儲存庫和群組存取原則

StorageGRID 11.8

NetApp
March 19, 2024

目錄

儲存庫和群組存取原則

使用貯體和群組存取原則

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

存取原則總覽

支援的存取原則有兩種。StorageGRID

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

群組原則和儲存庫原則之間的優先順序沒有差異。

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

- 對帳單ID（Sid）（選用）
- 效果
- 委託人/未委託人
- 資源/未資源
- 行動/未行動
- 條件（選用）

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

每個原則元素都用於特定功能：

元素	說明
SID	Sid元素為選用項目。Sid僅供使用者說明使用。它會儲存、但StorageGRID 不會被作業系統解讀。
效果	使用effect元素來確定是否允許或拒絕指定的作業。您必須使用支援的Action元素關鍵字、識別您允許（或拒絕）的貯體或物件作業。

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

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

```
s3:*Object
```

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

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

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

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

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

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

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

原則的一致性

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

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

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

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

在原則聲明中使用**ARN**

在原則聲明中、ARN用於主要和資源元素。

- 使用此語法來指定S3資源ARN：

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

- 使用此語法來指定身分識別資源ARN（使用者和群組）：

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

其他考量事項：

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

  "RFC 2141 URN語法"

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

在原則中指定資源

在原則聲明中、您可以使用資源元素來指定允許或拒絕權限的儲存區或物件。

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

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

- 您也可以在物件機碼內使用原則變數。例如：

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

- 資源值可以指定在建立群組原則時尚未存在的儲存區。

在原則中指定主體

使用主體元素來識別原則聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

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

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

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

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

- 您只能指定帳戶根目錄：

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

- 您可以指定特定的聯盟使用者（「Alex」）：

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

- 您可以指定特定的聯盟群組（「經理」）：

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

- 您可以指定匿名主體：

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

- 為了避免混淆、您可以使用使用者UUID、而非使用者名稱：

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

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

- 主要值可以指定建立儲存區原則時尚未存在的群組/使用者名稱。

在原則中指定權限

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

這些表格列出套用至儲存區的權限、以及套用至物件的權限。

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

使用 Put 覆寫現有值時會執行刪除。

套用至貯體的權限

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

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3：GetBucketPolicy	GetBucketPolicy	
S3：GetBucketting	GetBucketTagging	
S3：GetBucketVersion	GetBucketVersion	
S3：Get生命 週期組態	GetBucketLifecycleConfiguration	
S3：GetReplicationConfiguration	GetBucketReplication	
S3：ListAllMyb桶	• 列表桶 • 取得儲存使用量	是的、用於取得儲存使用量。 • 附註 * ：僅用於群組原則。
S3：清單庫	• 清單物件 • 標題庫 • RestoreObject	
S3：listBucketMultiPartUploads	• ListMultipartUploads • RestoreObject	
S3：listBucketVerions	取得Bucket版本	
S3：PuttBucketCompliance	符合資源桶規範（已過時）	是的
S3：PuttBucketConsistency	實現庫位一致性	是的
S3：PuttBucketCORS	• 刪除 BucketCors † • PuttBucketCors	
S3：PuttEncryptionConfiguration	• 刪除 BucketEncryption • PuttBucketEncryption	
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：PuttBucketNotification	PutBucketNotificationConfiguration	
S3：PuttBucketObjectLockConfiguration	• 與一起使用的 CreateBucket `x-amz-bucket-object-lock-enabled: true` 要求標頭（也需要S3：建立桶權限） • PutObjectLockConfiguration	
S3：PuttBucketPolicy	PuttBucketPolicy	
S3：PuttBucketting	• 刪除標籤† • PuttBucketTagging	
S3：PuttBucketVersion	PuttBucketVersion	
S3：Putt升降 器組態	• 刪除 BucketLifecycle † • PuttBucketLifecycleConfiguration	
S3：PuttReplicationConfiguration	PutBucketReplication	是、請分別授予和刪除權限

套用至物件的權限

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：中止多重角色上傳	• AbortMultiPart上 傳 • RestoreObject	
S3：BypassGovernanceRetention	• 刪除物件 • 刪除物件 • PutObjectRetention	
S3：刪除物件	• 刪除物件 • 刪除物件 • RestoreObject	
S3：刪除ObjectTagging	刪除ObjectTagging	
S3：刪除ObjectVersion標記	刪除物件標籤（物件的特定版本）	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：刪除ObjectVersion	DeleteObject （物件的特定版本）	
S3：GetObject	• GetObject • 標題物件 • RestoreObject • 選取物件內容	
S3：GetObjectAcl	GetObjectAcl	
S3：GetObjectLegalHold	GetObjectLegalHold	
S3：GetObjectRetention	GetObjectRetention	
S3：GetObjectTagging	GetObjectTagging	
S3：GetObjectVersion標記	GetObjectTagging(物件的特定版本)	
S3：GetObjectVersion	GetObject （物件的特定版本）	
S3：列出多個零件上傳零件	ListParts 、 RestoreObject	
S3：PuttObject	• PuttObject • CopyObject • RestoreObject • 建立多個部分上傳 • 完成多個部分上傳 • 上傳零件 • 上傳PartCopy	
S3：PuttObjectLegalHold	PutObjectLegalHold	
S3：PuttObjectRetention	PutObjectRetention	
S3：PuttObjectTagging	PuttObjectTagging	
S3：PuttObjectVersion標記	PutObjectTagging(物件的特定版本)	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：PuttOverwriteObject	• PuttObject • CopyObject • PuttObjectTagging • 刪除ObjectTagging • 完成多個部分上傳	是的
S3：恢復物件	RestoreObject	

使用**PuttOverwriteObject**權限

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

此權限的可能設定包括：

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

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

在原則中指定條件

條件會定義原則的生效時間。條件包括運算子和金鑰值配對。

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

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

在下列範例中、ipAddress條件使用SourceIp條件金鑰。

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

支援的條件運算子

條件運算子的分類如下：

- 字串
- 數字
- 布林值
- IP 位址
- null檢查

條件運算子	說明
擷取等量資料	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。
擷取NotEquals	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。
StringEqualsIgnoreCase	根據完全相符的結果（忽略大小寫）、將金鑰與字串值進行比較。
StringNotEqualsIgnoreCase	根據否定比對（忽略大小寫）、將金鑰與字串值進行比較。
StringLike	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
StringNotLike	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。可以包括*和？萬用字元。
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。

條件運算子	說明
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據 "TRUE 或 FALSE" 比對、將金鑰與布林值進行比較。
IP地址	比較金鑰與IP位址或IP位址範圍。
NotIppAddress	根據已否定的比對、將金鑰與IP位址或IP位址範圍進行比較。
null	檢查條件金鑰是否存在於目前的要求內容中。

支援的條件金鑰

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

條件金鑰	行動	說明
S3 ： <tag-key>	S3：刪除ObjectTagging S3：刪除ObjectVersion標記 S3：GetObject S3：GetObjectAcl 3 ： GetObjectTagging S3：GetObjectVersion S3：GetObjectVerionAcl S3：GetObjectVersion標記 S3 ： PutObjectAcl S3：PuttObjectTagging S3 ： PutObjectVersionAcl S3：PuttObjectVersion標記	需要現有物件具有特定的標記金鑰和值。
S3：金鑰上限	S3：清單儲存庫和 S3：listBucketVerions權限	將與 ListObjects 或 ListObjectVerions 要求中指定的 max-keys 參數進行比較。
S3：物件鎖定剩餘保留天數	S3：PuttObject	與中指定的保留截止日期比較 `x-amz-object-lock-retain-until-date` 要求標頭或從貯體預設保留期間計算、以確保這些值在下列要求的允許範圍內： • PuttObject • CopyObject • 建立多個部分上傳
S3：物件鎖定剩餘保留天數	S3：PuttObjectRetention	與 PutObjectRetention 要求中指定的保留截止日期進行比較、以確保其在允許範圍內。

條件金鑰	行動	說明
S3：前置碼	S3：清單儲存庫和 S3：listBucketVerions權限	將與 ListObjects 或 ListObjectVerions 要求中指定的前置參數進行比較。
<tag-key>	S3：PuttObject S3：PuttObjectTagging S3：PuttObjectVersion標記	當物件要求包含標記時、需要特定的標記金鑰和值。

在原則中指定變數

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

在此範例中、變數 `${aws:username}` 是資源元素的一部分：

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

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

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

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

變動	說明
`${?}`	特殊字元。使用字元做為字型？字元。
`${$}`	特殊字元。使用字元做為文字$字元。

建立需要特殊處理的原則

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

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕root帳戶的任何權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
拒絕對使用者/群組擁有任何權限	群組	有效且強制	相同
允許外部帳戶群組擁有任何權限	鏟斗	無效的主體	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤
允許外部帳戶root或使用者擁有任何權限	鏟斗	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤	相同
允許每個人都有權執行所有動作	鏟斗	有效、但所有S3儲存區原則作業的權限都會傳回異帳戶根目錄和使用者不允許的「405方法」錯誤	相同
拒絕所有人對所有動作的權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
主體是不存在的使用者或群組	鏟斗	無效的主體	有效
資源是不存在的S3儲存區	群組	有效	相同
主體是本機群組	鏟斗	無效的主體	有效

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
原則會授與非擁有者帳戶（包括匿名帳戶）權限、以放置物件。	鏟斗	有效。物件由建立者帳戶擁有、且庫位原則不適用。建立者帳戶必須使用物件ACL來授與物件的存取權限。	有效。物件由庫位擁有者帳戶擁有。適用庫位政策。

一次寫入多讀（**WORM**）保護

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

為了確保覆寫永遠被拒絕、您可以：

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

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

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

情況**A**：並行寫入（不受保護）

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

情況**B**：連續完成覆寫（防範）

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

相關資訊

- "如何利用ILM規則來管理物件StorageGRID"
- "貯體原則範例"
- "群組原則範例"

- "使用ILM管理物件"
- "使用租戶帳戶"

貯體原則範例

使用本節中的範例、為貯體建立 StorageGRID 存取原則。

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

根據下列命令、可使用AWS CLI設定儲存區原則：

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

範例：允許每個人只讀存取儲存區

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

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

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

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

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

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

範例：允許每個人只讀存取儲存區、並由指定群組進行完整存取

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

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

範例：如果用戶端位於IP範圍、則允許每個人讀取及寫入儲存區的存取權

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

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

範例：允許特定同盟使用者專屬完整存取儲存區

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

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

範例：**PuttOverwriteObject**權限

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

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

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

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

群組原則範例

使用本節中的範例、為群組建置 StorageGRID 存取原則。

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

範例：使用租戶管理程式設定群組原則

當您在租戶管理器中新增或編輯群組時、可以選取群組原則、以判斷此群組成員將擁有哪些 S3 存取權限。請參

閱 "為S3租戶建立群組"。

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

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

- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。

範例：允許群組完整存取所有儲存區

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

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

範例：允許群組唯讀存取所有儲存區

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

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

範例：允許群組成員完全存取儲存庫中的「資料夾」

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

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

版權資訊

商標資訊