CMC Storage S3 - API

Contents

Ceph supports a RESTful API that is compatible with the basic data access model of the Amazon S3 API.

1. Features Support

The following table describes the support status for current Amazon S3 functional features:

Feature	Status	Remarks
List Buckets	Supported	
Delete Bucket	Supported	
Create Bucket	Supported	Different set of canned ACLs
Bucket Lifecycle	Supported	
Policy (Buckets, Objects)	Supported	ACLs & bucket policies are supported
Bucket Website	Supported	
Bucket ACLs (Get, Put)	Supported	Different set of canned ACLs
Bucket Location	Supported	
Bucket Notification	Supported	See S3 Notification Compatibility
Bucket Object Versions	Supported	
Get Bucket Info (HEAD)	Supported	
Bucket Request Payment	Supported	

Feature	Status	Remarks
Put Object	Supported	
Delete Object	Supported	
Get Object	Supported	
Object ACLs (Get, Put)	Supported	
Get Object Info (HEAD)	Supported	
POST Object	Supported	
Copy Object	Supported	
Multipart Uploads	Supported	
Object Tagging	Supported	See Object Related Operations for Policy verbs
Bucket Tagging	Supported	
Storage Class	Supported	See Storage Classes

2. Unsupported Header Fields

The following common request header fields are not supported:

Name	Type
x-amz-security-token	Request
Server	Response
x-amz-delete-marker	Response
x-amz-id-2	Response
x-amz-version-id	Response

3. SDK & Tool

3.1. CMC S3 SDK

CMC S3 API is compatible with AWS API so that it supported by AWS SDK

- Java: https://docs.aws.amazon.com/sdk-for-java/v2/developer-guide/s3-examples.html
- PHP: https://docs.aws.amazon.com/aws-sdk-php/v3/api/api-s3-2006-03-01.html
- .NET: https://docs.aws.amazon.com/sdkfornet/v3/apidocs/
- Python: https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/s3.html

3.2. Windows Tool

- S3 Browser: http://s3browser.com/
- CloudBerry S3: https://www.cloudberrylab.com/explorer/amazon-s3.aspx
- Other tool: https://twitgoo.com/best-s3-browsers-windows-mac-linux/

4. API

4.1. Common Entities

Bucket and Host Name

There are two different modes of accessing the buckets. The first (preferred) method identifies the bucket as the top-level directory in the URI.

GET /mybucket HTTP/1.1
Host: s3.cloud.cmctelecom.vn

The second method identifies the bucket via a virtual bucket host name. For example:

GET / HTTP/1.1
Host: mybucket.s3.cloud.cmctelecom.vn

Common Request Headers

Request Header	Description
CONTENT_LENGTH	Length of the request body.
DATE	Request time and date (in UTC).
HOST	The name of the host server.
AUTHORIZATION	Authorization token.

Common Response Status

HTTP Status	Response Code
100	Continue

HTTP Status	Response Code
200	Success
201	Created
202	Accepted
204	NoContent
206	Partial content
304	NotModified
400	InvalidArgument
400	InvalidDigest
400	BadDigest
400	InvalidBucketName
400	InvalidObjectName
400	UnresolvableGrantByEmailAddress
400	InvalidPart
400	InvalidPartOrder
400	RequestTimeout
400	EntityTooLarge

HTTP Status	Response Code
403	AccessDenied
403	UserSuspended
403	RequestTimeTooSkewed
404	NoSuchKey
404	NoSuchBucket
404	NoSuchUpload
405	MethodNotAllowed
408	RequestTimeout
409	BucketAlreadyExists
409	BucketNotEmpty
411	MissingContentLength
412	PreconditionFailed
416	InvalidRange
422	UnprocessableEntity
500	InternalError

4.2. Authentication and ACLs

Requests to the CMC S3 Gateway (CMC S3) can be either authenticated or unauthenticated. CMC S3 assumes unauthenticated requests are sent by an anonymous user. CMC S3 supports canned ACLs.

4.2.1. Authentication

Authenticating a request requires including an access key and a Hash-based Message Authentication Code (HMAC) in the request before it is sent to the CMC S3 server. CMC S3 uses an S3-compatible authentication approach.

HTTP/1.1
PUT /buckets/bucket/object.mpeg
Host: s3.cloud.cmctelecom.vn
Date: Mon, 2 Jan 2012 00:01:01 +0000
Content-Encoding: mpeg
Content-Length: 9999999

Authorization: AWS {access-key}:{hash-of-header-and-secret}

In the foregoing example, replace {access-key} with the value for your access key ID followed by a colon (:). Replace {hash-of-header-and-secret} with a hash of the header string and the secret corresponding to the access key ID.

To generate the hash of the header string and secret, you must:

1. Get the value of the header string.
2. Normalize the request header string into canonical form.
3. Generate an HMAC using a SHA-1 hashing algorithm. See RFC 2104 and HMAC for details.
4. Encode the hmac result as base-64.

To normalize the header into canonical form:

1. Get all fields beginning with x-amz-.
2. Ensure that the fields are all lowercase.
3. Sort the fields lexicographically.
4. Combine multiple instances of the same field name into a single field and separate the field values with a comma.
5. Replace white space and line breaks in field values with a single space.
6. Remove white space before and after colons.
7. Append a new line after each field.
8. Merge the fields back into the header.

Replace the {hash-of-header-and-secret} with the base-64 encoded HMAC string.

4.2.2 Access Control Lists (ACLs)

CMC S3 supports S3-compatible ACL functionality. An ACL is a list of access grants that specify which operations a user can perform on a bucket or on an object. Each grant has a different meaning when applied to a bucket versus applied to an object:

Permission	Bucket	Object
READ	Grantee can list the objects in the bucket.	Grantee can read the object.
WRITE	Grantee can write or delete objects in the bucket.	N/A
READ_ACP	Grantee can read bucket ACL.	Grantee can read the object ACL.

Permission	Bucket	Object
WRITE_ACP	Grantee can write bucket ACL.	Grantee can write to the object ACL.
FULL_CONTROL	Grantee has full permissions for object in the bucket.	Grantee can read or write to the object ACL.

Internally, S3 operations are mapped to ACL permissions thus:

Operation	Permission
s3:GetObject	READ
s3:GetObjectTorrent	READ
s3:GetObjectVersion	READ
s3:GetObjectVersionTorrent	READ
s3:GetObjectTagging	READ
s3:GetObjectVersionTagging	READ
s3:ListAllMyBuckets	READ
s3:ListBucket	READ
s3:ListBucketMultipartUploads	READ
s3:ListBucketVersions	READ

Operation	Permission
s3:ListMultipartUploadParts	READ
s3:AbortMultipartUpload	WRITE
s3:CreateBucket	WRITE
s3:DeleteBucket	WRITE
s3:DeleteObject	WRITE
s3:s3DeleteObjectVersion	WRITE
s3:PutObject	WRITE
s3:PutObjectTagging	WRITE
s3:PutObjectVersionTagging	WRITE
s3:DeleteObjectTagging	WRITE
s3:DeleteObjectVersionTagging	WRITE
s3:RestoreObject	WRITE
s3:GetAccelerateConfiguration	READ_ACP
s3:GetBucketAcl	READ_ACP
s3:GetBucketCORS	READ_ACP
s3:GetBucketLocation	READ_ACP

Operation	Permission
s3:GetBucketLogging	READ_ACP
s3:GetBucketNotification	READ_ACP
s3:GetBucketPolicy	READ_ACP
s3:GetBucketRequestPayment	READ_ACP
s3:GetBucketTagging	READ_ACP
s3:GetBucketVersioning	READ_ACP
s3:GetBucketWebsite	READ_ACP
s3:GetLifecycleConfiguration	READ_ACP
s3:GetObjectAcl	READ_ACP
s3:GetObjectVersionAcl	READ_ACP
s3:GetReplicationConfiguration	READ_ACP
s3:DeleteBucketPolicy	WRITE_ACP
s3:DeleteBucketWebsite	WRITE_ACP
s3:DeleteReplicationConfiguration	WRITE_ACP
s3:PutAccelerateConfiguration	WRITE_ACP
s3:PutBucketAcl	WRITE_ACP

Operation	Permission
s3:PutBucketCORS	WRITE_ACP
s3:PutBucketLogging	WRITE_ACP
s3:PutBucketNotification	WRITE_ACP
s3:PutBucketPolicy	WRITE_ACP
s3:PutBucketRequestPayment	WRITE_ACP
s3:PutBucketTagging	WRITE_ACP
s3:PutPutBucketVersioning	WRITE_ACP
s3:PutBucketWebsite	WRITE_ACP
s3:PutLifecycleConfiguration	WRITE_ACP
s3:PutObjectAcl	WRITE_ACP
s3:PutObjectVersionAcl	WRITE_ACP
s3:PutReplicationConfiguration	WRITE_ACP

Some mappings, (e.g. s3:CreateBucket to WRITE) are not applicable to S3 operation, but are required to allow Swift and S3 to access the same resources when things like Swift user ACLs are in play. This is one of the many reasons that you should use S3 bucket policies rather than S3 ACLs when possible.

4.3. Service Operations

4.3.1. List Buckets

GET / returns a list of buckets created by the user making the request. GET / only returns buckets created by an authenticated user. You cannot make an anonymous request.

Syntax

GET / HTTP/1.1
Host: s3.cloud.cmctelecom.vn

Authorization: AWS {access-key}:{hash-of-header-and-secret}

Response Entities

Name	Type	Description
Buckets	Container	Container for list of buckets.
Bucket	Container	Container for bucket information.
Name	String	Bucket name.
CreationDate	Date	UTC time when the bucket was created.
ListAllMyBucketsResult	Container	A container for the result.
Owner	Container	A container for the bucket owner’s ID and DisplayName.

Name	Type	Description
ID	String	The bucket owner's ID.
DisplayName	String	The bucket owner's display name.

4.4. Bucket Operations

4.4.1. PUT Bucket

Creates a new bucket. To create a bucket, you must have a user ID and a valid AWS Access Key ID to authenticate requests. You may not create buckets as an anonymous user.

Constraints

In general, bucket names should follow domain name constraints.

- Bucket names must be unique.
- Bucket names must begin and end with a lowercase letter.
- Bucket names may contain a dash (-).

Syntax

PUT /{bucket} HTTP/1.1
Host: s3.cloud.cmctelecom.vn
x-amz-acl: public-read-write

Authorization: AWS {access-key}:{hash-of-header-and-secret}

Parameters

Name	Description	Valid Values	Required
x-amz-acl	Canned ACLs.	private, public-read, public-read-write, authenticated-read	No

Request Entities

Name	Type	Description
CreateBucketConfiguration	Container	A container for the bucket configuration.
LocationConstraint	String	A zonegroup api name, with optional S3 Bucket Placement

HTTP Response

If the bucket name is unique, within constraints and unused, the operation will succeed. If a bucket with the same name already exists and the user is the bucket owner, the operation will succeed. If the bucket name is already in use, the operation will fail.

HTTP Status	Status Code	Description
409	BucketAlreadyExists	Bucket already exists under different user's ownership.

4.4.2. DELETE Bucket

Deletes a bucket. You can reuse bucket names following a successful bucket removal.

Syntax

DELETE /{bucket} HTTP/1.1

Host: s3.cloud.cmctelecom.vn

Authorization: AWS {access-key}:{hash-of-header-and-secret}

HTTP Response

HTTP Status	Status Code	Description
204	No Content	Bucket removed.

4.4.3. GET Bucket

Returns a list of bucket objects.

Syntax

GET /{bucket}?max-keys=25 HTTP/1.1

Host: s3.cloud.cmctelecom.vn

Parameters

Name	Type	Description
prefix	String	Only returns objects that contain the specified prefix.
delimiter	String	The delimiter between the prefix and the rest of the object name.
marker	String	A beginning index for the list of objects returned.
max-keys	Integer	The maximum number of keys to return. Default is 1000.

Name	Type	Description
allow-unordered	Boolean	Non-standard extension. Allows results to be returned unordered. Cannot be used with delimiter.

HTTP Response

HTTP Status	Status Code	Description
200	OK	Buckets retrieved

Bucket Response Entities

GET /{bucket} returns a container for buckets with the following fields.

Name	Type	Description
ListBucketResult	Entity	The container for the list of objects.
Name	String	The name of the bucket whose contents will be returned.
Prefix	String	A prefix for the object keys.
Marker	String	A beginning index for the list of objects returned.
MaxKeys	Integer	The maximum number of keys returned.
Delimiter	String	If set, objects with the same prefix will appear in the CommonPrefixes list.

Name	Type	Description
IsTruncated	Boolean	If true, only a subset of the bucket's contents were returned.
CommonPrefixes	Container	If multiple objects contain the same prefix, they will appear in this list.

Object Response Entities

The ListBucketResult contains objects, where each object is within a Contents container.

Name	Type	Description
Contents	Object	A container for the object.
Key	String	The object's key.
LastModified	Date	The object's last-modified date/time.
ETag	String	An MD-5 hash of the object. (entity tag)
Size	Integer	The object's size.
StorageClass	String	Should always return STANDARD.
Type	String	Appendable or Normal.

4.4.4. Get Bucket Location

Retrieves the bucket's region. The user needs to be the bucket owner to call this. A bucket can be constrained to a region by providing LocationConstraint during a PUT request.

Syntax

Add the location subresource to bucket resource as shown below

GET /{bucket}?location HTTP/1.1
Host: s3.cloud.cmctelecom.vn

Authorization: AWS {access-key}:{hash-of-header-and-secret}

Response Entities

Name	Type	Description
LocationConstraint	String	The region where bucket resides, empty string for default region

4.4.5. Get Bucket ACL

Retrieves the bucket access control list. The user needs to be the bucket owner or to have been granted READ_ACP permission on the bucket.

Syntax

Add the acl subresource to the bucket request as shown below.

GET /{bucket}?acl HTTP/1.1
Host: s3.cloud.cmctelecom.vn

Authorization: AWS {access-key}:{hash-of-header-and-secret}

Response Entities

Name	Type	Description
AccessControlPolicy	Container	A container for the response.
AccessControlList	Container	A container for the ACL information.
Owner	Container	A container for the bucket owner's ID and DisplayName.
ID	String	The bucket owner's ID.
DisplayName	String	The bucket owner's display name.
Grant	Container	A container for Grantee and Permission.
Grantee	Container	A container for the DisplayName and ID of the user receiving a grant of permission.
Permission	String	The permission given to the Grantee bucket.

4.4.6. PUT Bucket ACL

Sets an access control to an existing bucket. The user needs to be the bucket owner or to have been granted WRITE_ACP permission on the bucket.

Syntax

Add the acl subresource to the bucket request as shown below.

PUT /{bucket}?acl HTTP/1.1

Request Entities

Name	Type	Description
AccessControlPolicy	Container	A container for the request.
AccessControlList	Container	A container for the ACL information.
Owner	Container	A container for the bucket owner's ID and DisplayName.
ID	String	The bucket owner's ID.
DisplayName	String	The bucket owner's display name.
Grant	Container	A container for Grantee and Permission.
Grantee	Container	A container for the DisplayName and ID of the user receiving a grant of permission.
Permission	String	The permission given to the Grantee bucket.

4.4.7. List Bucket Multipart Uploads

GET /?uploads returns a list of the current in-progress multipart uploads–i.e., the application initiates a multipart upload, but the service hasn't completed all the uploads yet.

Syntax

GET /{bucket}?uploads HTTP/1.1

Parameters

You may specify parameters for GET /{bucket}?uploads, but none of them are required.

Name	Type	Description
prefix	String	Returns in-progress uploads whose keys contains the specified prefix.
delimiter	String	The delimiter between the prefix and the rest of the object name.
key-marker	String	The beginning marker for the list of uploads.
max-keys	Integer	The maximum number of in-progress uploads. The default is 1000.
max-uploads	Integer	The maximum number of multipart uploads. The range from 1-1000. The default is 1000.
upload-id-marker	String	Ignored if key-marker is not specified. Specifies the ID of first upload to list in lexicographical order at or following the ID.

Response Entities

Name	Type	Description
ListMultipartUploadsResult	Container	A container for the results.
ListMultipartUploadsResult.Prefix	String	The prefix specified by the prefix request parameter (if any).

Name	Type	Description
Bucket	String	The bucket that will receive the bucket contents.
KeyMarker	String	The key marker specified by the key-marker request parameter (if any).
UploadIdMarker	String	The marker specified by the upload-id-marker request parameter (if any).
NextKeyMarker	String	The key marker to use in a subsequent request if IsTruncated is true.
NextUploadIdMarker	String	The upload ID marker to use in a subsequent request if IsTruncated is true.
MaxUploads	Integer	The max uploads specified by the max-uploads request parameter.
Delimiter	String	If set, objects with the same prefix will appear in the CommonPrefixes list.
IsTruncated	Boolean	If true, only a subset of the bucket's upload contents were returned.
Upload	Container	A container for Key, UploadId, InitiatorOwner, StorageClass, and Initiated elements.
Key	String	The key of the object once the multipart

Name	Type	Description
		upload is complete.
UploadId	String	The ID that identifies the multipart upload.
Initiator	Container	Contains the ID and DisplayName of the user who initiated the upload.
DisplayName	String	The initiator's display name.
ID	String	The initiator's ID.
Owner	Container	A container for the ID and DisplayName of the user who owns the uploaded object.
StorageClass	String	The method used to store the resulting object. STANDARD or REDUCED_REDUNDANCY
Initiated	Date	The date and time the user initiated the upload.
CommonPrefixes	Container	If multiple objects contain the same prefix, they will appear in this list.
CommonPrefixes.Prefix	String	The substring of the key after the prefix as defined by the prefix request parameter.

4.4.8. ENABLE/SUSPEND BUCKET VERSIONING

PUT /?versioning This subresource set the versioning state of an existing bucket. To set the versioning state, you must be the bucket owner.

You can set the versioning state with one of the following values:

- Enabled : Enables versioning for the objects in the bucket, All objects added to the bucket receive a unique version ID.
- Suspended : Disables versioning for the objects in the bucket, All objects added to the bucket receive the version ID null.

If the versioning state has never been set on a bucket, it has no versioning state; a GET versioning request does not return a versioning state value.

Syntax

PUT /{bucket}?versioning HTTP/1.1

REQUEST ENTITIES

Name	Type	Description
VersioningConfiguration	Container	A container for the request.
Status	String	Sets the versioning state of the bucket. Valid Values: Suspended/Enabled

4.5. Object Operations

4.5.1. Put Object

Adds an object to a bucket. You must have write permissions on the bucket to perform this operation.

Syntax

PUT /{bucket}/{object} HTTP/1.1

Request Headers

Name	Description	Valid Values	Required
content-md5	A base64 encoded MD-5 hash of the message.	A string. No defaults or constraints.	No
content-type	A standard MIME type.	Any MIME type. Default: binary/octet-stream	No
x-amz-meta-<…>	User metadata. Stored with the object.	A string up to 8kb. No defaults.	No
x-amz-acl	A canned ACL.	private, public-read, public-read-write, authenticated-read	No

4.5.2. Copy Object

To copy an object, use PUT and specify a destination bucket and the object name.

Syntax

PUT /{dest-bucket}/{dest-object} HTTP/1.1

x-amz-copy-source: {source-bucket}/{source-object}

Request Headers

Name	Description	Valid Values	Required
x-amz-copy-source	The source bucket name + object name.	{bucket}/{obj}	Yes
x-amz-acl	A canned ACL.	private, public-read, public-read-write, authenticated-read	No
x-amz-copy-if-modified-since	Copies only if modified since the timestamp.	Timestamp	No
x-amz-copy-if-unmodified-since	Copies only if unmodified since the timestamp.	Timestamp	No
x-amz-copy-if-match	Copies only if object ETag matches ETag.	Entity Tag	No
x-amz-copy-if-none-match	Copies only if object ETag doesn't match.	Entity Tag	No

Response Entities

Name	Type	Description
CopyObjectResult	Container	A container for the response elements.

Name	Type	Description
LastModified	Date	The last modified date of the source object.
Etag	String	The ETag of the new object.

4.5.3. Remove Object

Removes an object. Requires WRITE permission set on the containing bucket.

Syntax

DELETE /{bucket}/{object} HTTP/1.1

4.5.4. Get Object

Retrieves an object from a bucket.

Syntax

GET /{bucket}/{object} HTTP/1.1

Request Headers

Name	Description	Valid Values	Required
range	The range of the object to retrieve.	Range: bytes=beginbyte-endbyte	No
if-modified-since	Gets only if modified since the timestamp.	Timestamp	No
if-unmodified-	Gets only if not modified since	Timestamp	No

Name	Description	Valid Values	Required
since	the timestamp.		
if-match	Gets only if object ETag matches ETag.	Entity Tag	No
if-none-match	Gets only if object ETag matches ETag.	Entity Tag	No

Response Headers

Name	Description
Content-Range	Data range, will only be returned if the range header field was specified in the request

4.5.5. Get Object Info

Returns information about object. This request will return the same header information as with the Get Object request, but will include the metadata only, not the object data payload.

Syntax

HEAD /{bucket}/{object} HTTP/1.1

Request Headers

Name	Description	Valid Values	Required
range	The range of the object to	Range: bytes=beginbyte-	No

Name	Description	Valid Values	Required
	retrieve.	endbyte	
if-modified-since	Gets only if modified since the timestamp.	Timestamp	No
if-unmodified-since	Gets only if not modified since the timestamp.	Timestamp	No
if-match	Gets only if object ETag matches ETag.	Entity Tag	No
if-none-match	Gets only if object ETag matches ETag.	Entity Tag	No

4.5.6. Get Object ACL

Syntax

GET /{bucket}/{object}?acl HTTP/1.1

Response Entities

Name	Type	Description
AccessControlPolicy	Container	A container for the response.
AccessControlList	Container	A container for the ACL information.
Owner	Container	A container for the object owner's ID and DisplayName.

Name	Type	Description
ID	String	The object owner's ID.
DisplayName	String	The object owner's display name.
Grant	Container	A container for Grantee and Permission.
Grantee	Container	A container for the DisplayName and ID of the user receiving a grant of permission.
Permission	String	The permission given to the Grantee object.

4.5.7. Set Object ACL

Syntax

PUT /{bucket}/{object}?acl

Request Entities

Name	Type	Description
AccessControlPolicy	Container	A container for the response.
AccessControlList	Container	A container for the ACL information.
Owner	Container	A container for the object owner's ID and DisplayName.
ID	String	The object owner's ID.
DisplayName	String	The object owner's display name.

Name	Type	Description
Grant	Container	A container for Grantee and Permission.
Grantee	Container	A container for the DisplayName and ID of the user receiving a grant of permission.
Permission	String	The permission given to the Grantee object.

4.5.8. Initiate Multi-part Upload

Initiate a multi-part upload process.

Syntax

POST /{bucket}/{object}?uploads

Request Headers

Name	Description	Valid Values	Required
content-md5	A base64 encoded MD-5 hash of the message.	A string. No defaults or constraints.	No
content-type	A standard MIME type.	Any MIME type. Default: binary/octet-stream	No
x-amz-meta-<…>	User metadata. Stored with the object.	A string up to 8kb. No defaults.	No
x-amz-acl	A canned ACL.	private, public-read, public-read-write, authenticated-read	No

Response Entities

Name	Type	Description
InitiatedMultipartUploadsResult	Container	A container for the results.
Bucket	String	The bucket that will receive the object contents.
Key	String	The key specified by the key request parameter (if any).
UploadId	String	The ID specified by the upload-id request parameter identifying the multipart upload (if any).

4.5.9. Multipart Upload Part

Syntax

PUT /{bucket}/{object}?partNumber=&uploadId= HTTP/1.1

HTTP Response

The following HTTP response may be returned:

HTTP Status	Status Code	Description
404	NoSuchUpload	Specified upload-id does not match any initiated upload on this object

4.5.10. List Multipart Upload Parts

Syntax

GET /{bucket}/{object}?uploadId=123 HTTP/1.1

Response Entities

Name	Type	Description
ListPartsResult	Container	A container for the results.
Bucket	String	The bucket that will receive the object contents.
Key	String	The key specified by the key request parameter (if any).
UploadId	String	The ID specified by the upload-id request parameter identifying the multipart upload (if any).
Initiator	Container	Contains the ID and DisplayName of the user who initiated the upload.
ID	String	The initiator's ID.
DisplayName	String	The initiator's display name.
Owner	Container	A container for the ID and DisplayName of the user who owns the uploaded object.
StorageClass	String	The method used to store the resulting object. STANDARD or REDUCED_REDUNDANCY

Name	Type	Description
PartNumberMarker	String	The part marker to use in a subsequent request if IsTruncated is true. Precedes the list.
NextPartNumberMarker	String	The next part marker to use in a subsequent request if IsTruncated is true. The end of the list.
MaxParts	Integer	The max parts allowed in the response as specified by the max-parts request parameter.
IsTruncated	Boolean	If true, only a subset of the object's upload contents were returned.
Part	Container	A container for LastModified, PartNumber, ETag and Size elements.
LastModified	Date	Date and time at which the part was uploaded.
PartNumber	Integer	The identification number of the part.
ETag	String	The part's entity tag.
Size	Integer	The size of the uploaded part.

4.5.11. Complete Multipart Upload

Assembles uploaded parts and creates a new object, thereby completing a multipart upload.

Syntax

POST /{bucket}/{object}?uploadId= HTTP/1.1

Request Entities

Name	Type	Description	Required
CompleteMultipartUpload	Container	A container consisting of one or more parts.	Yes
Part	Container	A container for the PartNumber and ETag.	Yes
PartNumber	Integer	The identifier of the part.	Yes
ETag	String	The part's entity tag.	Yes

Response Entities

Name	Type	Description
CompleteMultipartUploadResult	Container	A container for the response.
Location	URI	The resource identifier (path) of the new object.
Bucket	String	The name of the bucket that contains the new object.
Key	String	The object's key.
ETag	String	The entity tag of the new object.

4.5.12. Abort Multipart Upload

Syntax

DELETE /{bucket}/{object}?uploadId= HTTP/1.1

4.5.13. Append Object

Append data to an object. You must have write permissions on the bucket to perform this operation. It is used to upload files in appending mode. The type of the objects created by the Append Object operation is Appendable Object, and the type of the objects uploaded with the Put Object operation is Normal Object. **Append Object can't be used if bucket versioning is enabled or suspended. Synced object will become normal in multisite, but you can still append to the original object.**

Syntax

PUT /{bucket}/{object}?append&position= HTTP/1.1

Request Headers

Name	Description	Valid Values	Required
content-md5	A base64 encoded MD-5 hash of the message.	A string. No defaults or constraints.	No
content-type	A standard MIME type.	Any MIME type. Default: binary/octet-stream	No
x-amz-meta-<…>	User metadata. Stored with the object.	A string up to 8kb. No defaults.	No
x-amz-acl	A canned ACL.	private, public-read, public-read-write, authenticated-read	No

Response Headers

Name	Description
x-rgw-next-append-position	Next position to append object

HTTP Response

The following HTTP response may be returned:

HTTP Status	Status Code	Description
409	PositionNotEqualToLength	Specified position does not match object length
409	ObjectNotAppendable	Specified object can not be appended
409	InvalidBucketstate	Bucket versioning is enabled or suspended