radosgw-admin user create --uid=s3 --display-name="objcet storage" --system

```
[root@node1 ~]# ceph -v
ceph version 15.2.16 (d46a73d6d0a67a79558054a3a5a72cb561724974) octopus (stable)
[root@node1 ~]# radosgw-admin user create --uid=s3 --display-name="objcet storage" --system
{
    "user_id": "s3",
    "display_name": "objcet storage",
    "email": "",
    "suspended": 0,
    "max_buckets": 1000,
    "subusers": [],
    "keys": [
        {
            "user": "s3",
            "access_key": "PLUY8ZAAEG2X48W32MFK",
            "secret_key": "39CdyljOqNzgD3wUN6CB9Dp1RIXS2gyI15IKizul"
        }
    ],
    "swift_keys": [],
    "caps": [],
```

radosgw-admin user info --uid=s3 | grep -E "access_key|secret_key"

```
[root@node1 ~]# radosgw-admin user info --uid=s3 | grep -E "access_key|secret_key"
            "access_key": "PLUY8ZAAEG2X48W32MFK",
            "secret_key": "39CdyljOqNzgD3wUN6CB9Dp1RIXS2gyI15IKizul"
[root@node1 ~]#
```

s3cmd --configure

```
[root@node1 ~]# s3cmd --configure

Enter new values or accept defaults in brackets with Enter.
Refer to user manual for detailed description of all options.

Access key and Secret key are your identifiers for Amazon S3. Leave them empty for using the env variables.
Access Key: PLUY8ZAAEG2X48W32MFK  ←
Secret Key: 39CdyljOqNzgD3wUN6CB9Dp1RIXS2gyI15IKizul  ←
Default Region [US]: CN  ←

Use "s3.amazonaws.com" for S3 Endpoint and not modify it to the target Amazon S3.
S3 Endpoint [s3.amazonaws.com]: 172.27.0.3:8080  ←        ceph地址

Use "%(bucket)s.s3.amazonaws.com" to the target Amazon S3. "%(bucket)s" and "%(location)s" vars can be used
if the target S3 system supports dns based buckets.
DNS-style bucket+hostname:port template for accessing a bucket [%(bucket)s.s3.amazonaws.com]: 172.27.0.3:8080

Encryption password is used to protect your files from reading
by unauthorized persons while in transfer to S3        ceph地址
Encryption password:
Path to GPG program [/usr/bin/gpg]:

When using secure HTTPS protocol all communication with Amazon S3
servers is protected from 3rd party eavesdropping. This method is
slower than plain HTTP, and can only be proxied with Python 2.7 or newer
Use HTTPS protocol [Yes]: NO  ←

On some networks all internet access must go through a HTTP proxy.
Try setting it here if you can't connect to S3 directly
HTTP Proxy server name:
```

```
by unauthorized persons while in transfer to S3
Encryption password:        ←        直接回车
Path to GPG program [/usr/bin/gpg]:

When using secure HTTPS protocol all communication with Amazon S3
servers is protected from 3rd party eavesdropping. This method is
slower than plain HTTP, and can only be proxied with Python 2.7 or newer
Use HTTPS protocol [Yes]: NO    ←

On some networks all internet access must go through a HTTP proxy.
Try setting it here if you can't connect to S3 directly
HTTP Proxy server name:

New settings:
  Access Key: PLUY8ZAAEG2X48W32MFK
  Secret Key: 39CdyljOqNzgD3wUN6CB9Dp1RIXS2gyI15IKizul
  Default Region: CN
  S3 Endpoint: 172.27.0.3:8080
  DNS-style bucket+hostname:port template for accessing a bucket: 172.27.0.3:8080
  Encryption password:
  Path to GPG program: /usr/bin/gpg
  Use HTTPS protocol: False
  HTTP Proxy server name:
  HTTP Proxy server port: 0

Test access with supplied credentials? [Y/n] Y
Please wait, attempting to list all buckets...
Success. Your access key and secret key worked fine :-)
```

s3cmd mb s3://demo --region ""

```
anaconda-ks.cfg
[root@node1 ~]# s3cmd mb s3://demo --region ""
Bucket 's3://demo/' created
[root@node1 ~]#
```