



使用**S3 REST API**

StorageGRID 11.8

NetApp
May 10, 2024

目錄

使用S3 REST API	1
S3 REST API 支援的版本與更新	1
快速參考：支援的 S3 API 要求	3
測試 S3 REST API 組態	22
如何實作S3 REST API StorageGRID	24
支援 Amazon S3 REST API	37
StorageGRID 自訂作業	80
儲存庫和群組存取原則	99
稽核記錄中追蹤的S3作業	124

使用S3 REST API

S3 REST API 支援的版本與更新

支援簡單儲存服務 (S3) API、此API是以代表狀態傳輸 (REST) 網路服務的形式實作。StorageGRID

S3 REST API 的支援可讓您將專為 S3 Web 服務開發的服務導向應用程式、與使用 StorageGRID 系統的內部部署物件儲存設備連線。用戶端應用程式目前使用 S3 REST API 呼叫的變更最少。

支援的版本

支援下列S3和HTTP的特定版本。StorageGRID

項目	版本
S3 API 規格	"Amazon Web Services (AWS) 文件：Amazon Simple Storage Service API Reference"
HTTP	1.1. 如需HTTP的詳細資訊、請參閱HTTP / 1.1 (RFC 7230-35) 。 "IETF RFC 2616：超文字傳輸傳輸協定 (HTTP / 1.1)" 附註 StorageGRID：不支援HTTP / 1.1鋪管。

S3 REST API 支援的更新

版本	註解
11.8	已更新 S3 作業的名稱、以符合中使用的名稱 "Amazon Web Services (AWS) 文件：Amazon Simple Storage Service API Reference" 。
11.7	<ul style="list-style-type: none">• 新增 "快速參考：支援的 S3 API 要求"。• 新增對使用 S3 物件鎖定的治理模式的支援。• 新增支援 StorageGRID 專屬 x-ntap-sg-cgr-replication-status GET 物件和 HEAD 物件要求的回應標頭。此標頭提供物件的跨網格複寫狀態。• SelectObjectContent 要求現在支援 Parquet 物件。

版本	註解
11.6%	<ul style="list-style-type: none"> • 新增使用的支援 <code>partNumber</code> 取得物件和標頭物件要求中的要求參數。 • 新增S3物件鎖定的預設保留模式支援、以及儲存區層級的預設保留期間。 • 新增對的支援 <code>s3:object-lock-remaining-retention-days</code> 原則條件金鑰、可設定物件的允許保留期間範圍。 • 將單一「放置物件」作業的最大大小_建議_變更為 5 GiB (5、368,709,120 位元組)。如果您的物件大於5 GiB、請改用多部份上傳。
11.5	<ul style="list-style-type: none"> • 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • ◦ <code>Content-MD5</code> 現在已正確支援要求標頭。
11.4.11.4	<ul style="list-style-type: none"> • 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 新增了對上的儲存區通知的支援 <code>s3:ObjectRestore:Post</code> 事件類型。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增 TLS 1.3 支援
11.3%	<ul style="list-style-type: none"> • 新增支援使用客戶提供的金鑰 (SSE-C) 進行物件資料的伺服器端加密。 • 新增刪除、取得及置放資源庫生命週期作業 (僅限到期行動) 和的支援 <code>x-amz-expiration</code> 回應標頭： • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 不再支援TLS 1.1密碼。
11.2.11.2.	<p>新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。</p> <p>*附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID (包括用於自訂的版本功能) 並未變更。</p>
11.1.	<p>新增支援跨來源資源共享 (CORS)、HTTP for S3 用戶端連線至網格節點、以及儲存區的法規遵循設定。</p>
11.0%	<p>新增支援、可設定適用於儲存區的平台服務 (CloudMirror複寫、通知及Elasticsearch整合)。此外、也新增對貯體物件標記位置限制的支援、以及可用的一致性。</p>

版本	註解
10.4%	新增對ILM掃描版本設定、端點網域名稱頁面更新、原則、原則範例及PuttoverwriteObject權限中的條件和變數的支援。
10.3.1	新增版本管理支援。
10.2%	新增對群組和庫位存取原則的支援、以及多部份複本（上傳零件-複本）的支援。
10.1.1	新增多部分上傳、虛擬託管樣式要求及v4驗證的支援。
10.0%	由整個系統初始支援S3 REST API StorageGRID。目前支援的_Simple Storage Service API Reference版本為2009-03-01。

快速參考：支援的 S3 API 要求

本頁概述 StorageGRID 如何支援 Amazon Simple Storage Service （ S3 ） API 。

本頁僅包含 StorageGRID 支援的 S3 作業。



若要查看每項作業的 AWS 文件、請選取標題中的連結。

通用 URI 查詢參數和要求標頭

除非另有說明、否則支援下列常見的 URI 查詢參數：

- versionId （視物件作業需求而定）

除非另有說明、否則支援下列常見的要求標頭：

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

相關資訊

- ["S3 REST API 實作詳細資料"](#)

- ["Amazon Simple Storage Service API 參考：一般要求標頭"](#)

"AbortMultiPart上傳"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上此額外的 URI 查詢參數：

- uploadId

申請本文

無

本文檔**StorageGRID**

"多部份上傳作業"

"完成多個部分上傳"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上此額外的 URI 查詢參數：

- uploadId

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- CompleteMultipartUpload
- ETag
- Part
- PartNumber

本文檔**StorageGRID**

"完成多個部分上傳"

"CopyObject"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外標頭：

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm

- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-<metadata-name>

申請本文

無

本文檔**StorageGRID**

"CopyObject"

"建立庫位"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外標頭：

- x-amz-bucket-object-lock-enabled

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"建立多個部分上傳"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外標頭：

- Cache-Control
- Content-Disposition

- Content-Encoding
- Content-Language
- Expires
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

申請本文

無

本文檔**StorageGRID**

["建立多個部分上傳"](#)

"刪除Bucket"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

本文檔**StorageGRID**

["在貯體上作業"](#)

"刪除 BucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

["在貯體上作業"](#)

"刪除 BucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"刪除 BucketLifecycle"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

- ["在貯體上作業"](#)
- ["建立S3生命週期組態"](#)

"刪除BucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"刪除 BucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"刪除 Buckettagging"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

["在貯體上作業"](#)

"刪除物件"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

無

本文檔**StorageGRID**

["物件上的作業"](#)

"刪除物件"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

["物件上的作業"](#)

"刪除ObjectTagging"

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

["物件上的作業"](#)

"GetBucketAcl"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

- ["在貯體上作業"](#)
- ["建立S3生命週期組態"](#)

"GetBucketLocation"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

["在貯體上作業"](#)

"GetBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"GetBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"GetObject"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列其他 URI 查詢參數：

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

以及這些額外的要求標頭：

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since

- If-None-Match
- If-Unmodified-Since

申請本文

無

本文檔**StorageGRID**

"GetObject"

"GetObjectAcl"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"GetObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"[使用 S3 REST API 來設定 S3 物件鎖定](#)"

"GetObjectTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"[物件上的作業](#)"

"標題庫"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔**StorageGRID**

"[在貯體上作業](#)"

"標題物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外標頭：

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

申請本文

無

本文檔StorageGRID

"標題物件"

"列表桶"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

無

本文檔StorageGRID

[服務](#) > [ListB桶](#) 的操作

"ListMultipartUploads"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外參數：

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

申請本文

無

本文檔StorageGRID

"ListMultipartUploads"

"清單物件"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外參數：

- delimiter
- encoding-type
- marker
- max-keys
- prefix

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"清單對象V2."

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外參數：

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"ListObjectVerions"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外參數：

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"清單零件"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外參數：

- max-parts
- part-number-marker
- uploadId

申請本文

無

本文檔**StorageGRID**

["ListMultipartUploads"](#)

"PuttBucketCors"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

["在貯體上作業"](#)

"PuttBucketEncryption"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

本文檔**StorageGRID**

["在貯體上作業"](#)

"PutBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

要求內文 XML 標記

StorageGRID 支援這些要求本文 XML 標記：

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

本文檔StorageGRID

- ["在貯體上作業"](#)
- ["建立S3生命週期組態"](#)

"PutBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

要求內文 XML 標記

StorageGRID 支援這些要求本文 XML 標記：

- Event
- Filter
- FilterRule

- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

本文檔**StorageGRID**

["在貯體上作業"](#)

"PuttBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

如需受支援 JSON 本文欄位的詳細資訊、請參閱 ["使用貯體和群組存取原則"](#)。

"PutBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

要求內文 **XML** 標記

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

本文檔**StorageGRID**

["在貯體上作業"](#)

"PuttBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔StorageGRID

["在貯體上作業"](#)

"PuttBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

要求主體參數

StorageGRID 支援下列要求主體參數：

- VersioningConfiguration
- Status

本文檔StorageGRID

["在貯體上作業"](#)

"PuttObject"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列額外標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date

- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

申請本文

- 物件的二進位資料

本文檔**StorageGRID**

"PutObject"

"PutObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上此額外標頭：

- x-amz-bypass-governance-retention

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectTagging"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

["物件上的作業"](#)

"RestoreObject"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

如需受支援實體欄位的詳細資訊、請參閱 ["RestoreObject"](#)。

"選取物件內容"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求。

申請本文

如需受支援實體欄位的詳細資訊、請參閱下列內容：

- ["使用S3 Select"](#)
- ["選取物件內容"](#)

"上傳零件"

URI 查詢參數和**要求標頭**

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列其他 URI 查詢參數：

- partNumber
- uploadId

以及這些額外的**要求標頭**：

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

申請本文

- 零件的二進位資料

本文檔**StorageGRID**

"上傳零件"

"上傳PartCopy"

URI 查詢參數和要求標頭

StorageGRID 支援所有功能 [通用參數和標頭](#) 針對此要求、加上下列其他 URI 查詢參數：

- partNumber
- uploadId

以及這些額外的要求標頭：

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

申請本文

無

本文檔**StorageGRID**

"上傳PartCopy"

測試 S3 REST API 組態

您可以使用 Amazon Web Services 命令列介面（AWS CLI）來測試與系統的連線、並驗證您是否可以讀寫物件。

開始之前

- 您已從下載並安裝AWS CLI "aws.amazon.com/cli"。
- 您也可以選擇 "[已建立負載平衡器端點](#)"。否則、您就知道要連線的儲存節點 IP 位址、以及要使用的連接埠號碼。請參閱 "[用戶端連線的 IP 位址和連接埠](#)"。

- 您有 "已建立 S3 租戶帳戶"。
- 您已登入租戶和 "已建立存取金鑰"。

如需這些步驟的詳細資訊、請參閱 ["設定用戶端連線"](#)。

步驟

1. 設定 AWS CLI 設定以使用您在 StorageGRID 系統中建立的帳戶：
 - a. 進入組態模式：`aws configure`
 - b. 輸入您所建立帳戶的存取金鑰 ID。
 - c. 輸入您所建立帳戶的秘密存取金鑰。
 - d. 輸入要使用的預設區域。例如、`us-east-1`。
 - e. 輸入要使用的預設輸出格式、或按* Enter *選取Json。
2. 建立儲存庫。

本範例假設您已將負載平衡器端點設定為使用 IP 位址 10.96.101.17 和連接埠 10443。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

如果成功建立了儲存區、則會傳回儲存區的位置、如下列範例所示：

```
"Location": "/testbucket"
```

3. 上傳物件。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

如果物件上傳成功、則會傳回Etag、這是物件資料的雜湊。

4. 列出儲存區的內容、以驗證物件是否已上傳。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. 刪除物件。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. 刪除儲存庫。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

如何實作S3 REST API StorageGRID

衝突的用戶端要求

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。

「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

一致性值

一致性可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。您可以根據應用程式的需求變更一致性。

根據預設StorageGRID、此功能可確保新建立物件的寫入後讀取一致性。任何「Get」追蹤成功完成的「PUT」、都能讀取新寫入的資料。覆寫現有物件、更新中繼資料及刪除的動作最終一致。覆寫通常需要幾秒鐘或幾分鐘才能傳播、但可能需要15天的時間。

如果您想要以不同的一致性執行物件作業、您可以：

- 指定一致性 [每個貯體](#)。
- 指定一致性 [每項 API 作業](#)。
- 執行下列其中一項工作、變更預設的全網格一致性：
 - 在 Grid Manager 中、前往 * 組態 * > * 系統 * > * 儲存設定 * > * 預設一致性 *。
 - 。



對全網格一致性所做的變更僅適用於變更設定後所建立的貯體。若要判斷變更的詳細資料、請參閱位於的稽核記錄 /var/local/log（搜尋 * 一致性層級 *）。

一致性值

一致性會影響 StorageGRID 用來追蹤物件的中繼資料如何在節點之間散佈、進而影響用戶端要求的物件可用度。

您可以將貯體或 API 作業的一致性設定為下列其中一個值：

- * 全部 * : 所有節點都會立即接收資料、否則要求將會失敗。
- **Strong-global** : 保證所有網站上所有用戶端要求的寫入後讀取一致性。
- **Strong-site** : 保證網站內所有用戶端要求的寫入後讀取一致性。
- * 新寫入後讀取 * : (預設) 提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
- * 可用 * : 提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用 (例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業) 。S3 FabricPool 儲存區不支援。

使用「讀取後新寫入」和「可用」一致性

當標頭或 GET 作業使用「讀取後新寫入」一致性時、StorageGRID 會以多個步驟執行查詢、如下所示：

- 它會先使用低一致性來查詢物件。
- 如果該查詢失敗、它會在下一個一致性值重複查詢、直到達到等同於 Strong-global 行為的一致性為止。

如果 HEAD 或 GET 作業使用「讀取後新寫入」一致性、但物件不存在、則物件查詢一律會達到等同於 Strong-global 行為的一致性。由於這種一致性需要在每個站台上提供多個物件中繼資料複本、因此如果同一個站台上兩個或多個儲存節點無法使用、您可能會收到大量 500 個內部伺服器錯誤。

除非您需要與 Amazon S3 類似的一致性保證、否則您可以將一致性設定為「可用」、以防止這些錯誤發生在 HEAD 和 GET 作業中。當前端或 GET 作業使用「可用」一致性時、StorageGRID 僅提供最終一致性。它不會在增加一致性時重試失敗的作業、因此不需要物件中繼資料的多個複本。

[[API- 作業 - 一致性控制]] 指定 API 作業的一致性

若要設定個別 API 作業的一致性、作業必須支援一致性值、而且您必須在要求標頭中指定一致性。此範例會將 GetObject 作業的一致性設定為「Strong-site」。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



PutObject 和 GetObject 作業必須使用相同的一致性。

指定貯體的一致性

若要設定貯體的一致性、您可以使用 StorageGRID ["實現庫位一致性"](#) 申請。您也可以 ["改變貯體的一致性"](#) 從租戶管理器。

設定貯體的一致性時、請注意下列事項：

- 設定貯體的一致性、可決定用於在貯體或貯體組態中的物件上執行 S3 作業的一致性。它不會影響儲存庫本身的作業。
- 個別 API 作業的一致性會覆寫貯體的一致性。

- 一般而言、貯體應使用預設的一致性「讀取後新寫入」。如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、設定用戶端以指定每個 API 要求的一致性。將貯體層級的一致性設為最後的方法。

[[how – consistency – controls – and – ILM – rules – arize] 一致性和 ILM 規則如何交互以影響數據保護

您選擇的一致性和 ILM 規則都會影響物件的保護方式。這些設定可以互動。

例如、儲存物件時所使用的一致性會影響物件中繼資料的初始放置位置、而為 ILM 規則選取的擷取行為則會影響物件複本的初始放置位置。由於 StorageGRID 需要同時存取物件的中繼資料及其資料、才能滿足用戶端要求、因此針對一致性和擷取行為選擇符合的保護層級、可以提供更好的初始資料保護、以及更可預測的系統回應。

以下內容 "擷取選項" 適用於 ILM 規則：

雙重承諾

StorageGRID 會立即製作物件的臨時複本、並將成功傳回給用戶端。在 ILM 規則中指定的複本會盡可能製作。

嚴格

在 ILM 規則中指定的所有複本都必須在成功傳回用戶端之前製作。

平衡

StorageGRID 會嘗試在擷取時製作 ILM 規則中指定的所有複本；如果不可能、則會製作過渡複本、並將成功傳回用戶端。ILM 規則中指定的複本會盡可能製作。

一致性與 ILM 規則如何互動的範例

假設您有一個雙站台網格、其中包含下列 ILM 規則及下列一致性：

- * ILM 規則*：建立兩個物件複本、一個在本機站台、一個在遠端站台。使用嚴格的擷取行為。
- * 一致性*：強式全域（物件中繼資料會立即發佈至所有站台）。

當用戶端將物件儲存到網格時、StorageGRID 在成功傳回用戶端之前、功能區會同時複製物件並將中繼資料散佈到兩個站台。

在擷取最成功的訊息時、物件會受到完整保護、不會遺失。例如、如果在擷取後不久即遺失本機站台、則物件資料和物件中繼資料的複本仍存在於遠端站台。物件可完全擷取。

如果您改用相同的 ILM 規則和強大的站台一致性、則在物件資料複寫到遠端站台、但在物件中繼資料散佈到該站台之前、用戶端可能會收到成功訊息。在此情況下、物件中繼資料的保護層級與物件資料的保護層級不符。如果在擷取後不久本機站台便會遺失、則物件中繼資料將會遺失。無法擷取物件。

一致性與 ILM 規則之間的相互關係可能很複雜。如需協助、請聯絡 NetApp。

物件版本管理

如果您要保留每個物件的多個版本、可以設定貯體的版本設定狀態。啟用貯體版本設定有助於防止意外刪除物件、並可讓您擷取及還原物件的舊版。

支援大部分功能的支援功能、以及部分限制、可讓整個系統執行版本管理。StorageGRID 支援多達 1、000 個版

本的每個物件。StorageGRID

物件版本管理可與StorageGRID 資訊的生命週期管理 (ILM) 或S3生命週期組態結合使用。您必須明確啟用每個儲存區的版本設定。當貯體啟用版本設定時、新增至貯體的每個物件都會指派版本 ID、由 StorageGRID 系統產生。

不支援使用MFA (多因素驗證) 刪除。



版本管理只能在StorageGRID 以不含更新版本的版本資訊版本10.3所建立的儲存庫上啟用。

ILM與版本管理

ILM原則會套用至物件的每個版本。ILM掃描程序會持續掃描所有物件、並根據目前的ILM原則重新評估這些物件。您對ILM原則所做的任何變更、都會套用至所有先前擷取的物件。如果啟用版本管理、則包括先前擷取的版本。ILM掃描會將新的ILM變更套用至先前擷取的物件。

對於啟用版本設定的儲存區中的 S3 物件、版本設定支援可讓您建立使用「非目前時間」做為參考時間的 ILM 規則 (針對「僅將此規則套用至舊版物件？」這個問題、請選取 * 是 *。在中 "[建立 ILM 規則精靈的步驟 1](#)")。更新物件時、其舊版本會變成非最新版本。使用「非目前時間」篩選器可讓您建立原則、以減少舊版物件的儲存影響。



當您使用多部分上傳作業上傳物件的新版本時、原始版本物件的非目前時間會反映新版本的多部分上傳時間、而非多部分上傳完成時。在有限的情況下、原始版本的非目前時間可能比目前版本的時間早上幾小時或幾天。

相關資訊

- "[如何刪除S3版本控制物件](#)"
- "[S3版本化物件的ILM規則和原則 \(範例4\)](#)"。

使用 **S3 REST API** 來設定 **S3** 物件鎖定

如果 StorageGRID 系統已啟用全域 S3 物件鎖定設定、您可以在啟用 S3 物件鎖定的情況下建立儲存區。您可以針對每個物件版本、指定每個儲存區或保留設定的預設保留。

如何為貯體啟用 **S3** 物件鎖定

如果StorageGRID 您的整個S3物件鎖定設定已啟用、則您可以在建立每個儲存區時、選擇性地啟用S3物件鎖定。

S3 物件鎖定是永久性設定、只有在建立貯體時才能啟用。建立貯體後、您無法新增或停用 S3 物件鎖定。

若要為貯體啟用 S3 物件鎖定、請使用下列其中一種方法：

- 使用租戶管理程式建立桶。請參閱 "[建立S3儲存區](#)"。
- 使用的 CreateBucket 要求建立貯體 `x-amz-bucket-object-lock-enabled` 要求標頭：請參閱 "[在貯體上作業](#)"。

S3 物件鎖定需要儲存區版本設定、此功能會在建立儲存區時自動啟用。您無法暫停儲存區的版本設定。請參閱 "[物件版本管理](#)"。

貯體的預設保留設定

為貯體啟用 S3 物件鎖定時、您可以選擇性地啟用貯體的預設保留、並指定預設保留模式和預設保留期間。

預設保留模式

- 在法規遵循模式中：
 - 直到達到物件的保留日期、才能刪除物件。
 - 物件的保留日期可以增加、但不能減少。
 - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
 - 的使用者 `s3:BypassGovernanceRetention` 權限可以使用 `x-amz-bypass-governance-retention: true` 要求標頭略過保留設定。
 - 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
 - 這些使用者可以增加、減少或移除物件的保留到目前為止。

預設保留期間

每個貯體都可以有一段以年或日為單位指定的預設保留期間。

如何設定貯體的預設保留

若要設定貯體的預設保留、請使用下列其中一種方法：

- 從 Tenant Manager 管理貯體設定。請參閱 ["建立S3儲存區"](#) 和 ["更新 S3 物件鎖定預設保留"](#)。
- 針對貯體發出 `PutObjectLockConfiguration` 要求、以指定預設模式和預設天數或年數。

PutObjectLockConfiguration

`PutObjectLockConfiguration` 要求可讓您設定及修改已啟用 S3 物件鎖定的儲存區的預設保留模式和預設保留期間。您也可以移除先前設定的預設保留設定。

將新物件版本擷取至貯體時、會套用預設保留模式 `x-amz-object-lock-mode` 和 `x-amz-object-lock-retain-until-date` 未指定。預設保留期間用於計算截止日期 IF `x-amz-object-lock-retain-until-date` 未指定。

如果在擷取物件版本之後修改預設保留期間、則物件版本的保留截止日期將維持不變、且不會使用新的預設保留期間重新計算。

您必須擁有 `s3:PutBucketObjectLockConfiguration` 完成此作業的權限、或是帳戶根目錄。

- `Content-MD5` 必須在 PUT 要求中指定要求標頭。

申請範例

此範例可為貯體啟用 S3 物件鎖定、並將預設保留模式設為符合法規、並將預設保留期間設為 6 年。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

如何決定貯體的預設保留

若要判斷儲存區是否啟用 S3 物件鎖定、並查看預設保留模式和保留期間、請使用下列其中一種方法：

- 在租戶管理器中檢視貯體。請參閱 ["檢視 S3 儲存區"](#)。
- 發出 `GetObjectLockConfiguration` 要求。

GetObjectLockConfiguration

`GetObjectLockConfiguration` 要求可讓您判斷儲存區是否已啟用 S3 物件鎖定、如果已啟用、請查看儲存區是否已設定預設保留模式和保留期間。

將新物件版本擷取至貯體時、會套用預設保留模式 `x-amz-object-lock-mode` 未指定。預設保留期間用於計算截止日期 IF `x-amz-object-lock-retain-until-date` 未指定。

您必須擁有 `s3:GetBucketObjectLockConfiguration` 完成此作業的權限、或是帳戶根目錄。

申請範例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

回應範例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

如何指定物件的保留設定

啟用 S3 物件鎖定的貯體可包含物件組合、並具有或不含 S3 物件鎖定保留設定。

物件層級保留設定是使用 S3 REST API 指定的。物件的保留設定會覆寫貯體的任何預設保留設定。

您可以為每個物件指定下列設定：

- * 保留模式 *：法規遵循或治理。
- * 截止日期 *：指定 StorageGRID 必須保留物件版本多久的日期。
 - 在規範模式中、如果保留截止日期是未來、則可以擷取物件、但無法修改或刪除物件。保留截止日期可以增加、但無法減少或移除此日期。
 - 在治理模式中、具有特殊權限的使用者可以略過保留到最新的設定。他們可以在物件版本的保留期間結

束之前刪除物件版本。他們也可以增加、減少或甚至移除截止日期的保留。

- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。

物件的合法保留設定不受保留模式和保留截止日期的影響。如果物件版本處於合法保留狀態、則沒有人可以刪除該版本。

若要在將物件版本新增至貯體時指定 S3 物件鎖定設定、請發出 "PutObject"、"CopyObject" 或 "建立多個部分上傳" 申請。

您可以使用下列項目：

- `x-amz-object-lock-mode`，可以是法規遵循或治理（區分大小寫）。



如果您指定 `x-amz-object-lock-mode`，您也必須指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
 - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
 - 保留截止日期必須為未來日期。
- `x-amz-object-lock-legal-hold`

如果已開啟合法持有（區分大小寫）、則物件將置於合法持有之下。如果法律保留已關閉、則不會保留任何合法的保留。任何其他值都會導致400個錯誤要求（InvalidArgument）錯誤。

如果您使用上述任一要求標頭、請注意下列限制：

- `Content-MD5` 如有任何要求、則要求標頭為必填欄位 `x-amz-object-lock-* PutObject` 要求中存在要求標頭。`Content-MD5` 複製物件或 `CreateMultipartUpload` 不需要。
- 如果儲存區未啟用S3物件鎖定和 `x-amz-object-lock-*` 出現要求標頭、傳回400個錯誤要求（InvalidRequest）錯誤。
- `PutObject` 要求支援使用 `x-amz-storage-class: REDUCED_REDUNDANCY` 以符合AWS行為。然而、當物件被擷取至啟用S3物件鎖定的儲存區時`StorageGRID`、則會一律執行雙重認可擷取。
- 後續的 `Get` 或 `HeadObject` 版本回應將包含標頭 `x-amz-object-lock-mode`、`x-amz-object-lock-retain-until-date` 和 `x-amz-object-lock-legal-hold`（如果已設定）以及要求傳送者是否正確 `s3:Get*` 權限：

您可以使用 `s3:object-lock-remaining-retention-days` 原則條件金鑰、可限制物件的最小和最大允許保留期間。

如何更新物件的保留設定

如果您需要更新現有物件版本的合法保留或保留設定、可以執行下列物件子資源作業：

- `PutObjectLegalHold`

如果新的合法持有值已開啟、則物件將置於合法持有之下。如果合法持有值為「關」、則合法持有將被解除。

- PutObjectRetention
 - 模式值可以是法規遵循或治理（區分大小寫）。
 - 保留截止日期值必須採用格式 2020-08-10T21:46:00Z。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
 - 如果物件版本有現有的截至日期保留、您只能增加。新的價值必須是未來的價值。

如何使用治理模式

擁有的使用者 s3:BypassGovernanceRetention 權限可以略過使用治理模式之物件的作用中保留設定。任何刪除或 PutObjectRetention 作業都必須包含 x-amz-bypass-governance-retention:true 要求標頭：這些使用者可以執行這些額外作業：

- 執行 DeleteObject 或 DeleteObjects 作業、以在物件版本的保留期間結束之前刪除物件版本。
合法持有的物件無法刪除。合法持有必須關閉。
- 在物件的保留期間結束之前、執行 PutObjectRetention 作業、將物件版本的模式從治理模式變更為法規遵循模式。
永遠不允許將模式從法規遵循變更為治理。
- 執行 PutObjectRetention 作業以增加、減少或移除物件版本的保留期間。

相關資訊

- ["使用S3物件鎖定來管理物件"](#)
- ["使用 S3 物件鎖定來保留物件"](#)
- ["Amazon簡易儲存服務使用者指南：使用S3物件鎖定"](#)

建立S3生命週期組態

您可以建立S3生命週期組態、以控制何時從StorageGRID 作業系統刪除特定物件。

本節的簡單範例說明S3生命週期組態如何控制從特定S3儲存區刪除（過期）特定物件的時間。本節範例僅供說明用途。如需建立S3生命週期組態的完整詳細資料、請參閱 ["Amazon Simple Storage Service 使用者指南：物件生命週期管理"](#)。請注意StorageGRID、僅支援過期行動、不支援轉換行動。

什麼是生命週期組態

生命週期組態是套用至特定S3儲存區中物件的一組規則。每個規則都會指定受影響的物件、以及這些物件何時到期（在特定日期或幾天之後）。

在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素：

- 過期：在達到指定日期或達到指定天數時刪除物件、從擷取物件開始算起。
- 非目前版本過期：在達到指定天數時刪除物件、從物件變成非目前的開始算起。

- 篩選器（前置、標記）
- 狀態
- ID

每個物件都遵循 S3 儲存區生命週期或 ILM 原則的保留設定。當 S3 貯體生命週期設定完成時、生命週期到期動作會覆寫符合貯體生命週期篩選器之物件的 ILM 原則。不符合貯體生命週期篩選器的物件、會使用 ILM 原則的保留設定。如果物件符合貯體生命週期篩選器、且未明確指定到期動作、則不會使用 ILM 原則的保留設定、而且會暗示物件版本會永遠保留。請參閱 "[S3 儲存區生命週期和 ILM 原則的優先順序範例](#)"。

因此、即使 ILM 規則中的放置指示仍套用至物件、也可能從網格中移除物件。或者、即使物件的任何 ILM 放置指示失效、物件仍可能保留在網格上。如需詳細資訊、請參閱 "[ILM 在物件生命週期內的運作方式](#)"。



庫位生命週期組態可搭配已啟用 S3 物件鎖定的庫位使用、但庫位生命週期組態不支援舊型符合標準的庫位。

支援使用下列庫位作業來管理生命週期組態：StorageGRID

- 刪除 BucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

建立生命週期組態

建立生命週期組態的第一步、就是建立一個包含一或多個規則的 Json 檔案。例如、此 Json 檔案包含三個規則、如下所示：

1. 規則 1 僅適用於符合前置碼的物件 category1/ 而且有 key2 的價值 tag2。Expiration 參數指定符合篩選條件的物件將於 2020 年 8 月 22 日午夜到期。
2. 規則 2 僅適用於符合前置碼的物件 category2/。Expiration 參數指定符合篩選條件的物件在擷取後 100 天過期。



指定天數的規則是相對於擷取物件的時間。如果目前日期超過擷取日期加上天數、則在套用生命週期組態後、部分物件可能會立即從儲存庫中移除。

3. 規則 3 僅適用於符合前置碼的物件 category3/。Expiration 參數指定任何非目前版本的相符物件在變成非目前物件 50 天後過期。

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

將生命週期組態套用至貯體

建立生命週期組態檔案之後、您可以發出 `PutBucketLifecycleConfiguration` 要求、將其套用至儲存庫。

此要求會將範例檔案中的生命週期組態套用至名為的儲存區中的物件 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

若要驗證已成功將生命週期組態套用至貯體、請發出 `GetBucketLifecycleConfiguration` 要求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

成功的回應會列出您剛套用的生命週期組態。

驗證目標是否適用庫位生命週期到期

您可以在發出 `PutObject`、`HeadObject` 或 `GetObject` 要求時、判斷生命週期組態中的到期規則是否適用於特定物件。如果適用規則、回應會包含 `Expiration` 指出物件到期時間及符合到期規則的參數。



因為儲存區生命週期會取代 ILM `expiry-date` 顯示的是物件刪除的實際日期。如需詳細資訊、請參閱 ["如何判斷物件保留"](#)。

例如、本 `PutObject` 申請於 2020 年 6 月 22 日發出、並在中放置物件 `testbucket` 鏟斗。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功回應表示物件將在 100 天（2020 年 10 月 1 日）後過期、且符合生命週期組態的規則 2。

```
{
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\" , rule-id=\"rule2\" ,
  ETag: "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如、此 `HeadObject` 要求用於取得 `testBucket` 儲存區中相同物件的中繼資料。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功回應包括物件的中繼資料、指出物件將在100天內過期、且符合規則2。

```
{
  "AcceptRanges": "bytes",
  *Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



對於啟用版本控制的儲存區、`x-amz-expiration` 回應標頭僅適用於物件的目前版本。

實作S3 REST API的建議

實作S3 REST API以搭配StorageGRID 使用時、請遵循以下建議。

針對不存在物件的使用者提出建議

如果您的應用程式會定期檢查某個物件是否存在於您不希望該物件實際存在的路徑、您應該使用「可用」**一致性**。例如、如果您的應用程式在放置前先找到某個位置、則應使用「可用」一致性。

否則、如果前端作業找不到物件、如果同一站台上有一個或多個儲存節點無法使用、或遠端站台無法連線、您可能會收到大量 500 個內部伺服器錯誤。

您可以使用設定每個貯體的「可用」一致性 **實現庫位一致性** 或者、您也可以在各別 API 作業的要求標頭中指定一致性。

物件金鑰建議

請根據第一次建立貯體的時間、遵循下列物件金鑰名稱建議。

在 **StorageGRID 11.4** 或更早版本中建立的貯體

- 請勿使用隨機值做為物件金鑰的前四個字元。這與前AWS關於金鑰前置碼的建議不同。請改用非隨機、非唯一的前置字元、例如 `image`。
- 如果您遵循前 AWS 的建議、在金鑰首碼中使用隨機和唯一字元、請在物件金鑰前加上目錄名稱。也就是使用此格式：

```
mybucket/mydir/f8e3-image3132.jpg
```

而非此格式：

```
mybucket/f8e3-image3132.jpg
```

在 **StorageGRID 11.4** 或更新版本中建立的貯體

不需要限制物件金鑰名稱以符合效能最佳實務做法。在大多數情況下、您可以對物件金鑰名稱的前四個字元使用隨機值。



S3 工作負載的例外情況是、它會在一段短時間後持續移除所有物件。為了將此使用案例的效能影響降至最低、請將金鑰名稱的前置部分變更為每數千個物件、例如日期。例如、假設 S3 用戶端通常每秒寫入 2、000 個物件、而 ILM 或儲存庫生命週期原則則會在三天後移除所有物件。若要將效能影響降至最低、您可以使用如下模式命名金鑰：`/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

「範圍讀取」建議

如果是 "[用於壓縮儲存物件的全域選項](#)" 啟用後、S3 用戶端應用程式應避免執行 GetObject 作業、以指定要傳回的位元組範圍。這些「範圍讀取」作業效率不彰、因為 StorageGRID 必須有效地解壓縮物件以存取要求的位元組。從非常大的物件要求少量位元組的 GetObject 作業尤其缺乏效率、例如從 50 GB 壓縮物件讀取 10 MB 範圍是效率不彰的。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。



如果您需要壓縮物件、而用戶端應用程式必須使用範圍讀取、請增加應用程式的讀取逾時。

支援 Amazon S3 REST API

S3 REST API 實作詳細資料

此系統實作簡單儲存服務API (API版本2002-03)、支援大部分作業、並有一些限制。StorageGRID整合S3 REST API用戶端應用程式時、您必須瞭解實作詳細資料。

支援虛擬託管型要求和路徑型要求的支援。StorageGRID

日期處理

S3 REST API的支援僅支援有效的HTTP日期格式。StorageGRID

支援此功能的僅支援接受日期值的任何標頭的有效HTTP日期格式。StorageGRID日期的時間部分可以格林尼治標準時間 (GMT) 格式指定、或以通用協調時間 (UTC) 格式指定、且無時區偏移 (必須指定+0000)。如果您包含 `x-amz-date` 標頭在您的要求中、會覆寫在「日期」要求標頭中指定的任何值。使用AWS簽名版本4時 `x-amz-date` 由於不支援日期標頭、因此標頭必須存在於簽署的要求中。

一般要求標頭

StorageGRID 系統支援定義的一般要求標頭 "[Amazon Simple Storage Service API 參考：一般要求標頭](#)"、但有一項例外。

要求標頭	實作
授權	完整支援AWS簽名版本2 支援AWS簽名版本4、但有下列例外： <ul style="list-style-type: none"> • SHA256值不會針對申請本文進行計算。使用者提交的值會在未經驗證的情況下接受、如同值一樣 <code>UNSIGNED-PAYLOAD</code> 已提供給 <code>x-amz-content-sha256</code> 標頭。
X-amz-security-token	未實作。退貨 <code>XNotImplemented</code> 。

通用回應標頭

支援所有由 `_Simple Storage Service API Reference`（簡易儲存服務API參考）定義的通用回應標頭、但有一項例外。StorageGRID

回應標頭	實作
X-amz-id-2	未使用

驗證要求

支援使用S3 API驗證和匿名存取物件的功能。StorageGRID

S3 API支援驗證S3 API要求的簽名版本2和簽名版本4。

驗證的要求必須使用您的存取金鑰ID和秘密存取金鑰來簽署。

支援兩種驗證方法：`HTTP StorageGRID Authorization` 標頭及使用查詢參數。

使用HTTP授權標頭

`HTTP Authorization` 標頭會被所有S3 API作業使用、但資源庫原則允許的匿名要求除外。
`Authorization` 標頭包含驗證要求所需的所有簽署資訊。

使用查詢參數

您可以使用查詢參數將驗證資訊新增至URL。這稱為URL預先簽署、可用來授予特定資源的暫時存取權。具有預先簽署 URL 的使用者不需要知道密碼存取金鑰即可存取資源、這可讓您提供第三方受限存取資源。

服務營運

支援下列服務作業的支援。StorageGRID

營運	實作
列表桶 (先前命名的 Get Service)	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
取得儲存使用量	StorageGRID "取得儲存使用量" 要求會告訴您帳戶使用的儲存空間總量、以及與帳戶相關的每個儲存區。這是服務上的作業、其路徑為/和自訂查詢參數 (?x-ntap-sg-usage) 新增。
選項/	用戶端應用程式可能會發生問題 OPTIONS / 要求儲存節點上的S3連接埠、但不提供S3驗證認證、以判斷儲存節點是否可用。您可以使用此要求進行監控、或允許外部負載平衡器識別儲存節點何時當機。

在貯體上作業

這個系統最多可為每個S3租戶帳戶支援1、000個貯體。StorageGRID

貯體名稱限制遵循 AWS 美國標準地區限制、但您應進一步將它們限制在 DNS 命名慣例、以支援 S3 虛擬託管式要求。

如需詳細資訊、請參閱下列內容：

- ["Amazon Simple Storage Service 使用者指南：貯體限制與限制"](#)
- ["設定 S3 端點網域名稱"](#)

ListObjects (Get Bucket) 和 ListObjectVerions (Get Bucket 物件版本) 作業支援 StorageGRID "一致性值"。

您可以檢查是否為個別的儲存區啟用或停用上次存取時間的更新。請參閱 ["取得時段上次存取時間"](#)。

下表說明StorageGRID 了為什麼由Ss哪些 人執行S3 REST API貯體作業。若要執行上述任何作業、必須為帳戶提供必要的存取認證資料。

營運	實作
建立庫位	<p>建立新的貯體。建立貯體後、您就成為了貯體的擁有者。</p> <ul style="list-style-type: none"> • 庫位名稱必須符合下列規則： <ul style="list-style-type: none"> ◦ 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 ◦ 必須符合DNS規範。 ◦ 必須包含至少3個字元、且不得超過63個字元。 ◦ 可以是一或多個標籤的系列、相鄰的標籤以句點分隔。每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 ◦ 不得看起來像是文字格式的IP位址。 ◦ 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 • 根據預設、會在中建立儲存區 <code>us-east-1</code> 區域；不過、您可以使用 <code>LocationConstraint</code> 要求主體中的要求元素、以指定不同的區域。使用時 <code>LocationConstraint</code> 元素、您必須指定已使用Grid Manager或Grid Management API定義的區域確切名稱。如果您不知道應該使用的地區名稱、請聯絡您的系統管理員。 • 附註 *：如果您的 <code>CreateBucket</code> 要求使用的區域尚未在 StorageGRID 中定義、則會發生錯誤。 • 您可以加入 <code>x-amz-bucket-object-lock-enabled</code> 要求標頭以建立啟用S3物件鎖定的儲存區。請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。 <p>建立儲存區時、您必須啟用S3物件鎖定。建立貯體後、您無法新增或停用 S3 物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。</p>
刪除Bucket	刪除貯體。
刪除 BucketCors	刪除貯體的 CORS 組態。
刪除 BucketEncryption	刪除儲存區中的預設加密。現有的加密物件會保持加密狀態、但新增至儲存庫的任何新物件都不會加密。
刪除 BucketLifecycle	從貯體刪除生命週期組態。請參閱 " 建立S3生命週期組態 "。
刪除BucketPolicy	刪除附加至貯體的原則。
刪除 BucketReplication	刪除附加至貯體的複寫組態。

營運	實作
刪除 Bucket tagging	<p>使用 tagging SubResource 可移除庫位中的所有標記。</p> <ul style="list-style-type: none"> • 注意 * : 如果為此貯體設定非預設的 ILM 原則標籤、則會有一個 NTAP-SG-ILM-BUCKET-TAG 指定值的貯體標記。如果有、請勿發出刪除標記要求 NTAP-SG-ILM-BUCKET-TAG 貯體標記。請改為僅使用發出 PutBucketTagging NTAP-SG-ILM-BUCKET-TAG 標記及其指定值、以移除貯體中的所有其他標記。請勿修改或移除 NTAP-SG-ILM-BUCKET-TAG 貯體標記。
GetBucketAcl	傳回正面回應、以及貯體擁有者的 ID、DisplayName 和權限、表示擁有者擁有該貯體的完整存取權。
GetBucketCors	傳回 cors 鏟斗組態。
GetBucketEncryption	傳回儲存區的預設加密組態。
GetBucketLifecycleConfiguration (先前命名的 Get Bucket 生命週期)	傳回貯體的生命週期組態。請參閱 "建立 S3 生命週期組態" 。
GetBucketLocation	傳回使用設定的區域 LocationConstraint CreateBucket 要求中的元素。如果庫位所在的區域是 us-east-1，則會傳回區域的空白字串。
GetBucketNotificationConfiguration (先前命名的 Get Bucket 通知)	傳回附加至貯體的通知組態。
GetBucketPolicy	傳回附加至貯體的原則。
GetBucketReplication	傳回附加至貯體的複寫組態。
GetBucketTagging	<p>使用 tagging SubResource 可傳回某個儲存區的所有標記。</p> <ul style="list-style-type: none"> • 注意 * : 如果為此貯體設定非預設的 ILM 原則標籤、則會有一個 NTAP-SG-ILM-BUCKET-TAG 指定值的貯體標記。請勿修改或移除此標記。

營運	實作
GetBucketVersion	<p>此實作使用 <code>versioning</code> SubResource可傳回儲存區的版本管理狀態。</p> <ul style="list-style-type: none"> • <code>_ 空白 _</code>：版本設定從未啟用（儲存庫「未版本化」） • 已啟用：已啟用版本管理 • 已暫停：先前已啟用版本管理、並已暫停
GetObjectLockConfiguration	<p>如果已設定、則會傳回儲存區預設保留模式和預設保留期間。</p> <p>請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。</p>
標題庫	<p>決定貯體是否存在、且您有存取權限。</p> <p>此作業會傳回：</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>：UUID 格式的儲存區 UUID。 • <code>x-ntap-sg-trace-id</code>：關聯請求的唯一跟蹤 ID。
ListObjects 和 ListObjectsV2 (先前命名的 GET Bucket)	<p>傳回貯體中的部分或全部物件（最多 1、000 個物件）。物件的儲存類別可以有兩個值之一、即使物件是使用擷取的 <code>REDUCED_REDUNDANCY</code> 儲存類別選項：</p> <ul style="list-style-type: none"> • <code>STANDARD</code>（表示物件儲存在儲存節點所組成的儲存資源池中）。 • <code>GLACIER</code>、表示物件已移至Cloud Storage Pool指定的外部儲存區。 <p>如果儲存區包含大量具有相同前置碼的刪除金鑰、回應可能會包含部分金鑰 <code>CommonPrefixes</code> 不包含金鑰。</p>
ListObjectVersions (先前命名的 Get Bucket 物件版本)	<p>在貯體上具有讀取存取權、可搭配使用此作業 <code>versions</code> 子資源會列出儲存區中所有物件版本的中繼資料。</p>
PutBucketCors	<p>設定貯體的 CORS 組態、以便該貯體能夠處理跨來源要求。跨來源資源共用 (CORS) 是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的S3儲存區 <code>images</code> 儲存圖形。設定的CORS 組態 <code>images</code> 儲存庫、您可以讓該儲存庫中的影像顯示在網站上 <code>http://www.example.com</code>。</p>
PutBucketEncryption	<p>設定現有儲存區的預設加密狀態。啟用桶層級加密時、任何新增至桶的新物件都會加密。StorageGRID支援使用StorageGRID管理的金鑰進行伺服器端加密。指定伺服器端加密組態規則時、請設定 <code>SSEAlgorithm</code> 參數至 <code>AES256</code>、請勿使用 <code>KMSMasterKeyID</code> 參數。</p> <p>如果物件上傳要求已指定加密（亦即、如果要求包含、則會忽略儲存區預設加密組態 <code>x-amz-server-side-encryption-*</code> 要求標頭）。</p>

營運	實作
PutBucketLifecycleConfiguration (先前命名的 Put Bucket 生命週期)	<p>為貯體建立新的生命週期組態、或取代現有的生命週期組態。在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素：</p> <ul style="list-style-type: none"> • 到期 (天數、日期、 ExpiredObjectDeleteMarker) • 非目前版本到期 (NewerNoncurrentVersions 、 NoncurrentDays) • 篩選器 (前置、標記) • 狀態 • ID <p>不支援下列動作：StorageGRID</p> <ul style="list-style-type: none"> • AbortIncompleteMultiPart上傳 • 移轉 <p>請參閱 "建立S3生命週期組態"。若要瞭解貯體生命週期中的到期動作如何與 ILM 放置指示互動、請參閱 "ILM如何在整個物件生命週期內運作"。</p> <p>附註：鏟斗生命週期組態可搭配已啟用S3物件鎖定的鏟斗使用、但舊型符合標準的鏟斗不支援鏟斗生命週期組態。</p>

營運	實作
<p>PutBucketNotificationConfiguration</p> <p>(先前命名的 Put Bucket 通知)</p>	<p>使用要求主體中的通知組態 XML 來設定貯體通知。您應該瞭解下列實作詳細資料：</p> <ul style="list-style-type: none"> • StorageGRID 支援 Amazon Simple Notification Service (Amazon SNS) 或 Kafka 主題做為目的地。不支援 Simple Queue Service (SQS) 或 Amazon Lambda 端點。 • 通知的目的地必須指定為StorageGRID 一個端點的URN。端點可以使用租戶管理程式或租戶管理API來建立。 <p>端點必須存在、通知組態才能成功。如果端點不存在、則為 400 Bad Request 程式碼傳回錯誤 InvalidArgument。</p> <ul style="list-style-type: none"> • 您無法設定下列事件類型的通知。這些事件類型*不支援*。 <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • 從 StorageGRID 傳送的事件通知使用標準 JSON 格式、但不包含某些金鑰、也不為其他金鑰使用特定值、如下表所示： <ul style="list-style-type: none"> ◦ 事件來源 <pre>sgws:s3</pre> ◦ * awsRegion * <p>不含</p> ◦ * X-amz-id-2* <p>不含</p> ◦ * arn* <pre>urn:sgws:s3:::bucket_name</pre>
PutBucketPolicy	<p>設定附加至貯體的原則。請參閱 "使用貯體和群組存取原則"。</p>

營運	實作
PutBucketReplication	<p>組態 "StorageGRID CloudMirror 複寫" 適用於要求主體中所提供的複寫組態 XML 的貯體。對於CloudMirror複寫、您應該瞭解下列實作詳細資料：</p> <ul style="list-style-type: none"> • 僅支援複寫組態的V1。StorageGRID這表示StorageGRID、不支援使用 Filter 規則元素、並遵循刪除物件版本的V1慣例。如需詳細資訊、請參閱 "Amazon Simple Storage Service 使用者指南：複寫組態"。 • 儲存區複寫可在版本控制或未版本控制的儲存區上進行設定。 • 您可以在複寫組態XML的每個規則中指定不同的目的地儲存區。來源儲存區可複寫至多個目的地儲存區。 • 目的地貯體必須指定為StorageGRID 租戶管理程式或租戶管理API中指定的非功能性端點的URN。請參閱 "設定CloudMirror複寫"。 <p>複寫組態必須存在端點才能成功。如果端點不存在、則要求會以的形式失敗 400 Bad Request。錯誤訊息指出：Unable to save the replication policy. The specified endpoint URN does not exist: URN.</p> <ul style="list-style-type: none"> • 您不需要指定 Role 在組態XML中。此值不供StorageGRID Some使用、如果提交、將會忽略此值。 • 如果您從組態XML中省略儲存類別、StorageGRID 則無法使用 STANDARD 預設為儲存類別。 • 如果您從來源儲存區刪除物件、或是刪除來源儲存區本身、跨區域複寫行為如下： <ul style="list-style-type: none"> ◦ 如果您在物件或貯體複寫之前刪除該物件或貯體、則不會複寫該物件 / 貯體、也不會通知您。 ◦ 如果您在複寫物件或儲存區之後將其刪除、StorageGRID 則針對跨區域複寫的V1、執行標準Amazon S3刪除行為。
PutBucketTagging	<p>使用 tagging 子資源：新增或更新一組庫位的標記。新增庫位標記時、請注意下列限制：</p> <ul style="list-style-type: none"> • 支援每個儲存區最多50個標籤的支援功能包括：StorageGRID • 與庫位關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元。 • 標記值長度最多可達256個UNICODE字元。 • 金鑰和值區分大小寫。 • 注意 *：如果為此貯體設定非預設的 ILM 原則標籤、則會有一個 NTAP-SG-ILM-BUCKET-TAG 指定值的貯體標記。請確定 NTAP-SG-ILM-BUCKET-TAG 貯體標記包含在所有 PutBucketTagged 要求中的指定值中。請勿修改或移除此標記。 • 附註 *：此作業將覆寫貯體已有的任何目前標記。如果集合中遺漏任何現有標記、則會移除該貯體的這些標記。

營運	實作
PutBucketVersion	<p>使用 <code>versioning SubResource</code> 可設定現有儲存區的版本管理狀態。您可以使用下列其中一個值來設定版本設定狀態：</p> <ul style="list-style-type: none"> • 已啟用：啟用儲存區中物件的版本管理。新增至儲存庫的所有物件都會收到唯一的版本ID。 • 暫停：停用儲存區中物件的版本設定。新增至儲存庫的所有物件都會收到版本ID <code>null</code>。
PutObjectLockConfiguration	<p>設定或移除貯體預設保留模式和預設保留期間。</p> <p>如果修改了預設保留期間、現有物件版本的保留截止日期將維持不變、且不會使用新的預設保留期間重新計算。</p> <p>請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以取得詳細資訊。</p>

物件上的作業

物件上的作業

本節說明StorageGRID 此「物件」的「物件」功能如何執行S3 REST API作業。

下列條件適用於所有物件作業：

- StorageGRID "[一致性值](#)" 受物件上的所有作業支援、但下列項目除外：
 - `GetObjectAcl`
 - `OPTIONS /`
 - `PutObjectLegalHold`
 - `PutObjectRetention`
 - 選取物件內容
- 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMWare系統完成指定的要求、而非S3用戶端開始作業的時間。
- 所有物件均由庫位擁有者擁有、包括匿名使用者或其他帳戶所建立的物件。StorageGRID
- 透過 Swift 擷取至 StorageGRID 系統的資料物件無法透過 S3 存取。

下表說明StorageGRID 了Ss哪些 物件是由S3 REST API物件執行。

營運	實作
刪除物件	<p>多因素驗證 (MFA) 和回應標頭 <code>x-amz-mfa</code> 不受支援。</p> <p>處理 <code>DeleteObject</code> 要求時、<code>StorageGRID</code> 會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、<code>StorageGRID</code> 則會立即將回應傳回給用戶端。如果無法在 30 秒內移除所有複本 (例如、因為某個位置暫時無法使用)、<code>StorageGRID</code> 會將複本排入佇列以供移除、然後表示用戶端成功。</p> <p>版本管理</p> <p>若要移除特定版本、申請者必須是貯體擁有者、並使用 <code>versionId</code> 子資源：使用此子資源會永久刪除版本。如果是 <code>versionId</code> 對應於刪除標記、即回應標頭 <code>x-amz-delete-marker</code> 傳回設定為 <code>true</code>。</p> <ul style="list-style-type: none"> • 如果刪除的物件不含 <code>versionId</code> 子資源在啟用版本的儲存區上、會產生刪除標記。◦ <code>versionId</code> 刪除標記會使用傳回 <code>x-amz-version-id</code> 回應標頭和 <code>x-amz-delete-marker</code> 回應標頭會傳回設定為 <code>true</code>。 • 如果刪除的物件不含 <code>versionId</code> 子資源在版本暫停的儲存區上、會永久刪除現有的 'null' 版本或 'null' 刪除標記、並產生新的 'null' 刪除標記。◦ <code>x-amz-delete-marker</code> 回應標頭會傳回設定為 <code>true</code>。 <p>附註：在某些情況下、物件可能會有多個刪除標記。</p> <p>請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以瞭解如何在治理模式中刪除物件版本。</p>
刪除物件 (先前命名的刪除多個物件)	<p>多因素驗證 (MFA) 和回應標頭 <code>x-amz-mfa</code> 不受支援。</p> <p>您可以在同一個要求訊息中刪除多個物件。</p> <p>請參閱 "使用 S3 REST API 來設定 S3 物件鎖定" 以瞭解如何在治理模式中刪除物件版本。</p>
刪除ObjectTagging	<p>使用 <code>tagging SubResource</code> 可移除物件的所有標記。</p> <p>版本管理</p> <p>如果是 <code>versionId</code> 查詢參數未在要求中指定、此作業會刪除版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「<code>MethodNotAllowed</code>」狀態 <code>x-amz-delete-marker</code> 回應標頭設定為 <code>true</code>。</p>
GetObject	"GetObject"
GetObjectAcl	如果提供帳戶所需的存取認證資料、則作業會傳回正面回應、並傳回物件擁有者的ID、顯示名稱和權限、表示擁有者擁有物件的完整存取權。

營運	實作
GetObjectLegalHold	"使用 S3 REST API 來設定 S3 物件鎖定"
GetObjectRetention	"使用 S3 REST API 來設定 S3 物件鎖定"
GetObjectTagging	<p>使用 tagging SubResource可傳回物件的所有標記。</p> <p>版本管理</p> <p>如果是 versionId 查詢參數未在要求中指定、此作業會傳回版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotAllowed」狀態 x-amz-delete-marker 回應標頭設定為 true。</p>
標題物件	"標題物件"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (先前命名的「Put 物件 - 複本」)	"CopyObject"
PutObjectLegalHold	"使用 S3 REST API 來設定 S3 物件鎖定"
PutObjectRetention	"使用 S3 REST API 來設定 S3 物件鎖定"

營運	實作
PuttObjectTagging	<p>使用 tagging SubResource可將一組標記新增至現有物件。</p> <p>物件標籤限制</p> <p>您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。</p> <p>標記更新和擷取行為</p> <p>當您使用 PuttObjectTagging 更新物件的標記時、StorageGRID 不會重新擷取物件。這表示不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。</p> <p>這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。</p> <p>解決衝突</p> <p>衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。</p> <p>版本管理</p> <p>如果是 versionId 查詢參數未在要求中指定、該作業會將標記新增至版本控制儲存區中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「MethodNotAllowed」狀態 x-amz-delete-marker 回應標頭設定為 true。</p>
選取物件內容	"選取物件內容"

使用S3 Select

StorageGRID 支援下列的 Amazon S3 Select 子句、資料類型和運算子 "[SelectObjectContent命令](#)"。



不支援任何未列出的項目。

如需語法、請參閱 "[選取物件內容](#)"。如需S3 Select的詳細資訊、請參閱 "[S3 Select的AWS文件](#)"。

只有啟用S3 Select的租戶帳戶才能發出SelectObjectContent查詢。請參閱 "[使用S3 Select的考量與要求](#)"。

條款

- [選取清單](#)

- from子句
- where子句
- 限制條款

資料類型

- 布爾
- 整數
- 字串
- 浮動
- 十進位、數字
- 時間戳記

運算子

邏輯運算子

- 和
- 不是
- 或

比較運算子

- <
- >
- < ; =
- >=
- =
- =
- <>
- !=
- 兩者之間
- 在中

模式比對運算子

- 喜歡
- _
- %

單一運算子

- 為空值
- 不是空值

數學運算子

- +
- -
- *
- /
- %

StorageGRID 遵循 Amazon S3 Select 運算子的優先順序。

Aggregate 函數

- 平均 ()
- 計數 (*)
- 最大 ()
- 最小 ()
- 總計 ()

條件式函數

- 案例
- 合併
- NULLIF

轉換功能

- CAST (適用於支援的資料類型)

日期函數

- 日期新增
- 日期_差異
- 擷取
- 至字串
- 目標時間戳記
- UTCNOW

字串函數

- char_length、字元長度

- 降低
- 子字串
- 修剪
- 上

使用伺服器端加密

伺服器端加密可讓您保護閒置的物件資料。當資料寫入物件時、系統會加密資料、並在您存取物件時解密資料。StorageGRID

如果您想要使用伺服器端加密、您可以根據加密金鑰的管理方式、選擇兩個互不相容的選項之一：

- * SSE (使用StorageGRID管理金鑰的伺服器端加密) *：當您發出S3要求以儲存物件時StorageGRID、用唯一的金鑰來加密物件。當您發出S3要求以擷取物件時StorageGRID、則會使用儲存的金鑰來解密物件。
- * SSE-C (使用客戶提供的金鑰進行伺服器端加密) *：當您發出S3要求以儲存物件時、您會提供自己的加密金鑰。擷取物件時、您提供的加密金鑰與要求的一部分相同。如果兩個加密金鑰相符、則會解密物件並傳回物件資料。

雖然此功能可管理所有物件加密與解密作業、但您必須管理所提供的加密金鑰。StorageGRID



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。



如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

使用SS

若要使用StorageGRID 由支援此功能的唯一金鑰來加密物件、請使用下列要求標頭：

```
x-amz-server-side-encryption
```

下列物件作業可支援SSE要求標頭：

- "PutObject"
- "CopyObject"
- "建立多個部分上傳"

使用SSE-C

若要使用您管理的唯一金鑰來加密物件、請使用三個要求標頭：

要求標頭	說明
x-amz-server-side-encryption-customer-algorithm	指定加密演算法。標頭值必須是 AES256。

要求標頭	說明
x-amz-server-side-encryption-customer-key	指定將用於加密或解密物件的加密金鑰。金鑰的值必須是256位元、已編碼的base64。
x-amz-server-side-encryption-customer-key-MD5	根據RFC 1321指定加密金鑰的md5摘要、以確保傳輸加密金鑰時不會發生錯誤。md5摘要的值必須是以64編碼的128位元。

下列物件作業可支援SSE-C要求標頭：

- "GetObject"
- "標題物件"
- "PutObject"
- "CopyObject"
- "建立多個部分上傳"
- "上傳零件"
- "上傳PartCopy"

使用伺服器端加密搭配客戶提供的金鑰（SSE-C）時的考量

使用SSE-C之前、請注意下列考量事項：

- 您必須使用https。



使用SSE-C時、不接受透過http提出的任何要求StorageGRID基於安全考量、您應該考慮使用http意外傳送的任何金鑰是否會遭到入侵。捨棄按鍵、然後視需要旋轉。

- 回應中的ETag不是物件資料的MD5。
- 您必須管理加密金鑰與物件之間的對應關係。不儲存加密金鑰。StorageGRID您必須負責追蹤為每個物件提供的加密金鑰。
- 如果您的儲存區已啟用版本管理功能、則每個物件版本都應該擁有自己的加密金鑰。您負責追蹤每個物件版本所使用的加密金鑰。
- 由於您管理用戶端的加密金鑰、因此也必須管理用戶端上的任何其他安全防護措施、例如金鑰輪替。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

- 如果為貯體設定了跨網格複寫或 CloudMirror 複寫、您就無法擷取 SSE-C 物件。擷取作業將會失敗。

相關資訊

["Amazon S3 使用者指南：使用伺服器端加密搭配客戶提供的金鑰（SSE-C）"](#)

CopyObject

您可以使用 S3 CopyObject 要求來建立已儲存在 S3 中的物件複本。CopyObject 作業與執

行 `GetObject` 之後的 `PutObject` 相同。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於 `StorageGRID` 何時由 `VMware` 系統完成指定的要求、而非 `S3` 用戶端開始作業的時間。

物件大小

單一 `PutObject` 作業的最大大小 `_建議_` 為 5 GiB（5、368、709、120 位元組）。如果物件大於 5 GiB、請使用 "多部分上傳" 而是。

單一 `PutObject` 作業的最大 `_支援_` 大小為 5 TiB（5、497、558、138、880 位元組）。



如果您從 `StorageGRID 11.6` 或更早版本升級、當您嘗試上傳超過 5 GiB 的物件時、會觸發 `S3` 「將物件大小設得太大」警示。如果您有新的 `StorageGRID 11.7` 或 `11.8` 安裝、在這種情況下不會觸發警示。不過、為了符合 `AWS S3` 標準、未來的 `StorageGRID` 版本不支援上傳大於 5 GiB 的物件。

使用者中繼資料中的 `UTF-8` 字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）`utf-8` 值、`StorageGRID` 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式 `utf-8` 字元。`StorageGRID` 轉義的 `UTF-8` 字元會視為 `Ascii` 字元：

- 如果使用者定義的中繼資料包含轉義的 `utf-8` 字元、則要求會成功。
- 無法歸還 `StorageGRID x-amz-missing-meta` 標頭：金鑰名稱或值的解譯值包含不可列印的字元。

支援的要求標頭

支援下列要求標頭：

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對
- `x-amz-metadata-directive`：預設值為 ``COPY`` 可讓您複製物件及相關的中繼資料。

您可以指定 `REPLACE` 可在複製物件時覆寫現有的中繼資料、或更新物件中繼資料。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：預設值為 ``COPY`` 可讓您複製物件和所有標記。

您可以指定 REPLACE 覆寫複製物件時的現有標記、或更新標記。

- S3物件鎖定要求標頭：

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱 ["使用 S3 REST API 來設定 S3 物件鎖定"](#)。

- SSe要求標頭：

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

請參閱 [\[要求伺服器端加密的標頭\]](#)

不支援的要求標頭

不支援下列要求標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

儲存類別選項

◦ x-amz-storage-class 支援要求標頭、如果相符的 ILM 規則使用雙重提交或平衡、則會影響 StorageGRID 建立的物件複本數量 ["擷取選項"](#)。

- STANDARD

(預設) 當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- REDUCED_REDUNDANCY

當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。



如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 REDUCED_REDUNDANCY 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 REDUCED_REDUNDANCY 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

在 CopyObject 中使用 x-amz-copy-source

如果來源儲存區和金鑰、請在中指定 x-amz-copy-source 標頭與目的地桶和金鑰不同、來源物件資料的複本會寫入目的地。

如果來源和目的地相符、則會顯示和 x-amz-metadata-directive 標頭指定為 REPLACE、會以要求中提供的中繼資料值來更新物件的中繼資料。在這種情況StorageGRID 下、無法重新擷取物件。這有兩個重要後果：

- 您無法使用 CopyObject 來加密現有物件、或變更現有物件的加密。如果您提供 x-amz-server-side-encryption 標頭或 x-amz-server-side-encryption-customer-algorithm 標頭StorageGRID、不接受要求並退貨 XNotImplemented。
- 不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。

這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。

要求伺服器端加密的標頭

如果您 ["使用伺服器端加密"](#)、您提供的要求標頭取決於來源物件是否已加密、以及您是否打算加密目標物件。

- 如果來源物件是使用客戶提供的金鑰（SSE-C）加密、則必須在 CopyObject 要求中包含下列三個標頭、以便將物件解密後再複製：
 - x-amz-copy-source-server-side-encryption-customer-algorithm：指定 AES256。
 - x-amz-copy-source-server-side-encryption-customer-key：指定在創建源對象時提供的加密密鑰。
 - x-amz-copy-source-server-side-encryption-customer-key-MD5：指定在創建源對象時提供的md5摘要。
- 如果您要使用您提供及管理的唯一金鑰來加密目標物件（複本）、請包含下列三個標頭：
 - x-amz-server-side-encryption-customer-algorithm：指定 AES256。
 - x-amz-server-side-encryption-customer-key：指定目標物件的新加密金鑰。
 - x-amz-server-side-encryption-customer-key-MD5：指定新加密金鑰的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 ["使用伺服器端加密"](#)。

- 如果您要使用由 StorageGRID（SSE）管理的唯一金鑰來加密目標物件（複本）、請在 CopyObject 要求中加入此標頭：
 - x-amz-server-side-encryption



- `server-side-encryption` 物件的值無法更新。改用新的複本 `server-side-encryption` 使用價值 `x-amz-metadata-directive`：REPLACE。

版本管理

如果來源儲存區已版本化、您可以使用 `x-amz-copy-source` 標頭以複製物件的最新版本。若要複製物件的特定版本、您必須使用明確指定要複製的版本 `versionId` 子資源：如果目標儲存區已版本化、則會在中傳回所產生的版本 `x-amz-version-id` 回應標頭：如果目標儲存區的版本設定已暫停、則 `x-amz-version-id` 傳回「null」值。

GetObject

您可以使用 S3 GetObject 要求、從 S3 貯體擷取物件。

GetObject 和多部分物件

您可以使用 `partNumber` 要求參數以擷取多部分或分割物件的特定部分。◦ `x-amz-mp-parts-count` 回應元素指出物件有多少部分。

您可以設定 `partNumber` 對於分割 / 多個零件物件和非分割 / 非多個零件物件、則為 1；不過、`x-amz-mp-parts-count` 只會針對分割或多個零件物件傳回回應元素。

使用者中繼資料中的UTF-8字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID取得使用者定義中繼資料中含有轉義式 UTF-8 字元的物件要求、並不會傳回 `x-amz-missing-meta` 如果金鑰名稱或值包含不可列印的字元、則為標頭。

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本管理

如果是 `versionId` 未指定 `SubResource`、此作業會擷取版本控制儲存區中最新版本的物件。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態和 `x-amz-delete-marker` 回應標頭設定為 `true`。

使用客戶提供的加密金鑰 (SSE-C) 要求伺服器端加密標頭

如果物件是以您提供的唯一金鑰加密、請使用所有三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定對象加密金鑰的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 ["使用伺服器端加密"](#)。

GetObject for Cloud Storage Pool 物件的行為

如果物件已儲存在中 "雲端儲存資源池"， GetObject 要求的行為取決於物件的狀態。請參閱 "標題物件" 以取得更多詳細資料。



如果某個物件儲存在雲端儲存池中、且該物件的一個或多個複本也存在於網格上、則 GetObject 要求會嘗試從網格擷取資料、然後再從雲端儲存池擷取資料。

物件狀態	GetObject 的行為
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	200 OK 系統會擷取物件複本。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	200 OK 系統會擷取物件複本。
物件移轉至無法擷取的狀態	403 Forbidden、InvalidObjectState 使用 "RestoreObject" 要求將物件還原至可擷取狀態。
正在從無法擷取的狀態還原的物件	403 Forbidden、InvalidObjectState 等待 RestoreObject 要求完成。
物件已完全還原至雲端儲存資源池	200 OK 系統會擷取物件複本。

雲端儲存資源池中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、GetObject 要求可能會錯誤傳回 200 OK 當物件的某些部分已轉換為無法擷取的狀態、或物件的某些部分尚未還原時。

在這些情況下：

- GetObject 要求可能會傳回一些資料、但中途停止傳輸。
- 後續的 GetObject 要求可能會傳回 403 Forbidden。

GetObject 和跨網格複寫

如果您使用 "網格同盟" 和 "跨網格複寫" 已啟用貯體、S3 用戶端可藉由發出 GetObject 要求來驗證物件的複寫狀態。回應包括 StorageGRID 專屬 x-ntap-sg-cgr-replication-status 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	<ul style="list-style-type: none"> • * 成功 * : 複寫成功。 • * 擱置 * : 物件尚未複寫。 • * 失敗 * : 複寫失敗且持續失敗。使用者必須解決此錯誤。
目的地	<ul style="list-style-type: none"> • 複本 * : 物件已從來源網格複寫。



不支援StorageGRID `x-amz-replication-status` 標頭。

標題物件

您可以使用 S3 `HeadObject` 要求、從物件擷取中繼資料、而無需傳回物件本身。如果物件儲存在雲端儲存池中、您可以使用 `HeadObject` 來判斷物件的轉換狀態。

HeadObject 和多個零件物件

您可以使用 `partNumber` 要求參數以擷取多部分或分割物件特定部分的中繼資料。◦ `x-amz-mp-parts-count` 回應元素指出物件有多少部分。

您可以設定 `partNumber` 對於分割 / 多個零件物件和非分割 / 非多個零件物件、則為 1 ; 不過、`x-amz-mp-parts-count` 只會針對分割或多個零件物件傳回回應元素。

使用者中繼資料中的UTF-8字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID使用者定義中繼資料中的轉義式UTF-8 字元物件的標頭要求不會傳回 `x-amz-missing-meta` 如果金鑰名稱或值包含不可列印的字元、則為標頭。

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented` :

- `x-amz-website-redirect-location`

版本管理

如果是 `versionId` 未指定SubResource、此作業會擷取版本控制儲存區中最新版本的物件。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態和 `x-amz-delete-marker` 回應標頭設定為 `true`。

使用客戶提供的加密金鑰 (SSE-C) 要求伺服器端加密標頭

如果物件使用您提供的唯一金鑰加密、請使用這三個標頭。

- `x-amz-server-side-encryption-customer-algorithm` : 指定 AES256。
- `x-amz-server-side-encryption-customer-key` : 指定物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5` : 指定對象加密密鑰的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 "使用伺服器端加密"。

Cloud Storage Pool 物件的 HeadObject 回應

如果物件儲存在中 "雲端儲存資源池"，會傳回下列回應標頭：

- x-amz-storage-class: GLACIER
- x-amz-restore

回應標頭會提供物件移至雲端儲存集區時的狀態資訊、並選擇性地移轉至無法擷取的狀態、然後還原。

物件狀態	對 HeadObject 的回應
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	200 OK (未傳回特殊回應標頭。)
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	200 OK x-amz-storage-class: GLACIER 「x-amz-restore : n未定 要求 = 假」、過期日期 = 「星期六、7 月 23 日 203000:00 GMT」 在物件轉換為無法擷取的狀態之前、其值為 expiry-date 設定為未來的某段時間。確切的轉換時間不受StorageGRID 此功能的控制。
物件已轉換為無法擷取的狀態、但網格上至少也有一個複本	200 OK x-amz-storage-class: GLACIER 「x-amz-restore : n未定 要求 = 假」、過期日期 = 「星期六、7 月 23 日 203000:00 GMT」 的價值 expiry-date 設定為未來的某段時間。 • 注意 * : 如果網格上的複本不可用 (例如、儲存節點停機)、您必須發出 "RestoreObject" 要求從雲端儲存池還原複本、然後才能成功擷取物件。
物件移轉至無法擷取的狀態、而且網格上不存在複本	200 OK x-amz-storage-class: GLACIER

物件狀態	對 HeadObject 的回應
正在從無法擷取的狀態還原的物件	200 OK x-amz-storage-class: GLACIER 「 x-amz-restore : 後續要求 ="true"」
物件已完全還原至雲端儲存資源池	200 OK x-amz-storage-class: GLACIER 「 x-amz-restore : n未定 要求 ="false" 、到期日 = 「2018 年 7 月 23 日星期六 00 : 00 : 00 GMT」 ◦ expiry-date 指出Cloud Storage Pool中的物件何時會傳回無法擷取的狀態。

Cloud Storage Pool中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、當物件的某些部分已經轉換為無法擷取的狀態、或物件的某些部分尚未還原時、HeadObject 要求可能會錯誤傳回「 x-amz-restore : non-reqstore= 」。

HeadObject 和跨網格複寫

如果您使用 "網格同盟" 和 "跨網格複寫" 為儲存區啟用 S3 用戶端、可發出 HeadObject 要求、以驗證物件的複寫狀態。回應包括 StorageGRID 專屬 x-ntap-sg-cgr-replication-status 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	<ul style="list-style-type: none"> • * 成功 * : 複寫成功。 • * 擱置 * : 物件尚未複寫。 • * 失敗 * : 複寫失敗且持續失敗。使用者必須解決此錯誤。
目的地	<ul style="list-style-type: none"> • 複本 * : 物件已從來源網格複寫。



不支援StorageGRID x-amz-replication-status 標頭。

PuttObject

您可以使用 S3 PuttObject 要求、將物件新增至貯體。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時

間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一 PutObject 作業的最大大小 **建議** 為 5 GiB (5 、 368 、 709 、 120 位元組) 。如果物件大於 5 GiB 、請使用 "多部分上傳" 而是。

單一 PutObject 作業的最大 **支援** 大小為 5 TiB (5 、 497 、 558 、 138 、 880 位元組) 。



如果您從 StorageGRID 11.6 或更早版本升級、當您嘗試上傳超過 5 GiB 的物件時、會觸發 S3 「將物件大小設得太大」 警示。如果您有新的 StorageGRID 11.7 或 11.8 安裝、在這種情況下不會觸發警示。不過、為了符合 AWS S3 標準、未來的 StorageGRID 版本不支援上傳大於 5 GiB 的物件。

使用者中繼資料大小

Amazon S3會將每個PUT要求標頭內使用者定義的中繼資料大小限制為2 KB。支援範圍將使用者中繼資料限制為24 KiB。StorageGRID使用者定義的中繼資料大小是以每個金鑰和值的utf-8編碼方式、計算出位元組數的總和。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含 (未轉義) utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義式 UTF-8 字元、則 PutObject 、 CopyObject 、 GetObject 和 HeadObject 要求會成功。
- 無法歸還StorageGRID x-amz-missing-meta 標頭：金鑰名稱或值的解譯值包含不可列印的字元。

物件標籤限制

您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。

物件擁有權

在功能區中StorageGRID 、所有物件均歸庫位擁有者帳戶所有、包括非擁有者帳戶或匿名使用者所建立的物件。

支援的要求標頭

支援下列要求標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding

當您指定時 `aws-chunked` 適用於 `Content-Encoding` 無法驗證下列項目 `StorageGRID`：

- 無法驗證 `StorageGRID chunk-signature` 根據區塊資料。
- 無法驗證您提供的價值 `StorageGRID x-amz-decoded-content-length` 針對物件。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

如果支援 `Chunked` 傳輸編碼 `aws-chunked` 也會使用有效負載簽署。

- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對。

為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

```
x-amz-meta-name: value
```

如果您要使用 * 使用者定義的建立時間 * 選項做為 `ILM` 規則的參考時間、則必須使用 `creation-time` 做為建立物件時記錄的中繼資料名稱。例如：

```
x-amz-meta-creation-time: 1443399726
```

的價值 `creation-time` 自1970年1月1日起算為秒數。



ILM 規則不能同時使用 * 使用者定義的建立時間 * 作為參考時間、也不能同時使用平衡或嚴格擷取選項。建立ILM規則時會傳回錯誤。

- `x-amz-tagging`
- **S3物件鎖定要求標頭**
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱 ["使用 S3 REST API 來設定 S3 物件鎖定"](#)。

- **SSE要求標頭：**
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`

- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

請參閱 [\[要求伺服器端加密的標頭\]](#)

不支援的要求標頭

不支援下列要求標頭：

- x-amz-acl 不支援要求標頭。
- x-amz-website-redirect-location 不支援要求標頭並傳回 XNotImplemented。

儲存類別選項

◦ x-amz-storage-class 支援要求標頭。提交的值 x-amz-storage-class 影響StorageGRID 到在擷取期間、如何保護物件資料、而非StorageGRID 物件的持續複本儲存在整個系統（由ILM決定）中。

如果符合擷取物件的 ILM 規則使用嚴格擷取選項、則會使用 x-amz-storage-class 標頭沒有作用。

下列值可用於 x-amz-storage-class：

- STANDARD（預設）
 - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估 ILM 時、StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
 - *Balanced*：如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

如果StorageGRID 能夠立即建立ILM規則中指定的所有物件複本（同步放置） x-amz-storage-class 標頭沒有作用。

- REDUCED_REDUNDANCY
 - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
 - *Balanced*：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID 的 REDUCED_REDUNDANCY 當符合物件的ILM規則建立單一複寫複本時、最適合使用此選項。在此案例中、請使用 REDUCED_REDUNDANCY 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

使用 REDUCED_REDUNDANCY 在其他情況下不建議使用此選項。REDUCED_REDUNDANCY 增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。



在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 REDUCED_REDUNDANCY 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中 ILM 原則評估物件時所製作的物件複本數量、也不會導致資料儲存在 StorageGRID 系統中較低的備援層級。



如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 REDUCED_REDUNDANCY 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 REDUCED_REDUNDANCY 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想使用StorageGRID 由支援的唯一金鑰來加密物件、請使用下列標頭。
 - x-amz-server-side-encryption
- * SSE-C*：如果您想使用您提供及管理的唯一金鑰來加密物件、請使用這三個標頭。
 - x-amz-server-side-encryption-customer-algorithm：指定 AES256。
 - x-amz-server-side-encryption-customer-key：指定新物件的加密金鑰。
 - x-amz-server-side-encryption-customer-key-MD5：指定新對象加密密鑰的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 "[使用伺服器端加密](#)"。



如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

版本管理

如果已啟用儲存區的版本管理功能、則為唯一的 versionId 會針對儲存的物件版本自動產生。這 versionId 也會使用傳回回應 x-amz-version-id 回應標頭：

如果版本控制暫停、則物件版本會以null儲存 versionId 如果空版本已經存在、則會覆寫。

授權標頭的簽名計算

使用時 Authorization 用於驗證要求的標頭、StorageGRID 與 AWS 有下列不同：

- StorageGRID 不需要 host 要包含的標頭 CanonicalHeaders。
- StorageGRID 不需要 Content-Type 包括在內 CanonicalHeaders。
- StorageGRID 不需要 x-amz-* 要包含的標頭 CanonicalHeaders。



一般最佳實務做法是一律將這些標頭包含在內 CanonicalHeaders 為了確保這些標頭已通過驗證、但如果您排除這些標頭、StorageGRID 不會傳回錯誤。

如需詳細資訊、請參閱 "[授權標頭的簽名計算：在單一區塊中傳輸有效負載（AWS 簽名版本 4）](#)"。

相關資訊

["使用ILM管理物件"](#)

RestoreObject

您可以使用 S3 RestoreObject 要求來還原儲存在雲端儲存池中的物件。

支援的要求類型

StorageGRID 僅支援還原物件的 RestoreObject 要求。它不支援 SELECT 還原類型。選取「要求傳回」XNotImplemented。

版本管理

或者、請指定 `versionId` 還原版本化儲存區中物件的特定版本。如果您沒有指定 `versionId`，則會還原物件的最新版本

Cloud Storage Pool 物件上的 RestoreObject 行為

如果物件已儲存在中 "雲端儲存資源池"，RestoreObject 要求會根據物件的狀態而有下列行為。請參閱 "標題物件" 以取得更多詳細資料。



如果物件儲存在雲端儲存池中、且網絡上也有一個或多個物件複本、則無需透過發出 RestoreObject 要求來還原物件。而是可以使用 GetObject 要求直接擷取本機複本。

物件狀態	RestoreObject 的行為
物件擷取至StorageGRID 不受ILM評估、或物件不在雲端儲存資源池中	403 Forbidden、InvalidObjectState
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	200 OK 不會進行任何變更。 • 注意 *：在物件轉換為不可擷取的狀態之前、您無法變更物件 expiry-date。
物件移轉至無法擷取的狀態	202 Accepted 將物件的可擷取複本還原至Cloud Storage Pool、直到要求本文指定的天數。在此期間結束時、物件會返回無法擷取的狀態。 您也可以選擇使用 Tier 要求元素以決定還原工作完成所需的時間 (Expedited、Standard、或 Bulk)。如果您沒有指定 Tier、Standard 使用階層。 • 重要 *：如果物件已移轉至 S3 Glacier Deep Archive、或雲端儲存池使用 Azure Blob 儲存設備、則無法使用還原 Expedited 層級。傳回下列錯誤 403 Forbidden、InvalidTier: Retrieval option is not supported by this storage class。
正在從無法擷取的狀態還原的物件	409 Conflict、RestoreAlreadyInProgress

物件狀態	RestoreObject 的行為
物件已完全還原至雲端儲存資源池	200 OK *附註：*如果物件已還原為可擷取的狀態、您可以變更物件 expiry-date 以新值重新發出 RestoreObject 要求 Days。還原日期會根據申請時間而更新。

選取物件內容

您可以使用 S3 SelectObjectContent 要求、根據簡單的 SQL 陳述來篩選 S3 物件的內容。

如需詳細資訊、請參閱 "[Amazon Simple Storage Service API 參考資料： SelectObjectContent](#)"。

開始之前

- 租戶帳戶具有 S3 Select 權限。
- 您有 s3:GetObject 您要查詢之物件的權限。
- 您要查詢的物件必須採用下列其中一種格式：
 - * CSV * ◦ 可依原樣使用、也可壓縮至 GZIP 或 bzip2 歸檔。
 - * 硬地板 * ◦ 硬地板物件的其他需求：
 - S3 Select 僅支援使用 GZIP 或 Snappy 進行柱式壓縮。S3 Select 不支援 Parquet 物件的全物件壓縮。
 - S3 Select 不支援硬地板輸出。您必須將輸出格式指定為 CSV 或 JSON。
 - 最大未壓縮列群組大小為 512 MB。
 - 您必須使用物件架構中指定的資料類型。
 - 您無法使用時間間隔、JSON、清單、時間或 UUID 邏輯類型。
- SQL 運算式的最大長度為 256 KB。
- 輸入或結果中的任何記錄最大長度為 1 個 MiB。

CSV 要求語法範例

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

拼花地板要求語法範例

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

SQL查詢範例

此查詢會取得州名、2010年人口、2015年估計人口、以及美國統計資料的變更百分比。檔案中非狀態的記錄會被忽略。

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

要查詢的檔案前幾行：SUB-EST2020_ALL.csv、如下所示：

```

SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717

```

AWS-CLI 使用範例 (CSV)

```

aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv

```

輸出檔案的前幾行、changes.csv、如下所示：

```

Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246

```


AWS-CLI 使用範例 (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
 '{"CSV": {}}' changes.csv
```

輸出檔案的前幾行： changes.csv 、如下所示：

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

多部份上傳作業

多部分上傳作業：總覽

本節說明StorageGRID 此功能如何支援多部份上傳作業。

下列條件與附註適用於所有多重部分上傳作業：

- 您不應超過 1、000 次同時上傳多個部分至單一儲存庫、因為該儲存庫的 ListMultipartuploADS 查詢結果可能會傳回不完整的結果。
- 針對多個零件執行AWS大小限制。StorageGRIDS3用戶端必須遵循下列準則：
 - 多部份上傳的每個部分必須介於5個mib (5、242,880位元組) 和5 GiB (5、368,709,120位元組) 之間。
 - 最後一部分可小於5個mib (5、242,880位元組) 。
 - 一般而言、零件尺寸應盡量大。例如、對於100 GiB物件使用5 GiB的零件大小。因為每個零件都被視為唯一的物件、所以使用較大的零件大小可降低 StorageGRID 中繼資料的負荷。
 - 對於小於5 GiB的物件、請考慮改用非多部份上傳。
- 如果 ILM 規則使用平衡或嚴格、則會在擷取時針對多個部分物件的每個部分進行 ILM 評估、並在完成多個部分上傳時針對整個物件進行評估 "[擷取選項](#)"。您應該瞭解這會如何影響物件和零件放置：
 - 如果在 S3 多部分上傳進行期間 ILM 有所變更、則當多部分上傳完成時、物件的某些部分可能不符合目前的 ILM 需求。未正確放置的任何零件都會排入 ILM 重新評估的佇列、稍後移至正確位置。
 - 評估零件的ILM時StorageGRID、會根據零件大小而非物件大小來篩選。這表示物件的部分可以儲存在不符合整體物件 ILM 需求的位置。例如、如果規則指定所有 10 GB 或更大的物件都儲存在 DC1、而所有較小的物件都儲存在 DC2、則 10 部分多部分上傳的每 1 GB 部分都會儲存在 DC2 的擷取位置。不

過、評估整體物件的 ILM 時、物件的所有部分都會移至 DC1。

- 所有的多部分上傳作業都支援 StorageGRID "一致性值"。
- 您可以視需要使用 "伺服器端加密" 多部分上傳。若要使用SSE（伺服器端加密搭配StorageGRID管理金鑰）、請加入 `x-amz-server-side-encryption` 僅限 CreateMultipartUpload 要求中的要求標頭。若要使用 SSE-C（伺服器端加密搭配客戶提供的金鑰）、您可以在 CreateMultipartUpload 要求和每個後續的 UploPart 要求中指定相同的三個加密金鑰要求標頭。

營運	實作
AbortMultiPart上傳	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
完成多個部分上傳	請參閱 "完成多個部分上傳"
建立多個部分上傳 (先前命名的「Initiate Multifart Upload」)	請參閱 "建立多個部分上傳"
ListMultipartUploads	請參閱 "ListMultipartUploads"
清單零件	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
上傳零件	請參閱 "上傳零件"
上傳PartCopy	請參閱 "上傳PartCopy"

完成多個部分上傳

「CompleteMultipartUpload」（CompleteMultipartupload）作業可組合先前上傳的零件、完成物件的多部分上傳。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

要求標頭

◦ `x-amz-storage-class` 支援要求標頭、如果相符的 ILM 規則指定雙重認可或平衡、則會影響 StorageGRID 建立的物件複本數量 "擷取選項"。

- STANDARD

（預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- REDUCED_REDUNDANCY

當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。



如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 REDUCED_REDUNDANCY 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 REDUCED_REDUNDANCY 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID



如果多部分上傳未在15天內完成、則該作業會標示為非作用中、且所有相關資料都會從系統中刪除。



- ETag 傳回的值不是資料的MD5總和、而是在的Amazon S3 API實作之後 ETag 多部分物件的值。

版本管理

此作業會完成多部份上傳。如果已啟用貯體的版本設定功能、則物件版本會在完成多重部分上傳後建立。

如果已啟用儲存區的版本管理功能、則為唯一的 versionId 會針對儲存的物件版本自動產生。這 versionId 也會使用傳回回應 x-amz-version-id 回應標頭：

如果版本控制暫停、則物件版本會以null儲存 versionId 如果空版本已經存在、則會覆寫。



當某個儲存區啟用版本管理時、完成多部份上傳會一律建立新版本、即使在同一個物件金鑰上同時完成多部份上傳也一樣。如果未針對某個儲存區啟用版本管理、則可以啟動多重部分上傳、然後在同一個物件金鑰上啟動並完成另一個多重部分上傳。在非版本的儲存區上、完成最後一次的多部分上傳優先。

複寫失敗、通知或中繼資料通知

如果平台服務已設定多重零件上傳的儲存區、即使相關的複寫或通知動作失敗、多重零件上傳仍會成功。

如果發生這種情況、則會在Grid Manager中針對Total事件 (SMT) 發出警示。上次事件訊息會針對通知失敗的最後一個物件、顯示「發佈 Bucket 名稱物件金鑰通知失敗」。(要查看此訊息、請選取*節點*>*儲存節點_*>*事件*。檢視表格頂端的最後一個事件。) 中也會列出事件訊息 /var/local/log/bycast-err.log。

租戶可透過更新物件的中繼資料或標記來觸發失敗的複寫或通知。租戶可以重新提交現有的值、以避免進行不必要的變更。

建立多個部分上傳

CreateMultipartupload (先前命名為「Initiate Multifart Upload」(起始多重部分上傳)) 作業會啟動物件的多重部分上傳、並傳回上傳 ID。

- x-amz-storage-class 支援要求標頭。提交的值 x-amz-storage-class 影響StorageGRID 到在擷取期間、如何保護物件資料、而非StorageGRID 物件的持續複本儲存在整個系統 (由ILM決定) 中。

如果符合擷取物件的 ILM 規則使用嚴格的 "擷取選項"、x-amz-storage-class 標頭沒有作用。

下列值可用於 x-amz-storage-class：

- STANDARD (預設)

- * 雙重認可 * : 如果 ILM 規則指定「雙重認可擷取」選項、則只要物件擷取第二個物件複本、就會建立並發佈至不同的儲存節點 (雙重認可) 。評估 ILM 時、StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
- *Balanced* : 如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

如果StorageGRID 能夠立即建立ILM規則中指定的所有物件複本 (同步放置) `x-amz-storage-class` 標頭沒有作用。

- REDUCED_REDUNDANCY

- * 雙重認可 * : 如果 ILM 規則指定雙重認可選項、StorageGRID 會在擷取物件時 (單一認可) 建立單一的臨時複本。
- *Balanced* : 如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID 的 REDUCED_REDUNDANCY 當符合物件的ILM規則建立單一複寫複本時、最適合使用此選項。在此案例中、請使用 REDUCED_REDUNDANCY 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

使用 REDUCED_REDUNDANCY 在其他情況下不建議使用此選項。REDUCED_REDUNDANCY 增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。



在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 REDUCED_REDUNDANCY 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中 ILM 原則評估物件時所製作的物件複本數量、也不會導致資料儲存在 StorageGRID 系統中較低的備援層級。



如果您將物件擷取至啟用S3物件鎖定的儲存區、則會顯示 REDUCED_REDUNDANCY 選項會被忽略。如果您要將物件擷取至舊版相容的儲存區、請使用 REDUCED_REDUNDANCY 選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

支援下列要求標頭：

- Content-Type
- `x-amz-meta-` , 然後是包含使用者定義中繼資料的名稱值配對

為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

```
x-amz-meta-_name_: `value`
```

如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須使用 `creation-time` 做為建立物件時記錄的中繼資料名稱。例如：

```
x-amz-meta-creation-time: 1443399726
```

的價值 `creation-time` 自1970年1月1日起算為秒數。



新增 `creation-time` 如果您要將物件新增至已啟用舊版規範的儲存區、則不允許使用者定義的中繼資料。將傳回錯誤。

• S3物件鎖定要求標頭：

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

["使用 S3 REST API 來設定 S3 物件鎖定"](#)

• SSE要求標頭：

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[\[要求伺服器端加密的標頭\]](#)



如需 StorageGRID 如何處理 UTF-8 字元的相關資訊、請參閱 ["PutObject"](#)。

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密多部份物件。「SSE」和「SSE-C」選項互不相關。

- ***SSE***：如果您想使用由 StorageGRID 管理的唯一金鑰來加密物件、請在 `CreateMultipartUpload` 要求中使用下列標頭。請勿在任何上傳組件要求中指定此標頭。
 - `x-amz-server-side-encryption`
- **SSE-C**：如果您想要使用您提供和管理的唯一金鑰來加密物件、請在 `CreateMultipartUpload` 要求（以及每個後續的 `UploadPart` 要求）中使用這三個標頭。
 - `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
 - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
 - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱的考量事項 ["使用伺服器端加密"](#)。

不支援的要求標頭

不支援並傳回下列要求標頭 XNotImplemented

- x-amz-website-redirect-location

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「CompleteMultipartUpload」（CompleteMultipartUpload）作業時、即會建立物件（並在適用的情況下進行版本控制）。

ListMultipartUploads

ListMultipartUploads 作業會列出某個儲存庫的進行中多個部分上傳。

支援下列要求參數：

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「CompleteMultipartUpload」（CompleteMultipartUpload）作業時、即會建立物件（並在適用的情況下進行版本控制）。

上傳零件

上傳 Part 作業會上傳物件的多部分上傳中的某個零件。

支援的要求標頭

支援下列要求標頭：

- Content-Length
- Content-MD5

要求伺服器端加密的標頭

如果您為 CreateMultipartUpload 要求指定了 SSE-C 加密、則每個 UploadPart 要求中也必須包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定您在 `CreateMultipartUpload` 要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 `CreateMultipartUpload` 要求中提供的相同 MD5 摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 ["使用伺服器端加密"](#)。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「`CompleteMultipartUpload`」 (`CompleteMultipartUpload`) 作業時、即會建立物件（並在適用的情況下進行版本控制）。

上傳PartCopy

上傳 `PartCopy` 作業會將現有物件的資料複製為資料來源、以上傳物件的一部分。

所有 Amazon S3 REST API 行為都會實作上傳 `PartCopy` 作業。如有變更、恕不另行通知。

此要求會讀取及寫入中指定的物件資料 `x-amz-copy-source-range` 在整個系統中StorageGRID。

支援下列要求標頭：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

要求伺服器端加密的標頭

如果您為 `CreateMultipartUpload` 要求指定了 SSE-C 加密、則每個 `UploadPartCopy` 要求中也必須包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定您在 `CreateMultipartUpload` 要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 `CreateMultipartUpload` 要求中提供的相同 MD5 摘要。

如果來源物件是使用客戶提供的金鑰（SSE-C）加密、則必須在上傳 `PartCopy` 要求中包含下列三個標頭、以便將物件解密後再複製：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定在創建源對象時提供的加密密鑰。

- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的md5摘要。



您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前、請先檢閱中的考量事項 ["使用伺服器端加密"](#)。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「CompleteMultipartUpload」（CompleteMultipartUpload）作業時、即會建立物件（並在適用的情況下進行版本控制）。

錯誤回應

支援所有適用的標準S3 REST API錯誤回應。StorageGRID此外、此功能還會加入數個自訂回應。StorageGRID

支援的S3 API錯誤代碼

名稱	HTTP 狀態
ACCESSDENIED	403禁止
《標誌摘要》	400個錯誤要求
BucketAlreadyEx分子	衝突
BucketNotEmpty	衝突
不完整正文	400個錯誤要求
內部錯誤	500內部伺服器錯誤
InvalidAccessKeyId	403禁止
InvalidArgument	400個錯誤要求
InvalidBucketName	400個錯誤要求
InvalidBucketState	衝突
InvalidDigest	400個錯誤要求
InvalidEncryptionAlgorithm錯誤	400個錯誤要求

名稱	HTTP 狀態
InvalidPart	400個錯誤要求
InvalidPartOrder	400個錯誤要求
InvalidRang	無法滿足416個要求的範圍
InvalidRequest	400個錯誤要求
InvalidStorageClass	400個錯誤要求
InvalidTag	400個錯誤要求
InvalidURI	400個錯誤要求
KeyTooLong	400個錯誤要求
MalformedXML	400個錯誤要求
Metadata TooLarg	400個錯誤要求
方法未允許	不允許使用405方法
內容長度	需要411長度
MissingRequestBodyError	400個錯誤要求
MISingSecurityHeader	400個錯誤要求
NoSuchBucket	找不到404
NoSuchKey	找不到404
NoSuchUpload	找不到404
未實作	501未實作
NoSuchBucketPolicy	找不到404
ObjectLockConfiguration未找到錯誤	找不到404
預先條件失敗	412先決條件失敗

名稱	HTTP 狀態
要求時間TooSkewed	403禁止
服務無法使用	503服務無法使用
簽名DoesNotMatch	403禁止
TooManyboo	400個錯誤要求
使用者KeyMustBeSpecified	400個錯誤要求

零點自訂錯誤代碼StorageGRID

名稱	說明	HTTP 狀態
XBucketLifecycleNotSupported	不允許在符合舊版規範的儲存庫中進行貯體生命週期組態	400個錯誤要求
XBucketPolicyParseException	無法剖析收到的儲存區原則Json。	400個錯誤要求
XComplianceConflict	因為舊版規範設定而拒絕作業。	403禁止
XComplianceReducedRedundancyForbidden	舊型符合標準的儲存區不允許減少備援	400個錯誤要求
XMaxBucketPolicyLengthExceed	您的原則超過允許的儲存區原則長度上限。	400個錯誤要求
XMissingInternalRequestHeader	缺少內部要求的標頭。	400個錯誤要求
XNoSuchBucketCompliance	指定的儲存庫未啟用舊版法規遵循。	找不到404
XNotAcceptable	要求包含一或多個無法滿足的Accept標頭。	無法接受的406
XNotImplemed	您提供的要求暗示功能尚未實作。	501未實作

StorageGRID 自訂作業

StorageGRID 自訂作業：總覽

StorageGRID 系統支援新增至 S3 REST API 的自訂作業。

下表列出 StorageGRID 支援的自訂作業。

營運	說明
"取得庫位一致性"	傳回套用至特定儲存區的一致性。
"實現庫位一致性"	設定套用至特定貯體的一致性。
"取得時段上次存取時間"	傳回是否為特定儲存區啟用或停用上次存取時間更新。
"將資源桶放在最後存取時間"	可讓您啟用或停用特定儲存區的上次存取時間更新。
"刪除時段中繼資料通知組態"	刪除與特定儲存區相關聯的中繼資料通知組態XML。
"取得Bucket中繼資料通知組態"	傳回與特定儲存區相關聯的中繼資料通知組態XML。
"放置時段中繼資料通知組態"	設定區段的中繼資料通知服務。
"取得儲存使用量"	告訴您帳戶使用的儲存空間總量、以及與帳戶相關的每個儲存區。
"已過時：具有規範設定的 CreateBucket"	已過時且不受支援：您無法再建立啟用「符合性」的新儲存區。
"已過時：取得 Bucket 法規遵循"	已過時但受支援：傳回現有舊版相容儲存區目前有效的法規遵循設定。
"已過時：符合 Put Bucket 規範"	已過時但受支援：可讓您修改現有舊版相容儲存區的法規遵循設定。

取得庫位一致性

「取得貯體一致性」要求可讓您判斷套用至特定貯體的一致性。

預設一致性設定為保證新建立物件的寫入後讀取。

您必須具有S3：GetBucketConsistency權限或帳戶根權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

在回應XML中、<Consistency> 會傳回下列其中一個值：

一致性	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	(預設) 為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用 (例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業)。S3 FabricPool 儲存區不支援。

回應範例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相關資訊

["一致性值"](#)

實現庫位一致性

「放置貯體一致性」要求可讓您指定套用至在貯體上執行之作業的一致性。

預設一致性設定為保證新建立物件的寫入後讀取。

開始之前

您必須具有 S3:PutBucketConsistency 權限或帳戶 root 權限、才能完成此作業。

申請

- x-ntap-sg-consistency 參數必須包含下列其中一個值：

一致性	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	(預設) 為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用 (例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業)。S3 FabricPool 儲存區不支援。

- 注意：* 一般而言、您應該使用「新寫入後讀取」的一致性。如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、設定用戶端以指定每個 API 要求的一致性。將貯體層級的一致性設為最後的方法。

申請範例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相關資訊

["一致性值"](#)

取得時段上次存取時間

「取得時段上次存取時間」要求可讓您決定是否為個別的時區啟用或停用上次存取時間更新。

您必須具有 S3 : GetBucketLastAccessTime 權限或帳戶根權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示已針對儲存庫啟用上次存取時間更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

將資源桶放在最後存取時間

「放置時段上次存取時間」要求可讓您針對個別的時段啟用或停用上次存取時間更新。停用上次存取時間更新可改善效能、是所有以10.3.0版或更新版本建立之儲存區的預設設定。

您必須擁有儲存區的S3：PutBucketLastAccessTime權限、或是帳戶root權限、才能完成此作業。



從版本10.3開始StorageGRID、所有新的儲存庫預設都會停用上次存取時間的更新。如果您有使用StorageGRID 舊版的更新程式建立的儲存區、而且想要符合新的預設行為、則必須明確停用這些舊版儲存區的上次存取時間更新。您可以使用 Put Bucket 上次存取時間要求、或從租戶管理器中的儲存區詳細資料頁面、啟用或停用上次存取時間的更新。請參閱 ["啟用或停用上次存取時間更新"](#)。

如果某個儲存區的上次存取時間更新已停用、則會將下列行為套用至儲存區上的作業：

- GetObject、GetObjectAcl、GetObjectTagging, 和 HeadObject 要求不會更新上次存取時間。不會將物件新增至佇列、以進行資訊生命週期管理 (ILM) 評估。
- 僅更新中繼資料的 CopyObject 和 PutObjectTaggings 要求也會更新上次存取時間。物件會新增至佇列以進行ILM評估。
- 如果來源貯體的上次存取時間更新已停用、則 CopyObject 要求不會更新來源貯體的上次存取時間。複製的物件不會新增至來源儲存區的ILM評估佇列。不過、對於目的地、CopyObject 要求一律會更新上次存取時間。物件複本會新增至佇列以進行ILM評估。
- CompleteMultipartUpload 要求上次更新存取時間。完成的物件會新增至佇列以進行ILM評估。

申請範例

此範例可讓儲存區的上次存取時間達到。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此範例會停用儲存區的上次存取時間。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

刪除時段中繼資料通知組態

刪除庫位中繼資料通知組態要求可讓您刪除組態XML、以停用個別庫位的搜尋整合服務。

您必須擁有儲存區的S3：刪除BucketMetadata通知權限、或是帳戶根權限、才能完成此作業。

申請範例

此範例顯示停用區段的搜尋整合服務。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

取得Bucket中繼資料通知組態

「Get Bucket中繼資料」通知組態要求可讓您擷取組態XML、以設定個別儲存區的搜尋整合。

您必須具有S3：GetBucketMetadata通知權限、或是帳戶root、才能完成此作業。

申請範例

此要求會擷取名為的儲存區之中繼資料通知組態 bucket。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

回應本文包含儲存區的中繼資料通知組態。中繼資料通知組態可讓您決定儲存區的搜尋整合設定方式。也就是、它可讓您決定要建立索引的物件、以及要將物件中繼資料傳送至哪個端點。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

每個中繼資料通知組態都包含一或多個規則。每個規則都會指定套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。目的地必須使用StorageGRID 不實端點的URN來指定。

名稱	說明	必要
Metadata NotificationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotificationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	<p>符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。</p> <p>若要符合所有物件、請指定一個空白首碼。</p> <p>包含在Rule元素中。</p>	是的
目的地	<p>規則目的地的容器標記。</p> <p>包含在Rule元素中。</p>	是的
urn	<p>傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN：</p> <ul style="list-style-type: none"> • es 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 domain-name/myindex/mytype。 <p>端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式：</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。</p> <p>目標元素中包含urn.</p>	是的

回應範例

之間包含的XML

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> 標記顯示如何為儲存區設定與搜尋整合端點的整合。在此範例中、物件中繼資料會傳送至名為的Elasticsearch索引 current 並輸入named 2017 這是以AWS網域命名的 records。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

相關資訊

["使用租戶帳戶"](#)

放置時段中繼資料通知組態

「置入庫位元資料」通知組態要求可讓您針對個別的庫位啟用搜尋整合服務。您在要求本文中提供的中繼資料通知組態XML、會指定將中繼資料傳送至目的地搜尋索引的物件。

您必須擁有儲存區的S3：PuttBucketMetadata通知權限、或是帳戶根權限、才能完成此作業。

申請

要求必須在要求本文中包含中繼資料通知組態。每個中繼資料通知組態都包含一或多個規則。每個規則都會指定要套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。

物件可依物件名稱的前置詞進行篩選。例如、您可以傳送具有前置碼之物件的中繼資料 /images 至一個目的地、以及具有前置碼的物件 /videos 到另一個。

有重疊前置字元的組態無效、提交時會遭到拒絕。例如、含有前置字元物件規則的組態 test 和第二個規則、用於具有前置碼的物件 test2 不允許。

目的地必須使用StorageGRID 不實端點的URN來指定。當中繼資料通知組態已提交、或要求以失敗的方式提交時、端點必須存在 400 Bad Request。錯誤訊息指出：Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

下表說明中繼資料通知組態XML中的元素。

名稱	說明	必要
Metadata NotifiationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifiationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	<p>符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。</p> <p>若要符合所有物件、請指定一個空白首碼。</p> <p>包含在Rule元素中。</p>	是的
目的地	<p>規則目的地的容器標記。</p> <p>包含在Rule元素中。</p>	是的
urn	<p>傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN：</p> <ul style="list-style-type: none"> • es 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 domain-name/myindex/mytype。 <p>端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式：</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。</p> <p>目標元素中包含urn.</p>	是的

申請範例

此範例顯示啟用儲存庫的搜尋整合功能。在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

```

PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

在此範例中、物件的中繼資料會與前置詞相符 `/images` 會傳送至一個目的地、而物件中繼資料則會與前置詞相符 `/videos` 傳送至第二個目的地。

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

由搜尋整合服務產生的JSON

當您啟用儲存區的搜尋整合服務時、每次新增、更新或刪除物件中繼資料或標記時、都會產生Json文件並傳送至目的地端點。

此範例顯示Json範例、該範例可在具有金鑰的物件產生時產生 SGWS/Tagging.txt 在名為的儲存區中建立 test。test 儲存區沒有版本、因此 versionId 標記為空白。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

中繼資料通知中包含的物件中繼資料

此表格列出JSON文件中所有欄位、這些欄位會在啟用搜尋整合時傳送至目的地端點。

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱	說明
儲存區和物件資訊	鏟斗	庫位名稱
儲存區和物件資訊	金鑰	物件金鑰名稱
儲存區和物件資訊	版本ID	物件版本、適用於版本控制的儲存區中的物件
儲存區和物件資訊	區域	例如、儲存區 us-east-1
系統中繼資料	尺寸	HTTP用戶端可見的物件大小（以位元組為單位）
系統中繼資料	md5	物件雜湊

類型	項目名稱	說明
使用者中繼資料	中繼資料 <i>key:value</i>	物件的所有使用者中繼資料、做為金鑰值配對
標記	標記 <i>key:value</i>	為物件定義的所有物件標記、做為金鑰值配對



針對標記和使用者中繼資料StorageGRID、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

相關資訊

["使用租戶帳戶"](#)

取得儲存使用量要求

「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。

帳戶使用的儲存容量及其儲存區可透過修改後的 Listbuckets 要求取得 `x-ntap-sg-usage` 查詢參數。儲存區的使用量會與系統處理的PUT和DELETE要求分開追蹤。使用值可能會在處理要求時延遲、使其符合預期值、尤其是系統負載過重時。

根據預設StorageGRID、功能區會嘗試使用強大的全域一致性來擷取使用資訊。如果無法達成強大的全球一致性、StorageGRID 會嘗試以強大的站台一致性來擷取使用資訊。

您必須具有S3：`listAllMyb`桶 權限、或是帳戶root、才能完成此作業。

申請範例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示一個帳戶、其中兩個儲存區中有四個物件和12個位元組的資料。每個儲存區包含兩個物件和六個位元組的資料。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本管理

儲存的每個物件版本都有助於 ObjectCount 和 DataBytes 回應中的值。刪除標記不會新增至 ObjectCount 總計。

相關資訊

["一致性值"](#)

已過時的資源桶要求、適用於舊版法規遵循

已過時的資源桶要求、適用於舊版法規遵循

您可能需要使用StorageGRID Sfs3 REST API來管理使用舊版Compliance功能所建立的儲存區。

法規遵循功能已過時

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

如果您先前已啟用「全域符合性」設定、StorageGRID 則會在「支援物件鎖定」中啟用「全域S3物件鎖定」設定。您不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、您可以視需要使用StorageGRID「S3 REST API」來管理任何現有的符合舊規範的儲存庫。

- ["使用 S3 REST API 來設定 S3 物件鎖定"](#)
- ["使用ILM管理物件"](#)
- ["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章》"](#)

過時的法規遵循要求：

- ["已過時-將資源桶要求修改以符合法規要求"](#)

SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

- ["已過時 - 取得 Bucket 法規遵循"](#)

Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

- ["已過時 - 符合 Put Bucket 規範"](#)

「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

已過時：為符合性而修改 **CreateBucket** 要求

SGCompliance XML元素已過時。以前、您可以將此 StorageGRID 自訂元素納入 CreateBucket 要求的選用 XML 要求本文、以建立符合法規的儲存區。

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：



- ["使用 S3 REST API 來設定 S3 物件鎖定"](#)
- ["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章》"](#)

您無法再建立啟用「法規遵循」的新庫位。如果您嘗試使用 CreateBucket 要求修改來建立新的相容貯體、則會傳回下列錯誤訊息：

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

已過時：**Get Bucket Compliance**要求

Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。



先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：

- "使用 S3 REST API 來設定 S3 物件鎖定"
- "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您必須具有S3：GetBucketCompliance權限、或是帳戶root、才能完成此作業。

申請範例

此範例要求可讓您決定名為的儲存區的法規遵循設定 mybucket。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

在回應XML中、<SGCompliance> 列出庫位有效的法規遵循設定。此回應範例顯示儲存區的法規遵循設定、其中每個物件將保留一年（525600分鐘）、從物件擷取到網格開始算起。此庫位目前沒有合法持有。每個物件將在一年後自動刪除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>
```

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。

名稱	說明
LegalHold	<ul style="list-style-type: none"> • 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	<ul style="list-style-type: none"> • 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

錯誤回應

如果儲存區建立不合法規要求、則回應的HTTP狀態代碼為 404 Not Found 的S3錯誤代碼 `XNoSuchBucketCompliance`。

已過時：提出資源桶法規遵循要求

「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。



先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：

- ["使用 S3 REST API 來設定 S3 物件鎖定"](#)
- ["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"](#)

您必須具有S3：PuttBucketCompliance權限、或是帳戶root、才能完成此作業。

在發出「放入庫位」法規遵循要求時、您必須為法規遵循設定的每個欄位指定一個值。

申請範例

此範例要求會修改名為的儲存區的規範設定 mybucket。在此範例中、物件位於 mybucket 現在將保留兩年（1、051、200分鐘）、而非一年、從物件進入網格開始算起。此庫位沒有合法持有。每個物件將在兩年後自動刪除。

```

PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>

```

名稱	說明
RetentionPeriodMinutes	<p>新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。</p> <ul style="list-style-type: none"> • 重要 * 為 RetentionPeriodMinutes 指定新值時、您必須指定一個值、該值等於或大於該貯體目前的保留期間。設定貯體保留期間之後、您就無法減少該值、只能增加該值。
LegalHold	<ul style="list-style-type: none"> • 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	<ul style="list-style-type: none"> • 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

法規遵循設定的一致性

當您更新S3儲存區的法規遵循設定、並提出「置放儲存區法規遵循」要求時StorageGRID、即可嘗試更新整個網格的儲存區中繼資料。根據預設、StorageGRID 會使用 * 強式全域 * 一致性來保證所有資料中心站台和所有包含儲存區中繼資料的儲存節點、對於變更的法規遵循設定、都具有寫入後讀取一致性。

如果 StorageGRID 因為某個站台的資料中心站台或多個儲存節點無法使用而無法達到 * 強式全域 * 一致性、則回應的 HTTP 狀態代碼為 503 Service Unavailable.

如果您收到此回應、則必須聯絡網格管理員、以確保所需的儲存服務能夠儘快提供。如果網格管理員無法在每個網站上提供足夠的儲存節點、技術支援可能會強制使用 **Strong-site** 一致性、引導您重試失敗的要求。



除非技術支援人員指示您遵守、否則切勿強迫 * 強式站台 * 一致性、除非您瞭解使用此層級的潛在後果。

當一致性降至 * 強式站台 * 時、StorageGRID 保證更新的法規遵循設定只會對站台內的用戶端要求具有讀寫後一致性。這表示StorageGRID 在所有站台和儲存節點都可用之前、此儲存區的設定可能會暫時有多個不一致的設定。不一致的設定可能會導致非預期和非預期的行為。例如、如果您將貯體置於合法保留之下、而您強制降低一致性、則貯體先前的法規遵循設定（即合法保留）可能會繼續在某些資料中心站台生效。因此、您認為合法保留的物件、可能會在保留期間到期時遭到刪除、使用者或自動刪除（如果已啟用）。

若要強制使用 * 強式站台 * 一致性、請重新發出「放置庫位」法規遵循要求、並加入 Consistency-Control HTTP要求標頭、如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

錯誤回應

- 如果儲存區建立不合法規要求、則回應的HTTP狀態代碼為 404 Not Found。
- 如果 RetentionPeriodMinutes 在要求中、HTTP狀態代碼小於儲存區目前的保留期間 400 Bad Request。

相關資訊

["已過時：將資源桶要求修改以符合法規要求"](#)

儲存庫和群組存取原則

使用貯體和群組存取原則

支援使用Amazon Web Services (AWS) 原則語言、讓S3租戶能夠控制對這些儲存區內的儲存區和物件的存取。StorageGRID此系統實作S3 REST API原則語言的子集。StorageGRIDS3 API的存取原則是以Json撰寫。

存取原則總覽

支援的存取原則有兩種。StorageGRID

- * Bucket Policies *、使用 GetBucketPolicy、PuttBucketPolicy 及 DeleteBucketPolicy S3 API 作業來管理。庫位原則會附加至庫位、因此這些原則可設定為控制庫位擁有者帳戶或其他帳戶中的使用者對庫位及其物件的存取。庫位原則僅適用於一個庫位、可能也適用於多個群組。
- 群組原則、使用租戶管理程式或租戶管理API進行設定。群組原則會附加至帳戶中的群組、因此這些原則會設定為允許該群組存取該帳戶所擁有的特定資源。群組原則僅適用於一個群組、可能也適用於多個儲存區。



群組原則和儲存庫原則之間的優先順序沒有差異。

根據Amazon定義的特定語法、執行庫位和群組原則。StorageGRID每個原則內部都有一組原則聲明、每個陳述都包含下列元素：

- 對帳單ID (Sid) (選用)
- 效果

- 委託人/未委託人
- 資源/未資源
- 行動/未行動
- 條件（選用）

原則陳述是使用此結構來指定權限：在套用<condition>時，授與<effect>允許/拒絕<Principle>執行<Action"。

每個原則元素都用於特定功能：

元素	說明
SID	Sid元素為選用項目。Sid僅供使用者說明使用。它會儲存、但StorageGRID 不會被作業系統解讀。
效果	使用effect元素來確定是否允許或拒絕指定的作業。您必須使用支援的Action元素關鍵字、識別您允許（或拒絕）的貯體或物件作業。
委託人/未委託人	您可以允許使用者、群組和帳戶存取特定資源並執行特定動作。如果要求中未包含S3簽名、則可指定萬用字元（*）做為主體、以匿名存取。根據預設、只有root帳戶可以存取該帳戶擁有的資源。 您只需要在庫位原則中指定主要元素。對於群組原則而言、附加原則的群組是內含的主體元素。
資源/未資源	資源元素可識別儲存區和物件。您可以使用Amazon資源名稱（ARN）來允許或拒絕貯體和物件的權限、以識別資源。
行動/未行動	「行動」和「效果」元素是權限的兩個元件。當群組要求資源時、系統會將資源的存取權限授予或拒絕。除非您特別指派權限、否則存取會遭拒、但您可以使用明確拒絕來覆寫其他原則所授予的權限。
條件	條件元素為選用項目。條件可讓您建置運算式、以判斷何時應套用原則。

在Action元素中、您可以使用萬用字元（*）來指定所有作業或作業子集。例如、此動作會比對S3：GetObject、S3：PuttObject和S3：Delete物件等權限。

```
s3:*Object
```

在資源元素中、您可以使用萬用字元（*）和（?）。星號（*）與0個以上的字元相符、但問號（?）符合任何單一字元。

在 Principal 元素中、除了設定匿名存取外、不支援萬用字元、這會將權限授予每個人。例如、您將萬用字元（*）設為主要值。

```
"Principal": "*"
```

```
"Principal":{"AWS":"*"}
```

在下列範例中、陳述式使用的是「效果」、「主要」、「行動」和「資源」元素。此範例顯示完整的Bucket原則聲明、其使用「允許」的效果來賦予主體（即管理群組） `federated-group/admin` 以及財務團隊 `federated-group/finance` 的權限 `s3:ListBucket` 在名為的儲存區上 `mybucket` 和行動 `s3:GetObject` 儲存區內的所有物件。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

儲存區原則的大小上限為20、480個位元組、而且群組原則的大小上限為5、120個位元組。

原則的一致性

根據預設、您對群組原則所做的任何更新最終都是一致的。當群組原則變得一致時、由於原則快取、變更可能需要額外 15 分鐘才能生效。根據預設、您對儲存庫原則所做的任何更新都是非常一致的。

您可以視需要變更庫位原則更新的一致性保證。例如、您可能想要在站台中斷期間變更貯體原則。

在此情況下、您可以設定 `Consistency-Control PuttBucketPolicy` 要求中的標頭、或者您可以使用 `Put Bucket` 一致性要求。當貯體原則變得一致時、由於原則快取、變更可能需要額外 8 秒的時間才能生效。



如果您將一致性設定為不同的值來因應暫時情況、請務必在完成時將貯體層級設定恢復為原始值。否則、所有未來的貯體要求都會使用修改後的設定。

在原則聲明中使用ARN

在原則聲明中、ARN用於主要和資源元素。

- 使用此語法來指定S3資源ARN：

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 使用此語法來指定身分識別資源ARN（使用者和群組）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他考量事項：

- 您可以使用星號 (*) 做為萬用字元、以比對物件金鑰內的零個或多個字元。
- 可以在物件金鑰中指定的國際字元、應使用Json utf-8或Json \u轉義序列進行編碼。不支援百分比編碼。

"RFC 2141 URN語法"

PuttBucketPolicy 作業的 HTTP 要求主體必須以 charset=UTF-8 編碼。

在原則中指定資源

在原則聲明中、您可以使用資源元素來指定允許或拒絕權限的儲存區或物件。

- 每個原則聲明都需要資源元素。在原則中、資源會以元素表示 Resource`或是`NotResource 排除。
- 您可以使用S3資源ARN來指定資源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以物件機碼內使用原則變數。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 資源值可以指定在建立群組原則時尚未存在的儲存區。

在原則中指定主體

使用主體元素來識別原則聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 庫位原則中的每個原則聲明都必須包含主要元素。群組原則中的原則聲明不需要 Principal 元素、因為群組被理解為主體。
- 在原則中、主體會以元素「Principal」表示、或是以「NotPrincipal」表示排除。
- 帳戶型身分識別必須使用ID或ARN來指定：

```
"Principal": { "AWS": "account_id" }
"Principal": { "AWS": "identity_arn" }
```

- 此範例使用租戶帳戶ID 27233906934684427525、其中包含帳戶root和帳戶中的所有使用者：

```
"Principal": { "AWS": "27233906934684427525" }
```

- 您只能指定帳戶根目錄：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定特定的聯盟使用者（「Alex」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 您可以指定特定的聯盟群組（「經理」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers" }
```

- 您可以指定匿名主體：

```
"Principal": "*" 
```

- 為了避免混淆、您可以使用使用者UUID、而非使用者名稱：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

例如、假設Alex離開組織和使用者名稱 Alex 已刪除。如果有新的Alex加入組織、則指派給他們的任務相同 Alex 使用者名稱、新使用者可能會不小心繼承授予原始使用者的權限。

- 主要值可以指定建立儲存區原則時尚未存在的群組/使用者名稱。

在原則中指定權限

在原則中、會使用Action元素來允許/拒絕資源的權限。您可以在原則中指定一組權限、以元素「Action」表示、或是以「NotAction」表示排除權限。每個元素都對應到特定的S3 REST API作業。

這些表格列出套用至儲存區的權限、以及套用至物件的權限。



Amazon S3 現在會針對 PutBucketReplication 和 DeleteBucketReplication 動作使用 S3:PutReplicationConfiguration 權限。針對每個行動使用不同的權限、這與原始的Amazon S3規格相符。StorageGRID



使用 Put 覆寫現有值時會執行刪除。

套用至貯體的權限

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：建立桶	建立庫位	是的。 • 附註 *：僅用於群組原則。
S3：刪除資源桶	刪除Bucket	
S3：刪除BucketMetadata通知	刪除時段中繼資料通知組態	是的
S3：刪除BucketPolicy	刪除BucketPolicy	
S3：刪除複製組態	刪除 BucketReplication	是、請分別授予和刪除權限
S3：GetBucketAcl	GetBucketAcl	
S3：GetBucketCompliance	取得資源桶法規遵循（已過時）	是的
S3：GetBucketConsistency	取得庫位一致性	是的
S3：GetBucketCORS	GetBucketCors	
S3：GetEncryptionConfiguration	GetBucketEncryption	

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3 : GetBucketLastAccessTime	取得時段上次存取時間	是的
S3 : GetBucketLocation	GetBucketLocation	
S3 : GetBucketMetadata通知	取得Bucket中繼資料通知組態	是的
S3 : GetBucketNotification	GetBucketNotificationConfiguration	
S3 : GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3 : GetBucketPolicy	GetBucketPolicy	
S3 : GetBucketting	GetBucketTagging	
S3 : GetBucketVersion	GetBucketVersion	
S3 : Get生命週期組態	GetBucketLifecycleConfiguration	
S3 : GetReplicationConfiguration	GetBucketReplication	
S3 : ListAllMyb桶	<ul style="list-style-type: none"> • 列表桶 • 取得儲存使用量 	<p>是的、用於取得儲存使用量。</p> <p>• 附註 * : 僅用於群組原則。</p>
S3 : 清單庫	<ul style="list-style-type: none"> • 清單物件 • 標題庫 • RestoreObject 	
S3 : listBucketMultiPartUploads	<ul style="list-style-type: none"> • ListMultipartUploads • RestoreObject 	
S3 : listBucketVerions	取得Bucket版本	
S3 : PuttBucketCompliance	符合資源桶規範 (已過時)	是的
S3 : PuttBucketConsistency	實現庫位一致性	是的

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：PuttBucketCORS	<ul style="list-style-type: none"> 刪除 BucketCors † PuttBucketCors 	
S3：PuttEncryptionConfiguration	<ul style="list-style-type: none"> 刪除 BucketEncryption PuttBucketEncryption 	
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的
S3：PuttBucketNotification	PutBucketNotificationConfiguration	
S3：PuttBucketObjectLockConfiguration	<ul style="list-style-type: none"> 與一起使用的 CreateBucket x-amz-bucket-object-lock-enabled:true 要求標頭（也需要S3：建立桶權限） PutObjectLockConfiguration 	
S3：PuttBucketPolicy	PuttBucketPolicy	
S3：PuttBucketting	<ul style="list-style-type: none"> 刪除標籤† PuttBucketTagging 	
S3：PuttBucketVersion	PuttBucketVersion	
S3：Putt升降 器組態	<ul style="list-style-type: none"> 刪除 BucketLifecycle † PuttBucketLifecycleConfiguration 	
S3：PuttReplicationConfiguration	PutBucketReplication	是、請分別授予和刪除權限

套用至物件的權限

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：中止多重角色上傳	<ul style="list-style-type: none"> AbortMultiPart上傳 RestoreObject 	

權限	S3 REST API作業	客製StorageGRID 化以供選擇
S3 : BypassGovernanceRetention	<ul style="list-style-type: none"> • 刪除物件 • 刪除物件 • PutObjectRetention 	
S3 : 刪除物件	<ul style="list-style-type: none"> • 刪除物件 • 刪除物件 • RestoreObject 	
S3 : 刪除ObjectTagging	刪除ObjectTagging	
S3 : 刪除ObjectVersion標記	刪除物件標籤 (物件的特定版本)	
S3 : 刪除ObjectVersion	DeleteObject (物件的特定版本)	
S3 : GetObject	<ul style="list-style-type: none"> • GetObject • 標題物件 • RestoreObject • 選取物件內容 	
S3 : GetObjectAcl	GetObjectAcl	
S3 : GetObjectLegalHold	GetObjectLegalHold	
S3 : GetObjectRetention	GetObjectRetention	
S3 : GetObjectTagging	GetObjectTagging	
S3 : GetObjectVersion標記	GetObjectTagging(物件的特定版本)	
S3 : GetObjectVersion	GetObject (物件的特定版本)	
S3 : 列出多個零件上傳零件	ListParts 、 RestoreObject	

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3 : PuttObject	<ul style="list-style-type: none"> • PuttObject • CopyObject • RestoreObject • 建立多個部分上傳 • 完成多個部分上傳 • 上傳零件 • 上傳PartCopy 	
S3 : PuttObjectLegalHold	PutObjectLegalHold	
S3 : PuttObjectRetention	PutObjectRetention	
S3 : PuttObjectTagging	PuttObjectTagging	
S3 : PuttObjectVersion標記	PutObjectTagging(物件的特定版本)	
S3 : PuttOverwriteObject	<ul style="list-style-type: none"> • PuttObject • CopyObject • PuttObjectTagging • 刪除ObjectTagging • 完成多個部分上傳 	是的
S3 : 恢復物件	RestoreObject	

使用PuttOverwriteObject權限

S3 : PuttOverwriteObject權限是套StorageGRID 用至建立或更新物件之作業的自訂功能。此權限的設定決定用戶端是否可以覆寫物件的資料、使用者定義的中繼資料或S3物件標記。

此權限的可能設定包括：

- 允許：用戶端可以覆寫物件。這是預設設定。
- * 拒絕 *：用戶端無法覆寫物件。設為「拒絕」時、PuttOverwriteObject權限的運作方式如下：
 - 如果在同一路徑找到現有物件：
 - 物件的資料、使用者定義的中繼資料或 S3 物件標記無法覆寫。
 - 任何進行中的擷取作業都會取消、並傳回錯誤。
 - 如果啟用 S3 版本設定、則「拒絕」設定會防止 PutObjectTagging 或 DeleteObjectTagging 作業修改物件及其非目前版本的 TagSet 。

- 如果找不到現有的物件、此權限將不會生效。
- 當此權限不存在時、效果與「允許」設定相同。



如果目前的 S3 原則允許覆寫、而 PutOverwriteObject 權限設定為拒絕、則用戶端無法覆寫物件的資料、使用者定義的中繼資料或物件標記。此外、如果選取 * 禁止用戶端修改 * 核取方塊（ * 組態 * > * 安全性設定 * > * 網路和物件 * ）、則該設定會覆寫 PutOverwriteObject 權限的設定。

在原則中指定條件

條件會定義原則的生效時間。條件包括運算子和金鑰值配對。

條件使用金鑰值配對進行評估。條件元素可以包含多個條件、而且每個條件可以包含多個金鑰值配對。條件區塊使用下列格式：

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

在下列範例中、ipAddress條件使用SourceIp條件金鑰。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

支援的條件運算子

條件運算子的分類如下：

- 字串
- 數字
- 布林值
- IP 位址
- null檢查

條件運算子	說明
擷取等量資料	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。
擷取NotEquals	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。

條件運算子	說明
StringEqualsIgnoreCase	根據完全相符的結果（忽略大小寫）、將金鑰與字串值進行比較。
StringNotEqualsIgnoreCase	根據否定比對（忽略大小寫）、將金鑰與字串值進行比較。
StringLike	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
StringNotLike	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據 "TRUE 或 FALSE" 比對、將金鑰與布林值進行比較。
IP地址	比較金鑰與IP位址或IP位址範圍。
NotIppAddress	根據已否定的比對、將金鑰與IP位址或IP位址範圍進行比較。
null	檢查條件金鑰是否存在於目前的要求內容中。

支援的條件金鑰

條件金鑰	行動	說明
AWS：來源Ip	IP營運者	<p>將會與傳送要求的IP位址進行比較。可用於庫位或物件作業。</p> <p>*附註：*如果S3要求是透過管理節點和閘道節點上的負載平衡器服務傳送、則這會與負載平衡器服務上游的IP位址進行比較。</p> <p>附註：如果使用第三方、不透明的負載平衡器、則會比較該負載平衡器的IP位址。任何 X-Forwarded-For 標頭將會被忽略、因為無法確定其有效性。</p>
AWS：使用者名稱	資源/身分識別	將會比較傳送者的使用者名稱、以從中傳送要求。可用於庫位或物件作業。
S3：分隔符號	<p>S3：清單儲存庫和</p> <p>S3：listBucketVerions權限</p>	將與 ListObjects 或 ListObjectVerions 要求中指定的分隔參數進行比較。
S3：<tag-key>	<p>S3：刪除ObjectTagging</p> <p>S3：刪除ObjectVersion標記</p> <p>S3：GetObject</p> <p>S3：GetObjectAcl</p> <p>3：GetObjectTagging</p> <p>S3：GetObjectVersion</p> <p>S3：GetObjectVerionAcl</p> <p>S3：GetObjectVersion標記</p> <p>S3：PutObjectAcl</p> <p>S3：PuttObjectTagging</p> <p>S3：PutObjectVersionAcl</p> <p>S3：PuttObjectVersion標記</p>	需要現有物件具有特定的標記金鑰和值。

條件金鑰	行動	說明
S3：金鑰上限	S3：清單儲存庫和 S3：listBucketVerions權 限	將與 ListObjects 或 ListObjectVerions 要求中指定的 max-keys 參數進行比較。
S3：物件鎖定剩餘保留天數	S3：PutObject	與中指定的保留截止日期比較 x-amz-object-lock-retain-until-date 要求標頭或從貯體預設保留期間計算、以確保這些值在下列要求的允許範圍內： <ul style="list-style-type: none"> • PutObject • CopyObject • 建立多個部分上傳
S3：物件鎖定剩餘保留天數	S3：PutObjectRetention	與 PutObjectRetention 要求中指定的保留截止日期進行比較、以確保其在允許範圍內。
S3：前置碼	S3：清單儲存庫和 S3：listBucketVerions權 限	將與 ListObjects 或 ListObjectVerions 要求中指定的前置參數進行比較。
<tag-key>	S3：PutObject S3：PutObjectTagging S3：PutObjectVersion標 記	當物件要求包含標記時、需要特定的標記金鑰和值。

在原則中指定變數

您可以在原則中使用變數、在原則可用時填入原則資訊。您可以在中使用原則變數 Resource 中的元素和字串比較 Condition 元素。

在此範例中、變數 `${aws:username}` 是資源元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在此範例中、變數 `${aws:username}` 是條件區塊中條件值的一部分：

```

"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}

```

變動	說明
<code>\${aws:SourceIp}</code>	使用來源Ip金鑰作為提供的變數。
<code>\${aws:username}</code>	使用UserName金鑰做為提供的變數。
<code>\${s3:prefix}</code>	使用服務專屬的前置碼作為提供的變數。
<code>\${s3:max-keys}</code>	使用服務專屬的最大金鑰作為提供的變數。
<code>\${*}</code>	特殊字元。使用字元做為文字*字元。
<code>\${?}</code>	特殊字元。使用字元做為字型?字元。
<code>\${\$}</code>	特殊字元。使用字元做為文字\$字元。

建立需要特殊處理的原則

有時候原則可能會授與安全性危險或危險的權限、以便繼續執行作業、例如封鎖帳戶的root使用者。在原則驗證期間、不像Amazon、StorageGRID 執行「支援S3 REST API」的限制較少、但在原則評估期間同樣嚴格。

原則說明	原則類型	Amazon行為	運作方式StorageGRID
拒絕root帳戶的任何權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
拒絕對使用者/群組擁有任何權限	群組	有效且強制	相同
允許外部帳戶群組擁有任何權限	鏟斗	無效的主體	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤

原則說明	原則類型	Amazon行為	運作方式StorageGRID
允許外部帳戶root或使用者擁有任何權限	鏟斗	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤	相同
允許每個人都有權執行所有動作	鏟斗	有效、但所有S3儲存區原則作業的權限都會傳回異帳戶根目錄和使用者不允許的「405方法」錯誤	相同
拒絕所有人對所有動作的權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
主體是不存在的使用者或群組	鏟斗	無效的主體	有效
資源是不存在的S3儲存區	群組	有效	相同
主體是本機群組	鏟斗	無效的主體	有效
原則會授與非擁有者帳戶（包括匿名帳戶）權限、以放置物件。	鏟斗	有效。物件由建立者帳戶擁有、且庫位原則不適用。建立者帳戶必須使用物件ACL來授與物件的存取權限。	有效。物件由庫位擁有者帳戶擁有。適用庫位政策。

一次寫入多讀（WORM）保護

您可以建立一次寫入多次讀取（WORM）儲存區、以保護資料、使用者定義的物件中繼資料、以及S3物件標記。您可以設定WORM儲存區、以允許建立新物件、並防止覆寫或刪除現有內容。請使用本文所述的其中一種方法。

為了確保覆寫永遠被拒絕、您可以：

- 從 Grid Manager 移至 * 組態 * > * 安全性 * > * 安全性設定 * > * 網路和物件 *、然後選取 * 禁止用戶端修改 * 核取方塊。
- 套用下列規則和S3原則：
 - 將PutOverwriteObject拒絕作業新增至S3原則。
 - 將刪除物件拒絕作業新增至S3原則。
 - 將 PutObject 允許作業新增至 S3 原則。



在 S3 原則中將 DeleteObject 設定為拒絕、並不會在存在「30 天後零複本」等規則時、阻止 ILM 刪除物件。



即使套用了所有這些規則和原則、也無法防範並行寫入（請參閱情況A）。它們確實能防止連續完成的覆寫（請參閱情況B）。

情況A：並行寫入（不受保護）

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

情況B：連續完成覆寫（防範）

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

相關資訊

- ["如何利用ILM規則來管理物件StorageGRID"](#)
- ["貯體原則範例"](#)
- ["群組原則範例"](#)
- ["使用ILM管理物件"](#)
- ["使用租戶帳戶"](#)

貯體原則範例

使用本節中的範例、為貯體建立 StorageGRID 存取原則。

儲存區原則會指定原則附加的儲存區存取權限。儲存區原則是使用S3 PuttBucketPolicy API進行設定。請參閱 ["在貯體上作業"](#)。

根據下列命令、可使用AWS CLI設定儲存區原則：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

範例：允許每個人只讀存取儲存區

在此範例中、每個人（包括匿名）都可以列出貯體中的物件、並對貯體中的所有物件執行 GetObject 作業。所有其他作業都將遭拒。請注意、這項原則可能並不特別有用、因為除了帳戶根目錄之外、沒有其他人擁有寫入貯體的權限。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

範例：允許同一個帳戶中的每個人都擁有完整存取權、以及其他帳戶中的每個人只讀存取庫位

在此範例中、某個指定帳戶中的每個人都可以完整存取某個儲存區、而另一個指定帳戶中的每個人只能列出該儲存區、並從開始對儲存區中的物件執行GetObject作業 shared/ 物件金鑰前置碼。



在功能區中StorageGRID、非擁有者帳戶所建立的物件（包括匿名帳戶）、均由庫位擁有者帳戶擁有。庫位原則適用於這些物件。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

範例：允許每個人只讀存取儲存區、並由指定群組進行完整存取

在此範例中、包括匿名在內的每個人都可以列出貯體、並在貯體中的所有物件上執行 GetObject 作業、而只能列出屬於群組的使用者 Marketing 在指定的帳戶中、允許完整存取。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

範例：如果用戶端位於IP範圍、則允許每個人讀取及寫入儲存區的存取權

在此範例中、每個人（包括匿名）都可以列出儲存區、並在儲存區中的所有物件上執行任何物件作業、前提是要來自指定的IP範圍（54.240.143.0至54.240.143.255、但54.240.143.188除外）。所有其他作業都會遭到拒絕、而且IP範圍以外的所有要求都會遭到拒絕。


```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

範例：允許特定同盟使用者專屬完整存取儲存區

在此範例中、聯盟使用者Alex可以完整存取 examplebucket 儲存區及其物件。所有其他使用者、包括「root」、都會明確拒絕所有作業。不過請注意、「root」永遠不會被拒絕存取權限來放置/取得/刪除 BucketPolicy。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

範例：PuttOverwriteObject權限

在此範例中 Deny PuttoverwriteObject和Delete物件的效果可確保任何人都無法覆寫或刪除物件的資料、使用者定義的中繼資料和S3物件標記。

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

群組原則範例

使用本節中的範例、為群組建置 StorageGRID 存取原則。

群組原則會指定原則所附加之群組的存取權限。沒有 Principal 原則中的元素、因為它是隱含的。群組原則是使用租戶管理程式或API來設定。

範例：使用租戶管理程式設定群組原則

當您在租戶管理器中新增或編輯群組時、可以選取群組原則、以判斷此群組成員將擁有哪些 S3 存取權限。請參閱 ["為S3租戶建立群組"](#)。

- **無S3存取**：預設選項。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
- **唯讀存取**：此群組中的使用者擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
- **完整存取**：此群組中的使用者可完整存取S3資源、包括儲存區。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
- *** 勒索軟體緩解 ***：此範例原則適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。

擁有「管理所有貯體」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（MFA）。

- **自訂**：群組中的使用者會被授予您在文字方塊中指定的權限。

範例：允許群組完整存取所有儲存區

在此範例中、除非庫位原則明確拒絕、否則群組的所有成員都可以完整存取租戶帳戶擁有的所有庫位。

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

範例：允許群組唯讀存取所有儲存區

在此範例中、除非資源庫原則明確拒絕、否則群組的所有成員都擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組成員完全存取儲存庫中的「資料夾」

在此範例中、群組成員只能在指定的儲存區中列出及存取其特定資料夾（金鑰首碼）。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

稽核記錄中追蹤的S3作業

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。您可以在稽核記錄中檢閱 S3 特定的稽核訊息、以取得有關貯體和物件作業的詳細資料。

稽核記錄中追蹤的庫位作業

- 建立庫位
- 刪除Bucket
- 刪除 Bucket tagging
- 刪除物件
- GetBucketTagging
- 標題庫
- 清單物件
- ListObjectVersions
- 符合資源需求
- PutBucketTagging
- PutBucketVersion

稽核記錄中追蹤的物件作業

- 完成多個部分上傳
- CopyObject
- 刪除物件
- GetObject
- 標題物件
- PuttObject
- RestoreObject
- SelectObject
- 上傳組件（當 ILM 規則使用平衡或嚴格擷取時）
- 上傳 PartCopy（當 ILM 規則使用平衡或嚴格擷取時）

相關資訊

- ["存取稽核記錄檔"](#)
- ["用戶端寫入稽核訊息"](#)
- ["用戶端讀取稽核訊息"](#)

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。