AUTHENTICATION AND ACLS

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

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 RGW server. RGW uses an S3-compatible authentication approach.

```
HTTP/1.1
PUT /buckets/bucket/object.mpeg
Host: cname.domain.com
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.

ACCESS CONTROL LISTS (ACLS)

RGW 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.
`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.