管理存取原則

StorageGRID software

NetApp

July 23, 2026

目錄

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。

元素	說明
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/*"
```

- 您也可以在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	
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	

權限	**S3 REST API** 操作	**StorageGRID** 客製
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	
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

權限	**S3 REST API** 操作	**StorageGRID** 客製
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	
s3:BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging（該物件的特定版本）	

權限	**S3 REST API** 操作	**StorageGRID** 客製
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	
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）	

權限	**S3 REST API** 操作	**StorageGRID** 客製
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）。
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。

條件算子	說明
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不存在。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。

條件鍵	動作	說明
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3：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。
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

條件鍵	動作	說明
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
`${aws:SourceIp}`	使用 SourceIp 金鑰作為提供的變數。

變數	說明
`${aws:username}`	使用使用者名稱鍵作為提供的變數。
`${s3:prefix}`	使用服務專屬前置詞金鑰作為提供的變數。
`${s3:max-keys}`	使用服務專屬的 max-keys 金鑰作為提供的變數。
`${*}`	特殊字元。使用該字元作為字面意義上的 * 字元。
`${?}`	特殊字元。將字元用作文字？字元。
`${$}`	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
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

原則執行摘要	原則類型	**Amazon** 行為	**StorageGRID** 行為
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人對某個儲存桶擁有完全存取，而允許另一個帳戶中的所有人擁有唯讀存取。

在此範例中，一個指定帳戶中的所有人都可以完全存取儲存桶，而另一個指定帳戶中的所有人只能列出儲存桶，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}/*"
    }
  ]
}
```