



使用 **S3 REST API**

StorageGRID software

NetApp
July 23, 2026

目錄

使用 S3 REST API	1
StorageGRID S3 REST API 支援的版本和更新	1
支援的版本	1
S3 REST API 支援的更新	1
StorageGRID 中支援的 S3 API 要求	4
常用的 URI 查詢參數和請求標頭	4
"AbortMultipartUpload"	4
"CompleteMultipartUpload"	5
"CopyObject"	5
"CreateBucket"	6
"CreateMultipartUpload"	6
>DeleteBucket"	7
>DeleteBucketCors"	7
>DeleteBucketEncryption"	7
>DeleteBucketLifecycle"	8
>DeleteBucketPolicy"	8
>DeleteBucketReplication"	8
>DeleteBucketTagging"	8
>DeleteObject"	9
>DeleteObjects"	9
>DeleteObjectTagging"	9
"GetBucketAcl"	9
"GetBucketCors"	10
"GetBucketEncryption"	10
"GetBucketLifecycleConfiguration"	10
"GetBucketLocation"	10
"GetBucketNotificationConfiguration"	11
"GetBucketPolicy"	11
"GetBucketReplication"	11
"GetBucketTagging"	11
"GetBucketVersioning"	12
"GetObject"	12
"GetObjectAcl"	13
"GetObjectLegalHold"	13
"GetObjectLockConfiguration"	13
"GetObjectRetention"	13
"GetObjectTagging"	14
"HeadBucket"	14
"HeadObject"	14
>ListBuckets"	15
>ListMultipartUploads"	15
>ListObjects"	15

"ListObjectsV2"	16
"ListObjectVersions"	16
"ListParts"	16
"PutBucketCors"	17
"PutBucketEncryption"	17
"PutBucketLifecycleConfiguration"	17
"PutBucketNotificationConfiguration"	18
"PutBucketPolicy"	19
"PutBucketReplication"	19
"PutBucketTagging"	19
"PutBucketVersioning"	20
"PutObject"	20
"PutObjectLegalHold"	21
"PutObjectLockConfiguration"	21
"PutObjectRetention"	21
"PutObjectTagging"	21
"RestoreObject"	22
"SelectObjectContent"	22
"UploadPart"	22
"UploadPartCopy"	22
測試 StorageGRID S3 REST API 組態	23
StorageGRID 如何實作 S3 REST API	25
StorageGRID S3 REST API 如何解決衝突的用戶端請求	25
StorageGRID S3 REST API 如何平衡可用性和一致性	25
StorageGRID 如何使用物件版本控制	28
使用 S3 REST API 設定 StorageGRID S3 Object Lock	28
了解 StorageGRID 的 S3 生命週期組態	33
使用 StorageGRID 實作 S3 REST API 的建議	37
支援 Amazon S3 REST API	38
StorageGRID 中支援的 S3 REST API 作業和限制	38
StorageGRID S3 REST API 如何驗證請求	39
StorageGRID 中支援的服務作業	39
StorageGRID 中的 S3 儲存貯體作業和實作詳細資料	40
對物件進行操作	47
多部分上傳作業	73
StorageGRID S3 REST API 錯誤回應	81
StorageGRID 自訂操作	84
StorageGRID 中支援的自訂儲存貯體作業	84
使用 GET Bucket consistency 請求在 StorageGRID 中檢索儲存桶一致性層級	84
使用 PUT Bucket 一致性請求在 StorageGRID 中指定一致性層級	86
使用 GET Bucket last access time 請求從 StorageGRID 中擷取儲存區的最後存取時間狀態	86
使用 PUT Bucket last access time 請求在 StorageGRID 中啟用和停用最後存取時間更新	87
使用 StorageGRID 中的 DELETE Bucket 中繼資料通知組態要求停用搜尋整合服務	88

使用 GET Bucket 元資料通知組態要求在 StorageGRID 中設定搜尋整合	88
使用 PUT Bucket 元資料通知設定請求在 StorageGRID 中啟用搜尋整合服務	91
使用 GET Storage Usage 請求擷取 StorageGRID 中的帳戶和儲存桶儲存使用量	96
已棄用的舊版法規遵循儲存桶請求	97
管理存取原則	102
StorageGRID 如何使用 AWS 原則來控制對 S3 儲存貯體和物件的存取	102
StorageGRID S3 REST API 工作階段原則範例	118
StorageGRID S3 REST API 儲存區原則範例	119
StorageGRID S3 REST API 群組原則範例	124
StorageGRID 稽核日誌中追蹤的 S3 操作	127
稽核日誌中追蹤的儲存桶操作	127
稽核日誌中追蹤的物件操作	128

使用 S3 REST API

StorageGRID S3 REST API 支援的版本和更新

StorageGRID 支援 Simple Storage Service (S3) API，該 API 以一組表述性狀態轉移 (REST) Web 服務的形式實作。

支援 S3 REST API 可讓您將為 S3 Web 服務開發的服務導向應用程式與使用 StorageGRID 系統的內部環境物件儲存連接起來。用戶端應用程式目前對 S3 REST API 呼叫的使用只需進行極少的變更。

支援的版本

StorageGRID 支援以下特定版本的 STS、S3 和 HTTP：

項目	版本
STS AssumeRole API 規範	"Amazon Web Services (AWS) 文件：Amazon Assumerole API 參考" 有關 AssumeRole 的詳細資訊，請參閱 "設定 AssumeRole"。
S3 API 規範	"AWS 文件：Amazon Simple Storage Service API 參考"
HTTP	1.1 有關 HTTP 的詳細資訊，請參閱 HTTP/1.1 (RFCs 7230-35)。 "IETF RFC 2616：超文字傳輸協定 (HTTP/1.1)" 注意：StorageGRID 不支援 HTTP/1.1 管線。

S3 REST API 支援的更新

發布	註解
12.0	- 為管理介面新增了跨來源資源共享 (CORS) 支援，允許另一個網域使用管理 API 存取 StorageGRID 中的資料。"深入瞭解"。 - 新增對 STS AssumeRole 和工作階段原則的支援。請參閱 "工作階段原則範例"。您可以在租戶群組下設定 AssumeRole。

發布	註解
11.9	• 新增對以下請求和支援標頭的預先計算 SHA-256 Checksum 值的支援。您可以使用此功能來驗證上傳物件的完整性： ◦ CompleteMultipartUpload：x-amz-checksum-sha256 ◦ CreateMultipartUpload：x-amz-checksum-algorithm ◦ GetObject：x-amz-checksum-mode ◦ HeadObject：x-amz-checksum-mode ◦ ListParts ◦ PutObject：x-amz-checksum-sha256 ◦ UploadPart：x-amz-checksum-sha256 • 新增了網格系統管理員控制租戶層級保留和 Compliance 設定的功能。這些設定會影響 S3 物件鎖定設定。 ◦ 儲存桶預設保留模式和物件保留模式：治理或合規性（如果網格系統管理員允許）。 ◦ 儲存桶預設保留期間和物件 Retain Until Date：必須小於或等於網格系統管理員設定的最大保留期間所允許的值。 • 改進了對 `aws-chunked` 內容編碼和串流 `x-amz-content-sha256` 值的支援。限制： ◦ 如果存在，`chunk-signature` 則為可選，且未經驗證 ◦ 如果存在，`x-amz-trailer` 則忽略該內容。
11.8	更新了 S3 操作的名稱，使其與 "Amazon Web Services (AWS) 文件：Amazon Simple Storage Service API 參考"中使用的名稱相符。
11.7	• 已新增 "快速參考：支援的 S3 API 請求"。 • 新增對搭配 S3 Object Lock 使用 GOVERNANCE 模式的支援。 • 新增了對 StorageGRID 特有的 x-ntap-sg-cgr-replication-status GET Object 和 HEAD Object 請求回應標頭的支援。此回應標頭提供物件在跨網格複寫中的複寫狀態。 • SelectObjectContent requests 現在支援 Parquet 物件。
11.6	• 新增在 GET Object 和 HEAD Object 請求中使用 partNumber 請求參數的支援。 • 為 S3 Object Lock 在儲存桶層級新增預設保留模式和預設保留期間的支援。 • 新增對原則條件鍵 s3:object-lock-remaining-retention-days 的支援，用於設定物件的允許保留期間範圍。 • 已將單一 PUT Object 操作的最大_建議_大小變更為 5 GiB（5,368,709,120 位元組）。如果物件大於 5 GiB，請改用分段上傳。

發布	註解
11.5	• 新增管理儲存桶加密的支援。 • 新增對 S3 Object Lock 的支援，並棄用舊版法規遵循請求。 • 新增對版本化儲存桶使用 DELETE Multiple Objects 的支援。 • The `Content-MD5` 請求標頭現已正確支援。
11.4	• 新增了對 DELETE Bucket tagging、GET Bucket tagging 和 PUT Bucket tagging 的支援。不支援成本分配標籤。 • 對於在 StorageGRID 11.4 中建立的儲存桶，不再需要限制物件金鑰名稱以符合效能最佳實務。 • 新增對 `s3:ObjectRestore:Post` 事件類型的儲存桶通知支援。 • AWS 現在強制執行分段上傳的大小限制。分段上傳中的每個部分都必須介於 5 MiB 和 5 GiB 之間。最後一個部分可以小於 5 MiB。 • 新增對 TLS 1.3 的支援
11.3	• 新增使用客戶提供的金鑰對物件資料進行伺服器端加密 (SSE-C) 的支援。 • 新增對 DELETE、GET 和 PUT Bucket 生命週期操作（僅限到期行動）以及 <code>x-amz-expiration</code> 回應標頭的支援。 • 更新了 PUT Object、PUT Object - Copy 和 Multipart Upload，以描述在擷取時使用同步放置的 ILM 規則的影響。 • TLS 1.1 加密演算法已不再受支援。
11.2	新增對 POST 物件還原的支援，可用於雲端儲存池。新增對在群組原則和儲存貯體原則中使用 AWS 語法來定義 ARN、原則條件鍵和原則變數的支援。使用 StorageGRID 語法的現有群組原則和儲存貯體原則將繼續獲得支援。 *注意：*在其他組態 JSON/XML 中使用 ARN/URN 的方式（包括在自訂 StorageGRID 功能中使用的方式）沒有改變。
11.1	新增對跨來源資源共用 (CORS)、S3 用戶端連線至網格節點的 HTTP，以及儲存桶法規遵循設定的支援。
11.0	新增了為儲存桶設定平台服務（CloudMirror 複寫、通知和 Elasticsearch 搜尋整合）的支援。此外，還新增了對儲存桶物件標籤位置限制和 Available 一致性的支援。
10.4	新增對 ILM 掃描變更的支援，包括版本控制、端點網域名稱頁面更新、原則中的條件和變數、原則範例以及 PutOverwriteObject 權限。
10.3	新增版本控制支援。
10.2	新增對群組和儲存桶存取原則以及多部分複本（Upload Part - Copy）的支援。

發布	註解
10.1	新增對多部分上傳、虛擬託管式請求及 v4 驗證的支援。
10.0	StorageGRID 系統已初步支援 S3 REST API。目前支援的 <i>Simple Storage Service API Reference</i> 版本為 2006-03-01。

StorageGRID 中支援的 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 操作。



若要查看每個操作的 AWS 文件，請選擇標題中的連結。

常用的 URI 查詢參數和請求標頭

除非另有說明，否則支援以下常見的 URI 查詢參數：

- versionId (物件操作所需)

除非另有說明，否則支援以下常用請求標頭：

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

相關資訊

- ["S3 REST API 實作詳細資訊"](#)
- ["Amazon Simple Storage Service API 參考：常用請求標頭"](#)

"AbortMultipartUpload"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加 URI 查詢參數：

- uploadId

請求本文

無

`${post_edited_translations.segment}`

"多部分上傳作業"

"CompleteMultipartUpload"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加 URI 查詢參數：

- uploadId
- x-amz-checksum-sha256

請求體 **XML** 標籤

StorageGRID 支援以下請求本文 XML 標籤：

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

`${post_edited_translations.segment}`

"CompleteMultipartUpload"

"CopyObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

- 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>`

請求本文

無

`${post_edited_translations.segment}`

"CopyObject"

"CreateBucket"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

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

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"CreateMultipartUpload"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- 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>`

請求本文

無

`${post_edited_translations.segment}`

"CreateMultipartUpload"

"DeleteBucket"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"DeleteBucketCors"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"DeleteBucketEncryption"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"DeleteBucketLifecycle"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

- "儲存貯體上的作業"
- "建立 S3 生命週期組態"

"DeleteBucketPolicy"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"DeleteBucketReplication"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"DeleteBucketTagging"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"DeleteObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加請求標頭：

- x-amz-bypass-governance-retention

請求本文

無

\${post_edited_translations.segment}

["對物件進行操作"](#)

"DeleteObjects"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加請求標頭：

- x-amz-bypass-governance-retention

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

\${post_edited_translations.segment}

["對物件進行操作"](#)

"DeleteObjectTagging"

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

["對物件進行操作"](#)

"GetBucketAcl"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

["儲存貯體上的作業"](#)

"GetBucketCors"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketEncryption"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketLifecycleConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

- "儲存貯體上的作業"
- "建立 S3 生命週期組態"

"GetBucketLocation"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketNotificationConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketPolicy"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketReplication"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketTagging"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetBucketVersioning"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"GetObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) URI 查詢參數，以及以下附加 URI 查詢參數：

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

以及以下附加請求標頭：

- 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

請求本文

無

\${post_edited_translations.segment}

"GetObject"

"GetObjectAcl"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"對物件進行操作"

"GetObjectLegalHold"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"GetObjectLockConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"GetObjectRetention"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"GetObjectTagging"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

["對物件進行操作"](#)

"HeadBucket"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

\${post_edited_translations.segment}

["儲存貯體上的作業"](#)

"HeadObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

- x-amz-checksum-mode
- 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

請求本文

無

\${post_edited_translations.segment}

["HeadObject"](#)

"ListBuckets"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

無

`${post_edited_translations.segment}`

[服務操作](#) > [ListBuckets](#)

"ListMultipartUploads"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) 以及以下附加參數：

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

請求本文

無

`${post_edited_translations.segment}`

["ListMultipartUploads"](#)

"ListObjects"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) 以及以下附加參數：

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

請求本文

無

`${post_edited_translations.segment}`

["儲存貯體上的作業"](#)

"ListObjectsV2"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) 以及以下附加參數：

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

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"ListObjectVersions"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) 以及以下附加參數：

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

請求本文

無

\${post_edited_translations.segment}

"儲存貯體上的作業"

"ListParts"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) 以及以下附加參數：

- max-parts

- part-number-marker
- uploadId

請求本文

無

`${post_edited_translations.segment}`

["ListMultipartUploads"](#)

"PutBucketCors"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

`${post_edited_translations.segment}`

["儲存貯體上的作業"](#)

"PutBucketEncryption"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求體 **XML** 標籤

StorageGRID 支援以下請求本文 XML 標籤：

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

`${post_edited_translations.segment}`

["儲存貯體上的作業"](#)

"PutBucketLifecycleConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求體 **XML** 標籤

StorageGRID 支援以下請求本文 XML 標籤：

- And
- Days

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

`${post_edited_translations.segment}`

- "儲存貯體上的作業"
- "建立 S3 生命週期組態"

"PutBucketNotificationConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求體 **XML** 標籤

StorageGRID 支援以下請求本文 XML 標籤：

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration

- Value

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"PutBucketPolicy"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

有關支援的 JSON 本文欄位的詳細資訊，請參閱 ["使用儲存桶和群組存取原則"](#)。

"PutBucketReplication"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求體 **XML** 標籤

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

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"PutBucketTagging"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

`${post_edited_translations.segment}`

"儲存貯體上的作業"

"PutBucketVersioning"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求體參數

StorageGRID 支援以下請求本文參數：

- VersioningConfiguration
- Status

\${post_edited_translations.segment}

"儲存貯體上的作業"

"PutObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- 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>

請求本文

- 物件的二進位資料

\${post_edited_translations.segment}

"PutObject"

"PutObjectLegalHold"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"PutObjectLockConfiguration"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"PutObjectRetention"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)，以及以下附加標頭：

- x-amz-bypass-governance-retention

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

\${post_edited_translations.segment}

"使用 S3 REST API 設定 S3 物件鎖定"

"PutObjectTagging"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的所有請求本文參數。

\${post_edited_translations.segment}

"對物件進行操作"

"RestoreObject"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

有關支援的本文欄位的詳細資訊，請參閱 ["RestoreObject"](#)。

"SelectObjectContent"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#)。

請求本文

如需支援的本文欄位的詳細資訊，請參閱下列內容：

- ["使用 S3 Select"](#)
- ["SelectObjectContent"](#)

"UploadPart"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) URI 查詢參數，以及以下附加 URI 查詢參數：

- partNumber
- uploadId

以及以下附加請求標頭：

- x-amz-checksum-sha256
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

請求本文

- 零件的二進位資料

`${post_edited_translations.segment}`

["UploadPart"](#)

"UploadPartCopy"

URI 查詢參數和請求標頭

StorageGRID 支援此請求的所有 [常用參數和標頭](#) URI 查詢參數，以及以下附加 URI 查詢參數：

- partNumber

- uploadId

以及以下附加請求標頭：

- 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

請求本文

無

`${post_edited_translations.segment}`

["UploadPartCopy"](#)

測試 StorageGRID S3 REST API 組態

您可以使用 Amazon Web Services 命令列介面（AWS CLI）來測試您與系統的連線，並驗證您是否可以讀取和寫入物件。

開始之前

- 您已從 ["aws.amazon.com/cli"](https://aws.amazon.com/cli) 下載並安裝 AWS CLI。
- （可選）您擁有["已建立負載平衡器端點"](#)。否則，您需要知道要連線的儲存節點的 IP 位址和要使用的連接埠號碼。請參閱["用戶端連接的 IP 位址和連接埠"](#)。
- 您有["建立了一個 S3 租戶帳戶"](#)。
- 您已登入租戶並["建立了存取金鑰"](#)。

有關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. 請輸入您建立的帳戶的存取金鑰 ID。

- c. 請輸入您建立之帳戶的秘密存取金鑰。
 - d. 請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** 選擇 JSON。
2. 建立一個儲存桶。

本範例假設您已設定負載平衡器端點以使用 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
```

如果儲存桶建立成功，則會傳回儲存桶的位置，如下例所示：

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

3. 上傳一個物件。

```
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，則會傳回一個 Etag，它是物件資料的雜湊值。

4. 列出儲存桶的內容，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. 刪除該物件。

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

6. 刪除儲存桶。

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

StorageGRID 如何實作 S3 REST API

StorageGRID S3 REST API 如何解決衝突的用戶端請求

如果用戶端請求發生衝突，例如兩個用戶端寫入同一個金鑰，則依照「最新優先」的原則進行解決。

「最新獲勝」評估的時間是根據 StorageGRID 系統完成給定請求的時間，而不是根據 S3 用戶端開始操作的時間。

StorageGRID S3 REST API 如何平衡可用性和一致性

一致性機制在物件的可用度和這些物件在不同儲存節點和站點間的一致性之間取得了平衡。您可以根據應用程式的需要變更一致性設定。

預設情況下，StorageGRID 保證新建立物件的寫入後讀取一致性。任何在 PUT 操作成功完成後執行的 GET 操作都可以讀取新寫入的資料。對現有物件的覆寫、中繼資料更新和刪除操作則最終一致。

如果要以不同的一致性執行物件操作，可以：

- 指定 [每個儲存桶](#) 的一致性。
- 指定 [每個 API 作業](#) 的一致性。
- 若要變更預設的網格級一致性，請執行下列操作之一：
 - 在 Grid Manager 中，前往 **Configuration > System > Storage settings > Default bucket consistency**。
 - 。



對網格整體一致性的變更僅適用於變更設定後所建立的儲存桶。若要了解變更的詳細資訊，請參閱位於 `/var/local/log` 的稽核日誌（搜尋 **consistencyLevel**）。

一致性值

一致性會影響 StorageGRID 用於追蹤物件的中繼資料在節點間的分佈方式。一致性會影響用戶端請求對物件的可用度。

您可以將儲存桶或 API 作業的一致性設定為下列值之一：

- 全部：所有節點立即接收物件中繼資料，否則要求將失敗。
- **Strong-global**：保證所有站台上所有用戶端請求的寫入後讀取一致性。設定 Quorum 語意後，將套用以下行為：
 - 當網格具有三個或更多站台時，允許用戶端要求具有站台故障容許度。雙站台網格將不具備站台故障容許度。
 - 如果其中一個站台停機，以下 S3 作業將無法成功：
 - DeleteBucketEncryption

- PutBucketBranch
- PutBucketEncryption
- PutBucketVersioning
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObjectRetention

如果需要，您可以 `"${post_edited_translations.segment}"`。

- **Strong-site**：物件中繼資料會立即分發至站台內的其他節點。保證站台內所有用戶端請求的寫後讀一致性。
- **Read-after-new-write**：為新物件提供寫入後讀取一致性，並為物件更新提供最終一致性。提供高可用度和資料保護保證。建議在大多數情況下使用。
- **Available**：為新物件和物件更新提供最終一致性。對於 S3 儲存貯體，請僅在需要時使用（例如，對於包含極少讀取之記錄值的儲存貯體，或針對不存在的金鑰進行 HEAD 或 GET 作業）。不支援 S3 FabricPool 儲存貯體。

使用「新寫後讀取」和「可用」一致性

當 HEAD 或 GET 操作使用「新寫後讀取」一致性時，StorageGRID 會分多個步驟執行查詢，如下所示：

- 它首先使用低一致性查詢物件。
- 如果查詢失敗，則會在下一個一致性值處重複查詢，直到達到與 strong-global 的行為等效的一致性。

如果 HEAD 或 GET 操作使用「新寫後讀取」一致性，但物件不存在，則物件查找將一律達到與 strong-global 行為相同的一致性。由於此一致性要求每個站台都必須有物件中繼資料的多個複本，因此如果同一站台上有多個儲存節點無法使用，您可能會收到大量 500 Internal Server 錯誤。

除非您需要類似 Amazon S3 的一致性保證，否則可以透過將一致性設為「Available」來避免 HEAD 和 GET 操作出現這些錯誤。當 HEAD 或 GET 操作使用「Available」一致性時，StorageGRID 僅提供最終一致性。它不會以提高一致性的方式重試失敗的操作，因此不需要提供多個物件中繼資料複本。

指定 API 操作的一致性

若要為單一 API 操作設定一致性，該操作必須支援對應的一致性值，並且必須在請求標頭中指定一致性。此範例將 GetObject 操作的一致性設定為「Strong-site」。

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



對於 PutObject 和 GetObject 操作，必須使用相同的一致性。

指定儲存桶的一致性

若要設定儲存桶的一致性，可以使用 StorageGRID **"PUT Bucket 一致性"** 請求。或者，也可以**"變更儲存桶的一致性"**從 Tenant Manager 進行設定。

設定儲存桶的一致性時，請注意以下事項：

- 設定儲存桶的一致性，可決定對儲存桶中的物件或儲存桶組態執行的 S3 操作所使用的一致性。此設定不會影響對儲存桶本身的操作。
- 單一 API 操作的一致性會置換儲存桶的一致性。
- 通常情況下，儲存桶應使用預設的一致性原則「新寫入後讀取」。如果請求無法正常運作，請盡可能變更應用程式用戶端的行為。或者，設定用戶端為每個 API 請求指定一致性原則。只有在萬不得已的情況下才在儲存桶層級設定一致性原則。

一致性與 ILM 規則如何互動以影響資料保護

您選擇的一致性設定和 ILM 規則都會影響物件的保護方式。這些設定可能會互動。

例如，物件儲存時採用的一致性策略會影響物件中繼資料的初始位置，而為 ILM 規則選擇的擷取行為則會影響物件副本的初始位置。由於 StorageGRID 需要存取物件的中繼資料和資料才能滿足用戶端請求，因此為一致性策略和擷取行為選擇相符的保護層級可以提供更好的初始資料保護和更可預測的系統回應。

以下**"擷取選項"**適用於 ILM 規則：

雙重承諾

StorageGRID 會立即建立物件的臨時副本，並向用戶端傳回成功。ILM 規則中指定的副本會在可能的情況下建立。

嚴格

在向用戶端返回成功之前，必須完成 ILM 規則中指定的所有副本。

均衡

StorageGRID 會在擷取時嘗試建立 ILM 規則中指定的所有副本；如果無法全部建立，則會建立臨時副本並向用戶端傳回成功資訊。ILM 規則中指定的副本會在條件允許的情況下建立。

一致性規則和 ILM 規則如何互動的範例

假設您有一個三站台網格，具有以下 ILM 規則和以下一致性：

- **ILM 規則**：建立三個物件複本，一個在本機站台，每個遠端站台各一個。使用 Strict 擷取行為。
- **一致性**：強全域性（物件中繼資料立即分發至多個站台）。

當用戶端將物件儲存到網格時，StorageGRID 會建立所有三個物件複本，並將中繼資料分發到多個站台，然後向用戶端傳回成功。

在收到擷取成功訊息時，該物件已受到完整保護，可防止遺失。例如，如果本機站台在擷取後不久發生故障，物件資料和物件中繼資料的複本仍會存在於遠端站台。您可以從其他站台完整擷取該物件。

如果您改為使用相同的 ILM 規則和強站台一致性，則用戶端可能會在物件資料複寫到遠端站台之後，但在物件中繼資料發配到該處之前，收到成功訊息。在這種情況下，物件中繼資料的保護層級與物件資料的保護層級不

符。如果在本機站台擷取後不久即遺失，則物件中繼資料將會遺失。該物件將無法擷取。

一致性與 ILM 規則之間的相互關係可能非常複雜。如果您需要協助，請聯絡 NetApp。

StorageGRID 如何使用物件版本控制

如果您希望保留每個物件的多個版本，可以設定儲存貯體的版本控制狀態。啟用儲存貯體的版本控制有助於防止意外刪除物件，並可讓您擷取和還原物件的早期版本。

StorageGRID 系統實作版本控制，支援大多數功能，但有一些限制。StorageGRID 支援每個物件最多 10,000 個版本。

物件版本控制可以與 StorageGRID 資訊生命週期管理 (ILM) 或 S3 儲存桶生命週期組態結合使用。您必須為每個儲存桶明確啟用版本控制。啟用儲存桶的版本控制後，新增至該儲存桶的每個物件都會被指派一個版本 ID，該 ID 由 StorageGRID 系統產生。

使用 MFA（多因素驗證）時，不支援刪除功能。



版本控制只能在以 StorageGRID 版本 10.3 或更新版本建立的儲存桶上啟用。

ILM 和版本控制

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 原則重新評估它們。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。如果啟用了版本控制，則包含先前擷取的版本。ILM 掃描會將新的 ILM 變更套用至先前擷取的物件。

對於已啟用版本控制的 S3 儲存貯體中的物件，版本控制支援可讓您建立使用「非目前時間」作為參考時間的 ILM 規則（在 ["建立 ILM 規則精靈的步驟 1"](#) 中，針對「僅將此規則套用至舊版物件？」此問題選擇*是*）。當物件更新時，其先前版本將變為非目前版本。使用「非目前時間」篩選器，您可以建立原則來減少物件先前版本對儲存設備的影響。



當您使用分段上傳作業上傳物件的新版本時，原始物件的非目前時間反映的是建立新版本分段上傳的時間，而不是分段上傳完成的時間。在少數情況下，原始版本的非目前時間可能比目前版本的時間早幾個小時甚至幾天。

相關資訊

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

使用 S3 REST API 設定 StorageGRID S3 Object Lock

如果您的 StorageGRID 系統已啟用全域 S3 Object Lock 設定，則可以建立已啟用 S3 Object Lock 的儲存桶。您可以為每個儲存桶指定預設保留，也可以為每個物件版本指定保留設定。

如何為儲存桶啟用 S3 物件鎖定

如果您的 StorageGRID 系統已啟用全域 S3 物件鎖定設定，您可以在建立每個儲存桶時選擇性地啟用 S3 物件鎖定。

S3 Object Lock 是一項永久性設定，只能在建立儲存桶時啟用。儲存桶建立後，無法新增或停用 S3 Object Lock。

若要為儲存桶啟用 S3 物件鎖定，請使用下列任一方法：

- 使用租用戶管理器建立儲存桶。參見["建立 S3 儲存桶"](#)。
- 使用含有 `x-amz-bucket-object-lock-enabled` 請求標頭的 `CreateBucket` 請求建立儲存桶。請參閱 ["儲存貯體上的作業"](#)。

S3 Object Lock 需要儲存桶版本控制，該功能在建立儲存桶時會自動啟用。您無法暫停儲存桶的版本控制。請參閱["物件版本控制"](#)。

儲存桶的預設保留設定

當為儲存桶啟用 S3 Object Lock 時，您可以選擇為儲存桶啟用預設保留，並指定預設保留模式和預設保留期間。

預設保留模式

- 處於合規模式：
 - 物件只有在達到其保留期限後才能刪除。
 - `${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
- 處於 GOVERNANCE 模式：
 - 擁有 `s3:BypassGovernanceRetention` 權限的使用者可以使用 ``x-amz-bypass-governance-retention: true`` 請求標頭繞過保留設定。
 - `${post_edited_translations.segment}`
 - 這些使用者可以增加、減少或移除物件的保留截止日期。

預設保留期間

每個儲存桶都可以設定預設保留期間，以年或天為單位。

如何為儲存桶設定預設保留期間

若要設定儲存桶的預設保留期限，可以使用下列任一方法：

- 從租戶管理器管理儲存桶設定。請參閱 ["建立 S3 儲存桶"](#) 和 ["更新 S3 物件鎖定預設保留"](#)。
- 向儲存桶發出 `PutObjectLockConfiguration` 請求，以指定預設模式和預設天數或年數。

PutObjectLockConfiguration

此 `PutObjectLockConfiguration` 請求可讓您設定和修改已啟用 S3 物件鎖定的儲存桶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。

當新的物件版本被擷取至儲存桶時，如果未指定 `x-amz-object-lock-mode`` 和 ``x-amz-object-lock-retain-until-date`，則套用預設保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，則使用預設保留期間來計算保留截止日期。

如果在擷取物件版本後修改了預設保留期間，則物件版本的保留截止日期保持不變，不會使用新的預設保留期間重新計算。

您必須擁有 `s3:PutBucketObjectLockConfiguration` 權限，或具備帳戶根目錄存取權，才能完成此操作。

The Content-MD5 請求標頭必須在 PUT 請求中指定。

請求範例

此範例為儲存桶啟用 S3 Object Lock，並將預設保留模式設為 COMPLIANCE，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>
```

如何確定儲存桶的預設保留期間

若要確定儲存桶是否啟用了 S3 Object Lock，並查看預設保留模式和保留期間，請使用下列任一方法：

- 在租戶管理員中查看儲存桶。請參閱[查看 S3 儲存桶](#)。
- 發出 GetObjectLockConfiguration 請求。

GetObjectLockConfiguration

GetObjectLockConfiguration 請求可讓您確定是否為儲存桶啟用了 S3 物件鎖定，如果已啟用，則查看是否為該儲存桶配置了預設保留模式和保留期間。

當新的物件版本擷取至儲存桶時，如果未指定 x-amz-object-lock-mode，則套用預設保留模式。如果未指定 x-amz-object-lock-retain-until-date，則使用預設保留期間來計算保留截止日期。

您必須擁有 `s3:GetBucketObjectLockConfiguration` 權限，或具備帳戶根目錄存取權，才能完成此操作。

請求範例

```
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>
```

如何為物件指定保留設定

啟用了 S3 物件鎖定的儲存桶可以包含具有 S3 物件鎖定保留設定的物件和不具有 S3 物件鎖定保留設定的物件的組合。

物件層級的保留設定透過 S3 REST API 指定。物件的保留設定會置換儲存桶的任何預設保留設定。

您可以為每個物件指定以下設定：

- 保留模式：COMPLIANCE 或 GOVERNANCE。
- **Retain-until-date**：指定 StorageGRID 必須保留物件版本多久的日期。

- 在 COMPLIANCE 模式下，如果保留截止日期在未來，則可以擷取該物件，但無法修改或刪除。保留截止日期可以延長，但不能縮短或移除。
- 在 GOVERNANCE 模式下，擁有特殊權限的使用者可以繞過保留期限設定。他們可以在物件版本的保留期間結束前將其刪除。他們還可以增加、減少甚至移除保留期限。
- 合法持有：對物件版本套用合法持有會立即鎖定該物件。例如，您可能需要對與調查或法律糾紛相關的物件套用合法持有。合法持有沒有失效日期，會一直有效，直到明確移除為止。

物件的合法持有設定獨立於保留模式和保留截止日期。如果某個物件版本處於合法持有，則任何人均無法刪除該版本。

若要在新增物件版本至儲存桶時指定 S3 Object Lock 設定，請發出 "PutObject"、"CopyObject" 或 "CreateMultipartUpload" 請求。

您可以使用以下方法：

- x-amz-object-lock-mode，可以是 COMPLIANCE 或 GOVERNANCE（區分大小寫）。



如果指定了 x-amz-object-lock-mode，則必須也指定 x-amz-object-lock-retain-until-date。

- x-amz-object-lock-retain-until-date
 - 保留至日期的值必須採用特定格式 2020-08-10T21:46:00Z。允許使用秒的小數部分，但僅保留 3 位小數（毫秒精度）。不允許使用其他 ISO 8601 格式。
 - 保留截止日期必須在未來。
- x-amz-object-lock-legal-hold

如果合法持有設定為「ON」（區分大小寫），則物件將被置於合法持有狀態。如果合法持有設定為「OFF」，則不會進行任何合法持有。任何其他值都會導致 400 Bad Request (InvalidArgument) 錯誤。

如果您使用以下任何請求標頭，請注意以下限制：

- 如果 PutObject 要求中存在任何 x-amz-object-lock-* 要求標頭，則需要 Content-MD5 要求標頭。Content-MD5 不需要用於 CopyObject 或 CreateMultipartUpload。
- 如果儲存桶未啟用 S3 物件鎖定，且 `x-amz-object-lock-\*` 請求標頭存在，則會傳回 400 Bad Request (InvalidRequest) 錯誤。
- 該 PutObject 請求支援使用 `x-amz-storage-class: REDUCED\_REDUNDANCY` 以符合 AWS 行為。但是，當物件擷取至已啟用 S3 物件鎖定的儲存桶時，StorageGRID 將一律執行雙重提交擷取。
- 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（如果已配置，且請求發送者擁有正確的 s3:Get* 權限）。

您可以使用 s3:object-lock-remaining-retention-days 原則條件鍵來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

如果需要更新現有物件版本的合法持有或保留設定，可以執行下列物件子資源操作：

- `PutObjectLegalHold`

如果新的合法持有值為 ON，該物件將置於合法持有。如果合法持有值為 OFF，合法持有將解除。

- `PutObjectRetention`

- 模式值可以是 COMPLIANCE 或 GOVERNANCE（區分大小寫）。
- 保留至日期的值必須採用特定格式 2020-08-10T21:46:00Z。允許使用秒的小數部分，但僅保留 3 位小數（毫秒精度）。不允許使用其他 ISO 8601 格式。
- 如果物件版本已設定保留至日期，則只能增加該日期值。新值必須為未來日期。

如何使用 **GOVERNANCE** 模式

擁有 `s3:BypassGovernanceRetention` 權限的使用者可以略過使用治理模式物件的作用中保留設定。任何 DELETE 或 `PutObjectRetention` 操作都必須包含 `x-amz-bypass-governance-retention:true` 請求標頭。這些使用者可以執行以下額外操作：

- 在物件版本的保留期間到期之前，執行 `DeleteObject` 或 `DeleteObjects` 操作以刪除物件版本。

受合法持有的物件無法刪除。合法持有必須關閉。

- 執行 `PutObjectRetention` 操作，在物件的保留期間到期之前，將物件版本的模式從 GOVERNANCE 變更為 COMPLIANCE。

絕對不允許將模式從 COMPLIANCE 變更為 GOVERNANCE。

- 執行 `PutObjectRetention` 操作，以增加、減少或移除物件版本的保留期間。

相關資訊

- ["使用 S3 Object Lock 管理物件"](#)
- ["使用 S3 物件鎖定來保留物件"](#)
- ["Amazon Simple Storage Service 使用者指南：鎖定物件"](#)

了解 **StorageGRID** 的 **S3** 生命週期組態

您可以建立 S3 生命週期組態來控制何時從 StorageGRID 系統中刪除特定物件。

本節中的簡單範例說明如何透過 S3 生命週期組態來控制何時從特定的 S3 儲存桶中刪除（過期）某些物件。本節中的範例僅用於說明目的。有關建立 S3 生命週期組態的完整詳細資訊，請參閱 ["Amazon Simple Storage Service 使用者指南：物件生命週期管理"](#)。請注意，StorageGRID 僅支援過期動作，不支援轉換動作。

生命週期組態是什麼？

生命週期組態是一組應用於特定 S3 儲存桶中物件的規則。每條規則都指定哪些物件會受到影響，以及這些物件何時過期（在特定日期或經過一定天數後）。

StorageGRID 在生命週期組態中支援最多 1,000 條生命週期規則。每條規則可以包含以下 XML 元素：

- 過期時間：當達到指定日期或達到指定天數時（從物件被擷取之日起算），刪除該物件。
- NoncurrentVersionExpiration：當達到指定的天數時，從物件變成非目前版本之日起刪除該物件。
- 篩選（前綴，標籤）
- 狀態
- ID

每個物件都遵循 S3 儲存桶生命週期或 ILM 原則的保留設定。設定 S3 儲存桶生命週期後，對於符合該儲存桶生命週期篩選器的物件，生命週期過期動作會置換 ILM 原則。不符合該儲存桶生命週期篩選器的物件，則使用 ILM 原則的保留設定。如果物件符合儲存桶生命週期篩選器，但未明確指定過期動作，則不會使用 ILM 原則的保留設定，並且預設物件版本將永久保留。請參閱 ["S3 儲存桶生命週期和 ILM 原則的優先順序範例"](#)。

因此，即使 ILM 規則中的放置指令仍然適用於某個物件，該物件也可能從網格中移除。或者，即使針對該物件的任何 ILM 放置指令都已失效，該物件也可能保留在網格中。如需詳細資訊，請參閱 ["ILM 如何在物件的整個生命週期中運作"](#)。



儲存桶生命週期組態可用於已啟用 S3 Object Lock 的儲存桶，但舊版 Compliant 儲存桶不支援儲存桶生命週期組態。

StorageGRID 支援使用下列儲存桶操作來管理生命週期組態：

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

建立生命週期組態

建立生命週期組態的第一步是建立一個包含一條或多條規則的 JSON 檔案。例如，以下 JSON 檔案包含三條規則：

1. 規則 1 僅適用於前綴為 `category1/` 且 ``key2`` 值為 ``tag2`` 的物件。此 ``Expiration`` 參數指定符合篩選條件的物件將於 2020 年 8 月 22 日午夜過期。
2. 規則 2 僅適用於前綴為 `category2/` 的物件。此 ``Expiration`` 參數指定符合篩選條件的物件將在擷取後 100 天過期。



指定天數的規則是相對於物件擷取時間而言的。如果目前日期超過擷取日期加上指定天數，則在套用生命週期組態後，某些物件可能會立即從儲存桶中移除。

3. 規則 3 僅適用於前綴為 `category3/` 的物件。此 ``Expiration`` 參數指定任何符合物件的非目前版本將在變成非目前版本後 50 天過期。

```

{
  "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儲存桶

建立生命週期組態檔案後，透過發出 PutBucketLifecycleConfiguration 請求將其套用到儲存桶。

此請求將範例檔案中的生命週期組態套用至名為 `testbucket` 的儲存貯體中的物件。

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

若要驗證生命週期組態是否已成功套用到儲存桶，請發出 GetBucketLifecycleConfiguration 請求。例如：

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

成功回應會列出您剛剛套用的生命週期組態。

驗證儲存貯體生命週期到期是否適用於物件

您可以在發出 PutObject、HeadObject 或 GetObject 請求時，確定生命週期組態中的過期規則是否適用於特定物件。如果規則適用，則回應將包含一個 `Expiration` 參數，用於指示物件的過期時間以及符合的過期規則。



由於儲存桶生命週期會置換 ILM，因此 `expiry-date` 顯示的日期是物件實際刪除的日期。如需詳細資訊，請參閱[如何確定物件保留](#)。

例如，此 PutObject 請求於 2020 年 6 月 22 日發出，並將物件放入 `testbucket` 儲存桶中。

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

成功回應表示該物件將在 100 天後（2020 年 10 月 1 日）過期，並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 請求用於取得 testbucket 儲存桶中相同物件的中繼資料。

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

成功回應包含物件的中繼資料，並指示該物件將在 100 天後過期，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貯體，`x-amz-expiration` 回應標頭僅適用於物件的目前版本。

使用 StorageGRID 實作 S3 REST API 的建議

在實作搭配 StorageGRID 使用的 S3 REST API 時，您應該遵循以下建議。

針對不存在物件的 HEAD 建議

如果您的應用程式會例行檢查某個物件是否存在於預期該物件實際上不存在的路徑，則應使用「Available」"[\\${post_edited_translations.segment}](#)"一致性。例如，如果您的應用程式在向某個位置執行 PUT 操作之前先執行 HEAD 操作，則應使用「Available」一致性。

否則，如果 HEAD 操作找不到物件，當同一站台的兩個或多個儲存節點無法使用或遠端站台無法連線時，您可能會收到大量 500 內部伺服器錯誤。

您可以使用"[PUT Bucket 一致性](#)"請求為每個儲存桶設定「可用」一致性，也可以在單一 API 操作的請求標頭中指定一致性。

物件鍵的建議

請根據儲存貯體首次建立時間，遵循以下物件索引鍵名稱建議。

在 StorageGRID 11.4 或更早版本中建立的儲存桶

- 不要使用隨機值作為物件鍵的前四個字元。這與 AWS 先前關於鍵前綴的建議相反。相反，請使用非隨機、非唯一的前綴，例如 `image`。
- 如果您遵循 AWS 之前的建議，在鍵前綴中使用隨機且唯一的字元，請在物件鍵前加上目錄名稱作為前綴。也就是說，請使用以下格式：

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

而不是這種格式：

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

在 **StorageGRID 11.4** 或更高版本中建立的儲存桶

限制物件金鑰名稱以符合效能最佳實務並非必要。在大多數情況下，您可以為物件金鑰名稱的前四個字元使用隨機值。



但有一種例外情況，即某些 S3 工作負載會在短時間內持續刪除所有物件。為了將此使用案例的效能影響降至最低，可以每隔幾千個物件變更金鑰名稱的前導部分，例如新增日期。例如，假設一個 S3 用戶端通常每秒寫入 2,000 個物件，而 ILM 或儲存桶生命週期原則在三天後刪除所有物件。為了將效能影響降至最低，您可以採用以下模式命名金鑰：

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

關於「範圍讀取」的建議

如果"[用於壓縮儲存物件的全域選項](#)"已啟用，S3 用戶端應用程式應避免執行指定要傳回位元組範圍的 `GetObject` 操作。這些「範圍讀取」操作效率低下，因為 StorageGRID 必須有效地解壓縮物件才能存取所要求的位元組。從非常大的物件中要求少量位元組範圍的 `GetObject` 操作效率尤其低下；例如，從 50 GB 的壓縮物件中讀取 10 MB 範圍的效率很低。

如果從壓縮物件讀取範圍，用戶端請求可能會逾時。



如果需要壓縮物件，且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時間。

支援 Amazon S3 REST API

StorageGRID 中支援的 S3 REST API 作業和限制

StorageGRID 系統實作了 Simple Storage Service API（API 版本 2006-03-01），支援大多數操作，但存在一些限制。在整合 S3 REST API 用戶端應用程式時，您需要了解具體的實作細節。

StorageGRID 系統同時支援虛擬託管式請求和路徑式請求。

日期處理

StorageGRID 實作的 S3 REST API 僅支援有效的 HTTP 日期格式。

StorageGRID 系統僅支援所有接受日期值的標頭之有效 HTTP 日期格式。日期的時間部分可以採用格林威治標準時間（GMT）格式，或採用協調世界時（UTC）格式，但不含時區偏移量（必須指定 +0000）。如果在請求中包含 `x-amz-date` 標頭，它將覆寫 Date 請求標頭中指定的任何值。使用 AWS Signature Version 4 時，由於不支援 date 標頭，因此簽署的請求中必須包含 `x-amz-date` 標頭。

常用要求標頭

StorageGRID 系統支援由 "[Amazon Simple Storage Service API 參考：常用請求標頭](#)" 定義的通用請求標頭，但有一個例外。

要求標頭	實作
授權	完全支援 AWS Signature Version 2 支援 AWS Signature Version 4，但以下情況除外： 當您在 <code>x-amz-content-sha256</code> 中提供實際的有效負載 Checksum 值時，該值將在未經驗證的情況下被接受，就像已為標頭提供值 <code>UNSIGNED-PAYLOAD</code> 一樣。當您提供 <code>x-amz-content-sha256</code> 標頭值且該值隱含 <code>aws-chunked</code> 串流時（例如 <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>），系統不會針對區塊資料驗證區塊簽章。

常用回應標頭

StorageGRID 系統支援 *Simple Storage Service API Reference* 中定義的所有常見回應標頭，只有一個例外。

回應標頭	實作
<code>x-amz-id-2</code>	未使用

StorageGRID S3 REST API 如何驗證請求

StorageGRID 系統支援使用 S3 API 對物件進行驗證和匿名存取。

S3 API 支援簽章版本 2 和簽章版本 4，用於驗證 S3 API 請求。

經過驗證的要求必須使用您的存取金鑰 ID 和秘密存取金鑰進行簽署。

StorageGRID 系統支援兩種驗證方法：HTTP Authorization 標頭和使用查詢參數。

使用 HTTP Authorization 標頭

HTTP Authorization 標頭用於所有 S3 API 操作，但儲存桶原則允許的匿名請求除外。Authorization 標頭包含驗證請求所需的所有簽名資訊。

使用查詢參數

您可以使用查詢參數向 URL 新增驗證資訊。這稱為 URL 預簽名，可用於授予對特定資源的臨時存取。擁有預簽名 URL 的用戶端無需知道秘密存取金鑰即可存取資源，這使您能夠為第三方提供對資源的受限存取。

StorageGRID 中支援的服務作業

StorageGRID 系統支援對服務執行下列操作。

操作	實作
ListBuckets (之前名為 GET 服務)	已實作所有 Amazon S3 REST API 行為。如有更改，恕不另行通知。
取得儲存使用情況	StorageGRID " 取得儲存使用情況 " 要求會告訴您某個帳戶正在使用的總儲存設備量，以及與該帳戶關聯的每個儲存桶的儲存設備使用情況。這是對服務執行的操作，路徑為 /，並新增了自訂查詢參數 (?x-ntap-sg-usage) 。
OPTIONS /	用戶端應用程式無需提供 S3 身分驗證認證資料，即可向儲存節點上的 S3 連接埠發出 `OPTIONS /` 請求，以確定儲存節點是否可用。您可以使用此請求進行監控，或允許外部負載平衡器識別儲存節點何時發生故障。

StorageGRID 中的 S3 儲存貯體作業和實作詳細資料

StorageGRID 系統為每個 S3 租戶帳戶支援最多 5,000 個儲存桶。

每個網格最多可以有 100,000 個儲存桶。

為了支援 5,000 個儲存桶，網格中的每個儲存節點必須至少有 64 GB 的 RAM。

儲存桶名稱限制遵循 AWS 美國標準區域限制，但為了支援 S3 虛擬託管式請求，您應該進一步將其限制為 DNS 命名慣例。

如需更多資訊，請參閱下列內容：

- "[Amazon Simple Storage Service 使用者指南：儲存桶配額、限制與約束](#)"
- "[設定 S3 端點網域名稱](#)"

ListObjects (GET Bucket) 和 ListObjectVersions (GET Bucket 物件版本) 操作支援 StorageGRID "[一致性值](#)"。

您可以檢查是否已為各個儲存桶啟用或停用上次存取時間更新。請參閱"[取得儲存桶上次存取時間](#)"。

下表說明 StorageGRID 如何實作 S3 REST API 儲存桶操作。若要執行任何這些操作，必須提供帳戶所需的存取憑證。

操作	實作
CreateBucket	建立新的儲存桶。建立儲存桶後，您將成為該儲存桶的擁有者。 - 儲存桶名稱必須符合以下規則： - 必須在每個 StorageGRID 系統中是唯一的（而不僅僅是在租戶帳戶內是唯一的）。 - 必須符合 DNS 規範。 - 必須包含至少 3 個字元，且不超過 63 個字元。 - 可以是一個或多個標籤的系列，相鄰標籤之間以句點分隔。每個標籤必須以小寫字母或數字開頭和結尾，且只能使用小寫字母、數字和連字號。 - 不能看起來像文字格式的 IP 位址。 - 在虛擬託管風格的請求中，不應使用句點。句點會導致伺服器萬用字元憑證驗證出現問題。 - 預設情況下，儲存貯體是在 us-east-1 區域中建立；不過，您可以使用要求本文中的 LocationConstraint 要求元素來指定不同的區域。使用 LocationConstraint 元素時，您必須指定已使用 Grid Manager 或 Grid Management API 定義之區域的確切名稱。如果您不知道應使用的區域名稱，請聯絡您的系統管理員。 注意：如果您的 CreateBucket 要求使用了 StorageGRID 中未定義的區域，則會發生錯誤。 - 您可以透過新增 `x-amz-bucket-object-lock-enabled` 請求標頭來建立啟用了 S3 物件鎖定的儲存桶。請參閱"使用 S3 REST API 設定 S3 物件鎖定"。 建立儲存桶時必須啟用 S3 物件鎖定。儲存桶建立後無法新增或停用 S3 物件鎖定。S3 物件鎖定需要儲存桶版本控制，該功能會在建立儲存桶時自動啟用。
DeleteBucket	刪除儲存桶。
DeleteBucketCors	刪除儲存桶的 CORS 組態。
DeleteBucketEncryption	刪除儲存桶中的預設加密。現有加密物件仍保持加密狀態，但新增至儲存桶中的任何新物件都不會加密。
DeleteBucketLifecycle	從儲存桶中刪除生命週期組態。請參閱 "建立 S3 生命週期組態" 。
DeleteBucketPolicy	刪除附加至儲存桶的原則。
DeleteBucketReplication	刪除附加至儲存貯體的複寫組態。

操作	實作
DeleteBucketTagging	使用 `tagging` 子資源從儲存桶中移除所有標籤。 注意：如果此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤並已賦值。如果存在 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤，請勿發出 DeleteBucketTagging 要求。而應發出僅包含 `NTAP-SG-ILM-BUCKET-TAG` 標籤及其賦值的 PutBucketTagging 要求，以移除儲存桶中的所有其他標籤。請勿修改或移除 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤。
GetBucketAcl	傳回肯定回應以及儲存桶擁有者的 ID、DisplayName 和權限，表示擁有者對儲存桶擁有完全存取權限。
GetBucketCors	傳回 `cors` 儲存桶的組態。
GetBucketEncryption	傳回儲存桶的預設加密組態。
GetBucketLifecycleConfiguration (之前名為 GET Bucket lifecycle)	傳回儲存桶的生命週期組態。參見 "建立 S3 生命週期組態" 。
GetBucketLocation	傳回在 CreateBucket 請求中使用 LocationConstraint 元素設定的區域。如果儲存桶的區域為 `us-east-1`，則該區域傳回空字串。
GetBucketNotificationConfiguration (之前名為 GET Bucket notification)	傳回附加至儲存貯體的通知組態。
GetBucketPolicy	傳回附加至儲存貯體的原則。
GetBucketReplication	傳回附加至儲存貯體的複寫組態。
GetBucketTagging	使用 `tagging` 子資源傳回儲存桶的所有標籤。 注意：如果為此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤被賦予一個值。請勿修改或移除此標籤。
GetBucketVersioning	此實作使用 `versioning` 子資源傳回儲存桶的版本控制狀態。 • <i>blank</i>: 版本控制從未啟用（儲存桶為「未版本化」） • 已啟用：版本控制已啟用 • 已暫停：版本控制功能先前已啟用，現已暫停

操作	實作
GetObjectLockConfiguration	傳回儲存桶的預設保留模式和預設保留期間（如果已設定）。 請參閱 "使用 S3 REST API 設定 S3 物件鎖定" 。
HeadBucket	判斷儲存桶是否存在以及您是否擁有存取權限。 此作業會傳回： • x-ntap-sg-bucket-id：儲存桶的 UUID（UUID 格式）。 • x-ntap-sg-trace-id：關聯請求的唯一追蹤 ID。
ListObjects 和 ListObjectsV2 (之前名為 GET Bucket)	傳回儲存桶中的部分或全部物件（最多 1,000 個）。物件的 Storage Class 可以有兩個值之一，即使物件是使用 REDUCED_REDUNDANCY storage class 選項匯入的： • STANDARD，這表示該物件儲存在由 Storage Nodes 組成的儲存資源池中。 • GLACIER，這表示該物件已移至 Cloud Storage Pool 指定的外部儲存桶。 如果儲存桶中包含大量具有相同前綴的已刪除金鑰，則回應可能包含一些 `CommonPrefixes` 不包含金鑰的項目。 對於 HeadObject 和 ListObject 請求，StorageGRID 傳回的 LastModified 時間戳記精度不同，而 AWS 傳回的時間戳記精度相同，如下列範例所示： • StorageGRID HeadObject: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRID ListObject: "LastModified": "2024-09-26T16:43:24.931000+00:00" • AWS HeadObject: "LastModified": "2023-10-17T00:19:54+00:00" • AWS ListObject: "LastModified": "2023-10-17T00:19:54+00:00"
ListObjectVersions (以前稱為 GET Bucket Object versions)	對儲存貯體具有 READ 存取權限時，搭配 versions 子資源使用此操作，可列出儲存貯體中所有物件版本的中繼資料。
PutBucketCors	設定儲存桶的 CORS 組態，以便該儲存桶可以處理跨域請求。跨域資源共用 (CORS) 是一種安全性機制，可讓一個網域中的用戶端 Web 應用程式存取另一個網域中的資源。例如，假設您使用名為 `images` 的 S3 儲存桶來儲存圖形。透過設定 `images` 儲存桶的 CORS 組態，您可以允許該儲存桶中的圖像顯示在網站 `http://www.example.com` 上。

操作	實作
PutBucketEncryption	設定現有儲存桶的預設加密狀態。啟用儲存桶級加密後，新增至儲存桶的任何新物件都將被加密。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，請將 <code>SSEAlgorithm</code> 參數設為 <code>AES256</code>，並且不要使用 <code>KMSMasterKeyID</code> 參數。 如果物件上傳請求已指定加密（即請求包含 <code>x-amz-server-side-encryption-*</code> 請求標頭），則忽略儲存桶預設加密組態。
PutBucketLifecycleConfiguration (之前稱為 PUT Bucket lifecycle)	為儲存桶建立新的生命週期組態或取代現有的生命週期組態。StorageGRID 的生命週期組態中支援最多 1,000 條生命週期規則。每條規則可以包含以下 XML 元素： - 到期時間（天數、日期、ExpiredObjectDeleteMarker） - NoncurrentVersionExpiration（NewerNoncurrentVersions，NoncurrentDays） - 篩選（前綴，標籤） - 狀態 - ID StorageGRID 不支援這些動作： - AbortIncompleteMultipartUpload - 過渡 請參閱"建立 S3 生命週期組態"。若要了解儲存桶生命週期中的到期行動如何與 ILM 放置指令互動，請參閱"ILM 如何在物件的整個生命週期中運作"。 注意：儲存桶生命週期組態可用於已啟用 S3 Object Lock 的儲存桶，但不支援舊版 Compliant 儲存桶的儲存桶生命週期組態。

操作	實作
PutBucketNotificationConfiguration (之前稱為 PUT Bucket notification)	使用請求正文中包含的通知組態 XML 設定儲存貯體的通知。您應注意以下實作細節： - StorageGRID 支援將 Amazon Simple Notification Service (Amazon SNS) 主題、Kafka 主題或 Webhook 端點作為目的地。不支援 Simple Queue Service (SQS) 或 AWS Lambda 端點。 - 通知的目的地必須指定為 StorageGRID 端點的 URN。可以使用 Tenant Manager 或 Tenant Management API 建立端點。 端點必須存在，通知組態才能成功。如果端點不存在，則會傳回 400 Bad Request 錯誤，錯誤代碼為 <code>InvalidArgument</code>。 - 您無法為以下事件類型設定通知。這些事件類型*不受*支援。 <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> - StorageGRID 傳送的事件通知使用標準 JSON 格式，但不包含某些索引鍵，而其他索引鍵則使用特定值，如下列清單所示： eventSource <code>sgws:s3</code> awsRegion 未包含 x-amz-id-2 未包含 arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	設定附加到儲存桶的原則。參見 "使用儲存桶和群組存取原則" 。

操作	實作
PutBucketReplication	使用請求正文中提供的複寫組態 XML，為儲存桶設定 "StorageGRID CloudMirror 複寫"。對於 CloudMirror 複寫，您應該注意以下實作細節： - StorageGRID 僅支援複寫組態的 V1 版本。這表示 StorageGRID 不支援在規則中使用 `Filter` 元素，並遵循 V1 慣例來刪除物件版本。如需詳細資訊，請參閱 "Amazon Simple Storage Service 使用者指南：複寫組態"。 - 可以在版本化儲存桶或非版本化儲存桶上設定儲存桶複寫。 - 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桶。一個來源儲存桶可以複寫到多個目的地儲存桶。 - 目標儲存桶必須指定為租用戶管理器或租用戶管理 API 中指定的 StorageGRID 端點的 URN。請參閱"設定 CloudMirror 複寫"。 要成功進行複寫組態，端點必須存在。如果端點不存在，則請求失敗為 400 Bad Request。錯誤訊息如下：Unable to save the replication policy. The specified endpoint URN does not exist: URN. - 您無需在組態 XML 中指定 Role。StorageGRID 不使用此值，提交後將被忽略。 - 如果從組態 XML 中省略儲存設備類別，StorageGRID 預設會使用 `STANDARD` 儲存設備類別。 - 如果從來源儲存桶中移除物件或移除來源桶本身，則跨區域複寫行為如下： - 如果在物件或儲存桶複寫之前將其刪除，該物件/儲存桶將不會被複寫，您也不會收到通知。 - 如果在複寫完成後刪除物件或儲存桶，StorageGRID 將遵循 Amazon S3 跨區域複寫 V1 的標準刪除行為。
PutBucketTagging	使用 `tagging` 子資源為儲存桶新增或更新一組標籤。在新增儲存桶標籤時，請注意以下限制： - StorageGRID 和 Amazon S3 都支援每個儲存桶最多 50 個標籤。 - 與儲存桶關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多可達 128 個 Unicode 字元。 - 標籤值最多可以包含 256 個 Unicode 字元。 - 鍵和值區分大小寫。 注意：如果為此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤及其賦值。請確保所有 PutBucketTagging 請求中都包含 `NTAP-SG-ILM-BUCKET-TAG` 儲存桶標籤及其賦值。請勿修改或移除此標籤。 注意：此操作將覆寫儲存貯體中已有的所有標籤。如果從清單中省略任何現有標籤，這些標籤將從該儲存貯體中移除。

操作	實作
PutBucketVersioning	使用 `versioning` 子資源設定現有儲存貯體的版本控制狀態。您可以使用下列值之一設定版本控制狀態： - 已啟用：啟用儲存桶中物件的版本控制。新增到儲存桶的所有物件都會獲得一個唯一的版本 ID。 - 已暫停：停用儲存桶中物件的版本控制。新增到儲存桶的所有物件都將獲得版本 ID <code>null</code>。
PutObjectLockConfiguration	設定或移除儲存桶的預設保留模式和預設保留期間。 如果修改預設保留期間，現有物件版本的保留截止日期保持不變，不會使用新的預設保留期間重新計算。 詳情請見 "使用 S3 REST API 設定 S3 物件鎖定"。

對物件進行操作

StorageGRID 如何實作物件的 S3 REST API 作業

本節說明 StorageGRID 系統如何實作物件的 S3 REST API 操作。

以下條件適用於所有物件操作：

- StorageGRID ["一致性值"](#) 支援對物件的所有操作，但下列情況除外：
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- 當用戶端請求發生衝突時，例如兩個用戶端同時寫入同一個金鑰，系統會遵循「最新優先」的原則來解決衝突。這種「最新優先」的判斷依據是 StorageGRID 系統完成請求的時間，而不是 S3 用戶端開始操作的時間。
- StorageGRID 儲存桶中的所有物件均由儲存桶擁有者所有，包括匿名使用者或其他帳戶建立的物件。

下表說明 StorageGRID 如何實作 S3 REST API 物件操作。

操作	實作
DeleteObject	處理 DeleteObject 請求時，StorageGRID 會嘗試立即從所有儲存位置移除物件的所有副本。如果成功，StorageGRID 會立即向用戶端傳回回應。如果無法在 30 秒內移除所有副本（例如，由於某個位置暫時無法使用），StorageGRID 會將副本放入移除佇列，然後向用戶端指示成功。 限制 • 多因素驗證 (MFA) 和回應標頭 `x-amz-mfa` 不受支援。 • The If-None 和 If-None-Match 標頭已被接受，但無法正常工作。 版本控制 要移除特定版本，申請者必須是儲存桶擁有者並使用 <code>versionId</code> 子資源。使用此子資源會永久刪除該版本。如果 <code>versionId</code> 對應於刪除標記，則會傳回回應標頭 <code>x-amz-delete-marker</code>，並設定為 <code>true</code>。 • 如果在已啟用版本控制的儲存桶中刪除物件時未指定 <code>versionId</code> 子資源，則會產生刪除標記。刪除標記的 <code>versionId</code> 會透過 <code>x-amz-version-id</code> 回應標頭傳回，且 <code>x-amz-delete-marker</code> 回應標頭傳回時設定為 <code>true</code>。 • 如果在版本控制已暫停的儲存貯體上刪除物件而未指定 <code>versionId</code> 子資源，則會導致已存在的「null」版本或「null」刪除標記永久刪除，並產生一個新的「null」刪除標記。<code>x-amz-delete-marker</code> 回應標頭將設定為 <code>true</code>。 注意：在某些情況下，一個物件可能存在多個刪除標記。 請參閱 "使用 S3 REST API 設定 S3 物件鎖定" 以了解如何在 GOVERNANCE 模式下刪除物件版本。
DeleteObjects (原名 DELETE Multiple Objects)	多因素驗證 (MFA) 和回應標頭 `x-amz-mfa` 不受支援。 同一請求訊息中可以刪除多個物件。 請參閱 "使用 S3 REST API 設定 S3 物件鎖定" 以了解如何在 GOVERNANCE 模式下刪除物件版本。
DeleteObjectTagging	使用 <code>tagging</code> 子資源從物件中移除所有標籤。 版本控制 如果 <code>versionId</code> 查詢參數未在請求中指定，則此操作會刪除版本化儲存桶中物件最新版本的所有標籤。如果物件的目前版本是刪除標記，則會傳回「MethodNotAllowed」狀態，並將 <code>x-amz-delete-marker</code> 回應標頭設為 <code>true</code>。
GetObject	"GetObject"

操作	實作
GetObjectAcl	如果為帳戶提供了必要的存取憑證，則操作將傳回肯定的回應以及物件擁有者的 ID、DisplayName 和權限，表示擁有者對該物件擁有完全存取權。
GetObjectLegalHold	" 使用 S3 REST API 設定 S3 物件鎖定 "
GetObjectRetention	" 使用 S3 REST API 設定 S3 物件鎖定 "
GetObjectTagging	使用 `tagging` 子資源傳回物件的所有標籤。 版本控制 如果 <code>versionId</code> 查詢參數未在請求中指定，則此操作將傳回版本化儲存桶中物件最新版本的所有標籤。如果物件的目前版本是刪除標記，則會傳回「MethodNotAllowed」狀態，並將 `x-amz-delete-marker` 回應標頭設為 `true`。
HeadObject	" HeadObject "
RestoreObject	" RestoreObject "
PutObject	" PutObject "
CopyObject (之前名為 PUT Object - Copy)	" CopyObject "
PutObjectLegalHold	" 使用 S3 REST API 設定 S3 物件鎖定 "
PutObjectRetention	" 使用 S3 REST API 設定 S3 物件鎖定 "

操作	實作
PutObjectTagging	使用 `tagging` 子資源為現有物件新增一組標籤。 物件標籤限制 您可以在上傳新物件時為其新增標籤，也可以為現有物件新增標籤。StorageGRID 和 Amazon S3 都支援每個物件最多新增 10 個標籤。與物件關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多為 128 個 Unicode 字元，標籤值的長度最多為 256 個 Unicode 字元。鍵和值均區分大小寫。 標籤更新和擷取行為 當您使用 PutObjectTagging 更新物件標籤時，StorageGRID 不會重新擷取該物件。這表示符合的 ILM 規則中所指定的擷取行為選項將不會被使用。由更新所觸發的任何物件放置變更，都會在正常的背景 ILM 程序重新評估 ILM 時生效。 這意味著，如果 ILM 規則使用「嚴格」選項進行擷取行為，則當無法進行所需的物件放置時（例如，因為新要求的放置位置無法使用），不會採取任何行動。更新後的物件將保持其目前位置，直到可以進行所需的放置為止。 解決衝突 當用戶端請求發生衝突時，例如兩個用戶端同時寫入同一個金鑰，系統會遵循「最新優先」的原則來解決衝突。這種「最新優先」的判斷依據是 StorageGRID 系統完成請求的時間，而不是 S3 用戶端開始操作的時間。 版本控制 如果 versionId 查詢參數未在請求中指定，則此操作會將標籤新增至版本化儲存桶中物件的最新版本。如果物件的目前版本是刪除標記，則會傳回「MethodNotAllowed」狀態，並將 `x-amz-delete-marker` 回應標頭設為 `true`。
SelectObjectContent	"SelectObjectContent"

StorageGRID 中支援的 Amazon S3 Select 作業

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



未列出的項目均不受支援。

如需語法，請參閱 ["SelectObjectContent"](#)。如需 S3 Select 的詳細資訊，請參閱 ["AWS S3 Select 文件"](#)。

只有啟用了 S3 Select 的租戶帳戶才能發出 SelectObjectContent 查詢。請參閱 ["使用 S3 Select 的注意事項和要求"](#)。

條款

- 選擇清單
- FROM 子句
- WHERE 子句
- LIMIT 子句

資料類型

- 布林值
- 整數
- 字串
- 浮點數
- 小數，數字
- 時間戳

營運者

邏輯運算符

- 和
- 不是
- 或者

比較運算子

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- 之間
- 在

模式匹配運算符

- LIKE
- _
- %

單位算子

- IS NULL
- 不為空

數學運算子

- +
- -
- *
- /
- %

StorageGRID 遵循 Amazon S3 Select 運算子優先順序。

聚合函數

- AVG()
- COUNT(*)
- MAX()
- MIN()
- SUM()

條件函數

- 案例
- COALESCE
- NULLIF

轉換函數

- CAST（適用於支援的資料類型）

日期函數

- DATE_ADD
- DATE_DIFF
- 擷取
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

字串函數

- CHAR_LENGTH, CHARACTER_LENGTH
- 降低

- 子字串
- TRIM
- 上

StorageGRID 如何使用伺服器端加密

伺服器端加密可以保護您的靜態物件資料。StorageGRID 在寫入物件時會對資料進行加密，並在您存取物件時對資料進行解密。

如果要使用伺服器端加密，可以根據加密金鑰的管理方式，選擇兩種互斥的選項之一：

- **SSE**（使用 **StorageGRID** 管理的金鑰進行伺服器端加密）：當您發出 S3 請求以儲存物件時，StorageGRID 會使用唯一金鑰對該物件進行加密。當您發出 S3 請求以擷取物件時，StorageGRID 會使用儲存的金鑰來解密該物件。
- **SSE-C**（使用客戶提供的金鑰進行伺服器端加密）：當您向 S3 發出儲存物件的請求時，您需要提供自己的加密金鑰。當您擷取物件時，您需要在請求中提供相同的加密金鑰。如果兩個加密金鑰相符，則物件將被解密並傳回您的物件資料。

StorageGRID 管理所有物件加密和解密作業，但您必須管理您提供的加密金鑰。



您提供的加密金鑰永遠不會儲存。如果您遺失了加密金鑰，您也會遺失對應的物件。



如果物件使用 SSE 或 SSE-C 加密，則任何儲存桶層級或網格層級的加密設定都會被忽略。

使用 SSE

若要使用 StorageGRID 管理的唯一金鑰加密物件，請使用下列請求標頭：

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

以下物件操作支援 SSE 請求標頭：

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

使用 SSE-C

若要使用您管理的唯一金鑰加密物件，您需要使用三個請求標頭：

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

要求標頭	說明
x-amz-server-side-encryption-customer-key	指定用於加密或解密物件的加密金鑰。金鑰值必須為 256 位元，並採用 base64 編碼。
x-amz-server-side-encryption-customer-key-MD5	根據 RFC 1321 規範，指定加密金鑰的 MD5 摘要，用於確保加密金鑰傳輸無誤。MD5 摘要的值必須採用 Base64 編碼，長度為 128 位元。

以下物件操作支援 SSE-C 請求標頭：

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

使用客戶提供的金鑰進行伺服器端加密（**SSE-C**）的注意事項

使用 SSE-C 之前，請注意以下事項：

- 您必須使用 https。



StorageGRID 在使用 SSE-C 時會拒絕所有透過 http 傳送的請求。出於安全性考慮，如果您不小心使用 http 傳送了金鑰，則應將其視為已洩露。請丟棄該金鑰，並視情況進行輪換。

- 回應中的 ETag 不是物件資料的 MD5 值。
- 您必須管理加密金鑰到物件的對應。StorageGRID 不儲存加密金鑰。您有責任追蹤您為每個物件提供的加密金鑰。
- 如果您的儲存桶啟用了版本控制，則每個物件版本都應該有自己的加密金鑰。您有責任追蹤每個物件版本所使用的加密金鑰。
- 因為加密金鑰是在用戶端管理的，所以任何其他安全措施（例如金鑰輪換）也必須在用戶端管理。



您提供的加密金鑰永遠不會儲存。如果您遺失了加密金鑰，您也會遺失對應的物件。

- 如果儲存桶已設定跨網格複寫或 CloudMirror 複寫，則無法擷取 SSE-C 物件。擷取作業將會失敗。

相關資訊

["Amazon S3 使用者指南：使用客戶提供的金鑰進行伺服器端加密（SSE-C）"](#)

使用 **S3 CopyObject** 請求在 **StorageGRID** 中建立物件的副本

您可以使用 S3 CopyObject 請求建立已儲存在 S3 中的物件的複本。CopyObject 操作與執

行 `GetObject` 後接 `PutObject` 相同。

解決衝突

當用戶端請求發生衝突時，例如兩個用戶端同時寫入同一個金鑰，系統會遵循「最新優先」的原則來解決衝突。這種「最新優先」的判斷依據是 `StorageGRID` 系統完成請求的時間，而不是 `S3` 用戶端開始操作的時間。

物件大小

單一 `PutObject` 操作的最大_建議_大小為 5 GiB（5,368,709,120 位元組）。如果物件大於 5 GiB，請改用 "[多部分上傳](#)"。

單一 `PutObject` 操作支援的最大大小為 5 TiB（5,497,558,138,880 位元組）。



如果您是從 `StorageGRID` 11.6 或更早版本升級而來，嘗試上傳超過 5 GiB 的物件時，將會觸發「S3 PUT 物件大小過大」警報。如果您全新安裝了 `StorageGRID` 11.7 或 11.8，則不會觸發此警報。但是，為了遵守 AWS S3 標準，`StorageGRID` 的未來版本將不再支援上傳大於 5 GiB 的物件。

使用者中繼資料中的 **UTF-8** 字元

如果請求中包含使用者定義中繼資料的鍵名或值中的（未轉義的）UTF-8 值，則 `StorageGRID` 的行為未定義。

`StorageGRID` 不會解析或解釋使用者自訂中繼資料鍵名或值中包含的轉義 UTF-8 字元。轉義 UTF-8 字元將被視為 ASCII 字元：

- 如果使用者定義的中繼資料包含逸出的 UTF-8 字元，則請求成功。
- `StorageGRID` 不會傳回 ``x-amz-missing-meta`` 標頭（如果鍵名或值的解釋值包含不可列印字符）。

支援的要求標頭

支援以下請求標頭：

- `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-`，後接包含使用者定義中繼資料的名稱值對
- `x-amz-metadata-directive`：預設值為 `COPY`，可讓您複製物件及其關聯的中繼資料。

您可以指定 ``REPLACE`` 在複製物件時覆寫現有中繼資料，或更新物件中繼資料。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：預設值為 `COPY`，可讓您複製物件及其所有標籤。

您可以指定 `REPLACE` 在複製物件時覆寫現有標籤，或更新標籤。

- S3 物件鎖定請求標頭：

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

如果請求中未包含這些標頭，則使用儲存桶的預設保留設定來計算物件版本模式和保留至日期。請參閱"[使用 S3 REST API 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 [\[伺服器端加密的要求標頭\]](#)

不支援的要求標頭

不支援以下請求標頭：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

`If-Match` header 已被接受，但無法正常使用。

- If-None-Match

`If-None-Match` header 已被接受，但無法正常使用。

- x-amz-checksum-algorithm

複製物件時，如果來源物件包含 Checksum，StorageGRID 不會將該 Checksum 值複製到新物件。無論您是否嘗試在物件請求中使用 `x-amz-checksum-algorithm`，此行為均適用。

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

儲存類別選項

支援 `x-amz-storage-class` 請求標頭，如果符合的 ILM 規則使用雙重提交或平衡 "擷取選項"，則會影響 StorageGRID 建立的物件複本數量。

- STANDARD

(預設) 指定當 ILM 規則使用 Dual commit 選項，或當 Balanced 選項回退到建立臨時複本時執行雙重提交擷取操作。

- REDUCED_REDUNDANCY

指定當 ILM 規則使用雙重提交選項，或當平衡選項回退到建立臨時複本時，執行單次提交擷取操作。



如果將物件擷取至已啟用 S3 物件鎖定的儲存桶，則 `REDUCED_REDUNDANCY` 選項將被忽略。如果將物件擷取至舊版法規遵循儲存桶，則 `REDUCED_REDUNDANCY` 選項會傳回錯誤。StorageGRID 一律會執行雙重提交擷取，以確保符合法規遵循要求。

使用 `x-amz-copy-source` 於 CopyObject

如果標頭中指定的來源儲存桶和金鑰 `x-amz-copy-source` 與目的地儲存桶和金鑰不同，則來源物件資料的複本將寫入目的地。

如果來源和目的地相符，且 `x-amz-metadata-directive` 標頭指定為 `REPLACE`，則物件的中繼資料將使用請求中提供的中繼資料值進行更新。在這種情況下，StorageGRID 不會重新擷取物件。這會產生兩個重要後果：

- 您無法使用 CopyObject 對現有物件進行原地加密，也無法變更現有物件的原地加密。如果您提供 `x-amz-server-side-encryption` 標頭或 `x-amz-server-side-encryption-customer-algorithm` 標頭，StorageGRID 將拒絕請求並傳回 `XNotImplemented`。
- 符合的 ILM 規則中指定的「擷取行為」選項不會被使用。由更新觸發的任何物件放置變更，都會在正常的背景 ILM 程序重新評估 ILM 時生效。

這意味著，如果 ILM 規則使用「嚴格」選項進行擷取行為，則當無法進行所需的物件放置時（例如，因為新要求的放置位置無法使用），不會採取任何行動。更新後的物件將保持其目前位置，直到可以進行所需的放置為止。

伺服器端加密的要求標頭

如果您"使用伺服器端加密"，您提供的請求標頭取決於來源物件是否已加密，以及您是否計劃對目標物件進行加密。

- 如果來源物件使用客戶提供的金鑰 (SSE-C) 加密，則必須在 CopyObject 請求中包含以下三個標頭，以便解密並複製該物件：
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 AES256。

- `x-amz-copy-source-server-side-encryption-customer-key`：指定您在建立來源物件時提供的加密金鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定您在建立來源物件時提供的 MD5 摘要。

• 如果要使用您提供和管理的唯一加密金鑰對目標物件（複本）加密，請包含以下三個標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：為目標物件指定新的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定新加密金鑰的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請審查 ["使用伺服器端加密"](#) 的相關注意事項。

• 如果要使用由 StorageGRID（SSE）管理的唯一加密金鑰來加密目標物件（複本），請在 CopyObject 請求中包含下列標頭：

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



無法更新物件的 `server-side-encryption` 值。請改用 `x-amz-metadata-directive: REPLACE` 建立具有新 `server-side-encryption` 值的複本。

版本控制

如果來源儲存桶已啟用版本控制，您可以使用 ``x-amz-copy-source`` 標頭來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 ``versionId`` 子資源明確指定要複製的版本。如果目的地儲存桶已啟用版本控制，則產生的版本會在 ``x-amz-version-id`` 回應標頭中傳回。如果目標儲存桶的版本控制已暫停，則 ``x-amz-version-id`` 會傳回「null」值。

使用 **GetObject** 請求從 **StorageGRID** 中的儲存桶檢索物件

您可以使用 S3 GetObject 請求從 S3 儲存桶中擷取物件。

GetObject 和多部分物件

您可以使用 ``partNumber`` 請求參數來擷取多部分物件或分段物件中的特定部分。``x-amz-mp-parts-count`` 回應元素指示物件包含多少個部分。

您可以將 ``partNumber`` 設為 1，適用於分段/多部分物件和非分段/非多部分物件；但是，``x-amz-mp-parts-count`` 回應元素僅針對分段或多部分物件傳回。

使用者中繼資料中的 UTF-8 字元

StorageGRID 不會解析或解釋使用者自訂中繼資料中的轉義 UTF-8 字元。如果索引鍵名稱或值包含不可列印字元，則針對使用者自訂中繼資料中含有轉義 UTF-8 字元之物件的 GET 請求不會傳回 ``x-amz-missing-meta`` 標頭。

支援的請求標頭

支援下列要求標頭：

- `x-amz-checksum-mode`：指定 `ENABLED`

針對 `GetObject`，不支援將 `Range` 標頭與 `x-amz-checksum-mode` 搭配使用。當您在啟用 `x-amz-checksum-mode` 的情況下，於要求中包含 `Range` 時，`StorageGRID` 不會在回應中傳回 `Checksum` 值。

不支援的要求標頭

以下請求標頭不受支援，並傳回 `XNotImplemented`：

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

版本控制

如果 `versionId` 未指定子資源，則操作會從版本化儲存桶中擷取物件的最新版本。如果物件的目前版本是刪除標記，則會傳回「找不到」狀態，並將 `x-amz-delete-marker` 回應標頭設為 `true`。

使用客戶提供的加密金鑰進行伺服器端加密的請求標頭 (SSE-C)

如果物件使用您提供的唯一加密金鑰進行加密，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`：指定物件加密金鑰的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請審查 ["使用伺服器端加密"](#) 中的注意事項。

Cloud Storage Pool 物件的 `GetObject` 行為

如果物件已儲存在 ["雲端儲存資源池"](#) 中，`GetObject` 請求的行為取決於該物件的狀態。如需詳細資訊，請參閱 ["HeadObject"](#)。



如果物件儲存在雲端儲存資源池中，且該物件的一個或多個複本也存在於網格中，`GetObject` 請求將嘗試先從網格擷取資料，再從雲端儲存資源池擷取資料。

物件狀態	<code>GetObject</code> 的行為
已擷取至 <code>StorageGRID</code> 但尚未由 ILM 評估的物件，或儲存於傳統儲存資源池或使用銷毀編碼的物件。	200 OK 已擷取物件的複本。
物件位於雲端儲存資源池中，但尚未轉換為不可擷取狀態	200 OK 已擷取物件的複本。
物件已轉換為不可擷取狀態	403 Forbidden, InvalidObjectState 使用 "RestoreObject" 請求將物件還原至可擷取狀態。

物件狀態	GetObject 的行為
正在從不可擷取狀態還原的物件	403 Forbidden, InvalidObjectState 等待 RestoreObject 請求完成。
物件已完全還原至雲端儲存資源池	200 OK 已擷取物件的複本。

雲端儲存資源池中的多部分或分段物件

如果您上傳的是多部分物件，或者 StorageGRID 將大型物件分割為多個區段，StorageGRID 會透過對物件的部分或區段進行抽樣，來確定該物件是否在雲端儲存資源池中可用。在某些情況下，GetObject 請求可能會在物件的某些部分已轉換為不可擷取狀態，或物件的某些部分尚未還原時，錯誤地傳回 200 OK。

在這些情況下：

- GetObject 請求可能會傳回一些資料，但傳輸過程中會中途停止。
- 後續 GetObject 請求可能會傳回 403 Forbidden。

GetObject 以及跨網格複寫

如果您正在使用 "\${post_edited_translations.segment}" 且已為儲存桶啟用 "\${post_edited_translations.segment}"，則 S3 用戶端可以透過發出 GetObject 請求來驗證物件的複寫狀態。回應包含 StorageGRID 特有的 x-ntap-sg-cgr-replication-status 回應標頭，該標頭將具有下列其中一個值：

\${post_edited_translations.segment}	\${post_edited_translations.segment}
來源	• COMPLETED: 複寫成功。 • PENDING: 該物件尚未複寫。 • 失敗: 複寫發生永久性故障。使用者必須解決此錯誤。
目的地	\${post_edited_translations.segment}



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

使用 S3 HeadObject 請求從 StorageGRID 中的物件擷取中繼資料

您可以使用 S3 HeadObject 請求從物件中擷取中繼資料，而無需傳回物件本身。如果物件儲存在雲端儲存資源池中，您可以使用 HeadObject 來確定物件的轉換狀態。

HeadObject 和多部分物件

您可以使用 `partNumber` 請求參數來擷取多部分物件或分段物件中特定部分的中繼資料。`x-amz-mp-parts-

count` 回應元素指示物件包含多少個部分。

您可以將 `partNumber` 設為 1，適用於分段/多部分物件和非分段/非多部分物件；但是，`x-amz-mp-parts-count` 回應元素僅針對分段或多部分物件傳回。

使用者中繼資料中的 **UTF-8** 字元

StorageGRID 不會解析或解釋使用者自訂中繼資料中的轉義 UTF-8 字元。如果鍵名或值包含不可列印字元，則針對使用者自訂中繼資料中含有轉義 UTF-8 字元之物件的 HEAD 請求不會傳回 `x-amz-missing-meta` 標頭。

支援的請求標頭

支援下列要求標頭：

- x-amz-checksum-mode

The `partNumber` 參數和 `Range` 標頭不支援 `x-amz-checksum-mode` 用於 `HeadObject`。當您在啟用 `x-amz-checksum-mode` 的情況下將它們包含在請求中時，StorageGRID 不會在回應中傳回 Checksum 值。

不支援的要求標頭

以下請求標頭不受支援，並傳回 `XNotImplemented`：

- x-amz-website-redirect-location

版本控制

如果 `versionId` 未指定子資源，則操作會從版本化儲存桶中擷取物件的最新版本。如果物件的目前版本是刪除標記，則會傳回「找不到」狀態，並將 `x-amz-delete-marker` 回應標頭設為 `true`。

使用客戶提供的加密金鑰進行伺服器端加密的請求標頭 (SSE-C)

如果物件使用您提供的唯一加密金鑰進行加密，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：指定物件加密金鑰的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請審查 ["使用伺服器端加密"](#) 中的注意事項。

HeadObject 雲端儲存資源池物件的回應

如果物件儲存在 ["雲端儲存資源池"](#) 中，則會傳回下列回應標頭：

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

回應標頭提供物件移至 Cloud Storage Pool、選擇性轉換為無法擷取狀態及還原時的狀態相關資訊。

物件狀態	回應 HeadObject
已擷取至 StorageGRID 但尚未由 ILM 評估的物件，或儲存於傳統儲存資源池或使用銷毀編碼的物件。	200 OK（不回傳特殊回應標頭。）
物件位於雲端儲存資源池中，但尚未轉換為不可擷取狀態	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" 在物件轉換為不可擷取狀態之前，expiry-date 的值會設定為未來的某個遙遠時間點。轉換的確切時間並非由 StorageGRID 系統控制。
物件已轉換為不可擷取狀態，但網格上至少還存在一個複本。	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" <code>`expiry-date`</code> 的值設定為遙遠未來的某個時間點。 注意：如果網格上的複本不可用（例如，儲存節點當機），則必須先發出 "RestoreObject" 請求，從 Cloud Storage Pool 還原複本，才能成功擷取物件。
物件已轉換為不可擷取狀態，且網格上不存在複本。	200 OK x-amz-storage-class: GLACIER
正在從不可擷取狀態還原的物件	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"

物件狀態	回應 HeadObject
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: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" 此 `expiry-date` 參數指示雲端儲存資源池中的物件何時 將恢復至不可擷取狀態。

雲端儲存資源池中的多部分或分段物件

如果您上傳了多部分物件，或 StorageGRID 將大型物件分割為多個區段，StorageGRID 會透過對物件的部分或區段進行抽樣，來判斷該物件是否可在雲端儲存資源池中使用。在某些情況下，當物件的某些部分已轉換為不可擷取狀態，或物件的某些部分尚未還原時，HeadObject 請求可能會錯誤地傳回 `x-amz-restore: ongoing-request="false"`。

HeadObject 以及跨網格複寫

如果您正在使用 `"${post_edited_translations.segment}"` 且已為儲存桶啟用 `"${post_edited_translations.segment}"`，則 S3 用戶端可以透過發出 HeadObject 請求來驗證物件的複寫狀態。回應包含 StorageGRID 特有的 `x-ntap-sg-cgr-replication-status` 回應標頭，該標頭將具有下列其中一個值：

<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
來源	• COMPLETED: 複寫成功。 • PENDING: 該物件尚未複寫。 • 失敗: 複寫發生永久性故障。使用者必須解決此錯誤。
目的地	<code>\${post_edited_translations.segment}</code>



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

使用 **S3 PutObject** 請求將物件新增至 **StorageGRID** 中的儲存區

您可以使用 S3 PutObject 請求將物件新增至儲存桶。

解決衝突

當用戶端請求發生衝突時，例如兩個用戶端同時寫入同一個金鑰，系統會遵循「最新優先」的原則來解決衝突。這種「最新優先」的判斷依據是 StorageGRID 系統完成請求的時間，而不是 S3 用戶端開始操作的時間。

物件大小

單一 PutObject 操作的最大_建議_大小為 5 GiB (5,368,709,120 位元組)。如果物件大於 5 GiB，請改用 ["多部分上傳"](#)。

單一 PutObject 操作支援的最大大小為 5 TiB (5,497,558,138,880 位元組)。



如果您是從 StorageGRID 11.6 或更早版本升級而來，嘗試上傳超過 5 GiB 的物件時，將會觸發「S3 PUT 物件大小過大」警報。如果您全新增裝了 StorageGRID 11.7 或 11.8，則不會觸發此警報。但是，為了遵守 AWS S3 標準，StorageGRID 的未來版本將不再支援上傳大於 5 GiB 的物件。

使用者中繼資料大小

Amazon S3 將每個 PUT 請求標頭中使用者自訂中繼資料的大小限制為 2 KB。StorageGRID 將使用者中繼資料限制為 24 KiB。使用者自訂中繼資料的大小是透過計算每個索引鍵和值在 UTF-8 編碼下的位元組數總和來衡量的。

使用者中繼資料中的 UTF-8 字元

如果請求中包含使用者定義中繼資料的鍵名或值中的（未轉義的）UTF-8 值，則 StorageGRID 的行為未定義。

StorageGRID 不會解析或解釋使用者自訂中繼資料鍵名或值中包含的轉義 UTF-8 字元。轉義 UTF-8 字元將被視為 ASCII 字元：

- PutObject、CopyObject、GetObject 和 HeadObject 請求在使用者定義的中繼資料包含轉義的 UTF-8 字元時將成功。
- StorageGRID 不會傳回 `x-amz-missing-meta` 標頭（如果鍵名或值的解釋值包含不可列印字符）。

物件標籤限制

您可以在上傳新物件時為其新增標籤，也可以為現有物件新增標籤。StorageGRID 和 Amazon S3 都支援每個物件最多新增 10 個標籤。與物件關聯的標籤必須具有唯一的標籤鍵。標籤鍵的長度最多為 128 個 Unicode 字元，標籤值的長度最多為 256 個 Unicode 字元。鍵和值均區分大小寫。

物件所有權

在 StorageGRID 中，所有物件都歸儲存桶擁有者帳戶所有，包括由非擁有者帳戶或匿名使用者建立的物件。

支援的要求標頭

支援以下請求標頭：

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

當您為 Content-Encoding 指定 aws-chunked 時，StorageGRID 不會驗證以下項目：

- StorageGRID 不會針對資料區塊驗證 chunk-signature。

- StorageGRID 不會驗證您提供的值 `x-amz-decoded-content-length` 是否與物件相符。

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

如果 `aws-chunked` 同時使用有效負載簽名，則支援分塊傳輸編碼。

- x-amz-checksum-sha256
- x-amz-meta-，後面接著包含使用者定義中繼資料的名稱值對。

指定使用者自訂中繼資料的名稱-值對時，請使用以下通用格式：

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

如果要將「使用者定義的建立時間」選項用作 ILM 規則的參考時間，則必須使用 `creation-time` 作為記錄物件建立時間的中繼資料名稱。例如：

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

的值 `creation-time` 以自 1970 年 1 月 1 日以後的秒數來評估。



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，以及「平衡」或「嚴格」擷取選項。建立 ILM 規則時會傳回錯誤。

- x-amz-tagging
- S3 物件鎖定請求標頭
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

如果請求中未包含這些標頭，則使用儲存桶的預設保留設定來計算物件版本模式和保留至日期。請參閱[使用 S3 REST API 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 [\[伺服器端加密的要求標頭\]](#)

不支援的要求標頭

不支援以下請求標頭：

- If-Match

⋮If-Match header⋮已被接受，但無法正常使用。

- If-None-Match

⋮If-None-Match header⋮已被接受，但無法正常使用。

- x-amz-acl
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

The x-amz-website-redirect-location⋮標頭返回 ⋮XNotImplemented。

儲存類別選項

The ⋮x-amz-storage-class⋮請求標頭受支援。提交的 ⋮x-amz-storage-class⋮值會影響 StorageGRID 在擷取期間如何保護物件資料，而不會影響 StorageGRID 系統中儲存的物件持久複本數量（該數量由 ILM 決定）。

如果與已擷取物件相符的 ILM 規則使用嚴格擷取選項，則 x-amz-storage-class 標頭無效。

以下數值可用於 x-amz-storage-class：

- STANDARD（預設）
 - 雙重提交：如果 ILM 規則為擷取行為指定了雙重提交選項，則物件擷取後會立即建立該物件的第二個複本，並將其分發到不同的儲存節點（雙重提交）。在評估 ILM 時，StorageGRID 會決定這些初始臨時複本是否符合規則中的放置指令。如果不符合，則可能需要在不同的位置建立新的物件複本，並且可能需要刪除初始臨時複本。
 - 平衡：如果 ILM 規則指定了平衡選項，且 StorageGRID 無法立即建立規則中指定的所有複本，StorageGRID 會在不同的 Storage Nodes 上建立兩個暫存複本。

如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件複本（同步放置），則 x-amz-storage-class 標頭無效。

- REDUCED_REDUNDANCY

- 雙重提交：如果 ILM 規則為擷取行為指定了雙重提交選項，StorageGRID 會在擷取物件時建立單一臨時複本（單一提交）。
- 平衡：如果 ILM 規則指定了「平衡」選項，則僅當系統無法立即建立規則中指定的所有複本時，StorageGRID 才會建立單一臨時複本。如果 StorageGRID 可以執行同步放置，則此標頭無效。REDUCED_REDUNDANCY 選項最適合在與物件相符的 ILM 規則建立單一複寫複本時使用。在這種情況下，使用 REDUCED_REDUNDANCY 可避免每次擷取作業都不必要地建立和刪除額外的物件複本。

不建議在其他情況下使用 REDUCED_REDUNDANCY 選項。REDUCED_REDUNDANCY 會增加擷取期間物件資料遺失的風險。例如，如果單一複本最初儲存在儲存節點上，而該儲存節點在 ILM 評估完成之前發生故障，則可能會遺失資料。



在任何時間段內，僅保留一份複寫複本都會使資料面臨永久遺失的風險。如果某個物件僅存在一份複寫複本，則一旦 Storage Node 發生故障或發生重大錯誤，該物件就會遺失。此外，在升級等維護程序期間，您也會暫時失去對該物件的存取。

指定 `REDUCED\_REDUNDANCY` 僅影響物件首次擷取時所建立的複本數量。它不會影響作用中 ILM 原則評估物件時所建立的物件複本數量，也不會導致 StorageGRID 系統中的資料以較低的備援等級儲存。



如果將物件擷取至已啟用 S3 物件鎖定的儲存桶，則 `REDUCED\_REDUNDANCY` 選項將被忽略。如果將物件擷取至舊版法規遵循儲存桶，則 `REDUCED\_REDUNDANCY` 選項會傳回錯誤。StorageGRID 一律會執行雙重提交擷取，以確保符合法規遵循要求。

伺服器端加密的要求標頭

您可以使用下列請求標頭，透過伺服器端加密對物件進行加密。SSE 和 SSE-C 選項互斥。

- **SSE**：如果要使用 StorageGRID 管理的唯一金鑰加密物件，請使用下列標頭。

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

當 `x-amz-server-side-encryption` 標頭未包含在 PutObject 請求中時，網格範圍的["儲存物件加密設定"](#)將從 PutObject 回應中省略。

- **SSE-C**：如果您想使用您提供和管理的唯一金鑰對物件進行加密，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`：指定新物件的加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定新物件加密金鑰的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請審查["使用伺服器端加密"](#)的相關注意事項。



如果物件使用 SSE 或 SSE-C 加密，則任何儲存桶層級或網格層級的加密設定都會被忽略。

版本控制

如果儲存桶啟用了版本控制，則會自動為儲存物件的版本產生一個唯一 `versionId` 識別碼。此 `versionId` 識別碼也會透過 `x-amz-version-id` 回應標頭在回應中傳回。

如果版本控制暫停，物件版本將以 null versionId 值儲存；如果已存在 null 版本，則會被覆寫。

在使用 `Authorization` 標頭進行請求驗證時，StorageGRID 與 AWS 有以下不同：

- StorageGRID 不需要將 `host` 標頭包含在 `CanonicalHeaders` 中。
- StorageGRID 不需要 `Content-Type` 包含在 `CanonicalHeaders` 中。
- StorageGRID 不需要將 `x-amz-*` 標頭包含在 `CanonicalHeaders` 內。



一般而言，最佳實務做法是始終在 `CanonicalHeaders` 中包含這些標頭，以確保它們得到驗證；但是，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 ["授權標頭的簽章計算：以單一資料區塊傳輸有效負載 \(AWS 簽章版本 4\)"](#)。

相關資訊

- ["使用 ILM 管理物件"](#)
- ["Amazon Simple Storage Service API 參考：PutObject"](#)

使用 **S3 RestoreObject** 請求在 **StorageGRID** 中還原物件

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

支援的請求類型

StorageGRID 僅支援 RestoreObject 要求來還原物件。不支援 `SELECT` 還原類型。`Select` 要求會傳回 `NotImplemented`。

版本控制

(可選) 指定 `versionId` 以還原版本化儲存貯體中物件的特定版本。如果未指定 `versionId`，則會還原物件的最新版本。

雲端儲存池物件上 RestoreObject 的行為

如果物件已儲存在 ["雲端儲存資源池"](#) 中，RestoreObject 請求將根據該物件的狀態呈現以下行為。如需更多詳細資訊，請參閱 ["HeadObject"](#)。



如果物件儲存在 Cloud Storage Pool 中，且該物件的一個或多個複本也存在於網格中，則無需發出 RestoreObject 請求來還原物件。相反，可以直接使用 GetObject 請求來擷取本機複本。

物件狀態	RestoreObject 的行為
物件已匯入 StorageGRID 但尚未由 ILM 進行評估，或物件不在雲端儲存池中。	403 Forbidden, InvalidObjectState
物件位於雲端儲存資源池中，但尚未轉換為不可擷取狀態	<code>200 OK</code> 不做任何變更。 注意：在物件轉換為不可檢索狀態之前，您無法變更其 <code>expiry-date</code> 。

物件狀態	RestoreObject 的行為
物件已轉換為不可擷取狀態	`202 Accepted`將物件的可擷取複本還原至 Cloud Storage Pool，保留天數由要求本文指定。此期限結束後，物件將恢復為不可擷取狀態。 （可選）使用 Tier 請求元素來確定還原作業完成所需的時間（`Expedited`、`Standard` 或 `Bulk`）。如果未指定 Tier，則使用 `Standard` 分層。 重要提示：如果物件已移轉到 S3 Glacier Deep Archive 或雲端儲存池使用 Azure Blob 儲存設備，則無法使用 Expedited 分層還原物件。系統將傳回下列錯誤 `403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class`。
正在從不可擷取狀態還原的物件	409 Conflict, RestoreAlreadyInProgress
物件已完全還原至雲端儲存資源池	200 OK 附註：如果物件已還原至可檢索狀態，您可以變更其 expiry-date，方法是重新發出 RestoreObject 要求，並使用 Days 的新值。還原日期會相對於要求的時間進行更新。

使用 **S3 SelectObjectContent** 請求在 **StorageGRID** 中篩選物件資料

您可以使用 S3 SelectObjectContent 請求根據簡單的 SQL 聲明來篩選 S3 物件的內容。

更多資訊請參閱 ["Amazon Simple Storage Service API 參考：SelectObjectContent"](#)。

開始之前

- 租戶帳戶擁有 S3 Select 權限。
- 您擁有 `s3:GetObject` 查詢物件的權限。
- `${post_edited_translations.segment}`
 - **CSV**。可直接使用，也可壓縮成 GZIP 或 BZIP2 壓縮包。
 - **Parquet**。Parquet 物件的其他需求：
 - S3 Select 僅支援使用 GZIP 或 Snappy 的欄式壓縮。S3 Select 不支援 Parquet 物件的整個物件壓縮。
 - S3 Select 不支援 Parquet 輸出。您必須將輸出格式指定為 CSV 或 JSON。
 - 未壓縮資料列群組的最大大小為 512 MB。
 - 必須使用物件架構中指定的資料類型。
 - 您不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 邏輯類型。
- 您的 SQL 表示式長度上限為 256 KB。
- 輸入或結果中的任何記錄最大長度為 1 MiB。

CSV 請求語法範例

```
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>
```

Parquet 請求語法範例

```

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

此查詢取得州名、2010 年人口資料、2015 年人口估計資料以及與美國人口普查資料相比的變化百分比。檔案中非州名的記錄將被忽略。

```

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

```

待查詢檔案的前幾行 `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 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 changes.csv 的前幾行如下：

```
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
```

多部分上傳作業

StorageGRID 中支援的多部分上傳作業

本節說明 StorageGRID 如何支援多部分上傳作業。

以下條件和注意事項適用於所有分段上傳作業：

- 不應向單一儲存桶同時進行超過 1,000 次的多部分上傳，因為該儲存桶的 ListMultipartUploads 查詢結果可能不完整。
- StorageGRID 強制執行 AWS 多部分的大小限制。S3 用戶端必須遵循以下準則：
 - 多部分上傳的每個部分必須介於 5 MiB (5,242,880 位元組) 和 5 GiB (5,368,709,120 位元組) 之間。
 - 最後一部分可以小於 5 MiB (5,242,880 位元組)。
 - 一般來說，分割區大小應盡可能大。例如，對於 100 GiB 的物件，可以使用 5 GiB 的分割區大小。由於每個分割區都被視為一個獨立的物件，因此使用較大的分割區大小可以減少 StorageGRID 中繼資料例行成本。
 - 對於小於 5 GiB 的物件，請考慮改用非分段上傳。
- 如果 ILM 規則使用「平衡」或「嚴格」[擷取選項](#)，則在擷取多部分物件的每個部分時，ILM 會對其進行評估；在多部分上傳完成後，ILM 也會針對整個物件進行評估。您應該瞭解這會對物件和部分的放置產生哪些影響：
 - 如果在 S3 多部分上傳過程中 ILM 發生變化，則物件中的某些部分在多部分上傳完成後可能無法滿足目前的 ILM 要求。任何放置不正確的部分都會排入佇列，等待 ILM 重新評估，並在稍後移至正確的位置。
 - 在評估某部分的 ILM 時，StorageGRID 會根據部分的大小進行篩選，而不是根據物件的大小。這表示物

件的某些部分可能儲存在不符合物件整體 ILM 要求的位置。例如，如果一條規則規定所有 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，那麼一個包含 10 個部分的多部分上傳檔案在擷取時，每個 1 GB 的部分都會儲存在 DC2。但是，當評估物件整體的 ILM 時，物件的所有部分都會移至 DC1。

- 所有多部分上傳作業均支援 StorageGRID "一致性值"。
- 當使用分段上傳方式擷取物件時，此規則 "物件分割臨界值 (1 GiB)" 不適用。
- 如有需要，您可以使用 "伺服器端加密" 進行分段上傳。若要使用 SSE（使用 StorageGRID 管理的金鑰進行伺服器端加密），只需在 CreateMultipartUpload 請求中包含 `x-amz-server-side-encryption` 請求標頭即可。若要使用 SSE-C（使用客戶提供的金鑰進行伺服器端加密），需要在 CreateMultipartUpload 請求及其後的每個 UploadPart 請求中指定相同的三個加密金鑰請求標頭。
- 如果在基本儲存桶的 Before 時間戳記之前啟動擷取，則多部分上傳物件會包含在 "分支桶" 中，無論上傳何時完成。

操作	實作
AbortMultipartUpload	已實作所有 Amazon S3 REST API 行為。如有更改，恕不另行通知。
CompleteMultipartUpload	請參閱 "CompleteMultipartUpload"
CreateMultipartUpload (之前名為「啟動多部分上傳」)	請參閱 "CreateMultipartUpload"
ListMultipartUploads	請參閱 "ListMultipartUploads"
ListParts	已實作所有 Amazon S3 REST API 行為。如有更改，恕不另行通知。
UploadPart	請參閱 "UploadPart"
UploadPartCopy	請參閱 "UploadPartCopy"

StorageGRID S3 REST API 如何完成多部分上傳

CompleteMultipartUpload 操作透過組裝先前上傳的各個部分，完成物件的多部分上傳。



StorageGRID 支援 CompleteMultipartUpload 的 `partNumber` 請求參數使用非連續值，並依升序排列。此參數可以從任何值開始。

解決衝突

當用戶端請求發生衝突時，例如兩個用戶端同時寫入同一個金鑰，系統會遵循「最新優先」的原則來解決衝突。這種「最新優先」的判斷依據是 StorageGRID 系統完成請求的時間，而不是 S3 用戶端開始操作的時間。

支援的要求標頭

支援以下請求標頭：

- x-amz-checksum-sha256
- x-amz-storage-class

The x-amz-storage-class 標頭會影響 StorageGRID 建立的物件複本數量（如果符合的 ILM 規則指定了["雙重提交或平衡擷取選項"](#)）。

- STANDARD

（預設）指定當 ILM 規則使用 Dual commit 選項，或當 Balanced 選項回退到建立臨時複本時執行雙重提交擷取操作。

- REDUCED_REDUNDANCY

指定當 ILM 規則使用雙重提交選項，或當平衡選項回退到建立臨時複本時，執行單次提交擷取操作。



如果將物件擷取至已啟用 S3 物件鎖定的儲存桶，則 `REDUCED\_REDUNDANCY` 選項將被忽略。如果將物件擷取至舊版法規遵循儲存桶，則 `REDUCED\_REDUNDANCY` 選項會傳回錯誤。StorageGRID 一律會執行雙重提交擷取，以確保符合法規遵循要求。



如果多部分上傳在 15 天內未完成，該作業將標記為非作用中狀態，且所有相關資料將從系統中刪除。



傳回的值 `ETag` 不是資料的 MD5 總和，而是遵循 Amazon S3 API 對多部分物件的 `ETag` 值實作。

不支援的要求標頭

不支援以下請求標頭：

- If-Match

`If-Match header` 已被接受，但無法正常使用。

- If-None-Match

`If-None-Match header` 已被接受，但無法正常使用。

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

此操作完成分段上傳。如果儲存桶啟用了版本控制，則會在分段上傳完成後建立物件版本。

如果儲存桶啟用了版本控制，則會自動為儲存物件的版本產生一個唯一 `versionId` 識別碼。此 `versionId` 識別碼也會透過 `x-amz-version-id` 回應標頭在回應中傳回。

如果版本控制暫停，物件版本將以 `null versionId` 值儲存；如果已存在 `null` 版本，則會被覆寫。



如果儲存桶啟用了版本控制，即使在同一物件金鑰上同時存在多個已完成的多部分上傳，完成一次多部分上傳也總是會建立一個新版本。如果儲存桶未啟用版本控制，則可能出現以下情況：啟動一次多部分上傳後，同一物件金鑰上的另一個多部分上傳會先啟動並完成。對於未啟用版本控制的儲存桶，最後完成的多部分上傳將優先。

複寫失敗、通知失敗或中繼資料通知失敗

如果進行分段上傳的儲存桶已設定為平台服務，即使相關的複寫或通知行動失敗，分段上傳也會成功。

租戶可以透過更新物件的中繼資料或標籤來觸發失敗的複寫或通知。租戶可以重新提交現有值，以避免進行不必要的變更。

請參閱 ["平台服務疑難排解"](#)。

StorageGRID 中的 S3 CreateMultipartUpload 請求標頭和選項

CreateMultipartUpload（以前稱為 Initiate Multipart Upload）操作會為物件啟動多部分上傳，並傳回上傳 ID。

The `x-amz-storage-class` 請求標頭受支援。提交的 `x-amz-storage-class` 值會影響 StorageGRID 在擷取期間如何保護物件資料，而不會影響 StorageGRID 系統中儲存的物件持久複本數量（該數量由 ILM 決定）。

如果與已擷取物件相符的 ILM 規則使用 Strict ["擷取選項"](#)，則 `x-amz-storage-class` 標頭無效。

以下數值可用於 `x-amz-storage-class`：

- STANDARD（預設）
 - 雙重提交：如果 ILM 規則指定了雙重提交擷取選項，則物件擷取後會立即建立該物件的第二個複本，並將其分發到不同的儲存節點（雙重提交）。在評估 ILM 時，StorageGRID 會決定這些初始臨時複本是否符合規則中的放置指令。如果不符合，則可能需要在不同的位置建立新的物件複本，並且可能需要刪除初始臨時複本。
 - 平衡：如果 ILM 規則指定了平衡選項，且 StorageGRID 無法立即建立規則中指定的所有複本，StorageGRID 會在不同的 Storage Nodes 上建立兩個暫存複本。

如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件複本（同步放置），則 `x-amz-storage-class` 標頭無效。

- REDUCED_REDUNDANCY
 - 雙重提交：如果 ILM 規則指定了雙重提交選項，StorageGRID 會在物件被擷取時建立單一臨時複本（單一提交）。

- 平衡：如果 ILM 規則指定了「平衡」選項，則僅當系統無法立即建立規則中指定的所有複本時，StorageGRID 才會建立單一臨時複本。如果 StorageGRID 可以執行同步放置，則此標頭無效。REDUCED_REDUNDANCY 選項最適合在與物件相符的 ILM 規則建立單一複寫複本時使用。在這種情況下，使用 REDUCED_REDUNDANCY 可避免每次擷取作業都不必要地建立和刪除額外的物件複本。

不建議在其他情況下使用 REDUCED_REDUNDANCY 選項。REDUCED_REDUNDANCY 會增加擷取期間物件資料遺失的風險。例如，如果單一複本最初儲存在儲存節點上，而該儲存節點在 ILM 評估完成之前發生故障，則可能會遺失資料。



在任何時間段內，僅保留一份複寫複本都會使資料面臨永久遺失的風險。如果某個物件僅存在一份複寫複本，則一旦 Storage Node 發生故障或發生重大錯誤，該物件就會遺失。此外，在升級等維護程序期間，您也會暫時失去對該物件的存取。

指定 `REDUCED\_REDUNDANCY` 僅影響物件首次擷取時所建立的複本數量。它不會影響作用中 ILM 原則評估物件時所建立的物件複本數量，也不會導致 StorageGRID 系統中的資料以較低的備援等級儲存。



如果將物件擷取至已啟用 S3 物件鎖定的儲存桶，則 `REDUCED\_REDUNDANCY` 選項將被忽略。如果將物件擷取至舊版法規遵循儲存桶，則 `REDUCED\_REDUNDANCY` 選項會傳回錯誤。StorageGRID 一律會執行雙重提交擷取，以確保符合法規遵循要求。

支援的要求標頭

支援以下請求標頭：

- Content-Type
- x-amz-checksum-algorithm

目前僅支援 x-amz-checksum-algorithm 的 SHA256 值。

- x-amz-meta-，後接包含使用者定義中繼資料的名稱值對

指定使用者自訂中繼資料的名稱-值對時，請使用以下通用格式：

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

如果要將「使用者定義的建立時間」選項用作 ILM 規則的參考時間，則必須使用 `creation-time` 作為記錄物件建立時間的中繼資料名稱。例如：

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

的值 `creation-time` 以自 1970 年 1 月 1 日以後的秒數來評估。



如果您要將物件新增至已啟用舊版合規性的儲存桶中，則不允許將 creation-time 新增為使用者自訂中繼資料。系統將傳回錯誤。

- S3 物件鎖定請求標頭：

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

如果請求中沒有這些標頭，則使用儲存桶預設保留設定來計算物件版本的保留期限。

"使用 S3 REST API 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

[伺服器端加密的要求標頭]



有關 StorageGRID 如何處理 UTF-8 字元的資訊，請參閱["PutObject"](#)。

伺服器端加密的要求標頭

您可以使用下列請求標頭，以伺服器端加密方式對多部分物件進行加密。SSE 和 SSE-C 選項互斥。

- **SSE**：如果您希望使用由 StorageGRID 管理的唯一加密金鑰來加密物件，請在 CreateMultipartUpload 請求中使用下列標頭。請勿在任何 UploadPart 請求中指定此標頭。
 - x-amz-server-side-encryption
- **SSE-C**：如果您想使用您提供和管理的唯一金鑰對物件加密，請在 CreateMultipartUpload 請求（以及每個後續 UploadPart 請求）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：指定新物件加密金鑰的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請審查 ["使用伺服器端加密"](#) 的相關注意事項。

不支援的要求標頭

不支援以下請求標頭：

- x-amz-website-redirect-location

The x-amz-website-redirect-location 標頭返回 `XNotImplemented`。

版本控制

多部分上傳包含啟動上傳、列出上傳檔案、上傳各個部分、組裝已上傳部分及完成上傳等分隔操作。執行 CompleteMultipartUpload 操作時會建立物件（如果適用，也會進行版本控制）。

S3 ListMultipartUploads 操作和 StorageGRID 中支援的參數

此 ListMultipartUploads 操作列出儲存桶中正在進行的多部分上傳任務。

支援以下請求參數：

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

版本控制

多部分上傳包含啟動上傳、列出上傳檔案、上傳各個部分、組裝已上傳部分及完成上傳等分隔操作。執行 CompleteMultipartUpload 操作時會建立物件（如果適用，也會進行版本控制）。

StorageGRID 中 S3 UploadPart 作業支援和不支援的要求標頭

UploadPart 操作會上傳物件多部分上傳中的一個部分。

支援的要求標頭

支援以下請求標頭：

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

伺服器端加密的要求標頭

如果為 CreateMultipartUpload 請求指定了 SSE-C 加密，則還必須在每個 UploadPart 請求中包含以下請求標頭：

- x-amz-server-side-encryption-customer-algorithm：指定 AES256。
- x-amz-server-side-encryption-customer-key：指定與 CreateMultipartUpload 請求中提供的相同加密金鑰。
- x-amz-server-side-encryption-customer-key-MD5：指定與 CreateMultipartUpload 請求中提供

的相同 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請審查 ["使用伺服器端加密"](#) 中的注意事項。

如果您在 `CreateMultipartUpload` 請求中指定了 SHA-256 Checksum，則必須在每個 `UploadPart` 請求中包含下列請求標頭：

- `x-amz-checksum-sha256`：指定此部分的 SHA-256 Checksum。

不支援的要求標頭

不支援以下請求標頭：

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

版本控制

多部分上傳包含啟動上傳、列出上傳檔案、上傳各個部分、組裝已上傳部分及完成上傳等分隔操作。執行 `CompleteMultipartUpload` 操作時會建立物件（如果適用，也會進行版本控制）。

使用 **S3 UploadPartCopy** 操作將物件的一部分上傳到 **StorageGRID**

`UploadPartCopy` 操作透過從現有物件複製資料作為資料來源，上傳物件的一部分。

`UploadPartCopy` 操作完全按照 Amazon S3 REST API 的行為方式實作。如有更改，恕不另行通知。

此要求會讀取和寫入 `StorageGRID` 系統中 `x-amz-copy-source-range` 所指定的物件資料。

支援以下請求標頭：

- `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`

伺服器端加密的要求標頭

如果為 `CreateMultipartUpload` 請求指定了 SSE-C 加密，則還必須在每個 `UploadPartCopy` 請求中包含以下請求標頭：

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

如果來源物件使用客戶提供的金鑰（SSE-C）加密，則必須在 UploadPartCopy 請求中包含以下三個標頭，以便解密並複製該物件：

- x-amz-copy-source-server-side-encryption-customer-algorithm：指定 AES256。
- x-amz-copy-source-server-side-encryption-customer-key：指定您在建立來源物件時提供的加密金鑰。
- x-amz-copy-source-server-side-encryption-customer-key-MD5：指定您在建立來源物件時提供的 MD5 摘要。



您提供的加密金鑰不會被儲存。如果您遺失加密金鑰，您將遺失對應的物件。在使用客戶提供的金鑰保護物件資料之前，請審查 ["使用伺服器端加密"](#) 中的注意事項。

版本控制

多部分上傳包含啟動上傳、列出上傳檔案、上傳各個部分、組裝已上傳部分及完成上傳等分隔操作。執行 CompleteMultipartUpload 操作時會建立物件（如果適用，也會進行版本控制）。

StorageGRID S3 REST API 錯誤回應

StorageGRID 系統支援所有適用的標準 S3 REST API 錯誤回應。此外，StorageGRID 實作還新增了一些自訂回應。

支援的 S3 API 錯誤代碼

Name	HTTP 狀態
AccessDenied	403 禁止存取
BadDigest	400 Bad Request
BucketAlreadyExists	409 衝突
BucketNotEmpty	409 衝突
IncompleteBody	400 Bad Request
InternalError	500 內部伺服器錯誤
InvalidAccessKeyId	403 禁止存取
InvalidArgument	400 Bad Request
InvalidBucketName	400 Bad Request
InvalidBucketState	409 衝突

Name	HTTP 狀態
InvalidDigest	400 Bad Request
InvalidEncryptionAlgorithmError	400 Bad Request
InvalidPart	400 Bad Request
InvalidPartOrder	400 Bad Request
InvalidRange	416 要求的範圍無法滿足
InvalidRequest	400 Bad Request
InvalidStorageClass	400 Bad Request
InvalidTag	400 Bad Request
InvalidURI	400 Bad Request
KeyTooLong	400 Bad Request
MalformedXML	400 Bad Request
MetadataTooLarge	400 Bad Request
MethodNotAllowed	405 Method Not Allowed
MissingContentLength	411 必須提供長度
MissingRequestBodyError	400 Bad Request
MissingSecurityHeader	400 Bad Request
NoSuchBucket	404 找不到
NoSuchKey	404 找不到
NoSuchUpload	404 找不到
NotImplemented	501 未實作
NoSuchBucketPolicy	404 找不到

Name	HTTP 狀態
ObjectLockConfigurationNotFoundError	404 找不到
PreconditionFailed	412 先決條件失敗
RequestTimeTooSkewed	403 禁止存取
ServiceUnavailable	503 服務無法使用
SignatureDoesNotMatch	403 禁止存取
TooManyBuckets	400 Bad Request
UserKeyMustBeSpecified	400 Bad Request

StorageGRID 自訂錯誤代碼

Name	說明	HTTP 狀態
XBucketLifecycleNotAllowed	舊版符合法規的儲存桶不允許儲存桶生命週期組態。	400 Bad Request
XBucketPolicyParseException	無法解析接收的儲存桶原則 JSON。	400 Bad Request
XComplianceConflict	由於舊版法規遵循設定，操作遭拒。	403 禁止存取
XComplianceReducedRedundancyForbidden	舊版符合法規儲存桶不允許降低備援	400 Bad Request
XMaxBucketPolicyLengthExceeded	您的原則超過了允許的最大儲存桶原則長度。	400 Bad Request
XMissingInternalRequestHeader	內部請求缺少標頭。	400 Bad Request
XNoSuchBucketCompliance	指定的儲存桶未啟用舊版合規性。	404 找不到
XNotAcceptable	請求中包含一個或多個無法滿足的 Accept 標頭。	406 Not Acceptable
XNotImplemented	您提出的要求涉及的功能尚未實作。	501 未實作

StorageGRID 自訂操作

StorageGRID 中支援的自訂儲存貯體作業

StorageGRID 系統支援新增至 S3 REST API 的自訂操作。

下表列出 StorageGRID 支援的自訂操作。

操作	說明
"GET 儲存貯體一致性"	傳回套用至特定儲存貯體的一致性。
"PUT Bucket 一致性"	設定套用至特定儲存貯體的一致性。
"取得儲存桶上次存取時間"	傳回特定儲存桶是否啟用或停用上次存取時間更新。
"PUT 儲存貯體最後存取時間"	允許您啟用或停用特定儲存桶的最後存取時間更新。
"刪除 Bucket 中繼資料通知組態"	刪除與特定儲存桶關聯的中繼資料通知組態 XML。
"取得 Bucket 中繼資料通知組態"	傳回與特定儲存桶關聯的中繼資料通知組態 XML。
"PUT Bucket 中繼資料通知組態"	為儲存桶設定中繼資料通知服務。
"取得儲存使用情況"	顯示帳戶正在使用的總儲存設備量，以及與該帳戶關聯的每個儲存桶的儲存設備量。
"已棄用：CreateBucket 帶有法規遵循設定"	已棄用且不再支援：您無法再建立啟用法規遵循的新儲存桶。
"已棄用：GET Bucket 法規遵循"	已棄用但仍受支援：傳回現有舊版 Compliant 儲存桶目前生效的法規遵循設定。
"已棄用：PUT Bucket 法規遵循"	已棄用但仍受支援：允許您修改現有舊版 Compliant 儲存桶的法規遵循設定。

使用 **GET Bucket consistency** 請求在 **StorageGRID** 中檢索儲存桶一致性層級

GET Bucket 一致性請求可讓您確定套用於特定儲存桶的一致性。

預設一致性設定為確保新建立的物件的寫入後讀取。

您必須擁有 s3:GetBucketConsistency 權限，或者是帳戶 root 使用者，才能完成此操作。

請求範例

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

回應

在回應 XML 中，<Consistency> 將傳回下列其中一個值：

一致性	說明
全部	所有節點必須立即收到資料，否則請求將失敗。
strong-global	保證所有站台上所有用戶端請求的寫入後讀取一致性。
strong-site	保證站台內所有用戶端請求的寫入後讀取一致性。
新寫後讀取	（預設）為新物件提供寫入後讀取一致性，為物件更新提供最終一致性。提供高可用度和資料保護保證。建議用於大多數情況。
可用	為新建物件和物件更新提供最終一致性。對於 S3 儲存桶，僅在必要時使用（例如，用於包含很少讀取的日誌值的儲存桶，或對不存在的鍵執行 HEAD 或 GET 操作）。不支援 S3 FabricPool 儲存桶。

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"](#)

使用 PUT Bucket 一致性請求在 StorageGRID 中指定一致性層級

PUT Bucket 一致性要求可讓您指定要套用於儲存貯體上所執行作業的一致性。

預設一致性設定為確保新建立的物件的寫入後讀取。

開始之前

您必須擁有 s3:PutBucketConsistency 權限，或是帳戶根目錄使用者，才能完成此操作。

要求

此 `x-ntap-sg-consistency` 參數必須包含以下值之一：

一致性	說明
全部	所有節點必須立即收到資料，否則請求將失敗。
strong-global	保證所有站台上所有用戶端請求的寫入後讀取一致性。
strong-site	保證站台內所有用戶端請求的寫入後讀取一致性。
新寫後讀取	（預設）為新物件提供寫入後讀取一致性，為物件更新提供最終一致性。提供高可用度和資料保護保證。建議用於大多數情況。
可用	為新建物件和物件更新提供最終一致性。對於 S3 儲存桶，僅在必要時使用（例如，用於包含很少讀取的日誌值的儲存桶，或對不存在的鍵執行 HEAD 或 GET 操作）。不支援 S3 FabricPool 儲存桶。

注意：通常情況下，您應該使用「新寫後讀取」一致性。如果請求無法正常運作，請盡可能變更應用程式用戶端的行為。或者，設定用戶端為每個 API 請求指定一致性。僅在萬不得已的情況下才在儲存桶層級設定一致性。

請求範例

```
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"](#)

使用 GET Bucket last access time 請求從 StorageGRID 中擷取儲存區的最後存取時間狀態

GET Bucket last access time 請求可讓您確定是否為個別儲存桶啟用或停用上次存取時間

更新。

您必須擁有 `s3:GetBucketLastAccessTime` 權限，或者是帳戶 `root` 使用者，才能完成此操作。

請求範例

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

回應範例

此範例表示已為儲存桶啟用最後存取時間更新。

```
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>
```

使用 **PUT Bucket last access time** 請求在 **StorageGRID** 中啟用和停用最後存取時間更新

PUT Bucket 最後存取時間請求可讓您啟用或停用單一儲存桶的最後存取時間更新。停用最後存取時間更新可提升效能，且是使用 10.3.0 或更新版本建立的所有儲存桶的預設設定。

您必須擁有儲存桶的 `s3:PutBucketLastAccessTime` 權限，或是帳戶根目錄使用者，才能完成此操作。



從 StorageGRID 10.3 版本開始，所有新建儲存桶的最後存取時間更新預設為停用狀態。如果您有使用早期版本 StorageGRID 建立的儲存桶，並且希望與新的預設行為保持一致，則必須明確地為每個早期儲存桶停用最後存取時間更新。您可以使用 PUT Bucket last access time 請求或在租用戶管理員中儲存桶的詳細資訊頁面啟用或停用最後存取時間更新。請參閱 ["啟用或停用上次存取時間更新"](#)。

如果對儲存桶停用了最後存取時間更新，則對儲存桶的操作將套用下列行為：

- `GetObject`、`GetObjectAcl`、`GetObjectTagging` 和 `HeadObject` 請求不會更新上次存取時間。該物件不會新增至資訊生命週期管理 (ILM) 評估佇列。

- CopyObject 和 PutObjectTagging 僅更新中繼資料的請求也會更新上次存取時間。物件會新增至 ILM 評估佇列。
- 如果來源儲存桶的最後存取時間更新已停用，CopyObject 請求不會更新來源儲存桶的最後存取時間。複製的物件不會新增至來源儲存桶的 ILM 評估佇列。但是，對於目的地，CopyObject 請求一律會更新最後存取時間。物件的複本會新增至 ILM 評估佇列。
- CompleteMultipartUpload 請求更新最後存取時間。已完成的物件會加入 ILM 評估佇列。

請求範例

此範例可啟用儲存桶的最後存取時間。

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

此範例停用儲存桶的最後存取時間。

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

使用 **StorageGRID** 中的 **DELETE Bucket** 中繼資料通知組態要求停用搜尋整合服務

DELETE Bucket 中繼資料通知組態請求可讓您透過刪除組態 XML 來停用個別儲存桶的搜尋整合服務。

您必須擁有某個儲存桶的 s3:DeleteBucketMetadataNotification 權限，或是帳戶根目錄使用者，才能完成此操作。

請求範例

此範例示範如何停用儲存桶的搜尋整合服務。

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

使用 **GET Bucket** 元資料通知組態要求在 **StorageGRID** 中設定搜尋整合

GET Bucket 中繼資料通知組態請求可讓您擷取用於設定各個儲存桶搜尋整合的組態 XML。

您必須擁有 `s3:GetBucketMetadataNotification` 權限，或者是帳戶 `root` 使用者，才能完成此操作。

請求範例

此請求會擷取名為 `'bucket'` 的儲存桶的中繼資料通知組態。

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

回應

回應正文包含儲存桶的中繼資料通知組態。中繼資料通知組態可讓您確定如何設定儲存桶以進行搜尋整合。也就是說，它可讓您確定哪些物件會被索引，以及其物件中繼資料會傳送至哪些端點。

```
<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條或多條規則。每條規則指定其適用的物件以及 `StorageGRID` 應將物件中繼資料傳送到的目的地。目的地必須使用 `StorageGRID` 端點的 URN 指定。

Name	說明	必填
MetadataNotificationConfiguration	用於指定中繼資料通知的物件和目的地的規則容器標籤。 包含一個或多個規則元素。	是的

Name	說明	必填
規則	用於識別應將其中繼資料新增至指定索引之物件規則的容器標籤。 前綴重疊的規則將被拒絕。 包含在 MetadataNotificationConfiguration 元素中。	是的
ID	規則的唯一識別碼。 包含在規則元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。對於已停用的規則，不會採取任何行動。 包含在規則元素中。	是的
前綴	與前綴相符的物件會受到該規則的影響，其中繼資料會傳送至指定的目的地。 若要符合所有物件，請指定空白前綴。 包含在規則元素中。	是的
目的地	規則目的地的容器標籤。 包含在規則元素中。	是的
Urn	物件中繼資料發送到的目的地的 URN。必須是具有以下屬性的 StorageGRID 端點的 URN： • `es` 必須是第三個元素。 • URN 必須以中繼資料儲存的索引和類型結尾，格式為 domain-name/myindex/mytype。 端點透過 Tenant Manager 或租戶管理 API 進行設定。它們採用以下形式： • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype 必須先設定端點，然後才能提交組態 XML，否則組態將失敗並出現 404 錯誤。 Urn 包含在 Destination 元素中。	是的

```
`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`  
標籤之間的 XML
```

程式碼展示如何為儲存桶設定與搜尋整合端點的整合。在本例中，物件中繼資料被傳送到名為 `current`、類型名為 `2017` 的 Elasticsearch 索引，該索引託管在名為 `records` 的 AWS 網域中。

```
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-  
1:33333333:domain/records/current/2017</Urn>  
    </Destination>  
  </Rule>  
</MetadataNotificationConfiguration>
```

相關資訊

["使用租戶帳戶"](#)

使用 **PUT Bucket** 元資料通知設定請求在 **StorageGRID** 中啟用搜尋整合服務

PUT Bucket 中繼資料通知組態請求可讓您為單一儲存桶啟用搜尋整合服務。您在請求內文中提供的中繼資料通知組態 XML 指定要將其中繼資料傳送至目的地搜尋索引的物件。

您必須擁有儲存貯體的 s3:PutBucketMetadataNotification 權限，或是帳戶根目錄使用者，才能完成此操作。

要求

請求正文中必須包含中繼資料通知組態。每個中繼資料通知組態包含一或多條規則。每條規則指定其適用的物件，以及 StorageGRID 應將物件中繼資料傳送至的目的地。

可以根據物件名稱的前綴對物件進行篩選。例如，您可以將具有前綴 `/images` 的物件中繼資料傳送到一個目的地，並將具有前綴 `/videos` 的物件中繼資料傳送到另一個目的地。

前綴重疊的組態無效，提交時會被拒絕。例如，若某組態包含兩條規則，一條針對前綴為 `test` 的物件，另一條針對前綴為 `test2` 的物件，則該組態將不被允許。

目的地必須使用 StorageGRID 端點的 URN 來指定。提交中繼資料通知組態時，端點必須存在，否則請求將失敗為 400 Bad Request。錯誤訊息如下：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>
```

此表說明中繼資料通知組態 XML 中的元素。

Name	說明	必填
MetadataNotificationConfiguration	用於指定中繼資料通知的物件和目的地的規則容器標籤。 包含一個或多個規則元素。	是的
規則	用於識別應將其中繼資料新增至指定索引之物件規則的容器標籤。 前綴重疊的規則將被拒絕。 包含在 MetadataNotificationConfiguration 元素中。	是的
ID	規則的唯一識別碼。 包含在規則元素中。	否

Name	說明	必填
狀態	狀態可以是「已啟用」或「已停用」。對於已停用的規則，不會採取任何行動。 包含在規則元素中。	是的
前綴	與前綴相符的物件會受到該規則的影響，其中繼資料會傳送至指定的目的地。 若要符合所有物件，請指定空白前綴。 包含在規則元素中。	是的
目的地	規則目的地的容器標籤。 包含在規則元素中。	是的
Urn	物件中繼資料發送到的目的地的 URN。必須是具有以下屬性的 StorageGRID 端點的 URN： • `es` 必須是第三個元素。 • URN 必須以中繼資料儲存的索引和類型結尾，格式為 <code>domain-name/myindex/mytype</code>。 端點透過 Tenant Manager 或租戶管理 API 進行設定。它們採用以下形式： • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> 必須先設定端點，然後才能提交組態 XML，否則組態將失敗並出現 404 錯誤。 Urn 包含在 Destination 元素中。	是的

請求範例

此範例示範如何為儲存桶啟用搜尋整合。在本範例中，所有物件的物件中繼資料都會傳送到相同目的地。

```

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，符合前綴 `/images` 的物件之物件中繼資料會傳送至一個目的地，而符合前綴 `/videos` 的物件之物件中繼資料則會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-1:3333333: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>

```

搜尋整合服務產生的 JSON

為儲存桶啟用搜尋整合服務時，每次新增、更新或刪除物件中繼資料或標籤時，都會產生一個 JSON 文件並將其傳送至目的地端點。

此範例顯示在名為 test 的儲存貯體中建立具有金鑰 SGWS/Tagging.txt 的物件時，可能產生的 JSON 範例。test 儲存貯體未啟用版本控制，因此 versionId 標記為空。

```
{
  "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

此表列出啟用搜尋整合時傳送至目的地端點的 JSON 文件中所包含的所有欄位。

文件名稱包含儲存桶名稱、物件名稱和版本 ID（如果有）。

類型	物品名稱	說明
儲存桶和物件資訊	儲存貯體	儲存貯體的名稱
儲存桶和物件資訊	金鑰	物件鍵名
儲存桶和物件資訊	versionID	物件版本，適用於版本化儲存貯體中的物件
儲存桶和物件資訊	區域	儲存貯體區域，例如 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	物品名稱	說明
使用者中繼資料	中繼資料 <i>key:value</i>	該物件的所有使用者中繼資料，以鍵值對的形式呈現。
標籤	標籤 <i>key:value</i>	物件的所有定義物件標籤，以鍵值對的形式呈現



對於標籤和使用者中繼資料，StorageGRID 會將日期和數字作為字串或 S3 事件通知傳遞給 Elasticsearch。若要設定 Elasticsearch 將這些字串解釋為日期或數字，請按照 Elasticsearch 的動態欄位對應和日期格式對應說明進行操作。您必須先在索引上啟用動態欄位對應，然後才能設定搜尋整合服務。文件建立索引後，您將無法在索引中編輯該文件的欄位類型。

相關資訊

["使用租戶帳戶"](#)

使用 GET Storage Usage 請求擷取 StorageGRID 中的帳戶和儲存桶儲存使用量

GET Storage Usage 要求會告訴您帳戶正在使用的總儲存設備量，以及與該帳戶關聯的每個儲存桶的使用量。

可以透過具有 `x-ntap-sg-usage` 查詢參數的修改版 ListBuckets 請求來取得帳戶及其儲存桶所使用的儲存設備空間。儲存桶的儲存設備使用情況與系統處理的 PUT 和 DELETE 請求是分開追蹤的。由於請求處理需要時間，尤其是在系統負載較高的情況下，使用量值與預期值之間可能會有一些延遲。

預設情況下，StorageGRID 嘗試使用強全域一致性來擷取使用量資訊。如果無法達成強全域一致性，StorageGRID 則嘗試使用強站點一致性來擷取使用量資訊。

您必須擁有 `s3:ListAllMyBuckets` 權限，或者是帳戶根目錄使用者，才能完成此操作。

請求範例

```
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，該帳戶在兩個儲存桶中包含四個物件和 12 個位元組的資料。每個儲存桶包含兩個物件和 6 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>
```

版本控制

每個儲存的物件版本都會對回應中的 `ObjectCount` 和 `DataBytes` 值產生貢獻。刪除標記不會計入 `ObjectCount` 總數。

相關資訊

["一致性"](#)

已棄用的舊版法規遵循儲存桶請求

已棄用的儲存區請求（針對舊版 **StorageGRID** 法規遵循）

您可能需要使用 StorageGRID S3 REST API 來管理使用舊版法規遵循功能建立的儲存桶。

法規遵循功能已棄用

先前 StorageGRID 版本中提供的 StorageGRID 法規遵循功能已過時，並已由 S3 Object Lock 取代。

如果您之前啟用了全域法規遵循設定，則在 StorageGRID 11.6 中也會啟用全域 S3 物件鎖定設定。您將無法再建立啟用法規遵循的新儲存桶；但是，您可以視需要使用 StorageGRID S3 REST API 來管理任何現有的舊版合規儲存桶。

- ["使用 S3 REST API 設定 S3 物件鎖定"](#)
- ["使用 ILM 管理物件"](#)
- ["NetApp 知識庫：如何在 StorageGRID 11.5 中管理舊版符合法規的儲存桶"](#)

已棄用的法規遵循請求：

- ["已棄用 - 為法規遵循而對 PUT Bucket 請求進行的修改"](#)

SGCompliance XML 元素已棄用。以前，您可以在 PUT Bucket 請求的選用 XML 請求本文中包含此 StorageGRID 自訂元素，以建立法規遵循儲存桶。

- ["已棄用 - GET Bucket compliance"](#)

GET Bucket 法規遵循請求已棄用。但是，您仍然可以使用此要求來確定現有舊版 Compliant 儲存桶目前生效的法規遵循設定。

- ["已棄用 - PUT Bucket 法規遵循"](#)

PUT Bucket 法規遵循請求已棄用。但是，您仍然可以使用此請求來修改現有舊版符合法規儲存桶的法規遵循設定。例如，您可以將現有儲存桶置於合法持有或增加其保留期間。

StorageGRID 中已棄用的 SGCompliance 元素

SGCompliance XML 元素已棄用。先前，您可以將此 StorageGRID 自訂元素包含在 CreateBucket 請求的選用 XML 請求本文中，以建立符合法規的儲存桶。



先前 StorageGRID 版本中提供的 StorageGRID 法規遵循功能已過時，並已由 S3 Object Lock 取代。如需詳細資訊，請參閱下列內容：

- ["使用 S3 REST API 設定 S3 物件鎖定"](#)
- ["NetApp 知識庫：如何在 StorageGRID 11.5 中管理舊版符合法規的儲存桶"](#)

您無法再建立啟用法規遵循的新儲存桶。如果您嘗試使用 CreateBucket 法規遵循請求修改來建立新的符合法規儲存桶，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.
```

StorageGRID 中已棄用的 GET Bucket 合規性要求

GET Bucket 法規遵循請求已棄用。但是，您仍然可以使用此要求來確定現有舊版 Compliant 儲存桶目前生效的法規遵循設定。



先前 StorageGRID 版本中提供的 StorageGRID 法規遵循功能已過時，並已由 S3 Object Lock 取代。如需詳細資訊，請參閱下列內容：

- ["使用 S3 REST API 設定 S3 物件鎖定"](#)
- ["NetApp 知識庫：如何在 StorageGRID 11.5 中管理舊版符合法規的儲存桶"](#)

您必須擁有 s3:GetBucketCompliance 權限，或者是帳戶根目錄使用者，才能完成此操作。

請求範例

此範例請求可讓您確定名為 `mybucket` 的儲存桶的法規遵循設定。

```
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>` 列出了儲存桶生效的法規遵循設定。此範例回應顯示了一個儲存桶的法規遵循設定，其中每個物件將從被擷取到網格之日起保留一年（525,600 分鐘）。此儲存桶目前沒有合法持有。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>
```

Name	說明
RetentionPeriodMinutes	新增至此儲存桶中的物件的保留期間，以分鐘為單位。保留期間從物件納入網格時開始計算。

Name	說明
LegalHold	• True：此儲存桶目前處於合法持有狀態。即使物件的保留期間已過，在合法持有解除之前，也無法刪除此儲存桶中的物件。 • False：此儲存桶目前未處於合法持有。此儲存桶中的物件可在其保留期間到期後刪除。
AutoDelete	• 正確：除非儲存桶受到合法持有，否則此儲存桶中的物件將在其保留期間到期時自動刪除。 • 錯誤：此儲存桶中的物件不會在保留期間到期後自動刪除。如果您需要刪除這些物件，則必須手動刪除。

錯誤回應

如果儲存桶建立時不合法規，則回應的 HTTP 狀態代碼為 404 Not Found，S3 錯誤代碼為 XNoSuchBucketCompliance。

StorageGRID 中已棄用的 PUT Bucket 合規性要求

PUT Bucket 法規遵循請求已棄用。但是，您仍然可以使用此請求來修改現有舊版符合法規儲存桶的法規遵循設定。例如，您可以將現有儲存桶置於合法持有或增加其保留期間。



先前 StorageGRID 版本中提供的 StorageGRID 法規遵循功能已過時，並已由 S3 Object Lock 取代。如需詳細資訊，請參閱下列內容：

- ["使用 S3 REST API 設定 S3 物件鎖定"](#)
- ["NetApp 知識庫：如何在 StorageGRID 11.5 中管理舊版符合法規的儲存桶"](#)

您必須擁有 s3:PutBucketCompliance 權限，或者是帳戶根目錄使用者，才能完成此操作。

發出 PUT Bucket 法規遵循請求時，必須為法規遵循設定的每個欄位指定一個值。

請求範例

此範例請求修改名為 `mybucket` 的儲存貯體的法規遵循設定。在此範例中，`mybucket` 中的物件將從物件擷取至網格時起保留兩年（1,051,200 分鐘），而非一年。此儲存貯體沒有合法持有。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>

```

Name	說明
RetentionPeriodMinutes	新增至此儲存桶中的物件的保留期間，以分鐘為單位。保留期間從物件納入網格時開始計算。 重要提示 為 RetentionPeriodMinutes 指定新值時，必須指定等於或大於儲存桶目前保留期間的值。儲存桶的保留期間設定後，無法減少該值，只能增加。
LegalHold	• True：此儲存桶目前處於合法持有狀態。即使物件的保留期間已過，在合法持有解除之前，也無法刪除此儲存桶中的物件。 • False：此儲存桶目前未處於合法持有。此儲存桶中的物件可在其保留期間到期後刪除。
AutoDelete	• 正確：除非儲存桶受到合法持有，否則此儲存桶中的物件將在其保留期間到期時自動刪除。 • 錯誤：此儲存桶中的物件不會在保留期間到期後自動刪除。如果您需要刪除這些物件，則必須手動刪除。

法規遵循設定的一致性

當您使用 PUT Bucket 法規遵循要求更新 S3 儲存桶的法規遵循設定時，StorageGRID 會嘗試在整個網格中更新該儲存桶的中繼資料。預設情況下，StorageGRID 使用 **Strong-global** 一致性來確保所有資料中心站台和所有包含儲存桶中繼資料的儲存節點，對於已變更的法規遵循設定都具有寫入後讀取一致性。

如果由於資料中心站台或站台上的多個 Storage Node 無法使用，StorageGRID 無法達到 **Strong-global** 一致性，則回應的 HTTP 狀態碼為 503 Service Unavailable。

如果您收到此回應，則必須聯絡網格系統管理員，以確保盡快提供所需的儲存設備服務。如果網格系統管理員無法在每個站台提供足夠的儲存節點，技術支援可能會指導您透過強制執行 **Strong-site** 一致性來重試失敗的請求。



除非技術支援人員指示您這樣做，並且您了解使用此層級可能造成的後果，否則切勿強制 PUT bucket 法規遵循採用 **Strong-site** 一致性。

當一致性降低至「強站台」時，StorageGRID 僅保證更新後的法規遵循設定對站台內的用戶端請求具有寫入後讀取一致性。這意味著在所有站台和儲存節點可用之前，StorageGRID 系統可能會暫時為該儲存桶設定多個不一致的設定。這些不一致的設定可能會導致意外且不希望出現的行為。例如，如果您將儲存桶置於合法持有狀態，並強制降低一致性，則該儲存桶先前的法規遵循設定（即關閉合法持有）可能在某些資料中心站台仍然有效。因此，您認為處於合法持有狀態的物件，可能會在其保留期間到期時遭使用者刪除，或在啟用 AutoDelete 的情況下遭其刪除。

若要強制使用 **Strong-site** 一致性，請重新發出 PUT Bucket 法規遵循請求，並包含 Consistency-Control HTTP 請求標頭，如下所示：

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

錯誤回應

- 如果儲存桶的建立不合法規，則回應的 HTTP 狀態代碼為 404 Not Found。
- 如果 RetentionPeriodMinutes 請求中的值小於儲存桶的目前保留期間，則 HTTP 狀態碼為 400 Bad Request。

相關資訊

["已棄用：為法規遵循而對 PUT Bucket 請求進行的修改"](#)

管理存取原則

StorageGRID 如何使用 AWS 原則來控制對 S3 儲存貯體和物件的存取

StorageGRID 使用 Amazon Web Services (AWS) 原則語言，讓 S3 租戶控制對儲存桶及其內部物件的存取。StorageGRID 系統實作了 S3 REST API 原則語言的子集。S3 API 的存取原則以 JSON 格式編寫。

存取原則總覽

StorageGRID 支援三種存取原則：

- 儲存桶原則，可透過 GetBucketPolicy、PutBucketPolicy 和 DeleteBucketPolicy S3 API 操作或 Tenant Manager 或 Tenant Management API 進行管理。儲存桶原則附加至儲存桶，因此可設定為控制儲存桶擁有者帳戶或其他帳戶中的使用者對儲存桶及其中物件的存取。一個儲存桶原則僅適用於一個儲存桶，但可能適用於多個群組。
- *群組原則*是透過 Tenant Manager 或租戶管理 API 進行設定。群組原則會附加到帳戶中的某個群組，因此可設定為允許該群組存取該帳戶所擁有的特定資源。一個群組原則只適用於一個群組，但可能適用於多個儲存桶。
- 工作階段原則，包含在發出 AssumeRole 請求的過程中。工作階段原則僅適用於指定的工作階段，進一步定義使用者所擁有的權限，以及群組原則和儲存桶原則所授予的權限。



群組原則、儲存桶原則和工作階段原則的優先順序沒有區別。

StorageGRID 儲存貯體和群組原則遵循 Amazon 定義的特定語法。每個原則內都包含一個原則聲明陣列，每個

聲明包含以下元素：

- 聲明 ID (Sid) (選用)
- 影響
- Principal/NotPrincipal
- 資源/NotResource
- 動作/NotAction
- 條件 (選用)

原則聲明是使用此結構建立的，以指定權限：授予 <Effect> 以允許/拒絕 <Principal> 在 <Condition> 適用時對 <Resource> 執行 <Action>。

每個原則要素都有其特定的功能：

元素	說明
Sid	Sid 元素是選用的。Sid 僅用於向使用者提供執行摘要。它會被儲存，但不會被 StorageGRID 系統解析。
影響	使用 Effect 元素來決定是否允許或拒絕指定的操作。您必須使用支援的 Action 元素關鍵字來識別對儲存桶或物件允許（或拒絕）的操作。
Principal/NotPrincipal	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。如果請求中未包含 S3 簽署，則可以透過將萬用字元 (*) 指定為主體來允許匿名存取。預設情況下，只有帳戶根目錄才能存取該帳戶擁有的資源。 您只需在儲存桶原則中指定 Principal 元素。對於群組原則，原則所附加的群組即為隱含的 Principal 元素。
資源/NotResource	Resource 元素用於識別儲存桶和物件。您可以使用 Amazon Resource Name (ARN) 來識別資源，以允許或拒絕儲存桶和物件的權限。
動作/NotAction	Action 和 Effect 元素是權限的兩個組成部分。當群組請求資源時，系統會授予或拒絕其存取該資源的權限。除非您明確指定權限，否則存取將被拒絕；但您可以使用明確拒絕來置換其他原則授予的權限。
狀態	Condition 元素是選用的。條件可讓您建立運算式，以判斷何時應套用原則。

在 Action 元素中，您可以使用萬用字元 (*) 來指定所有動作或動作的子集。例如，此 Action 符合諸如 s3:GetObject、s3:PutObject 和 s3:DeleteObject 之類的權限。

```
s3:*Object
```

在 Resource 元素中，您可以使用萬用字元 (*) 和 (?)。星號 (*) 符合 0 個或多個字元，而問號 (?) 則符合任意單一字元。

在 Principal 元素中，除設定匿名存取（授予所有人權限）外，不支援萬用字元。例如，您可以將萬用字元 (*) 設定為 Principal 值。

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

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

以下範例中，聲明使用了 Effect、Principal、Action 和 Resource 元素。此範例展示了一個完整的儲存貯體原則聲明，該聲明使用 Effect「Allow」授予 Principal、管理員群組 federated-group/admin 和財務群組 federated-group/finance 執行 Action s3:ListBucket（針對名為 mybucket 的儲存貯體）以及 Action s3:GetObject（針對該儲存貯體內所有物件）的權限。

```
{
  "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:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

儲存桶原則的大小限制為 20,480 位元組，群組原則的大小限制為 5,120 位元組。

原則的一致性

預設情況下，對群組原則所做的任何更新最終都是一致的。由於原則快取機制，群組原則達到一致後，變更可能需要額外 15 分鐘才能生效。預設情況下，對儲存貯體原則所做的任何更新都是強一致的。

您可以根據需要變更儲存桶原則更新的一致性保證。例如，您可能希望在站台停電期間，儲存桶原則的變更仍然有效。

在這種情況下，您可以在 PutBucketPolicy 請求中設定 Consistency-Control 標頭，或使用 PUT Bucket 一致性

請求。當儲存桶原則達成一致，由於原則快取，變更可能需要額外 8 秒才能生效。



如果為了應對臨時情況而將一致性設定為不同的值，請務必在完成後將儲存桶層級的設定還原為原始值。否則，所有後續的儲存桶請求都將使用修改後的設定。

什麼是工作階段原則？

工作階段原則是一種存取原則，它會在特定工作階段期間（例如使用者加入某個群組時）暫時限制使用者的權限。工作階段原則只能允許一部分權限，而不能授予額外的權限。群組本身可能擁有更廣泛的權限。

在原則聲明中使用 **ARN**

在原則聲明中，ARN 用於 Principal 和 Resource 元素。

- 使用下列語法指定 S3 資源 ARN：

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

- 使用此語法指定身分資源 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
```

其他考慮因素：

- 您可以使用星號 (*) 作為萬用字元，以比對物件索引鍵中的零個或多個字元。
- 物件鍵中可指定的國際字元應使用 JSON UTF-8 編碼或使用 JSON \u 轉義序列進行編碼。不支援百分比編碼。

["RFC 2141 URN 語法"](#)

PutBucketPolicy 操作的 HTTP 請求本文必須使用 charset=UTF-8 進行編碼。

在原則中指定資源

在原則聲明中，您可以使用 Resource 元素來指定允許或拒絕權限的儲存桶或物件。

- 每條原則聲明都需要一個資源元素。在原則中，資源以元素 Resource 表示，或以 NotResource 表示排除項。
- 您可以使用 S3 資源 ARN 指定資源。例如：

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

- 您也可以物件鍵中使用原則變數。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不存在的儲存桶。

在原則中指定主體

使用 Principal 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。

- 儲存桶原則中的每個原則聲明都必須包含一個 Principal 元素。群組原則中的原則聲明不需要 Principal 元素，因為群組本身即被視為主體。
- 在原則中，委託人以元素「Principal」表示，或以「NotPrincipal」表示排除。
- 必須使用 ID 或 ARN 指定以帳戶為基礎的身分識別：

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

- 此範例使用租戶帳戶 ID 27233906934684427525，其中包括帳戶根目錄和帳戶中的所有使用者：

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

- 您可以只指定帳戶根目錄：

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

- 您可以指定一個特定的聯合使用者（「Alex」）：

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

- 您可以指定一個特定的聯合群組（「Managers」）：

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

- 您可以指定匿名主體：

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

- 為避免歧義，您可以使用使用者 UUID 來取代使用者名稱：

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

例如，假設 Alex 離開了組織，使用者名稱 `Alex` 被刪除。如果新的 Alex 加入組織並被指派了相同的 `Alex` 使用者名稱，則新使用者可能會無意中繼承原始使用者的權限。

- 主值可以指定在建立儲存桶原則時尚不存在的群組/使用者名稱。

在原則中指定權限

在原則中，Action 元素用於允許/拒絕對資源的權限。您可以在原則中指定一系列權限，這些權限由元素「Action」表示，或以「NotAction」表示排除。每個元素都對應特定的 S3 REST API 操作。

表中列出了適用於儲存桶的權限和適用於物件的權限。



Amazon S3 現在針對 PutBucketReplication 和 DeleteBucketReplication 行動，皆使用 s3:PutReplicationConfiguration 權限。StorageGRID 針對每個行動使用分隔的權限，這與原始的 Amazon S3 規格相符。



當使用 put 操作置換現有值時，執行的是 delete 操作。

適用於儲存桶的權限

權限	S3 REST API 操作	StorageGRID 客製
s3:CreateBucket	CreateBucket	是的。 注意：僅限在群組原則中使用。
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	刪除 Bucket 中繼資料通知組態	是的
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	是的，PUT 和 DELETE 需要分隔的權限
s3:GetBucketAcl	GetBucketAcl	

權限	S3 REST API 操作	StorageGRID 客製
s3:GetBucketCompliance	GET Bucket 法規遵循 (已淘汰)	是的
s3:GetBucketConsistency	GET 儲存貯器一致性	是的
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	取得儲存桶上次存取時間	是的
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	取得 Bucket 中繼資料通知組態	是的
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	- ListBuckets - 取得儲存使用情況	是的，適用於 GET Storage Usage。 注意：僅限在群組原則中使用。
s3 : ListBucket	- ListObjects - HeadBucket - RestoreObject	
s3:ListBucketMultipartUploads	- ListMultipartUploads - RestoreObject	
s3:ListBucketVersions	取得儲存桶版本	

權限	S3 REST API 操作	StorageGRID 客製
s3:PutBucketCompliance	PUT Bucket 法規遵循（已棄用）	是的
s3:PutBucketConsistency	PUT Bucket 一致性	是的
s3:PutBucketCORS	- DeleteBucketCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT 儲存貯體最後存取時間	是的
s3:PutBucketMetadataNotification	PUT Bucket 中繼資料通知組態	是的
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	- CreateBucket 透過 x-amz-bucket-object-lock-enabled: true 請求標頭（還需要 s3:CreateBucket 權限） - PutObjectLockConfiguration	
s3 : PutBucketPolicy	PutBucketPolicy	
s3 : PutBucketTagging	- DeleteBucketTagging† - PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	是的，PUT 和 DELETE 需要分隔的權限

適用於物件的權限

權限	S3 REST API 操作	StorageGRID 客製
s3:AbortMultipartUpload	- AbortMultipartUpload - RestoreObject	

權限	S3 REST API 操作	StorageGRID 客製
s3:BypassGovernanceRetention	- DeleteObject - DeleteObjects - PutObjectRetention	
s3:DeleteObject	- DeleteObject - DeleteObjects - RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (該物件的特定版本)	
s3:DeleteObjectVersion	DeleteObject (該物件的特定版本)	
s3:GetObject	- GetObject - HeadObject - RestoreObject - SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3 : GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (該物件的特定版本)	
s3:GetObjectVersion	GetObject (該物件的特定版本)	
s3:ListMultipartUploadParts	ListParts 、 RestoreObject	

權限	S3 REST API 操作	StorageGRID 客製
s3:PutObject	- PutObject - CopyObject - RestoreObject - CreateMultipartUpload - CompleteMultipartUpload - UploadPart - UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (該物件的特定版本)	
s3:PutOverwriteObject	- PutObject - CopyObject - PutObjectTagging - DeleteObjectTagging - CompleteMultipartUpload	是的
s3:RestoreObject	RestoreObject	

使用 PutOverwriteObject 權限

s3:PutOverwriteObject 權限是 StorageGRID 的自訂權限，適用於建立或更新物件的操作。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 物件標籤。

此權限的可能設定包括：

- 允許：用戶端可以覆蓋物件。這是預設值。
- 拒絕：用戶端無法覆蓋物件。設定為「拒絕」時，PutOverwriteObject 權限運作方式如下：
 - 如果在同一路徑下找到已存在的物件：
 - 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。
 - 正在進行的所有擷取操作均被取消，並傳回錯誤。
 - 如果啟用了 S3 版本控制，則「拒絕」設定會阻止 PutObjectTagging 或 DeleteObjectTagging 操作修改物件及其非目前版本的 TagSet。
 - 如果找不到現有物件，則此權限無效。
- 如果此權限不存在，則效果與設定了「允許」權限相同。



如果目前的 S3 原則允許覆蓋，且 PutOverwriteObject 權限設定為「拒絕」，則用戶端無法覆蓋物件的資料、使用者定義的中繼資料或物件標記。此外，如果勾選「封鎖用戶端修改」核取方塊（「組態」>「安全性設定」>「網路和物件」），則該設定會覆寫 PutOverwriteObject 權限設定。

在原則中指定條件

條件定義了原則何時生效。條件由運算子和鍵值對組成。

條件使用鍵值對進行評估。一個 Condition 元素可以包含多個條件，每個條件又可以包含多個鍵值對。條件區塊的格式如下：

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

在以下範例中，IpAddress 條件使用 SourceIp 條件索引鍵。

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

支援的條件運算子

條件運算子依下列方式分類：

- 字串
- 數值
- 布林值
- IP 位址
- 空值檢查

條件算子	說明
StringEquals	將鍵與字串值進行精確比對（區分大小寫）。
StringNotEquals	根據否定匹配（區分大小寫）將鍵與字串值進行比較。
StringEqualsIgnoreCase	將鍵與字串值進行精確比對（忽略大小寫）。

條件算子	說明
StringNotEqualsIgnoreCase	將鍵與字串值進行比較，採用否定匹配（忽略大小寫）。
StringLike	將鍵與字串值進行精確比對（區分大小寫）。支援 * 和 ? 萬用字元。
StringNotLike	將鍵與字串值進行比較，採用取反匹配（區分大小寫）。可包含 * 和 ? 萬用字元。
NumericEquals	將鍵與數值進行精確比對。
NumericNotEquals	將金鑰與數值進行比較，基於否定匹配。
NumericGreaterThan	將金鑰與數值進行比較，基於「大於」匹配。
NumericGreaterThanEquals	將金鑰與數值進行比較，依據「大於或等於」的比對規則。
NumericLessThan	將金鑰與數值進行比較，基於「小於」匹配。
NumericLessThanEquals	將金鑰與數值進行比較，依據「小於或等於」的比對規則。
布林值	根據「真或假」比對，將鍵與布林值進行比較。
IpAddress	將金鑰與 IP 位址或 IP 位址範圍進行比較。
NotIpAddress	根據否定匹配，將金鑰與 IP 位址或 IP 位址範圍進行比較。
Null	檢查目前請求內容中是否存在條件索引鍵。
IfExists	附加到除 Null 條件之外的任何條件運算子，以檢查該條件索引鍵是否存在。如果條件索引鍵不存在，則傳回 TRUE。

支援的條件鍵

條件鍵	動作	說明
aws:SourceIp	IP 營運者	將與傳送請求的 IP 位址進行比較。可用於儲存桶或物件操作。 *注意：*如果 S3 請求是透過管理節點和閘道節點上的負載平衡器服務發送的，則會與負載平衡器服務上游的 IP 位址進行比較。 注意：如果使用第三方非透明負載平衡器，則會與該負載平衡器的 IP 位址進行比較。任何 `X-Forwarded-For` 標頭都將被忽略，因為無法確定其有效性。
aws:username	資源/身分	將與發送請求的發送者使用者名稱進行比較。可用於儲存桶或物件操作。
s3:delimiter	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的分隔符號參數進行比較。
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	要求現有物件具有特定的標籤鍵和值。
s3:max-keys	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的 max-keys 參數進行比較。

條件鍵	動作	說明
s3:object-lock-mode	s3:PutObject	與 PutObject、CopyObject 和 CreateMultipartUpload 請求的請求標頭中展開的 `object-lock-mode` 進行比較。
s3:object-lock-mode	s3:PutObjectRetention	與 PutObjectRetention 請求中 XML 正文展開的 `object-lock-mode` 進行比較。
s3:object-lock-remaining-retention-days	s3:PutObject	與 `x-amz-object-lock-retain-until-date` 請求標頭中指定的保留期限或根據儲存桶預設保留期間計算出的保留期限進行比較，以確保這些值在以下請求的允許範圍內： • PutObject • CopyObject • CreateMultipartUpload
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	與 PutObjectRetention 請求中指定的保留截止日期進行比較，以確保其在允許的範圍內。
s3:prefix	s3:ListBucket 和 s3:ListBucketVersions 權 限	將與 ListObjects 或 ListObjectVersions 請求中指定的前綴參數進行比較。
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	當物件請求包含標籤時，需要特定的標籤金鑰和值。
s3:x-amz-server-side-encryption-customer-algorithm	s3:PutObject	與 `sse-customer-algorithm` 或與從 PutObject、CopyObject、CreateMultipartUpload、UploadPart、UploadPartCopy 和 CompleteMultipartUpload 請求標頭中展開的 `copy-source-sse-customer-algorithm` 進行比較。

在原則中指定變數

您可以在原則中使用變數，以在資訊可用時填入原則資訊。您可以在 Resource 元素中使用原則變數，也可以在 Condition 元素中的字串比較中使用原則變數。

在這個例子中，該變數 `\${aws:username}` 是 Resource 元素的一部分：

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

在這個例子中，該變數 `\${aws:username}` 是條件區塊中條件值的一部分：

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

變數	說明
<code>\${aws:SourceIp}</code>	使用 SourceIp 金鑰作為提供的變數。
<code>\${aws:username}</code>	使用使用者名稱鍵作為提供的變數。
<code>\${s3:prefix}</code>	使用服務專屬前置詞金鑰作為提供的變數。
<code>\${s3:max-keys}</code>	使用服務專屬的 max-keys 金鑰作為提供的變數。
<code>\${*}</code>	特殊字元。使用該字元作為字面意義上的 * 字元。
<code>\${?}</code>	特殊字元。將字元用作文字 ? 字元。
<code>\${\$}</code>	特殊字元。將該字元用作實際的美元符號 \$ 字元。

建立需要特殊處理的原則

有時，原則授予的權限可能會對安全性或持續營運構成威脅，例如鎖定帳戶的 root 使用者。StorageGRID S3 REST API 實作的原則驗證限制比 Amazon 寬鬆，但原則評估同樣嚴格。

原則執行摘要	原則類型	Amazon 行為	StorageGRID 行為
拒絕自己擁有任何根目錄帳戶權限	儲存貯體	原則有效且已強制執行，但 root 使用者帳戶保留對所有 S3 儲存桶原則操作的權限	相同
拒絕自己對使用者/群組的任何權限	群組	有效且強制執行	相同
允許外部帳戶群組擁有任何權限	儲存貯體	無效的委託人	有效，但當原則允許時，所有 S3 儲存貯體原則操作的權限都會傳回 405 Method Not Allowed 錯誤

原則執行摘要	原則類型	Amazon 行為	StorageGRID 行為
允許外部帳戶 root 使用者或使用者擁有任何權限	儲存貯體	有效，但當原則允許時，所有 S3 儲存貯體原則操作的權限都會傳回 405 Method Not Allowed 錯誤	相同
允許所有人執行所有操作	儲存貯體	有效，但所有 S3 儲存貯體原則操作的權限對外部帳戶 root 使用者和使用者傳回 405 Method Not Allowed 錯誤	相同
拒絕所有人執行所有操作的權限	儲存貯體	原則有效且已強制執行，但 root 使用者帳戶保留對所有 S3 儲存桶原則操作的權限	相同
Principal 是一個不存在的使用者或群組	儲存貯體	無效的委託人	有效的
資源是一個不存在的 S3 儲存桶	群組	有效的	相同
主體是本機群組	儲存貯體	無效的委託人	有效的
此原則授予非所有者帳戶（包括匿名帳戶）放置物件的權限。	儲存貯體	有效。物件歸建立者帳戶所有，儲存桶原則不適用。建立者帳戶必須使用物件 ACL 授予物件的存取權限。	有效。物件歸儲存桶擁有者帳戶所有。儲存桶原則適用。

一次寫入多次讀取 (WORM) 保護

您可以建立一次寫入多次讀取 (WORM) 儲存桶來保護資料、使用者定義的物件中繼資料和 S3 物件標籤。您可設定 WORM 儲存桶，以允許建立新物件並防止覆寫或刪除現有內容。請使用此處所述的其中一種方法。

為確保始終拒絕覆寫作業，您可以：

- 從 Grid Manager 中，前往 **Configuration > Security > Security settings > Network and objects**，然後選取 **Prevent client modification** 核取方塊。
- 請套用以下規則和 S3 原則：
 - 在 S3 原則中新增 PutOverwriteObject DENY 操作。
 - 在 S3 原則中新增 DeleteObject DENY 操作。
 - 向 S3 原則新增 PutObject ALLOW 操作。



在 S3 原則中將 DeleteObject 設定為 DENY，並不能防止 ILM 在存在「30 天後零份複本」之類的規則時刪除物件。



即使套用了所有這些規則和原則，它們也無法防止並行寫入（請參閱情況 A）。但它們可以防止連續的已完成覆寫（請參閱情況 B）。

情況 A：併發寫入（未採取防護措施）

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

情況 B：連續的完成覆寫（已採取措施防止）

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

相關資訊

- ["StorageGRID ILM 規則如何管理物件"](#)
- ["範例儲存桶原則"](#)
- ["範例群組原則"](#)
- ["工作階段原則範例"](#)
- ["使用 ILM 管理物件"](#)
- ["使用租戶帳戶"](#)

StorageGRID S3 REST API 工作階段原則範例

使用以下範例建立 StorageGRID 工作階段原則。

範例：設定允許物件擷取的工作階段原則

在本例中，工作階段的主體僅被允許從 bucket1 擷取物件。所有其他動作均被隱含拒絕，但 StorageGRID 特有的動作（例如使用 ["s3:PutOverwriteObject"](#) 權限）除外。工作階段原則可以在呼叫 AssumeRole API 時以 JSON 檔案的形式提供。

```
{  
  "Statement": [  
    {  
      "Action": "s3:GetObject",  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::bucket1/*"  
    }  
  ]  
}
```

StorageGRID S3 REST API 儲存區原則範例

使用本節中的範例為儲存桶建立 StorageGRID 存取原則。

儲存桶原則指定該原則所附加的儲存桶的存取權限。您可以透過下列其中一種工具，使用 S3 PutBucketPolicy API 設定儲存桶原則：

- `"${post_edited_translations.segment}"`。
- 使用 AWS CLI 執行以下命令（請參閱["儲存貯體上的作業"](#)）：

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

例如：允許所有人對儲存桶擁有唯讀存取。

在這個例子中，包括匿名使用者在內的所有使用者都可以列出儲存貯體中的物件，並對儲存貯體中的所有物件執行 GetObject 操作。所有其他操作都將被拒絕。請注意，此原則可能並非特別有用，因為除了帳戶 root 使用者之外，其他使用者都沒有寫入儲存貯體的權限。

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

例如：允許一個帳戶中的所有對某個儲存桶擁有完全存取，而允許另一個帳戶中的所有擁有唯讀存取。

在此範例中，一個指定帳戶中的所有都可以完全存取儲存桶，而另一個指定帳戶中的所有只能列出儲存桶，並對儲存桶中以 ``shared/`` 物件金鑰前綴開頭的物件執行 GetObject 操作。



在 StorageGRID 中，非擁有者帳戶（包括匿名帳戶）建立的物件歸儲存桶擁有者帳戶所有。儲存桶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/*"
        }
      }
    }
  ]
}

```

例如：允許所有人對儲存桶擁有唯讀存取，並允許特定群組擁有完全存取

在此範例中，包括匿名使用者在內的所有人都可以列出儲存桶並對儲存桶中的所有物件執行 GetObject 操作，而只有屬於指定帳戶中特定群組 `Marketing` 的使用者才能獲得完整存取權限。

```

{
  "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：允許所有位於 **IP** 位址範圍內的用戶端對儲存桶進行讀取和寫入存取

在這個例子中，所有使用者（包括匿名使用者）都可以列出儲存桶並對儲存桶中的所有物件執行任何物件操作，前提是請求必須來自指定的 IP 位址範圍（54.240.143.0 到 54.240.143.255，但不包括 54.240.143.188）。所有其他操作將遭到拒絕，所有來自 IP 位址範圍之外的請求也將遭到拒絕。

```

{
  "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：僅允許指定的聯合使用者完全存取儲存桶

在此範例中，同盟使用者 Alex 被允許完整存取 examplebucket 貯器及其物件。所有其他使用者（包括「root」）都會被明確拒絕所有作業。但請注意，系統絕不會拒絕「root」對 Put/Get/DeleteBucketPolicy 的權限。

```

{
  "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：PutOverwriteObject 權限

在此範例中，Deny PutOverwriteObject 和 DeleteObject 的 Effect 可確保沒有人能夠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/*"
    }
  ]
}

```

StorageGRID S3 REST API 群組原則範例

使用本節中的範例為群組建置 StorageGRID 存取原則。

群組原則指定該原則所附加群組的存取權限。原則中沒有 Principal 元素，因為它是隱含的。群組原則可使用 Tenant Manager 或 API 進行設定。

範例：使用 **Tenant Manager** 設定群組原則

在 Tenant Manager 中新增或編輯群組時，您可以選擇群組原則來確定該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 存取權限：**預設選項。此群組中的使用者無法存取 S3 資源，除非透過儲存桶原則授予存取權限。如果選擇此選項，預設只有 root 使用者可以存取 S3 資源。
- **唯讀存取：**此群組中的使用者對 S3 資源擁有唯讀存取。例如，此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標籤。選擇此選項後，唯讀群組原則的 JSON 字串將顯示在文字方塊中。您無法編輯此字串。
- **完全存取：**此群組中的使用者擁有對 S3 資源（包括儲存桶）的完全存取權。選取此選項後，文字方塊中將顯示完全存取群組原則的 JSON 字串。您無法編輯此字串。
- **Ransomware Mitigation：**此範例原則適用於此租戶的所有儲存桶。此群組中的使用者可以執行常見操作，但無法從已啟用物件版本控制的儲存桶中永久刪除物件。

擁有「管理所有儲存桶」權限的 Tenant Manager 使用者可以置換此群組原則。將「管理所有儲存桶」權限限制為受信任的用戶端，並在可用時使用多因素驗證（MFA）。

- **自訂：**群組內使用者將獲得您在文字方塊中指定的權限。

範例：允許群組對所有儲存桶擁有完全存取

在本例中，除非儲存桶原則明確拒絕，否則群組的所有成員都可以完全存取租戶帳戶擁有的所有儲存桶。

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

範例：允許群組對所有儲存桶進行唯讀存取

在這個範例中，除非儲存桶原則明確禁止，否則群組中的所有成員都對 S3 資源擁有唯讀存取權限。例如，該群組中的使用者可以列出物件並讀取物件資料、中繼資料和標籤。

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

例如：允許群組成員僅對其在儲存桶中的「資料夾」擁有完全存取

在本例中，群組成員僅可列出及存取指定儲存桶中屬於他們的特定資料夾（鍵前綴）。請注意，在確定這些資料夾的隱私等級時，應考慮其他群組原則和儲存桶原則中的存取權限。

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

StorageGRID 稽核日誌中追蹤的 S3 操作

StorageGRID 服務會產生稽核訊息並儲存在文字日誌檔案中。您可以在稽核日誌中審查 S3 特有的稽核訊息，以取得有關儲存桶和物件操作的詳細資訊。

稽核日誌中追蹤的儲存桶操作

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- PUT Bucket 法規遵循
- PutBucketTagging
- PutBucketVersioning

稽核日誌中追蹤的物件操作

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- SelectObject
- UploadPart (當 ILM 規則使用平衡或嚴格擷取)
- UploadPartCopy (當 ILM 規則使用平衡或嚴格擷取)

相關資訊

- ["存取稽核日誌檔案"](#)
- ["用戶端寫入稽核訊息"](#)
- ["用戶端讀取稽核訊息"](#)

版權資訊

Copyright © 2026 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。