Wie erlaubt man Zugriff für andere Logins auf eigene S3-Buckets?

03.07.2025 13:57:02

FAQ-Artikel-Ausdruck

Kategorie:	Datenspeicher & Datenablage::Gruppenlaufwerk	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	11:18:38 - 23.09.2024

Schlüsselwörter

S3 Zugriffsrechte S3

Lösung (öffentlich)

Dazu muss man für das Bucket, auf das ein anderes ZIH-Login Zugriff haben soll eine Policy setzen. Am einfachsten funktioniert das via s3cmd.

Die Policy legt man in einer Datei ab. Im Beispiel nennen wir die "example_policy.test.json". Diese Datei hat folgenden Inhalt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<anderesLogin>:user/<anderesLogin>"
      },
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3::<eigenesLogin>:<bucketname>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<anderesLogin>:user/<anderesLogin>"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3::<eigenesLogin>:<bucketname>/*"
    }
  ]
}
```

Ersetzen Sie alle Vorkommen von <eigenesLogin>, <anderesLogin> und <bucketname> inklusive der Klammern durch die korrekten Werte.

Die Policy wird mit dem Kommando:

s3cmd setpolicy example_policy.test.json s3://<bucketname>

gesetzt.