儲存桶和群組存取策略

StorageGRID software

NetApp
May 29, 2026

目錄

儲存桶和群組存取策略

使用儲存桶和群組存取策略

StorageGRID使用 Amazon Web Services (AWS) 原則語言可讓 S3 租用戶控制對儲存桶及其儲存體桶內物件的存取。 StorageGRID系統實作了 S3 REST API 原則語言的子集。 S3 API 的存取策略以 JSON 編寫。

訪問策略概述

StorageGRID支援兩種存取策略。

- **Bucket** 政策，使用 GetBucketPolicy、PutBucketPolicy 和 DeleteBucketPolicy S3 API 操作或 Tenant Manager 或 Tenant Management API 進行管理。儲存桶策略附加到儲存桶，因此它們配置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的物件的存取。一個儲存桶策略僅適用於一個儲存桶，也可能適用於多個群組。
- 群組原則，使用租用戶管理器或租用戶管理 API 進行設定。群組原則會附加到帳戶中的群組，因此它們配置為允許該群組存取該帳戶擁有的特定資源。群組原則僅適用於一個群組，也可能適用於多個儲存桶。

> 組策略和儲存桶策略之間的優先順序沒有區別。

StorageGRID桶和群組原則遵循 Amazon 定義的特定語法。每個策略內部都有一個策略語句數組，每個語句包含以下元素：

- 語句 ID (Sid)（可選）
- 影響
- 校長/非校長
- 資源/非資源
- 行動/不行動
- 條件（可選）

策略語句使用此結構建構以指定權限：授予<Effect>以允許/拒絕<Principal>在適用<Condition>時對<Resource>執行<Action>。

每個策略元素都有其特定的功能：

元素	描述
席德	Sid 元素是可選的。 Sid 僅供使用者描述。它被儲存但不被StorageGRID系統解釋。
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。

元素	描述
校長/非校長	您可以允許使用者、群組和帳戶存取特定資源並執行特定操作。如果請求中不包含 S3 簽名，則透過指定通配符 (*) 作為主體來允許匿名存取。預設情況下，只有帳戶根可以存取該帳戶擁有的資源。 您只需要在儲存桶策略中指定 Principal 元素。對於群組策略，策略所附加到的群組是隱式的 Principal 元素。
資源/非資源	Resource 元素標識儲存桶和物件。您可以使用 Amazon 資源名稱 (ARN) 來識別資源，從而允許或拒絕對儲存桶和物件的權限。
行動/不行動	Action 和 Effect 元素是權限的兩個組成部分。當一個群組請求資源時，他們要麼被授予存取該資源的權限，要麼被拒絕存取該資源。除非您明確指派權限，否則存取將被拒絕，但您可以使用明確拒絕來覆寫另一個策略授予的權限。
狀態	Condition 元素是可選的。條件允許您建立表達式來確定何時應用策略。

在 Action 元素中，可以使用通配符 (*) 來指定所有動作或部分動作。例如，此 Action 符合 s3:GetObject 、s3:PutObject 和 s3:DeleteObject 等權限。

```
s3:*Object
```

在 Resource 元素中，可以使用通配符 (*) 和 (?)。星號 (*) 符合 0 個或多個字符，而問號 (?) 則匹配任意單一字符。

在 Principal 元素中，不支援通配符，除非設定匿名存取（向所有人授予權限）。例如，您將通配符 (*) 設定為主體值。

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

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

在以下範例中，該語句使用了 Effect、Principal、Action 和 Resource 元素。此範例展示了一個完整的儲存桶策略語句，該語句使用效果「允許」來授予 Principals、管理群組 `federated-group/admin`以及財務集團 `federated-group/finance`，執行操作的權限 `s3:ListBucket`在名為 `mybucket`和行動 `s3:GetObject`在該儲存桶內的所有物件上。

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

儲存桶策略的大小限制為 20,480 字節，群組原則的大小限制為 5,120 位元組。

政策一致性

預設情況下，您對群組原則所做的任何更新最終都是一致的。當群組原則變得一致時，由於策略緩存，變更可能需要額外 15 分鐘才能生效。預設情況下，您對儲存桶策略所做的任何更新都是高度一致的。

根據需要，您可以變更儲存桶策略更新的一致性保證。例如，您可能希望在網站中斷期間變更儲存桶策略。

在這種情況下，您可以設定 `Consistency-Control`PutBucketPolicy 請求中的標頭，或者您可以使用 PUT Bucket 一致性請求。當儲存桶策略變得一致時，由於策略快取，變更可能需要額外 8 秒才能生效。

> 如果您將一致性設為不同的值以解決臨時情況，請確保在完成後將儲存桶層級設定還原為其原始值。否則，所有未來的儲存桶請求都將使用修改後的設定。

在策略聲明中使用 **ARN**

在策略聲明中，ARN 用於 Principal 和 Resource 元素。

- 使用此語法指定 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 (*) 作為通配符來匹配物件鍵內的零個或多個字元。
- 可以在物件鍵中指定的國際字元應使用 JSON UTF-8 或 JSON \u 轉義序列進行編碼。不支援百分比編碼。

  "RFC 2141 URN語法"

  PutBucketPolicy 操作的 HTTP 請求主體必須使用 charset=UTF-8 進行編碼。

在策略中指定資源

在策略語句中，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。

- 每個策略聲明都需要一個資源元素。在策略中，資源由元素表示 `Resource`或者， `NotResource`以進行排除。
- 您可以使用 S3 資源 ARN 指定資源。例如：

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

- 您也可以在物件鍵內使用策略變數。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。

在策略中指定主體

使用 Principal 元素來識別政策聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 儲存桶策略中的每個策略語句都必須包含一個 Principal 元素。群組原則中的策略語句不需要 Principal 元素，因為群組被視為主體。
- 在策略中，主體由元素「Principal」表示，或由「NotPrincipal」表示排除。
- 必須使用 ID 或 ARN 指定基於帳戶的身份：

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

- 本範例使用租用戶帳號 ID 27233906934684427525，其中包括帳號 root 和帳號內的所有使用者：

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

- 您可以僅指定帳戶根：

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

- 您可以指定特定的聯合使用者（「Alex」）：

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

- 您可以指定特定的聯合群組（「管理員」）：

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

- 您可以指定一個匿名主體：

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

- 為了避免歧義，您可以使用使用者 UUID 而不是使用者名稱：

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

  例如，假設 Alex 離開了組織，而用戶名 `Alex`被刪除。如果一個新的 Alex 加入組織並且被分配相同的 `Alex`使用者名，新使用者可能會無意中繼承授予原始使用者的權限。

- 主體值可以指定在建立儲存桶策略時尚不存在的群組/使用者名稱。

在策略中指定權限

在策略中，Action 元素用於允許/拒絕對資源的權限。您可以在策略中指定一組權限，這些權限由元素「Action」表示，或由「NotAction」表示排除。每個元素都對應到特定的 S3 REST API 操作。

表格列出了適用於儲存桶的權限和適用於物件的權限。

> Amazon S3 現在對 PutBucketReplication 和 DeleteBucketReplication 作業使用 s3:PutReplicationConfiguration 權限。 StorageGRID對每個操作使用單獨的權限，這與原始 Amazon S3 規格相符。

> 當使用 put 覆寫現有值時，將執行刪除。

適用於儲存桶的權限

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：創建桶	創建桶	是的。 注意：僅在群組原則中使用。
s3：刪除桶	刪除桶	
s3：刪除儲存桶元資料通知	刪除儲存桶元資料通知配置	是的
s3：刪除儲存桶策略	刪除桶策略	
s3：刪除複製配置	刪除桶複製	是的，PUT 和 DELETE 的權限是分開的
s3：取得儲存桶Acl	獲取BucketAcl	
s3：取得儲存桶合規性	GET Bucket 合規性（已棄用）	是的
s3：取得儲存桶一致性	取得桶一致性	是的
s3：取得儲存桶CORS	獲取BucketCors	
s3:取得加密配置	取得桶加密	
s3：取得儲存桶上次存取時間	取得 Bucket 上次造訪時間	是的
s3：取得儲存桶位置	取得儲存桶位置	
s3：取得儲存桶元資料通知	取得 Bucket 元資料通知配置	是的
s3：取得儲存桶通知	取得儲存桶通知配置	

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：取得儲存桶物件鎖配置	取得物件鎖配置	
s3：取得儲存桶策略	取得BucketPolicy	
s3：取得儲存桶標記	取得桶標記	
s3：取得儲存桶版本	取得Bucket版本	
s3:獲取生命週期配置	取得BucketLifecycleConfiguration	
s3：取得複製配置	獲取Bucket複製	
s3：列出所有我的儲存桶	• 列表桶 • 取得儲存使用情況	是的，用於獲取儲存使用情況。 注意：僅在群組原則中使用。
s3：列表桶	• 清單對象 • 頭桶 • 復原對象	
s3：列出桶多部分上傳	• 列出多部分上傳 • 復原對象	
s3：列出儲存桶版本	取得儲存桶版本	
s3：PutBucket合規性	PUT Bucket 合規性（已棄用）	是的
s3:PutBucket一致性	PUT桶一致性	是的
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3：PutEncryption配置	• 刪除桶加密 • PutBucket加密	
s3:PutBucket上次訪問時間	PUT Bucket 上次訪問時間	是的
s3：PutBucketMetadata通知	PUT Bucket 元資料通知配置	是的

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：PutBucket通知	PutBucketNotification配置	
s3:PutBucketObjectLock配置	• 使用 CreateBucket `x-amz-bucket-object-lock-enabled: true`請求標頭（也需要 s3:CreateBucket 權限） • PutObjectLock配置	
s3：PutBucket策略	PutBucketPolicy	
s3：PutBucket標記	• 刪除儲存桶標記† • PutBucketTagging	
s3：PutBucket版本控制	PutBucket版本控制	
s3：PutLifecycle配置	• DeleteBucketLifecycle† • PutBucket生命週期配置	
s3：Put複製配置	PutBucket複製	是的，PUT 和 DELETE 的權限是分開的

適用於物件的權限

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：中止分段上傳	• 中止分段上傳 • 復原對象	
s3：繞過治理保留	• 刪除對象 • 刪除對象 • PutObjectRetention	
s3：刪除對象	• 刪除對象 • 刪除對象 • 復原對象	
s3：刪除物件標記	刪除物件標記	
s3：刪除物件版本標記	DeleteObjectTagging（物件的特定版本）	

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：刪除物件版本	DeleteObject（物件的特定版本）	
s3：獲取對象	• 取得對象 • 頭部對象 • 復原對象 • 選擇對象內容	
s3:獲取對象Acl	取得對象Acl	
s3：獲取對象合法持有狀態	獲取對象合法持有	
s3：取得對象保留	取得對象保留	
s3:取得物件標記	取得物件標記	
s3:取得物件版本標記	GetObjectTagging（物件的特定版本）	
s3：取得物件版本	GetObject（物件的特定版本）	
s3:列出多部分上傳部分	列出零件，恢復對象	
s3：Put對象	• 放置對象 • 複製對象 • 復原對象 • 建立多部分上傳 • 完成多部分上傳 • 上傳部分 • 上傳部分複製	
s3：PutObjectLegalHold	放置對象合法保留	
s3：PutObjectRetention	PutObjectRetention	
s3：PutObjectTagging	PutObjectTagging	
s3：PutObjectVersionTagging	PutObjectTagging（物件的特定版本）	

權限	**S3 REST API** 操作	為**StorageGRID**定制
s3：PutOverwrite對象	• 放置對象 • 複製對象 • PutObjectTagging • 刪除物件標記 • 完成多部分上傳	是的
s3：恢復對象	復原對象	

使用 **PutOverwriteObject** 權限

s3:PutOverwriteObject 權限是自訂StorageGRID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、使用者定義的元資料或 S3 物件標記。

此權限的可能設定包括：

- 允許：客戶端可以覆蓋物件。這是預設值。
- 拒絕：客戶端無法覆蓋物件。當設定為 Deny 時，PutOverwriteObject 權限的工作方式如下：
  - 如果在同一路徑上找到現有物件：
    - 物件的資料、使用者定義的元資料或 S3 物件標記無法被覆寫。
    - 任何正在進行的攝取操作都將被取消，並傳回錯誤。
    - 如果啟用了 S3 版本控制，則 Deny 設定會阻止 PutObjectTagging 或 DeleteObjectTagging 操作修改物件及其非目前版本的 TagSet。
  - 如果未找到現有對象，則此權限無效。
- 當不存在此權限時，效果與設定「允許」相同。

> 如果目前 S3 策略允許覆蓋，且 PutOverwriteObject 權限設定為 Deny，則用戶端無法覆寫物件的資料、使用者定義的元資料或物件標記。此外，如果選取了「防止用戶端修改」核取方塊（配置 > 安全設定 > 網路和物件），則該設定將覆寫 PutOverwriteObject 權限的設定。

在策略中指定條件

條件定義了政策何時生效。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，每個條件可以包含多個鍵值對。條件區塊使用以下格式：

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

在下列範例中，IpAddress 條件使用 SourceIp 條件鍵。

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

支援的條件運算符

條件運算子分類如下：

- 細繩
- 數位
- 布林值
- IP 位址
- 空值檢查

條件運算符	描述
字串等於	根據精確匹配（區分大小寫）將鍵與字串值進行比較。
字串不等於	根據否定匹配（區分大小寫）將鍵與字串值進行比較。
字串等於忽略大小寫	根據精確匹配（忽略大小寫）將鍵與字串值進行比較。
字串不等於忽略大小寫	根據否定匹配（忽略大小寫）將鍵與字串值進行比較。
StringLike	根據精確匹配（區分大小寫）將鍵與字串值進行比較。可以包含 * 和？通配符。
StringNotLike	根據否定匹配（區分大小寫）將鍵與字串值進行比較。可以包含 * 和？通配符。
數字等於	根據精確匹配將鍵與數值進行比較。
數字不等於	根據否定匹配將鍵與數值進行比較。
數字大於	根據“大於”匹配將鍵與數值進行比較。
數字大於等於	根據“大於或等於”匹配將鍵與數值進行比較。

條件運算符	描述
數字小於	根據“小於”匹配將鍵與數值進行比較。
數字小於等於	根據“小於或等於”匹配將鍵與數值進行比較。
布林值	根據“真或假”匹配將鍵與布林值進行比較。
IP位址	將金鑰與 IP 位址或 IP 位址範圍進行比較。
不存在IP位址	根據否定匹配將鍵與 IP 位址或 IP 位址範圍進行比較。
無效的	檢查目前請求上下文中是否存在條件鍵。

支援的條件鍵

條件鍵	行動	描述
aws:來源IP	IP營運商	將與發送請求的 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網關節點上的負載平衡器服務發送的，這將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，這將與該負載平衡器的 IP 位址進行比較。任何 `X-Forwarded-For`標頭將被忽略，因為無法確定其有效性。
aws:用戶名	資源/身份	將與發送請求的寄件者的使用者名稱進行比較。可用於儲存桶或物件操作。
s3:分隔符	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	行動	描述
s3:ExistingObjectTag/<標籤鍵>	s3：刪除物件標記 s3：刪除物件版本標記 s3：獲取對象 s3:獲取對象Acl 3：取得物件標記 s3：取得物件版本 s3:取得物件版本Acl s3:取得物件版本標記 s3：PutObjectAcl s3：PutObjectTagging s3:PutObjectVersionAcl s3 ：PutObjectVersionTaggi ng	將要求現有物件具有特定的標籤鍵和值。
s3:最大鍵數	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：對象鎖剩餘保留天數	s3：Put對象	與保留至日期中指定的日期進行比較 `x-amz-object-lock-retain-until-date`請求標頭或根據儲存桶預設保留期間計算得出，以確保這些值在以下請求的允許範圍內： • 放置對象 • 複製對象 • 建立多部分上傳
s3：對象鎖剩餘保留天數	s3：PutObjectRetention	與 PutObjectRetention 請求中指定的 retain-until-date 進行比較，以確保其在允許範圍內。
s3:前綴	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。

條件鍵	行動	描述
s3:RequestObjectTag/<標籤鍵>	s3：Put對象 s3：PutObjectTagging s3 ：PutObjectVersionTagging	當物件請求包含標記時，將需要特定的標籤鍵和值。

在策略中指定變數

您可以使用策略中的變數來填入可用的策略資訊。您可以在 `Resource`元素和字串比較中的 `Condition`元素。

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

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

多變的	描述
`${aws:SourceIp}`	使用 SourceIp 鍵作為提供的變數。
`${aws:username}`	使用使用者名稱鍵作為提供的變數。
`${s3:prefix}`	使用特定於服務的前綴鍵作為提供的變數。
`${s3:max-keys}`	使用特定於服務的 max-keys 鍵作為提供的變數。
`${*}`	特殊字元。將該字元用作文字 * 字元。
`${?}`	特殊字元。將該字元用作文字？字元。
`${$}`	特殊字元。將該字元用作文字 $ 字元。

創建需要特殊處理的政策

有時，政策授予的權限可能會對安全性造成危險，或對持續操作造成危險，例如鎖定帳戶的根使用者。StorageGRID S3 REST API 實作在政策驗證期間的限制比 Amazon 少，但在策略評估期間同樣嚴格。

政策說明	策略類型	亞馬遜行為	**StorageGRID**行為
拒絕自己對 root 帳號的任何權限	桶	有效且強制執行，但根用戶帳戶保留所有 S3 儲存桶策略操作的權限	相同的
拒絕任何使用者/群組權限	團體	有效且強制執行	相同的
允許外部帳戶群組任何權限	桶	無效的委託人	有效，但所有 S3 儲存桶策略操作的權限在策略允許的情況下都會傳回 405 方法不允許錯誤
允許外部帳戶root或使用者任何權限	桶	有效，但所有 S3 儲存桶策略操作的權限在策略允許的情況下都會傳回 405 方法不允許錯誤	相同的
允許每個人執行所有操作的權限	桶	有效，但所有 S3 儲存桶策略操作的權限都會為外部帳戶根和使用者傳回 405 方法不允許錯誤	相同的
拒絕所有人執行所有操作的權限	桶	有效且強制執行，但根用戶帳戶保留所有 S3 儲存桶策略操作的權限	相同的
主體是不存在的使用者或群組	桶	無效的委託人	有效的
資源是不存在的 S3 儲存桶	團體	有效的	相同的
校長是當地團體	桶	無效的委託人	有效的
策略授予非所有者帳戶（包括匿名帳戶）放置物件的權限。	桶	有效的。物件歸創建者帳戶所有，且儲存桶策略不適用。創建者帳戶必須使用物件 ACL 授予該物件的存取權限。	有效的。物件歸儲存桶擁有者帳戶所有。儲存桶策略適用。

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、使用者定義的物件元資料和 S3 物件標記。您可以配置 WORM 儲存桶以允許建立新物件並防止覆蓋或刪除現有內容。使用此處描述的方法之一。

為了確保始終拒絕覆蓋，您可以：

- 從網格管理員中，前往 配置 > 安全 > 安全設定 > 網路和物件，然後選擇 *防止客戶端修改*複選框。
- 應用以下規則和 S3 策略：
  - 將 PutOverwriteObject DENY 操作新增至 S3 策略。
  - 在 S3 策略中新增 DeleteObject DENY 操作。
  - 在 S3 策略中新增 PutObject ALLOW 操作。

> 當存在「30 天後零副本」等規則時，在 S3 策略中將 DeleteObject 設為 DENY 並不能阻止 ILM 刪除物件。

> 即使應用了所有這些規則和策略，它們也無法防止並發寫入（請參閱情況 A）。它們確實可以防止連續完成的覆蓋（參見情況 B）。

情況 **A**：併發寫入（未防範）

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

情況 **B**：順序完成覆蓋（防範）

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

相關資訊

- "StorageGRID ILM 規則如何管理對象"
- "儲存桶策略範例"
- "群組原則範例"
- "使用 ILM 管理對象"
- "使用租用戶帳戶"

儲存桶策略範例

使用本節中的範例為儲存桶建立StorageGRID存取策略。

儲存桶策略指定該策略所附加到的儲存桶的存取權限。您可以透過以下工具之一使用 S3 PutBucketPolicy API 設定儲存桶策略：

- "租戶經理" 。
- AWS CLI 使用此命令（請參閱"對 bucket 的操作"):

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

範例：允許每個人對儲存桶進行唯讀訪問

在這個例子中，允許所有人（包括匿名使用者）列出儲存桶中的對象，並對儲存桶中的所有物件執行 GetObject 操作。所有其他操作都將被拒絕。請注意，此策略可能不是特別有用，因為除了帳戶根之外沒有人有權限寫入儲存桶。

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

範例：允許一個帳戶中的每個人對儲存桶進行完全訪問，並允許另一個帳戶中的每個人對儲存桶進行唯讀訪問

在此範例中，一個指定帳戶中的每個人都被允許完全存取儲存桶，而另一個指定帳戶中的每個人只被允許列出儲存桶並對儲存桶中以 開頭的物件執行 GetObject 操作 `shared/`物件鍵前綴。

> 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。儲存桶策略適用於這些物件。

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

範例：允許每個人對儲存桶進行唯讀訪問，並允許指定群組進行完全訪問

在這個例子中，包括匿名用戶在內的每個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，而只有屬於該群組的用戶 `Marketing`指定帳戶中的使用者可以獲得完全存取權限。

```
{
  "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：如果客戶端在 IP 範圍內，則允許每個人對儲存桶進行讀寫訪問

在此範例中，允許所有人（包括匿名使用者）列出儲存桶並對儲存桶中的所有物件執行任何物件操作，前提是請求來自指定的 IP 範圍（54.240.143.0 到 54.240.143.255，54.240.143.188 除外）。所有其他操作都將被拒絕，並且所有超出 IP 範圍的請求都將被拒絕。

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

範例：允許指定聯合用戶獨佔存取儲存桶的完全權限

在此範例中，聯合用戶 Alex 被允許完全訪問 `examplebucket`bucket 及其物件。所有其他使用者（包括“root”）均被明確拒絕所有操作。但請注意，「root」永遠不會被拒絕 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

在這個例子中， `Deny` PutOverwriteObject 和 DeleteObject 的效果可確保沒有人可以覆寫或刪除物件的資料、使用者定義的元資料和 S3 物件標記。

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

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

群組原則範例

使用本節中的範例為群組建置StorageGRID存取策略。

群組原則指定該策略所屬群組的存取權限。沒有 `Principal`元素，因為它是隱含的。群組原則是使用租用戶管理器或 API 進行設定的。

範例：使用租用戶管理器設定群組原則

當您在租用戶管理員中新增或編輯群組時，您可以選擇一個群組原則來確定該群組的成員將擁有哪些 S3 存取

權。看"為 S3 租用戶建立群組" 。

- 無 **S3** 存取：預設選項。除非透過儲存桶策略授予存取權限，否則該群組中的使用者無權存取 S3 資源。如果選擇此選項，則預設只有 root 使用者才有權存取 S3 資源。
- 唯讀存取：此群組中的使用者對 S3 資源具有唯讀存取權限。例如，該群組中的使用者可以列出物件並讀取物件資料、元資料和標籤。選擇此選項時，唯讀群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。
- 完全存取：此群組中的使用者對 S3 資源（包括儲存桶）擁有完全存取權。當您選擇此選項時，完全存取群組原則的 JSON 字串將出現在文字方塊中。您無法編輯此字串。
- 勒索軟體緩解：此範例策略適用於此租戶的所有儲存桶。該群組中的使用者可以執行常見操作，但無法從啟用了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租用戶管理員使用者可以覆寫此群組原則。將管理所有儲存桶的權限限制為受信任的用戶，並在可用的情況下使用多重身份驗證 (MFA)。

- 自訂：群組中的使用者被授予您在文字方塊中指定的權限。

範例：允許群組完全存取所有儲存桶

在此範例中，除非儲存桶策略明確拒絕，否則群組中的所有成員都被允許完全存取租用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訪問

在此範例中，群組中的所有成員都具有對 S3 資源的唯讀存取權限，除非儲存桶策略明確拒絕。例如，該群組中的使用者可以列出物件並讀取物件資料、元資料和標籤。

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

範例：允許群組成員僅完全存取儲存桶中的“資料夾”

在此範例中，群組成員只被允許列出和存取指定儲存桶中的特定資料夾（鍵前綴）。請注意，在確定這些資料夾的隱私時，應考慮來自其他群組原則和儲存桶策略的存取權限。

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