Beispiele für Verfahren und APIs

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Inhalt

Beispiele für Verfahren und APIs 1
Testen und Demonstrieren der S3 Verschlüsselungsoptionen auf StorageGRID 1
S3-Objektsperre auf StorageGRID testen und demonstrieren 4
Beispiel für Bucket- und Gruppenrichtlinien (IAM) 9

Beispiele für Verfahren und APIs

Testen und Demonstrieren der S3 Verschlüsselungsoptionen auf StorageGRID

StorageGRID und die S3-API bieten verschiedene Methoden zur Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter "Prüfen Sie die StorageGRID Verschlüsselungsmethoden".

In diesem Leitfaden werden die S3-API-Verschlüsselungsmethoden demonstriert.

Serverseitige Verschlüsselung (SSE)

Mit SSE kann der Client ein Objekt speichern und mit einem eindeutigen Schlüssel verschlüsseln, der von StorageGRID verwaltet wird. Wenn das Objekt angefordert wird, wird das Objekt durch den in StorageGRID gespeicherten Schlüssel entschlüsselt.

Beispiel: SSE

- SETZEN Sie ein Objekt mit SSE

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- LEITEN Sie das Objekt, um die Verschlüsselung zu überprüfen

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- GET das Objekt

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Mit SSE kann der Client ein Objekt speichern und mit einem eindeutigen Schlüssel verschlüsseln, der vom Client mit dem Objekt bereitgestellt wird. Wenn das Objekt angefordert wird, muss derselbe Schlüssel bereitgestellt werden, um das Objekt zu entschlüsseln und zurückzugeben.

Beispiel SSE-C

- Sie können zu Test- oder Demonstrationszwecken einen Schlüssel erstellen
  - Erstellen eines Verschlüsselungsschlüssels

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- Legen Sie ein Objekt mit dem generierten Schlüssel

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- Das Objekt in den Kopf stellen

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:20:02+00:00",
    "ContentLength": 47,
    "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
    "ContentType": "binary/octet-stream",
    "Metadata": {},
    "SSECustomerAlgorithm": "AES256",
    "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
}
```

Wenn Sie den Verschlüsselungsschlüssel nicht angeben, erhalten Sie einen Fehler „ein Fehler ist aufgetreten (404), wenn Sie den HeadObject-Vorgang aufrufen: Nicht gefunden“.

- Get das Objekt

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

Wenn Sie den Verschlüsselungsschlüssel nicht bereitstellen, erhalten Sie beim Aufruf des GetObject-Vorgangs einen Fehler „aufgetreten (InvalidRequest): Das Objekt wurde mit einer Form von serverseitiger Verschlüsselung gespeichert. Zum Abrufen des Objekts müssen die richtigen Parameter angegeben werden.“

Bucket-serverseitige Verschlüsselung (SSE-S3)

Mit SSE-S3 kann der Client ein Standardverschlüsselungsverhalten für alle in einem Bucket gespeicherten Objekte definieren. Die Objekte werden mit einem eindeutigen Schlüssel verschlüsselt, der von StorageGRID gemanagt wird. Wenn das Objekt angefordert wird, wird das Objekt von dem in StorageGRID gespeicherten Schlüssel entschlüsselt.

Beispiel für Bucket SSE-S3

- Erstellen eines neuen Buckets und Festlegen einer Standardverschlüsselungsrichtlinie
  - Erstellen eines neuen Buckets

    ```
    aws s3api create-bucket --bucket <bucket> --region us-east-1
    --endpoint-url https://s3.example.com
    ```

  - Put Bucket-Verschlüsselung

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- Legen Sie ein Objekt in den Bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Das Objekt in den Kopf stellen

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- GET das Objekt

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Von Aron Klein

S3-Objektsperre auf StorageGRID testen und demonstrieren

Object Lock bietet ein WORM-Modell, um das Löschen oder Überschreiben von Objekten zu verhindern. Die StorageGRID Implementierung von Objektsperrung wird auf Cohasset überprüft, um gesetzliche Vorgaben einzuhalten, den gesetzlichen Aufbewahrungs- und Compliance-Modus für Objektspeicherung zu unterstützen und standardmäßige Bucket-Aufbewahrungsrichtlinien einzuhalten.

In diesem Handbuch wird die S3-Objekt-Lock-API demonstriert.

Gesetzliche Aufbewahrungspflichten

- Object Lock Legal Hold ist ein einfacher ein-/Ausschaltstatus, der auf ein Objekt angewendet wird.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- Überprüfen Sie es mit EINEM GET-Vorgang.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Deaktivieren Sie die gesetzliche Aufbewahrungspflichten

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- Überprüfen Sie es mit EINEM GET-Vorgang.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Compliance-Modus

- Die Objektspeicherung erfolgt mit einer Aufbewahrung bis zum Zeitstempel.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- Überprüfen Sie den Aufbewahrungsstatus

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

Standardaufbewahrung

- Legen Sie den Aufbewahrungszeitraum in Tagen und Jahren als Aufbewahrungsdatum fest, das mit der API pro Objekt definiert wurde.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- Überprüfen Sie den Aufbewahrungsstatus

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- Legen Sie ein Objekt in den Bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Die auf dem Bucket festgelegte Aufbewahrungsdauer wird in einen Aufbewahrungszeitstempel des Objekts konvertiert.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Testen Löschen eines Objekts mit einer definierten Aufbewahrung

Objekt Lock basiert auf der Versionierung. Die Aufbewahrung ist für eine Version des Objekts definiert. Wenn versucht wird, ein Objekt mit einer definierten Aufbewahrung zu löschen, und keine Version angegeben wird, wird als aktuelle Version des Objekts eine Löschmarkierung erstellt.

- Löschen Sie das Objekt mit definierter Aufbewahrung

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- Listen Sie die Objekte im Bucket auf

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - Beachten Sie, dass das Objekt nicht aufgeführt ist.
- Listen Sie Versionen auf, um die Löschen-Markierung und die ursprüngliche gesperrte Version anzuzeigen

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Löschen Sie die gesperrte Version des Objekts

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

Von Aron Klein

Beispiel für Bucket- und Gruppenrichtlinien (IAM)

Hier sind Beispiele für Bucket-Richtlinien und Gruppenrichtlinien (IAM-Richtlinien).

Gruppenrichtlinien (IAM)

Bucket-Zugriff im Home Directory-Stil

Diese Gruppenrichtlinie erlaubt Benutzern nur den Zugriff auf Objekte im Bucket mit dem Namen „username“.

```
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

Erstellung von Bucket-Objektsperrung verweigern

Diese Gruppenrichtlinie schränkt Benutzer am Erstellen eines Buckets ein, für den die Objektsperre für den Bucket aktiviert ist.

Diese Richtlinie wird in der StorageGRID-Benutzeroberfläche nicht durchgesetzt, sie wird nur durch die S3-API durchgesetzt.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Aufbewahrungslimit für Objektsperre

Diese Bucket-Richtlinie beschränkt die Aufbewahrungsdauer der Objektsperre auf maximal 10 Tage

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

Benutzer daran hindern, Objekte mit VersionID zu löschen

Diese Gruppenrichtlinie schränkt Benutzer davon ab, versionierte Objekte nach VersionID zu löschen

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Diese Bucket-Richtlinie beschränkt das Löschen versionierter Objekte durch einen Benutzer (identifiziert durch Benutzer-ID „56622399308951294926“) nach VersionID

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

Bucket auf einzelnen Benutzer mit schreibgeschütztem Zugriff beschränken

Diese Richtlinie erlaubt einem einzelnen Benutzer, schreibgeschützten Zugriff auf einen Bucket zu haben und explizit allen anderen Benutzern den zugriff zu verweigert. Die Gruppierung der Ablehenserklärungen an der Spitze der Richtlinie ist eine gute Methode für eine schnellere Bewertung.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "urn:sgws:s3:::bucket1",
                "urn:sgws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "urn:sgws:s3:::bucket1",
                "urn:sgws:s3:::bucket1/*"
            ]
        }
    ]
}
```

Beschränken Sie eine Gruppe auf ein einzelnes Unterverzeichnis (Präfix) mit Lesezugriff

Diese Richtlinie ermöglicht Mitgliedern der Gruppe schreibgeschützten Zugriff auf ein Unterverzeichnis (Präfix) innerhalb eines Buckets. Der Bucket-Name lautet „Study“ und das Unterverzeichnis lautet „study01“.

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
```

```
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3::: study"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```