Swift API

This chapter describes the subset of the OpenStack Swift API that is implemented for COS. The Swift API uses the Storage FQDN that is assigned to the COS cluster.

Note The COS cluster is assigned an Authentication FQDN (used with the Swauth API) and a Storage FQDN (used with the Swift API). Currently the Authentication FQDN and the Storage FQDN must be the same, for example, auth01.cos.acme.com.

Listing Containers

To retrieve a list of existing storage containers, use the following HTTP GET request:

Note To make this request, you must be an account admin or a reseller admin.

GET /v1/<account>[?<param>=<value>[&<param>=<value>]] HTTP/1.1

The names of the containers in the list are sorted based on a binary comparison of the UTF-8 encoded container names.

Required Request Header

X-Auth-Token: <user token>

Optional Query Parameters

The following parameters can be used in the query:

- limit — Specifies the maximum number of results to be retrieved.
- marker — Retrieves container names whose characters have a greater Unicode alphabetical value than those of the specified string.
- end_marker — Retrieves container names whose characters have a lower Unicode alphabetical value than those of the specified string.
- prefix — Retrieves container names beginning with the specified characters.

• delimiter — Retrieves container names that do not have the specified character, except in the prefix, if any.

• format — Specifies either json or xml as the format of the serialized response.

Listing Objects

To list the objects in the storage container, use the following HTTP GET request:

✎ **Note** To make this request, you must be an account administrator or COS reseller-administrator. Or, if a read-ACL has been specified for a container, either you must have been assigned a role listed in the ACL, or '*' must be listed as a role, permitting anonymous access.

GET /v1/<account>/<container>[?<param>=<value>[&<parm>=<value>]] HTTP/1.1

The names of the objects in the list are sorted based on a binary comparison of the UTF-8 encoded object names.

Optional Query Parameters

The following parameters can be used in the query:

• limit — Specifies the maximum number of results to be retrieved.

• marker — Retrieves object names whose characters have a greater Unicode alphabetical value than those of the specified string.

• end_marker — Retrieves object names whose characters have a lower Unicode alphabetical value than those of the specified string.

• prefix — Retrieves object names beginning with the specified characters.

• delimiter — Retrieves object names that do not have the specified character, except in the prefix, if any.

• path — Retrieves names of objects nested in the specified path.

• format — Specifies either json or xml as the format of the serialized response.

✎ **Note** If a response format is not specified as a query parameter, a list of object names is returned in the response body, one name per line.

Response Status Codes

The response status code is one of the following:

- 2xx — indicates a successful execution of the request.
- 204 (No Content) — indicates that either the container is empty, or none of the objects in the container match the query parameters specified in the request.

Creating a Container

To create a storage container, use the following HTTP PUT request:

Note To make this request, you must be an account admin, a COS reseller admin or the super admin.

PUT /v1/<account>/<container> HTTP/1.1

The name of the container must adhere to the following restrictions:

- The name cannot include the forward slash (/) character or the encoded forward slash character (%2F or %2f).
- The name should not exceed 256 bytes when it is encoded in URL.

Required Request Header

- X-Auth-Token: <user token>

Optional Request Headers

- X-Container-Read: <read acl>
- X-Container-Write: <write acl>

Assigning Custom Attributes

To assign custom attributes to a storage container, include additional HTTP headers in the HTTP PUT request shown above. The additional headers should be of the following form:

X-Container-Meta-<attribute name>: <attribute value>

Response Status Codes

The response status code is one of the following:

- 201 (Created) — The container was created.
- 202 (Accepted) — The container already exists.
- 400 (Bad Request) — Invalid container name.
- 401 (Unauthorized) — The user token is missing or invalid.
- 403 (Forbidden) — The user does not have permission to create the container.
- 404 (Not Found) — The storage URL references a non-existent account.

Deleting a Container

To permanently remove a storage container, use the following HTTP DELETE request:

Note   To make this request, you must be an account admin, a reseller admin, or the super admin.

DELETE /v1/<account>/<container> HTTP/1.

Note   Only empty storage containers can be deleted.

Required Request Header

X-Auth-Token: <user token>

Response Status Codes

The response status code is one of the following:

- 204 (No Content) — The container was deleted.
- 400 (Bad Request) — Invalid container name.
- 401 (Unauthorized) — The user token is missing or invalid.
- 403 (Forbidden) — The user does not have permission to delete the container.
- 404 (Not Found) — The storage URL references a non-existent account.
- 409 (Conflict) — The container is not empty.

Retrieving an Object

To retrieve the data of an object, use the following HTTP GET request:

Note   To make this request, you must be an account admin or COS reseller-admin; or if a read-ACL has been specified for the container, either you are assigned a role listed in the ACL, or ***** is specified as a role, permitting anonymous access.

GET /v1/<account>/<container>/<object> HTTP/1.1

Note   You may retrieve data from an object while it is being created. If you do, the response will have the X-Object-Is-Dynamic: yes header.

Required Request Header

X-Auth-Token: <user token>

Note   If the container read-ACL permits anonymous access, this header is not required.

Optional Request Headers

- X-Follow-Redirect: true

    – If the request has this header, the COS node may respond with a 307 (Temporary Redirect) code and include a Location response header having the URL at which the client should retry the request.

    – If the request does not have this header, or the value of the header is not true, the COS node receiving the request will respond with the requested object.

    Note   The X-Follow-Redirect request header is a COS extension.

- X-Transfer-Rate: <bits-per-second>

    – This header specifies a transfer rate in decimal bits per second.

    – Valid range of values for this header is 400000 to 50000000, that is, 400 Kbps to 50 Mbps.

    – If the header is not included, data is transferred at the best-effort rate that does not delay other transfers which were requested along with an X-Transfer-Rate header.

    – A transfer rate of 0 is valid and indicates a best-effort transfer of data.

    Note   The X-Transfer-Rate request header is a COS extension.

- X-Transfer-Delay: <delta-time-in-milliseconds>

    – This header specifies a signed delay in milliseconds.

    – If the delay is positive, COS waits for the time interval specified before starting the transfer of object data at the requested transfer rate. The positive delay can have a maximum value of 30 seconds.

    – A negative delay indicates that the client wants to use an elasticity buffer and intends to transmit data from the partially full buffer that receives data from COS at the requested transfer rate. In this case, COS starts transferring the data as soon as the retrieve request is received, and attempts to send data at a rate higher than the requested rate. COS, in essence, tries to match the amount of data that would have been sent to the client if the data transfer had been initiated "delay" seconds before the receipt of the request. The negative delay can have maximum magnitude of four seconds.

    Note   The X-Transfer-Delay request header is a COS extension.

- Range: bytes = <byte-range>

    – To request the transfer of specific portions of the object data, in accordance with the specifications in section 14.35 of RFC 2616, include this header.

    – Only byte-ranges are supported.

    – Multiple byte ranges are supported.

- If the range did not include the entire object, a response status code of 206 (Partial Content) is returned by COS.

- The Partial Content response to a request for multiple non-overlapping ranges of data contains multiple parts in the message body.

- If-Match: ETag

- The object data is retrieved only if the client specified ETag value matches the ETag of the content. Else, 412 (Precondition Failed) is returned.

- If-None-Match: ETag

- 304 (Not Modified) is returned if the client specified ETag value matches the ETag of the content, indicating to the client that the object cached by it has not been modified since.

- If-Modified-Since: time

- 304 (Not Modified) is returned if the client specified time is equal to or later than the last modified time of the object.

- If-Unmodified-Since: time

- The object data is retrieved only if the client specified time is equal to or later than the last modified time of the object. Else, 412 (Precondition Failed) is returned.

Response Status Codes

A response status code of **2xx** indicates successful completion of the request.

Response Headers

The response will include one of the following headers:

- Last Modified — A time-stamp of when the object was created or modified.

- ETag — The hexadecimal representation of the MD5 hash of the object data.

- Content-Type — The content type associated with the object when it was created.

- Content-Length — The number of bytes in the object.

- X-Object-Goid — The global object identifier assigned by COS when the object was created.

Note   The X-Object-Goid response header is a COS extension.

- X-Object-Meta-* — Custom object attributes of the object.

- X-Object-Is-Dynamic: yes — The object being retrieved is being extended. This occurs when you retrieve object data while object creation is in progress. Such a retrieval of the data is useful when a large object is being created and you want to access the data that has been stored, even as more data is being appended to the object. This response header is a COS extension.

Note   The X-Object-Is-Dynamic response header is a COS extension.

Creating or Updating An Object

To create or update an object, that is, to write or overwrite an object's content and metadata, use the following HTTP PUT request:

PUT /v1/<account>/<container>/<object> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>

Note   This header may be excluded if the container write ACL permits anonymous access.

- Content-Type
    - If this header is not included, the system will attempt to guess the type of the content based on the object's name/metadata. If the system is unsuccessful, the Content-Type is set to the default application/octet-stream value.
- Content-Length/ Transfer-Encoding: chunked
    - Either a valid Content-Length header, stating the size of the object, or a Transfer-Encoding: chunked header, indicating that the data length is encoded in-line at the start of each chunk of the object data sent in the request, must be included.

Optional Request Headers

- ETag
    - The request may include this header with the value set to the hexadecimal representation of the MD5 hash of the object data.
    - If the ETag value does not match MD5 hash computed by COS, a 422 (Unprocessable Entity) response status code is returned.
- X-Object-Meta-<attribute name>: <attribute value>
    - Include this header to set custom attributes for an object.
- X-Follow-Redirect: true
    - If this header is included, the COS node may respond with a status code of 307 (Temporary Redirect) and include a Location response header indicating the URL to which the client should address the request.
    - If this header is absent, or the value of the header is not true, the COS node receiving the request will perform the necessary operation.

Note   The X-Follow-Redirect request header is a COS extension.

- Expect: 100-Continue
    - It is recommended that you include this header in the initial request and omit object content from the body of the request.

- The receiving COS node will respond with either a 100 (Continue) status code, a 307 (Temporary Redirect) status code, or an error status code.
- If the 100 (Continue) status code is received, repeat the request along with the object content in the body.

Response Status Codes

The response will include one of the following headers:

- 2xx — Indicates the successful completion of the HTTP PUT request.
- 5xx — Indicates failure of the HTTP PUT request.

Response Headers

The response will include one of the following headers:

- Last Modified — A time-stamp of when the object was created or updated.
- ETag — A hexadecimal representation of the MD5 hash of the object data.

Deleting an Object

To permanently remove an object, use the following HTTP DELETE request:

Note To make this request, one of the following must be true:

- You are an account admin or a COS reseller admin.
- If a write-ACL has been specified for the container, either you are assigned a role listed in the ACL, or the role * is included in the ACL, permitting anonymous access.

DELETE /v1/<account>/<container>/<object> HTTP/1.1

Deleting an object removes both the object data and metadata. Any subsequent operations attempted on the object will return a 404 (Not Found) response status code.

Required Request Header

✎
Note   If the container write-ACL permits anonymous access, this header is not required.

X-Auth-Token: <user token>

Response Status Code

204 (No Content) — Indicates the object has been deleted.

Creating or Updating Container Metadata

To create or update custom container attributes, use the following HTTP POST request:

✎
Note   To make this request, you must be an account admin or a COS reseller admin.

POST /v1/<account>/<container> HTTP/1.1

The attributes are specified in HTTP headers included in the HTTP POST request. If the attribute exists, its value will be overwritten. Else, a new attribute is created.

Required Request Header

- X-Auth-Token: <user token>
- X-Container-Meta-<attribute name>: <attribute value>

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST request is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5xx — Internal Server Error

Retrieving Container Metadata

To retrieve a container's metadata to learn its status, use the following HTTP HEAD request:

Note   • To make this request, you must be an account admin or a COS reseller admin.

   • Or, if a read-ACL has been specified for the container, you must be assigned a role listed in the ACL.

   • Or, the '*' role must be included in the ACL, permitting anonymous access.

HEAD /v1/<account>/<container> HTTP/1.1

This request can be used against a container to determine the number of objects, and the total byte size of all objects stored in the container.

Required Request Header

Note   If the container read-ACL permits anonymous access, this header is not required.

X-Auth-Token: <user token>

Response Status Code

The response status code is one of the following:

   • 2xx (Success) — The HEAD operation succeeded
   • 400 (Bad Request) — The POST request is not valid
   • 401 (Unauthorized) — The user token is missing or invalid
   • 403 (Forbidden) — The user does not have permission to modify the container attributes
   • 404 (Not Found) — The storage URL references a non-existent account or container
   • 5xx — Internal Server Error

Response Headers

   • X-Container-Object-Count

      – The value of this header is the number of objects in the container.

   • X-Container-Bytes-Used

      – The value of this header is the total byte size of all the objects in the container.

   • X-Container-Meta-<attribute name>: <attribute value>

      – This header returns the custom attributes of the container.

Deleting Container Metadata

To delete custom container attributes, use the following HTTP POST request:

Note   To make this request, you must be an account admin or a reseller admin.

POST /v1/<account>/<container> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>
- X-Container-Meta-<attribute name>
  - An empty header of this type without the attribute value can be used to delete the custom attribute named in the header.
- X-Remove-Container-Meta-<attribute name>: <arbitrary value>
  - Alternatively, a header of this type can be used to delete the custom attribute named in the header.
  - The arbitrary attribute value is ignored by the system.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST request is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5XX — Internal Server Error

Creating or Updating Object Metadata

To create or update custom object attributes, use the following HTTP POST request:

Note
- To make this request, you must be an account admin or a COS reseller admin.
- Or, if a write-ACL has been specified for the container, you must be assigned a role listed in the ACL.
- Or, the '*' role must be included in the ACL, permitting anonymous access.

POST /v1/<account>/<container>/<object> HTTP/1.1

Assigning custom attributes to objects enables you to better categorize the objects.

Required Request Header

- X-Auth-Token: <user token>

✎

Note   If the container write-ACL permits anonymous access, this header is not required.

- X-Object-Meta-<attribute name>: <attribute value>
    - If the attribute exists, its value is updated to that specified in the header. Else, the attribute is created.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST request is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5XX — Internal Server Error

Retrieving Object Metadata

To retrieve an object's metadata, including its custom attributes, use the following HTTP HEAD request:

✎

Note
- To make this request, you must be an account admin or a COS reseller admin.
- Or, if a read-ACL has been specified for the container, you must be assigned a role listed in the ACL, and the Referrer header in the request must match the ACL referrer pattern.
- Or, the '*' role must be included in the ACL, permitting anonymous access.

HEAD /v1/<account>/<container>/<object> HTTP/1.

Required Request Header

✎

Note   If the container read-ACL permits anonymous access, this header is not required.

X-Auth-Token: <user token>

Response Status Code

The response status code is one of the following:

- 2xx (Success) — The HEAD operation succeeded

- 400 (Bad Request) — The HEAD operation is not valid

- 401 (Unauthorized) — The user token is missing or invalid

- 403 (Forbidden) — The user does not have permission to modify the container attributes

- 404 (Not Found) — The storage URL references a non-existent account or container

- 5xx — Internal Server Error

Response Headers

- Last Modified — a time-stamp of when the object was created or modified.

- ETag — the hexadecimal representation of the MD5 hash of the object data.

- Content-Type — the content type associated with the object when it was created.

- Content-Length — the number of bytes in the object.

- X-Object-Meta-<attribute-name>: <attribute-value> — custom object attributes, if any.

Deleting Object Metadata

To delete custom object attributes, use the following HTTP POST request:

✎
Note
- To make this request, you must be an account admin or a COS reseller admin.

- Or, if a write-ACL has been specified for the container, you must be assigned a role listed in the ACL.

- Or, the '*' role must be included in the ACL, permitting anonymous access.

POST /v1/<account> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>

- X-Object-Meta-<attribute name>:

  - An empty header of this type without the attribute value can be used to delete the custom attribute named in the header.

- X-Remove-Object-Meta-<attribute name>: <arbitrary value>

  - Alternatively, a header of this type can be used to delete the custom attribute named in the header.

  - The arbitrary value is ignored by the system.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded

- 400 (Bad Request) — The POST operation is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5xx — Internal Server Error

Creating or Updating Account Metadata

To create or update custom account attributes, use the following HTTP POST request:

Note To perform this operation, you must be an account administrator or a COS reseller admin.

POST /v1/<account> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>
- X-Account-Meta-<attribute name>: <attribute value>
    - If the attribute exists, its value is updated to that specified in the header. Else, the attribute is created.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST operation is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account
- 5xx — Internal Server Error

Retrieving Account Metadata

To retrieve account metadata to check the account statistics, use the following HTTP HEAD request:

Note To perform the operation, you must be an account administrator or a COS reseller admin.

HEAD /v1/<account> HTTP/1.1

Required Request Headers

X-Auth-Token: <user token>

Response Status Codes

The response status code is one of the following:

- 2xx (Success) — The HEAD operation succeeded
- 400 (Bad Request) — The HEAD operation is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account
- 5xx — Internal Server Error

Response Headers

- X-Account-Container-Count: <value>
  - The value of the header is the number of containers in the account.
- X-Account-Object-Count: <value>
  - The value of the header is the number of objects in the account.
- X-Account-Bytes-Used: <value>
  - The value of the header is the total number of bytes in COS for the specified account.
- X-Account-Meta-<attribute name>: <attribute value>
  - The header returns custom account attributes and their values.

Deleting Account Metadata

To delete custom account attributes, use the following HTTP POST request:

Note   To perform the operation, you must be an account administrator or a COS reseller admin.

POST /v1/<account> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>
- X-Account-Meta-<attribute name>:
  - An empty header of this type without the attribute value can be used to delete the custom attribute named in the header.
- X-Remove-Account-Meta-<attribute name>: <arbitrary value>
  - Alternatively, a header of this type can be used to delete the custom attribute named in the header.

– The arbitrary value is ignored by the system.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST operation is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account
- 5xx — Internal Server Error

Access Control Lists (ACLs)

By default, to access a storage object, a requester must be an account administrator of the account containing the object. An administrator can modify the access policy for a container and its storage objects by using container access control lists (ACLs). The administrator can specify the read and write access control lists as part of the container metadata. When an ACL is deleted, the default access policy is restored.

An ACL has the following form:

[item [, item...]]

An ACL item can be one of the following:

- <account name>

  – All the users of specified account are granted access to objects in the container.

- <account name>: <user name>

  – Users identified by the combination of the specified account and user names are granted access to objects in the container.

- *

  – An asterisk permits anonymous access. This option is a COS extension.

Creating or Updating ACLs

To create or update an ACL, use the following HTTP POST request:

Note   To perform the operation, you must be an account administrator or a COS reseller admin.

POST /v1/<account>/<container> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>
- X-Container-Read: <read acl>
    - Specify the read ACL as the value of this header.
- X-Container-Write: <write acl>
    - Specify the write ACL as the value of this header.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST request is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5xx — Internal Server Error

Deleting ACLs

To delete an ACL, use the following HTTP POST request:

> **Note**   To perform the operation, you must be an account administrator or a COS reseller admin.

POST /v1/<account>/<container> HTTP/1.1

Required Request Headers

- X-Auth-Token: <user token>
- X-Container-Read: <read acl>
    - Specify an empty list as the value of this header to delete the read ACL.
- X-Remove-Container-Read: <arbitrary value>
    - Alternatively, a header of this type can be used to delete the read ACL.
    - The arbitrary value is ignored by the system.
- X-Container-Write: <write acl>
    - Specify an empty list as the value of this header to delete the write ACL.
- X-Remove-Container-Write: <arbitrary value>
    - Alternatively, a header of this type can be used to delete the write ACL.
    - The arbitrary value is ignored by the system.

Response Status Code

The response status code is one of the following:

- 204 (No Content) — The POST operation succeeded
- 400 (Bad Request) — The POST request is not valid
- 401 (Unauthorized) — The user token is missing or invalid
- 403 (Forbidden) — The user does not have permission to modify the container attributes
- 404 (Not Found) — The storage URL references a non-existent account or container
- 5xx — Internal Server Error