IBM Cloud Object Storage System
Version 3.14.3

Container Mode Service API Guide – Bucket Management

This edition applies to IBM Cloud Object Storage System and is valid until replaced by new editions.

Contents

Chapter 1. Overview

The IBM Cloud Object Storage *Container Mode Service API Guide – Bucket Management*describes a resource configuration Service API at the bucket-level intended for deployment, system management, and service-operator usage. These interfaces extend the Service API as defined in IBM Cloud Object Storage *Container Mode Storage Account Management API Developer Guide*. IBM Cloud Object Storage System™.

Chapter 2. Roles and permissions

The Container Mode Service API Guide is intended to be used by development operations, system management, and service operators.

The service API is intended to be used by the authenticated user assigned a “Service User” role. The Service User role grants permission to use the service API to perform storage account management. This user will authenticate using existing methods supported on the IBM Cloud Object Storage System. For more details, refer to the *IBM Cloud Object Storage System Manager Administration Guide*.

Chapter 3. Service capabilities

.

In Container Mode, the IBM Cloud Object Storage System allows the capability for a service provider to provision or configure a bucket and perform access control on the bucket, on behalf of a client, using the Service API. The Service API supports bucket-level provisioning and configuration capability on quotas, IP access control, and authorization in container mode.

In IBM Cloud Object Storage Container Mode, bucket-level resource configuration service API support below service operations through a service port inside a firewall. These operations are not restricted by IP access control.

- Create a bucket
- Delete a bucket
- Retrieve bucket metadata
- Update bucket metadata such as IP access control, quota, and ACL

Bucket level resource service API command summary

Following section defines available bucket level commands.

The following table provides a listing of the available commands covered in this specification.

Table 1. Command Summary

Interface	Method	Command	Description
Bucket creation	PUT	<accesser>:8338/container/{bucket.name}	Create a bucket
Update bucket metadata	PATCH	<accesser>:8338/container/{bucket.name}	Update bucket mutable metadata field.
Retrieve bucket metadata	GET	<accesser>:8338/container/{bucket.name}	Retrieve bucket metadata information
Delete bucket	DELETE	<accesser>:8338/container/{bucket.name}	Permanently delete an empty bucket

Chapter 4. Interface details

Common request headers

Request headers that are commonly used.

The following are request headers that are commonly used for all messages.

Table 2. Common request headers

Request Parameter	Style	Type	Description
X-Trans-Id-Extra (Optional)	header	String	Extra transaction information. Use the **X-Trans-Id-Extra** request header to include extra information to help you debug any errors that might occur with large object upload and other COS transactions. COS appends the first 32 characters of the **X-Trans-Id-Extra** request header value to the transaction ID value in the generated **X-Trans-Id** response header. You must UTF-8-encode and then URL-encode the extra transaction information before you include it in the **X-Trans-Id-Extra** request header. You can also use **X-Trans-Id-Extra** strings to help operators debug requests that fail to receive responses. The operator can search for the extra information in the logs.

Common response headers

Response headers that are commonly used.

The following are response headers that are commonly used for all messages or for specific logical groupings of messages.

Table 3. Common response headers

Response Parameter	Style	Type	Description
X-Trans-Id-Extra (Optional)	header/body	String	This value is the length of the error text in the response body.
Content-Type	header/body	String	If the operation fails, this value is the MIME type of the error text in the response body.
X-Trans-Id	header/body	String	A unique transaction ID for this request. Your service provider might need this value if you report a problem.
Date	header/body	DateTime	The transaction date and time. The date and time stamp format is ISO 8601: `CCYY-MM-DDThh:mm:ss-hh:mm`. For example, `2015-08-27T09:49:58-05:00`. The `-hh:mm` value, if included, is the time zone as an offset from UTC. In the previous example, the offset value is `-05:00`. A null value indicates that the token never expires.

Error code

High-level listing of all of the available commands that are covered in this specification.

Table 4. Error Code

Error Code	Description	HTTP Error Code
TemporaryRedirect	You are being redirected to the bucket while DNS updates.	**307 Moved Temporarily**
BadRequest	Bad Request	**400 Bad Request**
InvalidBucketName	The specified bucket name is not valid.	**400 Bad Request**
InvalidLocationConstraint	The specified storage location is not valid.	**400 Bad Request**
MalformedACLError	The JSON you provided for ACL was not well-formed or did not validate against our published schema.	**400 Bad Request**
MalformedFirewallError	The JSON you provided for Firewall was not well-formed or was not valid against our published schema such as invalid IP v4 or IP v6 CIDRA notation, more than 1000 allowed_ip or more than 1000 denied_ip CIDR notation specified in the request, or neither allowed_ip nor denied_ip is specified in the firewall configuration request.	**400 Bad Request**
MalformedQuota	The hard quota is not a valid BigInteger.	**400 Bad Request**
BadRequest	Your metadata headers exceed the maximum allowed metadata size.	400 Bad Request
TooManyBuckets	You have attempted to create more buckets than allowed.	400 Bad Request
Unauthorized	Unauthorized	401 Unauthorized
Forbidden	You have attempted to create more buckets than allowed.	403 Forbidden
NoSuchUser	There is no such user that exists	404 Not Found
StorageAccountDoesNotExist	The storage account does not exist	404 Not Found
NoSuchBucket	The specified bucket does not exist.	404 Not Found
MethodNotAllowed	Method not allowed	405 Method Not Allowed
MalformedQuota		
Conflict	Conflict	409 Conflict
BucketNotEmpty	The bucket you tried to delete is not empty.	409 Conflict
OperationAborted	A conflicting conditional operation is currently in progress against this resource. Try again. This applies to when simultaneous patch firewall requests are processed on the same bucket where some requests specified If-Unmodified-Since yet others do not.	409 Conflict

Table 4. Error Code (continued)

Error Code	Description	HTTP Error Code
Gone	The bucket is already deleted.	410 Gone
PreconditionFailed	At least one of the preconditions you specified did not hold.	412 Precondition Failed
InternalError	Internal Server Error	500 Internal Server Error
NotImplemented	Operation is not implemented	501 Not Implemented
ServiceUnavailable	Service unavailable	503 Service Unavailable

Bucket creation

This sections describes bucket creation.

Base Command :

```
Put <accesser>:8338/container/{bucket.name}
```

A PUT issued to the container followed by a string that specifies the name of the bucket to be created. Bucket names must be unique. Bucket names must be DNS-compliant, i.e., 3 - 63 characters long and must be made of lower case letters, numbers, and dashes. Bucket names must begin and end with a lower case letter or number. Bucket names that resemble IP addresses are not allowed. This operation does not use operation-specific headers or query parameters.

Request

Table 5. Request Parameters

Request Parameter	Style	Required	Type	Description
storage_location	Body	Optional	String	Corresponding to the provisioning code of a container vault; it is also referred as the location of the container in the Cloud mode; when it is not provided, the default provisioning code from container vault template would be used. When this parameter is not provided in either, the request will be rejected with 400 HTTP error.
service_instance	Body	Required	String	The service instance or storage account id that owns the bucket.
acl	Body	Optional	Object	A JSON map of grantee and permission on the bucket. **Refer to table below called "acl JSON (request)"**
hard_quota	Body	Optional	String	Container hard quota in bytes, default 0 (no limit). Format BigInteger.

Table 5. Request Parameters (continued)

Request Parameter	Style	Required	Type	Description
firewall	Body	Optional	Object	The firewall restriction, includes allowed or denied IP addresses lists. When the field is not specified in the request, it defaults to empty, i.e. no IP restriction at the bucket-level. In such a case, IP access control configured at the container vault level is applied to the bucket. If no IP access control specified for the container vault, then the bucket can be accessed from public IP. **Refer to table below called "Firewall (request)"**

Table 6. acl JSON (request)

Parameter	Type	Description
grantee	string	The Storage account ID or service instance granted to the permissions
permission	string	The access permission for the grantee in format of enum of “READ”, “WRITE”, and “FULL-CONTROL”.

Table 7. Firewall (request)

Parameter	Type	Description	Format
allowed_ip	string	Array of string of allowed continuous non-overlapping IP address ranges for the container. If a request from a client IP that is not in this IP address list, the client request is rejected. When this parameter is not provided, the bucket is allowed to be accessed from IP address other than those in denied_ip list. If neither is provided, bucket is allowed to be accessed from any IP address	Array of IP v4 or V6 addresses in CIDR format

Table 7. Firewall (request) (continued)

Parameter	Type	Description	Format
denied_ip	string	Array of string of denied continuous non-overlapping IP address ranges for the container. If a request from a client IP that is in this IP address list, the client request is rejected. Denied IP addresses might be used together with allowed IP as the “excluded sub-range of IP address” from the allowed large IP address range. When this parameter is not provided, the bucket is allowed to be accessed from IP address defined in allowed_ip list.	Array of IP v4 or V6 addresses in CIDR format

Response

Table 8. Response Parameters

Response Parameter	Style	Type	Description
X-Timestamp	Header	String	The date and time in UNIX Epoch time stamp format when the container was initially created for current version
storage_location	Body	String	The provisioning Code of the bucket.
name	Body	String	The name of the bucket
service_instance	body	String	The service instance or storage account id that owns the bucket
acl	Body	Object	A JSON map of grantee and permission on the bucket. See format in GET command. Do not return the object if no content defined. **Refer to table below called "acl JSON (response)"**
retention_policy	Body	String	Bucket retention policy. Return JSON element with container vault “status” with value in format of enum of “ENABLED” | “DISABLED”
cors	Body	Object	The bucket's Cross-Origin Resource Sharing (CORS) configuration. Default value is “null” indicating no CORS configuration. When no content defined, do not show the object. If content is defined, it includes below properties. **Refer to table below called "CORS (response) Parameter"**
hard_quota	Body	String	Container hard quota in bytes. When this is not provided, returns 0 - there is no quota restriction on the bucket. To remove the quota, set the value to 0. Format BigInteger.

Table 8. Response Parameters (continued)

Response Parameter	Style	Type	Description
firewall	Body	Object	Container IP access control restriction information. See format in GET command. If firewall is not specified in container creation request, the field contains null, but service provider should refer to container vault configuration to determine final access control list for the bucket.
time_created	Body	String	The creation time of the bucket in RFC 3339 format. Format “date-time”
time_updated	Body	String	The modification time of the bucket in RFC 3339 format. Format “date-time”

Table 9. acl JSON (response)

Property	Type	Description
permission	string	The list of string of access permission for the grantee in format of enum of "read", "write", and "full-control"
grantee	string	The storage account id or service instance granted the permission.

Table 10. CORS (response) Parameter

Parameter	Type	Description	Format
Origin	String	The list of Origins eligible to receive CORS response headers. Note: "*" is permitted in the list of origins, and means "any Origin"	An array of string type
method	String	The list of HTTP methods on which to include CORS response headers, (GET, OPTIONS, POST, etc) Note: "*" means any method	An array of string type
max_age_seconds	Integer	The value, in seconds, to return in the Access-Control-Max-Age header used in preflight responses.	Int32
allowed_header	String	Headers you want the browser to be allowed to send.	An array of string type
exposed_header	String	Identifies the response headers such as server-side-encryption, request-id etc that customers are able to access from their applications.	An array of string type

Table 11. HTTP response code

HTTP Response Code	Description
201 Created	The bucket was properly created
400 Bad Request	Request the bucket is a vault, invalid hard_quota, invalid storage_location, malformed acl, firewall or JSON, too many buckets, etc.. Detail error message is be provided on specific error.
401 Unauthorized	The provided token is invalid or could not be verified.
403 Forbidden	Access Denied
404 Not Found	The specified account does not exist
409 Conflict	Conflict from the ranges in IP restriction, or a conflict bucket creation is in progress.
500 Internal Server Error	Internal Server Error

Example Output

Create bucket example without mutable parameters

Request

```
PUT <accesser>:8338/container/my-bucket
{
      "storage_location":"us-south",
      "service_instance" : "731fc6f265cd486d900f16e84c5cb594"
}
```

Response

```
HTTP/1.1 201 CREATED
Content-Length: 263
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Fri, 12 Apr 2019 00:56:10 GMT
X-Timestamp: 1555083117.22774

{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"731fc6f265cd486d900f16e84c5cb594",
   "acl":{

   },
   "retention_policy":{
      "status":"DISABLED"
   },
   "cors":null,
   "hard_quota":0,
   "firewall":null,
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-12T00:56:10Z"
}
```

Example Output

Create bucket command with ACL, IP, and quota Request

Request

```
PUT <accesser>:8338/container/my-bucket
{
   "storage_location":"us-south",
   "service_instance":"731fc6f265cd486d900f16e84c5cb594",
   "acl":{
```

```
      "user1":[
         "WRITE"
      ]
   },
   "hard_quota":107374182400,
   "firewall":{
      "allowed_ip":[
         "192.168.28.100/24",
         "192.168.25.200/32"
      ],
      "denied_ip":[
         "192.169.10.100/30"
      ]
   }
}
```

Response

```
HTTP/1.1 201 CREATED
Content-Length: 263
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Fri, 12 Apr 2019 00:56:10 GMT
X-Timestamp: 1555083117.22774
VALID JSON (RFC 4627)
Formatted JSON Data
{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"731fc6f265cd486d900f16e84c5cb594",
   "acl":{
      "user1":[
         "WRITE"
      ]
   },
   "retention_policy":{
      "status":"DISABLED"
   },
   "cors":null,
   "hard_quota":107374182400,
   "firewall":{
      "allowed_ip":[
         "192.168.28.100/24",
         "192.168.25.200/32"
      ],
      "denied_ip":[
         "192.169.10.100/30"
      ]
   },
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-12T00:56:10Z"
}
```

Update Bucket Metadata

This API covers how to update bucket metadata

A PATCH issued to the container metadata followed by a JSON string overwrites the specified mutable container metadata field.

Base Command :

```
PUT <accesser>:8338/container/{bucket.name}
```

Table 12. Common Request Parameters

Request Parameter	Style	Required	Type	Description
If-Unmodified-Since	header	Optional	String	Perform modification on the specified mutable metadata parameter if the container is not modified since the specified time, which user get from the "time_updated" field in metadata response; otherwise reject the change with conflict error, HTTP code 409. This header field is required for allowed_ip and denied_ip to avoid one user accidentally overwriting the change from the other users during concurrent modification. The format is HTTP-date according to RFC7232, https://tools.ietf.org/html/rfc7232#section-3.4. For example, If-Unmodified-Since: Sat, 29 Oct 1994 19:43:31 GMT.
acl	body	Optional	Object	An JSON map of grantee and permission on the bucket **Refer to table below called "acl JSON (patch)"**
hard_quota	body	Optional	String	Container hard quota bytes, default 0, no quota. Format BigInteger.
Firewall	Body	Optional	Object	The firewall restriction, including allowed or denied IP addresses list. When the firewall object is not provided in the body of the PATCH request, no change to the firewall rule. If only allowed IP address or denied IP address is provided, only the corresponding field will be updated, the other field that is omitted in the PATCH request will not be changed. To remove the denied IP or allowed IP address of a bucket, an empty array value must be explicitly provided. For example: allowed_ip: [], denied_ip:[] or both. When both are deleted, then no IP restriction, whether the bucket can be accessed depends on the IP access control at the vault level. If no IP access control specified for the vault, the bucket could be accessed from public IP. Update any parameter will replace its content. If firewall section is specified, either allowed_ip or denied_ip must be provided; otherwise return MalformedFirewallError. **Refer to table below called "Firewall (patch)"**

Table 13. acl JSON (patch)

Parameter	Style	Type	Description
grantee	N/A	String	The entity holding the permission.
permission	N/A	String	The list of string access permission for the entity in format of enum of “READ”, “WRITE”, and “FULL-CONTROL”.

Table 14. Firewall (patch)

Parameter	Type	Description	Format
allowed_ip	string	Array of string of allowed continuous non-overlapping IP address ranges for the container. If a request from a client IP that is not in this IP address list, the client request would be rejected. When this parameter is not provided, the bucket is allowed to be accessed from IP address other than those in denied_ip list. If neither is provided, bucket is allowed to be accessed from any IP address	Array of IP v4 or V6 addresses in CIDR format
denied_ip	string	Array of string of denied continuous non-overlapping IP address ranges for the container. If a request from a client IP that is in this IP address list, the client request would be rejected. Denied IP addresses might be used together with allowed IP as the "excluded sub-range of IP address" from the allowed large IP address range. When this parameter is not provided, the bucket is allowed to be accessed from IP address defined in allowed_ip list.	Array of IP v4 or V6 addresses in CIDR format

Table 15. Response parameter

Response Parameter	Style	Type	Description
Parameter	Body	String	The container name
Bucket parameters	Body	Object	Metadata information for the bucket, see Get command Response

Table 16. HTTP response codes

HTTP Response Code	Description
`200 OK`	The bucket was properly updated
`400 Bad Request`	Request the bucket is invalid, invalid hard quota, malformed acl, firewall or JSON. Detail error message is be provided on specific error etc. Detail error message is be provided on specific error.
`401 Unauthorized`	The provided token is invalid or could not be verified.
`403 Forbidden`	Access Denied
`404 Not Found`	The specified bucket does not exist

Table 16. HTTP response codes (continued)

HTTP Response Code	Description
409 Conflict	Conflict in the patch request such as "If-Unmodified-Since" is evaluated to be true against the given container metadata last "time_updated" field, conflict in the ranges in IP restriction, between allowed_ip and denied_ip, or a conflict bucket creation is in progress.
500 Internal Server Error	Internal Server Error

Request to update quota example

```
Request
PATCH <accesser>:8338/container/my-bucket
{
   "hard_quota": "107374182400"
}


Response
HTTP/1.1 200 OK
Content-Length: 263
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Mon, 15 Apr 2019 08:23:42 GMT
X-Timestamp: 1537818417.22774
{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"0050b1acd467454cbd693b279d72c3d2",
   "acl":{
      "user1":[
         "write"
      ]
   },
   "retention_policy":{
      "status":"DISABLED"
   },
   "cors":{
      "max_age_seconds":"6000",
      "method":"GET",
      "origin":"*.ibm.com"
   },
   "hard_quota":"107374182400",
   "firewall":{
      "allowed_ip":[
         "192.168.10.0/24",
         "192.168.25.200/32"
      ],
      "denied_ip":[
         "192.169.10.100/30"
      ]
   },
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-15T08:23:42Z"
}
```

Update IP Access Control Example

A PATCH issued to the container metadata followed by a JSON string will update a specific mutable container security metadata field.

Below is an example for a request to update IP whitelisting using If-Unmodified-Since to prevent the accidentally overwritten from other user's simultaneous change.

Note that there is a gap of 192.168.10.100 to 192.168.10.103.

- 192.168.10.0 to 192.168.10.99
- 192.168.10.104 .. 192.168.10.255
- 192.168.25.200

```
Request
PATCH <accessor>:8338/container/my-bucket
If-Unmodified-Since: Mon, 15 Apr 2019 08:23:42 GMT
{
   "firewall":{
      "allowed_ip":[
          "192.168.28.100/24",
          "192.168.25.200",
                       "2001:db8::/128",
          "fe80::202:b3ff:fe1e:832"
      ]
   }
}

A response for the entire metadata is returned, including both allowed IP and denied IP, since only the allowed_ip is overw
     allowed_ip:"192.168.10.0/24","192.168.25.200/32", "2001:db8::/128", "fe80::202:b3ff:fe1e:832"
   denied_ip: "192.168.10.100/30

Response
HTTP/1.1 200 OK
Content-Length: 263
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Mon, 15 Apr 2019 08:23:42 GMT
X-Timestamp: 1537818417.22774
{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"0050b1acd467454cbd693b279d72c3d2",
   "acl":{
      "user1":[
          "WRITE"
      ]
   },
   "retention_policy":{
      "minimum_retention":"3650",
      "maximum_retention":"7300",
      "default_retention":"3650",
      "permanent_retention":false
   },
   "cors":{
      "max_age_seconds":6000,
      "method":["GET"],
      "origin":"*.ibm.com",
      "allowed_header":["*"],
      "expose_header":[
         "x-amz-server-side-encryption"
      ]
   },
   "hard_quota":107374182400,
   "firewall":{
      "allowed_ip":[
         "192.168.10.0/24",
         "192.168.25.200/32",
                       "2001:db8::/128",
         "fe80::202:b3ff:fe1e:832"

      ],
```

```
      "denied_ip":[
         "192.169.10.100/30"
      ]
   },
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-15T08:23:42Z"
}
```

Delete IP Access Control Example

Below is an example for a request to delete the IP whitelist, which will not impact existing IP blacklist (denied IP).

Assume that below are configured for the bucket firewall.

- allowed IP: 192.168.28.100/24
- denied IP: 192.168.10.100/30

```
Request
PATCH <accessor>:8338/container/my-bucket
If-Unmodified-Since: Mon, 15 Apr 2019 08:23:42 GMT
{
   "firewall":{
      "allowed_ip":[]
   }
}

A response for the entire metadata is returned, including denied IP, but not the allowed_IP since the allowed_ip is remov
      denied_ip: "192.168.10.100/30"

Response
HTTP/1.1 200 OK
Content-Length: 263
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Mon, 15 Apr 2019 08:23:42 GMT
X-Timestamp: 1537818417.22774
{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"0050b1acd467454cbd693b279d72c3d2",
   "acl":{
      "user1":[
          "WRITE"
      ]
   },
   "retention_policy":{
      "minimum_retention":"3650",
      "maximum_retention":"7300",
      "default_retention":"3650",
      "permanent_retention":false
   },
   "cors":{
      "max_age_seconds":6000,
      "method":["GET"],
      "origin":"*.ibm.com",
      "allowed_header":["*"],
      "expose_header":[
         "x-amz-server-side-encryption"
      ]
   },
   "hard_quota":107374182400,
   "firewall":{
      "denied_ip":[
         "192.169.10.100/30"
      ]
```

```
   },
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-15T08:23:42Z"
}
```

Example Update Bucket ACL

A bucket PATCH request with input of full list of acl object will return the full acl objects in response, and the entire acl list is overwritten.

```
Request
PATCH <accessor>:8338/container/my-bucket
{
   "acl":{
      "user1":[
         "WRITE"
      ],
      "user2":[
         "FULL-CONTROL"
      ]
   }
}
```

Response:
See GET command, all parameters are retrieved.

Retrieve Bucket Metadata

This API covers how to retrieve bucket metadata

Base Command :

```
GET <accesser>:8338/container/{bucket.name}
```

A GET issued to a bucket metadata resource will return the metadata for that bucket.

Request

This operation does not make use of operation specific headers, query parameters, or payload elements

Table 17. Response Parameters

Request Parameter	Style	Type	Description
X-Timestamp	Header	String	The date and time in UNIX Epoch time stamp format when the container was initially created for current version
storage_location	Body	String	Refer to the "provisioning code" in the vault mode, this is typically used as "location" in cloud mode.
name	Body	String	The name of the bucket
service_instance	Body	String	The service instance tor storage account id for the account that owns the bucket
acl	Body	Object	An JSON map of grantee and permission on the bucket 1. Property / Type / Description a. grantee / string / The storage account id or service instance granted to the permission. b. permission / string / The list of access permission for the grantee in format of enum of “READ”, “WRITE”, and “FULL-CONTROL”. \

Table 17. Response Parameters (continued)

Request Parameter	Style	Type	Description
retention_policy	Body	Object	If bucket protection is not set through PUT bucket?protection S3 extension command, return JSON element with container vault "status" with value in format of enum of "ENABLED" | "DISABLED"; otherwise return below JSON elements. (See PATCH command response example.) 1. Parameter / Type / Description / Format a. default_retention / string / The default days / Int64 b. maxium_retention / string / The maxim days / Int64 c. minimum_retention / string / The minimum days / Int64 d. permanent_retention / string / Retain until explicitly cleared / Default: false
cors	Body	Object	The bucket's Cross-Origin Resource Sharing (CORS) configuration. It includes below properties: 1. Parameters / Type / Description / Format a. origin / string / The list of Origins eligible to receive CORS response headers. Note: "*" is permitted in the list of origins, and means "any Origin" / An array of string type b. method / string / The list of HTTP methods on which to include CORS response headers, (GET, OPTIONS, POST, etc.) Note: "*" means any method / An array of string type. c. max_age_seconds / interger / The value, in seconds, to return in the Access-Control-Max-Age header used in preflight responses. / Int32 d. allowed_header / string / Headers you want the browser to be allowed to send. / An array of string type e. expose_header / string / Identifies the response headers such as server-side-encryption, request-id etc. that customers are able to access from their applications / An array of string type
hard_quota	Body	String	Container hard quota in bytes. Quotas apply only to new operations after a quota is exceeded. For example: If bucket quota is 100 GB and usage is 99GB, yet new request 10 GB, then the PUT Object request would be allowed to the bucket, usage after request will be 109 GB. The user will not be able to write more objects until usage brought below 100 GB (user must delete objects). When this field is not specified, there is no quota restriction on the bucket. To remove the quota, set the value to 0. Format BigInteger.

Table 17. Response Parameters (continued)

Request Parameter	Style	Type	Description
firewall	Body	Object	Firewall information including IP access control. If firewall is modified, then either allowed_ip or denied_ip must be provided else return MalformedFirewallError. 1. Parameter / Type /. Description / Format a. allowed_ip / string / Array of string of allowed continuous non-overlapping IP address ranges for the container. If a request from a client IP that is not in this IP address list, the client request would be rejected. When this parameter is not provided, the bucket is allowed to be accessed from IP address other than those in denied_ip list. If neither is provided, bucket is allowed to be accessed from any IP address / Array of IP v4 or IP V6 addresses in CIDR format b. denied_ip / string / Array of string of denied continuous non-overlapping IP address ranges for the container. If a request from a client IP that is in this IP address list, the client request would be rejected. Denied IP addresses might be used together with allowed IP as the "excluded sub-range of IP address" from the allowed large IP address range. When this parameter is not provided, the bucket is allowed to be accessed from IP address defined in allowed_ip list. / Array of IP v4 or IP V6 addresses in CIDR format
time_created	Body	String	The creation time of the bucket in RFC 3339 format. Format "date-time"
time_updated	Body	String	The modification time of the bucket in RFC 3339 format. Format "date-time"

Table 18. HTTP response codes

HTTP Response Code	Description
200 OK	The bucket metadata retrieval was successful
400 Bad Request	The bucket name is invalid.
401 Unauthorized	The provided token is invalid or could not be verified.
403 Forbidden	Access Denied
404 Not Found	The specified bucket does not exist
500 Internal Server Error	Internal Server Error

Example Output

```
Request
GET <accesser>:8338/container/my-bucket

Response
HTTP/1.1 200 OK
Content-Length: 63
Content-Type: application/JSON; charset=utf-8
X-Trans-Id: tx8ea13a3a835544d8bebf1-0056eb522a
Date: Fri, 12 Apr 2019 00:56:10 GMT
X-Timestamp: 1537818417.22774
{
   "storage_location":"us-south",
   "name":"my-bucket",
   "service_instance":"0050b1acd467454cbd693b279d72c3d2",
```

```
   "acl":{
      "user1":[
         "WRITE"
      ],
      "user2":[
         "FULL-CONTROL"
      ]
   },
   "retention_policy":{
      "minimum_retention":"3650",
      "maximum_retention":"7300",
      "default_retention":"3650",
      "permanent_retention":false
   },
   "cors":{
      "max_age_seconds":"6000",
      "method":["GET"],
      "origin":"*.ibm.com",
      "allowed_header":["*"],
      "expose_header":[
         "server-side-encryption",
         "request-id"
      ]
   },
   "hard_quota":54975581388800,
   "firewall":null,
   "time_created":"2019-04-12T00:56:10Z",
   "time_updated":"2019-04-12T00:56:10Z"
}
```

Delete Bucket

This API covers how to delete a bucket via the Service API.

Base Command :

```
DELETE <accesser>:8338/container/{bucket.name}
```

A DELETE issued to an empty bucket resource deletes the bucket.

After deleting a bucket the name is reserved by the system for 10 minutes and then released for re-use. *Only empty buckets can be deleted*.

This operation does not make sure use of operation specific headers, query parameters, or payload elements

There is no specific response parameter.

Table 19. HTTP Response Code

HTTP Response Code	Description
`204 No content`	No content
`400 Bad Request`	Request contains invalid the bucket name etc.
`401 Unauthorized`	The provided token is invalid or could not be verified.
`403 Forbidden`	Access Denied
404 Not Found	The specified bucket does not exist
409 Conflict	The bucket is not empty
410 Gone	The bucket is already deleted.
500 Internal Server Error	Internal Server Error

Example Output

```
Request
Delete <accesser>:8338/container/my-bucket

Response
HTTP/1.1 204 No Content
```

Chapter 5. Reference

These sections describe the interface details.

1. IBM Container Mode Storage Account Management API Developer Guide
2. IBM Cloud Object Storage System Manager Administration Guide

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Accesser®, Cleversafe®, ClevOS™, Dispersed Storage®, dsNet®, IBM Cloud Object Storage Accesser®, IBM Cloud Object Storage Dedicated™, IBM Cloud Object Storage Insight™, IBM Cloud Object Storage Manager™, IBM Cloud Object Storage Slicestor®, IBM Cloud Object Storage Standard™, IBM Cloud Object Storage System™, IBM Cloud Object Storage Vault™, SecureSlice™, and Slicestor® are trademarks or registered trademarks of Cleversafe, an IBM Company and/or International Business Machines Corp.

Other product and service names might be trademarks of IBM or other companies.

Printed in USA