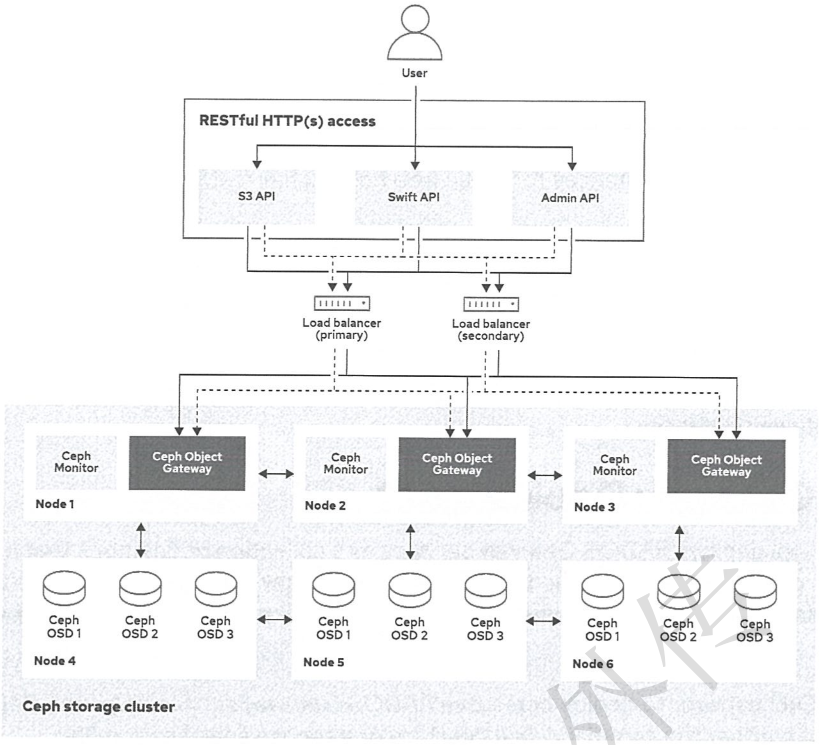

Figure 8.1: RADOS Gateway service architecture

The RADOS Gateway provides the `radosgw-admin` utility for creating users for using the gateway. These users can only access the gateway, and are not `cdephx` users with direct access to the storage cluster. RADOS Gateway clients authenticate using these gateway user accounts when submitting Amazon S3 or OpenStack Swift API requests. After a gateway user is authenticated by the RADOS Gateway, the gateway uses `cephx` credentials to authenticate to the storage cluster to handle the object request. Gateway users can also be managed by integrating an external LDAP-based authentication service.

The RADOS Gateway service automatically creates pools on a per-zone basis. These pools use placement group values from the configuration database and use the default CRUSH hierarchy. The default pool settings might not be optimal for a production environment.

The RADOS Gateway creates multiple pools for the default zone.

- **`.rgw.root`** - Stores information records
- **`.default.rgw.control`** - Used as the control pool
- **`.default.rgw.meta`** - Stores user_keys and other critical metadata
- **`.default.rgw.log`** - Contains logs of all bucket/container and object actions such as create, read, and delete
- **`.default.rgw.buckets.index`** - Stores indexes of the buckets
- **`.default.rgw.buckets.data`** - Stores bucket data
- **`.default.rgw.buckets.non-ec`** - Used for multipart object metadata uploads

You can manually create pools with custom settings. Red Hat recommends using the zone name as a prefix for manually created pools, as in `.<zone-name>.rgw.control`. For example, using `.us-east-1.rgw.buckets.data` as a pool name when `us-east-1` is the zone name.