参考

用户管理

http://docs.ceph.org.cn/rados/operations/user-management/

配置cephx

http://docs.ceph.org.cn/rados/configuration/auth-config-ref/

概念

当Ceph运行认证和授权启用（默认启用）时，必须指定包含指定用户（通常通过命令行）的密钥的用户名和密钥环。
如果不指定用户名，Ceph将使用client.admin作为默认用户名。
如果没有指定密钥环，Ceph将通过Ceph配置中的密钥环设置寻找密钥环。

正常情形下，ceph命令的格式如下：

```
ceph -n client.admin --keyring=/etc/ceph/ceph.client.admin.keyring health
```

ceph中的用户

在Ceph用户分成不同类型，如client、osd、mon，标识用户方式为 type.id，下图列出所有的用户，以及用户的key和对应的cap。

```
[root@vmlq my-cluster]# ceph auth list
installed auth entries:

mds.vmlq-1
        key: AQCqW7ZZaWz6DxAA+cuPpOLnkLQNtXA9uJ02yw==
        caps: [mds] allow
        caps: [mon] allow profile mds
        caps: [osd] allow rwx
osd.0
        key: AQBtgLJZy1ILOBAA1ORbgUVLaeH/CrxxrnrvLw==
        caps: [mon] allow profile osd
        caps: [osd] allow *
osd.1
        key: AQB2gLJZT9tgHRAAhesjIYUYXILzsWNRwfcClA==
        caps: [mon] allow profile osd
        caps: [osd] allow *
osd.2
        key: AQAhWrZZgoy6LBAAMC0ZL+crPjTr+MM/fvcyaQ==
        caps: [mon] allow profile osd
        caps: [osd] allow *
client.admin
        key: AQDpfrJZTuYZGhAAzdUBHeToa1STkAELWiWs3w==
        caps: [mds] allow *
        caps: [mon] allow *
        caps: [osd] allow *
client.bootstrap-mds
        key: AQDqfrJZC6A+CxAAxhoMyQJ+A9RSmDhhUvouZg==
        caps: [mon] allow profile bootstrap-mds
client.bootstrap-mgr
        key: AQDtfrJZI6J4GhAAvkhezqe5LQiPU4F5q4LKDA==
        caps: [mon] allow profile bootstrap-mgr
client.bootstrap-osd
        key: AQDpfrJZJgqpKRAAwMQEa4hW+b2FEVzduzlhCw==
        caps: [mon] allow profile bootstrap-osd
client.bootstrap-rgw
        key: AQDpfrJZAkNIOBAA70816vU6JHFsjmx7Yj78Wg==
        caps: [mon] allow profile bootstrap-rgw
client.rgw.vmlq-1
        key: AQD6abZZ6jyjGBAAvxBkU5o/JjeaiwGldKVpEQ==
        caps: [mon] allow rw
        caps: [osd] allow rwx
```

ceph中的cap

ceph中第一个用户可以被赋予多个cap，不同cap有不同类型，包括：监视器能力(mon)、OSD 能力(osd)、元数据服务器能力(mds)。
参考：http://docs.ceph.org.cn/rados/operations/user-management/

创建Ceph用户

典型的用户至少具有Ceph监视器上的读取功能以及Ceph OSD上的读写能力。 此外，用户的OSD权限通常限于访问特定池。

```
# 创建一个典型的用户
ceph auth add client.john mon 'allow r' osd 'allow rw pool=<pool name>'
ceph auth get-or-create client.paul mon 'allow r' osd 'allow rw pool=liver
ceph auth get-or-create client.george mon 'allow r' osd 'allow rw pool=liv
ceph auth get-or-create-key client.ringo mon 'allow r' osd 'allow rw pool=
```

keyring管理

Ceph客户端访问Ceph时，Ceph客户端将寻找本地密钥环。
Ceph默认使用以下keyring，因此无需在配置文件中定义：

```
/etc/ceph/$cluster.$name.keyring
/etc/ceph/$cluster.keyring
/etc/ceph/keyring
/etc/ceph/keyring.bin
```

*cluster*是*Ceph*集群名称，由*Ceph*配置文件的名称定义。 name是用户类型和用户ID，如client.admin。

使用ceph-authtool工具

CEPH-DEPLOY如何生成client.admin

当执行ceph-deploy new {initial-monitor(s)}时，Ceph将创建一个ceph.mon.keyring（该keyring只能用来引导监视器），同时该命令还生成一个初始的Ceph配置文件，包含以下身份验证设置 ，表示Ceph默认启用身份验证：

```
[root@vmlq my-cluster]# ll
total 316
-rw-------. 1 root root    113 Sep  8 07:28 ceph.bootstrap-mds.keyring
-rw-------. 1 root root     71 Sep  8 07:28 ceph.bootstrap-mgr.keyring
-rw-------. 1 root root    113 Sep  8 07:28 ceph.bootstrap-osd.keyring
-rw-------. 1 root root    113 Sep  8 07:28 ceph.bootstrap-rgw.keyring
-rw-------. 1 root root    129 Sep  8 07:28 ceph.client.admin.keyring
-rw-r--r--. 1 root root    221 Sep  8 07:18 ceph.conf
-rw-r--r--. 1 root root 285487 Sep 11 08:17 ceph-deploy-ceph.log
-rw-------. 1 root root     73 Sep  8 07:18 ceph.mon.keyring
-rw-r--r--. 1 root root     12 Sep 11 06:49 testfile.txt
```

```
auth_cluster_required = cephx
auth_service_required = cephx
auth_client_required = cephx
```

当执行ceph-deploy mon create-initial时，Ceph将引导初始监视器，生成ceph.client.admin.keyring文件。之后当执行ceph-deploy admin {node-name}时，ceph-deploy将Ceph配置文件和ceph.client.admin.keyring推送到节点的/etc/ceph目录。 这样在该节点就可以以root身份执行Ceph管理功能。