Hitachi Content Platform for Cloud Scale

v2.0.0

Management API Reference

This document describes the management REST API methods available in the Hitachi Content Platform for cloud scale (HCP for cloud scale) software.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at https://www.hitachivantara.com/en-us/company/legal.html.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Contents

Preface

About this document

This document describes the management REST API methods available in the Hitachi Content Platform for cloud scale (HCP for cloud scale) software.

Intended audience

This document is intended for people who are managing or administering HCP for cloud scale systems. It assumes you have experience with APIs and some experience writing scripts that issue API methods.

Product version

This document applies to v2.0.0 of Hitachi Content Platform for cloud scale.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents.

Related documents

This is the set of documents containing information about HCP for cloud scale. You should have these documents available before using the product.

- *Hitachi Content Platform for Cloud Scale Release Notes* (RN-HCPCS004-07): This document is for customers and describes new features, product documentation, and resolved and known issues, and provides other useful information about this release of the product.
- *Installing Hitachi Content Platform for Cloud Scale* (MK-HCPCS002-07): This document gives you the information you need to install or update the HCP for cloud scale software.

- *Hitachi Content Platform for Cloud Scale Administration Guide* (MK-HCPCS008-03): This document explains how to use the HCP for cloud scale applications to configure and operate a common object storage interface for clients to interact with; configure HCP for cloud scale for your users; enable and disable system features; and monitor the system and its connections.

- *Hitachi Content Platform for Cloud Scale S3 Console Guide* (MK-HCPCS009-00): This document is for end users and explains how to use the HCP for cloud scale S3 Console application to use S3 credentials and to simplify the process of creating, monitoring, and maintaining S3 buckets.

- *Hitachi Content Platform for Cloud Scale Management API Reference* (MK-HCPCS007-05): This document is for customers and describes the management application programming interface (API) methods available for customer use.

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	- Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. - Indicates emphasized words in list items.
Italic	- Indicates a document title or emphasized words in text. - Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: - Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` - Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.

Convention	Description
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
📄	Note	Calls attention to important or additional information.
💡	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
⚠	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Introducing Hitachi Content Platform for cloud scale

Hitachi Content Platform for cloud scale (HCP for cloud scale) is a software-defined object storage solution that is based on a massively parallel microservice architecture and is compatible with the Amazon S3 application programming interface (API).

HCP for cloud scale is especially well suited to service applications requiring high bandwidth and compatibility with the Amazon S3 API.

HCP for cloud scale has the ability to federate S3-compatible storage from virtually any private or public source, and present the combined capacity in a single, centrally managed, global namespace.

You can install HCP for cloud scale on any server, in the cloud or on premise, that supports the minimum requirements.

HCP for cloud scale lets you manage and scale storage components. You can add storage components, monitor their states, and take them online or offline for maintenance and repair. The HCP for cloud scale system includes functions to send notification of alerts, track and monitor throughput and performance, and trace actions through the system.

Getting started with the mangement API

HCP for cloud scale includes a RESTful HTTP interface for the following functions:

- Managing storage components and Amazon Simple Storage Service (Amazon S3) settings
- Managing administrative resources such as serial numbers and system events
- Managing user resources such as S3 user credentials and OAuth tokens

The Object Storage Management management API (MAPI) methods are served by the MAPI Gateway service from any HCP for cloud scale node.

You can execute all functions supported in the Object Storage Management application and the S3 User Credentials application using MAPI methods.

All URLs for the Object Storage Management MAPI methods have the following base, or root, uniform resource identifier (URI):

```
https://hcpcs_ip_address:9099/mapi/v1
```

> 📄 **Note:** You can execute all system configuration, management, and monitoring functions supported in the System Management application using System Management MAPI methods. Those methods are separate and use a separate port.

Input and output formats

The API accepts and returns JSON.

The REST API accepts and returns JavaScript Object Notation (JSON). It does not support HTTPS 1.0 requests; all HTTPS 1.0 requests are denied. When the body of the request has contents, the MAPI accepts and returns JSON; when the body is empty, JSON format is unnecessary.

Requesting and submitting an access token

You need to request an access token from the system. Send an `HTTP POST` request to the method `/auth/oauth`.

To use the API interface, the account you're using must have the appropriate permissions assigned, and you need a valid OAuth access token. For information about the permissions needed for making API calls, see the online help. The security access token, known as a *Bearer token*, authorizes all requests made to access and manage storage components and S3 settings in an HCP for cloud scale system.

> 📄 **Note:**
>
> - To get a list of security realms for the system, send an `HTTP GET` request to the method `/setup`. For example, to do this with cURL, send this command:
>
>   ```
>   curl -k -X GET --header 'Accept: application/json' 'https://
>   mysystem.example.com:admin-app-port/api/admin/setup'
>   ```
>
> - To get an access token for the local admin user account, you can omit the realm option for the request, or specify a realm value of `Local`.

To request an access token:

Procedure

1. Send an `HTTP POST` request to the method `/auth/oauth` in the System Management application API.

   The payload of the request must include your username, password, and realm for a user account.

   The system sends you a JSON response body containing an `access_token` field. The value of this field is your token.

2. Include your access token as part of all REST API requests that you make by submitting an `Authorization` header along with your request.

Example

Here's an example of requesting an authentication token using the cURL command-line tool:

```
curl -ik -X POST https://mysystem.example.com:8000/auth/oauth/ \
-d grant_type=password \
-d username=user1 \
-d password=password1 \
-d scope=* \
-d client_secret=my-client \
-d client_id=my-client \
-d realm=marketingUsers
```

In response to this request, you receive a JSON response body containing an `access_token` field. The value of this field is your token. For example:

```
{
"access_token": "eyJr287bjle..."
"expires_in": 7200
}
```

Here's an example that uses cURL of including an access token as part of a request:

```
curl -X GET --header "Accept:application/json"
    https://mysystem.example.com:admin_app_port/api/admin/instances  --
header "Authorization:
    Bearer eyJr287bjle..."
```

Viewing and using API methods

Your system includes web-based documentation pages where you can view all supported API methods, including the request bodies, request URLs, response bodies, and return codes for each. You can also use these pages to run each API method.

You can use the API documentation pages to experiment with the API. Any requests you submit on the REST API page take effect on the system.

> 📄 **Note:** If you specify UUIDs when creating resources, the UUIDs are ignored.

To use the API page to run a method:

Procedure

1. In either the Object Storage Management App or the System Management App, select the user profile icon, in the upper right portion of the page.
2. Select **API**.
3. Select the row for the method you want.
4. If the method you want needs a UUID:

a. Select the row for the GET method for the resource type that you want.

b. Click **Try It Out!**

c. In the JSON response body, copy the value for the `uuid` field for the resource that you want.

5. If the method you want needs a request body, in the **Parameters** section, under **Model Schema**, click inside the JSON text box.
The JSON text is added to the **Value** field.

> 📄 **Note:** Some methods might need other information in addition to or instead of UUIDs or JSON-formatted text. Some need particular string values or need you to browse for and select a file to upload.

6. Click **Try It Out!**

Including security tokens in MAPI Swagger requests

HCP for cloud scale prevents cross-site request forgery by requiring an `xsrf-token` cookie and passing the header `x-xsrf-token` in API requests. Swagger does not automatically populate this header when executing MAPI requests.

To execute a MAPI request through Swagger:

Procedure

1. From the user profile icon on the top right of the Dashboard, select **REST API**. Swagger opens in a new tab.

2. Locate and copy the value of the cookie XSRF-TOKEN:

   ▪ In Firefox, from the **Open** menu (in the upper right corner), select **Web Developer > Storage Inspector**. From the **Developer Tools** window select **Cookies**. Select and copy the value of the cookie XSRF-TOKEN.

   ▪ In Chrome, from the **Customize** menu (in the upper right corner), select **More tools > Developer tools**. From the **Developer Tools** window select **Storage > Cookies**. Select and copy the value of the cookie XSRF-TOKEN.

3. Select the management API you want to execute and then click **Try it out**.

4. Paste the value of the cookie into the field **X-XSRF TOKEN**.

5. Click **Execute**.

HTTP status codes

When an HTTP request is sent to a server, the server sends back an HTTP response message. The HTTP response message consists of an HTTP header and, optionally, a message body. The response header contains an HTTP status code that gives the status of the request.

The following table contains a list of HTTP status codes, their descriptions, and the types of HTTP requests that can generate each status code.

Status code	Meaning	Description	Methods
200	OK	The request was executed successfully.	PATCH POST
400	Bad Request	The request body contains one or more of these: • An entry that is not valid • A value for an entry that is not valid • JSON formatting that is not valid If the request includes a UUID, the UUID might not be validly formatted.	PATCH POST
401	Unauthorized	Your access is not authorized. Possible reasons: • No credentials are given with the request. • The credentials provided with the request are not valid.	PATCH POST
404	Not Found	The resource you are trying to retrieve, edit, or delete cannot be found.	PATCH POST

Status code	Meaning	Description	Methods
405	Method Not Allowed	A request was made using a request method not supported by that resource; for example, using GET with a form that needs data to be presented using POST.	PATCH POST
501	Unimplemented	An API was invoked that HCP for cloud scale doesn't support.	

Chapter 2: Storage component management methods

The management API includes storage component management methods.

> **Note:** If you're working with a storage component that is configured with multiple retries and long timeouts, and if the endpoint for the storage component is unreachable, and if as a result you send multiple verification or activation requests to the endpoint, the MAPI Gateway service can become unresponsive.
>
> If the MAPI Gateway service becomes unresponsive, use the System Management Services function Repair on it.

Activate storage components

When you define a storage component, it is marked as UNVERIFIED and not available to serve requests until you activate it. You can activate a storage component that is in the UNVERIFIED state.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/activate
```

Request structure

The request body is:

```
{
    "id": "uuid"
    }
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the storage component.

Response structure

The response body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "verified": true|false,
  "httpStatus": nnn,
  "errorCode": "code_text",
  "errorMessage": "message_text",
  "daysUntilCertificateExpiration": nnn,
  "state": "state"
}
```

Parameter	Type	Description
id	UUID	The UUID of the storage component.
storageType	String	The type of storage component: ▪ `AMAZON_S3`: An Amazon Web Services S3-compatible node ▪ `HCP_S3`: A Hitachi Content Platform node ▪ `HCPS_S3`: An HCP S Series node ▪ `GENERIC_S3`: An S3-compatible node
verified	Boolean	If `true`, the storage component has been activated. If `false`, it is not verified and awaits administrative action.
httpStatus	32-bit integer	The HTTP status code with which the storage component responded to your request. If `0`, the storage component can't be reached. You can use other values to diagnose the issue.
errorCode	String	Any error code associated with the storage component.
errorMessage	String	Any error message associated with the storage component.
daysUntilCertificate Expiration	32-bit integer	Number of days until the current HTTPS certificate expires.

Parameter	Type	Description
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The MAPI metadata ID is not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component does not exist.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/activate
```

JSON request:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
}
```

JSON response:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageType": "AMAZON_S3",
  "verified": true,
  "httpStatus": 200,
  "errorCode": null,
  "errorMessage": null,
  "daysUntilCertificateExpiration": 364,
  "state": "ACTIVE"
}
```

Configure S3 settings

You can configure custom S3 settings for buckets. You can use this endpoint to configure settings, then use the endpoint `/s3_settings/get` to verify them.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_settings/set
```

Request structure

The request body is:

```
{
  "maxFileSizeBytes": nnnnnnnnnn,
  "maxBucketsPerUser": buckets,
  "maxBulkDeleteRequestSizeBytes": size,
  "maxBulkDeleteRequestSizeCount": count
}
```

Parameter	Required	Type	Description
maxFileSizeBytes	No	Integer	The maximum size, in bytes, of a single object that can be uploaded to an HCP for cloud scale system. Limit: 5 GB, default: 5 GB.

Parameter	Required	Type	Description
maxBucketsPerUser	No	Integer	The maximum number of buckets that a single user can create and own. No limit, default: 100 buckets.
maxBulkDeleteRequest SizeBytes	No	Integer	The maximum, total size of objects, in bytes, allowed in a single bulk deletion. Default: 3 MB.
maxBulkDeleteRequest SizeCount	No	Integer	The maximum, total number of objects allowed in a single bulk deletion. Default: 1000 objects.

Response structure

The response returns the same parameters as the request. The response body structure is:

```
{
  "maxFileSizeBytes": ,
  "maxBucketsPerUser": ,
  "maxBulkDeleteRequestSizeBytes": ,
  "maxBulkDeleteRequestSizeCount":
}
```

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_settings/set
```

JSON request:

```
{
  "maxBucketsPerUser": 1000
}
```

JSON response:

```
{
  "maxFileSizeBytes": 1099511627776,
  "maxBucketsPerUser": 1000,
  "maxBulkDeleteRequestSizeBytes": 3145728,
  "maxBulkDeleteRequestSizeCount": 1000
}
```

Configure storage component

You can configure a storage component, which exposes the S3 buckets for storage of data on various storage back-end systems. Buckets must already be created on the storage component before you can configure it. Ensure that the buckets are empty.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/create
```

Request structure

The request body is:

```
{
  "storageType": "type",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
    "port": [nnnnn],
    "bucket": "bucket_name",
    "region": "[region_name]",
    "authType": "[V2|V4]",
    "siteAffiliation": {
      "id": "uuid"
    },
    "accessKey": "key",
    "secretKey": "key",
    "useProxy": [true|false],
    "proxyHost": "[host_name]",
    "proxyPort": [nnnnn],
    "proxyUserName": "[user_name]",
```

Chapter 2: Storage component management methods

```
      "proxyPassword": "[password]",
      "proxyDomain": "[domain_name]",
      "usePathStyleAlways": [true|false],
      "connectionTimeout": [ms],
      "socketTimeout": [ms],
      "connectionTTL": [ms],
      "maxConnections": [nnnnnnn],
      "userAgentPrefix": "[prefix]",
      "socketSendBufferSizeHint": [nnnnnnn],
      "socketRecvBufferSizeHint": [nnnnnnn],
      "activateNow": {true|false}
   }
}
```

Parameter	Required	Type	Description
storageType	Yes	String	The type of storage component: ▪ `AMAZON_S3`: An Amazon Web Services S3-compatible node ▪ `HCP_S3`: A Hitachi Content Platform node ▪ `HCPS_S3`: An HCP S Series node ▪ `GENERIC_S3`: An S3-compatible node
storageComponent Config	Yes	List	The following storage component configuration values:
label	No	String	The name of the storage component.
host	Yes	String	The URL of the storage component back-end host domain.
https	Yes	Boolean	If `true`, use an HTTPS connection to the back-end system. If `false`, use an HTTP connection. Default: `false`.
port	No	Integer	HTTP port of back-end system.
bucket	Yes	String	Name of the bucket. The bucket must already exist.
region	No	String	The S3 region. Default: `us-west-2`.

Parameter	Required	Type	Description
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: • `V2` • `V4`
siteAffiliation	Yes	UUID	For `id`, the UUID representing the storage component or the user.
accessKey	Yes		Access key of the S3 credentials for access to the bucket.
secretKey	Yes		Secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If `true`, a proxy server is defined. If `false`, it is not. If `true`, then values are required for `proxyHost` and `proxyHost`. Default: `false`.
proxyHost	No	String	The proxy host, if used.
proxyPort	No	Integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. Not supported.
usePathStyleAlways	No	Boolean	If `true`, use path-style syntax to send requests to the back-end system. If `false`, use virtual-hosted style. Default: `true`.
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	No	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request.

Parameter	Required	Type	Description
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify `socketRecvBufferSizeHint`.
socketRecvBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify `socketSendBufferSizeHint`.
activateNow	No	Boolean	If `true`, activate the storage component immediately. If `false`, do not activate the storage component. Default: `true`.

Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
[
  {
    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
      "useProxy": ,
      "proxyHost": "",
      "proxyPort": ,
      "proxyUserName": "",
      "proxyPassword": "",
```

Chapter 2: Storage component management methods

```
        "proxyDomain": "",
        "usePathStyleAlways": ,
        "connectionTimeout": ,
        "socketTimeout": ,
        "connectionTTL": ,
        "maxConnections": ,
        "userAgentPrefix": "",
        "socketSendBufferSizeHint": ,
        "socketRecvBufferSizeHint": ,
        "readOnly": ,
        "state": "state"
      }
    }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/create
```

JSON request:

```
{
  "storageType": "AMAZON_S3",
  "storageComponentConfig": {
    "label": "Cloud AWS Bucket",
    "host": "URL of an existing storage component backend",
    "https": true,
    "port": 0,
    "bucket": "string",
    "region": "string",
    "authType": "V2",
    "siteAffiliation": {
      "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
    },
    "accessKey": "string",
    "secretKey": "string",
    "useProxy": true,
    "proxyHost": "string",
    "proxyPort": null,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyDomain": "string",
    "usePathStyleAlways": true,
    "connectionTimeout": null,
```

Chapter 2: Storage component management methods

```
      "socketTimeout": null,
      "connectionTTL": null,
      "maxConnections": null,
      "userAgentPrefix": "string",
      "socketSendBufferSizeHint": null,
      "socketRecvBufferSizeHint": null,
      "activateNow": true
  }
}
```

JSON response:

```
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Cloud AWS Bucket",
      "host": "URL of an existing storage component backend",
      "https": false,
      "port": 0,
      "bucket": "string",
      "region": "string",
      "authType": "V2",
      "siteAffiliation": {
        "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
      },
      "useProxy": true,
      "proxyHost": "string",
      "proxyPort": 0,
      "proxyUserName": "string",
      "proxyPassword": "string",
      "proxyDomain": "string",
      "usePathStyleAlways": true,
      "connectionTimeout": 0,
      "socketTimeout": 0,
      "connectionTTL": 0,
      "maxConnections": 0,
      "userAgentPrefix": "string",
      "socketSendBufferSizeHint": 0,
      "socketRecvBufferSizeHint": 0,
      "readOnly": true,
      "state": "ACTIVE"
    }
  }
]
```

Chapter 2: Storage component management methods

Get S3 settings

You can retrieve the current S3 settings. You can use the endpoint `/s3_settings/set` to configure settings, then use this endpoint to verify them.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_settings/get
```

Request structure

Not applicable.

Response structure

The response body is:

```
{
  "maxFileSizeBytes": nnnnnnnnnn,
  "maxBucketsPerUser": buckets,
  "maxBulkDeleteRequestSizeBytes": size,
  "maxBulkDeleteRequestSizeCount": count
}
```

Parameter	Required	Type	Description
maxFileSizeBytes	No	Integer	The maximum size, in bytes, of a single object that can be uploaded to an HCP for cloud scale system. Limit: 5 GB, default: 5 GB.
maxBucketsPerUser	No	Integer	The maximum number of buckets that a single user can create and own. No limit, default: 100 buckets.
maxBulkDeleteRequest SizeBytes	No	Integer	The maximum, total size of objects, in bytes, allowed in a single bulk deletion. Default: 3 MB.
maxBulkDeleteRequest SizeCount	No	Integer	The maximum, total number of objects allowed in a single bulk deletion. Default: 1000 objects.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_settings/get
```

JSON response:

```
{
  "maxFileSizeBytes": 4294967296,
  "maxBucketsPerUser": 100,
  "maxBulkDeleteRequestSizeBytes": 3145728,
  "maxBulkDeleteRequestSizeCount": 1000
}
```

List storage component alerts

You can retrieve a list of active storage component alerts. Alerts are triggered by events and remain active until the condition that caused the event is removed. For example, HCP for cloud scale sends an alert when a storage component is unavailable or its certificate is about to expire. When the event is resolved, the alert is cleared.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/alert/list
```

Request structure

Not applicable.

Response structure

The response body is:

```
[
  {
    "id": "uuid",
    "timestamp": date_time,
    "category": "STORAGECOMPONENT",
    "description": "alert_description"
  }
  .
  .
  .
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
timestamp	64-bit integer	The date and time, in milliseconds since 1 January 1970 GMT, when the alert was generated.
category	String	Alert category: ▪ STORAGECOMPONENT
description	String	The text of the alert.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/alert/list
```

JSON response:

```
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "timestamp": 1571912640205,
```

Chapter 2: Storage component management methods

```
      "category": "STORAGECOMPONENT",
      "description": "string"
    }
]
```

List storage components

You can retrieve a list of all storage components created in the HCP for cloud scale system along with their component settings.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/list
```

Request structure

Not applicable.

Response structure

The response body is:

```
[
  {
    "id": "uuid",
    "storageType": "enum",
    "storageComponentConfig": {
      "label": "label",
      "host": "url",
      "https": true|false,
      "port": nnnnn,
      "bucket": "bucket_name",
      "region": "region_name",
      "authType": "V2|V4",
      "siteAffiliation": {
        "id": "uuid"
      },
      "useProxy": true|false,
      "proxyHost": "host_name",
      "proxyPort": nnnnn,
      "proxyUserName": "user_name",
      "proxyPassword": "password",
      "proxyDomain": "domain_name",
      "usePathStyleAlways": true|false,
      "connectionTimeout": ms,
      "socketTimeout": ms,
      "connectionTTL": ms,
      "maxConnections": nnnnnnn,
      "userAgentPrefix": "prefix",
```

Chapter 2: Storage component management methods

```
      "socketSendBufferSizeHint": nnnnnnn,
      "socketRecvBufferSizeHint": nnnnnnn,
      "readOnly": true|false,
      "state": "state"
    }
  }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
storageType	Enum	The type of storage component: ▪ `AMAZON_S3`: An Amazon Web Services S3-compatible node ▪ `HCP_S3`: A Hitachi Content Platform node ▪ `HCPS_S3`: An HCP S Series node ▪ `GENERIC_S3`: An S3-compatible node
storageComponentConfig	List	The following storage component configuration values:
label	String	The name of the storage component.
host	String	The URL of the storage component back-end host domain.
https	Boolean	`true` for HTTPS connection to back-end system, `false` for HTTP.
port	32-bit integer	HTTP port to back-end system.
bucket	String	The name of the bucket.
region	String	The S3 region.
authType	String	AWS Signature Version, used for authenticating all interactions with Amazon S3: ▪ `V2` ▪ `V4`
siteAffiliation	UUID	The value of `id`, a UUID representing the storage component or the user.
useProxy	Boolean	If `true`, a proxy server is defined. If `false`, a proxy server is not defined.

Parameter	Type	Description
proxyHost	String	The proxy host, if used; otherwise, `null`.
proxyPort	32-bit integer	The proxy port number, if used; otherwise, `null`.
proxyUserName	String	The proxy domain user name, if used; otherwise, `null`.
proxyPassword	String	The proxy domain password, if used; otherwise, `null`).
proxyDomain	String	The proxy domain, if used; otherwise, `null`.
usePathStyleAlways	Boolean	If `true`, use path-style syntax to send requests to the back-end system; if `false`, use virtual-hosted style.
connectionTimeout	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer.
socketRecvBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer.
readOnly	Boolean	If `true`, the storage component is marked as read-only. If `false`, the storage component is available for reading and writing data.

Parameter	Type	Description
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/list
```

JSON response:

```
[
  {
    "id": "8bff981b-5894-43ce-bd41-5a6f548cc241",
    "storageType": "GENERIC_S3",
    "storageComponentConfig": {
      "label": null,
      "host": "172.19.54.102",
```

Chapter 2: Storage component management methods

```
        "https": false,
        "port": 9000,
        "bucket": "samplebucket",
        "region": "us-west-2",
        "authType": null,
        "siteAffiliation": {
          "id": "19b96ae2-38dd-4686-b298-b5bebe173e96"
        },
        "useProxy": false,
        "proxyHost": null,
        "proxyPort": null,
        "proxyUserName": null,
        "proxyPassword": null,
        "proxyDomain": null,
        "usePathStyleAlways": true,
        "connectionTimeout": null,
        "socketTimeout": null,
        "connectionTTL": null,
        "maxConnections": null,
        "userAgentPrefix": null,
        "socketSendBufferSizeHint": null,
        "socketRecvBufferSizeHint": null,
        "readOnly": false,
        "state": "ACTIVE"
      }
    }
]
```

Patch storage component configuration

You can update the configuration of specific storage component settings. Use the endpoint `/storage_component/list` to verify existing settings or changes. Use the endpoint `/storage_component/update` to update all settings.

HTTP request syntax (URI)

```
PATCH https://host_ip:9099/mapi/v1/storage_component/update
```

Request structure

The full request body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
```

Chapter 2: Storage component management methods

```
      "port": [nnnnn],
      "bucket": "bucket_name",
      "region": "[region_name]",
      "authType": "[V2|V4]",
      "siteAffiliation": {
        "id": "uuid"
      },
      "accessKey": "key",
      "secretKey": "key",
      "useProxy": [true|false],
      "proxyHost": "[host_name]",
      "proxyPort": [nnnnn],
      "proxyUserName": "[user_name]",
      "proxyPassword": "[password]",
      "proxyDomain": "[domain_name]",
      "usePathStyleAlways": [true|false],
      "connectionTimeout": [ms],
      "socketTimeout": [ms],
      "connectionTTL": [ms],
      "maxConnections": [nnnnnnn],
      "userAgentPrefix": "[prefix]",
      "socketSendBufferSizeHint": [nnnnnnn],
      "socketRecvBufferSizeHint": [nnnnnnn],
      "readOnly":
    }
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageComponent Config	No	List	The following storage component configuration values as needed:
label	No	String	The name of the storage component.
host	No	String	The URL of the storage component back-end host domain.
https	No	Boolean	If `true`, use an HTTPS connection to the back-end system. If `false`, use an HTTP connection.
port	No	32-bit integer	HTTP port of back-end system.
bucket	No	String	The name of the bucket. The bucket must already exist.

Parameter	Required	Type	Description
region	No	String	The S3 region.
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: ▪ `V2` ▪ `V4`
siteAffiliation	No	UUID	For `id`, the UUID representing the storage component or the user.
accessKey	No	String	The access key of the S3 credentials for access to the bucket.
secretKey	No	String	The secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If `true`, a proxy server is defined. If `false`, a proxy server is not defined. If `true`, then you must provide values for `proxyHost` and `proxyHost`.
proxyHost	No	String	The proxy host, if used.
proxyPort	No	32-bit integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. This is not supported.
usePathStyleAlways	No	Boolean	If `true`, use path-style syntax to send requests to the back-end system. If `false`, use virtual-hosted style.
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	No	32-bit integer	The timeout value for reading from a connected socket.

Chapter 2: Storage component management methods

Parameter	Required	Type	Description
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify `socketRecvBufferSizeHint`.
socketRecvBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify `socketSendBufferSizeHint`.
readOnly	No	Boolean	If `true`, objects can be read and deleted but writes aren't allowed. If `false`, writes are allowed.

Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
[
  {
    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
      "useProxy": ,
      "proxyHost": "",
      "proxyPort": ,
      "proxyUserName": "",
```

Chapter 2: Storage component management methods

```
          "proxyPassword": "",
          "proxyDomain": "",
          "usePathStyleAlways": ,
          "connectionTimeout": ,
          "socketTimeout": ,
          "connectionTTL": ,
          "maxConnections": ,
          "userAgentPrefix": "",
          "socketSendBufferSizeHint": ,
          "socketRecvBufferSizeHint": ,
          "readOnly": ,
          "state": "state"
       }
    }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.

Status code	HTTP name	Description
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
PATCH https://10.10.24.195:9099/mapi/v1/storage_component/update
```

JSON request:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageComponentConfig": {
    "label": "Test cloud"
  }
}
```

JSON response:

```
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Test cloud",
      "host": "172.19.54.102",
      "https": false,
      "port": 9000,
      "bucket": "testbucket",
      "region": "us-west-2",
      "authType": null,
      "siteAffiliation": {
        "id": "19546ae2-38dd-4686-b298-b5beb9173e96"
      },
      "useProxy": false,
      "proxyHost": null,
      "proxyPort": null,
      "proxyUserName": null,
```

Chapter 2: Storage component management methods

```
        "proxyPassword": null,
        "proxyDomain": null,
        "usePathStyleAlways": true,
        "connectionTimeout": null,
        "socketTimeout": null,
        "connectionTTL": null,
        "maxConnections": null,
        "userAgentPrefix": null,
        "socketSendBufferSizeHint": null,
        "socketRecvBufferSizeHint": null,
        "readOnly": false,
        "state": "ACTIVE"
      }
    }
]
```

Set storage component state

You can set the state of a storage component to either ACTIVE or INACTIVE.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/update_state
```

Request structure

The request body is:

```
{
  "id": "uuid",
  "storageComponentState": "{ACTIVE|INACTIVE}"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageComponent State	Yes	String	The storage component state: • `ACTIVE`: Available to serve requests. • `INACTIVE`: Not available to serve requests (administrative pause).

Response structure

The response body structure is:

```
[
  {
    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
      "useProxy": ,
      "proxyHost": "",
      "proxyPort": ,
      "proxyUserName": "",
      "proxyPassword": "",
      "proxyDomain": "",
      "usePathStyleAlways": ,
      "connectionTimeout": ,
      "socketTimeout": ,
      "connectionTTL": ,
      "maxConnections": ,
      "userAgentPrefix": "",
      "socketSendBufferSizeHint": ,
      "socketRecvBufferSizeHint": ,
      "readOnly": ,
      "state": "state"
    }
  }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
storageType	Enum	The type of storage component: ▪ `AMAZON_S3`: An Amazon Web Services S3-compatible node ▪ `HCP_S3`: A Hitachi Content Platform node

Chapter 2: Storage component management methods

Parameter	Type	Description
		`HCPS_S3`: An HCP S Series node `GENERIC_S3`: An S3-compatible node
storageComponentConfig	List	The following storage component configuration values:
label	String	The name of the storage component.
host	String	The URL of the storage component back-end host domain.
https	Boolean	`true` for HTTPS connection to back-end system, `false` for HTTP.
port	32-bit integer	HTTP port to back-end system.
bucket	String	The name of the bucket.
region	String	The S3 region.
authType	String	AWS Signature Version, used for authenticating all interactions with Amazon S3: `V2` `V4`
siteAffiliation	UUID	The value of `id`, a UUID representing the storage component or the user.
useProxy	Boolean	If `true`, a proxy server is defined. If `false`, a proxy server is not defined.
proxyHost	String	The proxy host, if used; otherwise, `null`.
proxyPort	32-bit integer	The proxy port number, if used; otherwise, `null`.
proxyUserName	String	The proxy domain user name, if used; otherwise, `null`.
proxyPassword	String	The proxy domain password, if used; otherwise, `null`).
proxyDomain	String	The proxy domain, if used; otherwise, `null`.
usePathStyleAlways	Boolean	If `true`, use path-style syntax to send requests to the back-end system; if `false`, use virtual-hosted style.

Chapter 2: Storage component management methods

Parameter	Type	Description
connectionTimeout	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer.
socketRecvBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer.
readOnly	Boolean	If `true`, the storage component is marked as read-only. If `false`, the storage component is available for reading and writing data.
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Chapter 2: Storage component management methods

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/update_state
```

JSON request:

```
{
  "id": "8bff981b-5894-43ce-bd41-5a6f558cc241",
  "storageComponentState": "INACTIVE"
}
```

JSON response:

```
[
  {
  "id": "8bff981b-5894-43ce-bd41-5a6f558cc241",
  "storageType": "GENERIC_S3",
  "storageComponentConfig": {
    "label": null,
    "host": "172.19.54.102",
    "https": false,
    "port": 9000,
    "bucket": "samplebucket",
    "region": "us-west-2",
    "authType": null,
    "siteAffiliation": {
```

```
      "id": "19b96ae2-38ef-4686-b298-b5bebe173e96"
    },
    "useProxy": false,
    "proxyHost": null,
    "proxyPort": null,
    "proxyUserName": null,
    "proxyPassword": null,
    "proxyDomain": null,
    "usePathStyleAlways": true,
    "connectionTimeout": null,
    "socketTimeout": null,
    "connectionTTL": null,
    "maxConnections": null,
    "userAgentPrefix": null,
    "socketSendBufferSizeHint": null,
    "socketRecvBufferSizeHint": null,
    "readOnly": false,
    "state": "INACTIVE"
  }
}
]
```

Test storage component access

You can test whether a storage component is accessible.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/test
```

Request structure

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.

Response structure

The response body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "verified": true|false,
  "httpStatus": nnn,
  "errorCode": "code_text",
  "errorMessage": "error_text",
  "daysUntilCertificateExpiration": nnn,
  "state": "state"
}
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
storageType	String	The type of storage component: ▪ `AMAZON_S3`: An Amazon Web Services S3-compatible node ▪ `HCP_S3`: A Hitachi Content Platform node ▪ `HCPS_S3`: An HCP S Series node ▪ `GENERIC_S3`: An S3-compatible node
verified	Boolean	If `true`, the storage component is activated. If `false`, it has not been verified and is awaiting for an administrative action.
httpStatus	Integer	The HTTP status code the storage component responded with. If `0`, the storage component can't be reached. Otherwise, the code can help explain why it can't be verified.
errorCode	String	Any error codes associated with the storage component; otherwise, null.
errorMessage	String	Any error messages associated with the storage component; otherwise, null.
daysUntilCertificate Expiration	32-bit integer	The number of days left until the current HTTP certificate expires.

Parameter	Type	Description
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component ID.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/test
```

JSON request:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
}
```

JSON response:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageType": "AMAZON_S3",
  "verified": true,
  "httpStatus": 200,
  "errorCode": null,
  "errorMessage": null,
  "daysUntilCertificateExpiration": null,
  "state": "ACTIVE"
}
```

Update storage component configuration

You can update the configuration of a storage component, which overwrites the existing settings. Use the endpoint /storage_component/list to verify existing settings or changes. Use the endpoint PATCH /storage_component/update to update specific settings.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/update
```

Request structure

The request body is:

```
{
  "id": "uuid",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
    "port": [nnnnn],
    "bucket": "bucket_name",
    "region": "[region_name]",
    "authType": "[V2|V4]",
    "siteAffiliation": {
      "id": "uuid"
    },
    "accessKey": "key",
```

```
      "secretKey": "key",
      "useProxy": [true|false],
      "proxyHost": "[host_name]",
      "proxyPort": [nnnnn],
      "proxyUserName": "[user_name]",
      "proxyPassword": "[password]",
      "proxyDomain": "[domain_name]",
      "usePathStyleAlways": [true|false],
      "connectionTimeout": [ms],
      "socketTimeout": [ms],
      "connectionTTL": [ms],
      "maxConnections": [nnnnnnn],
      "userAgentPrefix": "[prefix]",
      "socketSendBufferSizeHint": [nnnnnnn],
      "socketRecvBufferSizeHint": [nnnnnnn],
      "readOnly": {true|false}
   }
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageComponent Config	Yes	List	The following storage component configuration values:
label	No	String	The name of the storage component.
host	Yes	String	The URL of the storage component back-end host domain.
https	Yes	Boolean	If `true`, use an HTTPS connection to the back-end system. If `false`, use an HTTP connection to the back-end system. Default: `false`.
port	No	Integer	The HTTP port of the back-end system.
bucket	Yes	String	The name of the bucket. The bucket must already exist.
region	No	String	The S3 region. Default: `us-west-2`.
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: ▪ `V2` ▪ `V4`

Parameter	Required	Type	Description
siteAffiliation	Yes	UUID	For `id`, the UUID representing the storage component or the user.
accessKey	Yes		The access key of the S3 credentials for access to the bucket.
secretKey	Yes		The secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If `true`, a proxy server is defined. If `false`, a proxy server is not defined. If `true`, then values are required for `proxyHost` and `proxyHost`. Default: `false`.
proxyHost	No	String	The proxy host, if used.
proxyPort	No	Integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. This is not supported.
usePathStyleAlways	No	Boolean	If `true`, use path-style syntax to send requests to the back-end system. If `false`, use virtual-hosted style. Default: `true`.
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	No	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.

Parameter	Required	Type	Description
socketSendBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify `socketRecvBufferSizeHint`.
socketRecvBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify `socketSendBufferSizeHint`.
readOnly	No	Boolean	If `true`, objects can be read and deleted but writes aren't allowed. If `false`, writes are allowed.

Response structure

The response returns the same parameters as the request with one addition. The response body structure is:

```
[
  {
    "id": "",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
      "useProxy": ,
      "proxyHost": "",
      "proxyPort": ,
      "proxyUserName": "",
      "proxyPassword": "",
      "proxyDomain": "",
      "usePathStyleAlways": ,
      "connectionTimeout": ,
      "socketTimeout": ,
      "connectionTTL": ,
      "maxConnections": ,
      "userAgentPrefix": "",
      "socketSendBufferSizeHint": ,
      "socketRecvBufferSizeHint": ,
```

Chapter 2: Storage component management methods

```
      "readOnly": true|false,
      "state": "state"
    }
  }
]
```

Parameter	Type	Description
state	Enum	The state of the storage component, indicating its availability to serve requests: ▪ `ACTIVE`: The storage component is ready for requests. ▪ `INACTIVE`: The storage component is on an administrative pause. ▪ `INACCESSIBLE`: The storage component is not accessible. This can be caused by network, authentication, or certificate errors. ▪ `UNVERIFIED`: The storage component has not been activated or has failed to activate.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/update
```

Chapter 2: Storage component management methods

JSON request:

```json
{
  "storageType": "AMAZON_S3",
  "storageComponentConfig": {
    "label": "Cloud AWS Bucket",
    "host": "172.19.54.102",
    "https": false,
    "port": 9000,
    "bucket": "testbucket",
    "region": "us-west-2",
    "authType": "V2",
    "siteAffiliation": {
      "id": "3fa85f64-1024-4562-bffc-2c963f66afa6"
    },
    "useProxy": false,
    "proxyHost": ,
    "proxyPort": ,
    "proxyUserName": ,
    "proxyPassword": ,
    "proxyDomain": ,
    "usePathStyleAlways": true,
    "connectionTimeout": ,
    "socketTimeout": ,
    "connectionTTL": ,
    "maxConnections": ,
    "userAgentPrefix": ,
    "socketSendBufferSizeHint": ,
    "socketRecvBufferSizeHint": ,
    "readOnly":
  }
}
```

JSON response:

```json
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Cloud AWS Bucket",
      "host": "URL of an existing storage component backend",
      "https": false,
      "port": 0,
      "bucket": "string",
      "region": "string",
      "authType": "V2",
      "siteAffiliation": {
        "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
      },
      "useProxy": true,
```

Chapter 2: Storage component management methods

```
        "proxyHost": "string",
        "proxyPort": 0,
        "proxyUserName": "string",
        "proxyPassword": "string",
        "proxyDomain": "string",
        "usePathStyleAlways": true,
        "connectionTimeout": 0,
        "socketTimeout": 0,
        "connectionTTL": 0,
        "maxConnections": 0,
        "userAgentPrefix": "string",
        "socketSendBufferSizeHint": 0,
        "socketRecvBufferSizeHint": 0,
        "readOnly": false,
        "state": "ACTIVE"
      }
    }
]
```

Chapter 3: Encryption management methods

The management API includes storage component encryption methods.

Get encryption state

You can get the state of encryption for the HCP for cloud scale system.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_encryption/get
```

Request structure

Not applicable.

Response structure

The response body structure is:

```
{
  MAPIS3EncryptionSetting {
    "value": "{true|false}"
    }
  }
```

Parameter	Type	Description
MAPIS3EncryptionSetting	Boolean	`true` if encryption is on, `false` otherwise.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/get
```

JSON response:

```
{
  MAPIS3EncryptionSetting {
    "value": "true"
    }
  }
```

Set encryption state

You can start encryption globally for the HCP for cloud scale system. Starting encryption initializes, configures, and unseals the key management server and returns an initial root token and a set of unseal keys. Once encryption is started, it can't be removed. The best practice is to encrypt and securely store the initial root token and unseal keys separately.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_encryption/set
```

Request structure

Not applicable.

Response structure

The response body structure is:

```
{
  "value": {true|false},
  "rootToken":"root_token,
  "unsealKeys":["unseal_key_1","unseal_key_2","unseal_key_3",
"unseal_key_4","unseal_key_5"]
  }
```

Parameter	Type	Description
value	Boolean	`true` if encryption is on, `false` otherwise.
rootToken	Hex	The initial root token, used to authenticate login to the key management server.
unsealKeys	Hex	A set of unseal keys. A quorum of unseal keys is required to restart the key management server.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
503	Service Unavailable	The key management system has not been set up.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/set
```

Chapter 3: Encryption management methods

JSON response:

```
{
  "value":true,
  "rootToken":"s.FBZngLG9RcyjBzddCxTwoMkk",
  "unsealKeys":[
    "f7a0652cbe07d573a7eeab127ff102454c33adc9402e49622ffa5b5f43cec0794e",
    "4d7e620a694cb607dd1e503027f82880f376edfb1024548d0121572a3dc989c685",
    "6c6081054e26ec55824eb97481acd1f31d660d99e4ba158ca4248e39a8d4de1e16",
    "5dd42c8c60d60469d675dbaad15ff2a78d262cb42e2f9a798aa0b09f368b8caff4",
    "fdc2f29b4359a550916b43071501dab257b73f911960c7fc793f1a279f71091482"]
}
```

Unseal

You can unseal all the instances of the key management server for the HCP for cloud scale system.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_encryption/unseal
```

Request structure

The request body is:

```
{
  "unsealKey1": "string",
  "unsealKey2": "string",
  "unsealKey3": "string"
}
```

Parameter	Required	Type	Description
unsealKey1, unsealKey2, unsealKey3	Yes	String	An unseal key. You must provide three unseal keys in the request.

Response structure

Not applicable.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid unseal key.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/unseal
```

JSON request:

```
{
  "unsealKey1":
"f7a0652cbe07d573a7eeab127ff102454c33adc9402e49622ffa5b5f43cec0794e",
  "unsealKey2":
"4d7e620a694cb607dd1e503027f82880f376edfb1024548d0121572a3dc989c685",
  "unsealKey3":
"6c6081054e26ec55824eb97481acd1f31d660d99e4ba158ca4248e39a8d4de1e16"
}
```

Chapter 4: Administrative management methods

The management API includes administrative management methods.

Add license

You can add a license for your HCP for cloud scale system. You must provide a valid license file for the licensed function to function. The method decrypts, validates, and stores the license file.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/license/add
```

Request structure

The request body is:

```
{
  "value": "license_file"
}
```

Parameter	Required	Type	Description
value	Yes	String	The file path of your HCP for cloud scale license.

Response structure

Not applicable.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials were noit valid.

Status code	HTTP name	Description
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/license/add
```

JSON request:

```
{
  "value": "hcpcs_license.plk"
}
```

Get serial number

You can retrieve the current serial number of your HCP for cloud scale system.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/serial_number/get
```

Request structure

Not applicable.

Response structure

The response body is:

```
{
  "value": "serial_number"
}
```

Parameter	Type	Description
value	String	The serial number of your HCP for cloud scale system.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/serial_number/get
```

JSON response:

```
{
  "value": "SerialNumber48692"
}
```

Get system events

You can retrieve the 100 most recent system events.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/system/info
```

Request structure

Not applicable.

Response structure

The response body is:

```
{
  "events": [
    {
      "severity": "INFO|WARNING|SEVERE",
      "subject": "event_subject",
```

```
        "message": "event_message",
        "subsystem": "event_subsystem",
        "timestamp": date_time
     },
      .
       .
        .
   ]
}
```

Parameter	Type	Description
severity	String	The severity of the event: ▪ INFO ▪ WARNING ▪ SEVERE
subject	String	Summary of the event.
message	String	Details about the event.
subsystem	String	The event category (for example, User, Bucket, or S3 settings).
timestamp	64-bit integer	The date and time, in milliseconds since 1 January 1970 GMT, when the event was generated.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/system/info
```

JSON response:

```
{
  "events": [
    {
      "severity": "INFO",
      "subject": "User admin@company.com authenticated",
      "message": "User admin@company.com with Id d3c01db4-ac18-4d90-a321-
899bb210baf7 authenticated successfully to the Administration App.",
      "subsystem": "User",
      "timestamp": 1559547959735
    },
    {
      "severity": "INFO",
      "subject": "Unexpectedly failed authentication request by user
admin@company.com",
      "message": "An authentication request unexpectedly failed for
username admin@company.com.",
      "subsystem": "User",
      "timestamp": 1559547646844
    }
  ]
}
```

List licenses

You can retrieve information about the current licenses for your HCP for cloud scale
system.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/license/list
```

Request structure

Not applicable.

Response structure

The response body is:

```
{
  "featureName": "feature",
```

Chapter 4: Administrative management methods

```
  "uploadDate": "date_time",
  "expirationDate": "date_time0",
  "valid": {true|false},
  "message": "message"
  }
```

Parameter	Type	Description
featureName	String	Name of the licensed feature.
uploadDate		The date and time, in the format *Ddd Mmm dd hh*:*mm*:*ss TMZ yyyy*, when the license was uploaded.
expirationDate		The date and time, in the format *Ddd Mmm dd hh*:*mm*:*ss TMZ yyyy*, when the license expires.
valid	Boolean	If `true`, the license is valid. If `false`, the license is invalid.
message	String	State of the license: ▪ `License is expired` ▪ `License is valid` ▪ `License not set`

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/license/list
```

JSON response:

```
{
  "featureName": "DARE",
  "uploadDate": "Tue Jun 16 00:00:00 GMT 2020",
  "expirationDate": "Sat Oct 24 10:24:54 GMT 2020",
  "valid": true,
  "message": "License is valid"
  }
```

Refresh client certificates

If your system uses the HTTPS protocol and you change an SSL certificate, you need to update the certificates on storage components.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/certificates/refresh
```

Request structure

Not applicable.

Response structure

Not applicable.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/certificates/refresh
```

Chapter 4: Administrative management methods

Set serial number

You can set the serial number of your HCP for cloud scale system. You must provide a valid serial number for the system to function.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/serial_number/set
```

Request structure

The request body is:

```
{
  "value": "serial_number"
}
```

Parameter	Required	Type	Description
value	Yes	String	The serial number of your HCP for cloud scale system.

Response structure

The response returns the same parameter as the request.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials were noit valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/serial_number/set
```

JSON request:

```json
{
  "value": "SerialNumber48692"
}
```

JSON response:

```json
{
  "value": "SerialNumber48692"
}
```

Chapter 5: User management methods

The management API includes user management methods.

Generate S3 user credentials

You can generate new S3 user credentials for access to the bucket. This endpoint returns a new secretKey-accessKey pair corresponding to the user associated with the OAuth token that was submitted. The creation of a new key pair invalidates any previous key pairs for the user. A user account cannot generate S3 credentials associated with a different user account.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3/user/generate_credentials
```

Request structure

Not applicable.

Response structure

The response body is:

```
{
  "id": {
    "id": "uuid"
  },
  "secretKey": "key",
  "accessKey": "key"
}
```

Parameter	Type	Description
id	UUID	The ID of the user.
secretKey	String	The secret key of the S3 credentials to access the bucket.
accessKey	String	The access key of the S3 credentials to access the bucket.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3/user/generate_credentials
```

JSON response:

```
{
  "id": {
    "id": "edded8d-99f1-43f4-88fa-0cd9032ef7bd"
  },
  "secretKey": "bff...",
  "accessKey": "TSPl8Pop..."
}
```

List users

You can retrieve a list of all users of the HCP for cloud scale system by user ID, display name, and realm. You can also filter the list to retrieve a subset.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/list
```

Request structure

The request body is:

```
{
  "count": [nnnn],
  "startingFrom": ["uuid"],
  "nameFilter": ["match_string"]
}
```

Chapter 5: User management methods

Parameter	Required	Type	Description
count	No	Integer	The number of users to return. Up to 1000 users; default: 1000.
startingFrom	No	UUID	The UUID to start from. Leave blank to start from the beginning of the list.
nameFilter	No	String	A string used to filter the list to return only names that start with this string.

Response structure

The response body structure is:

```
[
  {
    "displayName": "",
    "id": "",
    "realmId": ""
  }
  .
  .
  .
]
```

Parameter	Type	Description
displayName	String	The display name of the user.
id	UUID	The ID of the user.
realmId	String	The realm of the user.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.

Chapter 5: User management methods

Status code	HTTP name	Description
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/list
```

JSON request:

```
{
  "count": 1,
  "startingFrom": "3fa85f64-0810-1954-b3fc-2c963f66afa6",
  "nameFilter": ""
}
```

JSON response:

```
[
  {
    "displayName": "Zhang.Guo-Ming@company.com",
    "id": "3fa85f64-0810-1954-b3fc-2c963f66afa6"
    "realmId": "2d64d267-a23b-54c8-9be5-a3832faad4b2"
  }
]
```

List user buckets

You can retrieve a list of buckets owned by users of the HCP for cloud scale system by user ID and bucket name. You can also filter the list to retrieve a subset.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/list_buckets
```

Request structure

The request body is:

```
{
  "id": "uuid",
  "count": [nnnn],
```

```
    "startingAfter": ["string"]
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the user.
count	No	Integer	The number of buckets to return. Up to 1000 buckets; default: 1000.
startingAfter	No	String	The bucket name to start after alphabetically. Leave blank to start from the beginning of the list. Use this parameter to retrieve bucket lists in groups.

Response structure

> **Note:** If the user ID provided does not exist, the response is an empty list.

The response body structure is:

```
[
  {
    "bucketId": "",
    "bucketName": ""
  },
  .
  .
  .
]
```

Parameter	Type	Description
bucketId	UUID	The UUID of the bucket.
bucketName	String	The display name of the bucket.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.

Chapter 5: User management methods

Status code	HTTP name	Description
400	Bad Request	The request is missing a valid parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/list_buckets
```

JSON request:

```
{
  "id": "3fa85f64-0810-1954-b3fc-2c963f66afa6",
  "count": 1,
  "startingAfter": "September"
}
```

JSON response:

```
[
  {
    "bucketId: "9b805cee-56aa-42a7-b89e-9087d6ade984",
    "bucketName": "October"
  }
]
```

Revoke OAuth user tokens

You can revoke OAuth tokens belonging to a specific user. You can use the endpoint /user/list to look up the ID of the user whose tokens you want to revoke.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/revoke_tokens
```

Request structure

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the user whose OAuth credentials you are revoking.

Response structure

Not applicable.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	User ID not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The user ID was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/revoke_tokens
```

JSON request:

```
{
    "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
  }
```

Revoke S3 user credentials

You can revoke all S3 credentials belonging to a specific user. Users can revoke their own S3 credentials. Users with appropriate permissions can revoke other users' S3 credentials. You can use the endpoint `/user/list` to look up the ID of the user whose credentials you want to revoke.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/revoke_credentials
```

Request structure

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the user whose S3 credentials you are revoking.

Response structure

The response body is:

```
{
  "id": {
    "id": "uuid"
  },
  "secretKey": "key",
  "accessKey": "key"
}
```

Parameter	Type	Description
id	UUID	The ID of the user.
secretKey	String	The secret key of the S3 credentials.
accessKey	String	The access key of the S3 credentials.

Chapter 5: User management methods

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	User ID is not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The user ID was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/revoke_credentials
```

JSON request:

```
{
    "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
  }
```

JSON response:

```
{
  "id": {
    "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
  },
  "secretKey": "bff...",
  "accessKey": "TSPl8Pop..."
}
```

Chapter 6: Public methods

The management API includes public methods.

Get service port

You can retrieve the external port used by an HCP for cloud scale service. You don't need an OAuth token to use this method.

HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/public/discovery/get_service_port
```

Request structure

The request body is:

```
{
   "portType": "type"
}
```

Parameter	Required	Type	Description
portType	Yes	String	The type of service: ▪ ADMIN_APP: System Management application. ▪ JAEGER_QUERY: Tracing service. ▪ MAPI: Management API. ▪ PROMETHEUS: Metrics service.

Response structure

The response body is:

```
{
   "portType": "type",
   "portNumber": nnnnn
}
```

Parameter	Type	Description
portNumber	Integer	The HTTP port of service.

Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for public data. Resend using POST.

Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/discovery/get_service_port
```

JSON request:

```
{
  "portType": "ADMIN_APP"
}
```

JSON response:

```
{
  "portType": "ADMIN_APP",
  "portNumber": 8000
}
```

Hitachi Vantara