

1 Hinweise

```
# Zugriff auf ozone cli
ozone fs

# Beispielsyntax
ozone sh <object> <operation> <--Parameter> /Pfad/Zu/Datei
ozone sh bucket create --enforcegdpr=true /demo/bucketencr

# Hilfe zu Befehlen
# Objekte: volume, bucket, key, snapshot
# Operation: delete, create, list, put, info
ozone sh <object> <operation> --help

# Bash Umgebung einer bestimmten Docker Instanz öffnen
docker exec -it <ContainerName> bash
# z.B. docker exec -it docker_ozone-om-1 bash
# z.B. docker exec -it docker_ozone-datanode-2 bash

ozone version
```

2 Übungen

2.1 Erstellen von Objekten

- Erstellen eines Volume namens demo

```
ozone sh volume create /demo
```

- Liste von Volumes anzeigen lassen

```
ozone sh volume list
```

- Erstellen eines Buckets: bucket1

```
ozone sh bucket create /demo/bucket1
```

- Erstellen und hochladen einer Datei in /demo/bucket1
- z.B. hello.text

```
echo "Hello Ozone" > hello.txt
```

```
ozone sh key put /demo/bucket1/hello.txt hello.txt
```

- Ausgabe der Dateien des Buckets `bucket1`

```
ozone sh key list /demo/bucket1
```

2.2 Dateien herunterladen

- Herunterladen der Datei mit dem Operator `get`

2.3 GDPR Compliant Buckets

- Erstelle ein Bucket `bucketencr` im Volume `demo`, welches Keys nur verschlüsselt abspeichert
- Erstelle in diesem Bucket eine Datei (Key)
- Mit dem `info` Operator können Informationen über Objekte wie Buckets, Keys oder Volumes ausgegeben werden
- Dabei wird die Stelle gesucht, bei der die GDPR Verschlüsselung im Objekt markiert ist.
- Lade die verschlüsselte Datei aus dem Bucket `bucketencr` Datei herunter. Die Datei wird dabei wieder entschlüsselt.

2.4 Inspektion von Datanodes

- Schaue, dir die Datanodes auf der Command Line an

```
ozone admin datanode list
```

- Öffne Bash auf der Instanz eines Datanodes
- Öffne dazu ein neues Terminal und verbinde dich via Bash mit einem Datanode:

```
docker exec -it <Containername> bash  
# z.B. docker exec -it docker_ozone-datanode-2 bash
```

- Oder gehe auf einen Datanode in Docker und wähle "Open in terminal"
- Schau dir unter `/data/hdds` die Blöcken sowie Metadata an
- Finde die physischen Blöcke der verschlüsselten und entschlüsselten Dateien

```
cat /data/hdds.../chunks
cat /data/hdds.../netadata
ls /data/hdds....
```

2.5 Ozone Snapshots

- Lade eine Datei in `/demo/bucket1`

```
echo "Snapshot 1" > snapshot1.txt
```

```
ozone sh key put /demo/bucket1/snapshot1.txt snapshot1.txt
```

- Erstelle einen Snapshot des Buckets `/demo/bucket1`

```
ozone sh snapshot create /demo/bucket1
```

- Lade eine zweite Datei hoch
- Erstelle einen zweiten Snapshot von Bucket in `/demo/bucket1`
- Anzeigen einer Liste aller Snapshots in Bucket `/demo/bucket1` mit `snapshot + list` Operator
- Zeige die Unterschiede zwischen zwei Snapshots mit `snapshot diff` an

```
ozone sh snapshot diff /demo/bucket1 <NameSnapshot1> <NameSnapshot2>
```

- Anzeige der Infos eines Snapshot

```
ozone sh snapshot info /demo/bucket1 s20250205-030511.101
```

2.6 Quota

- Erstelle ein neues volume `demoquo` mit der Einschränkung bezüglich der Namen (Maximum 2)

```
ozone sh volume create --namespace-quota 2 /demoqu
```

- Versuche 3 Buckets in diesem Volume zu erstellen
- Beim Erstellen wird ein Fehler auftreten, da nur 2 Buckets in diesem Volume erlaubt sind
- Kontrolliere die tatsächlich und die erlaubte Anzahl der Namespaces für das Volume

```
ozone sh volume info /demoqu
```

- Erhöhe die Anzahl der Buckets im Volume auf 5 mit `setquota`
- Danach kann ein neues Bucket ohne Fehlermeldung erstellt werden
- Versuche jetzt ein drittes Bucket zu erstellen

2.7 Ozone Insight

Use Ozone Insight

- Zeige Komponenten an

```
ozone insight list
```

- Benutze `ozone insight metrics` um dir Metriken zu verschiedenen Komponenten anzuschauen (z.B. Heartbeat)
- Stelle eine Verbindung mit `ozone insight logs` zum Client Protokoll Service her
- In einem anderen Terminal sollen jetzt Daten an ein beliebiges Bucket gesendet werden.
- Im ersten Terminal können jetzt die Ereignisse verfolgt werden