CEPHFS CLIENT CAPABILITIES

Use Ceph authentication capabilities to restrict your filesystem clients to the lowest possible level of authority needed.

> **Note:** Path restriction and layout modification restriction are new features in the Jewel release of Ceph.

PATH RESTRICTION

By default, clients are not restricted in what paths they are allowed to mount. Further, when clients mount a subdirectory, e.g., /home/user, the MDS does not by default verify that subsequent operations are 'locked' within that directory.

To restrict clients to only mount and work within a certain directory, use path-based MDS authentication capabilities.

SYNTAX

To grant rw access to the specified directory only, we mention the specified directory while creating key for a client using the following syntax.

```
ceph fs authorize *filesystem_name* client.*client_name* /*specified_directory* rw
```

for example, to restrict client `foo` to writing only in the `bar` directory of filesystem `cephfs`, use

```
ceph fs authorize cephfs client.foo / r /bar rw

results in:

client.foo
  key: *key*
  caps: [mds] allow r, allow rw path=/bar
  caps: [mon] allow r
  caps: [osd] allow rw tag cephfs data=cephfs_a
```

To completely restrict the client to the `bar` directory, omit the root directory

```
ceph fs authorize cephfs client.foo /bar rw
```

Note that if a client's read access is restricted to a path, they will only be able to mount the filesystem when specifying a readable path in the mount command (see below).

Supplying `all` or * as the filesystem name will grant access to every file system. Note that it is usually necessary to quote * to protect it from the shell.

See User Management - Add a User to a Keyring. for additional details on user management

To restrict a client to the specfied sub-directory only, we mention the specified directory while mounting using the following syntax.

```
./ceph-fuse -n client.*client_name* *mount_path* -r *directory_to_be_mounted*
```

for example, to restrict client `foo` to `mnt/bar` directory, we will use.

```
./ceph-fuse -n client.foo mnt -r /bar
```

FREE SPACE REPORTING

By default, when a client is mounting a sub-directory, the used space (`df`) will be calculated from the quota on that sub-directory, rather than reporting the overall amount of space used on the cluster.

If you would like the client to report the overall usage of the filesystem, and not just the quota usage on the sub-directory mounted, then set the following config option on the client:

```
client quota df = false
```

If quotas are not enabled, or no quota is set on the sub-directory mounted, then the overall usage of the filesystem will be reported irrespective of the value of this setting.

LAYOUT AND QUOTA RESTRICTION (THE ‘P’ FLAG)

To set layouts or quotas, clients require the ‘p’ flag in addition to ‘rw’. This restricts all the attributes that are set by special extended attributes with a “ceph.” prefix, as well as restricting other means of setting these fields (such as openc operations with layouts).

For example, in the following snippet client.0 can modify layouts and quotas on the filesystem cephfs_a, but client.1 cannot.

```
client.0
    key: AQAz7EVWygILFRAAdIcuJ12opU/JKyfFmxhuaw==
    caps: [mds] allow rwp
    caps: [mon] allow r
    caps: [osd] allow rw tag cephfs data=cephfs_a

client.1
    key: AQAz7EVWygILFRAAdIcuJ12opU/JKyfFmxhuaw==
    caps: [mds] allow rw
    caps: [mon] allow r
    caps: [osd] allow rw tag cephfs data=cephfs_a
```