



Procédures et exemples d'API

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Sommaire

- Procédures et exemples d'API 1
 - Tester et démontrer les options de cryptage S3 sur StorageGRID 1
 - Testez et faites une démonstration du verrouillage d'objet S3 sur StorageGRID 4
 - Exemples de règles de compartiment et de groupe (IAM) 9

Procédures et exemples d'API

Tester et démontrer les options de cryptage S3 sur StorageGRID

StorageGRID et l'API S3 proposent plusieurs façons de chiffrer vos données au repos. Pour en savoir plus, voir "[Étudiez les méthodes de cryptage StorageGRID](#)".

Ce guide présente les méthodes de chiffrement de l'API S3.

Chiffrement côté serveur (SSE)

SSE permet au client de stocker un objet et de le chiffrer à l'aide d'une clé unique gérée par StorageGRID. Lorsque l'objet est demandé, il est déchiffré par la clé stockée dans StorageGRID.

Exemple SSE

- PLACER un objet avec SSE

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

- DIRIGEZ l'objet pour vérifier le chiffrement

```
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": {}  
}
```

- OBTENIR l'objet

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

Chiffrement côté serveur avec clés fournies par le client (SSE-C)

SSE permet au client de stocker un objet et de le chiffrer à l'aide d'une clé unique fournie par le client avec l'objet. Lorsque l'objet est demandé, la même clé doit être fournie pour décrypter et renvoyer l'objet.

Exemple SSE-C.

- Vous pouvez créer une clé de chiffrement à des fins de test ou de démonstration
 - Créez une clé de chiffrement

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

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

- Placer un objet avec la clé générée

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

- Dirigez l'objet

```
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=="  
}
```



Si vous ne fournissez pas la clé de cryptage, vous recevrez une erreur « une erreur s'est produite (404) lors de l'appel de l'opération HeadObject : introuvable ».

- Obtenir l'objet

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



Si vous ne fournissez pas la clé de cryptage, vous recevrez une erreur "une erreur s'est produite (InvalidRequest) lors de l'appel de l'opération GetObject: L'objet a été stocké à l'aide d'une forme de chiffrement côté serveur. Les paramètres corrects doivent être fournis pour récupérer l'objet. »

Chiffrement côté serveur godet (SSE-S3)

SSE-S3 permet au client de définir un comportement de cryptage par défaut pour tous les objets stockés dans un compartiment. Les objets sont chiffrés avec une clé unique gérée par StorageGRID. À la demande de l'objet, celui-ci est décrypté par la clé stockée dans StorageGRID.

Exemple de godet SSE-S3

- Créez un compartiment et définissez une règle de chiffrement par défaut
 - Créer un nouveau compartiment

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

- Put bucket Encryption

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

- Placer un objet dans le godet

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

- Dirigez l'objet

```
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": "\"82e8fb872e778a4687a26e6c0b36bc1\"",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```

- OBTENIR l'objet

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

Par Aron Klein

Testez et faites une démonstration du verrouillage d'objet S3 sur StorageGRID

Le verrouillage d'objet fournit un modèle WORM pour éviter que les objets ne soient supprimés ou remplacés. L'implémentation StorageGRID du verrouillage d'objet est une fonctionnalité qui est évaluée afin de respecter les exigences réglementaires, et qui prend en charge le mode de conservation légale et de conformité pour la conservation des objets et les règles de conservation des compartiments par défaut.

Ce guide présente l'API de verrouillage d'objet S3.

Obligation légale

- La mise en attente légale de verrouillage d'objet est un état activé/désactivé simple appliqué à un objet.

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

- Vérifiez-le avec une opération GET.

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

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

- Désactiver la mise en attente légale

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

- Vérifiez-le avec une opération GET.

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

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

Mode de conformité

- La conservation de l'objet s'effectue avec une conservation jusqu'à l'horodatage.

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

- Vérifiez l'état de la rétention

```
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"
  }
}
```

Conservation par défaut

- Définissez la période de conservation en jours et années par rapport à une date de conservation définie avec l'api par objet.

```
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
```

- Vérifiez l'état de la rétention

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

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

- Placer un objet dans le godet

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

- La durée de conservation définie dans le compartiment est convertie en horodatage de conservation sur l'objet.


```
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"  
  }  
}
```

Test de la suppression d'un objet avec une rétention définie

Le verrouillage d'objet est basé sur la gestion des versions. La conservation est définie sur une version de l'objet. Si une tentative de suppression d'un objet avec une rétention définie et qu'aucune version n'est spécifiée, un marqueur de suppression est créé comme version actuelle de l'objet.

- Supprimez l'objet dont la conservation est définie

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

- Lister les objets dans le compartiment

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

- Notez que l'objet n'est pas répertorié.
- Répertorier les versions pour voir le marqueur de suppression et la version verrouillée d'origine

```
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":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
      "IsLatest": true,
      "LastModified": "2022-05-03T15:35:50.248000+00:00"
    }
  ]
}

```

- Supprimer la version verrouillée de l'objet

```

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

Exemples de règles de compartiment et de groupe (IAM)

Voici des exemples de politiques de compartiment et de règles de groupe (règles IAM).

Stratégies de groupe (IAM)

Accès au compartiment de style Home Directory

Cette stratégie de groupe autorise uniquement les utilisateurs à accéder aux objets du compartiment nommé nom d'utilisateur utilisateurs.

```
"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}/*"  
  }  
]  
}
```

Refuser la création de compartiments de verrouillage d'objet

Cette stratégie de groupe empêche les utilisateurs de créer un compartiment avec le verrouillage d'objet activé sur le compartiment.



Cette règle n'est pas appliquée dans l'interface utilisateur de StorageGRID et elle n'est appliquée que par l'API S3.

```

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

```

Limite de conservation du verrouillage des objets

Cette stratégie de compartiment limite la durée de conservation du verrouillage de l'objet à 10 jours ou moins

```

{
  "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"
        }
      }
    }
  ]
}

```

Empêcher les utilisateurs de supprimer des objets par ID de version

Cette stratégie de groupe empêche les utilisateurs de supprimer des objets multiversion par ID de version

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

Cette stratégie de compartiment empêche un utilisateur (identifié par l'ID utilisateur « 56622399308951294926 ») de supprimer des objets multiversion par l'ID de version

```

{
  "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"
        ]
      }
    }
  ]
}

```

Restriction du compartiment à un seul utilisateur avec un accès en lecture seule

Cette stratégie permet à un seul utilisateur de disposer d'un accès en lecture seule à un compartiment et d'accéder explicitement à tous les autres utilisateurs. Le regroupement des déclarations de refus en haut de la politique est une bonne pratique pour une évaluation plus rapide.

```

{
  "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/*"
      ]
    }
  ]
}

```

Limiter un groupe à un sous-répertoire unique (préfixe) avec accès en lecture seule

Cette règle permet aux membres du groupe d'accéder en lecture seule à un sous-répertoire (préfixe) au sein d'un compartiment. Le nom du compartiment est « Study » et le sous-répertoire est « 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/*"
  ]
}
]
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.