phoenixNAP Object Storage Service API User Guide

Table of Contents

Purpose and Scope

This help document is intended for developers and will provide general guidance on developing S3 applications for the phoenixNAP Object Storage Service (OSS). Here you will find the details of the phoenixNAP Object Storage System's compliance with the S3 REST API. Links to specific parts of the Amazon S3 API Reference are provided for your convenience.

Introduction

This document lays out in detail the Amazon S3 REST API features supported by OSS. This includes service, bucket, and object operations as well as specific request parameters, request headers, request elements, response headers, response elements, and special errors.

Items not listed in this document are currently not supported by the phoenixNAP Object Storage Service.

To support additional functionalities, phoenixNAP's Object Storage system extends the Amazon S3 API to provide additional functionality to standard object or bucket operations. This document defines these extensions, which are in the form of additional request parameters or request headers; search for sub-topics named 'Extension Elements to the Amazon S3 API'.

1. General Information on Developing S3 Applications for phoenixNAP's Object Storage Service

In many ways, developing client applications for phoenixNAP's Object Storage System is the same as doing so for Amazon S3. This means that when designing and building S3 applications for OSS you can utilize the many helpful resources available to Amazon S3 developers at the Amazon S3 website. The Amazon Web Services (AWS) Developer Centers provide SDKs, community libraries, and user guides for a plethora of development technologies, such as:

- AWS Ruby Developer Center
- AWS PHP Developer Center
- AWS Windows/.NET Developer Center
- AWS Java Developer Center
- AWS Python Developer Center

Other good resources:

- Amazon S3 Articles & Tutorials
- Amazon S3 Sample Code & Libraries

1.1 Distinct attributes of the phoenixNAP Object Storage Service

The main distinctions are:

- phoenixNAP Object Storage Service offers a limited number of extensions to the Amazon S3 API.
- Most, but not all Amazon S3 API services are available with the phoenixNAP Object Storage Service.

- phoenixNAP Object Storage Service client applications must use the Object Storage Service endpoint rather than the S3 service endpoint.
- Use the Management Console to create and manage user accounts.

1.2. Maximum Number of Objects per S3 Bucket and Mass Deletes

Cassandra storage architecture is used for storing object metadata. This architecture influences bucket capacity and client application design.

Cassandra has a maximum of two billion columns per row. As a consequence, the Object Storage Service supports up to two billion S3 objects per bucket. If you need support for a higher number of objects, the best practice is to create multiple buckets and spread objects evenly. To delete multiple objects from a single bucket, follow Amazon's best practice recommendations in the Efficiently Deleting Objects section of the Amazon documentation.

2. Error Responses

The following Amazon S3 API error responses are supported:

Error Response	Description
AccessDenied	Access Denied
AccountProblem	There is a problem with your account that prevents the operation from completing successfully. Please contact support.
AmbiguousGrantByEmailAddress	The email address you provided is associated with more than one account.
BadDigest	The Content-MD5 you specified did not match what we received.
BucketAlreadyExists	The requested bucket name is already in use. The bucket namespace is shared by all users of the system. Please select a different name.
BucketAlreadyOwnedByYou	Your previous request to create the named bucket succeeded and you already own it.
BucketNotEmpty	The bucket you attempted to delete has objects in it.
CrossLocationLoggingProhibited	Cross-location logging not allowed. Buckets in one geographic location cannot log information to a bucket in another location.
EntityTooLarge	Your proposed upload exceeds the maximum allowed object size.
IllegalVersioningConfigurationException	Indicates that the versioning configuration specified in the request is invalid.
IncorrectNumberOfFilesInPostRequest	POST requires exactly one file upload per request.
InternalError	We are experiencing an internal error. Please try again later.
InvalidAccessKeyId	The access key Id you provided does not exist in our records.
InvalidArgument	Invalid argument.
InvalidBucketName	The bucket name you provided is not valid.

InvalidBucketState	The request is not valid with the current state of the bucket.
InvalidDigest	The Content-MD5 you specified is not valid.
InvalidLocationConstraint	The specified location constraint is not valid.
InvalidObjectState	The operation is not valid for the current state of the object.
InvalidPart	One or more of the specified parts cannot be found. The part might not have been uploaded, or the specified entity tag might not have matched the part's entity tag.
InvalidPartOrder	The list of parts was not in ascending order.Parts list must specified in order by part number.
InvalidPolicyDocument	The content of the form does not meet the conditions specified in the policy document.
InvalidRange	The requested range cannot be satisfied.
InvalidRequest	Refer to this link.
InvalidSecurity	Security credentials are not valid.
InvalidTargetBucketForLogging	The target bucket for logging does not exist, is not owned by you, or does not have the appropriate grants for the log-delivery group.
InvalidURI	Couldn't parse the specified URI.
KeyTooLong	The provided key is too long.
MalformedACLError	The XML you provided was not well-formed or did not validate against our published schema.
MalformedPOSTRequest	The body of your POST request is not well-formed multipart/form-data.
MalformedXML	Malformed xml error (xml does not conform to the published xsd).
MaxMessageLengthExceeded	Your request was too big.
MaxPostPreDataLengthExceededError	Your POST request fields preceding the upload file were too large.
MetadataTooLarge	Your metadata headers exceed the maximum allowed metadata size.
MethodNotAllowed	The specified method is not allowed.
MissingContentLength	You must provide the Content-Length HTTP header.
NoSuchBucket	Specified bucket does not exist.
NoSuchKey	Specified key does not exist.
NoSuchLifecycleConfiguration	Specified lifecycle configuration does not exist.
NoSuchReplicationConfiguration	Specified replication configuration does not exist.
NoSuchUpload	The specified multipart upload does not exist. The upload ID might be invalid, or the multipart upload might have been aborted or completed.
NoSuchVersion	Indicates that the version ID specified in the request does not match an existing version.
NotImplemented	Provided header indicates that the functionality is not implemented.

PermanentRedirect	The bucket you are attempting to access must be addressed using the specified endpoint. Send all future requests to this endpoint.
PreconditionFailed	At least one of the preconditions you specified has failed.
Redirect	Temporary redirect.
RestoreAlreadyInProgress	Object restore is already in progress.
RequestIsNotMultiPartContent	Bucket POST must be of the enclosure-type multipart/form-data.
RequestTimeTooSkewed	The difference between the request time and the server's time is too large.
SignatureDoesNotMatch	The request signature you provided does not match the signature we calculated. Check your secret access key and signing method.
ServiceUnavailable	Reduce your request rate.
SlowDown	Reduce your request rate.
TemporaryRedirect	You are being redirected to the bucket during DNS updates.
UnresolvableGrantByEmailAddress	The email address you provided does not match any account on record.
UserKeyMustBeSpecified	The bucket POST must contain the specified field name. If already specified, check the order of the fields.

The **REST error format** is specified in the REST Error Responses section of the Amazon S3 API. If an error response code is not listed in this document, OSS does not support it. If that is the case, please refer to the Error Responses section of the Amazon S3 API.

3. Common Request Headers

The following **Common Request Headers** of the Amazon S3 REST API are supported:

- Authorization
- Content-Length
- Content-Type
- Content-MD5
- Date
- Expect
- Host
- x-amz-date

If a common request header from the Amazon S3 API is not listed above, the phoenixNAP Object Storage Service does not support it. For further clarification and description of common headers, please refer to the Common Response Headers section of the Amazon S3 REST API.

4. Authenticating Requests (AWS Signature Version 4)

AWS Signature Version 4 for authenticating inbound API requests is supported by the phoenixNAP Object Storage Service and is compliant with Amazon's specification of this component. Provide authentication information in the HTTP Authorization header or in query string parameters and you can generate a checksum of the entire payload prior to transmission. For large uploads you can use chunked upload.

AWS Signature Version 2 is supported as well.

Note: Further information on AWS Signature Version 4 can be found in the Authenticating Requests (AWS Signature Version 4) section of the Amazon S3 REST API.

5. Service Operations

Find the list of supported Service Operations below. If a service operation is not listed in this document, phoenixNAP Object Storage Service does not support it. Follow the links below to see the list of specific headers and parameters supported by OSS.

5.1 GET Service

For the Amazon GET Service operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the GET Service section of the Amazon S3 REST API document.

5.1.1 Response Element

- Bucket
- Buckets
- CreationDate
- DisplayName
- ID
- ListAllMyBucketsResult
- Name
- Owner

Note: If you need information on service operations, or request and response items, please refer to the GET Service section of the Amazon S3 REST API specification.

6. Bucket Operations

The following bucket operations are supported:

- DELETE Bucket
- DELETE Bucket cors
- DELETE Bucket lifecycle
- DELETE Bucket policy
- DELETE Bucket website

- GET Bucket (List Objects)
- GET Bucket acl
- GET Bucket cors
- GET Bucket lifecycle
- GET Bucket policy
- GET Bucket location
- GET Bucket logging
- GET Bucket Object versions
- GET Bucket versioning
- GET Bucket website
- HEAD Bucket
- List Multipart Uploads
- PUT Bucket
- PUT Bucket acl
- PUT Bucket cors
- PUT Bucket lifecycle
- PUT Bucket policy
- PUT Bucket logging
- PUT Bucket versioning
- PUT Bucket website

Note: If a bucket operation is not listed above, Object Storage Service does not support it.

6.1 DELETE Bucket

For the Amazon S3 DELETE Bucket operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket section of the Amazon S3 REST API document.

6.2 DELETE Bucket cors

For the Amazon S3 DELETE Bucket cors operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket cors section of the Amazon S3 REST API document.

6.3 DELETE Bucket lifecycle

For the Amazon S3 DELETE Bucket lifecycle operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket lifecycle section of the Amazon S3 REST API document.

6.4DELETE Bucket policy

For the Amazon S3 DELETE Bucket policy operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket policy section of the Amazon S3 REST API document.

6.5 DELETE Bucket replication

For the Amazon S3 DELETE Bucket replication operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket replication section of the Amazon S3 REST API document.

6.6 DELETE Bucket website

For the Amazon S3 DELETE Bucket website operation, OSS supports the S3 common request headers and common response headers. For usage details, please refer to the DELETE Bucket website section of the Amazon S3 REST API document.

6.7 GET Bucket (List Objects)

For the Amazon S3 GET Bucket (List Objects) operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket (List Objects) section of the Amazon S3 REST API specification.

6.7.1 Request Parameters

- delimiter
  Note: *%c2%85(U+0085)* is not supported as a delimiter value.
- encoding-type
- marker
- max-keys
- prefix

Extension Elements to the Amazon S3 API

The following Request Parameters are supported as an extension to the GET Bucket (List Objects) operation:

Request Parameter	Description	Mandatory
meta	Use the ***meta=true*** request parameter to return user-defined object metadata with the GET Bucket response. Without this phoenixNAP OSS extension, the standard S3 GET Bucket method returns only the metadata associated with each object (no user-defined metadata).	No (default=”false”)

With the standard S3 API calls you need to do a *GET Object* on individual objects to receive user-defined object metadata. (See Object Metadata for further details.)

By using our ***meta=true*** request parameter for *GET Bucket*, user-defined metadata associated with each object is presented as metadata within the XML response body, nested in the *Contents* element for each object.

In the example below, the three lines that follow the Owner element show how user-defined metadata for the object *my-image.jpg* would be included in the GET Bucket response body.

```
HTTP/1.1 200 OK
...

<ListBucketResult
xmlns="http://s3.cloudian.com/2013-10-01/">
  ...
    <Contents>
        <Key>my-image.jpg</Key>
        <LastModified>2014-10-
12T17:50:30.000Z</LastModified>

<ETag>&quot;fba9dede5f27731c9771645a39863328&
quot;</ETag>
        <Size>434234</Size>
        <StorageClass>STANDARD</StorageClass>
        <Owner>

<ID>75aa57f09aa0c8caeab4f8c24e99d10f8e7faeebf
76c078efc7c6caea54ba06a</ID>

<DisplayName>mtd@amazon.com</DisplayName>
        </Owner>
        <metadata
name="name1">value1</metadata>
        <metadata
name="name2">value2</metadata>
        <metadata
name="name3">value3</metadata>
    </Contents>
    ...
  ...
</ListBucketResult>
```

The **x-amz-meta-*** extension header prefixes used to create user-defined object metadata items (with the **PUT Object** operation or **POST Object** operation) are not included in the metadata names in the **GET Bucket** response.

6.7.2 Response Headers

- x-amz-bucket-region

Extension Elements to the Amazon S3 API

The following Response Header is supported as an extension to the GET Bucket (List Objects) operation:

Parameter	Description	Mandatory
x-gmt-policyid	Specifies the unique ID of the storage policy assigned to a bucket. See PUT Bucket for further details.	No

6.7.3 Response Elements

- Contents
- CommonPrefixes
- Delimiter
- DisplayName
- Encoding-Type
- ETag
- ID
- IsTruncated
- Key
- LastModified
- ListBucketResult
- Marker
- MaxKeys
- Name
- NextMarker
- Owner
- Prefix
- Size
- StorageClass (values STANDARD and GLACIER only)

Extension Elements to the Amazon S3 API

The *metadata* response element as described in the Request Parameters section above is a supported extension to the standard S3 API.

6.8 GET Bucket acl

For the Amazon S3 GET Bucket acl operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket acl section of the Amazon S3 REST API specification.

6.8.1 Response Elements

- AccessControlList
- AccessControlPolicy
- DisplayName
- Grant
- Grantee
- ID
- Owner
- Permission

6.9 GET Bucket cors

For the Amazon S3 GET Bucket cors operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket cors section of the Amazon S3 REST API specification.

6.1.1 Response Elements

- CORSConfiguration
- CORSRule
- AllowedHeader
- AllowedMethod
- AllowedOrigin
- ExposeHeader
- ID
- MaxAgeSeconds

6.10 GET Bucket lifecycle

For the Amazon S3 GET Bucket lifecycle operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket lifecycle section of the Amazon S3 REST API specification.

6.10.1 Response Headers

Extension Elements to the Amazon S3 API

The following Response Headers are supported as an extension to the GET Bucket lifecycle operation:

Parameter	Description	Mandatory
x-gmt-tieringinfo	See PUT Bucket lifecycle	No
x-gmt-compare	See PUT Bucket lifecycle	No

6.10.2 Response Elements

- Date
- Days
- Expiration
- ID
- LifecycleConfiguration
- Prefix
- Rule
- Status
- StorageClass
- Transition

6.10.3 Special

- NoSuchLifecycleConfiguration

6.11 GET Bucket policy

For the Amazon S3 GET Bucket policy operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket policy section of the Amazon S3 REST API specification.

6.11.1 Response Elements

The response elements contain the (JSON) policy of that specific bucket.

6.12 GET Bucket Location

For the Amazon S3 GET Bucket location operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket location section of the Amazon S3 REST API specification.

6.11.2 Response Elements

- LocationConstraint

6.13 GET Bucket logging

For the Amazon S3 GET Bucket logging operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket logging section of the Amazon S3 REST API specification.

6.13.1 Response Elements

- BucketLoggingStatus
- Grant
- Grantee
- LoggingEnabled
- Permission
- TargetBucket
- TargetGrants
- TargetPrefix

6.14 GET Bucket replication

For the Amazon S3 GET Bucket replication operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket replication section of the Amazon S3 REST API specification.

6.14.1 Response Headers

Extension Elements to the Amazon S3 API

- x-gmt-crr-endpoint

- x-gmt-crr-credentials

6.14.2 Response Elements

- ReplicationConfiguration
- Role
- Rule
- ID
- Status
- Prefix
- Destination
- Bucket
- StorageClass

6.14.3 Special Characters

- NoSuchReplicationConfiguration

6.15 GET Bucket Object versions

For the Amazon S3 GET Bucket Object versions operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket Object versions section of the Amazon S3 REST API specification.

6.15.1 Request Parameters

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Extension Elements to the Amazon S3 API

A supported extension is **meta=true**. It works exactly the same as described for GET Bucket (List Objects), except that in the response body the metadata element will be nested in the **Versions** element and **DeleteMarker** element of the **ListVersionsResult** object.

6.15.2 Response Elements

- DeleteMarker
- DisplayName

- Encoding-Type
- ETag
- ID
- IsLatest
- IsTruncated
- Key
- KeyMarker
- LastModified
- ListVersionsResult
- MaxKeys
- Name
- NextKeyMarker
- NextVersionIdMarker
- Owner
- Prefix
- Size
- StorageClass
- Version
- VersionId
- VersionIdMarker

Extension Elements to the Amazon S3 API

Object Storage Service supports a metadata response element that retrieves user-defined metadata. It works just as described for GET Bucket (List Objects) with the exception of where the metadata element is nested in the response body; you will find the metadata element nested in the *Version* element and *DeleteMarker* element of the *ListVersionsResult* object.

6.16 GET Bucket versioning

For the Amazon S3 GET Bucket versioning operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket versioning section of the Amazon S3 REST API specification.

6.16.1 Response Element

- Status
- VersioningConfiguration

6.17 GET Bucket website

For the Amazon S3 GET Bucket website operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the GET Bucket website section of the Amazon S3 REST API specification.

6.17.1 Response Elements

In the response XML you will find the same elements that were uploaded when the bucket was configured as a website.

6.18 HEAD Bucket

For the Amazon S3 HEAD Bucket operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the HEAD Bucket section of the Amazon S3 REST API specification.

6.18.1 Response Element

- x-amz-bucket-region

Extension Elements to the Amazon S3 API

The following Response Header is supported as an extension to the HEAD Bucket operation:

Parameter	Description	Mandatory
x-gmt-policyid	Specifies the unique ID of the storage policy assigned to the bucket. See PUT Bucket for more information.	No

6.19 List Multipart Uploads

For the Amazon S3 List Multipart Uploads, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the List Multipart Uploads section of the Amazon S3 REST API specification.

6.19.1 Request Parameters

- delimiter
- encoding-type
- max-uploads

- key-marker
- prefix
- upload-id-marker

6.19.2 Response Elements

- ListMultipartUploadsResult
- Bucket
- KeyMarker
- UploadIdMarker
- NextKeyMarker
- NextUploadIdMarker
- Encoding-Type
- MaxUploads
- IsTruncated
- Upload
- Key
- UploadId
- Initiator
- ID
- DisplayName
- Owner
- StorageClass
- Initiated
- ListMultipartUploadsResult.Prefix
- Delimiter
- CommonPrefixes
- CommonPrefixes.Prefix

6.20 PUT Bucket

For the Amazon S3 PUT Bucket, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket section of the Amazon S3 REST API specification.

6.20.1 Request Headers

- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control

Extension Elements to the Amazon S3 API

The following Request Header is supported as an extension to the PUT Bucket operation:

Parameter	Description	Mandatory

x-gmt-policyid	Use this header to specify the unique ID of the storage policy you choose to assign to a newly created bucket. Once the bucket is created, you cannot assign a different storage policy. To obtain a list of storage policies for your system and their policy IDs, you can use the Admin API's **GET /bppolicy/listpolicy** parameter.
	If the "PUT Bucket" request does not include the **x-gmt-policyid** request header, the system will automatically assign the default storage policy to the bucket during.
	The storage policy assigned at creation time will be that bucket's designated policy until the bucket exists.
	403 Error – This error response is received when a specified policy ID does not exist, has been disabled, is unavailable, or is unavailable to the bucket owner. A 403 error response is also returned if the system does not have a default storage policy and you do not specify an "x-gmt-policyid" header.
	`Example:`
	`xgmtpolicyid:1bc90238f9f11cb32f5e4e901675d50b`
		No

Note: Storage Policy governs how data in a bucket is distributed and protected. Multiple storage policies can be created through the interface console or the Admin API. Every storage policy is assigned a unique ID that is an integral component of the policy definition. In order to retrieve a list of your system's storage policies, use the Admin API's **GET /bppolicy/listpolicy** parameter.

6.20.2 Request Elements

- CreateBucketConfiguration
- LocationConstraint

Note: phoenixNAP Object Storage Service carries out the same bucket-name restrictions as does Amazon S3.

6.21 PUT Bucket acl

For the Amazon S3 PUT Bucket acl, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage Service doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket acl section of the Amazon S3 REST API specification.

6.21.1 Request Headers

- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control

6.21.2 Request Elements

- AccessControlList
- AccessControlPolicy
- DisplayName
- Grant
- Grantee
- ID
- Owner
- Permission

6.22 PUT Bucket cors

For the Amazon S3 PUT Bucket cors, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket cors section of the Amazon S3 REST API specification.

6.22.1 Request Headers

- Content-MD5

6.22.2 Request Elements

- CORSConfiguration
- CORSRule
- ID
- AllowedMethod
- AllowedOrigin
- AllowedHeader
- MaxAgeSeconds
- ExposeHeader

6.23 PUT Bucket lifecycle

For the Amazon S3 PUT Bucket lifecycle, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it. **Only the bucket owner can create Lifecycle rules.**

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket lifecycle section of the Amazon S3 REST API specification.

6.23.1 Request Headers

- Content-MD5

Extension Elements to the Amazon S3 API

The following Request Headers are supported as an extension to the PUT Bucket lifecycle operation:

Parameter	Description	Mandatory
x-gmt-tieringinfo	Use this header to configure an automatic transitioning of objects from the Object Storage System to the Amazon S3 storage or Amazon Glacier storage. This is also known as “auto-tiering.” Formatted as follows: `x-gmt-tieringinfo: url encode(S3/S3GLACIER|EndPoint:url-encode(s3-endpoint),[Action:stream/nostream/redirect])` • **S3** or **S3GLACIER**: Specify ***S3*** if you want to transition the objects to Amazon S3 storage. If you want to transition	No

	objects to Amazon Glacier, specify ***S3GLACIER***. You cannot change this later on. • **EndPoint**: The Amazon S3 region endpoint which you will use as your auto-tiering destination. Even if your ultimate tiering destination is Glacier, specify an Amazon S3 endpoint, not a Glacier endpoint. • **[Action:]** — An optional element that specifies how the system will handles GET Object requests for objects that have been auto-tiered from this bucket to Amazon S3 (not Glacier). The supported methods for handling GET Object requests for objects in Amazon S3 are: o **stream** — The Object Storage Service GETs the object from Amazon S3 and streams it through to the client. This is the default method which will be used if you do not specify the **Action**: **option**. o **nostream** — Streaming of objects is disallowed. The GET is rejected and clients will need to execute a POST Object Restore request to restore a copy of the object to local storage. o **redirect** — When a user does a GET operation on a tiered object the response from the Object Storage system will be an HTTP 307 with a signed redirect URL to the object's location in Amazon S3. Objects can be tiered to Glacier ONLY using the POST Object Restore operation. Streaming and redirects are not supported.	
x-gmt-compare	Use this extension header as a part of your PUT Bucket lifecycle request and set the header value to "LAT". In the lifecycle rules that you configure with the *Days comparator* the rule will be implemented as the number of days since the object's **Last Access Time** parameter. If you don't use this header extension or assign it no value, then rules will be implemented as the number of days since the object's creation date, which is the standard Amazon S3 behavior. Use this extension header to: • Create a Last Access Time based auto-tiering rules (use this extension and the **x-gmt-tierinfo** header). • Create Last Access Time based expiration rules (use this extension, NOT the **x-gmt-tierinfo** header).	No

6.23.2. Request Elements

- Date
- Days
- Expiration
- ID
- LifecycleConfiguration
- Prefix
- Rule
- Status
- StorageClass

  Note: If you are using the special extension request header *x-gmt-tieringinfo,* then for the above mentioned request element StorageClass you have to designate “GLACIER”. Set Storage Class to GLACIER even if Amazon S3 is your final tiering destination.

- Transition

6.24 PUT Bucket policy

For the Amazon S3 PUT Bucket policy, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it. **Only the bucket owner can create Lifecycle rules.**

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket policy section of the Amazon S3 REST API specification. If you need further details on designing policies, see Amazon’s Using Bucket Policies, but be aware that **only the below mentioned policies are supported**.

6.24.1 Request Elements

The following bucket policy types are supported:

- Restricting Access to a Specific HTTP Referrer
- Restricting Access to Specific IP Addresses
- Policy for Server-Side Encryption
- Policy for Allowing Object Read Access for Specified Users
- Policy for Public Access to Buckets Configured as Websites

The body (a JSON string) contains the policy contents containing the policy statements.

Note: If a bucket owner is performing operations in the bucket, the systems will not check the bucket policy. When the object owner is performing a GET Object operation on it, the system will not check the bucket policy.

Restricting Access to a Specific HTTP Referrer

Below you will find the format that allows **GetObject** operations on the bucket form only a specified referrer URIs.

```
{
  "Version":"2012-10-17",
  "Id":"http referer policy example",
  "Statement":[
    {
      "Sid":"Allow get requests originated from URI-1 and URI-2",
      "Effect":"Allow",
      "Principal":"*",
      "Action":"s3:GetObject",
      "Resource":"arn:aws:s3:::examplebucket/*",
      "Condition":{
            "StringLike":{
               "aws:Referer":["URI-1"]
               },
            "StringLike":{
               "aws:Referer":["URI-2"]
               }
            }
         }
      }
   ]
}
```

- You can specify multiple "StringLike" conditions.
- URI value (e.g., URI-5 and URI-6) is compared to HTTP Referer header with case-insensitive matching and multi-character wildcard (*) and single-character wildcard (?).

Restricting Access to Specific IP Addresses

Use the "IpAddress" and/or "NotIpAddress" conditions and the "aws:SourceIp" condition key to restrict bucket access to a specific source IP address. In the example below, authenticated users from source address 54.240.144 to perform S3 actions in the bucket, with the exception of users from origin IP address 54.240.143.188.

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::examplebucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "54.240.144.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "54.240.144.188/32"
                }
            }
        }
    ]
}
```

Policy for Server-Side Encryption

Bucket policies that mandate server-side encryption are supported. If you set up this type of encryption, object upload request are rejected if they omit the server-side encryption request header.

Bucket policies that forbid server-side encryption are supported. If you set up this type of encryption, object upload request are rejected if they include the server-side encryption request header. Configure support for all three actions to allow the specified user(s) to list and read objects in the bucket. This applies to all future and current objects.

See example below:

```
{
   "Version":"2012-10-17",
   "Id":"PutObjPolicy",
   "Statement":[{
         "Sid":"DenyUnEncryptedObjectUploads",
         "Effect":"Deny",
         "Principal":"*"
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::YourBucket/*",
         "Condition":{
            "StringNotEquals":{
               "s3:x-amz-server-side-encryption":"AES256"
            }
         }
      }
   ]
}
```

Note: For more information on server-side encryption, including enabling support for the AES-256 encryption that is a requirement for standard Amazon compliant server-side encryption, see Server-Side Encryption.

Policy for Allowing Object Read Access for Specified Users

Bucket policies that allow object read-access to specified users are supported. Users are specified with the “Principal” element, and users need to be specified in format "CanonicalUser":"<canonicalUserId>". Supported actions are GetBucketLocation, ListBucket, and GetObject.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow read access to two specified users",
         "Effect": "Allow",
         "Principal": {"CanonicalUser":"3c60500e4c20208909b332b1bcdd3752",
             "CanonicalUser":"8773d93a05a663e5be8294afe8bd3652"},
         "Action": [
            "s3:GetBucketLocation",
            "s3:ListBucket",
             "s3:GetObject"
         ],
         "Resource": [
            "arn:aws:s3:::examplebucket/*"
         ]
      }
   ]
}
```

Policy for Public Access to Buckets Configured as Websites

If you are hosting a static website using the PUT Bucket website, you can create a bucket policy that allows public access:

```
{
  "Version":"2012-10-17",
  "Statement":[{
      "Sid":"PublicReadForGetBucketObjects",
      "Effect":"Allow",
      "Principal": "*"
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::example-bucket/*"
      ]
    }
  ]
}
```

Public access is via HTTP not HTTPS. Buckets configured as static websites do not support HTTPS (SSL).

Note: For any further details, see Setting Up a Website.

6.24.2 Response Elements

PUT response elements return, even if the operation is unsuccessful.

6.25 PUT Bucket logging

For the Amazon S3 PUT Bucket logging, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket logging section of the Amazon S3 REST API specification.

6.25.1 Request Elements

- BucketLoggingStatus
- EmailAddress
- Grant
- Grantee
- LoggingEnabled
- Permission

- TargetBucket
- TargetGrants
- TargetPrefix

6.26 PUT Bucket replication

For the Amazon S3 PUT Bucket replication, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket replication section of the Amazon S3 REST API specification. For an overview of this Amazon S3 feature, refer to the Cross-Region Replication in the Amazons S3 Developer's Guide.

Compared to Amazon S3, phoenixNAP Object Storage Service does not necessitate that you set up an IAM Role (or anything similar) in order to use this feature. Additionally, phoenixNAP Object Storage Service does not necessitate that the destination bucket is in a different region than the source bucket. You can freely replicate to a destination bucket that is in the same region as the source bucket. However, be aware that when replicating within the same region, you will not have the advantage of geographical dispersion of data that replicating across regions provides.

Besides the above mentioned discrepancies, phoenixNAP Object Storage Service has the same requirements as does Amazon S3 bucket replication, including that **versioning MUST be enabled** on both the source bucket and the destination bucket in order to implement bucket replication. (For this, use the PUT Bucket versioning operation).

Additionally, in order to replicate data to a destination bucket in a given service region, there has to be an entry to that region in the system configuration file **tiering-regions.xml**. This is a rule, and is so even if that service region is not a part of your phoenixNAP Object Storage system (e.g. Amazon S3). By default, **tiering-region.xml** is pre-configured with all the standard Amazon S3 service regions. If your destination bucket is in a region within phoenixNAP's Object Storage Service, or in an external S3 system other than Amazon's, you have to manually configure an entry for the region in **tiering-region.xml** before you can use the bucket replication feature.

7.26.1 Request Headers

- Content-MD5

Extension Elements to the Amazon S3 API

PhoenixNAP Object Storage Service supports additional extensions to the S3 Amazon API. These headers are only required if you are replicating to a destination bucket that is not in the same Object Storage system as the source bucket. For example, if you are replicating from a phoenixNAP OSS source bucket to a destination Amazon S3 bucket, or anytime you are replicating from one Object Storage system to another completely independent Object Storage system.

The following Request Headers are supported as an extension to the PUT Bucket replication operation:

Parameter	Description	Mandatory
x-gmt-crr-endpoint	Service endpoint of the destination S3 service, in format **<protocol>://<endpoint>:<port>.** The recommended protocol is https, since security credentials will be transmitted in this request (see "x-gmt-crr-credentials" below). phoenixNAP's Object Storage Service does not enforce the use of https, but for security reasons it is advisable to use https. This header is mandatory if the destination bucket is not in the same Object Service system as the source bucket. Do not use this header if the destination bucket is in the same region as the source bucket, or if it is in a different region within the same Object Storage system as the source bucket.	See description below
x-gmt-crr-credentials	Access key and secret key for the user account that the Object Storage system should use to write to the destination bucket in the destination S3 system, in format **<access-key>:<secret-key>**. Example: 00caf3940dc923c59406:Ku0bMR0H5nSA7t8N+ngP6uPPTINSxJ/Q2olCMexx	See description below

6.26.3. Request Elements

- ReplicationConfiguration
- Role

Note: In accordance with the Amazon S3 API specification, the **Role** element MUST be included in the PUT Bucket replication request. However phoenixNAP Object Storage Service ignores the **Role's** value, thus you can use any random string as its value. Object Storage Service does not use an IAM role (or anything similar) when implementing cross-region replication.

- Rule
- ID
- Status
- Prefix
- Destination
- Bucket

Note: Use the same **Bucket** value formatting as in the Amazon S3 API specification (e.g

arn:aws:s3:::<bucketname>).

- StorageClass

Note: This value is ignored by phoenixNAP's Object Storage Service.

6.27 PUT Bucket versioning

For the Amazon S3 PUT Bucket versioning, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket versioning section of the Amazon S3 REST API specification.

6.27.1 Request Elements

- Status
- VersioningConfiguration

6.28 PUT Bucket website

For the Amazon S3 PUT Bucket website operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Bucket website section of the Amazon S3 REST API specification.

6.28.1 Request Elements

- WebsiteConfiguration
- RedirectAllRequestsTo
- HostName
- Protocol
- WebsiteConfiguration
- IndexDocument
- ErrorDocument

7. Object Operations

The phoenixNAP Object Storage System supports the following object operations from the list of Amazon S3 Operations on Objects.

- DELETE Object
- Delete Multiple Objects
- GET Object
- GET Object ACL

- HEAD Object
- OPTIONS object
- POST Object
- POST Object restore
- PUT Object
- PUT Object acl
- PUT Object - Copy
- Initiate Multipart Upload
- Upload Part
- Upload Part - Copy
- Complete Multipart Upload
- Abort Multipart Upload
- List Parts

Note: If an object operation is not listed above, phoenixNAP's Object Storage Service does not support it.

7.1 DELETE Object

For the Amazon S3 DELETE Object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Do not attempt to delete more than 100,000 objects from a single bucket in less than an hour. Doing so will result in **TombstoneOverwhelmingException** errors in the Cassandra logs and you will be unable to successfully execute an S3 GET Bucket (List Objects) operation on the bucket.

Note: If you need information on request and response items, or usage, please refer to the DELETE Object section of the Amazon S3 REST API specification.

7.1.1 Response Headers

- x-amz-delete-marker
- x-amz-version-id

7.2 Delete Multiple Objects

For the Amazon S3 DELETE Multiple Objects operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Do not attempt to delete more than 100,000 objects from a single bucket in less than an hour. Doing so will result in **TombstoneOverwhelmingException** errors in the Cassandra logs and you will be unable to successfully execute an S3 GET Bucket (List Objects) operation on the bucket.

For deleting multiple objects from a single bucket, please follow Amazon’s recommendations for efficiently deleting objects.

Note: If you need information on request and response items, or usage, please refer to the DELETE Multiple Objects section of the Amazon S3 REST API specification.

7.2.1 Request Headers

- Content-MD5
- Content-Length

7.2.2 Request Elements

- Delete
- Quiet
- Object
- Key
- VersionId

7.2.3 Response Elements

- DeleteResult
- Deleted
- Key
- VersionId
- DeleteMarker
- DeleteMarkerVersionId
- Error
- Key
- VersionId
- Code
- Message

7.3 GET Object

For the Amazon S3 GET Object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the GET Object section of the Amazon S3 REST API specification.

7.3.1 Request Parameters

- response-content-type
- response-content-language
- response-expires
- response-cache-control
- response-content-disposition
- response-content-encoding

7.3.2 Request Headers

- Range
- If-Modified-Since
- If-Unmodified-Since
- If-Match
- If-None-Match
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

7.3.3 Response Headers

- x-amz-delete-marker
- x-amz-expiration
- x-amz-meta-*
- x-amz-server-side-encryption
- x-amz-restore
- x-amz-version-id
- x-amz-website-redirect-location
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5

7.4 GET Object ACL

For the Amazon S3 GET Object ACL operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the GET Object ACL section of the Amazon S3 REST API specification.

7.4.1 Response Elements

- AccessControlList
- AccessControlPolicy
- DisplayName
- Grant
- Grantee
- ID
- Owner
- Permission

7.5 HEAD Object

For the Amazon S3 HEAD Object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the HEAD Object section of the Amazon S3 REST API specification.

7.5.1 Request Headers

- Range
- If-Modified-Since
- If-Unmodified-Since
- If-Match
- If-None-Match
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

7.5.2 Response Headers

- x-amz-expiration
- x-amz-meta-*
- x-amz-restore
- x-amz-server-side-encryption

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-version-id

7.6 OPTIONS object

For the Amazon S3 Options object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the Options object section of the Amazon S3 REST API specification.

7.6.1 Request Headers

- Origin
- Access-Control-Request-Method
- Access-Control-Request-Headers

7.6.2 Response Headers

- Access-Control-Allow-Origin
- Access-Control-Max-Age
- Access-Control-Allow-Methods
- Access-Control-Allow-Headers
- Access-Control-Expose-Headers

7.7 POST Object

For the Amazon S3 POST Object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the POST Object section of the Amazon S3 REST API specification.

7.7.1 Form Fields

- AWSAccessKeyId
- acl
- Cache-Control, Content-Type, Content-Disposition, Content-Encoding, Expires
- file
- key
- policy

- success_action_redirect, redirect
- success_action_status
- x-amz-storage-class (STANDARD only)
- x-amz-meta-*

Note: The metadata values MUST be UTF-8 and mustn’t contain control characters less than 0x20 except for \r, \n, and \t. Also, normal XML escaping is required where appropriate.

- x-amz-website-redirect-location
- x-amz-server-side-encryption

Note: The **x-amz-server-side-encryption** header triggers server-side encryption, but the Object Storage Service disregards the value of this header. Instead it uses the encryption algorithm specified by the system setting **mts.properties: cloudian.s3.serverside.encryption.keylength**. By default, AES256 is not enabled in the system and AES128 is used. While AES128 may be acceptable for testing purposes, to be compliant with Amazon S3 you must first enable AES256 in the phoenixNAP Object Storage system.

- x-amz-server-side-encryption-customer-algorithm

Note: To use the SSE-C feature, AES256 must be enabled in the Object Storage system. By default it is not enabled. Contact support.

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

7.7.2 Request Headers: Extension Elements to the Amazon S3 API

Name	Description	Mandatory
x-gmt-hyperstore	Use this request header parameter to define the storage type to be used on the object that is being POST-ed. Your options are: • *CASSANDRA* – Store objects in the CASSANDRA database and protect it by means of replication. Replication is governed by system configuration (**region.csv: userdata_keyspace_strategy_options**). Do not use CASSANDRA for objects larger that the system configuration setting ***mts.properties: cassandra.fs.max_chunk_size***. Default is 10485760 bytes. • • *HSFS* – Store objects in our file system and protect them by means of replication. Replication is governed by system configuration (**region.csv: userdata_keyspace_strategy_options**). • • *EC* – Erasure coding used for storing and protecting objects.	No

7.7.3 Response Headers

- x-amz-expiration
- success_action_redirect, redirect
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-version-id

7.7.4 Response Elements

- Bucket
- ETag
- Key
- Location

7.8 POST Object restore

For the Amazon S3 POST Object restore operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the POST Object restore section of the Amazon S3 REST API specification.

7.8.1 Request Headers

- Content-MD5

7.8.2 Request Elements

- RestoreRequest
- Days

7.9 PUT Object

For the Amazon S3 PUT Object operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Object section of the Amazon S3 REST API specification.

7.9.1 Request Headers

- Cache-Control
- Content-Disposition

- Content-Encoding
- Content-Length
- Content-MD5
- Content-Type
- Expect
- Expires
- x-amz-meta-*
- x-amz-storage-class
- x-amz-website-redirect-location
- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control
- x-amz-server-side-encryption

Extension Elements to the Amazon S3 API

Name	Description	Mandatory
x-gmt-hyperstore	Use this request header parameter to define the storage type to be used on the object that is being POST-ed. Options are as followed: • *CASSANDRA* – Store objects in the CASSANDRA database and protect it by means of replication. Replication is governed by system configuration (region.csv: userdata_keyspace_strategy_options). Do not use CASSANDRA for objects larger that the system configuration setting *mts.properties: cassandra.fs.max_chunk_size*. Default is 10485760 bytes. • *HSFS* – Store objects in our file system and protect them by means of replication. Replication is governed by system configuration (region.csv: userdata_keyspace_strategy_options). • *EC* – Erasure coding used for storing and protecting objects.	No

Bucket and Object Name Restrictions

Certain characters are forbidden in object names (folder and file names) and using them will return a 400 Bad Request response.

Unsupported characters are:

0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A (“\n”), 0x0B, 0x0C, 0x0D (“\r”), 0x0E, 0x0F, 0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F

Also,

- 0xBF (inverted question mark) at the end of an object name and
- 0x09 (“\t”) at the beginning of an object name is unsupported.

Other examples of unsuitable character sequences that result in 400 Bad Request:

.	..	./	../
./.	./..	../.	../..
../a	../a/	a/../../b	

The following character sequences will be stored as a different name:

Supplied Object Name	Stored As
./a	a
./a/	a/
a//b	a/b
a/./b	a/b
a/../b	b
a/.././b	b

7.9.2 Response Headers

- x-amz-expiration
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-version-id

7.10 PUT Object acl

For the Amazon S3 PUT Object acl operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Object acl section of the Amazon S3 REST API specification.

7.10.1 Request Headers

- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control

7.10.2 Request Elements

- AccessControlList
- AccessControlPolicy
- DisplayName
- Grant
- Grantee
- ID
- Owner
- Permission

7.10.3 Response Headers

- x-amz-version-id

7.11 PUT Object – Copy

For the Amazon S3 PUT Object - Copy operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the PUT Object - Copy section of the Amazon S3 REST API specification.

7.11.1 Request Headers

- x-amz-copy-source
- x-amz-metadata-directive
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

- x-amz-storage-class
- x-amz-website-redirect-location
- x-amz-server-side-encryption

Note: The **x-amz-server-side-encryption** header triggers server-side encryption, but the Object Storage Service disregards the value of this header. Instead it uses the encryption algorithm specified by the system setting **mts.properties: cloudian.s3.serverside.encryption.keylength**. By default, AES256 is not enabled in the system and AES128 is used. While AES128 may be acceptable for testing purposes, to be compliant with Amazon S3 you must first enable AES256 in the phoenixNAP Object Storage system.

- x-amz-server-side-encryption-customer-algorithm

Note: To use the SSE-C feature, AES256 must be enabled in the Object Storage system. By default it is not enabled. Contact support.

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control

7.11.2 Response Headers

- x-amz-expiration
- x-amz-copy-source-version-id
- x-amz-server-side-encryption
- x-amz-version-id

7.11.3 Response Elements

- CopyObjectResult
- ETag

- LastModified

7.12 Initiate Multipart Upload

For the Amazon S3 Initiate Multipart Upload operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the Initiate Multipart Upload section of the Amazon S3 REST API specification.

7.12.1 Request Headers

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Type
- Expires
- x-amz-meta-
- x-amz-storage-class
- x-amz-website-redirect-location
- x-amz-acl
- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full-control
- x-amz-server-side-encryption

Note: The **x-amz-server-side-encryption** header triggers server-side encryption, but the Object Storage Service disregards the value of this header. Instead it uses the encryption algorithm specified by the system setting **mts.properties: cloudian.s3.serverside.encryption.keylength**. By default, AES256 is not enabled in the system and AES128 is used. While AES128 may be acceptable for testing purposes, to be compliant with Amazon S3 you must first enable AES256 in the phoenixNAP Object Storage system.

- x-amz-server-side-encryption-customer-algorithm

Note: To use the SSE-C feature, AES256 must be enabled in the Object Storage system. By default it is not enabled. Contact support.

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

Extension Elements to the Amazon S3 API

Name	Description	Mandatory
x-gmt-hyperstore	Use this request header parameter to define the storage type to be used on the object that is being POST-ed. Options are as followed: • ***HSFS*** – Store objects in our file system and protect them by means of replication. Replication is governed by system configuration (**region.csv: userdata_keyspace_strategy_options**). • ***EC*** – Erasure coding used for storing and protecting objects. When using **the *x-gmt-hyperstore*** header with POST Object or PUT Object operations, a third option is available. However, please note that CASSANDRA is not an option for multipart uploads.	No

7.12.2 Response Headers

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5

7.12.3 Response Elements

- InitiateMultipartUploadResult
- Bucket
- Key
- UploadId

7.13 Upload Part

For the Amazon S3 Upload Part operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the Upload Part section of the Amazon S3 REST API specification.

7.13.1 Request Headers

- Content-Length
- Content-MD5
- Expect
- x-amz-server-side-encryption

Note: The **x-amz-server-side-encryption** header triggers server-side encryption, but the Object Storage Service disregards the value of this header. Instead it uses the encryption algorithm specified by the system setting **mts.properties: cloudian.s3.serverside.encryption.keylength**. By default, AES256 is not enabled in the system and AES128 is used. While AES128 may be acceptable for testing purposes, to be compliant with Amazon S3 you must first enable AES256 in the phoenixNAP Object Storage system.

- x-amz-server-side-encryption-customer-algorithm

Note: To use the SSE-C feature, AES256 must be enabled in the Object Storage system. By default it is not enabled. Contact support.

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

7.13.2 Response Headers

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key-MD5

7.13.3 Special Errors

- NoSuchUpload

7.14 Upload Part – Copy

For the Amazon S3 Upload Part - Copy operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn't support it.

Note: If you need information on request and response items, or usage, please refer to the Upload Part - Copy section of the Amazon S3 REST API specification.

7.14.1 Request Headers

- x-amz-copy-source
- x-amz-copy-source-range
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

7.14.2 Response Headers

- x-amz-copy-source-version-id
- x-amz-server-side-encryption

7.14.3 Response Elements

- CopyPartResult
- ETag
- LastModified

7.14.4 Special Errors

- NoSuchUpload
- InvalidRequest

7.15 Complete Multipart Upload

For the Amazon S3 Complete Multipart Upload operation, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the Complete Multipart Upload section of the Amazon S3 REST API specification.

7.15.1 Request Elements

- CompleteMultipartUpload
- Part
- PartNumber
- ETag

7.15.2 Response Headers

- x-amz-expiration
- x-amz-server-side-encryption
- x-amz-version-id

7.15.3 Response Elements

- CompleteMultipartUploadResult
- Location
- Bucket
- Key
- ETag

7.15.4 Special Errors

- InvalidPart
- InvalidPartOrder

- NoSuchUpload

7.16 Abort Multipart Upload

For the Amazon S3 Abort Multipart Upload, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the Abort Multipart Upload section of the Amazon S3 REST API specification.

7.16.1 Special Errors

- NoSuchUpload

7.17 List Parts

For the Amazon S3 List Parts, OSS supports the S3 common request headers and common response headers, as well as operation-specific elements listed below. If an Amazon S3 header, element, parameter, or special error is not listed below, phoenixNAP Object Storage System doesn’t support it.

Note: If you need information on request and response items, or usage, please refer to the List Parts section of the Amazon S3 REST API specification.

7.17.1 Request Parameters

- encoding-type
- uploadId
- max-parts
- part-number-marker

7.17.2 Response Elements

- ListPartsResult
- Bucket
- Encoding-Type
- Key
- UploadId
- Initiator
- ID
- DisplayName
- Owner
- StorageClass
- PartNumberMarker

- NextPartNumberMarker
- MaxParts
- IsTruncated
- Part
- PartNumber
- LastModified
- ETag
- Size

8. Access Control List (ACL)

For the Access Control List (ACL) component, the Object Storage Service supports the elements listed below. If an Amazon S3 permission type, group, or canned ACL type is not listed below, phoenixNAP Object Storage System does not support it.

Note: If you need information on ACL elements, please refer to the Access Control List (ACL) Overview section of the Amazon S3 REST API specification.

8.11 Predefined Groups

- Authenticated users group
- All users group
- Log delivery group

8.12 Permission Types

- READ
- WRITE
- READ_ACP
- WRITE_ACP
- FULL_CONTROL

8.13 Canned ACL

- private
- public-read
- public-read-write
- authenticated-read
- bucket-owner-read
- bucket-owner-full-control

Extension Elements to the Amazon S3 API

The following canned ACLs are supported additions:

Canned ACL	Applies to	Permissions added to ACL
group-read-write	Bucket and object	Owner has FULL_Control. All other users in the owner's user group have READ and WRITE access.
group-read	Bucket and object	Owner has FULL_Control. All other users in the owner's user group have READ access.

Note: In order to grant access to groups other that the requester's own group, you mustn't use canned ACLs. As an alternative, when using standard Amazon S3 solutions (request headers and request body) for defining privileges to a grantee, specify "**<groupID>|**" as the grantee. This format with a vertical line means that the grantee is a group (e.g. "**<group8>|**").

Please note that if a group is assigned one permissions set and a member of the group another, the member will get the broader set of permissions. This means that if Group8 is granted read-write privileges and a specific member is assigned read privileges, that member will have read-write privileges.