



程序和API範例

How to enable StorageGRID in your environment

NetApp
April 26, 2024

目錄

程序和API範例	1
測試並示範StorageGRID 有關支援的S3加密選項	1
測試並示範StorageGRID S3物件鎖定功能	4
範例庫與群組 (IAM) 原則	9

程序和API範例

測試並示範StorageGRID 有關支援的S3加密選項

支援的支援功能有許多不同的方法可加密閒置的資料。StorageGRID若要深入瞭解、請參閱 ["檢閱StorageGRID 功能加密方法"](#)。

本指南將示範S3 API加密方法。

伺服器端加密 (SSE)

使用者可透過sse儲存物件、並使用StorageGRID 由支援的獨特金鑰來加密物件。當物件被要求時、物件會被儲存在StorageGRID 物件中的金鑰解密。

例如

- 將物件放入SS

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

- 驗證加密的目標

```
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": {}  
}
```

- 取得物件

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

使用客戶提供的金鑰進行伺服器端加密 (SSE-C)

使用者可透過SSE儲存物件、並使用用戶端隨物件提供的唯一金鑰來加密物件。要求物件時、必須提供相同的金鑰才能解密及傳回物件。

SSE-C範例

- 為了測試或示範目的、您可以建立加密金鑰
 - 建立加密金鑰

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

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

- 使用產生的金鑰放置物件

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

- 物件的前端

```
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=="  
}
```



如果您未提供加密金鑰、您將會收到「呼叫頭物件作業時發生錯誤 (404)：找不到」錯誤訊息。

- 取得物件

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



如果您未提供加密金鑰、則會在呼叫GetObject作業時收到錯誤訊息「發生錯誤 (InvalidRequest)：該物件是使用伺服器端加密的形式儲存。必須提供正確的參數才能擷取物件。」

儲存區伺服器端加密 (SSE-S3)

SSE-S3可讓用戶端針對儲存在儲存區中的所有物件、定義預設的加密行為。物件會使用StorageGRID 由支援的獨特金鑰進行加密。當物件被要求時、物件會被儲存在StorageGRID 檔中的金鑰解密。

Bucket SSE-S3範例

- 建立新儲存區並設定預設加密原則
 - 建立新的儲存庫

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

- 將儲存區加密

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

- 將物件放入儲存區

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

- 物件的前端

```
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": {}
}
```

- 取得物件

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

_ 作者：Aron Klein _

測試並示範StorageGRID S3物件鎖定功能

物件鎖定提供WORM模型、可防止物件遭到刪除或覆寫。物件鎖定的實作係由Cohasset進行評估、以協助符合法規要求、支援合法持有和符合法規的物件保留模式、以及預設的儲存貯體保留原則。StorageGRID

本指南將示範S3物件鎖定API。

合法持有

- 物件鎖定合法保留是套用至物件的簡單開啟/關閉狀態。

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

- 使用Get作業來驗證。

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

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

- 關閉合法保留

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

- 使用Get作業來驗證。

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

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

法規遵循模式

- 物件保留會以保留直到時間戳記完成。

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

- 確認保留狀態

```
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"
  }
}
```

預設保留

- 設定保留期間（以天數和年數為單位）、並使用「每個物件API」所定義的「保留截止日期」。

```
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
```

- 確認保留狀態

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

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

- 將物件放入儲存區

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

- 儲存區上設定的保留持續時間會轉換成物件上的保留時間戳記。


```
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"  
  }  
}
```

測試刪除具有定義保留的物件

物件鎖定是建置在版本管理之上。保留是在物件的某個版本上定義。如果嘗試刪除已定義保留的物件、但未指定版本、則會建立刪除標記作為物件的目前版本。

- 刪除已定義保留的物件

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

- 列出儲存區中的物件

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

◦ 請注意、此物件並未列出。

- 列出要查看刪除標記的版本、以及原始鎖定版本

```
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"
    }
  ]
}

```

- 刪除物件的鎖定版本

```

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

```

作者：Aron Klein

範例庫與群組 (IAM) 原則

以下是庫位原則和群組原則 (IAM原則) 的範例。

群組原則 (IAM)

主目錄樣式庫存取

此群組原則僅允許使用者存取名為使用者使用者名稱之儲存區中的物件。

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

拒絕建立物件鎖定儲存區

此群組原則會限制使用者建立在貯體上啟用物件鎖定的貯體。



此原則並未在StorageGRID SUI中強制執行、只有S3 API才會強制執行。

```

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

```

物件鎖定保留限制

此 Bucket 原則將物件鎖定保留期間限制為 10 天或更短

```

{
  "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"
        }
      }
    }
  ]
}

```

限制使用者以版本 ID 刪除物件

此群組原則會限制使用者依照版本 ID 刪除版本管理的物件

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

此貯體原則會限制使用者（由使用者 ID 「56622399308951294926」識別）依版本 ID 刪除版本管理物件

```

{
  "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"
        ]
      }
    }
  ]
}

```

將儲存區限制為具有唯讀存取權的單一使用者

此原則可讓單一使用者擁有儲存區的唯讀存取權、並明確地讓Denys存取所有其他使用者。將「拒絕」陳述式分組在原則頂端、是加速評估的好做法。

```

{
  "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/*"
      ]
    }
  ]
}

```

將群組限制為具有唯讀存取權的單一子目錄（首碼）

此原則可讓群組成員對儲存庫中的子目錄（前置）擁有唯讀存取權。貯體名稱為「study」、子目錄為「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/*"
  ]
}
]
```

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。