Restricting Access

Restrict user OSD permissions such that users can only access the pools they need. This example creates the `formyapp2` user and limits their access to read and write on the `myapp` pool:

```
[ceph: root@node /]# ceph auth get-or-create client.formyapp2 \
  mon 'allow r' osd 'allow rw pool=myapp'
```

If you do not specify a pool when you configure capabilities, then Ceph sets them on all existing pools.

The `cephx` mechanism can restrict access to objects by other means:

- By *object name prefix*. The following example restricts access to only those objects whose names start with `pref` in any pool.

```
[ceph: root@node /]# ceph auth get-or-create client.formyapp3 \
  mon 'allow r' osd 'allow rw object_prefix pref'
```

- By *namespace*. Implement namespaces to logically group objects within a pool. You can then restrict user accounts to objects belonging to a specific namespace:

```
[ceph: root@node /]# ceph auth get-or-create client.designer \
  mon 'allow r' osd 'allow rw namespace=photos'
```

- By *path*. The Ceph File System (CephFS) utilizes this method to restrict access to specific directories. This example creates a new user account, `webdesigner`, that can access only the `/webcontent` directory and its contents:

```
[ceph: root@node /]# ceph fs authorize cephfs client.webdesigner /webcontent rw
[ceph: root@node /]# ceph auth get client.webdesigner
exported keyring for client.webdesigner
[client.webdesigner]
        key = AQBrVE9aNwoEGRAApYR6m71ECRzUlLpp4wEJkw==
        caps mds = "allow rw path=/webcontent"
        caps mon = "allow r"
        caps osd = "allow rw pool=cephfs_data"
```

- By *Monitor command*. This method restricts administrators to a specific list of commands. The following example creates the `operator1` user account and limits its access to two commands:

```
[ceph: root@node /]# ceph auth get-or-create client.operator1 \
  mon 'allow r, allow command "auth get-or-create", allow command "auth list"'
```

User Management

To list existing user accounts, run the `ceph auth list` command:

```
[ceph: root@node /]# ceph auth list
...output omitted...
osd.0
        key: AQBW6Tha5z6OIhAAMQ7nY/4MogYecxKqQxX1sA==
        caps: [mgr] allow profile osd
```