



Procedure ed esempi di API

How to enable StorageGRID in your environment

NetApp
May 13, 2024

Sommario

- Procedure ed esempi di API 1
 - Testare e dimostrare le opzioni di crittografia S3 su StorageGRID 1
 - Testare e dimostrare il blocco di oggetti S3 su StorageGRID 4
 - Esempio di policy di bucket e di gruppo (IAM) 9

Procedure ed esempi di API

Testare e dimostrare le opzioni di crittografia S3 su StorageGRID

StorageGRID e l'API S3 offrono diversi modi per crittografare i dati inattivi. Per ulteriori informazioni, vedere ["Esaminare i metodi di crittografia StorageGRID"](#).

Questa guida illustra i metodi di crittografia dell'API S3.

Server Side Encryption (SSE)

SSE consente al client di memorizzare un oggetto e di crittografarlo con una chiave univoca gestita da StorageGRID. Quando l'oggetto viene richiesto, l'oggetto viene decrittografato dalla chiave memorizzata in StorageGRID.

Esempio SSE

- METTI un oggetto con SSE

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

- TESTA l'oggetto per verificare la crittografia

```
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": {}  
}
```

- OTTIENI l'oggetto

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

Crittografia lato server con chiavi fornite dal cliente (SSE-C)

SSE consente al client di memorizzare un oggetto e di crittografarlo con una chiave univoca fornita dal client con l'oggetto. Quando l'oggetto viene richiesto, è necessario fornire la stessa chiave per decrittare e restituire l'oggetto.

Esempio SSE-C.

- A scopo di test o dimostrazione, è possibile creare una chiave di crittografia
 - Creare una chiave di crittografia

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

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

- Inserire un oggetto con la chiave generata

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

- Testa l'oggetto

```
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=="  
}
```



Se non si fornisce la chiave di crittografia, viene visualizzato il messaggio di errore "si è verificato un errore (404) durante la chiamata dell'operazione HeadObject: Non trovata"

- Ottieni l'oggetto

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



Se non si fornisce la chiave di crittografia, viene visualizzato l'errore "si è verificato un errore (InvalidRequest) durante la chiamata dell'operazione GetObject: L'oggetto è stato memorizzato utilizzando un modulo di Server Side Encryption. Per recuperare l'oggetto, è necessario fornire i parametri corretti."

Crittografia lato server bucket (SSE-S3)

SSE-S3 consente al client di definire un comportamento di crittografia predefinito per tutti gli oggetti memorizzati in un bucket. Gli oggetti vengono crittografati con una chiave univoca gestita da StorageGRID. Quando l'oggetto viene richiesto, l'oggetto viene decrittografato dalla chiave memorizzata in StorageGRID.

Esempio di bucket SSE-S3

- Creare un nuovo bucket e impostare una policy di crittografia predefinita
 - Creare un nuovo bucket

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

- Metti la crittografia bucket

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

- Metti un oggetto nel bucket

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

- Testa l'oggetto

```
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": {}
}
```

- OTTIENI l'oggetto

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

Di Aron Klein

Testare e dimostrare il blocco di oggetti S3 su StorageGRID

Object Lock fornisce un modello WORM per impedire l'eliminazione o la sovrascrittura degli oggetti. L'implementazione StorageGRID del blocco degli oggetti viene valutata da Cohasset per soddisfare i requisiti normativi, supportare la modalità di conservazione legale e di conformità per la conservazione degli oggetti e le policy di conservazione predefinite dei bucket.

Questa guida illustra l'API S3 Object Lock.

Conservazione a fini giudiziari

- Object Lock legal hold è un semplice stato on/off applicato a un oggetto.

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

- Verificarlo con un'operazione GET.

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

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

- Disattivare la sospensione legale

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

- Verificarlo con un'operazione GET.

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

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

Modalità compliance

- La conservazione degli oggetti viene eseguita con un periodo di conservazione fino a data e ora.

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

- Verificare lo stato di conservazione

```
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"
  }
}
```

Conservazione predefinita

- Impostare il periodo di conservazione in giorni e anni rispetto alla data di conservazione definita con l'api per oggetto.

```
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
```

- Verificare lo stato di conservazione

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

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

- Metti un oggetto nel bucket

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

- La durata di conservazione impostata sul bucket viene convertita in un indicatore data e ora di conservazione sull'oggetto.


```
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"
  }
}
```

Verificare l'eliminazione di un oggetto con una conservazione definita

Il blocco degli oggetti si basa sul controllo delle versioni. La conservazione viene definita su una versione dell'oggetto. Se si tenta di eliminare un oggetto con una conservazione definita e non viene specificata alcuna versione, viene creato un indicatore di eliminazione come versione corrente dell'oggetto.

- Eliminare l'oggetto con la conservazione definita

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

- Elencare gli oggetti nel bucket

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

- Notare che l'oggetto non è elencato.
- Elencare le versioni per visualizzare il marker di eliminazione e la versione originale bloccata

```
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":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTkl",
      "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":
"QjVDQzgZOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjMl",
      "IsLatest": true,
      "LastModified": "2022-05-03T15:35:50.248000+00:00"
    }
  ]
}
```

- Eliminare la versione bloccata dell'oggetto

```
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

Esempio di policy di bucket e di gruppo (IAM)

Di seguito sono riportati alcuni esempi di policy bucket e di policy di gruppo (policy IAM).

Policy di gruppo (IAM)

Accesso bucket stile home directory

Questo criterio di gruppo consente solo agli utenti di accedere agli oggetti nel bucket denominato 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}/*"
  }
]
```

Negare la creazione del bucket di blocco degli oggetti

Questo criterio di gruppo limiterà gli utenti a creare un bucket con il blocco degli oggetti attivato nel bucket.



Questo criterio non viene applicato nell'interfaccia utente di StorageGRID, ma viene applicato solo dall'API S3.

```

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

```

Limite di conservazione del blocco degli oggetti

Questa policy di bucket limiterà la durata della conservazione del blocco oggetto a 10 giorni o meno

```

{
  "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"
        }
      }
    }
  ]
}

```

Impedire agli utenti di eliminare gli oggetti in base all'ID versione

Questo criterio di gruppo limita l'eliminazione degli oggetti con versione in base all'ID versione

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

Questo criterio bucket limiterà un utente (identificato dall'ID utente "56622399308951294926") a eliminare gli oggetti con versione in base all'ID versione

```

{
  "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"
        ]
      }
    }
  ]
}

```

Limitare il bucket a un singolo utente con accesso in sola lettura

Questo criterio consente a un singolo utente di avere accesso in sola lettura a un bucket e nega esplicitamente l'accesso a tutti gli altri utenti. Il raggruppamento delle istruzioni Nega in cima alla policy è una buona pratica per una valutazione più rapida.

```

{
  "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/*"
      ]
    }
  ]
}

```

Limitare un gruppo a una singola sottodirectory (prefisso) con accesso in sola lettura

Questo criterio consente ai membri del gruppo di accedere in sola lettura a una sottodirectory (prefisso) all'interno di un bucket. Il nome del bucket è "studio" e la sottodirectory è "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/*"
    ]
  }
}
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.