IBM Cloud Object Storage System
Version 3.15.3

# *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.<br><br>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.<br><br>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. |

| Table 3. Common response headers (continued) | | | |
|---|---|---|---|
| **Response Parameter** | **Style** | **Type** | **Description** |
| **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`.<br>For example, `2015-08-27T09:49:58-05:00`.<br>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** |
| **MalformedNotificationsError** | The JSON you provided for "notifications" was not well-formed or was not valid against our published schema such as invalid format for notifications object, notifications object present when container vault is not assigned to a Notification Service or is not set to configure the topic at the container, notifications object specified in cloud mode. | **400 Bad Request** |
| **MalformedQuota** | The hard quota is not a valid BigInteger. | **400 Bad Request** |

*Table 4. Error Code (continued)*

| Error Code | Description | HTTP Error Code |
|---|---|---|
| **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** |
| **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** |
| **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** |

# Chapter 5. Create bucket

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 | An array of pairs of grantee and permission. If there are multiple permissions for the same grantee, multiple entries are required.<br>**Refer to table below called "ACL JSON (request)"** |
| **hard_quota** | Body | Optional | String | Container hard quota in bytes, default 0 (no limit). Format BigInteger. |
| **firewall** | Body | Optional | Object | The firewall restriction, includes allowed or denied IP addresses lists.<br><br>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.<br>**Refer to table below called "Firewall (request)"** |

| *Table 5. Request Parameters (continued)* | | | | |
|---|---|---|---|---|
| **Request Parameter** | **Style** | **Required** | **Type** | **Description** |
| **notifications** | Body | Optional | Object | This object is valid in on-premises cloud Container Mode when the Operator has configured the container vault to specify the notification topic for the container using the Service API. If the notifications object is not present, then notifications is disabled for the container.<br>The Operator should use the Manager UI/ REST API to determine the topic configuration setting for a container vault.<br>**Refer to table below called Notifications (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 permission for the grantee in the format of **"READ"**, **"WRITE, "READ_ACP", "WRITE_ACP"** 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 IPv4 or IPv6 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 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 IPv4 or IPv6 addresses in CIDR format |

| *Table 8. Notifications (request)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **topic** | String | The topic on which the container's notifications shall be published.<br>Notification of object-change events are published on this topic of the Notification Service assigned to the container vault, if the Notification Service is enabled.<br>Only a single topic is supported for a container.<br>**Note:** Required, Yes if the notifications object is present | 1-249 characters in length.<br>Valid characters: Alphanumeric, hyphen, period, underscore. |

**Response**

| *Table 9. Response Parameters* | | | |
|---|---|---|---|
| **Response Parameter** | **Style** | **Type** | **Description** |
| **X-Timestamp** | Head | 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 **storage_location** of the bucket or the provisioning code of the container vault. |
| **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 grantees and their list of permissions on the bucket. It is not visible if content is not defined. |
| **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; when it is not defined, the object is not visible. |
| **hard_quota** | Body | String | Container hard quota bytes, default 0, no quota. Format BigInteger. |
| **firewall** | Body | Object | Container IP access control restriction information. When it is not defined the object is not visible. |

*Table 9. Response Parameters (continued)*

| Response Parameter | Style | Type | Description |
|---|---|---|---|
| **notifications** | Body | Object | Configuration of notifications for the container.<br>This object is optional and valid in On-Prem Container Mode only. If the notifications object is not present in the request, then notifications is disabled for this container.<br>**Refer to table below called "Notifications (response) Parameter"** |
| **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 10. Notifications (response)*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **topic** | String | The topic on which the container's notifications shall be published.<br>Notification of object-change events are published on this topic of the Notification Service assigned to the container vault, if the Notification Service is enabled.<br>Only a single topic is supported for a container.<br>**Note:** Required, Yes if the notifications object is present | 1-249 characters in length.<br>Valid characters: Alphanumeric, hyphen, period, underscore. |

*Table 11. HTTP response code*

| HTTP Response Code | Description |
|---|---|
| **201 Created** | The bucket was properly created |
| **400 Bad Request** | Request contains too many request element, request timeout, duplicate request header/fields, invalid argument, the bucket is a vault, invalid **hard_quota**, invalid **storage_location**, malformed acl, firewall or JSON, **UnresolvableGrantByEmailAddress**, metadata too large, too many buckets, missing request body, invalid format for notifications object, notifications object present when container vault is not assigned to a Notification Service or is not set to configure the topic at the container, notifications object specified in cloud mode, Notifications Service is disabled, etc.<br>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 |

| *Table 11. HTTP response code (continued)* | |
|---|---|
| **HTTP Response Code** | **Description** |
| **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 |

### Examples

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

**Example: Create bucket command with ACL, IP, notifications, and quota Request**

**Request**

```
{
   "storage_location":"us-south",
   "service_instance":"731fc6f265cd486d900f16e84c5cb594",
   "acl":[
      {
       "grantee":"user1",
       "permission":"WRITE"
      }
   ],
   "hard_quota":107374182400,
   "firewall":{
       "allowed_ip":[ "192.168.28.100/24", "192.168.25.200/32" ],
       "denied_ip":[ "192.169.10.100/30" ]
   },
   "notifications":{
      "topic":"my-bucket_topic"
   }
}
```

**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":{
      "user1":[ "WRITE" ]
    },
   "retention_policy":{
      "status":"DISABLED"
    },
   "hard_quota":107374182400,
   "firewall":{
     "allowed_ip":[ "192.168.28.100/24", "192.168.25.200/32" ],
     "denied_ip":[ "192.169.10.100/30" ]
    },
    "notifications":{
        "topic": "my-bucket_topic"
    },
    "time_created":"2019-04-12T00:56:10Z",
    "time_updated":"2019-04-12T00:56:10Z"
}
```

# Chapter 6. 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**

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

**Request**

*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.<br>For example, If-Unmodified-Since: Sat, 29 Oct 1994 19:43:31 GMT. |
| **acl** | Body | Optional | Array | An array of pairs of grantee and permission. If there are multiple permissions for the same grantee, multiple entries are required.<br>**Refer to table below called "acl array of pairs (PATCH)"** |
| **hard_quota** | Body | Optional | String | Container hard quota bytes in positive value. 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). Format BigInteger.<br>When this is not provide, there is no quota restriction on the bucket. To remove the quota, set the value to 0. |

| *Table 12. Common Request Parameters (continued)* | | | | |
|---|---|---|---|---|
| **Request Parameter** | **Style** | **Required** | **Type** | **Description** |
| **`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`**.<br><br>**Refer to table below called "Firewall (PATCH)"** |
| **`notifications`** | Body | Optional | Object | Optional notifications configuration for the container.<br><br>This object is valid in on-premises cloud Container Mode when the Operator has configured the container vault to specify the notification topic for the container using the Service API. If the notifications object is not present, then notifications is disabled for the container. If notifications is disabled for a container when there are outstanding notifications (due to ongoing requests or due to retries for prior requests), then such notifications shall not be published.<br><br>The Operator should use the Manager UI/ REST API to determine the topic configuration setting for a container vault.<br><br>**Refer to table below called "Notifications (PATCH)"** |

| *Table 13. ACL array of pairs (PATCH)* | | |
|---|---|---|
| **Parameter** | **Type** | **Description** |
| **`grantee`** | String | The storage account id or service instance granted to the permission. |

| *Table 13. ACL array of pairs (PATCH) (continued)* | | |
|---|---|---|
| **Parameter** | **Type** | **Description** |
| **permission** | String | The permission for the grantee such as "READ", "WRITE, "READ_ACP", "WRITE_ACP" 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 IPv4 or IPv6 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 IPv4 or IPv6 addresses in CIDR format |

| *Table 15. Notifications (request)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **topic** | String | The topic on which the container's notifications shall be published.<br>Notification of object-change events are published on this topic of the Notification Service assigned to the container vault, if the Notification Service is enabled. If topic is changed for a container when there are outstanding notifications (due to ongoing requests or due to retries for prior requests), then such notifications shall be published to the updated topic.<br>Only a single topic is supported for a container.<br>**Note:** Required, Yes if the notifications object is present. | 1-249 characters in length.<br>Valid characters: Alphanumeric, hyphen, period, underscore. |

**Response**

| *Table 16. Response parameter* | | | |
|---|---|---|---|
| **Response Parameter** | **Style** | **Type** | **Description** |
| **Bucket Object** | Body | Object | The container metadata information, see GET command Response |

| *Table 17. 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.<br>Request contains too many request element, request timeout, duplicate request header/fields, invalid argument, the bucket is a vault, invalid **hard_quota**, malformed acl, firewall or JSON, **UnresolvableGrantByEmailAddress**, Metadata too large, operation aborted, precondition failed,invalid format for notifications object, notifications object present when container vault is not assigned to a Notification Service or is not set to configure the topic at the container, notifications object specified in cloud mode, Notifications Service is disabled, etc .<br>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 17. 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. |

**Examples**

For existing examples, refer to container level configuration service API. This sections shows only new/ modified examples.

**Example: Enable notifications on a container**

**Request**

PATCH <accesser>:8338/container/my-bucket

```
{
    "notifications":{
        "topic":"my-bucket_topic"
    }
}
```

**Response**

The response shows the addition of notifications to existing container configuration.

```
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" ]
     },
    "notifications":{
        "topic":"my-bucket_topic"
    },
    "time_created":"2019-04-12T00:56:10Z",
    "time_updated":"2019-04-15T08:23:42Z"
}
```

**Example: Update quota**

**Request**

PATCH <accesser>:8338/container/my-bucket

```
{
   "hard_quota": 107374182400
}
```

**Response**

The response shows when the firewall content when it is defined..

```
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","READ"],
        "user2": ["FULL-CONTROL"]
    },
    "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" ]
     },
     "notifications": {
         "topic":"my-bucket_topic",
      },
    "time_created":"2019-04-12T00:56:10Z",
    "time_updated":"2019-04-15T08:23:42Z"
 }
```

**Example: Update IP access control**

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:** 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`

```
PATCH <accesser>: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"
      ]
   }
}
```

**Response**

If current metadata last "time_updated" time matches the input value of "If-Unmodified-Since" in the header, the corresponding firewall IP access control attributes will be changed; otherwise, it will be rejected with 409 error.

After change the metadata, a response for the entire metadata is returned, and its body includes both allowed IP and denied IP, since only the allowed_ip is overwritten. If there is an old allowed_ip value, it would be replaced with the new content.

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" (no change).

```
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","READ"],
      "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":[
         "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"
}
```

**Example: Delete IP access control**

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

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

**Response**

A response for the entire metadata is returned, including denied IP, but not the allowed_IP since the allowed_ip is removed.

denied_ip: "192.168.10.100/30"

```
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","READ"],
      "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":[
        "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: Disable notifications on a container**

**Request**

PATCH <accessor>:8338/container/my-bucket

```
{
   "notifications":{
   }
}
```

**Response**

A response with the entire metadata is returned. The notifications object is not present since notifications is disabled.

```
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","READ"],
      "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":[
        "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: Enable notifications on a container**

**Request**

PATCH <accesser>:8338/container/my-bucket

```
{
    "notifications":{
        "topic":"my-bucket_topic"
    }
}
```

**Response**

The response shows the addition of notifications to existing container configuration.

```
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","READ"],
       "user2": ["FULL-CONTROL"]
    },
    "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" ]
     },
    "notifications":{
        "topic":"my-bucket_topic"
    },
    "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 <accesser>:8338/container/my-bucket

```
{
  "acl": [
    { "grantee": "user1",
      "permission: "WRITE"
    },
    {
      "grantee": "user2",
      "permission": "FULL_CONTROL"
    }
  ]
}
```

**Response**

See GET command, all parameters retrieved.

# Chapter 7. 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.

**Response**

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

*Table 18. Response Parameters*

| Response Parameter | Style | Type | Description | Optional or Mandatory |
|---|---|---|---|---|
| **X-Timestamp** | Header | String | The date and time in UNIX Epoch time stamp format when the container was initially created for current version. | Mandatory |
| **storage_location** | Body | String | Refer to the "provisioning code" in the vault mode, this is typically used as "location" in cloud mode. | Mandatory |
| **name** | Body | String | The name of the bucket. | Mandatory |
| **service_instance** | Body | String | The service instance tor storage account id for the account that owns the bucket. | Mandatory |
| **acl** | Body | Object | A JSON map of grantees and their permissions on the bucket. Does not return the object if no content is defined.<br>See Table 19 on page 29. | Optional |
| **retention_policy** | Body | Object | Refers to the protection configuration of the bucket which is set through S3 Extension command **PUT bucket?protection**. If bucket protection configuration is not set, then return the protection configuration configured for the Container Vault if it exists.<br>See: Table 20 on page 29. | Optional |
| **cors** | Body | Array | The bucket's Cross-Origin Resource Sharing (CORS) configuration objects. See: Table 21 on page 30 for CORS configuration Objects. | Optional |
| **hard_quota** | Body | String | Container hard quota bytes in positive value. When this is not provided, it returns 0 - there is no quota restriction on the bucket. To remove the quota, set the value to 0. Format BigInteger. | Mandatory |

*Table 18. Response Parameters (continued)*

| Response Parameter | Style | Type | Description | Optional or Mandatory |
|---|---|---|---|---|
| **firewall** | Body | Object | Firewall information including IP access control. When it is not defined, the object is not visible.<br>**Note:** Although an integer "format" that is associated to the fields supported in the firewall object, and is stored in the metadata, it is not exposed to end user.<br>See: Table 22 on page 30. | Optional |
| **container_encryption** | Body | Object | An object that defines bucket encryption information. Specifically, kms endpoints.<br>See: Table 23 on page 31. | Optional |
| **notifications** | Body | Object | Notifications configuration for the container.<br>**Note:** This object is valid in on-premises cloud Container Mode only.<br>When the Operator has configured the container vault to specify the notification topic for the container using the Service API, the specified notifications configuration is applied to object-change events in the container when the Notification Service is enabled. If the notifications object is not present, then notifications is disabled for the container.<br>The Operator should use the Manager UI/REST API to determine the topic configuration setting for a container vault.<br>If the container vault is configured to use the notification topic specified at the container vault, then the configuration in this object shall not be applied to object-change events and the container vault's topic is used to publish notifications.<br>If the container vault is configured such that a Notification Service is not assigned to the container vault, then the configuration in this object is not applied and notifications is disabled for the container.<br>See: Table 24 on page 32 | Optional |

*Table 18. Response Parameters (continued)*

| Response Parameter | Style | Type | Description | Optional or Mandatory |
|---|---|---|---|---|
| **public_access_block_configuration** | Body | Object | An object that defines whether the public ACLs are blocked.<br>If this field is not present, then public access is permitted for a bucket created using this template, when the bucket or its objects are configured to permit public read.<br>Table 25 on page 32 | |
| **time_created** | Body | String | The creation time of the bucket in RFC 3339 format. Format “date-time” | Mandatory |
| **time_updated** | Body | String | The modification time of the bucket in RFC 3339 format. Format “date-time” | Mandatory |
| **has_lifecycle** | Body | String | Refers to if the bucket has a Lifecycle Policy configured or not. Valid values are **Present** (lifecycle configuration is present on the bucket) or **Not Present** (lifecycle configuration is not present on the bucket). If both the Expiration and the Archive features are disabled, the **has_lifecycle** field will be omitted in the response. | Optional |
| **static_website** | Body | Object | An object that defines the Website Configuration of the bucket. The **static_website** field is not affected by feature enablement. The value of this parameter will only be visible if a website configuration is **Present** on the bucket. See:<br>Table 26 on page 32 | Optional |

*Table 19. Each item of the JSON MAP for the ACL (response) Parameter*

| Parameter | Type | Description |
|---|---|---|
| **grantee** | String | The storage account id or service instance granted the permission. |
| **permission** | Array | The list of string of permissions for the grantee as **READ**, **WRITE**, **READ_ACP**, **WRITE_ACP** and **FULL_CONTROL**. |

*Table 20. Retention_Policy (response) Parameter*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **default_retention** | String | The default period | int64 |
| **maximumRetention** | String | The maximum period | int64 |
| **minimum_retention** | String | The minimum period | int64 |

| *Table 20. Retention_Policy (response) Parameter (continued)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **permanent_retention_enabled** | Boolean | Retain until explicitly cleared. | Default: False |
| **status** | String | Retention status. | Valid values are: **COMPLIANCE**, **RETENTION**, or **DISABLED**. |

| *Table 21. 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 22. Firewall (response) Parameter* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **allowed_ip** | Array | 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 |

| Table 22. Firewall (response) Parameter (continued) | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **denied_ip** | Array | 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. |
| **allowed_network_type** | Array | Array of string of allowed network types applied during bucket creation. It is enforced on the request headers: x-forwarded-for and ibm-client-originating-ip. If network type is not present in either of the headers, then network type is assumed to be "public" for the IP address in that header.<br>If the array is empty, there is no restriction on the network_type. The allowed_network_type configuration takes precedence over the allowed_ip configuration for enforcement of firewall.<br>Internal Note:<br>"adn" corresponds to the IBM COS network type "direct" .<br>"service" corresponds to the IBM COS network type "private". | Array of allowed network types<br>Valid values (any combination of): private, public, direct |

| Table 23. KMS_Endpoints (response) | | |
|---|---|---|
| **Parameter** | **Type** | **Description** |
| **public_kms_endpoint** | String | The public endpoint, in URL form, of the kms service; An empty endpoint ("") would remove the existing public endpoint stored in the container encryption md; At least one of the endpoints, **public_kms_endpoint** or **private_kms_endpoint** is required if **kms_endpoints** is included in the request. |
| **private_kms_endpoint** | String | The private endpoint, in URL form, of the kms service; An empty endpoint ("") would remove the existing private endpoint stored in the container encryption md; At least one of the endpoints, **public_kms_endpoint** or **private_kms_endpoint** is required if **kms_endpoints** is included in the request. |

| *Table 24. Notifications (response)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **topic** | String | The topic on which the container's notifications shall be published.<br>Notification of object-change events are published on this topic of the Notification Service assigned to the container vault, if the Notification Service is enabled.<br>Only a single topic is supported for a container.<br>**Note:** Required, Yes if the notifications object is present | 1-249 characters in length.<br>Valid characters: Alphanumeric, hyphen, period, underscore. |

| *Table 25. Public_Access_Block_Configuration (response)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **block_public_acls** | Boolean | This field controls public access for the container and its objects when access is set via S3 settings (canned-ACL, etc).<br>Blocking public access due to IAM policy (when no credentials are present) should be set in IAM.<br>false indicates that public access is permitted if the appropriate request is issued.<br>If the **public_block_access_configuration** is set to an empty block, then **block_public_acls** is set to false.<br>**Note:** Required, Optional | default: false |

**Response**

| *Table 26. static_website (response)* | | | |
|---|---|---|---|
| **Parameter** | **Type** | **Description** | **Format** |
| **index_document_suffix** | String | Name of the index document for the website. | |
| **error_document_key** | String | Name of the error document for the website | |
| **redirect_all_requests** | Object | Defines the redirect behavior for every request to the bucket's website endpoint | See: Table 27 on page 33 |
| **routing_rules** | Array | Rules that define when a redirect is applied and the corresponding redirect behavior | Array of **routing_rule**. See: Table 28 on page 33 |

*Table 27. redirect_all_requests (response)*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **hostname** | String | Name of the host where requests are redirected. | |
| **protocol** | String | Protocol to use when redirecting requests. | Valid values are **http** or **https** |

*Table 28. routing_rule (response)*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **condition** | Object | Defines a condition that must be met for a specified redirect to apply. | See: Table 29 on page 33. |
| **redirect** | Object | Defines redirect information to another host, another page or another protocol. In the event of an error a different error code to return can also be specified. | See: Table 30 on page 33. |

*Table 29. condition (response)*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **key_prefix** | String | Defines the object key name prefix when the redirect is applied. | |
| **http_error_code** | Integer | Defines an HTTP error code when the redirect is applied. | |

*Table 30. redirect (response)*

| Parameter | Type | Description | Format |
|---|---|---|---|
| **hostname** | String | Hostname to use in the redirect request. | |
| **protocol** | String | Protocol to use when redirecting requests. | |
| **http_redirect_code** | String | Defines the HTTP redirect code to include in the response. | |
| **replace_key_prefix_with** | String | Defines object key prefix to use in the redirect request. | |
| **replace_key_with** | String | Defines the object key to use in the redirect request. | |

*Table 31. 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. |

### Examples

#### Example: Retrieve bucket configuration in on-premises cloud (Bucket has notifications enabled)

**Request**

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

**Response**

This example does not show the firewall since it is not configured.

```
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": {
    "status": "COMPLIANCE",
    "minimum_retention": "3650",
    "maximumRetention": "7300",
    "default_retention": "3650",
    "permanent_retention_enabled": true
  },
  "cors": {
    "max_age_seconds": "6000",
    "method": [
      "GET"
    ],
    "origin": "*.ibm.com",
    "allowed_header": [
      "*"
    ],
    "expose_header": [
      "x-amz-server-side-encryption",
      "x-maz-request-id"
    ]
  },
  "notifications": {
    "topic": "my-bucket_topic"
  },
  "hard_quota": 54975581388800,
  "time_created": "2019-04-12T00:56:10Z",
  "time_updated": "2019-04-12T00:56:10Z",
  "static_website": {
    "index_document_suffix": "index.html",
    "error_document_key": "errors/my_error.html",
    "routing_rules": [
      {
        "condition": {
          "key_prefix": "foo/",
          "http_error_code": 404
        },
        "redirect": {
          "replace_key_prefix_with": "bar/",
          "replace_key_with": "something",
          "http_redirect_code": 301,
          "hostname": "ibm.com",
          "protocol": "HTTP"
        }
      }
    ]
  }
}
```

# Chapter 8. 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 32. HTTP Response Code*

| **HTTP Response Code** | **Description** |
|---|---|
| `204 No content` | No content |
| `400 Bad Request` | Request contains too many request element, request timeout, invalid argument, the bucket is a vault, etc |
| `401 Unauthorized` | Unauthorized |
| `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
```

**Example Delete Bucket Endpoint**

**Note:** 204 No Content should be returned even if the container metadata does not have **`kms_endpoints`** or **`encryption_metadata`** in it.

```
Request
Delete <accesser>:8338/containers/container/{container-name}/metadata/encryption/kms_endpoints

Response
HTTP/1.1 204 No Content
```

# Chapter 9. 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