDFS proxyuser member through the PUT method.

**Request example**

```
PUT /platform/1/protocols/hdfs/proxyusers/proxy_user_test/members/
USER:proxy_user_member_test
Authorization: Basic QWxhZGRpbjpvvcGVuIHN1c2FtZQ==

{}
```

**Response example**

```
204 No Content
Content-type: text/plain
```

**Isilon Swift**

OneFS supports Isilon Swift, an object storage interface compatible with the OpenStack Swift 1.0 application programming interface (API). Through Isilon Swift,

you can access file-based data stored on your cluster as objects. The Swift API is implemented as a set of Representational State Transfer (REST) web services over HTTP or secure HTTP (HTTPS). Since the Swift API is considered as a protocol, content and metadata can be ingested as objects and concurrently accessed through protocols configured on the cluster. The cluster must also be licensed to support Isilon Swift.

The Isilon Swift protocol service is a licensed feature. Contact your Dell EMC EMC Isilon representative to obtain a license key to access the Swift protocol and RESTful APIs for object storage operations.

## Swift resources

You can list, create, modify, or delete Swift account information.

### Swift accounts resource

List, modify, create, or delete Swift accounts.

Operation	Method and URI
List all Swift accounts	GET <cluster-ip:port>/platform/3/protocols/swift/accounts
List a specific Swift account	GET <cluster-ip:port>/platform/3/protocols/swift/accounts/<account-id>
Create a Swift account	POST <cluster-ip:port>/platform/3/protocols/swift/accounts
Modify a Swift account	PUT <cluster-ip:port>/platform/3/protocols/swift/accounts/<account-id>
Delete a Swift account	DELETE <cluster-ip:port>/platform/3/protocols/swift/accounts/<account-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/swift/accounts?describe
	GET <cluster-ip:port>/platform/3/protocols/swift/accounts/<account-id>?describe

## Networking

After you determine the topology of your network, you can set up and manage your internal and external networks.

There are two types of networks on the Dell EMC EMC Isilon cluster:

### Internal

Nodes communicate with each other using a high speed low latency InfiniBand network. You can optionally configure a second InfiniBand network to enable failover for redundancy.

### External

Clients connect to the cluster through the external network with Ethernet. The cluster supports standard network communication protocols, including NFS, SMB, HDFS, HTTP, and FTP. The cluster includes various external Ethernet connections, providing flexibility for a wide variety of network configurations.

## Network resources

List, create, modify, or delete information specific to OneFS networks.

### Network external resource

View or modify external network settings.

Operation	Method and URI
View external network settings	GET <cluster-ip:port>/platform/3/network/external
Modify external network settings	PUT <cluster-ip:port>/platform/3/network/external
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/external?describe

### Network subnets resource

List OneFS network subnets.

Operation	Method and URI
List OneFS network subnets	GET <cluster-ip:port>/platform/3/network/subnets
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/subnets?describe

### Network DNS cache resource

View or modify network DNS cache settings.

Operation	Method and URI
View DNS cache settings	GET <cluster-ip:port>/platform/3/network/dnscache
Modify DNS cache settings	PUT <cluster-ip:port>/platform/3/network/dnscache
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/dnscache?describe

### Network DNS cache flush resource

Flush the DNS cache.

Operation	Method and URI
Flush the DNS cache	POST <cluster-ip:port>/platform/3/network/dnscache/flush

## Network interfaces resource

List OneFS network interfaces.

Operation	Method and URI
List all OneFS network interfaces	GET <cluster-ip:port>/platform/7/network/interfaces
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/network/interfaces?describe

## Network pools resource

List OneFS flexnet pools.

Operation	Method and URI
List OneFS flexnet pools	GET <cluster-ip:port>/platform/3/network/pools
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/pools?describe

## Network rules resource

List OneFS network rules.

Operation	Method and URI
List OneFS network rules	GET <cluster-ip:port>/platform/3/network/rules
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/rules?describe

## Network SmartConnect re-balance all IPs resource

Re-balance IP addresses in all pools.

Operation	Method and URI
Rebalance IP addresses in all pools	POST <cluster-ip:port>/platform/3/network/sc-rebalance-all
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/sc-rebalance-all?describe

## Network groupnets resource

List, create, modify, or delete OneFS network groupnets.

Operation	Method and URI
List all groupnets	GET <cluster-ip:port>/platform/3/network/groupnets
View a specific groupnet	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>
Create a groupnet	POST <cluster-ip:port>/platform/3/network/groupnets
Modify a groupnet	PUT <cluster-ip:port>/platform/3/network/groupnets/<groupnet>
Delete a groupnet	DELETE <cluster-ip:port>/platform/3/network/groupnets/<groupnet>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets?describe
	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>?describe

## Network groupnets subnets resource

List, create, modify, or delete OneFS network subnets.

Operation	Method and URI
List all subnets	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets
View a specific subnet	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>
Create a subnet	POST <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets
Modify a subnet	PUT <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>
Delete a groupnet	DELETE <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets?describe
	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>?describe

## Network groupnets subnets pools resource

Retrieve, create, modify, or delete OneFS network pools.

Operation	Method and URI
Retrieve all pools	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools
View a specific subnet pool	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>
Create a pool	POST <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets<subnet>/pools
Modify a pool	PUT <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>
Delete a pool	DELETE <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools?describe
	GET <cluster-ip:port>/platform/7/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>?describe

## Network groupnets subnets pools interfaces resource

List OneFS network interfaces within a pool.

Operation	Method and URI
List all OneFS network interfaces within a pool	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/interfaces
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/interfaces?describe

## Network groupnets subnets pools rebalance IPs resource

Rebalance IP addresses in a specified pool.

Operation	Method and URI
Rebalance IP addresses in a specified pool	POST <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets<subnet>/pools/<pool>/rebalance-ips

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rebalance-ips?describe

## Network groupnets subnets pools rules resource

List, create, modify, or delete OneFS network rules within a pool.

Operation	Method and URI
List all OneFS network rules within a pool	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules
View a specific OneFS network rule within a pool	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules/<name>
Create a OneFS network rule within a pool	POST <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules
Modify a OneFS network rule within a pool	PUT <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules/<name>
Delete a OneFS network rule within a pool	DELETE <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules/<name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules?describe
	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/rules/<name>?describe

## Network groupnets subnets pools SmartConnect suspend nodes resource

Suspend SmartConnect DNS query responses for a list of nodes.

Operation	Method and URI
Suspend SmartConnect DNS query responses for a list of nodes	POST <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/sc-suspend-nodes
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/sc-suspend-nodes?describe

## Network groupnets subnets pools SmartConnect resume nodes resource

Resume SmartConnect DNS query responses for a list of nodes.

Operation	Method and URI
Resume SmartConnect DNS query responses for a list of nodes	POST <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets<subnet>/pools/<pool>/sc-resume-nodes
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/network/groupnets/<groupnet>/subnets/<subnet>/pools/<pool>/sc-resume-nodes?describe

## System jobs overview

The most critical function of OneFS is maintaining the integrity of data on your Isilon cluster. Other important system maintenance functions include monitoring and optimizing performance, detecting and mitigating drive and node failures, and freeing up available space.

Because maintenance functions use system resources and can take hours to run, OneFS performs them as jobs that run in the background through a service called Job Engine. The time it takes for a job to run can vary significantly depending on a number of factors. These include other system jobs that are running at the same time; other processes that are taking up CPU and I/O cycles while the job is running; the configuration of your cluster; the size of your data set; and how long since the last iteration of the job was run.

Up to three jobs can run simultaneously. To ensure that maintenance jobs do not hinder your productivity or conflict with each other, Job Engine categorizes them, runs them at different priority and impact levels, and can temporarily suspend them (with no loss of progress) to enable higher priority jobs and administrator tasks to proceed.

In the case of a power failure, Job Engine uses a checkpoint system to resume jobs as close as possible to the point at which they were interrupted. The checkpoint system helps Job Engine keep track of job phases and tasks that have already been completed. When the cluster is back up and running, Job Engine restarts the job at the beginning of the phase or task that was in process when the power failure occurred.

As system administrator, through the Job Engine service, you can monitor, schedule, run, terminate, and apply other controls to system maintenance jobs. The Job Engine provides statistics and reporting tools that you can use to determine how long different system jobs take to run in your OneFS environment.

---

### Note

To initiate any Job Engine tasks, you must have the role of SystemAdmin in the OneFS system.

---

## System job resources

You can retrieve, create, modify, or delete system job settings and configurations.

## Jobs resource

Modify, create, or retrieve information about OneFS system jobs.

Operation	Method and URI
Get information about all system jobs	GET /platform/7/job/jobs
Get information about a system job	GET /platform/7/job/jobs/<id>
Create a system job	POST /platform/7/job/jobs
Modify a system job	PUT /platform/7/job/jobs/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET /platform/7/job/jobs?describe
	GET /platform/7/job/jobs/<id>?describe

## Job types resource

Modify or retrieve information about system job types.

Operation	Method and URI
Get all system job types	GET <cluster-ip:port>/platform/1/job/types
Get a system job type	GET <cluster-ip:port>/platform/1/job/types/<name>
Modify a system job type	PUT <cluster-ip:port>/platform/1/job/type/<name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/job/types?describe

## Job policies resource

Create, modify, delete, or retrieve information about job impact policies.

Operation	Method and URI
Get all job impact policies	GET <cluster-ip:port>/platform/1/job/policies
Get a job impact policy	GET <cluster-ip:port>/platform/1/job/policies/<name>
Create a job impact policy	POST <cluster-ip:port>/platform/1/job/policies
Modify a job impact policy	PUT <cluster-ip:port>/platform/1/job/policies/<name>
Delete a job impact policy	DELETE <cluster-ip:port>/platform/1/job/policies/<name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/job/policies?describe

## Job reports resource

Retrieve information about system job reports.

Operation	Method and URI
View all job reports	GET <cluster-ip:port>/platform/7/job/reports
View a specific job report	GET <cluster-ip:port>/platform/7/job/reports/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/job/reports?describe
	GET <cluster-ip:port>/platform/7/job/reports/<id>?describe

## Job summary resource

View job engine status.

Operation	Method and URI
View job engine status	GET <cluster-ip:port>/platform/7/job/system-job
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/job/system-job?describe

## Job events resource

Retrieve information about system job events.

Operation	Method and URI
Get information about job events	GET <cluster-ip:port>/platform/3/job/events
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/job/events?describe

## Job statistics resource

Retrieve statistics about system jobs and workers across the cluster.

Operation	Method and URI
Get system job statistics	GET <cluster-ip:port>/platform/1/job/statistics
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/job/statistics?describe

## Job recent resource

List recently completed jobs.

Operation	Method and URI
List recently completed jobs	GET <cluster-ip:port>/platform/3/job/recent
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/job/recent?describe

## System job API examples

You can see examples for some system job API calls.

### Modify a job type

You can modify a system job type.

#### Request example

```
PUT /platform/1/job/types/AVScan
Authorization: Basic QWxhZGRpbjpwGVuIHN1c2FtZQ==

{
  'policy': 'MEDIUM',
  'enabled': True
}
```

#### Response example

```
204 No Content
Content-type: 'text/plain',
Allow: 'GET, PUT, HEAD'
```

### Create a job policy

You can create a system job policy.

#### Request example

```
POST /platform/1/job/policies
Authorization: Basic QWxhZGRpbjpwGVuIHN1c2FtZQ==

{
  'intervals': [
    {
      'impact': 'High',
      'begin': 'Tuesday 00:00',
      'end': 'Thursday 23:59'
    }
  ],
  'name': 'myPolicy',
  'description': 'Custom policy'
}
```

**Response example**

```
201 CREATED
Content-type: application/json,
Allow: 'GET, PUT, POST, DELETE'

{
  'id': 'myPolicy'
}
```

**Modify a job policy**

You can retrieve modify a system job policy.

**Request example**

```
PUT /platform/1/job/policies/myPolicy
Authorization: Basic QWxhZGRpbjpvcmVudHh1c2FtZQ==

{
  'intervals': [
    {
      'impact': 'Medium',
      'begin': 'Tuesday 00:00',
      'end': 'Thursday 23:59'
    }
  ],
  'description': 'Custom policy - medium impact Tuesday through
Thursday'
}
```

**Response example**

```
204 No Content
Content-type: 'text/plain',
Allow: 'GET, PUT, POST, DELETE, HEAD'
```

**Start a new system job**

You can queue a new instance of a job to run after the current job has completed.

**Request example**

```
POST /platform/1/job/jobs
Authorization: Basic QWxhZGRpbjpvcmVudHh1c2FtZQ==

{
  'type': 'AVScan',
  'allow_dup': True
}
```

**Response example**

```
201 CREATED
Content-type: application/json,
Allow: 'GET, PUT, POST, HEAD'

{
```

```
    "id": 1234
  }
```

## Modify a system job

You can modify, cancel, pause, or resume a running system job.

### Request example

```
PUT /platform/1/job/jobs/AVScan
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{
  'state': 'pause'
}
```

### Response example

```
204 No Content
Content-type: 'text/plain',
Allow: 'GET, PUT, POST, HEAD'
```

## Cluster statistics

You can view performance, historical, and in-depth usage statistics for your Dell EMC EMC Isilon cluster, and control the output for each mode of statistics reporting.

### Statistics resources

You can retrieve information about OneFS statistics through the following resources.

#### Note

Statistic API resources are available, but are currently unsupported.

### Statistics current resource

Query OneFS current statistics. Current statistics are the most currently available metrics at the time of the request. For a list of available statistics keys with descriptions, see the `<cluster-ip:port>/platform/1/statistics/keys` or `<cluster-ip:port>/platform/1/statistics/keys/<key>` resources.

Operation	Method and URI
Get all current statistics	GET <code>&lt;cluster-ip:port&gt;/platform/1/statistics/current</code>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <code>&lt;cluster-ip:port&gt;/platform/1/statistics/current?describe</code>

## Statistics keys resource

Retrieve meta-data for matching statistics keys.

Operation	Method and URI
Get all statistic keys	GET <cluster-ip:port>/platform/1/statistics/keys
Get a statistics key	GET <cluster-ip:port>/platform/1/statistics/keys/<key>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/statistics/keys?describe
	GET <cluster-ip:port>/platform/1/statistics/keys/<key>?describe

## Statistics history resource

Query OneFS time-series statistics over custom time ranges. Not all statistics will have time-series enabled, and for those statistics with time-series enabled, the full extent of the requested time range may not be available due to configuration or system uptime. For a list of available statistics keys with descriptions, see the <cluster-ip:port>/platform/1/statistics/keys or <cluster-ip:port>/platform/1/statistics/keys/<key> resources. These resource also describe available history policies for each key.

Operation	Method and URI
Get all statistics history	GET <cluster-ip:port>/platform/1/statistics/history
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/statistics/history?describe

## Statistics operations resource

List all operations implemented for protocol and client statistics on a OneFS cluster.

Operation	Method and URI
List all statistics operations	GET <cluster-ip:port>/platform/3/statistics/operations
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/operations?describe

## Statistics protocols resource

Return a list of protocol and client statistics for OneFS.

Operation	Method and URI
Get all protocols	GET <cluster-ip:port>/platform/1/statistics/protocols

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/statistics/protocols?describe

### Statistics summary client resource

Display OneFS cluster usage statistics sorted by cluster hosts and users.

Operation	Method and URI
Display cluster usage statistics sorted by cluster hosts and users	GET <cluster-ip:port>/platform/3/statistics/summary/client
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/client?describe

### Statistics summary drive resource

Display OneFS performance statistics by drive.

Operation	Method and URI
Display performance statistics by drive	GET <cluster-ip:port>/platform/3/statistics/summary/drive
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/drive?describe

### Statistics summary heat resource

List OneFS files and directories that are considered the busiest, or *hottest*, sorted by various performance-related factors.

Operation	Method and URI
Display the busiest, or <i>hottest</i> , OneFS files and directories	GET <cluster-ip:port>/platform/3/statistics/summary/heat
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/heat?describe

### Statistics summary protocol resource

Display cluster usage statistics sorted by protocol.

Operation	Method and URI
Display cluster usage statistics sorted by protocol	GET <cluster-ip:port>/platform/3/statistics/summary/protocol
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/protocol?describe

## Statistics summary protocol stats resource

Display detailed statistics about protocol usage, as well as OneFS, CPU, network, and disk statistics.

Operation	Method and URI
Display detailed statistics about protocol usage	GET <cluster-ip:port>/platform/3/statistics/summary/protocol-stats
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/protocol-stats?describe

## Statistics summary system resource

Display general cluster statistics, including operation rates for all supported protocols, and network and disk traffic in kilobytes per second.

Operation	Method and URI
Display general cluster statistics	GET <cluster-ip:port>/platform/3/statistics/summary/system
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/statistics/summary/system?describe

## Statistics summary workload resource

This resource summarizes statistics about system processes and jobs.

Operation	Method and URI
Retrieve statistics about system processes and jobs	GET <cluster-ip:port>/platform/4/statistics/summary/workload
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/statistics/summary/workload?describe

## FSA

The FSAnalyze job gathers and reports information about all files and directories beneath the /ifs path. This job requires you to activate an InsightIQ license. You can use reports from this job to analyze the OneFS file system.

For more information, see the *Isilon InsightIQ User Guide*.

## FSA resources

Retrieve, create, modify, or delete FSAnalyze (FSA) job-related configurations and settings.

## FSA path resource

Retrieves the path that should be mounted to access results of the FSAalyze (FSA) job. Creates the FSA export rule if it does not previously exist.

Operation	Method and URI
Retrieve export path as plain text	GET <cluster-ip:port>/platform/3/fsa/path
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/path?describe

## FSA results resource

List all FSA job result sets, or list, modify, or delete individual result sets.

Operation	Method and URI
List all FSA job result sets	GET <cluster-ip:port>/platform/3/fsa/results
List individual FSA job result set	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>
Modify the pinned property for a FSA job result set	PUT <cluster-ip:port>/platform/3/fsa/results/<result-set-id>
Delete a FSA job result set	DELETE <cluster-ip:port>/platform/3/fsa/results/<result-set-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/results?describe
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>?describe

## FSA results directories resource

Retrieve results directory information for the directory specified by the query path argument or the directory specified by the logical inode number (LIN) parameter.

Operation	Method and URI
Retrieve results directory information for the directory specified by the query path argument	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/directories
Retrieve results directory information for the directory specified by the LIN	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/directories/<lin>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/directories?describe
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/directories/<lin>?describe

## FSA results histogram resource

Retrieve file count histograms sorted by the `stat` or `breakout` parameters.

Operation	Method and URI
Retrieve a histogram of file counts for an individual FSA result set.	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>
Retrieve a histogram breakout for an individual FSA result set.	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>/by
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>/by/<breakout>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram?describe
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>?describe
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>/by?describe
	GET <cluster-ip:port>/platform/3/fsa/results/<result-set-id>/histogram/<stat>/by/<breakout>?describe

## FSA results top directories resource

Retrieves the top directories according to the `stat` parameter.

Operation	Method and URI
Retrieve top directories	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-dirs
Retrieve top directories using query parameters	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-dirs/<stat>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-dirs?describe
	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-dirs/<stat>?describe

## FSA results top files resource

Retrieves the top files according to the `stat` parameter.

Operation	Method and URI
Retrieve top files	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-files

Operation	Method and URI
Retrieve top directories using query parameters	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-files/<stat>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-files?describe
	GET <cluster-ip:port>/platform/3/fsa/<result-set-id>/top-files/<stat>?describe

## FSA settings resource

List or modify FSA settings, or revert FSA settings to their default values.

Operation	Method and URI
List FSA settings	GET <cluster-ip:port>/platform/3/fsa/settings
Modify FSA settings	PUT <cluster-ip:port>/platform/3/fsa/settings
Revert FSA settings to their defaults	DELETE <cluster-ip:port>/platform/3/fsa/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/fsa/settings?describe

## Events and alerts

Events are individual occurrences or conditions related to the data workflow, maintenance operations, and hardware components of your cluster. An alert is a message that describes a change that has occurred in an event group.

Throughout OneFS there are processes that are constantly monitoring and collecting information on cluster operations.

When the status of a component or operation changes, the change is captured as an event and placed into a priority queue at the kernel level.

Every event has two ID numbers that help to establish the context of the event:

- The event type ID identifies the type of event that has occurred.
- The event instance ID is a unique number that is specific to a particular occurrence of an event type. When an event is submitted to the kernel queue, an event instance ID is assigned. You can reference the instance ID to determine the exact time that an event occurred.

You can view individual events. However, you manage events and alerts at the event group level.

At any point in time, you can view event groups to track situations occurring on your cluster. However, you can also create alerts that will proactively notify you if there is a change in an event group.

For example, you can generate an alert when a new event is added to an event group, when an event group is resolved, or when the severity of an event group changes.

You can configure your cluster to only generate alerts for specific conditions or event groups, or during limited time periods.

Alerts are delivered through channels. You can configure a channel to determine who will receive the alert and when.

## Event resources

Retrieve, create, modify, or delete event-related configurations and settings.

### Event alert conditions resource

List, create, modify, or delete event alert conditions.

Operation	Method and URI
List all event alert conditions	GET <cluster-ip:port>/platform/4/event/alert-conditions
List one event alert condition	GET <cluster-ip:port>/platform/4/event/alert-conditions/<condition-id>
Create an event alert condition	POST <cluster-ip:port>/platform/4/event/alert-conditions
Modify an event alert condition	PUT <cluster-ip:port>/platform/4/event/alert-conditions/<condition-id>
Bulk delete event alert conditions	DELETE <cluster-ip:port>/platform/4/event/alert-conditions
Delete an individual alert condition	DELETE <cluster-ip:port>/platform/4/event/alert-conditions/<condition-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/event/alert-conditions?describe
	GET <cluster-ip:port>/platform/4/event/alert-conditions/<condition-id>?describe

### Event categories resource

List one or all event categories.

Operation	Method and URI
List all event categories	GET <cluster-ip:port>/platform/3/event/categories
List one event category	GET <cluster-ip:port>/platform/3/event/categories/<category-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/event/categories?describe
	GET <cluster-ip:port>/platform/3/event/categories/<category-id>?describe

## Event channels resource

List, create, modify, or delete event channels.

Operation	Method and URI
List all event channels	GET <cluster-ip:port>/platform/7/event/channels
List one event channel	GET <cluster-ip:port>/platform/7/event/channels/<channel-id>
Create a new event channel	POST <cluster-ip:port>/platform/7/event/channels
Modify an event channel	PUT <cluster-ip:port>/platform/7/event/channels/<channel-id>
Delete an event channel	DELETE <cluster-ip:port>/platform/7/event/channels/<channel-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/event/channels?describe
	GET <cluster-ip:port>/platform/7/event/channels/<channel-id>?describe

## Event eventgroup definitions resource

List eventgroup definitions.

Operation	Method and URI
List all eventgroup definitions	GET <cluster-ip:port>/platform/4/event/eventgroup-definitions
List one eventgroup definition	GET <cluster-ip:port>/platform/4/event/eventgroup-definitions/<eventgroup-definition-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/event/eventgroup-definitions?describe
	GET <cluster-ip:port>/platform/4/event/eventgroup-definitions/<eventgroup-definition-id>?describe

## Event eventgroups occurrences resource

List or modify eventgroup occurrences.

Operation	Method and URI
List all eventgroup occurrences	GET <cluster-ip:port>/platform/3/event/eventgroup-occurrences
List one eventgroup occurrence	GET <cluster-ip:port>/platform/3/event/eventgroup-occurrences/<eventgroup-occurrence-id>

Operation	Method and URI
Modify all eventgroup occurrences (resolved or ignore all)	PUT <cluster-ip:port>/platform/3/event/eventgroup-occurrences
Modify an eventgroup occurrence	PUT <cluster-ip:port>/platform/3/event/eventgroup-occurrences/<eventgroup-occurrence-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/event/eventgroup-occurrences?describe
	GET <cluster-ip:port>/platform/3/event/eventgroup-occurrences/<eventgroup-occurrence-id>?describe

### Event eventlists resource

List events by eventgroup occurrence.

Operation	Method and URI
List all event occurrences grouped by eventgroup occurrences	GET <cluster-ip:port>/platform/7/event/eventlists
List all events for one eventgroup occurrence	GET <cluster-ip:port>/platform/7/event/eventlists/<event-occurrence-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/event/eventlists?describe
	GET <cluster-ip:port>/platform/7/event/eventlists/<event-occurrence-id>?describe

### Event events resource

Create a test event.

Operation	Method and URI
Create a test event	POST <cluster-ip:port>/platform/3/event/events
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/event/events?describe

### Event settings resource

List or modify event settings.

Operation	Method and URI
List all eventgroup occurrences	GET <cluster-ip:port>/platform/3/event/settings
Modify all eventgroup occurrences (resolved or ignore all)	PUT <cluster-ip:port>/platform/3/event/settings

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/event/settings?describe

## Snapshots overview

A OneFS snapshot is a logical pointer to data that is stored on a cluster at a specific point in time.

A snapshot references a directory on a cluster, including all data stored in the directory and its subdirectories. If the data referenced by a snapshot is modified, the snapshot stores a physical copy of the data that was modified. Snapshots are created according to user specifications or are automatically generated by OneFS to facilitate system operations.

To create and manage snapshots, you must activate a SnapshotIQ license on the cluster. Some applications must generate snapshots to function but do not require you to activate a SnapshotIQ license; by default, these snapshots are automatically deleted when OneFS no longer needs them. However, if you activate a SnapshotIQ license, you can retain these snapshots. You can view snapshots generated by other modules without activating a SnapshotIQ license.

You can identify and locate snapshots by name or ID. A snapshot name is specified by a user and assigned to the virtual directory that contains the snapshot. A snapshot ID is a numerical identifier that OneFS automatically assigns to a snapshot.

## Snapshots resources

You can retrieve, create, modify, or delete snapshot configurations and settings.

### Snapshot license resource

Retrieve license information for SnapshotIQ.

Operation	Method and URI
Get license information for SnapshotIQ	GET <cluster-ip:port>/platform/5/snapshot/license
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/snapshot/license?describe

### Snapshot summary resource

Retrieve summary information about file system snapshots.

Operation	Method and URI
Get summary information about file system snapshots	GET <cluster-ip:port>/platform/1/snapshot/snapshots-summary
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/snapshots-summary?describe

## Snapshots resource

Create, modify, delete, or retrieve information about file system snapshots.

Operation	Method and URI
Get a list of all snapshots	GET <cluster-ip:port>/platform/1/snapshot/snapshots
Get a single snapshot	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>
Create a snapshot	POST <cluster-ip:port>/platform/1/snapshot/snapshots
Modify a snapshot	PUT <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>
Delete all snapshots	DELETE <cluster-ip:port>/platform/1/snapshot/snapshots
Delete a snapshot	DELETE <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>?describe
	GET <cluster-ip:port>/platform/1/snapshot/snapshots?describe

## Snapshot schedules resource

Create, modify, delete, or retrieve information about snapshot schedules.

Operation	Method and URI
Get a list of all snapshot schedules	GET <cluster-ip:port>/platform/3/snapshot/schedules
Get a single snapshot schedule	GET <cluster-ip:port>/platform/3/snapshot/schedules/<schedule-id>
Create a snapshot schedule	POST <cluster-ip:port>/platform/3/snapshot/schedules
Modify a snapshot schedule	PUT <cluster-ip:port>/platform/3/snapshot/schedules/<schedule-id>
Delete all snapshot schedules	DELETE <cluster-ip:port>/platform/3/snapshot/schedules
Delete a snapshot schedule	DELETE <cluster-ip:port>/platform/3/snapshot/schedules/<schedule-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/snapshot/schedules?describe
	GET <cluster-ip:port>/platform/3/snapshot/schedules/<schedule-id>?describe

## Snapshot locks resource

Create, modify, remove, or retrieve information about locks on an individual snapshot.

Operation	Method and URI
Get a list of locks on a snapshot	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>/locks
Get a single lock on a snapshot	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<snapshot-name id>/locks/<lock-id>
Create a lock on a snapshot	POST <cluster-ip:port>/platform/1/snapshot/snapshots/<snapshot-name id>/locks
Modify a lock on a snapshot	PUT <cluster-ip:port>/platform/1/snapshot/snapshots/<snapshot-name id>/locks/<lock-id>
Remove a lock from a snapshot	DELETE <cluster-ip:port>/platform/1/snapshot/snapshots/<lock-id>/locks
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<snapshot-name id>/locks/<lock-id>?describe
	GET <cluster-ip:port>/platform/1/snapshot/snapshots/<id snapshot name>/locks?describe

## Snapshot pending resource

Retrieve information about snapshots that will be generated by a snapshot schedule.

Operation	Method and URI
Get a list of scheduled pending snapshots	GET <cluster-ip:port>/platform/1/snapshot/pending
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/pending?describe

## Snapshot aliases resource

Create, modify, delete, or retrieve information about snapshot aliases.

Operation	Method and URI
Get all snapshot aliases	GET <cluster-ip:port>/platform/1/snapshot/aliases
Get a snapshot alias	GET <cluster-ip:port>/platform/1/snapshot/aliases/<snapshot alias name or ID>
Create a snapshot alias	POST <cluster-ip:port>/platform/1/snapshot/aliases
Modify a snapshot alias	PUT <cluster-ip:port>/platform/1/snapshot/aliases/<snapshot alias name or ID>
Delete all snapshot aliases	DELETE <cluster-ip:port>/platform/1/snapshot/aliases/

Operation	Method and URI
Delete a snapshot alias	DELETE <cluster-ip:port>/platform/1/snapshot/aliases/<snapshot alias name or ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/aliases?describe
	GET <cluster-ip:port>/platform/1/snapshot/aliases/<snapshot alias name or ID>?describe

## Snapshot changelists resource

Delete or retrieve information about snapshot changelists.

Operation	Method and URI
Get all snapshot changelists	GET <cluster-ip:port>/platform/1/snapshot/changelists
Get a snapshot changelist	GET <cluster-ip:port>/platform/1/snapshot/changelists/<changelist>
Delete a snapshot changelist	DELETE <cluster-ip:port>/platform/1/snapshot/changelists/<changelist>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/changelists?describe

## Snapshot changelists changelist lins resource

Retrieve information about a snapshot changelist entry.

Operation	Method and URI
Get snapshot changelist entries	GET <cluster-ip:port>/platform/1/snapshot/changelists/<changelist>/lins
Get a snapshot changelist entry	GET <cluster-ip:port>/platform/1/snapshot/changelists/<changelist>/lins/<lin>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/changelists/<changelist>/lins?describe
	GET <cluster-ip:port>platform/1/snapshot/changelists/<changelist>/lins/<lin>?describe

## Snapshot repstates resource

Create or retrieve information about snapshot repstates.

Operation	Method and URI
Get all snapshot repstates	GET <cluster-ip:port>/platform/1/snapshot/repstates
Get a snapshot repstate	GET <cluster-ip:port>/platform/1/snapshot/repstates/<repstate>

Operation	Method and URI
Create a snapshot repstate	POST <cluster-ip:port>/platform/1/snapshot/repstates/<repstate>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/repstates?describe
	GET <cluster-ip:port>/platform/1/snapshot/repstates/<repstate>?describe

## Snapshot settings resource

Modify or retrieve information about global snapshot settings.

Operation	Method and URI
Get the current snapshot settings	GET <cluster-ip:port>/platform/1/snapshot/settings
Modify the current snapshot settings	PUT <cluster-ip:port>/platform/1/snapshot/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/snapshot/settings?describe

## Snapshots API examples

You can see examples for some snapshots API requests.

### Create a file pool policy

You can create a file pool policy.

#### Request example

```
POST /platform/1/filepool/policies
Authorization: Basic QWxhZGRpbjpvcmVudHh1c2FtZQ==

{
  "action_param": "true"
  "action_type": "set_requested_protection"
}
```

#### Response example

```
201 Created
Content-type: application/json

{
  "id" : "224731515-2571109568-2823010237-1003"
}
```

## Modify a snapshot alias

You can modify a snapshot alias.

### Request example

```
PUT /platform/1/snapshot/aliases/snapshot2541
Authorization: Basic QWxhZGRpbjpvGVuIHNlc2FtZQ==

{"name" : "snapshot2641"}
```

### Response example

No message body is returned for this request.

```
204 No Content
Content-type: text/plain
```

## NDMP backup and recovery

In OneFS, you can back up and recover file-system data through the Network Data Management Protocol (NDMP). From a backup server, you can direct backup and recovery processes between a cluster and backup devices such as tape devices, media servers, and virtual tape libraries (VTLs).

OneFS supports both three-way and two-way NDMP backup models.

Two-way NDMP backup is significantly faster than the three-way NDMP backup. It is also the most efficient method in terms of cluster resource consumption. However, a two-way NDMP backup requires that you attach one or more Backup Accelerator nodes to the cluster.

In both the two-way and three-way NDMP backup models, file history data is transferred from the cluster to the backup server. Before a backup begins, OneFS creates a snapshot of the targeted directory, then backs up the snapshot, which ensures that the backup image represents a specific point in time.

You do not need to activate a SnapshotIQ license on the cluster to perform NDMP backups. If you have activated a SnapshotIQ license on the cluster, you can generate a snapshot through the SnapshotIQ tool, and then back up the same snapshot. If you back up a SnapshotIQ snapshot, OneFS does not create another snapshot for the backup.

---

### Note

If you are recovering SmartLock directories, we recommend that you do not specify autocommit time periods for them.

---

You can also back up WORM domains through NDMP.

## NDMP resources

You can retrieve, create, modify, or delete NDMP configurations and settings.

### NDMP backup contexts

Retrieve information about NDMP backup contexts.

Operation	Method and URI
Get NDMP backup contexts	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/backup
Get a specific NDMP backup context	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/backup/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/backup?describe

### NDMP BRE contexts

Retrieve information about backup restartable extension (BRE) contexts.

Operation	Method and URI
Get NDMP BRE contexts	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/bre
Get a specific NDMP BRE context	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/bre/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/bre?describe

### NDMP restore contexts

Retrieve information about NDMP restore contexts.

Operation	Method and URI
Get NDMP restore contexts	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/restore
Get a specific NDMP restore context	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/restore/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/contexts/restore?describe

## NDMP diagnostics

Retrieve or modify NDMP diagnostic information.

Operation	Method and URI
Get NDMP diagnostic information	GET <cluster-ip:port>/platform/3/protocols/ndmp/diagnostics
Modify NDMP diagnostic information	PUT <cluster-ip:port>/platform/3/protocols/ndmp/diagnostics
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/diagnostics?describe

## NDMP dumpdates

Retrieve or delete information about NDMP dump dates.

Operation	Method and URI
Get NDMP dump date specifics	GET <cluster-ip:port>/platform/3/protocols/ndmp/dumpdates/<path*>
Delete NDMP dump date entries	DELETE <cluster-ip:port>/platform/3/protocols/ndmp/dumpdates/<path*>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/dumpdates/<path*>?describe

## NDMP logs

Retrieve NDMP logs.

Operation	Method and URI
Get NDMP logs	GET <cluster-ip:port>/platform/3/protocols/ndmp/logs
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/logs?describe

## NDMP sessions

Retrieve information about NDMP sessions

Operation	Method and URI
Get NDMP session information	GET <cluster-ip:port>/platform/3/protocols/ndmp/sessions
Get information about a specific NDMP session	GET <cluster-ip:port>/platform/3/protocols/ndmp/sessions/<session-ID>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/sessions?describe

## NDMP DMA settings

Retrieve a list of supported data management application (DMA) vendors

Operation	Method and URI
Get list of NDMP DMAs	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/dmas
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/dmas?describe

## NDMP global settings

Retrieve or modify NDMP global settings.

Operation	Method and URI
Get NDMP global settings	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/global
Modify NDMP global settings	PUT <cluster-ip:port>/platform/3/protocols/ndmp/settings/global
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/global?describe

## NDMP preferred IP preferences resources

Retrieve, modify, create, and delete preferred IP preferences.

Operation	Method and URI
Retrieve a list of preferred IP preferences	GET <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips
Retrieve a single IP preference by ID	GET <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips/<id>
Modify a preferred IP preference	PUT <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips/<id>
Create a preferred IP preference	POST <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips
Delete a preferred IP preference	DELETE <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips/<id>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips?describe
	GET <cluster-ip:port>/platform/4/protocols/ndmp/settings/preferred-ips/<id>?describe

## NDMP variable settings

Create, modify, view or delete NDMP environment variable settings.

Operation	Method and URI
Get list of preferred NDMP environment variables	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/variables/<path*>
Modify preferred NDMP environment variables	PUT <cluster-ip:port>/platform/3/protocols/ndmp/settings/variables/<path*>
Create preferred NDMP environment variables	POST <cluster-ip:port>/platform/3/protocols/ndmp/settings/variables/<path*>
Delete preferred NDMP environment variables	DELETE <cluster-ip:port>/platform/3/protocols/ndmp/settings/variables/<path*>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/settings/variables/<path*>?describe

## NDMP users

List, create, modify or delete NDMP administrators.

Operation	Method and URI
Get list of NDMP administrators	GET <cluster-ip:port>/platform/3/protocols/ndmp/users
Get information about a specific NDMP administrator	GET <cluster-ip:port>/platform/3/protocols/ndmp/users/<name>
Modify information about an NDMP administrator	PUT <cluster-ip:port>/platform/3/protocols/ndmp/users/<name>
Create an NDMP administrator	POST <cluster-ip:port>/platform/3/protocols/ndmp/users/<name>
Delete an NDMP administrator	DELETE <cluster-ip:port>/platform/3/protocols/ndmp/users/<name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ndmp/users?describe

## SyncIQ data replication overview

OneFS enables you to replicate data from one Isilon cluster to another through the SyncIQ software module. You must activate a SyncIQ license on both Isilon clusters before you can replicate data between them.

You can replicate data at the directory level while optionally excluding specific files and sub-directories from being replicated. SyncIQ creates and references snapshots to replicate a consistent point-in-time image of a source directory. Metadata such as access control lists (ACL) and alternate data streams (ADS) are replicated along with data.

SyncIQ enables you to maintain a consistent replica of your data on another Isilon cluster and to control the frequency of data replication. For example, you could configure SyncIQ to back up data from your primary cluster to a secondary cluster once a day at 10 PM. Depending on the size of your data set, the first replication operation could take considerable time. After that, however, replication operations would complete more quickly.

SyncIQ also offers automated failover and failback capabilities so you can continue operations on the secondary Isilon cluster should your primary cluster become unavailable.

## Sync resources

You can retrieve, create, modify, or delete resources for data replication with SyncIQ.

### File matching patterns

You can apply the following file matching pattern to filter specific objects in SyncIQ.

```
<file_matching_pattern> := {
  "or_criteria" : [
    {
      "and_criteria": [
        <file_criterion>,
        <file_criterion>,
        ...
      ]
    },
    {
      "and_criteria": [
        <file_criterion>,
        <file_criterion>,
        ...
      ]
    },
    ...
  ]
}

<file_criterion> = {
  "type": <string>,
  "operator": <string>,
  "value": {<string> | <integer>}
}
```

The following table defines available operators.

operator	Description
==	Equal
!=	Does not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
!	Not

The following table defines available file criteria types.

Type	Conditions
name	Paired with operators "==" or "!=".
path	Paired with operators "==" or "!=".
posix_regex_name	Paired with operators "==" or "!=".
accessed_time	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
accessed_before	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
accessed_after	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
birth_time	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
birth_before	No operator is required; every operation is set to "==".

Type	Conditions
	The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
birth_after	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
changed_time	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
changed_before	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
changed_after	No operator is required; every operation is set to "==".  The value must be in the following form: {<mm>/<dd>/<yyyy> [<HH>:<mm>]   <integer> {days   weeks   months   years} ago}
size	Paired with all operators except for "!".  The value must be in the following form: An integer, followed by B, KB, MB, GB, or TB (such as 100B or 12TB).
file_type	Paired with operators "==" or "!=".  The value must be in the following form: 'file', 'directory', or 'symlink'.
user_name	Paired with operators "==" or "!=".
user_id	Paired with operators "==" or "!=".
group_name	Paired with operators "==" or "!=".
group_id	Paired with operators "==" or "!=".
no_user	Paired with operators "!".
no_group	Paired with operators "!".

Type	Conditions
	Does not require a value.

The following example shows a sync policy filter.

```

"file_matching_filter": {
  "or_criteria": [
    {
      "and_criteria": [
        {
          "type": "size",
          "operator": ">=",
          "value": "500000KB"
        },
        {
          "type": "file_type",
          "operator": "==",
          "value": "file"
        }
      ]
    },
    {
      "and_criteria": [
        {
          "type": "posix_regex_name",
          "operator": "==",
          "value": "some_special_prefix_*"
        }
      ]
    },
    {
      "and_criteria": [
        {
          "type": "file_type",
          "operator": "==",
          "value": "symlink"
        }
      ]
    }
  ]
}

```

## Sync license resource

Retrieve license information for SyncIQ.

Operation	Method and URI
Get license information for SyncIQ	GET <cluster-ip:port>/platform/5/sync/license
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/sync/license?describe

## Sync certificates server resource

Import, modify, list, view, or delete TLS server certificates.

Operation	Method and URI
List all SyncIQ TLS server certificates	GET <cluster-ip:port>/platform/7/sync/certificates/server
View a specific SyncIQ TLS server certificate	GET <cluster-ip:port>/platform/7/sync/certificates/server/<server>
Import a SyncIQ TLS server certificate	POST <cluster-ip:port>/platform/7/sync/certificates/server
Modify a SyncIQ TLS server certificate	PUT <cluster-ip:port>/platform/7/sync/certificates/server/<server>
Delete a SyncIQ TLS server certificate	DELETE <cluster-ip:port>/platform/7/sync/certificates/server/<server>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/certificates/server?describe
	GET <cluster-ip:port>/platform/7/sync/certificates/server/<server>?describe

## Sync certificates peer resource

Import, modify, list, view or delete SyncIQ peer TLS certificates

Operation	Method and URI
List all trusted SyncIQ peer TLS certificates	GET <cluster-ip:port>/platform/7/sync/certificates/peer
View a specific SyncIQ peer TLS certificate	GET <cluster-ip:port>/platform/7/sync/certificates/peer/<peer>
Import a trusted SyncIQ TLS certificate	POST <cluster-ip:port>/platform/7/sync/certificates/peer
Modify a trusted SyncIQ TLS certificate	PUT <cluster-ip:port>/platform/7/sync/certificates/peer/<peer>
Delete a trusted SyncIQ TLS certificate	DELETE <cluster-ip:port>/platform/7/sync/certificates/peer/<peer>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/certificates/peer?describe
	GET <cluster-ip:port>/platform/7/sync/certificates/peer/<peer>?describe

## Sync jobs resource

Start, modify, or retrieve information about a SyncIQ replication jobs.

Operation	Method and URI
Get a list of all replication jobs	GET <cluster-ip:port>/platform/7/sync/jobs

Operation	Method and URI
Get the details of a replication job	GET <cluster-ip:port>/platform/7/sync/jobs/<job>
Start a replication job	POST <cluster-ip:port>/platform/7/sync/jobs
Modify an in-progress replication job	PUT <cluster-ip:port>/platform/7/sync/jobs/<job>
Cancel all replication jobs	DELETE <cluster-ip:port>/platform/7/sync/jobs
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/jobs?describe
	GET <cluster-ip:port>/platform/7/sync/jobs/<job>?describe

## Sync policies resource

Create, modify, delete, or retrieve information about SyncIQ replication policies.

Operation	Method and URI
Get all replication policies	GET <cluster-ip:port>/platform/7/sync/policies
Get a replication policy	GET <cluster-ip:port>/platform/7/sync/policies/<policy>
Create a replication policy	POST <cluster-ip:port>/platform/7/sync/policies
Modify a replication policy	PUT <cluster-ip:port>/platform/7/sync/policies/<policy>
Delete all replication policies	DELETE <cluster-ip:port>/platform/7/sync/policies
Delete a replication policy	DELETE <cluster-ip:port>/platform/7/sync/policies/<policy>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/policies?describe
	GET <cluster-ip:port>/platform/7/sync/policies/<policy>?describe

## Sync policies reset resource

Reset the incremental state of a replication policy and force a full sync or copy. You must post an empty object: {} to reset the policy.

Operation	Method and URI
Reset a replication policy.	POST <cluster-ip:port>/platform/1/sync/policy/<policy>/reset

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/sync/policy/<policy>/reset?describe

## Sync reports resource

Retrieve SyncIQ reports and subreports.

Operation	Method and URI
Retrieve all SyncIQ reports	GET <cluster-ip:port>/platform/7/sync/reports
Retrieve a single SyncIQ report	GET <cluster-ip:port>/platform/7/sync/reports/<report>
Retrieve a list of SyncIQ subreports for a report	GET <cluster-ip:port>/platform/7/sync/reports/<report>/subreports
Retrieve a single SyncIQ subreport	GET <cluster-ip:port>/platform/7/sync/reports/<report>/subreports/<report-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/reports?describe
	GET <cluster-ip:port>/platform/7/sync/reports/<report>?describe
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/reports/<report>/subreports?describe
	GET <cluster-ip:port>/platform/7/sync/reports/<report>/subreports/<report>?describe

## Sync reports rotate resource

Rotate the records in the database and periodically remove older reports from the system.

Operation	Method and URI
Retrieve information on whether the rotation is running.	GET <cluster-ip:port>/platform/1/sync/reports-rotate
Force the reports in the database to rotate.	POST <cluster-ip:port>/platform/1/sync/reports-rotate
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/sync/reports-rotate?describe

## Sync target policies resource

Retrieve information about SyncIQ target replication policies.

Operation	Method and URI
Get all target replication policies	GET <cluster-ip:port>/platform/1/sync/target/policies
Get a target replication policy	GET <cluster-ip:port>/platform/1/sync/target/policies/<policy-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/sync/target/policies?describe

## Sync target policies cancel resource

Cancel the most recent replication job for a replication policy from the target cluster.

Operation	Method and URI
Cancel the most recent replication job	POST <cluster-ip:port>/platform/1/sync/target/policies/<policy>/cancel
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/sync/target/policies/<policy>/cancel?describe

## SyncIQ target reports resource

Retrieve information about the SyncIQ reports and subreports running on a target cluster.

Operation	Method and URI
Retrieve all replication target reports	GET <cluster-ip:port>/platform/7/sync/target/reports
Retrieve a replication target report	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>
Retrieve all target subreports for a single report	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>/subreports
Retrieve a single target subreport	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>/subreports/<subreport-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/target/reports?describe
	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>?describe
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>/subreports?describe

Operation	Method and URI
	GET <cluster-ip:port>/platform/7/sync/target/reports/<report>/subreports/<subreport-id>?describe

## Sync service policies resource

List, view, create, modify, or delete SyncIQ service replication policies.

Operation	Method and URI
List all SyncIQ service replication policies	GET <cluster-ip:port>/platform/7/sync/service/policies
View a specific SyncIQ service replication policy	GET <cluster-ip:port>/platform/7/sync/service/policies/<policy>
Import a SyncIQ service replication policy	POST <cluster-ip:port>/platform/7/sync/service/policies
Modify a SyncIQ service replication policy	PUT <cluster-ip:port>/platform/7/service/policies/<policy>
Delete SyncIQ service replication policies	DELETE <cluster-ip:port>/platform/7/sync/service/policies
Delete a specific SyncIQ service replication policy	DELETE <cluster-ip:port>/platform/7/sync/service/policies/<policy>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/service/policies?describe
	GET <cluster-ip:port>/platform/7/sync/service/policies/<policy>?describe

## Sync service policies reset resource

Reset a SyncIQ service replication policy incremental state, and force a full sync/copy.

Operation	Method and URI
Import a SyncIQ service replication policy	POST <cluster-ip:port>/platform/7/sync/service/policies/<policy>/reset
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/service/policies/<policy>/reset?describe

## Sync service target policies reset resource

View or break association with replication policies on the SyncIQ target.

Operation	Method and URI
List all SyncIQ target service replication policies	GET <cluster-ip:port>/platform/7/sync/service/target/policies
View a specific SyncIQ target service replication policy	GET <cluster-ip:port>/platform/7/sync/service/target/policies/<policy>

Operation	Method and URI
Break association with a specific SyncIQ target service policy	DELETE <cluster-ip:port>/platform/7/sync/service/target/policies/<policy>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/service/target/policies?describe
	GET <cluster-ip:port>/platform/7/sync/service/target/policies/<policy>?describe

### Sync service target policies cancel resource

Cancel the most recent SyncIQ job for a service replication policy from the target.

Operation	Method and URI
Cancel a SyncIQ job for a service replication policy from the target	POST <cluster-ip:port>/platform/7/sync/service/target/policies/<policy>/cancel
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/service/target/policies/<policy>/cancel?describe

### Sync rules resource

Create, delete, or retrieve information about SyncIQ replication job performance rules. Rules can restrict the amount of network bandwidth or files transferred per second for replication policies.

Operation	Method and URI
Get all replication job performance rules	GET <cluster-ip:port>/platform/3/sync/rules
Create a replication job performance rule	POST <cluster-ip:port>/platform/3/sync/rules
Modify a replication job performance rule	PUT <cluster-ip:port>/platform/3/sync/rules/<rule>
Delete all replication job performance rules	DELETE <cluster-ip:port>/platform/3/sync/rules/
Delete all replication job performance rules by type	DELETE <cluster-ip:port>/platform/3/sync/rules?type=<string>
Delete a replication job performance rule	DELETE <cluster-ip:port>/platform/3/sync/rules/<rule>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/sync/rules?describe
	GET <cluster-ip:port>/platform/3/sync/rules/<rule>?describe

## Sync settings resource

Modify or retrieve information about global SyncIQ settings.

Operation	Method and URI
Get global SyncIQ settings	GET <cluster-ip:port>/platform/7/sync/settings
Modify global SyncIQ settings	PUT <cluster-ip:port>/platform/7/sync/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/settings?describe

## Sync advanced settings resource

Modify or retrieve information about advanced global SyncIQ settings.

Operation	Method and URI
Get advanced global SyncIQ settings	GET <cluster-ip:port>/platform/7/sync/settings/advanced
Modify advanced global SyncIQ settings	PUT <cluster-ip:port>/platform/7/sync/settings/advanced
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/settings/advanced?describe

## Sync history CPU resource

Retrieve CPU performance data.

Operation	Method and URI
Retrieve CPU performance data	GET <cluster-ip:port>/platform/3/sync/history/cpu
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/sync/history/cpu?describe

## Sync history file resource

Retrieve information about OneFS replication job performance reports. These reports indicate the number of files per second that were sent by replication policies at a given time.

Operation	Method and URI
Get all replication job performance reports.	GET <cluster-ip:port>/platform/1/sync/history/file
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/sync/history/file?describe

## Sync history network resource

Retrieve information about OneFS replication job performance reports. These reports indicate the amount of network bandwidth consumed by data replication policies at a given time.

Operation	Method and URI
List network operations performance data	GET <cluster-ip:port>/platform/7/sync/history/network
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/sync/history/network?describe

## Sync history worker resource

Retrieve worker performance data.

Operation	Method and URI
Retrieve worker performance data	GET <cluster-ip:port>/platform/3/sync/history/worker
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/sync/history/worker?describe

## SyncIQ API examples

You can see examples for some SyncIQ API calls.

### Start a replication job

Manually start a replication job on the system.

#### Request example

```
POST /platform/1/sync/jobs
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{
  'id': 'testpol'
}
```

#### Response example

```
201 Created
Content-type: application/json,
Allow: 'GET, POST, HEAD'

{
  "id":"testpol"
}
```

## Modify a replication job

Pause, cancel, or restart a job.

### Request example

You can only modify the `state` object property for a replication job. Options are pause, cancel, and restart.

```
PUT /platform/1/sync/jobs/testpol
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'state': cancel,
}
```

### Response example

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT'
```

## Create a replication policy

You can create a replication policy on the file system.

### Request example

```
POST /platform/1/sync/policies
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'log_level': 'fatal',
  'name': 'myNewPolicy',
  'schedule': 'every 3 weeks',
  'source_root_path': '/ifs/data/sync2',
  'target_path': '/ifs/data/sync/target2',
  'action': 'copy',
  'report_max_count': 144,
  'source_exclude_directories': ['/ifs/data/sync2/exclude'],
  'source_include_directories': ['/ifs/data/sync2/include'],
  'target_host': 'localhost'
}
```

### Response examples

In the following example, the request was successful and a replication policy ID is returned for the created object.

```
201 Created
Content-type: application/json,
Allow: 'DELETE, GET, POST, HEAD'

{
  "id": "a33006f364842eefb629fc6b95c92559"
}
```

In following example, the replication policy was not created and an error was returned.

```
500 Internal Server Error
Content-type: application/json,
Allow: 'DELETE, GET, POST, HEAD'

{
  "errors":[
    {
      "code":"AEC_EXCEPTION",
      "message":"duplicate policy <name,type> entry with id=
\'(null)\', name=\'myNewPolicy\'"
    }
  ]
}
```

## Modify a replication policy

You can modify a replication policy on the file system.

### Request example

```
PUT    /platform/1/sync/policies/myNewPolicy
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{
  'target_compare_initial_sync': True,
  'enabled': True,
  'description': 'New policy',
  'target_host': 'newHostname'
}
```

### Response examples

The request was successful. No message body is returned for this request.

```
204 No Content
content-type: text/plain,
allow: 'DELETE, GET, PUT, HEAD'
```

In the following example, the policy was not modified and an error message was returned.

```
500 Internal Server Error
Content-type: application/json,
Allow: 'DELETE, GET, PUT, HEAD'

{
  "errors":[
    {
      "code":"AEC_BAD_REQUEST",
      "field":"source_network",
      "message":"Flexnet subnet not found"
    }
  ]
}
```

## Reset a replication policy

Reset a replication policy and force a full sync and copy replication job.

### Request example

```
POST /platform/1/sync/policy/testPolicy/reset
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
```

### Response example

```
201 Created
Content-type: application/json,
Allow: 'POST'

{
  "id": "5275f97ebb3892ed4a47f71de20d4609"
}
```

## Force rotation for reports

Manually start rotation for the records in the database, which deletes reports that are older than the specified maximum retention period.

### Request example

```
POST /platform/1/sync/reports-rotate
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
```

### Response example

```
201 Created
Content-type: application/json,
Allow: 'DELETE, GET, POST, HEAD'

{
  "id": "a33006f364842eefb629fc6b95c92559"
}
```

## Cancel a target replication policy

You can cancel a replication policy from the target cluster.

### Request example

```
POST /platform/1/sync/target/policies/testpol/cancel
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
```

### Response example

```
200 OK
Content-type: application/json,
Allow: 'DELETE, GET, PUT, HEAD'

{
```

```

"policies" :
[
  {
    "failover_failback_state" : "writes_disabled",
    "id" : "021a24618064135c5df4c431fd132437",
    "last_job_state" : "paused",
    "last_source_coordinator_ip" : "127.0.0.1",
    "last_update_from_source" : 1371769450,
    "legacy_policy" : false,
    "name" : "testpol",
    "source_cluster_guid" :
"005056300217c137c2512b163880cb4d843d",
    "source_host" : "jgregory",
    "target_path" : "/ifs/data/tgt"
  }
]

```

## Create a replication policy rule on the system

You can create a replication policy rule on the file system.

### Request example

```

POST /platform/1/sync/rules
Authorization: Basic QWxhZGRpbjpvcmVudHJ1c2FtZQ==

{
  'type': 'file_count',
  'limit': 123,
  'schedule':
  {
    'begin': '09:00',
    'end': '17:00',
    'monday': True,
    'tuesday': True,
    'friday': True,
    'wednesday': True,
    'thursday': True,
    'sunday': False,
    'saturday': False
  }
}

```

### Response example

```

201 Created
Content-type: application/json,
Allow: 'DELETE, GET, POST, HEAD'

{
  "id": "fc-0"
}

```

## Modify a replication policy rule

You can modify replication policy rules on the system.

### Request example

```
PUT /platform/sync/rules/
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==
```

### Response example

```
204 No Content
Content-type: text/plain,
Allow: 'DELETE, GET, PUT, POST'
```

## Modify SyncIQ settings

You can modify the SyncIQ settings on the system.

### Request example

```
PUT /platform/1/sync/settings
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'report_max_count': 1234,
  'service': 'on'
}
```

### Response example

```
204 No Content
Content-type: text/plain,
Allow: 'DELETE, GET, PUT, HEAD'
```

## SmartLock overview

With the SmartLock software module, you can protect files on an Isilon cluster from being modified, overwritten, or deleted. To protect files in this manner, you must activate a SmartLock license.

With SmartLock, you can identify a directory in OneFS as a WORM domain. WORM stands for write once, read many. All files within the WORM domain can be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted.

After a file is removed from a WORM state, you can delete the file. However, you can never modify a file that has been committed to a WORM state, even after it is removed from a WORM state.

In OneFS, SmartLock can be deployed in one of two modes: compliance mode or enterprise mode.

### SmartLock resources

You can retrieve, create, or modify SmartLock configurations and settings.

## SmartLock domains resource

Create, modify, or retrieve information about a SmartLock domain.

Operation	Method and URI
Get all SmartLock domains	GET <cluster-ip:port>/platform/7/worm/domains
Get a SmartLock domain	GET <cluster-ip:port>/platform/7/worm/domains/<domain>
Create a SmartLock domain	POST <cluster-ip:port>/platform/7/worm/domains
Modify a SmartLock domain	PUT <cluster-ip:port>/platform/7/worm/domains/<domain>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/worm/domains?describe
	GET <cluster-ip:port>/platform/7/worm/domains?describe

## SmartLock settings resource

Modify or retrieve information about SmartLock global settings.

Operation	Method and URI
Get SmartLock global settings	GET <cluster-ip:port>/platform/1/worm/settings
Modify SmartLock global settings	PUT <cluster-ip:port>/platform/1/worm/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/worm/settings?describe

## SmartLock API examples

You can see examples for some SmartLock API requests.

### Create a SmartLock

You can create a SmartLock domain.

#### Request example

```
POST /platform/1/worm/domains
Authorization: Basic QWxhZGRpbjpvcmVudHh1c2FtZQ==

{
  "path": "/ifs/test/domain_test"
}
```

**Response example**

```
201 Created
Content-type: application/json

{
  "id" : "224731515-4837484-928237-1003"
}
```

**Modify a SmartLock**

You can modify a SmartLock domain.

**Request example**

```
PUT /platform/1/worm/domains/domaintest
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"privileged_delete":"on"}
```

**Response example**

No message body is returned for this request.

```
204 No Content
Content-type: text/plain
```

**Modify SmartLock settings**

You can modify SmartLock settings.

**Request example**

In this example, you can set the compliance clock to the current system time by sending a PUT request to this resource with an empty JSON object {} for the cdate value. This cluster must be in compliance mode to set the compliance clock.

```
PUT /platform/1/worm/domains/settings
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{"cdate" : }
```

**Response example**

No message body is returned for this request.

```
204 No Content
Content-type: text/plain
```

**Deduplication overview**

SmartDedupe enables you to save storage space on your cluster by reducing redundant data. Deduplication maximizes the efficiency of your cluster by decreasing the amount of storage required to store multiple files with identical blocks.

The SmartDedupe software module deduplicates data by scanning an Isilon cluster for identical data blocks. Each block is 8 KB. If SmartDedupe finds duplicate blocks, SmartDedupe moves a single copy of the blocks to a hidden file called a shadow store.

SmartDedupe then deletes the duplicate blocks from the original files and replaces the blocks with pointers to the shadow store.

Deduplication is applied at the directory level, targeting all files and directories underneath one or more root directories. SmartDedupe not only deduplicates identical blocks in different files, it also deduplicates identical blocks within a single file.

You can first assess a directory for deduplication and determine the estimated amount of space you can expect to save. You can then decide whether to deduplicate the directory. After you begin deduplicating a directory, you can monitor how much space is saved by deduplication in real time.

For two or more files to be deduplicated, the files must have the same disk pool policy ID and protection policy. If one or both of these attributes differs between two or more identical files, or files with identical 8K blocks, the files are not deduplicated.

Because it is possible to specify protection policies on a per-file or per-directory basis, deduplication can further be impacted. Consider the example of two files, `/ifs/data/projects/alpha/logo.jpg` and `/ifs/data/projects/beta/logo.jpg`. Even though the `logo.jpg` files in both directories are identical, if one has a different protection policy from the other, the two files would not be deduplicated.

In addition, if you have activated a SmartPools license on your cluster, you can specify custom file pool policies. These file pool policies might cause files that are identical or have identical 8K blocks to be stored in different node pools. Consequently, those files would have different disk pool policy IDs and would not be deduplicated.

SmartDedupe also does not deduplicate files that are 32 KB or smaller, because doing so would consume more cluster resources than the storage savings are worth. The default size of a shadow store is 2 GB. Each shadow store can contain up to 256,000 blocks. Each block in a shadow store can be referenced up to 32,000 times.

## Deduplication resources

You can retrieve, create, modify, or delete SmartDedupe configurations and settings.

### Deduplication summary resource

Retrieve summary information about deduplication jobs.

Operation	Method and URI
Get a summary of deduplication jobs	GET <cluster-ip:port>platform/1/dedupe/dedupe-summary
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/dedupe/dedupe-summary?describe

### Deduplication settings resource

Modify or retrieve information about OneFS deduplication settings.

Operation	Method and URI
Get deduplication settings	GET <cluster-ip:port>/platform/1/dedupe/settings
Modify deduplication settings	PUT <cluster-ip:port>/platform/1/dedupe/settings

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/dedupe/settings?describe

## Deduplication reports resource

Retrieve information about deduplication jobs.

Operation	Method and URI
Retrieve a report for all deduplication jobs	GET <cluster-ip:port>/platform/1/dedupe/reports
Retrieve a report about a single deduplication job	GET <cluster-ip:port>/platform/1/dedupe/reports/<id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/dedupe/reports?describe
	GET <cluster-ip:port>/platform/1/dedupe/reports/<id>?describe

## Deduplication API examples

You can see examples for some deduplication API calls.

### Modify deduplication settings

You can modify deduplication settings on the cluster.

#### Request example

```
PUT /platform/1/dedupe/settings
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  'paths': [
    '/ifs/data/dedupeme1',
    '/ifs/data/dedupeme2'
  ]
}
```

#### Response example

```
204 No Content
Content-type: 'text/plain,
Allow: 'GET, PUT, HEAD'
```

## General cluster configuration

You can manage general OneFS settings and module licenses for the Dell EMC EMC Isilon cluster.

General cluster administration covers several areas. You can:

- manage general settings such as cluster name, date and time, and email
- monitor the cluster status and performance, including hardware components

- configure how events and notifications are handled
- perform cluster maintenance such as adding, removing, and restarting nodes

Most management tasks are accomplished through both the web administration or command-line interface; however, you will occasionally encounter a task that can only be managed by one or the other.

## General cluster configuration resources

You can list, modify, create, and delete information regarding OneFS cluster configuration.

### Cluster configuration resource

View general information about a cluster.

Operation	Method and URI
View information about a cluster	GET <cluster-ip:port>/platform/3/cluster/config
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/config?describe

### Cluster configuration join mode resource

View or set the cluster join mode.

Operation	Method and URI
View information about a cluster join mode	GET <cluster-ip:port>/platform/7/cluster/config/join-mode
Modify information about a cluster join mode	PUT <cluster-ip:port>/platform/7/cluster/config/join-mode
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/config/join-mode?describe

### Cluster email resource

View or modify cluster email notification settings.

Operation	Method and URI
View cluster email notification settings	GET <cluster-ip:port>/platform/3/cluster/email
Modify cluster email notification settings	PUT <cluster-ip:port>/platform/3/cluster/email
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/email?describe

## Cluster identity resource

View or modify cluster information that displays at login.

Operation	Method and URI
View login display information	GET <cluster-ip:port>/platform/5/cluster/identity
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/identity?describe

## Cluster internal networks resource

View or modify internal network settings.

Operation	Method and URI
View information about a cluster internal network	GET <cluster-ip:port>/platform/7/cluster/internal-networks
Modify information about a cluster internal network	PUT <cluster-ip:port>/platform/7/cluster/internal-networks
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/internal-networks?describe

## Cluster nodes resource

View the nodes on a cluster.

Operation	Method and URI
View the nodes on a cluster	GET <cluster-ip:port>/platform/7/cluster/nodes
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes?describe

## Cluster add node resource

Add a node to a cluster.

Operation	Method and URI
Add a node to a cluster	POST <cluster-ip:port>/platform/3/cluster/add-node
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/add-node?describe

## Cluster nodes available resource

View all the nodes that are available to add to a cluster.

Operation	Method and URI
List all the nodes that are available to add to a cluster	GET <cluster-ip:port>/platform/3/cluster/nodes-available
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes-available?describe

## Cluster nodes LNN resource

View node information or modify one or more node settings.

Operation	Method and URI
View node information	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>
Modify one or more node settings	PUT <cluster-ip:port>/platform/7/cluster/nodes/<Inn>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>?describe

## Cluster update LNNs resource

Modify the list of current LNNs with respective new LNNs to be used for configuration.

Operation	Method and URI
Modify list of current LNNs to include new LNNs	PUT <cluster-ip:port>/platform/7/cluster/update-lnns
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/update-lnns?describe

## Cluster nodes Inn driveconfig resource

View or modify a node's drive subsystem XML configuration file.

Operation	Method and URI
View a node's drive subsystem XML configuration file	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/driveconfig
Modify a node's drive subsystem XML configuration file	PUT <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/driveconfig
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/driveconfig?describe

## Cluster nodes LNN drives resource

List the drives on the specified node.

Operation	Method and URI
List the drives on the specified node	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives?describe

## Cluster nodes LNN drives purpose list resource

View a list of the purposes that can be applied to drives on the specified node.

Operation	Method and URI
View a list of the purposes that can be applied to drives on the specified node	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives-purposelist
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives-purposelist?describe

## Cluster nodes LNN drives drive ID resource

View information about a specific drive.

Operation	Method and URI
View information about a specific drive	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives/<driveid>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives/<driveid>?describe

## Cluster nodes LNN drives add drive ID resource

Add drives to a node in a OneFS cluster.

Operation	Method and URI
Add drives to a node	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/add
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/add?describe

## Cluster nodes LNN drives drive ID firmware resource

View information about the firmware on the drives on a node.

Operation	Method and URI
View information about the firmware on a drive	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives/<driveid>/firmware
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes/<Inn>/drives/<driveid>/firmware?describe

## Cluster nodes LNN drives drive ID firmware update resource

View firmware update information for drives on this node.

Operation	Method and URI
View firmware update information	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/firmware/update
Start a drive firmware update	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/firmware/update
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/firmware/update?describe

## Cluster nodes LNN drives drive ID format resource

Format drives in a node on a OneFS cluster.

Operation	Method and URI
Format a drive for use by OneFS	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/format
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/format?describe

## Cluster nodes LNN drives drive ID purpose resource

Assign drives to specific use cases on a OneFS cluster.

Operation	Method and URI
Assign a drive to a specific use case	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/purpose
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/purpose?describe

## Cluster nodes LNN drives drive ID smartfail resource

Remove drives from a node on a OneFS cluster.

Operation	Method and URI
Remove a drive from use by OneFS.	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/smartfail
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/smartfail?describe

## Cluster nodes LNN drives drive ID stopfail resource

Stop smartfailing drives in a OneFS cluster.

Operation	Method and URI
Stop smartfailing a drive	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/stopfail
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/stopfail?describe

## Cluster nodes LNN drives drive ID suspend resource

Temporarily remove drives from a OneFS cluster.

Operation	Method and URI
Temporarily remove a drive from use by OneFS	POST <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/suspend
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/drives/<driveid>/suspend?describe

## Cluster nodes LNN hardware resource

Retrieve node hardware identification information.

Operation	Method and URI
View node hardware ID information	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/hardware
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/hardware?describe

## Cluster nodes LNN internal IP address resource

View a node's internal IP address information.

Operation	Method and URI
View internal IP address information for a node	GET <cluster-ip:port>/platform/7/cluster/nodes/<lnn>/internal-ip-address
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cluster/nodes/<lnn>/internal-ip-address?describe

## Cluster nodes LNN partitions resource

Retrieve node partition information.

Operation	Method and URI
View node partition information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/partition
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/partition?describe

## Cluster nodes LNN partitions resource

Retrieve node partition information.

Operation	Method and URI
View node partition information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/partition
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/partition?describe

## Cluster nodes LNN reboot resource

Reboot a node specified by logical node number (LNN).

Operation	Method and URI
Reboot a node specified by LNN	POST <cluster-ip:port>/platform/5/cluster/nodes/<lnn>/reboot
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<lnn>/reboot?describe

## Cluster nodes LNN sensors resource

Retrieve node sensor information.

Operation	Method and URI
View node sensor information	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/sensors
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<Inn>/sensors?describe

## Cluster nodes LNN shutdown resource

Shut down a node specified by logical node number (LNN).

Operation	Method and URI
Shut down a node specified by LNN	POST <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/shutdown
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/shutdown?describe

## Cluster nodes Inn sleds resource

Get detailed information for all sleds in this node.

Operation	Method and URI
View detailed information for all sleds in this node.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/sleds
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/sleds?describe

## Cluster nodes Inn sleds sledid resource

Get detailed information for the sled specified by <sledid>, or all sleds if <sledid> is all, in the node specified by <Inn>.

Operation	Method and URI
View detailed information for one or all sleds on the node specified by <Inn>	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/sleds/<sledid>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/cluster/nodes/<Inn>/sleds/<sledid>?describe

## Cluster nodes LNN state resource

Retrieve node state information by specified logical node number (LNN).

Operation	Method and URI
View node state information by specified LNN	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state?describe

## Cluster nodes LNN state readonly resource

Retrieve or modify node readonly state information.

Operation	Method and URI
View node readonly state information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/readonly
Modify one or more node readonly state settings	PUT <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/readonly
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/readonly?describe

## Cluster nodes LNN state service light resource

Retrieve or modify node service light state information.

Operation	Method and URI
View node service light state information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/servicelight
Modify one or more node service light state settings	PUT <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/servicelight
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/servicelight?describe

## Cluster nodes LNN state smartfail resource

Retrieve or modify node smartfail state information.

Operation	Method and URI
View node smartfail state information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/smartfail
Modify the smartfail state of a node.	PUT <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/smartfail
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/state/smartfail?describe

## Cluster nodes LNN status

Retrieve node status information.

Operation	Method and URI
View node status information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/status
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/status?describe

## Cluster nodes LNN status battery status resource

Retrieve node battery status information.

Operation	Method and URI
View node battery status information	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/status/batterystatus
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/nodes/<lnn>/status/batterystatus?describe

## Local cluster nodes resource

List the nodes on the cluster.

Operation	Method and URI
List the nodes on the cluster	GET <cluster-ip:port>/platform/7/local/cluster/nodes
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/local/cluster/nodes?describe

## Local cluster nodes LNN resource

Retrieve node settings by logical node number (LNN), or modify one or more node settings.

Operation	Method and URI
List node settings by LNN	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>
Modify node settings by LNN	PUT <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>?describe

## Local cluster nodes LNN drives resource

List the drives on a node, specified by logical node number (LNN).

Operation	Method and URI
List drives on a node by LNN	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drives
List a specific drive on a node by LNN	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drives/<drive-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drives?describe
	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drives/<drive-id>?describe

## Local cluster nodes LNN drives firmware resource

Retrieve firmware information for a specific drive on a node, specified by logical node number (LNN).

Operation	Method and URI
Retrieve firmware information for a specific drive on a node	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drive/<drive-id>/firmware
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/drive/<drive-id>/firmware?describe

## Local cluster nodes LNN internal IP address resource

View internal IP addresses for a node.

Operation	Method and URI
View internal IP addresses for a node.	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/internal-ip-address
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/local/cluster/nodes/<lnn-id>/internal-ip-address?describe

## Cluster owner resource

Retrieve cluster contact information settings.

Operation	Method and URI
View cluster contact information settings	GET <cluster-ip:port>/platform/1/cluster/owner
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/cluster/owner?describe

## Cluster file system statistics resource

Retrieve file system statistics.

Operation	Method and URI
View file system statistics	GET <cluster-ip:port>/platform/1/cluster/statfs
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/cluster/statfs?describe

## Cluster time resource

Retrieve the current time as reported by each node, or modify cluster time settings.

### Note

If NTP is configured for the cluster, the cluster time is automatically synchronized to the time reported by the configured NTP servers.

Operation	Method and URI
View the current time as reported by each node	GET <cluster-ip:port>/platform/3/cluster/time
Set cluster time. Time will mostly be synchronized across nodes, but there may be slight drift.	PUT <cluster-ip:port>/platform/3/cluster/time
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/time?describe

## Cluster time zone resource

View cluster time zone information, or set a new time zone for a cluster.

Operation	Method and URI
View the cluster time zone	GET <cluster-ip:port>/platform/3/cluster/timezone
Set a new time zone for a cluster	PUT <cluster-ip:port>/platform/3/cluster/timezone
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/timezone?describe

## Cluster time zone regions resource

List time zone regions.

Operation	Method and URI
List time zone regions	GET <cluster-ip:port>/platform/3/cluster/timezone/regions/<region>

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/timezone/regions/<region>?describe

### Cluster time zone settings resource

Retrieve or modify cluster time zone settings.

Operation	Method and URI
View cluster time zone setting information	GET <cluster-ip:port>/platform/3/cluster/timezone/settings
Modify one or more node readonly state settings	PUT <cluster-ip:port>/platform/3/cluster/timezone/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/timezone/settings?describe

### Local cluster time resource

View the current time on the local node.

Operation	Method and URI
View the current time on the local node	GET <cluster-ip:port>/platform/3/local/cluster/time
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/local/cluster/time?describe

### Cluster version resource

Retrieve the OneFS version of each node on the cluster.

#### Note

The versions of OneFS should be the same on all nodes unless an upgrade is in progress.

Operation	Method and URI
View the OneFS version on each node	GET <cluster-ip:port>/platform/3/cluster/version
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cluster/version

## SSH settings resource

View or modify SSH settings

Operation	Method and URI
List the SSH settings	GET <cluster-ip:port>/platform/7/protocols/ssh/settings
Modify SSH settings	PUT <cluster-ip:port>/platform/7/protocols/ssh/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/protocols/ssh/settings?describe

## IP address pools

Within a subnet, you can partition a cluster's external network interfaces into pools of IP address ranges. The pools enable you to customize your storage network to serve different groups of users. You can configure subnets in IPv4 or IPv6.

You can associate IP address pools with a node, a group of nodes, or NIC ports. For example, you can set up one subnet for storage nodes and another subnet for accelerator nodes. Similarly, you can allocate ranges of IP addresses on a subnet to different teams, such as engineering and sales. These options help you create a storage topology that matches the demands of your network.

In addition, network provisioning rules streamline the setup of external connections. After you configure the rules with network settings, you can apply the settings to new nodes.

As a standard feature, the OneFS SmartConnect module balances connections among nodes by using a round-robin policy with static IP addresses and one IP address pool for each subnet. Activating a SmartConnect Advanced license adds features, such as defining IP address pools to support multiple DNS zones.

## Cluster external IPs resource

Contains the external IP addresses for the cluster.

Operation	Method and URI
Get external IP addresses for the cluster	GET <cluster-ip:port>/platform/2/cluster/external-ips
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/2/cluster/external-ips?describe

## Structure of the file system

OneFS presents all the nodes in a cluster as a global namespace—that is, as the default file share, `/ifs`.

In the file system, directories are inode number links. An inode contains file metadata and an inode number, which identifies a file's location. OneFS dynamically allocates inodes, and there is no limit on the number of inodes.

To distribute data among nodes, OneFS sends messages with a globally routable block address through the cluster's internal network. The block address identifies the node and the drive storing the block of data.

#### Note

We recommend that you do not save data to the root `/ifs` file path but in directories below `/ifs`. The design of your data storage structure should be planned carefully. A well-designed directory optimizes cluster performance and cluster administration.

### File system settings character-encodings resource

Modify or retrieve information about settings for character-encodings.

Operation	Method and URI
Retrieve default character-encodings settings for the cluster	GET <cluster-ip:port>/platform/7/filesystem/settings/character-encodings
Modify the default character-encodings settings for the cluster	PUT <cluster-ip:port>/platform/7/filesystem/settings/character-encodings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/filesystem/settings/character-encodings?describe

### File system settings access-time resource

Modify or retrieve information about settings for the file system access-time.

Operation	Method and URI
Retrieve default access-time settings	GET <cluster-ip:port>/platform/1/filesystem/settings/access-time
Modify the default access-time settings	PUT <cluster-ip:port>/platform/1/filesystem/settings/access-time
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/filesystem/settings/access-time?describe

## Licensing

All Isilon software and hardware must be licensed through EMC Software Licensing Central (SLC).

A record of your active licenses and your cluster hardware is contained in a license file that is stored in two locations: one copy of the license file is stored in the SLC repository, and another copy of the license file is stored on your cluster. The license file contains a record of the following license types:

- OneFS
- Additional software modules

The license file on your cluster, and the license file in the SLC repository, must match your installed hardware and software. Therefore, you must submit a request to update your license file when you:

- Upgrade for the first time to OneFS 8.1 or later

- Add new hardware or upgrade the existing hardware in your cluster
- Require the activation of an optional software module

To request a change to your license file, you must create a file that contains an updated list of your required hardware and software licenses and submit it to EMC Software Licensing Central (SLC). You can generate that file, known as an activation file, from your OneFS interface.

Licenses are created after you generate an activation file, submit the file to EMC Software Licensing Central (SLC), receive a license file back from SLC, and upload the license file to your cluster.

---

#### Note

If you are running the free version of IsilonSD edge, you have access to all optional software modules except for Cloudpools, SmartLock, and SyncIQ. For access to any of those three modules, you must purchase an IsilonSD Edge license.

---

## Licensing resources

You can retrieve information about OneFS feature licenses, or install a new license key.

### License licenses resource

Retrieve information about OneFS feature licenses, or install a license key.

Operation	Method and URI
Retrieve license information for all licensable OneFS features	GET <cluster-ip>:<port>/platform/1/license/licenses
Retrieve license information for a specific OneFS features	GET <cluster-ip>:<port>/platform/1/license/licenses/<name>
Install a new license key	POST <cluster-ip>:<port>/platform/1/license/licenses
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip>:<port>/platform/1/license/licenses?describe
	GET <cluster-ip>:<port>/platform/1/license/licenses/<name>?describe

### License EULA resource

Retrieve the OneFS end user license agreement (EULA) as plain text.

Operation	Method and URI
Retrieve the OneFS EULA as plain text	GET <cluster-ip>:<port>/platform/1/license/eula
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip>:<port>/platform/1/license/eula?describe

## Security hardening

Security hardening is the process of configuring a system to reduce or eliminate as many security risks as possible.

When you apply a hardening profile on an Isilon cluster, OneFS reads the security profile file and applies the configuration defined in the profile to the cluster. If required, OneFS identifies configuration issues that prevent hardening on the nodes. For example, the file permissions on a particular directory might not be set to the expected value, or the required directories might be missing. When an issue is found, you can choose to allow OneFS to resolve the issue, or you can defer resolution and fix the issue manually.

---

### Note

The intention of the hardening profile is to support the Security Technical Implementation Guides (STIGs) that are defined by the Defense Information Systems Agency (DISA) and applicable to OneFS. Currently, the hardening profile only supports a subset of requirements defined by DISA in STIGs. The hardening profile is meant to be primarily used in Federal accounts.

---

If you determine that the hardening configuration is not right for your system, OneFS allows you to revert the security hardening profile. Reverting a hardening profile returns OneFS to the configuration achieved by resolving issues, if any, prior to hardening.

You must have an active security hardening license and be logged in to the Isilon cluster as the root user to apply hardening to OneFS. To obtain a license, contact your Isilon sales representative.

## Hardening resources

Apply, resolve, revert, or retrieve information about hardening on a cluster.

### Hardening apply resource

Apply hardening on a cluster.

Operation	Method and URI
Apply hardening on a cluster	POST <cluster-ip:port>/platform/3/hardening/apply

### Hardening resolve resource

Resolve issues related to hardening that are encountered in the current cluster configuration.

Operation	Method and URI
Resolve hardening issues on a cluster	POST <cluster-ip:port>/platform/3/hardening/resolve

## Hardening revert resource

Revert hardening on a cluster.

Operation	Method and URI
Revert hardening on a cluster	POST <cluster-ip:port>/platform/3/hardening/revert

## Hardening state resource

Retrieve the state of the current hardening operation, if one is in progress.

### Note

This is different from the hardening status resource, which retrieves the overall hardening status on the cluster.

Operation	Method and URI
Retrieve the state (apply or revert) of the current hardening operation	GET <cluster-ip:port>/platform/3/hardening/state
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/hardening/state?describe

## Hardening status resource

Retrieve a message indicating whether the cluster is hardened. This also includes node-specific hardening status if hardening is enabled on at least one node.

### Note

This is different from the hardening state resource, which returns that state of a specific hardening operation.

Operation	Method and URI
Retrieve a message indicating if a cluster is hardened	GET <cluster-ip:port>/platform/3/hardening/status
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/hardening/status?describe

## Upgrading OneFS

Two options are available for upgrading the OneFS operating system: a rolling upgrade or a simultaneous upgrade. Before upgrading OneFS software, a pre-upgrade check must be performed.

A rolling upgrade individually upgrades and restarts each node in the Isilon cluster sequentially. During a rolling upgrade, the cluster remains online and continues serving clients with no interruption in service, although some connection resets may occur on SMB clients. Rolling upgrades are performed sequentially by node number, so a rolling

upgrade takes longer to complete than a simultaneous upgrade. The final node in the upgrade process is the node that you used to start the upgrade process.

---

#### Note

Rolling upgrades are not available for all clusters. For instructions on how to plan an upgrade, prepare the cluster for upgrade, and perform an upgrade of the operating system, see the [OneFS Upgrades – Isilon Info Hub](#)

---

A simultaneous upgrade installs the new operating system and restarts all nodes in the cluster at the same time. Simultaneous upgrades are faster than rolling upgrades but require a temporary interruption of service during the upgrade process. Your data is inaccessible during the time that it takes to complete the upgrade process.

Before beginning either a simultaneous or rolling upgrade, OneFS compares the current cluster and operating system with the new version to ensure that the cluster meets certain criteria, such as configuration compatibility (SMB, LDAP, SmartPools), disk availability, and the absence of critical cluster events. If upgrading puts the cluster at risk, OneFS warns you, provides information about the risks, and prompts you to confirm whether to continue the upgrade.

If the cluster does not meet the pre-upgrade criteria, the upgrade does not proceed, and the unsupported statuses are listed.

---

#### Note

We recommend that you run the optional pre-upgrade checks. Before starting an upgrade, OneFS checks that your cluster is healthy enough to complete the upgrade process. Some of the pre-upgrade checks are mandatory, and will be performed even if you choose to skip the optional checks. All pre-upgrade checks contribute to a safer upgrade.

---

## Upgrade cluster resources

View, modify, create, or delete information related to OneFS cluster upgrades.

### Upgrade cluster resource

Retrieve cluster-wide OneFS upgrade status information.

Operation	Method and URI
Retrieve upgrade status information for the cluster	GET <cluster-ip:port>/platform/7/upgrade/cluster
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster?describe

### Upgrade cluster pause resource

Pause a running upgrade process.

Operation	Method and URI
Pause a running upgrade process	GET <cluster-ip:port>/platform/7/upgrade/cluster/pause

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster/pause?describe

### Upgrade cluster resume resource

Resume a paused upgrade process.

Operation	Method and URI
Resume a paused upgrade process	GET <cluster-ip:port>/platform/7/upgrade/cluster/resume
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster/resume?describe

### Upgrade cluster upgrade resource

Add nodes to a running upgrade, or modify settings in order to start an upgrade.

Operation	Method and URI
Add nodes to a running upgrade	POST <cluster-ip:port>/platform/7/upgrade/cluster/upgrade
Modify settings for an upgrade	PUT <cluster-ip:port>/platform/7/upgrade/cluster/upgrade
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster/upgrade?describe

### Upgrade cluster assess resource

Start an upgrade assessment for the cluster.

Operation	Method and URI
Start an upgrade assessment	POST <cluster-ip:port>/platform/5/upgrade/cluster/assess
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/upgrade/cluster/assess?describe

### Upgrade cluster commit resource

Commit the upgrade of a cluster.

Operation	Method and URI
Commit the upgrade of a cluster	POST <cluster-ip:port>/platform/3/upgrade/cluster/commit

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/commit?describe

### Upgrade cluster add remaining nodes resource

Absorb any remaining or new nodes into the existing upgrade.

Operation	Method and URI
Absorb remaining or new nodes into existing upgrade	POST <cluster-ip:port>/platform/3/upgrade/cluster/add_remaining_nodes
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/add_remaining_nodes?describe

### Upgrade cluster archive resource

Start an archive of an upgrade.

Operation	Method and URI
Start an archive of an upgrade	POST <cluster-ip:port>/platform/3/upgrade/cluster/archive
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/archive?describe

### Upgrade cluster nodes resource

View information about nodes during an upgrade, rollback, or pre-upgrade assessment.

Operation	Method and URI
View information about nodes during an upgrade, rollback, or pre-upgrade assessment	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes
View information about a specific node during an upgrade or assessment	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes/<Inn>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes?describe
	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes/<Inn>?describe

### Upgrade cluster nodes firmware status resource

View firmware status for a specific node.

Operation	Method and URI
Retrieve firmware status for a specific node	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes/<Inn>/firmware/status

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/nodes/<Lnn>/firmware/status?describe

### Upgrade cluster nodes patch synchronization resource

Retry all pending patch synchronization operations.

Operation	Method and URI
Retry all pending patch synchronization operations	POST <cluster-ip:port>/platform/4/upgrade/cluster/nodes/<LNN>/patch/sync
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/upgrade/cluster/nodes/<LNN>/patch/sync?describe

### Upgrade cluster firmware assess resource

Start a firmware upgrade assessment on the cluster.

Operation	Method and URI
Start a firmware upgrade assessment	POST <cluster-ip:port>/platform/3/upgrade/cluster/firmware/assess
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/assess?describe

### Upgrade cluster firmware progress resource

Retrieve cluster-wide firmware upgrade status information.

Operation	Method and URI
Retrieve cluster-wide firmware upgrade status information	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/progress
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/progress?describe

### Upgrade cluster firmware status resource

Retrieve the firmware status for the cluster.

Operation	Method and URI
Retrieve firmware status for the cluster	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/status
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/status?describe

## Upgrade cluster firmware upgrade resource

Upgrade firmware on a OneFS cluster.

Operation	Method and URI
Start a firmware upgrade	POST <cluster-ip:port>/platform/3/upgrade/cluster/firmware/upgrade
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/firmware/upgrade?describe

## Upgrade cluster retry last action resource

Retry the previous upgrade action if the previous attempt failed.

Operation	Method and URI
Retry the previous upgrade action	POST <cluster-ip:port>/platform/3/upgrade/cluster/retry_last_action
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/retry_last_action?describe

## Upgrade cluster rollback resource

Roll back the upgrade of a cluster.

Operation	Method and URI
Roll back the upgrade of a cluster	POST <cluster-ip:port>/platform/3/upgrade/cluster/rollback
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/rollback?describe

## Upgrade cluster rolling reboot resource

Perform a rolling reboot of the cluster.

Operation	Method and URI
Perform a rolling reboot of the cluster	POST <cluster-ip:port>/platform/7/upgrade/cluster/rolling-reboot
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster/rolling-reboot?describe

## Upgrade cluster patch patches resource

List, install, or delete patches.

Operation	Method and URI
List all patches	GET <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches
View a single patch	GET <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches/<patch>
Install a patch	POST <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches
Uninstall a patch	DELETE <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches/<patch>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches?describe
	GET <cluster-ip:port>/platform/7/upgrade/cluster/patch/patches/<patch>?describe

## Upgrade cluster patch abort resource

Cancel the previous action performed by the patch system.

Operation	Method and URI
Cancel the previous action performed by the patch system	POST <cluster-ip:port>/platform/3/upgrade/cluster/patch/abort
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/upgrade/cluster/patch/abort?describe

## Cluster date and time

The Network Time Protocol (NTP) service is configurable manually, so you can ensure that all nodes in a cluster are synchronized to the same time source.

The NTP method automatically synchronizes cluster date and time settings through an NTP server. Alternatively, you can set the date and time reported by the cluster by manually configuring the service.

Windows domains provide a mechanism to synchronize members of the domain to a master clock running on the domain controllers, so OneFS adjusts the cluster time to that of Active Directory with a service. If there are no external NTP servers configured, OneFS uses the Windows domain controller as the NTP time server. When the cluster and domain time become out of sync by more than 4 minutes, OneFS generates an event notification.

---

### Note

If the cluster and Active Directory become out of sync by more than 5 minutes, authentication will not work.

---

## NTP resources

List, modify, create, or delete Network Time Protocol (NTP) configuration information.

### NTP servers resource

Retrieve NTP servers, or create, modify or delete NTP server entries.

Operation	Method and URI
List all NTP servers	GET <cluster-ip:port>/platform/3/protocols/ntp/servers
Retrieve a specific NTP server	GET <cluster-ip:port>/platform/3/protocols/ntp/servers/<server-id>
Create an NTP server entry	POST <cluster-ip:port>/platform/3/protocols/ntp/servers
Modify the key value for a specific NTP server	PUT <cluster-ip:port>/platform/3/protocols/ntp/servers/<server-id>
Delete all NTP server entries	DELETE <cluster-ip:port>/platform/3/protocols/ntp/servers
Delete a specific NTP server entry	DELETE <cluster-ip:port>/platform/3/protocols/ntp/servers/<server-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ntp/servers?describe
	GET <cluster-ip:port>/platform/3/protocols/ntp/servers/<server-id>?describe

### NTP settings resource

List or modify Network Time Protocol (NTP) settings information.

Operation	Method and URI
List all NTP settings	GET <cluster-ip:port>/platform/3/protocols/ntp/settings
Modify NTP settings (all input fields are optional, but you must supply one or more)	PUT <cluster-ip:port>/platform/3/protocols/ntp/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/protocols/ntp/settings?describe

## Managing SNMP settings

You can use SNMP to monitor cluster hardware and system information. You can configure settings through either the web administration interface or the command-line interface.

You can enable SNMP monitoring on individual nodes in the cluster, and you can monitor information cluster-wide from any node when you enable SNMP on each

node. When using SNMP on an Isilon cluster, you should use a fixed general username. A password for the general user can be configured in the web administration interface.

You should configure a network monitoring system (NMS) to query each node directly through a static IPv4 or IPv6 address. This approach allows you to confirm that all nodes have external IP addresses and therefore respond to SNMP queries. Because the SNMP proxy is enabled by default, the SNMP implementation on each node is configured automatically to proxy for all other nodes in the cluster except itself. This proxy configuration allows the Isilon Management Information Base (MIB) and standard MIBs to be exposed seamlessly through the use of context strings for supported SNMP versions. After you download and save the appropriate MIBs, you can configure SNMP monitoring through either the web administration interface or through the command-line interface.

## SNMP settings resource

List or modify Simple Network Management Protocol (SNMP) settings.

Operation	Method and URI
List SNMP settings	GET <cluster-ip:port>/platform/5/protocols/snmp/settings
Modify SNMP settings (all input fields are optional, but you must supply one or more)	PUT <cluster-ip:port>/platform/5/protocols/snmp/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/protocols/snmp/settings?describe

## Hardware

You can update certain information about Isilon hardware ports and tapes through the OneFS system configuration API.

### Hardware resources

You can list, modify, or delete information about ports and tapes, and you can re-scan tape devices.

### Upgrade hardware start resource

Start the hardware upgrade process of a specified type on a specified node pool.

Operation	Method and URI
Start hardware upgrade process	POST <cluster-ip:port>/platform/5/upgrade/hardware/start
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/upgrade/hardware/start?describe

## Upgrade hardware status resource

View the status of hardware upgrades in progress.

Operation	Method and URI
View hardware upgrade status	GET <cluster-ip:port>/platform/5/upgrade/hardware/status
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/upgrade/hardware/status?describe

## Upgrade hardware stop resource

Stop a hardware upgrade that is in progress.

Operation	Method and URI
Stop a hardware upgrade process	POST <cluster-ip:port>/platform/5/upgrade/hardware/stop
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/upgrade/hardware/stop?describe

## Fibre Channel ports resource

Retrieve or modify information about Fibre Channel ports in Isilon hardware.

Operation	Method and URI
List Fibre Channel ports	GET <cluster-ip>:<port>/platform/3/hardware/fcports
Retrieve one Fibre Channel port	GET <cluster-ip>:<port>/platform/3/hardware/fcports/<port>
Change information about Fibre Channel ports	PUT <cluster-ip>:<port>/platform/3/hardware/fcports/<port>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip>:<port>/platform/3/hardware/fcports?describe
	GET <cluster-ip>:<port>/platform/3/hardware/fcports/<port>?describe

## Hardware tapes resource

List, modify, re-scan, or remove tape or media changer devices.

Operation	Method and URI
List tape and media changer devices	GET <cluster-ip>:<port>/platform/3/hardware/tapes
Modify tape and media changer devices	PUT GET <cluster-ip>:<port>/platform/3/hardware/tapes/<name*>

Operation	Method and URI
Re-scan tape and media changer devices	POST <cluster-ip>:<port>/platform/3/hardware/tape/<name*>
Remove tape and media changer devices	DELETE PUT <cluster-ip>:<port>/platform/3/hardware/tape/<name*>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip>:<port>/platform/3/hardware/tapes?describe
	GET GET <cluster-ip>:<port>/platform/3/hardware/tapes/<name*>?describe

## File pools

File pools are sets of files that you define to apply policy-based control of the storage characteristics of your data.

The initial installation of OneFS places all files in the cluster into a single file pool, which is subject to the default file pool policy. SmartPools enables you to define additional file pools, and create policies that move files in these pools to specific node pools and tiers.

File pool policies match specific file characteristics (such as file size, type, date of last access or a combination of these and other factors), and define specific storage operations for files that match them. The following examples demonstrate a few ways you can configure file pool policies:

- You can create a file pool policy for a specific file extension that requires high availability.
- You can configure a file pool policy to store that type of data in a storage pool that provides the fastest reads or read/writes.
- You can create another file pool policy to evaluate last accessed date, allowing you to store older files in storage pool best suited for archiving for historical or regulatory purposes.

## File pool resources

You can retrieve, create, modify, or delete file pool configurations and settings.

### File pool default policy resource

Modify or retrieve information about the default file pool policy.

Operation	Method and URI
Retrieve information about the default file pool policy	GET <cluster-ip:port>/platform/4/filepool/default-policy
Modify the default file pool policy	PUT <cluster-ip:port>/platform/4/filepool/default-policy
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/filepool/default-policy?describe

## File pool policies resource

Create, modify, delete, or retrieve information about file pool policies.

Operation	Method and URI
Retrieve information about all file pool policies	GET <cluster-ip:port>/platform/4/filepool/policies
Retrieve information about a file pool policy	GET <cluster-ip:port>/platform/4/filepool/policies/<policy name>
Create a file pool policy	POST <cluster-ip:port>/platform/4/filepool/policies
Modify a file pool policy	PUT <cluster-ip:port>/platform/4/filepool/policies/<policy name>
Delete a file pool policy	DELETE <cluster-ip:port>/platform/4/filepool/policies/<policy name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/filepool/policies?describe
	GET <cluster-ip:port>/platform/4/filepool/policies/<policy name>?describe

## File pool templates resource

Retrieve information about OneFS file pool policy templates.

Operation	Method and URI
Retrieve information about file pool policy templates	GET <cluster-ip:port>/platform/4/filepool/templates
Retrieve information about a file pool policy template	GET <cluster-ip:port>/platform/4/filepool/templates/<template name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/filepool/templates?describe
	GET <cluster-ip:port>/platform/4/filepool/templates/<template name>?describe

## File pools API examples

You can see examples for some file pools API requests.

### Create a file pool policy

You can create a file pool policy.

#### Request example

```
POST /platform/1/filepool/policies
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==

{'file_matching_pattern':
  {'or_criteria':
    [
```

```

        {'and_criteria':
          [
            {'operator': '==', 'type': 'path', 'value': '/ifs/
data/vms'}
          ]
        }
      ],
      'name': 'mirror_vms',
      'actions':
        [
          {
            'action_param': '8x',
            'action_type': 'set_requested_protection'
          }
        ]
      }
    }
  }
}

```

### Response example

```

201 Created
Content-type: application/json

{
  "id" : "mirror_vms"
}

```

## Modify a file pool policy

You can modify a file pool policy.

### Request example

In the following example, "vms\_mirror" is the ID of the file pool policy.

```

PUT /platform/1/filepool/policies/vms_mirror
Authorization: Basic QWxhZGRpbjpvGVuIHh1c2FtZQ==

{
  "action_param": "false"
  "action_type": "set_requested_protection"
}

```

### Response example

No message body is returned for this request.

```

204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'

```

## Modify the default file pool policy

You can modify the default file pool policy.

### Request example

```

PUT /platform/1/filepool/policies/
Authorization: Basic QWxhZGRpbjpvGVuIHh1c2FtZQ==

```

```
{
  "action_param": "random"
  "action_type": "set_data_access_pattern"
}
```

**Response example**

No message body is returned for this request.

```
204 No Content
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

**Storage pools overview**

OneFS organizes different node types into separate node pools. In addition, you can organize these node pools into logical tiers of storage. By activating a SmartPools license, you can create file pool policies that store files in these tiers automatically, based on file-matching criteria that you specify.

Without an active SmartPools license, OneFS manages all node pools as a single pool of storage. File data and metadata is striped across the entire cluster so that data is protected, secure, and readily accessible. All files belong to the default file pool and are governed by the default file pool policy. In this mode, OneFS provides functions such as autoprovisioning, compatibilities, virtual hot spare (VHS), SSD strategies, global namespace acceleration (GNA), L3 cache, and storage tiers.

When you activate a SmartPools license, additional functions become available, including custom file pool policies and spillover management. With a SmartPools license, you can manage your data set with more granularity to improve the performance of your cluster.

The following table summarizes storage pool functions based on whether a SmartPools license is active.

Function	Inactive SmartPools license	Active SmartPools license
Automatic storage pool provisioning	Yes	Yes
Node class compatibilities (node equivalency)	Yes	Yes
SSD capacity compatibilities	Yes	Yes
SSD count compatibilities	Yes	Yes
Virtual hot spare	Yes	Yes
SSD strategies	Yes	Yes
L3 cache	Yes	Yes
Tiers	Yes	Yes
GNA	Yes	Yes
File pool policies	No	Yes
Spillover management	No	Yes

## Storage pools resources

You can retrieve, create, modify, or delete system storage pool settings and configurations.

### Storage pool settings resource

Modify or retrieve information about storage pools.

Operation	Method and URI
Get storage pool settings	GET <cluster-ip:port>/platform/5/storagepool/settings
Modify storage pool settings	PUT <cluster-ip:port>/platform/5/storagepool/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/storagepool/settings?describe

### Storage pools tiers resource

Create, delete, or retrieve information about storage pool tiers.

Operation	Method and URI
Get a list of all tiers	GET <cluster-ip:port>/platform/1/storagepool/tiers
Get a single tier	GET <cluster-ip:port>/platform/1/storagepool/tiers/<name or id>
Create a new tier	POST <cluster-ip:port>/platform/1/storagepool/tiers
Delete all tiers	DELETE <cluster-ip:port>/platform/1/storagepool/tiers
Delete a single tier	DELETE <cluster-ip:port>/platform/1/storagepool/tiers/<name or id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/storagepool/tiers?describe

### Storage pools node pools resource

Create, modify, delete, or retrieve information about node pools.

Operation	Method and URI
Get information for all node pools	GET <cluster-ip:port>/platform/3/storagepool/nodepools
Get information for a single node pool	GET <cluster-ip:port>/platform/3/storagepool/nodepools/<pool name or id>
Create a new node pool	POST <cluster-ip:port>/platform/3/storagepool/nodepools

Operation	Method and URI
Modify a node pool	PUT <cluster-ip:port>/platform/3/storagepool/nodepools/<pool name or id>
Delete a manually managed node pool	DELETE <cluster-ip:port>/platform/3/storagepool/nodepools/<pool name or id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/storagepool/nodepools?describe
	GET <cluster-ip:port>/platform/3/storagepool/nodepools/<pool name or id>?describe

### Storage pools resource

Retrieve information about storage pools. You can supply a `toplevels` argument to filter out node pools within tiers.

Operation	Method and URI
Get information for all storage pools	GET <cluster-ip:port>/platform/3/storagepool/storagepools
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/storagepool/storagepools?describe

### Storage pools suggested protection resource

Retrieve information about the suggested protection policy for a storage pool.

Operation	Method and URI
Get information about the suggested protection policy	GET <cluster-ip:port>/platform/1/storagepool/suggested_protection/<NID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/storagepool/suggested_protection/<NID>?describe

### Storagepool compatibilities SSD active resource

Create, delete, modify, or view active SSD compatibilities

Operation	Method and URI
Get a list of active SSD compatibilities	GET <cluster-ip:port>/platform/3/storagepool/compatibilities/ssd/active
Get an SSD compatibility by ID	GET <cluster-ip:port>/platform/3/storagepool/compatibilities/ssd/active/<compatibility-id>
Create a new SSD compatibility	POST <cluster-ip:port>/platform/3/storagepool/compatibilities/ssd/active

Operation	Method and URI
Modify an SSD compatibility	PUT <cluster-ip:port>/platform/3/ storagepool/compatibilities/ssd/active/ <compatibility-id>
Delete an SSD compatibility	DELETE <cluster-ip:port>/platform/3/ storagepool/compatibilities/ssd/active/ <compatibility-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/ storagepool/compatibilities/ssd/active? describe
	GET <cluster-ip:port>/platform/3/ storagepool/compatibilities/ssd/active/ <compatibility-id>?describe

### Storagepool compatibilities SSD available resource

View a list of available SSD compatibilities.

Operation	Method and URI
Get a list of available SSD compatibilities	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/ssd/available
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/ssd/available? describe

### Storagepool compatibilities class available resource

View a list of available class compatibilities.

Operation	Method and URI
Get a list of available class compatibilities	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/class/available
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/class/available? describe

### Storage pool compatibilities class active resource

Create, delete, or retrieve information about a storage pool compatibility.

Operation	Method and URI
Get all storage pool compatibilities	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/class/active
Get a storage pool compatibility by ID	GET <cluster-ip:port>/platform/1/ storagepool/compatibilities/class/active/ <ID>
Create a storage pool compatibilities	POST <cluster-ip:port>/platform/1/ storagepool/compatibilities/class/active

Operation	Method and URI
Delete a storage pool compatibility by ID	DELETE <cluster-ip:port>/platform/1/storagepool/compatibilities/class/active/<ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/storagepool/compatibilities/class/active?describe
	GET <cluster-ip:port>/platform/1/storagepool/compatibilities/class/active/<ID>?describe

### Storage pool status resource

Retrieves the health status of the overall OneFS pool system.

Operation	Method and URI
Get the status of the OneFS pool system	GET <cluster-ip:port>/platform/1/storagepool/status
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/storagepool/status?describe

### Storage pools API examples

You can see examples for some storage pools API calls.

#### Modify storage pool settings

You can modify the global storage pool settings on the system.

##### Request example

You must specify at least one property in the request.

```
PUT /platform/1/storagepool/settings
Authorization: Basic QWxhZGRpbjpvCGVuIHN1c2FtZQ==

{
  'global_namespace_acceleration_enabled': false,
  'automatically_manage_protection': 'all'
}
```

##### Response example

No message body is returned for this request.

```
204 NO CONTENT
Content-type: text/plain,
Allow: 'GET, PUT, HEAD'
```

## Create a tier

Create a tier on the system.

### Request example

```
POST /platform/1/storagepool/tiers
Authorization: Basic QWxhZGRpbjpvVG9uIHN1c2FtZQ==

{
  'name': 'myTier'
}
```

### Response example

```
201 CREATED
Content-type: application/json,
Allow: 'GET, POST, HEAD, DELETE'

{
  "id": "myTier"
}
```

## Modify a tier

Modify a tier.

### Request example

When you modify a set of nodes that belong to a tier, you must also set the `tier` property on that node pool through the `/platform/1/storagepool/nodepools` URI.

```
PUT /platform/1/storagepool/tiers/myTier
Authorization: Basic QWxhZGRpbjpvVG9uIHN1c2FtZQ==

{
  "name": myTier
}
```

```
PUT /platform/1/storagepool/nodepools
Authorization: Basic QWxhZGRpbjpvVG9uIHN1c2FtZQ==

{
  "tier": myTier
}
```

### Response example

No message body is returned for this request.

```
204 NO CONTENT
Content-type: application/json,
Allow: 'GET, POST, PUT, DELETE'
```

## Create a node pool

Create and manually manage a node pool.

### Request example

You must specify a minimum of three lns. After these nodes are added to the newly created node pool and removed from their current node pool, the number of nodes in the original node pool must either be 0 or greater than 2.

```
POST /platform/1/storagepool/nodepools
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'name': 'myPool',
  'lns': [2, 3, 1]
}
```

### Response example

```
201 CREATED
Content-type: application/json,
Allow: 'GET, POST, HEAD, DELETE'

{
  "id": "myPool"
}
```

## Modify a node pool

You can modify a node pool on the system.

### Request example

You must specify at least one property in the body. Additionally, you can only specify lns for manually managed node pools and you must specify a minimum of three lns when modifying a manually managed node pool. If nodes are moved to a new node pool and removed from their current node pool, the number of nodes in the original node pool must either be 0 or greater than 2.

```
PUT /platform/1/storagepool/nodepools/myPool
Authorization: Basic QWxhZGRpbjpvGVuIHN1c2FtZQ==

{
  'tier': 'myTier',
  'name': 'myNewPoolName'
}
```

### Response example

No message body is returned for this request.

```
204 No Content
Content-type: application/json,
Allow: 'GET, POST, PUT, DELETE'
```

## CloudPools

CloudPools extends the capabilities of OneFS by enabling you to specify data to be moved to lower-cost cloud storage. CloudPools can seamlessly connect to

Dell EMC EMC-based cloud storage systems and to popular third-party providers, Amazon S3, Google, and Microsoft Azure.

CloudPools is a licensed module built on the SmartPools file pool policy framework, which gives you granular control of file storage on your cluster. CloudPools extends this file storage control to one or more cloud repositories, which act as additional tiers of OneFS storage.

Prior to the introduction of CloudPools, SmartPools enabled the grouping of nodes into storage pools called node pools, and the classification of node pools as different storage tiers. SmartPools includes a policy framework that allows you to segregate files into logical groups called file pools, and to store those file pools in specific storage tiers.

CloudPools expands the SmartPools framework by treating a cloud repository as an additional storage tier. This enables you to move older or seldom-used data to cloud storage and free up space on your cluster.

As with SmartPools, you define files to be stored in the cloud by creating file pool policies. These policies use file matching criteria to determine which file pools are to be moved to the cloud.

## CloudPools resources

List, create, modify, or delete CloudPools information.

### CloudPools pools resource

View, create, modify, or delete pools.

Operation	Method and URI
List all pools	GET <cluster-ip:port>/platform/7/cloud/pools
Retrieve information about a specific pool	GET <cluster-ip:port>/platform/7/cloud/pools/<pool>
Create a new pool	POST <cluster-ip:port>/platform/7/cloud/pools
Modify a pool	PUT <cluster-ip:port>/platform/7/cloud/pools/<pool>
Delete a pool	DELETE <cluster-ip:port>/platform/7/cloud/pools/<pool>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cloud/pools?describe
	GET <cluster-ip:port>/platform/7/cloud/pools/<pool>?describe

### CloudPools access resource

View, create, or delete cluster identifiers for cloud access.

Operation	Method and URI
List all accessible cluster identifiers	GET <cluster-ip:port>/platform/3/cloud/access

Operation	Method and URI
List cloud access information for a specific cluster	GET <cluster-ip:port>/platform/3/cloud/access/<guid>
Add a cluster to the identifier list	POST <cluster-ip:port>/platform/3/cloud/access
Delete cloud access	DELETE <cluster-ip:port>/platform/3/cloud/access/<guid>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/access?describe
	GET <cluster-ip:port>/platform/3/cloud/access/<guid>?describe

### CloudPools account resource

View, modify, create, or delete cloud account information.

Operation	Method and URI
List all cloud accounts	GET <cluster-ip:port>/platform/7/cloud/accounts
View a specific cloud account	GET <cluster-ip:port>/platform/7/cloud/accounts/<account-id>
Create a new cloud account	POST <cluster-ip:port>/platform/7/cloud/accounts
Modify a cloud account	PUT <cluster-ip:port>/platform/7/cloud/accounts/<account-id>
Delete a cloud account	DELETE <cluster-ip:port>/platform/7/cloud/accounts/<account-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cloud/accounts?describe
	GET <cluster-ip:port>/platform/7/cloud/accounts/<account-id>?describe

### CloudPools TLS client certificates resource

List, import, view, modify or delete a CloudPools TLS client certificate.

Operation	Method and URI
List all cloud TLS client certificates	GET <cluster-ip:port>/platform/7/cloud/certificates
View a specific cloud TLS client certificate	GET <cluster-ip:port>/platform/7/cloud/certificates/<certificate-id>
Create a new cloud TLS client certificate	POST <cluster-ip:port>/platform/7/cloud/certificates
Modify a cloud TLS client certificate	PUT <cluster-ip:port>/platform/7/cloud/certificates/<certificate-id>

Operation	Method and URI
Delete a cloud TLS client certificate	DELETE <cluster-ip:port>/platform/7/cloud/certificates/<certificate-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/cloud/certificates?describe
	GET <cluster-ip:port>/platform/7/cloud/certificates/<certificate-id>?describe

## CloudPools jobs resource

View, modify, or create CloudPools jobs.

Operation	Method and URI
List all CloudPools jobs	GET <cluster-ip:port>/platform/3/cloud/jobs
View a specific CloudPools job	GET <cluster-ip:port>/platform/3/cloud/jobs/<job-id>
Create a new CloudPools job	POST <cluster-ip:port>/platform/3/cloud/jobs
Modify a CloudPools job	PUT <cluster-ip:port>/platform/3/cloud/jobs/<job-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/jobs?describe
	GET <cluster-ip:port>/platform/3/cloud/jobs/<job-id>?describe

## CloudPools job files resource

Retrieve files associated with a Cloudpools job.

Operation	Method and URI
List files associated with a specific CloudPools job	GET <cluster-ip:port>/platform/3/cloud/jobs-files/<job-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/jobs-files/<job-id>?describe

## CloudPools network proxy resource

View, create, modify, or delete network proxy information.

Operation	Method and URI
List all cloud network proxies	GET <cluster-ip:port>/platform/4/cloud/proxies
View a specific cloud network proxy	GET <cluster-ip:port>/platform/4/cloud/proxies/<proxy-id>
Create a new cloud network proxy	POST <cluster-ip:port>/platform/4/cloud/proxies

Operation	Method and URI
Modify a cloud network proxy	PUT <cluster-ip:port>/platform/4/cloud/proxies/<proxy-id>
Delete a cloud network proxy	DELETE <cluster-ip:port>/platform/4/cloud/proxies/<proxy-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/4/cloud/proxies?describe
	GET <cluster-ip:port>/platform/4/cloud/proxies/<proxy-id> ?describe

### CloudPools settings resource

View or modify cloud settings.

Operation	Method and URI
List all cloud settings	GET <cluster-ip:port>/platform/3/cloud/settings
Modify cloud settings	PUT <cluster-ip:port>/platform/3/cloud/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/settings?describe

### CloudPools encryption key resource

Request creation of a new master encryption key for cloud pool encryption.

Operation	Method and URI
Create an encryption key	POST <cluster-ip:port>/platform/3/cloud/settings/encryption_key
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/settings/encryption_key?describe

### CloudPools end user license agreement resource

View, accept or revoke end user license agreement (EULA) telemetry information.

Operation	Method and URI
View telemetry collection EULA acceptance information	GET <cluster-ip:port>/platform/3/cloud/settings/reporting_eula
Accept telemetry collection EULA	POST <cluster-ip:port>/platform/3/cloud/settings/reporting_eula
Revoke acceptance of telemetry collection EULA	DELETE <cluster-ip:port>/platform/3/cloud/settings/reporting_eula

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/cloud/settings/reporting_eula?describe

## SmartQuotas overview

The SmartQuotas module is an optional quota-management tool that monitors and enforces administrator-defined storage limits. Using accounting and enforcement quota limits, reporting capabilities, and automated notifications, SmartQuotas manages storage use, monitors disk storage, and issues alerts when disk-storage limits are exceeded.

Quotas help you manage storage usage according to criteria that you define. Quotas are used for tracking—and sometimes limiting—the amount of storage that a user, group, or project consumes. Quotas help ensure that a user or department does not infringe on the storage that is allocated to other users or departments. In some quota implementations, writes beyond the defined space are denied, and in other cases, a simple notification is sent.

---

### Note

Do not apply quotas to `/ifs/.ifsvar/` or its subdirectories. If you limit the size of the `/ifs/.ifsvar/` directory through a quota, and the directory reaches its limit, jobs such as File-System Analytics fail. A quota blocks older job reports from being deleted from the `/ifs/.ifsvar/` subdirectories to make room for newer reports.

---

The SmartQuotas module requires a separate license. For more information about the SmartQuotas module or to activate the module, contact your EMC sales representative.

## Quotas resources

You can retrieve, create, modify, or delete SmartQuotas configurations and settings.

### Quota license resource

Retrieve license information for the SmartQuotas feature.

Operation	Method and URI
Get license information for SmartQuotas	GET <cluster-ip:port>/platform/5/quota/license
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/5/quota/license?describe

### Quota summary resource

Retrieve summary information about quotas.

Operation	Method and URI
Get summary information about quotas	GET <cluster-ip:port>/platform/1/quota/quotas-summary

Operation	Method and URI
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/quota/quotas-summary?describe

### Quota quotas notification rules resource

Create, modify, delete, or retrieve information about notification rules for a quota.

Operation	Method and URI
Get all notification rules for a quota	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications
Get a notification rule for a quota	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications/<notification-id>
Create notification rules for a quota	POST <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications
Create empty override notification rules for a quota	PUT <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications
Modify notification rules for a quota	PUT <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications/<notification-id>
Delete all notification rules for a quota	DELETE <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications
Delete notification rules for a quota	DELETE <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications/<notification-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications?describe
	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>/notifications/<notification-id>?describe

### Quotas resource

Create, modify, delete, or retrieve information about file system quotas.

Operation	Method and URI
Get all quotas	GET <cluster-ip:port>/platform/7/quota/quotas
Get one quota	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>
Create a quota	POST <cluster-ip:port>/platform/7/quota/quotas
Modify a quota	PUT <cluster-ip:port>/platform/7/quota/quotas/<quota-id>
Delete all quotas	DELETE <cluster-ip:port>/platform/7/quota/quotas
Delete a quota	DELETE <cluster-ip:port>/platform/7/quota/quotas/<quota-id>
View the detailed JSON schema for this resource, which has information	GET <cluster-ip:port>/platform/7/quota/quotas?describe

Operation	Method and URI
about query parameters and object properties.	GET <cluster-ip:port>/platform/7/quota/quotas/<quota-id>?describe

### Quota reports resource

Create, delete, or retrieve information about quota reports.

Operation	Method and URI
Get all quota reports	GET <cluster-ip:port>/platform/1/quota/reports
Get a quota report	GET <cluster-ip:port>/platform/1/quota/reports/<report-id>?contents
Create a quota report	POST <cluster-ip:port>/platform/1/quota/reports/<report-id>?contents
Delete a quota report	DELETE <cluster-ip:port>/platform/1/quota/reports/<report-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/quota/reports?describe
	GET <cluster-ip:port>/platform/1/quota/reports/<report-id>?describe

### Quota about reports resource

Retrieve metadata for individual quota reports.

Operation	Method and URI
Get metadata about a report	GET <cluster-ip:port>/platform/1/quota/reports/<report-id>/about
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/quota/reports/<report-id>/about?describe

### Quota report settings resource

Modify or retrieve information about quota report settings.

Operation	Method and URI
Get quota report settings	GET <cluster-ip:port>/platform/1/quota/settings/reports
Modify quota report settings	PUT <cluster-ip:port>/platform/1/quota/settings/reports
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/quota/settings/reports?describe

## Quota default notifications settings resource

Create, modify, delete, or retrieve information about default quota notification settings.

Operation	Method and URI
List default global notification settings	GET <cluster-ip:port>/platform/7/quota/settings/notifications
View a specific global notification setting	GET <cluster-ip:port>/platform/7/quota/settings/notifications/<notification-id>
Create global notification settings	POST <cluster-ip:port>/platform/7/quota/settings/notifications
Modify a default global notification settings	PUT <cluster-ip:port>/platform/7/quota/settings/notifications/<notification-id>
Delete global notification settings	DELETE <cluster-ip:port>/platform/7/quota/settings/notifications
Delete a specific global notification setting	DELETE <cluster-ip:port>/platform/7/quota/settings/notifications/<notification-id>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/quota/settings/notifications?describe
	GET <cluster-ip:port>/platform/7/quota/settings/notifications/<notification-id>?describe

## Quota mappings settings resource

Create, modify, delete, or retrieve information about quota notification email mapping rules.

Operation	Method and URI
Get quota email mapping settings	GET <cluster-ip:port>/platform/1/quota/settings/mappings
Create quota email mapping settings	POST <cluster-ip:port>/platform/1/quota/settings/mappings/<domain>
Modify quota email mapping setting	PUT <cluster-ip:port>/platform/1/quota/settings/mappings/<domain>
Delete all quota email mapping settings	DELETE <cluster-ip:port>/platform/1/quota/settings/mappings
Delete a quota email mapping setting	DELETE <cluster-ip:port>/platform/1/quota/settings/mappings/<domain>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/1/quota/settings/mappings?describe
	GET <cluster-ip:port>/platform/1/quota/settings/mappings/<domain>?describe

## Antivirus

You can scan the files you store on an Isilon cluster for computer viruses and other security threats by integrating with third-party scanning services through the Internet Content Adaptation Protocol (ICAP).

OneFS sends files through ICAP to a server running third-party antivirus scanning software. These servers are referred to as ICAP servers. ICAP servers scan files for viruses.

After an ICAP server scans a file, it informs OneFS of whether the file is a threat. If a threat is detected, OneFS informs system administrators by creating an event, displaying near real-time summary information, and documenting the threat in an antivirus scan report. You can configure OneFS to request that ICAP servers attempt to repair infected files. You can also configure OneFS to protect users against potentially dangerous files by truncating or quarantining infected files.

Before OneFS sends a file to be scanned, it ensures that the scan is not redundant. If a file has already been scanned and has not been modified, OneFS will not send the file to be scanned unless the virus database on the ICAP server has been updated since the last scan.

---

### Note

Antivirus scanning is available only if all nodes in the cluster are connected to the external network.

---

## Antivirus resources

Retrieve, create, modify, or delete antivirus configurations and settings.

### Antivirus policies resource

Modify, delete, or retrieve information about antivirus policies.

Operation	Method and URI
Get all antivirus policies	GET <cluster-ip:port>/platform/3/antivirus/policies
Create an antivirus policy	POST <cluster-ip:port>/platform/3/antivirus/policies
Delete all antivirus policies	DELETE <cluster-ip:port>/platform/3/antivirus/policies
Get an antivirus policies	GET <cluster-ip:port>/platform/3/antivirus/policies/<policy-name>
Modify an antivirus policy	PUT <cluster-ip:port>/platform/3/antivirus/policies/<policy-name>
Delete an antivirus policies	DELETE <cluster-ip:port>/platform/3/antivirus/policies/<policy-name>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/policies?describe
	GET <cluster-ip:port>/platform/3/antivirus/policies/<policy-name>?describe

## Antivirus quarantine resource

Retrieve or modify information about the quarantine status of files in the `/ifs` directory tree.

Operation	Method and URI
Get antivirus quarantine information	GET <cluster-ip:port>/platform/3/antivirus/quarantine/<path>
Modify antivirus quarantine information	PUT <cluster-ip:port>/platform/3/antivirus/quarantine/<path>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/quarantine/<path>?describe

## Antivirus scan report resource

View or delete information about antivirus scans.

Operation	Method and URI
List all antivirus scan reports	GET <cluster-ip:port>/platform/3/antivirus/reports/scans
View a specific antivirus scan report	GET <cluster-ip:port>/platform/3/antivirus/reports/scans/<ID>
Delete antivirus scan reports, and any threat reports associated with those scans	DELETE <cluster-ip:port>/platform/3/antivirus/reports/scans
Delete a specific antivirus scan report, and any threat reports associated with the scan	DELETE <cluster-ip:port>/platform/3/antivirus/reports/scans<ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/reports/scans?describe
	GET <cluster-ip:port>/platform/3/antivirus/reports/scans/<ID>?describe

## Antivirus threat reports resource

List all antivirus threat reports, or view a specific report.

Operation	Method and URI
List all antivirus threat reports	GET <cluster-ip:port>/platform/3/antivirus/reports/threats
View a specific antivirus threat report	GET <cluster-ip:port>/platform/3/antivirus/reports/threats/<ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/reports/threats?describe
	GET <cluster-ip:port>/platform/3/antivirus/reports/threats/<ID>?describe

## Antivirus scan resource

Enable a client to run an antivirus scan on a single file.

Operation	Method and URI
Manually scan a file	POST <cluster-ip:port>/platform/3/antivirus/scan/
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/scan/?describe

## Antivirus servers resource

List, create, modify or delete all antivirus servers or one antivirus server entry.

Operation	Method and URI
List all antivirus servers	GET <cluster-ip:port>/platform/3/antivirus/servers
Create an antivirus server	POST <cluster-ip:port>/platform/3/antivirus/servers
Delete all antivirus servers	DELETE <cluster-ip:port>/platform/3/antivirus/servers
View an antivirus server entry	GET <cluster-ip:port>/platform/3/antivirus/servers/<ID>
Modify an antivirus server entry	PUT <cluster-ip:port>/platform/3/antivirus/servers/<ID>
Delete an antivirus server entry	DELETE <cluster-ip:port>/platform/3/antivirus/servers/<ID>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/3/antivirus/servers?describe
	GET <cluster-ip:port>/platform/3/antivirus/servers/<ID>?describe

## Antivirus settings resource

View or modify antivirus settings.

Operation	Method and URI
List antivirus settings	GET <cluster-ip:port>/platform/7/antivirus/settings
Modify antivirus settings	PUT <cluster-ip:port>/platform/7/antivirus/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/antivirus/settings?describe

## Performance

This chapter documents the performance-related resource handlers for the OneFS system configuration API.

### Performance settings resource

Retrieve and configure performance settings.

Operation	Method and URI
Retrieve all performance settings	GET <cluster-ip:port>/platform/7/performance/settings
Modify performance settings	PUT <cluster-ip:port>/platform/7/performance/settings
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/performance/settings?describe

### Performance datasets resource

List, create, modify, or delete performance metric datasets.

A dataset is a set of metrics for which performance statistics are collected. For a list of available metrics, refer to the `/performance/metrics` API resource.

Operation	Method and URI
List performance datasets	GET <cluster-ip:port>/platform/7/performance/datasets
View a specific performance dataset	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>
Modify a performance dataset	PUT <cluster-ip:port>/platform/7/performance/datasets/<dataset>
Create a new performance dataset	POST <cluster-ip:port>/platform/7/performance/datasets
Delete a specific performance dataset	DELETE <cluster-ip:port>/platform/7/performance/datasets/<dataset>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/performance/datasets?describe
	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>?describe

### Performance datasets filters resource

List, create, modify, or delete performance dataset filters.

Operation	Method and URI
List performance dataset filters	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters

Operation	Method and URI
View a specific performance dataset filter	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters/<filter>
Modify a performance dataset filter	PUT <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters/<filter>
Create a new performance dataset filter	POST <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters
Delete a specific performance dataset	DELETE <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters/<filter>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters?describe
	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/filters/<filter>?describe

## Performance datasets workloads resource

List, create, modify, or delete performance dataset workloads.

Operation	Method and URI
List performance dataset workloads	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads
View a specific performance dataset workload	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads/<workload>
Modify a performance dataset workload	PUT <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads/<workload>
Create a new performance dataset workload	POST <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads
Delete a specific performance workload	DELETE <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads/<workload>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads?describe
	GET <cluster-ip:port>/platform/7/performance/datasets/<dataset>/workloads/<workload>?describe

## Performance metrics resource

List performance metrics for a dataset, or view a specific metric.

Operation	Method and URI
List performance metrics	GET <cluster-ip:port>/platform/7/performance/metrics
View a specific performance dataset workload	GET <cluster-ip:port>/platform/7/performance/metrics/<metric>
View the detailed JSON schema for this resource, which has information about query parameters and object properties.	GET <cluster-ip:port>/platform/7/performance/metrics?describe
	GET <cluster-ip:port>/platform/7/performance/metrics/<metric>?describe

## Code samples for file system configuration

Code samples illustrate the basic syntax of OneFS API requests for file system configuration.

You can download a zip file that contains code samples for the Python programming language and for curl commands from [Dell EMC EMC Online Support](#). The sample code provides brief examples on how to access, modify, and delete configuration settings on your cluster through OneFS API requests.

# CHAPTER 4

## File system access API

You can access files and directories on a cluster programmatically through the OneFS API, similar to the way you can access files and directories through SMB or NFS protocols.

- [File system access API overview](#) .....184
- [Troubleshooting](#) .....186
- [File system access operations](#) .....188
- [Code samples for file system access](#) ..... 257

## File system access API overview

You can access files and directories on a cluster programmatically through the OneFS API, similar to the way you can access files and directories through SMB or NFS protocols.

Through the OneFS API, you can perform the types of file system operations listed in the following table.

Operation	Description
Access points	Identify and configure access points and obtain protocol information
Directory	List directory content; get and set directory attributes; delete directories from the file system
File	View, move, copy, and delete files from the file system
Access control	Manage user rights; set ACL or POSIX permissions for files and directories
Query	Search and tag files
SmartLock	Allow retention dates to be set on files; commit a file to a WORM state

Additionally, you can create an external client or application to access the OneFS API in any major language, such as C, C++, Python, Java, or .Net.

## Common response headers

You may see the following response headers when you send a request to the namespace.

Name	Description	Type
Content-length	Provides the length of the body message in the response.	Integer
Connection	Provides the state of connection to the server.	String
Date	Provides the date when the object store last responded.	HTTP-date
Server	Provides platform and version information about the server that responded to the request.	String
x-isi-ifs-target-type	Provides the resource type. This value can be a container or an object.	String

## Common request headers

When you send a request to the OneFS API, you can access data through customized headers along with standard HTTP headers.

The following table provides information about common HTTP request headers:

Name	Description	Type	Required
Authorization	Specifies the authentication signature.	String	Yes
Content-length	Specifies the length of the message body.	Integer	Conditional
Date	Specifies the current date according to the requestor.	HTTP-date	No. A client should only send a Date header in a request that includes an entity-body, such as in PUT and POST requests. A client without a clock must not send a Date header in a request.
x-isi-ifs-spec-version	Specifies the protocol specification version. The client specifies the protocol version and the server determines if the protocol version is supported. You can test backwards compatibility with this header.	String	Conditional
x-isi-ifs-target-type	Specifies the resource type. For PUT operations, this value can be <code>container</code> or <code>object</code> . For GET operations, this value can be <code>container</code> , <code>object</code> , or <code>any</code> , or this parameter can be omitted.	String	Yes, for PUT operations. Conditional, for GET operations.

## Common namespace attributes

The following system attributes are common to directories and files in the namespace.

Attribute	Description	Type
name	Specifies the name of the object.	String
size	Specifies the size of the object in bytes.	Integer
block_size	Specifies the block size of the object.	Integer
blocks	Specifies the number of blocks that compose the object.	Integer
last_modified	Specifies the time when the object data was last modified in HTTP date/time format.	HTTP date
create_time	Specifies the date when the object data was created in HTTP date/time format.	HTTP date
access_time	Specifies the date when the object was last accessed in HTTP date/time format.	HTTP date
change_time	Specifies the date when the object was last changed (including data and metadata changes) in HTTP date/time format.	String

Attribute	Description	Type
type	Specifies the object type, which can be one of the following values: container, object, pipe, character_device, block_device, symbolic_link, socket, or whiteout_file.	String
mtime_val	Specifies the time when the object data was last modified in UNIX Epoch format.	Integer
btime_val	Specifies the time when the object data was created in UNIX Epoch format.	Integer
atime_val	Specifies the time when the object was last accessed in UNIX Epoch format.	Integer
ctime_val	Specifies the time when the object was last changed (including data and metadata changes) in UNIX Epoch format.	Integer
owner	Specifies the user name for the owner of the object.	String
group	Specifies the group name for the owner of the object.	String
uid	Specifies the UID for the owner.	Integer
gid	Specifies the GID for the owner.	Integer
mode	Specifies the UNIX mode octal number.	String
id	Specifies the object ID, which is also the INODE number.	Integer
nlink	Specifies the number of hard links to the object.	Integer
is_hidden	Specifies whether the file is hidden or not.	Boolean

## Troubleshooting

You can troubleshoot failed requests to the namespace by resolving common errors and viewing activity logs.

### Common error codes

The following example shows the common JSON error format:

```
{
  "errors": [
    {
      "code": "<Error code>",
      "message": "<some detailed error msg>"
    }
  ]
}
```

The following table shows the descriptions for common error codes.

Error Code	Description	HTTP status
AEC_TRANSIENT	The specified request returned a transient error code that is treated as OK.	200 OK

<b>Error Code</b>	<b>Description</b>	<b>HTTP status</b>
AEC_BAD_REQUEST	The specified request returned a bad request error.	400 Bad Request
AEC_ARG_REQUIRED	The specified request requires an argument for the operation.	400 Bad Request
AEC_ARG_SINGLE_ONLY	The specified request requires only a single argument for the operation.	400 Bad Request
AEC_UNAUTHORIZED	The specified request requires user authentication.	401 Unauthorized
AEC_FORBIDDEN	The specified request was denied by the server. Typically, this response includes permission errors on OneFS.	403 Forbidden
AEC_NOT_FOUND	The specified request has a target object that was not found.	404 Not Found
AEC_METHOD_NOT_ALLOWED	The specified request sent a method that is not allowed for the target object.	405 Method Not Allowed
AEC_NOT_ACCEPTABLE	The specified request is unacceptable.	406 Not Acceptable
AEC_CONFLICT	The specified request has a conflict that prevents the operation from completing.	409 Conflict
AEC_PRE_CONDITION_FAILED	The specified request has failed a precondition.	412 Precondition failed
AEC_INVALID_REQUEST_RANGE	The specified request has requested a range that cannot be satisfied.	416 Requested Range not Satisfiable
AEC_NOT_MODIFIED	The specified request was not modified.	304 Not Modified
AEC_LIMIT_EXCEEDED	The specified request exceeded the limit set on the server side.	403 Forbidden
AEC_INVALID_LICENSE	The specified request has an invalid license.	403 Forbidden
AEC_NAMETOOLONG	The specified request has an object name size that is too long.	403 Forbidden
AEC_SYSTEM_INTERNAL_ERROR	The specified request has failed because the server encountered an unexpected condition.	500 Internal Server Error

### Activity Logs

Activity logs capture server and object activity, and can help identify problems. The following table shows the location of different types of activity logs.

Server Logs	Object Daemon Log	Generic Log
<ul style="list-style-type: none"> <li>• /var/log/&lt;server&gt;/webui_httpd_error.log</li> <li>• /var/log/&lt;server&gt;/webui_httpd_access.log</li> </ul> <p>For &lt;server&gt;, type the path to the server directory. For example: /apache2.</p>	/var/log/isi_object_d.log	/var/log/message

## File system access operations

You can make requests through the OneFS API to perform operations on the file system.

### Access points

You can access the file system namespace through an access point. The default namespace access point for the OneFS file system is `/ifs`.

Root users can create an access point on the namespace, and initially only the root user has privileges for that access point. The root user can create an access control list (ACL) to provide read privileges for additional users.

The root user can also grant write privileges to users, but non-root users with write privileges are unable to reconfigure the path of an existing access point.

Additionally, each file or directory in an access point has its own permissions, so even if a user has privileges for an access point, the user must still be given permissions for each file and directory.

### Configure a user accounts for read privileges

You must configure user accounts with read privileges before users can access an access point. User access privileges (such as read, write, or read-write) for files and directories that are under an access point are governed by the OneFS system ACLs and permissions. Users privileges to an access point can be modified, however, the read privilege must be given to a user, or the user will be unable to access the access point.

#### Procedure

1. Create a user account by running the following command, where `user1` is the new user account name:

```
isi auth users create user1 --password user1 --home-directory /ifs/home/user1 --password-expires no
```

2. Grant users read-privilege to a OneFS access point through by applying the PUT method to the URI.

In the following example, user1 is granted access to the ifs-ap1 access point by modifying the ACL read-privilege on the access point.

```
PUT /namespace/ifs-ap1?acl&nsaccess=true HTTP/1.1
Authorization: Basic QWxhZGRpbjpvGcVvIHN1c2FtZQ==
Host: 10.245.107.17:8080
Content-Type:application/json
Content-Length: 140
{"authoritative":"acl", "acl":[{"trustee":
{"name":"user1","type":"user"}, "accesstype":"allow",
"accessrights":["file_read"], "op":"add"}]}
```

## Create a namespace access point

Creates a namespace access point in the file system. Only root users can create or change namespace access points.

### Request syntax

```
PUT /namespace/<access_point> HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>

{
  "path" : "<absolute_filesystem_path>"
}
```

---

### Note

The path to the namespace access point must begin at /ifs, which is the root directory of the OneFS file system.

---

### Request query parameters

There are no query parameters for this request.

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

### Example request

The following request creates an access point named 'accesspoint1' on the namespace.

```
PUT /namespace/accesspoint1 HTTP/1.1
Host my_cluster:8080
Date: Fri, 15 Mar 2013 21:51:50 GMT
Content-Type: text/xml

{
  "path": "/ifs/home/"
}
```

**Example response**

```

HTTP/1.1 200 OK
Date: Fri, 15 Mar 2013 21:51:50 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
x-isi-ifs-spec-version: 1.0
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=335
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

```

**Get namespace access points**

Retrieves the namespace access points available for the authenticated user.

**Request syntax**

```

GET /namespace/ HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

**Request query parameters**

There are no query parameters for this request.

**Request headers**

This call sends common request headers.

**Response header**

This call returns common response headers.

**Response body**

An array of namespace access points is output in JSON. Only the access points that the user has privileges for are returned.

**Example request**

This example retrieves a list of all access points for the namespace on this cluster by the root user.

```

GET /namespace/ HTTP/1.1
Host my_cluster:8080
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>

```

**Example response**

```

HTTP/1.1 200 OK
Allow: GET, HEAD
Connection: Keep-Alive
Content-Type: application/json
Date: Mon, 25 Mar 2013 20:31:33 GMT
Keep-Alive: timeout=15, max=499
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Transfer-Encoding: chunked

```

```

x-isi-ifs-spec-version: 1.0

{
  "namespaces": [
    {
      "name": "user1",
      "path": "/ifs/home/user1"
    },
    {
      "name": "ifs",
      "path": "/ifs/"
    }
  ]
}

```

## Get or set an access control list for a namespace access point

Retrieves or sets the access control list for a namespace access point.

### Request syntax

```

GET /namespace/<access_point>?acl&nsaccess=true HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date:<date>
Authorization: <signature>

```

```

PUT /namespace/<access_point>?acl&nsaccess=true HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>

```

### Request query parameters

Parameter Name	Description	Default	Type	Required
acl	This parameter is a functional keyword that does not have a value.	N/A	N/A	Yes
nsaccess	Indicates that the operation is on the access point instead of the store path. This value must be set to true. If set to false or left blank, the request behaves similarly to a GET or PUT operation.	N/A	Boolean	Yes

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

The access control list for the namespace access point is returned for the GET operation.

No message body is returned upon success for the PUT operation.

**Example request 1**

In this example, the GET operation retrieves the access control list from the namespace.

```
GET /namespace/ifs-ap1?acl&nsaccess=true HTTP/1.1
Host: my_cluster:8080
Authorization: <key>
```

**Example response 1**

```
HTTP/1.1 200 OK
Date: Mon, 25 Mar 2013 18:42:16 GMT
x-isi-ifs-spec-version: 1.0
Transfer-Encoding: chunked
Content-Type: application/json
```

```
{
  "acl": [
    {
      "accessrights": [
        "file_read"
      ],
      "accesstype": "allow",
      "inherit_flags": [
      ],
      "trustee": {
        "id": "UID:2000",
        "name": "user1",
        "type": "user"
      }
    }
  ],
  "authoritative": "acl",
  "group": {
    "id": "GID:0",
    "name": "wheel",
    "type": "group"
  },
  "mode": "0060",
  "owner": {
    "id": "UID:0",
    "name": "root",
    "type": "user"
  }
}
```

**Example request 2**

In this example, the request sets an access control list for the access point.

```
PUT /namespace/ifs-ap1?acl&nsaccess=true HTTP/1.1
Authorization: Basic QWxhZGRpbjpvYVUHN1c2FtZQ==
Host: 10.245.107.17:8080
Content-Type: application/json
Content-Length: 140
```

```
{
  "authoritative": "acl",
  "acl": [
    {
      "trustee": {
        "name": "user1",
```

```

        "type": "user"
      },
      "accesstype": "allow",
      "accessrights": [
        "file_read"
      ],
      "op": "add"
    }
  ]
}

```

### Example response 2

```

HTTP/1.1 200 OK
Date: Mon, 25 Mar 2013 17:24:55 GMT
Transfer-Encoding: chunked
Content-Type: text/plain
x-isi-ifs-spec-version: 1.0

```

## Get version information for the namespace access protocol

Retrieves the protocol versions that are supported for the current namespace access server.

### Request syntax

```

GET /namespace/?versions HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>

```

### Request query parameters

Parameter name	Description	Default	Type	Required
versions	This parameter is a functional keyword that does not have a value.	N/A	N/A	Yes

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

An array of version strings that are supported by the current namespace API server is output in JSON.

### Example request

This example retrieves a list of all versions supported for the namespace access server.

```

GET /namespace/?versions HTTP/1.1
Host my_cluster:8080

```

```
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

### Example response

This example shows that the namespace access server supports only version 1.0.

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

{"versions": ["1.0"]}
```

## Delete a namespace access point

Deletes a namespace access point. Only root users can delete namespace access points. Additionally, the deletion of a namespace access point does not delete the namespace resource that the access point references.

### Request syntax

```
DELETE /namespace/<access_point> HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>
```

### Request query parameters

There are no query parameters for this request.

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

### Example request

This example shows the delete operation for an access point named 'user1.'

```
DELETE /namespace/user1 HTTP/1.1
Host my_cluster:8080
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

### Example response

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Directory operations

You can perform directory operations on the namespace.

### Create a directory

Creates a directory with a specified path.

#### Request syntax

```
PUT /namespace/<access_point>/<container_path>[?recursive=<boolean>]
[?overwrite=<boolean>] HTTP/1.1
Host <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>
x-isi-ifs-target-type: container
```

#### Request query parameters

Parameter Name	Description	Default	Type	Required
recursive	Creates intermediate folders recursively, when set to true.	False	Boolean	No
overwrite	Deletes and replaces the existing user attributes and ACLs of the directory with user-specified attributes and ACLs from the header, when set to true. Returns an error if the directory already exists, when set to false. If the directory does not already exist, the directory is created and set with the user-specified attributes and ACLs from the header. If no ACLs are set in the header, the default mode is set to 0700.	True	Boolean	No

#### Request headers

Header Name	Description	Default	Type	Required
x-isi-ifs-access-control	Specifies a pre-defined ACL value or POSIX mode with a string. If this parameter is not provided, the mode for the directory is set to 0700 by default.	0700 (read, write, and execute with owner permissions)	String	No
x-isi-ifs-node-pool-name	Specifies the OneFS node pool name. When set to ANY, OneFS selects the pool for the directory. Only users with root access can set this header.	N/A	String	No

Header Name	Description	Default	Type	Required
x-isi-ifs-attr- <attr_name >	Specifies extended user attributes on the directory. The attributes names are stored in upper case, and all dashes (-) are converted to underscores (_).	N/A	String	No

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success.

**Example request**

This request creates a directory on the namespace named 'folder1/folder2'.

```
PUT /namespace/ifs/folder1/folder2/?recursive=true HTTP/1.1
Host my_cluster:8080
x-isi-ifs-target-type: container
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

**Get the attributes for a directory with the HEAD method**

Retrieves the attribute information for a specified directory without transferring the contents of the directory. Attributes that can be displayed are returned only as headers, such as x-isi-ifs-*<name>*=*<value>*.

**Request syntax**

```
HEAD /namespace/<access_point>/<container_path> HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

**Request query parameters**

There are no query parameters for this request.

**Request headers**

Header Name	Description	Default	Type	Required
If-Modified-Since	Returns directory content only if the directory was modified since the specified time. If no directory	None	HTTP date	No

Header Name	Description	Default	Type	Required
	content was modified, a 304 message is returned.			
If-Modified-Since	Returns directory content only if the directory was not modified since the specified time. If there is no unmodified directory content, a 412 message is returned to indicate that the precondition failed.	None	HTTP date	No

### Response headers

Header Name	Description	Default	Type	Required
Content-Encoding	Provides the content encoding that was applied to the object content, so that decoding can be applied when retrieving the content.	None	String	No
Content-Type	Provides a standard MIME-type description of the content format.	binary/octet-stream	String	No
x-isi-ifs-attr- <attr_name>	Provides the extended attributes that were set in the message header. The attribute names are stored in uppercase, and all dashes (-) are converted to underscores (_).	None	String	No
x-isi-ifs-missing-attr	Provides the number of attributes that cannot be displayed in the HTTP header. Missing attributes can be retrieved through the following operation: GET the extended attributes of a directory.	None	String	No
x-isi-ifs-access-control	Provides the access mode for the directory in octal notation.	None	String	No

### Response body

No message body is returned upon success.

### Example request

```
HEAD /namespace/ifs/my_folder/ HTTP/1.1
Host my_cluster:8080
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response**

```

HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Connection: close
Server: Apache2/2.2.19
Last-Modified: Wed, 21 Sep 2011 12:00:00 GMT
x-isi-ifs-access-control: 0600
x-isi-ifs-attr-color: red
x-isi-ifs-missing-attr: 1
x-isi-ifs-spec-version: 1.0
x-isi-ifs-target-type: container
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Type: text/xml; charset=UTF-8

```

**Get the extended attributes of a directory**

Retrieves the attribute information for a specified directory with the metadata query argument.

**Request syntax**

```

GET /namespace/<access_point>/<container_path>?metadata HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

**Request query parameters**

Parameter Name	Description	Default	Type	Required
metadata	This parameter is a functional keyword and does not have a value.	N/A	N/A	Yes

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

The object attribute information is returned in JSON format.

```

{
  "attrs": [
    {
      "name": "<key_name>",
      "value": "<key_value>",
      "namespace": "<namespace_value>"
    },
    ...
  ]
}

```

**Note**

The `namespace` parameter is optional. When this parameter is missing, the attribute is considered to be a system defined attribute. When `<namespace_value>` is set to `user`, the attribute is considered a user defined attribute.

**Example request**

```
GET /namespace/ifs/my_folder/?metadata HTTP/1.1
Host my_cluster:8080
Content-Length : <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <Length>
Content-Type: application/JSON
Connection: close
Server: Apache2/2.2.19

{
  "attrs":[
    {
      "name":"is_hidden",
      "value":false
    },
    {
      "name":"size",
      "value":96
    },
    {
      "name":"block_size",
      "value":8192
    },
    {
      "name":"blocks",
      "value":4
    },
    {
      "name":"last_modified",
      "value":"Fri, 23 Mar 2012 16:32:42 GMT"
    },
    {
      "name":"change_time",
      "value":"Fri, 23 Mar 2012 16:32:42 GMT"
    },
    {
      "name":"access_time",
      "value":"Fri, 23 Mar 2012 16:32:42 GMT"
    },
    {
      "name":"create_time",
      "value":"Wed, 21 Mar 2012 22:06:23 GMT"
    },
    {
      "name":"mtime_val",
      "value":1332520362
    },
    {
      "name":"ctime_val",
```

```

    "value":1332520362
  },
  {
    "name":"atime_val",
    "value":1332520362
  },
  {
    "name":"mtime_val",
    "value":1332367583
  },
  {
    "name":"owner",
    "value":"root"
  },
  {
    "name":"group",
    "value":"wheel"
  },
  {
    "name":"uid",
    "value":0
  },
  {
    "name":"gid",
    "value":0
  },
  {
    "name":"id",
    "value":2
  },
  {
    "name":"nlink",
    "value":6
  },
  {
    "name":"type",
    "value":"container"
  },
  {
    "name":"mode",
    "value":511
  }
]
}

```

## Get the contents of a directory

Retrieves a list of files and subdirectories from a directory.

### Request syntax

```

GET /namespace/<access_point>/<container_path>[?<query>] HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

---

### Note

The `query` argument is optional and can include the parameters in the following table.

---

## Request query parameters

Parameter Name	Description	Default	Type	Required
detail	Specifies which object attributes are displayed. If the <code>detail</code> parameter is excluded, only the name of the object is returned. You can specify multiple attribute names in CSV format. If you set this value to default, the following attributes are included: name, size, owner, last_modified, type, group, and mode.	None	String	No
limit	Specifies the maximum number of objects to send to the client. You can set the value to a negative number to retrieve all objects. Additionally, you can specify the maximum number of objects to return when sorting directory entries by opening a secure shell (SSH) connection to any node in the cluster, logging in, and running the following command:  <pre>isi_gconfig -t oapi max_sort_dir_sz=&lt;integer&gt;</pre>	1000	Integer	No
resume	Specifies a token to return in the JSON result to indicate when there is a next page. The client can include the resume token to access the next page.	None	String	No
sort	Specifies one or more attributes to sort on the directory entries. You can specify multiple attributes by separating the attributes with a comma, such as name, size, last_modified. When sorting is on, the maximum number of objects returned is 1000. The entries are sorted in the order that the attributes appear in the list, from left to right.	None	String	No
dir	Specifies the sort direction. This value can be either <code>ascending</code> (ASC) or <code>descending</code> (DESC).	None	String	No
type	Specifies the object type to return, which can be one of the following values: container, object, pipe, character_device, block_device,	None	String	No

Parameter Name	Description	Default	Type	Required
	symbolic_link, socket, or whiteout_file.			
hidden	Specifies if hidden objects are returned.	None	Boolean	No

### Request headers

Header Name	Description	Default	Type	Required
If-Modified-Since	Returns directory content only if the directory was modified since the specified time. If no directory content was modified, a 304 message is returned.	None	HTTP date	No
If-Unmodified-Since	Returns directory content only if the directory was not modified since the specified time. If there is no unmodified directory content, a 412 message is returned to indicate that the precondition failed.	None	HTTP date	No

### Response headers

Header Name	Description	Default	Type	Required
Content-Encoding	Provides the content encoding that was applied to the object content, so that decoding can be applied when retrieving the content.	None	String	No
Content-Type	Provides a standard MIME-type description of the content format.	application/json	String	No
x-isi-ifs-attr- <attr_name >	Provides the extended attributes that were set in the message header.	None	String	No
x-isi-ifs-missing-attr	Provides the number of attributes that cannot be displayed in the HTTP header.	None	Integer	No
x-isi-ifs-access-control	Provides the POSIX mode in octal notation.	None	String	No

### Response body

An array of objects in the directory is output in JSON format.

**Example request**

The following request returns the contents of a directory named 'folder1/folder2'.

```
GET /namespace/folder1/folder2 HTTP/1.1
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Type: application/JSON
Connection: close
Server: Apache2/2.2.19

{
  "children": [
    {
      "name": "cover"
    },
    {
      "name": "f2"
    },
    {
      "name": "cover.txt"
    },
    {
      "name": "cover8"
    }
  ]
}
```

**Request example 2**

This request returns object details for the directory named 'folder1/folder2'.

```
GET /namespace/folder1/folder2/?limit=500&detail=default HTTP/1.1
Host my_cluster:8080
Content-Length: 0
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Response example 2**

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Type: application/JSON
Connection: close

{
  "resume": "<the_resume_token>",
  "children": [
    {
      "last_modified": "Fri, 18 Nov 2011 22:45:31 GMT",
      "name": "cover",
      "size": 24,
      "type": "object",
    }
  ]
}
```

```

    },
    {
      "last_modified": "Fri, 18 Nov 2011 20:01:04 GMT",
      "name": "f2",
      "size": 4,
      "type": "object",
    },
  ],
  {
    "last_modified": "Fri, 18 Nov 2011 22:45:40 GMT",
    "name": "finance",
    "size": 0,
    "type": "container",
  }
]
}

```

## Copy a directory

Recursively copies a directory to a specified destination path. Symbolic links are copied as regular files.

### Request syntax

```

PUT /namespace/<access_point>/<container_path> HTTP/1.1
x-isi-ifs-copy-source: /namespace/<access_point>/<source_path>
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

### Request query parameters

Parameter Name	Description	Default	Type	Required
overwrite	Specifies if the existing file should be overwritten when a file with the same name exists.	False	Boolean	No
merge	Specifies if the contents of a directory should be merged with an existing directory with the same name.	False	Boolean	No
continue	Specifies whether to continue the copy operation on remaining objects when there is a conflict or error.	False	Boolean	No

### Request headers

Header Name	Description	Default	Type	Required
x-isi-ifs-copy-source	Specifies the full path to the source directory. The source and destination must share the same access point.	None	String	Yes

### Response headers

This call returns common response headers.

**Response body**

No message body is returned upon success.

For this operation, the HTTP status code 200 OK does not always indicate a complete success. If the response body contains a JSON message, the operation has partially failed, and the error message is reported in a structured JSON array.

If the server fails to initiate a copy due to an error (such as an invalid copy source), an error is returned. If the server initiates the copy, and then fails, "copy\_errors" are returned in structured JSON format.

Because the copy operation is synchronous, the client cannot stop an ongoing copy or check the status of a copy asynchronously.

**Example request 1**

```
PUT /namespace/ifs/dest1/ / HTTP/1.1
x-isi-ifs-copy-source: /namespace/ifs/src1/
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response 1**

```
HTTP/1.1 200 Ok
Date: Thu, 22 Sep 2011 12:00:00 GMT
Server: Apache2/2.2.19
Content-Encoding: gzip
x-isi-ifs-spec-version: 1.0
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain
```

**Example request 2**

In this example, the directory 'src1' contains files {f1, f2, f3, f4} and the directory 'dest1' exists and contains files {f1, f2}.

```
PUT /namespace/ifs/dest1/?merge=true&continue=true HTTP/1.1
x-isi-ifs-copy-source: /namespace/ifs/src1/
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response 2**

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2011 12:00:00 GMT
Server: Apache2/2.2.19
x-isi-ifs-spec-version: 1.0
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/json

{
  "copy_errors": [
    {
      "source": "/apl/src1/f1",
```

```

        "target":"/apl/dest1/f1",
        "error_src":"target side",
        "message":"target exists(not copied)",
    },
    {
        "source":"/apl/src1/f2",
        "target":"/apl/dest1/f2",
        "error_src":"target side",
        "message":"target exists(not copied)"
    }
],
}

```

## Move a directory

Moves a directory from an existing source to a new destination path.

### Request syntax

```

POST /namespace/<access_point>/<container_path> HTTP/1.1
x-isi-ifs-set-location: /namespace/<access_point>/<dest_path>
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

### Request query parameters

There are no query parameters for this request.

### Request headers

Header Name	Description	Default	Type	Required
x-isi-ifs-set-location	Specifies the full path for the destination directory. The source and destination directories must be in the same access point.	None	String	Yes

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

### Example request

```

POST /namespace/ifs/folder1/folder2/ HTTP/1.1
x-isi-ifs-set-location: /namespace/ifs/dest1/dest2/
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>

```

**Example response**

```
HTTP/1.1 204 No Content
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

**Delete a directory**

Deletes the directory at the specified path.

**Request syntax**

```
DELETE /namespace/<access_point>/<container_path>[?
recursive=<Boolean>] HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

**Request query parameters**

Parameter Name	Description	Default	Type	Required
recursive	Deletes directories recursively, when set to true. Returns an error if you attempt to delete a directory that is not empty, when set to false. When the <code>recursive</code> parameter is set to true, and there is an error deleting a child, the operation continues to delete other children. Only the last error is returned.	False	Boolean	No

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success.

**Example request**

```
DELETE /namespace/folder1/folder2 HTTP/1.1
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 204 No Content
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
```

```
Connection: close
Server: Apache2/2.2.19
```

## Set attributes on a directory

Sets attributes on a specified directory with the metadata query argument. You can also set attributes with a header when the directory is created with the header format `x-isi-ifs-<name>=<value>`.

### Request syntax

```
PUT /namespace/<access_point>/<container_path>?metadata HTTP/1.1
Host <hostname>[:<port>]
Content-Length : <length>
Content-Type : application/JSON
Date: <date>
Authorization: <signature>

{
  "action": "<action_value>",
  "attrs": [
    {
      "name": "<key_name>",
      "value": "<key_value>",
      "namespace": "<namespace_value>",
      "op": "<operation_value>"
    },
    ...
  ]
}
```

---

### Note

You can omit attribute values or enter "" for the value.

---

### Request query parameters

Parameter Name	Description	Default	Type	Required
metadata	The <code>metadata</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	No

### Request body parameters

Parameter Name	Description	Default	Type	Required
action	The values for the <code>&lt;action_value&gt;</code> field are <code>replace</code> or <code>update</code> . Note that the <code>&lt;action_value&gt;</code> field operates in conjunction with the <code>&lt;operation_value&gt;</code> field.  To modify the existing attributes, set both <code>&lt;action_value&gt;</code> and <code>&lt;operation_value&gt;</code> to <code>update</code> .	update	String	No

Parameter Name	Description	Default	Type	Required
	To delete the existing attributes, set <i>&lt;action_value&gt;</i> to <code>update</code> and <i>&lt;operation_value&gt;</i> to <code>delete</code> .  To remove all extended attributes first, and then replace the attributes with the values specified in the <code>attrs</code> parameter, set <i>&lt;action_value&gt;</i> to <code>replace</code> . When <i>&lt;action_value&gt;</i> is set to <code>replace</code> , the <i>&lt;operation_value&gt;</i> field is ignored.			
<code>op</code>	The values for the <i>&lt;operation_value&gt;</i> field are <code>update</code> or <code>delete</code> . The <i>&lt;operation_value&gt;</i> field is only applicable when <i>&lt;action_value&gt;</i> is set to <code>update</code> .	<code>update</code>	String	No
<code>namespace</code>	Specifies the namespace associated with the attributes set for the directory. The only supported value for this parameter is <code>user</code> .	<code>user</code>	String	No

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success.

**Example request**

```
PUT /namespace/ifs/my_folder/?metadata HTTP/1.1
Host my_cluster:8080
Content-Length : <length>
Date: <date>
Authorization: <signature>

{
  "action": "replace",
  "attrs": [
    {
      "name": "Manufacture",
      "value": "Foo",
      "namespace": "user"
    }
  ]
}
```

## Example response

```

HTTP/1.1 200 OK
Date: Wed, 20 Mar 2013 17:19:15 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
x-isi-ifs-spec-version: 1.0
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

```

## File operations

You can perform file operations on the namespace.

### Create a file object

Creates a file object with a given path. The file is either successfully created in whole, or no file is created at all. Partial files cannot be created.

#### Request syntax

```

PUT /namespace/<access_point>/<file_path>[?overwrite=<Boolean>]
HTTP/1.1
Host <hostname>[:<port>]
Content-Length : <length>
Date: <date>
Authorization: <signature>

[Message Body]

```

#### Request query parameters

Parameter Name	Description	Default	Type	Required
overwrite	If the <code>overwrite</code> parameter is set to true, the preset user attributes and ACLs of the file are deleted and replaced with the user-specified attributes and ACLs from the header. If the <code>overwrite</code> parameter is set to false and the file already exists, an error message is returned. If the file does not already exist, the file is created and set with the user-specified attributes and ACLs from the header.	True	Boolean	No

**Request headers**

Header Name	Description	Default	Type	Required
Content-Encoding	Specifies the content encoding that was applied to the object content, so that decoding can be applied when retrieving the content.	None	String	No
Content-Type	Specifies a standard MIME-type description of the content format.	binary/octet-stream	String	Conditional
x-isi-ifs-target-type	Specifies the resource type. This value can be <code>container</code> or <code>object</code> .	None	String	Yes. The value must be set to 'object.'
x-isi-ifs-access-control	Specifies a pre-defined ACL value or POSIX mode with a string in octal string format.	0600 (read, write with owner permissions)	String	No
x-isi-ifs-attr- <attr_name >	Specifies the extended attributes that were set in the message header. The attributes names are stored in upper case, and all dashes (-) are converted to underscores (_).	None	String	No

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success.

**Example request**

```
PUT /namespace/ifs/my_folder/picture.jpg HTTP/1.1
Host my_cluster:8080
x-isi-ifs-target-type: object
Content-Type: image/jpeg
Content-Length: 65536
Date: Thu Sep 22 16:06:32 GMT 2011
Authorization: <signature>

[Byte Streams of pictue.jpg]
```

**Example response**

```
HTTP/1.1 201 Created
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Get the contents of a file

Retrieves the contents of a file from a specified path.

### Request syntax

```
GET /namespace/<access_point>/<file_path> HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
Range: bytes=<byte_range>
```

### Request query parameters

There are no query parameters for this request.

### Request headers

Header Name	Description	Default	Type	Required
Range	Returns the specified range bytes of an object. Only the basic range is supported. The format is defined as:  <pre>first-byte-pos "-" last-byte-pos</pre> <p>The first-byte-pos value in a byte-range-spec gives the byte-offset of the first byte in a range. The last-byte-pos value gives the byte-offset of the last byte in the range; that is, the byte positions specified are inclusive. Byte offsets start at zero.</p>	None	String	No
If-Modified-Since	Returns only files that were modified since the specified time. If no files were modified since this time, a 304 message is returned.	None	HTTP date	No
If-Unmodified-Since	Returns only files that were not modified since the specified time. If there are no unmodified files since this time, a 412 message is returned to indicate that the precondition failed.	None	HTTP date	No

### Response headers

Header Name	Description
Content-Encoding	Provides the content encoding that was applied to the object content, so that decoding can be applied when retrieving the content.
Content-Type	Provides a standard MIME-type description of the content format.

Header Name	Description
x-isi-ifs-attr-<attr_name>	Provides the extended attributes that were set in the message header when the file was created.
x-isi-ifs-missing-attr	Provides the number of attributes that cannot be displayed in the HTTP header.
x-isi-ifs-access-control	Provides the access mode for the file in octal number format.

**Response body**

No message body is returned upon success.

**Example request**

```
GET /namespace/ifs/my_folder/picture.jpg HTTP/1.1
Host my_cluster:8080
Date: Thu Sep 22 16:06:32 GMT 2011
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 200 OK
Date: Thu Sep 22 16:06:32 GMT 2011
Content-Length: 54380
Content-Type: image/jpeg
Connection: close
Server: Apache2/2.2.19

[54380 bytes of data]
```

**Copy a file**

Copies a file to the specified destination path.

**Request syntax**

```
PUT /namespace/<access_point>/<file_path>[?overwrite=<Boolean>]
HTTP/1.1
x-isi-ifs-copy-source: /namespace/<access_point>/<source_path>
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

**Request query parameters**

Parameter Name	Description	Default	Type	Required
overwrite	Specifies if the existing file should be overwritten when a file with the same name exists.	False	Boolean	No

**Request headers**

Header Name	Description	Default	Type	Required
x-isi-ifs-copy-source	Specifies the full path of the source. The source and destination paths must be in the same access point.	N/A	String	Yes

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success. For this operation, the HTTP status code 200 OK may not indicate a complete success.

If the response body contains a JSON message, the operation has partially failed. If the server fails to initiate a copy due to an error (such as an invalid copy source), an error is returned. If the server initiates the copy, and then fails, "copy\_errors" are returned in structured JSON format. Because the copy operation is synchronous, the client cannot stop an ongoing copy operation or check the status of a copy operation asynchronously.

**Example request 1**

This example shows a successful copy.

```
PUT /namespace/ifs/folder1/myfile HTTP/1.1
x-isi-ifs-copy-source: /namespace/ifs/source1/myfile
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

**Example response 1**

```
HTTP/1.1 200 Ok
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

**Example request 2**

This example shows a failed copy, where the file is not overwritten.

```
PUT /namespace/accesspoint1/directory1/file2_copy HTTP/1.1
Host 10.245.105.110:8080
x-isi-ifs-copy-source: /namespace/accesspoint1/directory1/file2
Date: Wed, 20 Mar 2013 21:33:55 GMT
Authorization: <signature>
```

**Example response 2**

```
HTTP/1.1 200 OK
Date: Wed, 20 Mar 2013 21:33:55 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
```

```
x-isi-ifs-spec-version: 1.0
Keep-Alive: timeout=15, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/json

{
  "copy_errors":[
    {
      "error_src":"target side",
      "message":"target exists(not copied)",
      "source":"/accesspoint1/directory1/file2",
      "target":"/accesspoint1/directory1/file2_copy"
    }
  ],
  "success":false
}
```

## Move a file

Moves a file to a destination path that does not yet exist.

### Request syntax

```
POST /namespace/<access_point>/<file_path> HTTP/1.1
x-isi-ifs-set-location: /namespace/<access_point>/<dest_path>
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

### Request query parameters

There are no query parameters for this request.

### Request headers

Header Name	Description	Default	Type	Required
x-isi-ifs-set-location	Specifies the full path of the destination file. The source and destination paths must be in the same access point. If the x-isi-ifs-set-location points to a file name that is different than the source file name, the user can rename the file.	None	String	Yes

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

### Example request

```
POST /namespace/ifs/folder1/myfile HTTP/1.1
x-isi-ifs-set-location: /namespace/ifs/dest1/myfile
Host my_cluster:8080
Content-Length: <length>
```

```
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

### Example response

```
HTTP/1.1 204 Non Content
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Delete a file

Deletes the specified file.

### Request syntax

```
DELETE /namespace/<access_point>/<file_path> HTTP/1.1
Host <hostname>[:<port>]
Date:<date>
Authorization: <signature>
```

### Request query parameters

There are no query parameters for this request.

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

### Example request

```
DELETE /namespace/ifs/my_folder/test.txt HTTP/1.1
Host my_cluster:8080
Content-Length: <length>
Date: Thu, 22 Sep 2011 12:00:00 GMT
Authorization: <signature>
```

### Example response

```
HTTP/1.1 204 No Content
Date: Thu, 22 Sep 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Clone a file

Clone a file to the destination path. If the parameter is set as a snapshot name, the file is cloned from that snapshot.

### Request syntax

```
PUT /namespace/<access_point>/<file_path>[?<clone>][&<snapshot>]
[&<overwrite>] HTTP/1.1
x-isi-ifs-copy-source: <source_file_path>
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

### Request query parameters

Parameter Name	Description	Default	Type	Required
clone	You must set this parameter to true in order to clone a file.	False	Boolean	No
snapshot	Specifies a snapshot name to clone the file from. If a snapshot name is not given, a temporary snapshot is created. The temporary snapshot is deleted after the cloning operation is complete.	N/A	String	No
overwrite	Specifies if an existing file should be overwritten by a new file with the same name.	False	Boolean	No

### Request headers

Header Name	Description	Default	Type	Required
x-isi-ifs-copy-source	Specifies the full path of the source. The source and destination paths must be in the same access point.	N/A	String	Yes

### Response headers

This call returns common response headers.

### Response body

No response body is returned upon success.

### Example request

```
PUT /namespace/ifs/folder1/myfile?clone=true HTTP/1.1
x-isi-ifs-copy-source: /namespace/ifs/source1/myfile
Host my_cluster:8080
Content-Length : 0
Date: <date>
Authorization: <signature>
```

## Example response

```
HTTP/1.1 200 OK
Date: Thu, 21 Mar 2013 14:33:29 GMT
Content-Length: 0
Connection: close
```

## Set attributes on a file

Sets attributes on a specified file with the metadata query argument through the JSON body. You can also set attributes with a header when the file is created through a header with the format: `x-isi-ifs-<name>=<value>`.

### Request syntax

```
PUT /namespace/<access_point>/<file_path>?metadata HTTP/1.1
Host <hostname>[:<port>]
Content-Length : <length>
Content-Type : application/JSON
Date: <date>
Authorization: <signature>

{
  "action": "<action_value>",
  "attrs": [
    {
      "name": "<key_name>",
      "value": "<key_value>",
      "namespace": "<namespace_value>",
      "op": "<operation_value>"
    },
    ...
  ]
}
```

### Note

You can modify only the *<content\_type>* and user specified attributes. All other system attributes are ignored.

### Request query parameters

Parameter Name	Description	Default	Type	Required
metadata	The <i>metadata</i> argument must be placed at the first position of the argument list in the URI.	N/A	String	No

### Request body parameters

Parameter Name	Description	Default	Type	Required
action	The values for the <i>&lt;action_value&gt;</i> field are <code>replace</code> or <code>update</code> . The <i>&lt;action_value&gt;</i> field operates in conjunction with the <i>&lt;operation_value&gt;</i> field.	update	String	No

Parameter Name	Description	Default	Type	Required
	<p>To modify the existing attributes, set both <code>&lt;action_value&gt;</code> and <code>&lt;operation_value&gt;</code> fields to <code>update</code>.</p> <p>To delete the existing attribute, set the <code>&lt;action_value&gt;</code> field to <code>update</code> and <code>&lt;operation_value&gt;</code> to <code>delete</code>.</p> <p>To remove all extended attributes first and then replace the attributes with the values specified in the <code>attrs</code> parameter, set <code>&lt;action_value&gt;</code> to <code>replace</code>. When <code>&lt;action_value&gt;</code> is set to <code>replace</code>, the <code>&lt;operation_value&gt;</code> field is ignored.</p>			
<code>op</code>	The values for the <code>&lt;operation_value&gt;</code> field are <code>update</code> or <code>delete</code> . The <code>&lt;operation_value&gt;</code> field is only applicable when <code>&lt;action_value&gt;</code> is set to <code>update</code> .	<code>update</code>	String	No
<code>namespace</code>	Specifies the value for the namespace that the attribute associates with a directory. This parameter must be set to <code>user</code> if the attributes are specified by users.	<code>user</code>	String	No

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

No response body is returned upon success.

**Example request**

```
PUT /namespace/accesspoint1/my_folder/mytest.txt?metadata HTTP/1.1
Host my_cluster:8080
Content-Length : <length>
Date: <date>
Authorization: <signature>

{
  "action": "replace",
  "attrs": [
    {
      "name": "Manufacture",
      "value": "Foo",
      "namespace": "user"
    },
    {
      "name": "user.Material",
      "value": "Steel",
```

```

    "namespace": "user"
  }
]
}

```

### Example response

```

HTTP/1.1 200 OK
Date: Thu, 21 Mar 2013 14:33:29 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
x-isi-ifs-spec-version: 1.0
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

```

## Get the attributes for a file with the HEAD method

Retrieves the attribute information for a specified file. Attributes are returned as headers only if they can be displayed.

### Request syntax

```

HEAD /namespace/<access_point>/<file_path> HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

### Request query parameters

There are no query parameters for this request.

### Request headers

Header Name	Description	Default	Type	Required
If-Modified-Since	Returns only file content that was modified since the specified time. If no file content was modified, a 304 message is returned.	None	HTTP date	No
If-Unmodified-Since	Returns only file content that was not modified since the specified time. If there is no unmodified file content, a 412 message is returned to indicate that the precondition failed.	None	HTTP date	No

### Response headers

Header Name	Description	Default	Type	Required
Content-Encoding	Provides the content encoding that was applied to the object content,	None	String	No

Header Name	Description	Default	Type	Required
	so that decoding can be applied when retrieving the content.			
Content-Type	Provides a standard MIME-type description of the content format.	binary/octet-stream	String	No
x-isi-ifs-attr- <attr_name >	Provides the extended attributes that were set in the message header.	None	String	No
x-isi-ifs-missing-attr	Provides the number of attributes that cannot be displayed in the HTTP header. The missing attributes can be retrieved through the operation: GET extended attributes of a file operation.	None	Integer	No
x-isi-ifs-access-control	Provides a pre-defined ACL value or POSIX mode with a string, such as private, private_read, public_read, public_read_write, or public.	0700	String	No

**Response body**

No message body is returned upon success.

**Example request**

```
HEAD /namespace/ifs/my_folder/picture.jpg HTTP/1.1
Host my_cluster:8080
Date: Thu Sep 22 16:06:32 GMT 2011
Authorization: <signature>
```

**Example response**

```
HTTP/1.1 200 OK
Date: Thu Sep 22 16:06:32 GMT 2011
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
Last-Modified: Wed, 20 Mar 2013 18:16:17 GMT
x-isi-ifs-access-control: 0600
x-isi-ifs-attr-color: red
x-isi-ifs-missing-attr: 1
x-isi-ifs-spec-version: 1.0
x-isi-ifs-target-type: object
```

**Get the extended attributes of a file**

Retrieves the attribute information for a specified file with the metadata query argument.

## Request syntax

```
GET /namespace/<access_point>/<file_path>?metadata HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

## Request query parameters

Parameter Name	Description	Default	Type	Required
metadata	The <code>metadata</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	No

## Request headers

This call sends common request headers.

## Response headers

This call returns common response headers.

## Response body

The object attribute information is returned in JSON format.

```
{
  "attrs": [
    {
      "name": "<key_name>",
      "value": "<key_value>",
      "namespace": "<namespace_value>"
    },
    ...
  ]
}
```

---

## Note

The `namespace` parameter is optional. When this parameter is missing, the attribute is considered to be a system defined attribute. When the `<namespace_value>` field is set to `user`, the attribute is considered a user-defined attribute.

---

## Example request

```
GET /namespace/accesspoint1/directory1/file1?metadata HTTP/1.1
Host: 10.245.105.110:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:19.0) Gecko/20100101 Firefox/19.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _SID_=20130321154838-cffed57ca0a91f15a7dca80fc88ed0a8; isisessid=7651c367-71d1-4ff1-9dd0-1eee09a4b03d; legacy=1; ys-lastStatusDashView=n%3A1; ys-monitoringView=s%3ALIVE; ys-monitoringData=s%3AAVG
```

```
Connection: keep-alive
Cache-Control: max-age=0
```

### Example response

```
HTTP/1.1 200 Ok
Date: Thu, 21 Mar 2013 19:58:11 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8x
mod_webkit2/1.0 mod_fastcgi/2.4.6
Allow: DELETE, GET, HEAD, POST, PUT
x-is-iifs-spec-version: 1.0
Keep-Alive: timeout=15, max=436
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/json
```

```
{
  "attrs": [
    {
      "name": "content_type",
      "value": "text/xml; charset=UTF-8"
    },
    {
      "name": "is_hidden",
      "value": false
    },
    {
      "name": "size",
      "value": 27
    },
    {
      "name": "block_size",
      "value": 8192
    },
    {
      "name": "blocks",
      "value": 52
    },
    {
      "name": "last_modified",
      "value": "Wed, 20 Mar 2013 18:16:17 GMT"
    },
    {
      "name": "change_time",
      "value": "Wed, 20 Mar 2013 18:16:17 GMT"
    },
    {
      "name": "access_time",
      "value": "Wed, 20 Mar 2013 18:16:17 GMT"
    },
    {
      "name": "create_time",
      "value": "Wed, 20 Mar 2013 18:16:17 GMT"
    },
    {
      "name": "mtime_val",
      "value": 1363803377
    },
    {
      "name": "ctime_val",
      "value": 1363803377
    },
    {
      "name": "atime_val",
      "value": 1363803377
    }
  ]
}
```

```

    },
    {
      "name": "btime_val",
      "value": 1363803377
    },
    {
      "name": "owner",
      "value": "root"
    },
    {
      "name": "group",
      "value": "wheel"
    },
    {
      "name": "uid",
      "value": 0
    },
    {
      "name": "gid",
      "value": 0
    },
    {
      "name": "id",
      "value": 4300276817
    },
    {
      "name": "nlink",
      "value": 1
    },
    {
      "name": "type",
      "value": "object"
    },
    {
      "name": "mode",
      "value": "0600"
    },
    {
      "name": "Manufacture",
      "namespace": "user",
      "value": "Foo"
    },
    {
      "name": "user.Material",
      "namespace": "user",
      "value": "Steel"
    }
  ]
}

```

## Access control lists

You can configure access control lists (ACLs) or permissions modes for namespace directories and files.

For detailed information on access control lists, see the *OneFS Administration Guide*.

## Access control personas

Personas are a union of a user ID (UID), name, and type. Personas represent users and groups for access control list (ACL) operations.

The JSON format for personas is:

```
{
  "id": "<ID>",
  "name": "<name>",
  "type": "<type>"
}
```

where

```
<ID>: <"USER" | "GROUP" | "SID" | "UID" | "GID"> : <the ID string>
<name>: <the normal user name in a string>
<type>: <user, group, or wellknown>
```

For PUT operations, you can specify either the ID or both the name and type. The ID value takes precedence when all fields are available.

## Access rights for directories

The following table lists the access rights for directories.

Access rights	Functionality
list	The right to list entries
add_file	The right to create a file in the directory
add_subdir	The right to create a subdirectory
delete_child	The right to delete children, including read-only files
traverse	The right to access files in subdirectories
dir_read_attr	The right to read directory attributes
dir_write_attr	The right to write directory attributes
dir_read_ext_attr	The right to read extended directory attributes
dir_write_ext_attr	The right to write extended directory attributes
dir_gen_read	The right to list entries, read attributes, read extended attributes, and read access control lists
dir_gen_write	The right to create files, create subdirectories, write attributes, write extended attributes, and read access control lists
dir_gen_execute	The right to access files in subdirectories, and read access lists
dir_gen_all	Includes the rights specified in dir_gen_read, dir_gen_write, dir_gen_execute, delete_child, std_read_dac, std_write_dac, std_write_owner, and std_delete.

## Access rights for files

The following table lists the access rights for files.

Access rights	Functionality
file_read	The right to read file data.
file_write	The right to write file data.
append	The right to append to a file.
execute	The right to execute a file.
file_read_attr	The right to read file attributes.
file_write_attr	The right to write file attributes.
file_read_ext_attr	The right to read extended file attributes.
file_write_ext_attr	The right to write extended file attributes.
file_gen_read	The right to read files, read attributes, read extended attributes, and read access control lists.
file_gen_write	The right to write to the file, append to the file, write file attributes, write extended file attributes, and read access control lists.
file_gen_execute	The right to execute files, and read access control lists.
file_gen_all	Includes the rights specified by file_gen_read, file_gen_write, file_gen_execute, std_read_dac, std_write_dac, std_write_owner, and std_delete.

## Access rights for files and directories

The following table describes the access rights for both files and directories.

Access rights	Functionality
std_read_dac	The right to read the access control list of the directory or file.
std_write_dac	The right to write the access control list of the directory or file.
std_write_owner	The right to change the owner of the directory or file.
std_delete	The right to delete the current directory or file.
modify	Includes the following access rights for a directory: add_file, add_subdir, dir_write_ext_attr, dir_write_attr, delete_child, std_delete, std_write_dac and std_write_owner. Includes the following access rights for a file: file_write, append, file_write_ext_attr, file_write_attr, std_delete, std_write_dac and std_write_owner.

## Inherited access rights

The following table lists the inheritance flags for directories and sub-directories. Inheritance flags specify the access rights inherited by the children of a directory.

Inheritance Flags	Functionality
object_inherit	Only files inherit access rights from their parent directory.
container_inherit	Only directories inherit access rights from their parent directory.
no_prop_inherit	Stops the propagation of inherited rights for directories and files.
inherit_only	Access rights do not apply for the current directory, but are applied to child directories and files when they are inherited.
inherited_ace	Indicates that the access control list of the current directory or file was inherited from a parent directory or file.

## Get the ACL of a directory

Retrieves the access control list of the directory for the authenticated user.

### Request syntax

```
GET /namespace/<access_point>/<container_path>/<container_name>?acl
HTTP/1.1
Host: <hostname>[:<port>]
Date: <date>
Authorization: <signature>
```

### Request query parameters

Parameter Name	Description	Default	Type	Required
acl	The <code>acl</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	Yes

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

{
  "owner": {
    "id": "<owner id>",
```

```

    "name": "<owner name>",
    "type": "<type>"
  },
  "group": {
    "id": "<group id>",
    "name": "<group name>",
    "type": "<type>"
  },
  "authoritative": "acl" | "mode",
  "mode": "<POSIX mode>",
  "acl": [
    {
      "trustee": {
        "id": "<trustee id>",
        "name": "<trustee name>",
        "type": "<trustee type>"
      },
      "accesstype": "allow" | "deny",
      "accessrights": "<accessrights_list>",
      "inherit_flags": "<inherit_flags_list>"
    }
  ]
}

```

### Response body parameters

Parameter Name	Description
owner	Provides the JSON object for the owner persona.
group	Provides the JSON object for the group persona of the owner.
authoritative	Can be set to <code>acl</code> or <code>mode</code> . If the directory has access rights set, then this field is returned as <code>acl</code> . If the directory has POSIX permissions set, then this field is returned as <code>mode</code> .
mode	Provides the POSIX mode.
acl	Provides the JSON array of access rights.
accesstype	Can be set to <code>allow</code> or <code>deny</code> . <code>allow</code> : Allows access to the directory based on the access rights set for the trustee. <code>deny</code> : Denies access to the directory based on the access rights set for the trustee.
accessrights	Provides the list of access rights that are defined for the directory.
inherit_flags	Provides the inherit flags set for the directory.

### Example request

```

GET /namespace/ifs/dir1/dir2/dir?acl HTTP/1.1
Host: my_cluster:8080
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>

```

**Example response**

```

HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

{
  "owner":{
    "id":"UID:0",
    "name":"root",
    "type":"user"
  },
  "group":{
    "id":"GID:0",
    "name":"wheel",
    "type":"group"
  },
  "authoritative":"acl",
  "mode":"0722",
  "acl":[
    {
      "trustee":{
        "id":"UID:2001",
        "name":"fool",
        "type":"user"
      },
      "accesstype":"allow",
      "accessrights":[
        "dir_gen_read",
        "dir_gen_write"
      ],
      "inherit_flags":[
        "container_inherit"
      ]
    },
    {
      "trustee":{
        "id":"GID:23",
        "name":"group1",
        "type":"group"
      },
      "accesstype":"allow",
      "accessrights":[
        "dir_gen_read"
      ]
    }
  ]
}

```

**Get the ACL of a file**

Retrieves the access control list of the file for the authenticated user.

**Request syntax**

```

GET /namespace/<access_point>/<container_path>/<file_name>?acl HTTP/
1.1
Host: <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

**Request query parameters**

Parameter Name	Description	Default	Type	Required
acl	The <code>acl</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	Yes

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

```

HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

{
  "owner":{
    "id":"<owner id>",
    "name":"<owner name>",
    "type":"<type>"
  },
  "group":{
    "id":"<group id>",
    "name":"<group name>",
    "type":"<type>"
  },
  "authoritative":"acl"|"mode",
  "mode":"<POSIX mode>",
  "acl":[
    {
      "trustee":{
        "id":"<trustee id>",
        "name":"<trustee name>",
        "type":"<trustee type>"
      },
      "accesstype":"allow"|"deny",
      "accessrights":"<accessrights_list>",
      "inherit_flags":"<inherit_flags>"
    }
  ]
}

```

**Response body parameters**

Parameter Name	Description
owner	Provides the JSON object for the owner persona.
group	Provides the JSON object for the group persona of the owner.
authoritative	Can be set to <code>acl</code> or <code>mode</code> . If the directory has access rights set, then this field is returned as <code>acl</code> . If the directory has POSIX permissions set, then this field is returned as <code>mode</code> .

Parameter Name	Description
acl	Provides the JSON array of access rights.
acesstype	Can be set to <code>allow</code> or <code>deny</code> . <code>allow</code> : Allows access to the file based on the access rights set for the trustee. <code>deny</code> : Denies access to the file based on the access rights set for the trustee.
accessrights	Provides the list of access rights defined for the file.
inherit_flags	Provides the inherit flags set for the file.

### Example request

```
GET /namespace/ifs/dir1/dir2/file1?acl HTTP/1.1
Host: my_cluster:8080
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
```

### Example response

```
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2011 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

```
{
  "owner":{
    "id":"UID:0",
    "name":"root",
    "type":"user"
  },
  "group":{
    "id":"GID:0",
    "name":"wheel",
    "type":"group"
  },
  "authoritative":"acl",
  "mode":"0022",
  "acl":[
    {
      "trustee":{
        "id":"UID:2000",
        "name":"foo2",
        "type":"user"
      },
      "acesstype":"allow",
      "accessrights":[
        "file_gen_read",
        "file_gen_write"
      ]
    },
    {
      "trustee":{
        "id":"GID:1001",
        "name":"group2",
        "type":"group"
      },
      "acesstype":"allow",
```

```

    "accessrights":[
      "file_gen_read"
    ]
  }
}

```

## Set the ACL for a directory when the directory is created

Sets the access control list for a directory by setting the headers when the directory is created.

### Request syntax

```

PUT /namespace/<access_point>/<container_path>/<container_name>
HTTP/1.1
Host: <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>
x-isi-ifs-access-control : "private_read" | "private" |
"public_read" | "public_read_write" | "public" | "<POSIX mode>"

```

### Note

The attribute `x-isi-ifs-access-control` can be set to a pre-defined ACL value or to a POSIX mode in octal string. If this header is not specified, the directory mode is set to 0700 by default when the directory is created.

Pre-defined ACL value	Access rights	Access rights displayed
private_read	The directory owner has the following rights: list entries, read attributes, read extended attributes, access files in subdirectories, read access control list, and write access control list.	Directory owner: "accessrights": ["dir_gen_read","dir_gen_execute","std_write_dac"],"inherit_flags":[]
private	The directory owner has the following rights: list entries, read attributes, read extended attributes, read access control list, create files, create subdirectories, write attributes, write extended attributes, access files in subdirectories, delete children (including read-only files), change owner, write access control list, and delete current directory.	Directory owner:"accessrights": ["dir_gen_all"],"inherit_flags":[]
public_read	The directory owner has the following rights: list entries, read attributes, read extended attributes, read access control list, create files, create subdirectories, write attributes, write extended	Directory owner: "accessrights": ["dir_gen_all"],"inherit_flags":[] All users: "accessrights": ["dir_gen_read","dir_gen_execute"],"inherit_flags":[]

Pre-defined ACL value	Access rights	Access rights displayed
	attributes, access files in subdirectories, delete children (including read-only files), change owner, write the access control list, and delete current directory. All users have the following rights: list entries, read attributes, read extended attributes, read access control lists, and access files in subdirectories.	
public_read_write	The directory owner has the following rights: list entries, read attributes, read extended attributes, read access control list, create files, create subdirectories, write attributes, write extended attributes, access files in subdirectories, delete children (including read-only files), change owner, write the access control list, and delete current directory. All users have the following rights: list entries, read attributes, read extended attributes, read access control lists, create files, create subdirectories, write attributes, write extended attributes, and access files in subdirectories.	Directory owner: "accessrights": ["dir_gen_all"],"inherit_flags":[] All users: "accessrights": ["dir_gen_read","dir_gen_write","dir_gen_execute"],"inherit_flags":[]
public	All users have the following rights: list entries, read attributes, read extended attributes, read access control list, create files, create subdirectories, write attributes, write extended attributes, access files in subdirectories, delete children (including read-only files), change owner, write access control list, and delete current directory.	All users: "accessrights": ["dir_gen_all"],"inherit_flags":[]

The POSIX mode is an absolute mode that is constructed from the sum of one or more octal numbers listed in the following table.

Octal number	Description
4000	The set-user-ID-on-execution bit. Executable files with this bit have their UID set to the UID of the file owner.
2000	The set-group-ID-on-execution bit. Executable files with this bit have their GID set to the GID of the file owner.
1000	The sticky bit.

Octal number	Description
0400	Allows read by owner.
0200	Allows write by owner.
0100	For files, allows execution by owner. For directories, allows directory queries by owner.
0040	Allows read by group members.
0020	Allows write by group members.
0010	For files, allows execution by group members. For directories, allows directory queries by group members.
0004	Allows read by others.
0002	Allows write by others.
0001	For files, allows execution by others. For directories, allows directory queries by others.

**Request query parameters**

There are no query parameters for this request.

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

There is no message body for this response.

**Example request**

```
PUT /namespace/ifs/dir1/dir2/dir HTTP/1.1
Host: my_cluster:8080
Content-Length: <length>
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
x-isi-ifs-access-control: "public_read"
```

**Example response**

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Set the ACL for a file when the file is created

Sets the access control list for a file by setting the headers when the file is created.

### Request syntax

```
PUT /namespace/<access_point>/<container_path>/<file_name> HTTP/1.1
Host: <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>
x-isi-ifs-access-control : "private_read" | "private" |
"public_read" | "public_read_write" | "public" | "<POSIX mode>"
```

### Note

The attribute `x-isi-ifs-access-control` can be set to a pre-defined ACL value or to POSIX mode with octal string. By default, the mode for the file is set to 0600.

Pre-defined ACL value	Access rights	Access rights displayed
private_read	The file owner has the following rights: read files, read attributes, read extended attributes, read access control lists, execute files, and write access control list.	File owner: "accessrights": ["file_gen_read", "file_gen_execute", "std_write_dac"], "inherit_flags": []
private	The file owner has the following rights: read file, read attributes, read extended attributes, read access control list, write to the file, append to the file, write file attributes, write extended file attributes, execute file, write or modify the access control list, change owner, and delete current file.	File owner: "accessrights": ["file_gen_all"], "inherit_flags": []
public_read	The file owner has the following rights: read file, read attributes, read extended attributes, read access control list, write to the file, append to the file, write file attributes, write extended file attributes, execute file, write or modify the access control list, change owner, and delete current file. All users have the following rights: read files, read attributes, read extended attributes, read access control lists, and execute files.	File owner: "accessrights": ["file_gen_all"], "inherit_flags": [] All users: "accessrights": ["file_gen_read", "file_gen_execute"], "inherit_flags": []
public_read_write	The file owner has the following rights: read file, read attributes, read extended attributes, read access control list, write to the file, append	File owner: "accessrights": ["file_gen_all"], "inherit_flags": [] All users: "accessrights": ["file_gen_read", "file_gen_write",

Pre-defined ACL value	Access rights	Access rights displayed
	to the file, write file attributes, write extended file attributes, execute file, write/modify the access control list, change owner, and delete current file. All users have the following rights: read files, read attributes, read extended attributes, read access control lists, write to the file, append to the file, write file attributes, write extended file attributes, and execute files.	"file_gen_execute"],"inherit_flags":[]
public	All users have the following rights: read file, read attributes, read extended attributes, read access control list, write to the file, append to the file, write file attributes, write extended file attributes, execute file, write/modify the access control list, change owner, and delete current file.	All users: "accessrights": ["file_gen_all"],"inherit_flags":[]

The POSIX mode is an absolute mode, which consists of an octal number that is constructed from the sum of one or more octal numbers listed in the following table.

Octal number	Description
4000	The set-user-ID-on-execution bit. Executable files with this bit have their uid set to the uid of the file owner.
2000	The set-group-ID-on-execution bit. Executable files with this bit have their gid set to the gid of the file owner.
1000	The sticky bit.
0400	Allows read by owner.
0200	Allows write by owner.
0100	For files, allows execution by owner. For directories, allows directory queries by owner.
0040	Allows read by group members.
0020	Allows write by group members.
0010	For files, allows execution by group members. For directories, allows directory queries by group member.
0004	Allows read by others.
0002	Allows write by others.
0001	For files, allows execution by others. For directories, allows directory queries by others.

#### Request query parameters

There are no query parameters for this request.

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

There is no message body for this response.

**Example request**

```
PUT /namespace/ifs/dir1/dir2/file HTTP/1.1
Host: my_cluster:8080
Content-Length: <length>
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
x-isi-ifs-access-control: "public_read"
```

**Example response**

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

**Set the ACL of a directory**

Sets the access control list of the directory.

**Request syntax**

```
PUT /namespace/<access_point>/<container_path>/<container_name>?acl
HTTP/1.1
Host: <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>

{
  "owner":{
    "id": "<owner id>",
    "name": "<owner name>",
    "type": "<type>"
  },
  "group":{
    "id": "<group id>",
    "name": "<group name>",
    "type": "<type>"
  },
  "authoritative": "acl"|"mode",
  "mode": "<POSIX mode>",
  "action": "<action_value>",
  "acl": [
    {
      "trustee":{
        "id": "<trustee id>",
        "name": "<trustee name>",
        "type": "<trustee type>"
      },
      "accesstype": "allow"|"deny",
      "accessrights": "<accessrights_list>",
```

```

    "inherit_flags": "<inherit_flags_list>",
    "op": "<operation_value>"
  }
}

```

**Request query parameters**

Parameter Name	Description	Default	Type	Required
acl	The <code>acl</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	Yes

**Request body parameters**

Parameter Name	Description	Default	Type	Required
owner	Specifies the JSON object for the owner persona. You should only specify the owner persona if you want to change the owner of the target.	N/A	JSON object	No
group	Specifies the JSON object for the group persona of the owner. You should only specify the group persona if you want to change the group of the target.	N/A	JSON object	No
authoritative	The authoritative field is mandatory and can take the value of either <code>acl</code> or <code>mode</code> . <code>acl</code> : You can modify the owner, group personas, or access rights for the directory by setting the authoritative field to <code>acl</code> and by setting <code>&lt;action_value&gt;</code> to <code>update</code> . When the authoritative field is set to <code>acl</code> , access rights are set for the directory from the <code>acl</code> structure. Any value specified for the <code>mode</code> parameter is ignored.	N/A	String	Yes

Parameter Name	Description	Default	Type	Required
	<p><b>Note</b></p> <p>When the authoritative field is set to <code>acl</code>, the default value for the <code>&lt;action_value&gt;</code> field is <code>replace</code>. If the <code>&lt;action_value&gt;</code> field is set to <code>replace</code>, the system replaces the existing access rights of the directory with the access rights specified in the <code>acl</code> structure. If the <code>acl</code> structure is empty, the existing access rights are deleted and default access rights are provided by the system. The default access rights for directories are read access control list (<code>'std_read_dac'</code>) and write access control list (<code>'std_write_dac'</code>) for the owner.</p> <p><code>mode</code>: You can modify the owner and group personas by setting the authoritative field to <code>mode</code>. When the authoritative field is set to <code>mode</code>, POSIX permissions are set on the directory. The <code>&lt;action_value&gt;</code> field and <code>acl</code> structure are ignored. If <code>mode</code> is set on a directory that already has access rights or if access rights are set on a directory that already has POSIX permissions set, the result of the operation varies based on the Global ACL Policy.</p>			
<code>mode</code>	Specifies the POSIX mode.	0700 for directories 0600 for files	Octal number, specified as a string	No
<code>action</code>	<p>The <code>&lt;action_value&gt;</code> field is applied when the authoritative field is set to <code>acl</code>. You can set the <code>&lt;action_value&gt;</code> field to either <code>update</code> or <code>replace</code>.</p> <p>When set to <code>update</code>, the existing access control list of the directory is modified with the access control entries specified in the <code>acl</code> structure of the JSON body.</p> <p>When set to <code>replace</code>, the entire access control list is deleted and replaced with the access control</p>	<code>replace</code>	String	No

Parameter Name	Description	Default	Type	Required
	<p>entries specified in the <code>acl</code> structure of the JSON body.</p> <p>Additionally, when set to <code>replace</code>, the <code>acl</code> structure is optional. If the <code>acl</code> structure is left empty, the entire access control list is deleted and replaced with the system set default access rights. The default access rights for directories are read access control list ('<code>std_read_dac</code>') and write access control list ('<code>std_write_dac</code>') for the owner.</p>			
<code>acl</code>	Specifies the JSON array of access rights.	N/A	JSON object	Conditional. Mandatory when the <code>&lt;action_value&gt;</code> field is set to <code>update</code> ; optional when the <code>&lt;action_value&gt;</code> is set to <code>replace</code>
<code>accesstype</code>	<p>Can be set to <code>allow</code> or <code>deny</code>.</p> <p><code>allow</code>: Allows access to the directory based on the access rights set for the trustee.</p> <p><code>deny</code>: Denies access to the directory based on the access rights set for the trustee.</p>	N/A	String	Yes, unless the <code>&lt;action_value&gt;</code> field is set to <code>replace</code> and the <code>acl</code> structure is empty.
<code>accessrights</code>	Specifies the access right values defined for the directory.	N/A	List of string values	Conditional Mandatory when the <code>&lt;action_value&gt;</code> field is set to <code>update</code> and the <code>&lt;operation_value&gt;</code> field is set to either <code>add</code> or <code>replace</code> and the <code>&lt;inherit_flags_list&gt;</code>

Parameter Name	Description	Default	Type	Required
				field is unspecified. Optional when the <i>&lt;action_value&gt;</i> is set to update and the <i>&lt;operation_value&gt;</i> field is set to delete, or when the <i>&lt;action_value&gt;</i> field is set to replace.
inherit_flags	Specifies the inherit flag values for directories.	N/A	List of string values	Conditional
op	<p>The <i>&lt;operation_value&gt;</i> field is applied when the <i>&lt;action_value&gt;</i> field is set to update. You can set the <i>&lt;operation_value&gt;</i> field to add, replace, or delete. If no <i>&lt;operation_value&gt;</i> field is specified, the default value is add.</p> <p>add: Creates a new access control entry (ACE) if an ACE is not already present for a trustee and trustee access type. If an entry is already present for that trustee and trustee access type, this operation appends the access rights list to the current ACE for that trustee and trustee access type.</p> <p>delete: Removes the access rights list provided from the existing ACE for a trustee and trustee access type. If the input access rights list is empty, the entire ACE that corresponds to the trustee and trustee access type is deleted.</p> <p>replace: Replaces the entire ACE for the trustee and trustee access type with the input access rights list.</p>	add, when <i>&lt;action_value&gt;</i> is set to update.	String	No

### Request headers

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

There is no message body for this response.

**Example request 1**

This sample sets the ACL of a directory.

```
PUT /namespace/ifs/dir1/dir2/dir?acl HTTP/1.1
Host: my_cluster:8080
Content-Length: <length>
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
Content-Type: application/json

{
  "authoritative":"acl",
  "action":"update",
  "acl":[
    {
      "trustee":{
        "id":"UID:1001",
        "name":"user23",
        "type":"user"
      },
      "accesstype":"allow",
      "accessrights":[
        "std_write_dac"
      ],
      "inherit_flags":[
        "object_inherit",
        "inherit_only"
      ],
      "op":"add"
    },
    {
      "trustee":{
        "id":"GID:1210",
        "name":"group12",
        "type":"group"
      },
      "accesstype":"allow",
      "accessrights":[],
      "op":"delete"
    }
  ]
}
```

**Example response 1**

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

**Example request 2**

This sample replaces the existing ACL of the directory with the access control entries specified in the `acl` structure. If the `acl` structure is empty, the existing ACL is

replaced with default system values. The directory owner has default read and write access to the access control list.

```
PUT /namespace/ifs/dir1/dir2/dir?acl HTTP/1.1
Host: my_cluster:8080
Content-Length: <length>
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
Content-Type: application/json

{
  "owner":{
    "id":"UID:2001",
    "name":"fool",
    "type":"user"
  },
  "group":{
    "id":"GID:0",
    "name":"wheel",
    "type":"group"
  },
  "authoritative":"acl",
  "action":"replace",
  "acl":[]
}
```

### Example response 2

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19
```

## Set the ACL of a file

Sets the access control list of a file.

### Request syntax

```
PUT /namespace/<access_point>/<container_path>/<file_name>?acl HTTP/
1.1
Host: <hostname>[:<port>]
Content-Length: <length>
Date: <date>
Authorization: <signature>
x-isi-ifs-target-type: object
Content-Type: application/json

{
  "owner":{
    "id":"<owner id>",
    "name":"<owner name>",
    "type":"<type>"
  },
  "group":{
    "id":"<group id>",
    "name":"<group name>",
    "type":"<type>"
  },
  "authoritative":"acl|"mode",
  "mode":"<POSIX mode>",
```

```

"action": "<action_value>",
"acl": [
  {
    "trustee": {
      "id": "<trustee id>",
      "name": "<trustee name>",
      "type": "<trustee type>"
    },
    "accesstype": "allow"|"deny",
    "accessrights": "<accessrights_list>",
    "op": "<operation_value>"
  }
]
}

```

### Request query parameters

Parameter Name	Description	Default	Type	Required
acl	The <code>acl</code> argument must be placed at the first position of the argument list in the URI.	N/A	String	Yes

### Request body parameters

Parameter Name	Description	Default	Type	Required
owner	Specifies the JSON object for the owner persona. You should only specify the owner or group persona if you want to change the owner or group of the target.	N/A	JSON object	No
group	Specifies the JSON object for the group persona of the owner. You should only specify the owner or group persona if you want to change the owner or group of the target.	N/A	JSON object	No
authoritative	The authoritative field is mandatory and can take the value of either <code>acl</code> or <code>mode</code> . <code>acl</code> : You can modify the owner, group personas, or access rights for the file by setting the authoritative field to <code>acl</code> and by setting <code>&lt;action_value&gt;</code> to <code>update</code> . When the authoritative field is set to <code>acl</code> , access rights are set for the file from the <code>acl</code> structure. Any value specified for the <code>mode</code> parameter is ignored.	N/A	String	Yes

Parameter Name	Description	Default	Type	Required
	<p><b>Note</b></p> <p>When the authoritative field is set to <code>acl</code>, the default value for the <code>&lt;action_value&gt;</code> field is <code>replace</code>. If the <code>&lt;action_value&gt;</code> field is set to <code>replace</code>, the system replaces the existing access rights of the file with the access rights specified in the <code>acl</code> structure. If the <code>acl</code> structure is empty, the existing access rights are deleted and default access rights are provided by the system. The default access rights for files are read access control list ('<code>std_read_dac</code>') and write access control list ('<code>std_write_dac</code>') for the owner.</p> <hr/> <p><code>mode</code>: You can modify the owner and group personas by setting the authoritative field to <code>mode</code>. When the authoritative field is set to <code>mode</code>, POSIX permissions are set on the file. The <code>&lt;action_value&gt;</code> field and <code>acl</code> structure are ignored. If <code>mode</code> is set on a file that already has access rights or if access rights are set on a file that already has POSIX permissions set, the result of the operation varies based on the Global ACL Policy.</p>			
<code>mode</code>	Specifies the POSIX mode.	0700 for directories 0600 for files	Octal number, specified as a string	No
<code>action</code>	<p>The <code>&lt;action_value&gt;</code> field is applied when the authoritative field is set to <code>acl</code>. You can set the <code>&lt;action_value&gt;</code> field to either <code>update</code> or <code>replace</code>. The default value is <code>replace</code>.</p> <p>When set to <code>update</code>, the existing access control list of the file is modified with the access control entries specified in the <code>acl</code> structure of the JSON body.</p> <p>When set to <code>replace</code>, the entire access control list is deleted and</p>	<code>replace</code>	String	No

Parameter Name	Description	Default	Type	Required
	<p>replaced with the access control entries specified in the <code>acl</code> structure of the JSON body.</p> <p>Additionally, when set to <code>replace</code>, the <code>acl</code> structure is optional. If the <code>acl</code> structure is left empty, the entire access control list is deleted and replaced with the system set default access rights. The default access rights for files are read access control list ('<code>std_read_dac</code>') and write access control list ('<code>std_write_dac</code>') for the owner.</p>			
<code>acl</code>	Specifies the JSON array of access rights.	N/A	JSON object	Conditional Mandatory when the <code>&lt;action_value&gt;</code> field is set to <code>update</code> and optional when the <code>&lt;action_value&gt;</code> field is set to <code>replace</code> .
<code>accesstype</code>	<p>Can be set to <code>allow</code> or <code>deny</code>.</p> <p><code>allow</code>: Allows access to the file based on the access rights set for the trustee.</p> <p><code>deny</code>: Denies access to the file based on the access rights set for the trustee.</p>	N/A	String	Yes, unless the <code>&lt;action_value&gt;</code> field is set to <code>replace</code> and the <code>acl</code> structure is empty.
<code>accessrights</code>	Specifies the access right values defined for the file.	N/A	List of string values	Conditional Mandatory when the <code>&lt;action_value&gt;</code> field is set to <code>update</code> and the <code>&lt;operation_value&gt;</code> field is set to either <code>add</code> or <code>replace</code> ,

Parameter Name	Description	Default	Type	Required
				and when the <i>&lt;inherit_flags_list&gt;</i> field is unspecified.  Optional when the <i>&lt;action_value&gt;</i> field is set to update and the <i>&lt;operation_value&gt;</i> is set to delete.
inherit_flags	Specifies the inherit flag values for the file.	N/A	List of string values	Conditional Either the <i>&lt;accessrights_list&gt;</i> or <i>&lt;inherit_flags_list&gt;</i> must be specified when the <i>&lt;action_value&gt;</i> field is set to update and the <i>&lt;operation_value&gt;</i> field is set to add or replace.
op	The <i>&lt;operation_value&gt;</i> field is applied when the <i>&lt;action_value&gt;</i> field is set to update. You can set the <i>&lt;operation_value&gt;</i> field to add, replace, or delete. If no <i>&lt;operation_value&gt;</i> field is specified, the default value is add. add: Creates a new access control entry (ACE) if an ACE is not already present for a trustee and trustee access type. If an entry is already present for that trustee and trustee access type, this operation appends the access rights list to the current	add, when the <i>&lt;action_value&gt;</i> field is set to update	String	No

Parameter Name	Description	Default	Type	Required
	<p>ACE for that trustee and trustee access type.</p> <p><code>delete</code>: Removes the access rights list provided from the existing ACE for a trustee and trustee access type. If the input access rights list is empty , the entire ACE that corresponds to the trustee and trustee access type is deleted.</p> <p><code>replace</code>: Replaces the entire ACE for the trustee and trustee access type with the input access rights list.</p>			

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

No message body is returned upon success.

**Example request**

This sample sets the ACL of a file named 'file1'.

```
PUT /namespace/ifs/dir1/dir2/ns/file1?acl HTTP/1.1
Host: my_cluster:8080
Content-Length: <length>
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
Content-Type: application/json

{
  "owner":{
    "id":"UID:0",
    "name":"root",
    "type":"user"
  },
  "group":{
    "id":"GID:0",
    "name":"wheel",
    "type":"group"
  },
  "authoritative":"acl",
  "action":"update",
  "acl": [
    {
      "trustee":{
        "id":"UID:0",
        "name":"root",
        "type":"user"
      },
      "accesstype":"allow",
      "accessrights":[
        "file_read",
        "file_write"
      ]
    }
  ]
}
```

```

    ],
    "op": "add"
  },
  {
    "trustee": {
      "id": "GID:1201",
      "name": "group12",
      "type": "group"
    },
    "accesstype": "allow",
    "accessrights": "std_write_dac"
  },
  ],
  "op": "replace"
}
]
}

```

### Example response

```

HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

```

## Query operations

You can search for files and directories on the namespace that matches certain criteria. Files are searched for through a namespace traverse and a filtering mechanism.

### Query an object

Query objects by system-defined and user-defined attributes in a directory.

#### Request syntax

```

POST /namespace/<access_point>/<container_path>?
query[&<query_param>] HTTP/1.1
Host <hostname>[:<port>]
Date: <date>
Authorization: <signature>

[JSON BODY]

```

#### Request query parameters

The *query\_param* argument is optional and can be one or more of the parameters in the following table, separated by an “&”.

Parameter Name	Description	Default	Type	Required
limit	Specifies the maximum number of objects to send to the client. You can set the value to a negative number to retrieve all objects.	1000	String	No
detail	Specifies which object attributes are displayed. If the <code>detail</code> parameter	No	String	No

Parameter Name	Description	Default	Type	Required
	<p>is excluded, only the name of the object is returned. If the <code>detail</code> parameter is set to <code>yes</code>, then system information such as name, owner, group, mode, and size is returned. You can specify multiple attribute names in CSV format. For example:</p> <pre>detail=size,container,cont ent_type</pre> <p>If you set this value to default, the following attributes are included: name, size, owner, last_modified, type, group, and mode.</p>			
<code>max-depth</code>	Specifies the maximum directory level depth to search for objects. If set to 0, only the specified directory is searched for objects. If set to -1, the entire hierarchy below the specified directory is searched for objects.	0	String	No

**Request headers**

This call sends common request headers.

**Response headers**

This call returns common response headers.

**Response body**

An array of the objects that match the query filter criteria are returned in the JSON body.

**Example request**

```
POST /namespace/ifs/my_folder/?query HTTP/1.1
Host my_cluster:8080
Date: <date>
Authorization: <signature>

{
  "result": [
    "name",
    "size",
    "last_modified",
    "container_path",
    "user.color",
    "content_type"
  ],
  "scope": {
    "logic": "and",
    "conditions": [
      {
        "operator": ">=",
        "attr": "last_modified",
```

```

        "value":"Thu, 15 Dec 2011 06:41:04"
      },
      {
        "operator":"like",
        "attr":"name",
        "value":"ta.*"
      }
    ]
  }
}

```

### Example response

```

{
  "children" :
  [
    {
      "content_type " : "text/plain; charset=UTF-8",
      "container_path" : "/ifs/movie",
      "last_modified" : "Thu, 05 Jan 2012 04:29:56 GMT",
      "name" : "fantasy",
      "size" : 56
    },
    {
      "content_type " : "text/plain; charset=UTF-8",
      "container_path" : "/ifs/folder",
      "last_modified" : "Thu, 15 Dec 2011 06:41:04
GMT",
      "name" : "tar",
      "size" : 3359,
      "user.color" : "green"
    }
  ]
}

```

## JSON query format

You can apply the following JSON query format to refine your search.

The query is defined in the following format, in Backus-Naur Form (BNF) style.

```

query = <scope_query> |
{
  "result":<attribute_list>,
  "scope":<scope_query>
}scope_query = predicate |{
  "logic": "<logic_operator>",
  "conditions": [
    <condition>
  ]
}

```

The `attribute_list` is an array of attribute names, which include system attributes and user-defined attributes. For example:

```
["name", "last_modified", "user.color"]
```

In the results, the user-defined attribute is prefixed with "user."

The only logical operators supported are "and", "or", and "not", where "not" is an unary operator and only one condition is valid. The "not" operator negates the

condition evaluated in the conditions parameter. You must specify two or more conditions for the "and" and "or" operators in the conditions parameter.

```
logic_operator = and|or|not
```

The conditions parameter includes an array of conditions. Each condition is defined as follows:

```
condition = scope_query|predicate
```

The predicate value is defined as follows:

```
predicate =
{
  "operator": "<comparison_operator>",
  "attr": "attr_name",
  "value": "attr_value" | string_array
}
```

The <comparison\_operator> value can be any of the following operators: =, !=, <, <=, >, >=, like, or in.

The arithmetic comparison operators are self-explanatory. The "like" operator matches the specified attribute with a pattern of regular expressions. For example, the following JSON query returns all objects with the attribute "Model" prefixed with "T75":

```
{
  "operator": "like",
  "attr": "user.Model",
  "value": "^T75.*"
}
```

If the operator is set to "in", the value must be an array of strings, with at least one element in the array. When only one element is in the array, the "in" operator behaves the same way as the "=" operator. For example, the following query returns objects with the attribute "color" set to either "blue", "green", or "turquoise":

```
{
  "operator": "in",
  "attr": "user.color",
  "value": [
    "blue",
    "green",
    "turquoise"
  ]
}
```

The attribute name can be the name of a user-defined attribute or one of the system defined attributes, such as:

```
"name" : file or directory name
"size" : the object size in bytes
"last_modified" : last modified date
"content_type" : content type
```

```
"container" : the container name
"container_path" : the container full path
"owner": the owner of the object
```

If the attribute is the user-defined attribute, the attribute must be prefixed with "user." to differentiate the attribute from a system attribute with the same name. For example, if there is a user defined attribute called "name", you should write the attribute as "user.name."

Multiple query predicates can be combined through logical operators. For example, the following query returns objects that satisfy one of the following conditions: "Model" is prefixed with T75 or the "color" attribute is either "red," "green," or "turquoise," or the "manufacture" attribute is ACME.

```
{
  "logic": "or",
  "conditions": [
    {
      "operator": "like",
      "attr": "user.Model",
      "value": "^T75.*"
    },
    {
      "operator": "in",
      "attr": "user.color",
      "value": [
        "red",
        "green",
        "turquoise"
      ]
    },
    {
      "operator": "=",
      "attr": "user.manufacture",
      "value": "ACME"
    }
  ]
}
```

Instead of basic predicates, the element of the conditions array can be a sub-query, which allows more complex queries. For example, the following query returns objects in which either the attribute "manufacture" is set to "ACME" or the "model" attribute is set to "T750," and the "color" attribute is set to "black."

```
{
  "logic": "or",
  "conditions": [
    {
      "operator": "=",
      "attr": "user.manufacture",
      "value": "ACME"
    },
    {
      "logic": "and",
      "conditions": [
        {
          "operator": "=",
          "attr": "user.model",
          "value": "T750"
        },
        {
          "operator": "=",

```

```

        "attr": "user.color",
        "value": "black"
      }
    ]
  }
}

```

## SmartLock settings

Only root users can configure SmartLock Write Once Read Many (WORM) retention date and commit flag settings for a file in a SmartLock directory. A SmartLock license must be active on the cluster to configure these settings.

### Get the WORM properties of a file

Retrieves the WORM retention date and committed state of the file.

#### Request syntax

```

GET /namespace/<access_point>/<WORM_directory>/<file_name>?worm
HTTP/1.1
Host: <hostname>[:<port>]
Date: <date>
Authorization: <signature>

```

#### Request query parameters

Parameter Name	Description	Default	Type	Required
worm	The worm argument must be placed at the first position of the argument list in the URI.	N/A	String	No

#### Request headers

This call sends common request headers.

#### Response headers

This call returns common response headers.

#### Response body

```

{
  "worm_committed":<boolean>,
  "worm_override_retention_date":<"YYYY-MM-DD hh:mm:ss GMT">|null,
  "worm_override_retention_date_val":<seconds from the Epoch>|null,
  "worm_retention_date":<"YYYY-MM-DD hh:mm:ss GMT">|null,
  "worm_retention_date_val":<seconds from the Epoch>|null
}

```

#### Response body parameters

Parameter Name	Description
worm_committed	Indicates whether the file was committed to the WORM state.

Parameter Name	Description
worm_retention_date	Provides the retention expiration date in Coordinated Universal Time (such as UTC/GMT). If a value is not specified, the field has a null value.
worm_retention_date_val	Provides the retention expiration date in seconds from UNIX Epoch or UTC.
worm_override_retention_date	Provides the override retention date that is set on the SmartLock directory where the file resides. If the date is not set or is earlier than or equal to the existing file retention date, this field has a null value. Otherwise, the date is expressed in UTC/GMT, and is the retention expiration date for the file if the <code>worm_committed</code> parameter is also set to true.
worm_override_retention_date_val	Provides the override retention date that is set on the SmartLock directory where the file resides. If the date is not set or if the date is set to earlier than or equal to the file retention date, this field has a null value. Otherwise, the date is expressed in seconds from UNIX Epoch and UTC, and is the retention expiration date set for the file if the <code>worm_committed</code> parameter is set to true. This parameter is the same as <code>worm_override_retention_date</code> , but is expressed in seconds from the Epoch or UTC.

### Example request

```
GET /namespace/ifs/dir1/file?worm HTTP/1.1
Host: my_cluster:8080
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>
```

### Example response

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: <length>
Connection: close
Server: Apache2/2.2.19

{
  "worm_committed":true,
  "worm_retention_date":"2013-01-22 15:11:36 GMT",
  "worm_override_retention_date":null,
  "worm_retention_date_val":1358885496,
  "worm_override_retention_date_val":null
}
```

## Set the retention period and commit a file in a SmartLock directory

Sets the retention period and commits a file in a SmartLock directory.

### Request syntax

```
PUT /namespace/<access_point>/<WORM_directory>/<file_name>?worm
HTTP/1.1
```

```
Host: <hostname>[:<port>]
Date: <date>
Authorization: <signature>

{
  "worm_retention_date":<"YYYY-MM-DD hh:mm:ss GMT">,
  "commit_to_worm":<Boolean>
}
```

---

### Note

If a file is not explicitly committed and an autocommit time period is configured for the SmartLock directory where the file resides, the file is automatically committed when the autocommit period elapses.

If the file is committed without setting a retention expiration date, the default retention period specified for the SmartLock directory where the file resides is applied. The retention date on the file can also be limited by the maximum retention period set on the SmartLock directory.

For details about SmartLock WORM behavior, refer to the *OneFS Administration Guide*.

---

### Request query parameters

Parameter Name	Description	Default	Type	Required
worm	The worm argument must be placed at the first position of the argument list in the URI.	N/A	String	No

### Request body parameters

Parameter Name	Description	Default	Type	Required
worm_retention_date	Specifies the retention expiration date string in Coordinated Universal Time (UTC/GMT).	N/A	Time, in the string format of: "YYYY-MM-DD hh:m:ss GMT"	No
commit_to_worm	Specifies whether to commit the file to a WORM state after the retention date is set. If the file was committed before, the file remains committed regardless of the value in this field.	False	Boolean	No

### Request headers

This call sends common request headers.

### Response headers

This call returns common response headers.

### Response body

No message body is returned upon success.

**Example request**

Set the retention date for a file in a SmartLock directory.

```
PUT /namespace/ifs/dir1/file?worm HTTP/1.1
Host: my_cluster:8080
Date: Tue, 22 May 2012 12:00:00 GMT
Authorization: <signature>

{
  "worm_retention_date": "2013-04-11 12:00:00 GMT",
  "commit_to_worm": true
}
```

**Example response**

```
HTTP/1.1 200 OK
Date: Tue, 22 May 2012 12:00:00 GMT
Content-Length: 0
Connection: close
Server: Apache2/2.2.19
```

## Code samples for file system access

Code samples illustrate the basic syntax of OneFS API requests for file system access.

You can download a zip file that contains code samples for C++ and Python programming languages and for curl commands from [EMC Online Support](#). The sample code provides brief examples on how to access, modify, and delete files and directories on your cluster through OneFS API requests.

