- The `Principal` key defines the user to whom the policy allows or denies access to a resource.

```
{
  "Version": "2021-03-10",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::testaccount:user/testuser"]
      },
      "Action": "s3:ListBucket",
      "Resource": [
      "arn:aws:s3:::testbucket"
      ]
    }
  ]
}
```

Support for S3 MFA Delete

The RADOS Gateway service supports S3 MFA Delete by using Time-based, One-time Password (TOTP) passwords as an authentication factor. This feature adds security against inappropriate and unauthorized data removal. You can configure buckets to require a TOTP one-time token in addition to standard S3 authentication to delete data. To delete an object, the bucket owner must include a request header with the authentication device's serial number and the authentication code in HTTPS to permanently delete an object version or change the versioning state of the bucket. Without the header, the request fails.

Creating New IAM Policies and Roles Using REST APIs

REST APIs for IAM (identity and access management) roles and user policies are now available in the same namespace as S3 APIs and can be accessed using the same endpoint as S3 APIs in the Ceph Object Gateway. This feature allows end users to create new IAM policies and roles by using REST APIs.

Support for Amazon S3 Resources in Ceph Object Gateway

AWS provides the Security Token Service (STS) to allow secure federation with existing OpenID Connect/ OAuth 2.0 compliant identity services such as Keycloak. STS is a standalone REST service that provides temporary tokens for an application or user to access an S3 endpoint after the user authenticates against an identity provider. Previously, users without permanent Amazon Web Services (AWS) credentials could not access S3 resources through Ceph Object Gateway.

Ceph Object Gateway implements a subset of STS APIs that provide temporary credentials for identity and access management. These temporary credentials can be used to make subsequent S3 calls, which will be authenticated by the STS engine in RGW. Permissions of the temporary credentials can be further restricted via an IAM policy passed as a parameter to the STS APIs. Ceph Object Gateway supports STS `AssumeRoleWithWebIdentity`.