ENCRYPTION

New in version Luminous.

The Ceph Object Gateway supports server-side encryption of uploaded objects, with 3 options for the management of encryption keys. Server-side encryption means that the data is sent over HTTP in its unencrypted form, and the Ceph Object Gateway stores that data in the Ceph Storage Cluster in encrypted form.

CUSTOMER-PROVIDED KEYS

In this mode, the client passes an encryption key along with each request to read or write encrypted data. It is the client's responsibility to manage those keys and remember which key was used to encrypt each object.

This is implemented in S3 according to the Amazon SSE-C specification.

As all key management is handled by the client, no special configuration is needed to support this encryption mode.

KEY MANAGEMENT SERVICE

This mode allows keys to be stored in a secure key management service and retrieved on demand by the Ceph Object Gateway to serve requests to encrypt or decrypt data.

This is implemented in S3 according to the Amazon SSE-KMS specification.

In principle, any key management service could be used here, but currently only integration with Barbican is implemented.

See OpenStack Barbican Integration.

AUTOMATIC ENCRYPTION (FOR TESTING ONLY)

A `rgw crypt default encryption` key can be set in ceph.conf to force the encryption of all objects that do not otherwise specify an encryption mode.

The configuration expects a base64-encoded 256 bit key. For example:

```
rgw crypt default encryption key = 4YSmvJtBv0aZ7geVgAsdpRnLBEwWSWlMIGnRS8a9TSA=
```

Important: This mode is for diagnostic purposes only! The ceph configuration file is not a secure method for storing encryption keys. Keys that are accidentally exposed in this way should be considered compromised.