Note

Configure at least two separated hosts for `HAProxy` and `keepalived` services to maintain high availability.

You can configure the `HAProxy` service to use HTTPS. To enable HTTPS, generate SSL keys and certificates for the configuration. If you do not have a certificate from a Certificate Authority, then use a self-signed certificate.

Server-side Encryption

You can enable server-side encryption to allow sending requests to the RADOS Gateway service using unsecured HTTP when it is not possible to send encrypted requests over SSL. Currently, the server-side encryption scenario is only supported when using the Amazon S3 API.

There are two options to configure server-side encryption for the RADOS Gateway, customer-provided keys or a key management service.

Customer-provided Keys

This option is implemented according to the Amazon SSE-C specification. Each read or write request to the RADOS Gateway service contains an encryption key provided by the user via the S3 client.

An object can only be encrypted with one key and users use different keys to encrypt different objects. It is the user's responsibility to track the keys used to encrypt each object.

Key Management Service

You can configure a key management service to securely store keys for the RADOS Gateway service. When a key management service is configured, the RADOS Gateway service retrieves keys on demand to encrypt or decrypt objects.

Figure 8.2 demonstrates the encryption flow between RADOS Gateway and an example HashiCorp Vault key management service.

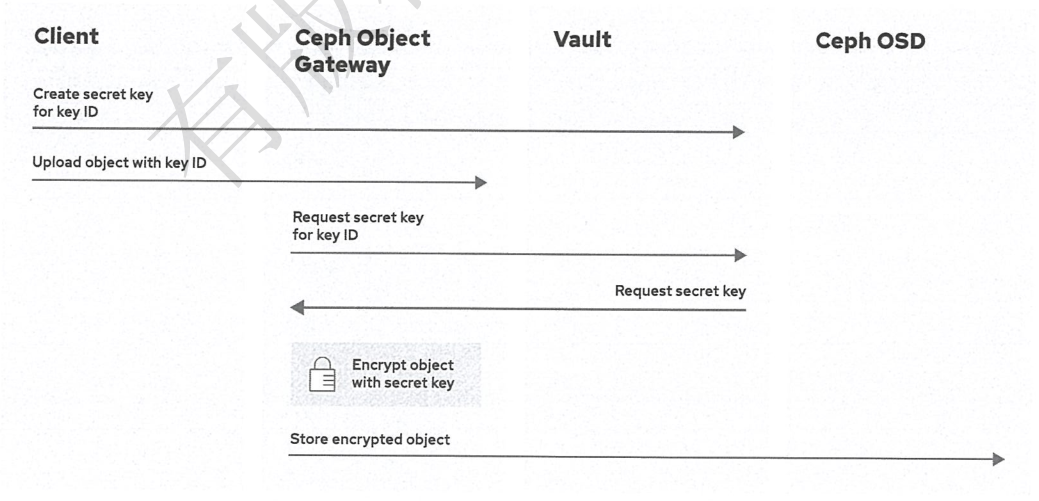
Client
Ceph Object Gateway
Vault
Ceph OSD
Create secret key for key ID
Upload object with key ID
Request secret key for key ID
Request secret key
Encrypt object with secret key
Store encrypted object

Figure 8.2: HashiCorp key management integration

Currently, HashiCorp Vault and OpenStack Barbican are the tested key management service implementations for RADOS Gateway.