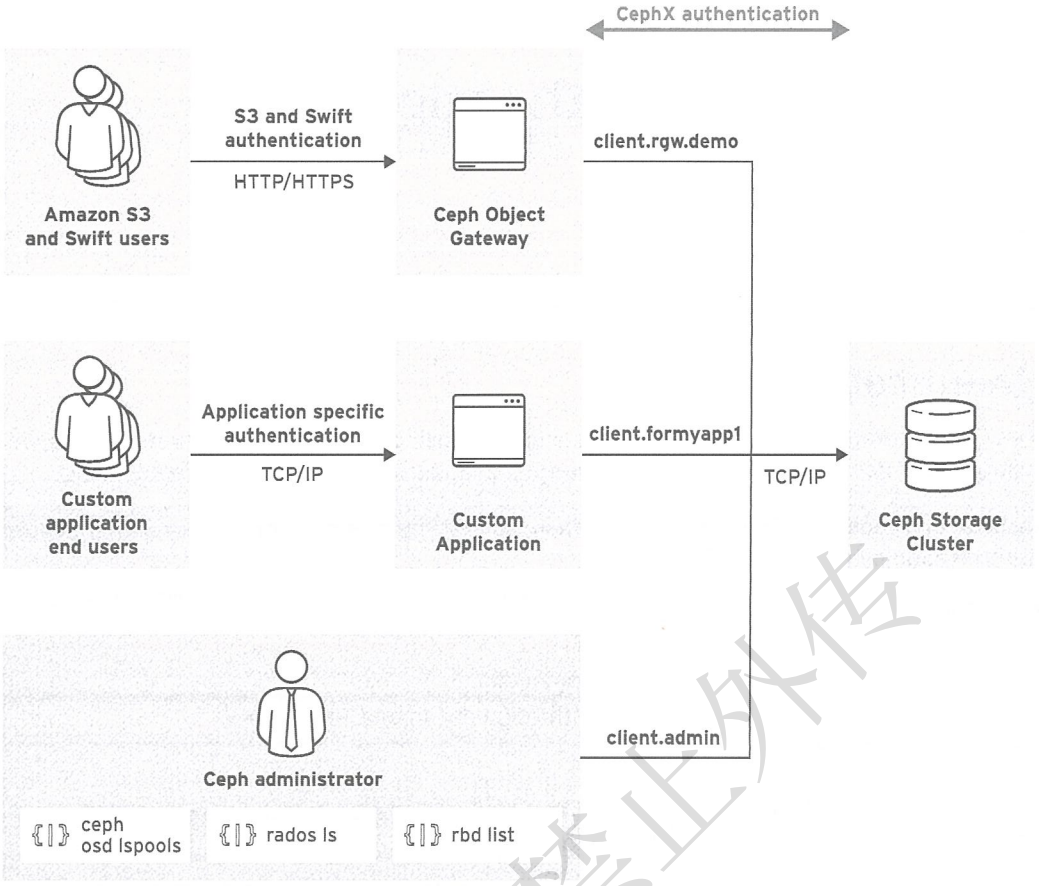

Figure 4.12: User authentication for Ceph applications

The Ceph Object Gateway has its own user database to authenticate Amazon S3 and Swift users, but uses the `client.rgw.`*`hostname`* account to access the cluster.

The Key-ring File

For authentication, clients are configured with a Ceph user name and a key-ring file containing the user's secret key. Ceph generates the key-ring file for each user account when it is created. However, you must copy this file to each client system or application server on which it is needed.

On these client systems, `librados` uses the `keyring` parameter from the `/etc/ceph/ceph.conf` configuration file to locate the key-ring file. Its default value is `/etc/ceph/$cluster.$name.keyring`. For example, for the `client.openstack` account, the key-ring file is `/etc/ceph/ceph.client.openstack.keyring`.

The key-ring file stores the secret key as plain text. Protect the file with appropriate Linux file permissions for access only by authorized Linux users. Only deploy a Ceph user's key-ring file on systems that need it for authentication.

Transmitting Secret Keys

The cephx protocol does not transmit the shared secret keys as plain text. Instead, a client requests a session key from a Monitor. The Monitor encrypts the session key with the client's shared secret key and provides the session key to the client. A client decrypts the session key and