使用S3 REST API

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-115/s3/changes-to-s3-rest-api-support.html on April 11, 2024. Always check docs.netapp.com for the latest.

目錄

使用S3

瞭解用戶端應用程式如何使用S3 API與StorageGRID 支援系統進行介面。

- "支援S3 REST API"
- "設定租戶帳戶和連線"
- "如何實作S3 REST API StorageGRID"
- "S3 REST API支援的作業和限制"
- "支援SS3 REST API作業StorageGRID"
- "儲存庫和群組存取原則"
- "設定REST API的安全性"
- "監控與稽核作業"
- "作用中、閒置及並行HTTP連線的優點"

支援S3 REST API

支援簡單儲存服務（S3）API、此API是以代表狀態傳輸（REST）網路服務的形式實作。StorageGRID支援S3 REST API、可讓您將專為S3網路服務開發的服務導向應用程式、連接到使用StorageGRID 該系統的內部部署物件儲存設備。這需要將用戶端應用程式目前使用S3 REST API呼叫的變更降至最低。

- "S3 REST API支援變更"
- "支援的版本"
- "支援StorageGRID 支援功能"

S3 REST API支援變更

您應該注意StorageGRID 到支援S3 REST API的功能有所變更。

版本	註解
11.5	• 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • 。 `Content-MD5` 現在已正確支援要求標頭。

版本	註解
11.4	• 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 新增了對上的儲存區通知的支援 `s3:ObjectRestore:Post` 事件類型。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增對TLS 1.3的支援、以及支援的TLS加密套件更新清單。 • CLB服務已過時。
11.3	• 新增支援使用客戶提供的金鑰（SSE-C）進行物件資料的伺服器端加密。 • 新增刪除、取得及置放資源庫生命週期作業（僅限到期行動）和的支援 `x-amz-expiration` 回應標頭： • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 更新支援的TLS加密套件清單。不再支援TLS 1.1密碼。
11.2	新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。 *附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID （包括用於自訂的版本功能）並未變更。
11.1.	新增跨來源資源共享（CORS）支援、S3用戶端連線至網格節點的HTTP、以及儲存區的法規遵循設定。
11.0	新增支援、可設定適用於儲存區的平台服務（CloudMirror複寫、通知及Elasticsearch整合）。此外、也新增了對儲存區物件標記位置限制的支援、以及可用的一致性控制設定。

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

支援的版本

支援下列S3和HTTP的特定版本。StorageGRID

項目	版本
S3規格	*Simple Storage Service API*參考資料 2006年3月1日
HTTP	1.1 如需HTTP的詳細資訊、請參閱HTTP / 1.1（RFC 7230-35）。 附註 StorageGRID ：不支援HTTP / 1.1鋪管。

相關資訊

"IETF RFC 2616：超文字傳輸傳輸協定（HTTP / 1.1）"

"Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"

支援**StorageGRID** 支援功能

透過支援此平台的服務、非重租戶帳戶可利用遠端S3儲存區、簡易通知服務（SNS）端點或彈性搜尋叢集等外部服務來擴充網格所提供的服務。StorageGRID StorageGRID

下表摘要說明可用的平台服務和用來設定的S3 API。

平台服務	目的	用來設定服務的**S3 API**
CloudMirror複寫	將物件從來源StorageGRID 的靜止庫複寫到設定的遠端S3庫位。	放入資源桶複寫
通知	將來源StorageGRID 資訊庫中的事件通知傳送至設定的簡易通知服務（SNS）端點。	放置時段通知
搜尋整合	將StorageGRID 儲存在物件庫的物件中繼資料傳送至已設定的彈性搜尋索引。	放置時段中繼資料通知 *附註：*這是StorageGRID 一套由人自訂的S3 API。

網格管理員必須先啟用租戶帳戶的平台服務、才能使用這些服務。然後、租戶管理員必須在租戶帳戶中建立代表遠端服務的端點。必須先執行此步驟、才能設定服務。

使用平台服務的建議

在使用平台服務之前、您必須瞭解下列建議：

- NetApp建議您允許不超過100個主動租戶、且S3要求需要CloudMirror複寫、通知及搜尋整合。擁有超過100個作用中租戶可能會導致S3用戶端效能變慢。
- 如果StorageGRID系統中的S3儲存區同時啟用版本管理和CloudMirror複寫、則NetApp建議目的地端點也啟用S3儲存區版本管理。這可讓CloudMirror複寫在端點上產生類似的物件版本。
- 如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。
- 如果目的地儲存區已啟用舊版法規遵循、CloudMirror複寫將會失敗並顯示「AccessDenied」錯誤。

相關資訊

"使用租戶帳戶"

"管理StorageGRID"

"在貯體上作業"

"放置時段中繼資料通知組態要求"

設定租戶帳戶和連線

若要設定StorageGRID 從用戶端應用程式接受連線、需要建立一或多個租戶帳戶並設定連線。

建立及設定**S3**租戶帳戶

S3 API用戶端必須先有S3租戶帳戶、才能將物件儲存及擷取StorageGRID 到支援區。每個租戶帳戶都有自己的帳戶ID、群組和使用者、以及容器和物件。

S3租戶帳戶是StorageGRID 由使用Grid Manager或Grid Management API的資訊網管理員所建立。建立S3租戶

帳戶時、網格管理員會指定下列資訊：

- 租戶的顯示名稱（租戶的帳戶ID會自動指派、無法變更）。
- 租戶帳戶是否允許使用平台服務。如果允許使用平台服務、則必須設定網格以支援其使用。
- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。
- 如果啟用StorageGRID 身分識別聯盟以供支援整個系統、則哪個聯盟群組具有root存取權限可設定租戶帳戶。
- 如果StorageGRID 不使用單一登入（SSO）進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機root使用者的初始密碼。

建立S3租戶帳戶之後、租戶使用者就能存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、並建立本機群組和使用者
- 管理S3存取金鑰
- 建立及管理S3儲存區、包括已啟用S3物件鎖定的儲存區
- 使用平台服務（若已啟用）
- 監控儲存使用量

> S3租戶使用者可以使用租戶管理程式來建立和管理S3儲存區、但必須擁有S3存取金鑰、並使用S3 REST API來擷取和管理物件。

相關資訊

"管理StorageGRID"

"使用租戶帳戶"

如何設定用戶端連線

網格管理員會做出組態選擇、影響S3用戶端連線StorageGRID 至以儲存及擷取資料的方式。建立連線所需的特定資訊取決於所選的組態。

用戶端應用程式可連線至下列任一項目、以儲存或擷取物件：

- 管理節點或閘道節點上的負載平衡器服務、或是管理節點或閘道節點之高可用度（HA）群組的虛擬IP位址（可選）
- 閘道節點上的CLB服務、或是閘道節點高可用度群組的虛擬IP位址（可選）

> CLB服務已過時。在發佈版推出之前設定的用戶端StorageGRID 、可以繼續在閘道節點上使用CLB服務。所有其他仰賴StorageGRID 以提供負載平衡的用戶端應用程式、都應該使用負載平衡器服務進行連線。

- 儲存節點、無論是否有外部負載平衡器

設定StorageGRID 功能時、網格管理員可以使用Grid Manager或Grid Management API來執行下列步驟、這些步驟都是選用的：

1. 設定負載平衡器服務的端點。

   您必須設定端點以使用負載平衡器服務。管理節點或閘道節點上的負載平衡器服務會將傳入的網路連線從用戶端應用程式分散到儲存節點。建立負載平衡器端點時StorageGRID 、系統管理員會指定連接埠號碼、端點是否接受HTTP或HTTPS連線、使用端點的用戶端類型（S3或Swift）、以及用於HTTPS連線的憑證（若適用）。

2. 設定不受信任的用戶端網路。

   如果StorageGRID 某個節點的用戶端網路設定為不受信任、則該節點僅接受用戶端網路上明確設定為負載平衡器端點之連接埠的傳入連線。

3. 設定高可用度群組。

   如果系統管理員建立HA群組、則多個管理節點或閘道節點的網路介面會置於主動備份組態中。用戶端連線是使用HA群組的虛擬IP位址進行。

如需每個選項的詳細資訊、請參閱《關於管理StorageGRID 功能的說明》。

相關資訊

"管理StorageGRID"

摘要：用於用戶端連線的**IP**位址和連接埠

用戶端應用程式StorageGRID 會使用網格節點的IP位址和該節點上服務的連接埠號碼來連線至功能區。如果已設定高可用度（HA）群組、用戶端應用程式就可以使用HA群組的虛擬IP位址進行連線。

建立用戶端連線所需的資訊

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如StorageGRID 需更多資訊、請聯絡您的管理員、或參閱《管理StorageGRID 》的說明、以瞭解如何在Grid Manager中找到這些資訊。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA群組	負載平衡器	HA群組的虛擬IP位址	• 負載平衡器端點連接埠
HA群組	CLB *附註： CLB服務已過時。	HA群組的虛擬IP位址	預設S3連接埠： • HTTPS：8082 • HTTP：8084
管理節點	負載平衡器	管理節點的IP位址	• 負載平衡器端點連接埠
閘道節點	負載平衡器	閘道節點的IP位址	• 負載平衡器端點連接埠

連線位置	用戶端連線的服務	IP 位址	連接埠
閘道節點	CLB *附註： CLB服務已過時。	閘道節點的IP位址 **附註：*根據預設、不會啟用CLB和LDR的HTTP連接埠。	預設S3連接埠： • HTTPS：8082 • HTTP：8084
儲存節點	LdR	儲存節點的IP位址	預設S3連接埠： • HTTPS：18082 • HTTP：18084

範例

若要將S3用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- `https://VIP-of-HA-group:_LB-endpoint-port_`

例如、如果HA群組的虛擬IP位址為192.0.2.5、而S3負載平衡器端點的連接埠號碼為10443、則S3用戶端可以使用下列URL連線StorageGRID 到SESH:

- `https://192.0.2.5:10443`

您可以為用戶端用來連線StorageGRID 到靜態的IP位址設定DNS名稱。請聯絡您的本機網路管理員。

相關資訊

"管理StorageGRID"

決定使用**HTTPS**或**HTTP**連線

使用負載平衡器端點進行用戶端連線時、必須使用為該端點指定的傳輸協定（HTTP或HTTPS）來建立連線。若要在用戶端連線至儲存節點或閘道節點上的CLB服務時使用HTTP、您必須啟用它的使用。

根據預設、當用戶端應用程式連線至閘道節點上的儲存節點或CLB服務時、它們必須使用加密的HTTPS進行所有連線。或者、您也可以選取「Grid Manager（網格管理器）」中的*「Enable HTTP Connection* Grid（啟用HTTP連線*網格）」選項、來啟用較不安全的HTTP連線。例如、用戶端應用程式在非正式作業環境中測試與儲存節點的連線時、可能會使用HTTP。

啟用正式作業網格的HTTP時請務必小心、因為要求會以不加密的方式傳送。

CLB服務已過時。

如果選取*「啟用HTTP連線*」選項、則用戶端的HTTP連接埠必須與HTTPS使用的連接埠不同。請參閱「管理StorageGRID 功能」的說明。

相關資訊

"管理StorageGRID"

"作用中、閒置及並行HTTP連線的優點"

S3要求的端點網域名稱

在用戶端要求使用S3網域名稱之前、StorageGRID 管理員必須先將系統設定為接受在S3路徑樣式和S3虛擬託管樣式要求中使用S3網域名稱的連線。

關於這項工作

若要使用S3虛擬託管樣式要求、網格管理員必須執行下列工作：

- 使用Grid Manager將S3端點網域名稱新增StorageGRID 至整個系統。
- 請確認用戶端用於HTTPS連線StorageGRID 的驗證書已針對用戶端所需的所有網域名稱簽署。

  例如、如果端點是 `s3.company.com`、網格管理員必須確保用於HTTPS連線的憑證包含 `s3.company.com` 端點和端點的萬用字元主體替代名稱（SAN）： `*.s3.company.com`。

- 設定用戶端使用的DNS伺服器、以納入符合端點網域名稱的DNS記錄、包括任何必要的萬用字元記錄。

如果用戶端使用負載平衡器服務連線、則網格管理員設定的憑證是用戶端使用的負載平衡器端點的憑證。

每個負載平衡器端點都有自己的憑證、而且每個端點都可設定為辨識不同的端點網域名稱。

如果用戶端連接儲存節點或閘道節點上的CLB服務、則網格管理員設定的憑證是用於網格的單一自訂伺服器憑證。

CLB服務已過時。

如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

完成這些步驟之後、您就可以使用虛擬託管樣式的要求（例如、 `bucket.s3.company.com`）。

相關資訊

"管理StorageGRID"

"設定REST API的安全性"

測試S3 REST API組態

您可以使用Amazon Web Services命令列介面（AWS CLI）來測試您與系統的連線、並確認您可以讀取物件並將物件寫入系統。

您需要的產品

- 您必須從下載並安裝AWS CLI "aws.amazon.com/cli"。
- 您必須已在StorageGRID The S目的地 系統中建立S3租戶帳戶。

步驟

1. 設定Amazon Web Services設定、以使用StorageGRID 您在該系統中建立的帳戶：
   a. 進入組態模式： `aws configure`

b. 輸入您所建立帳戶的AWS存取金鑰ID。

c. 輸入您所建立帳戶的AWS秘密存取金鑰。

d. 輸入要使用的預設區域、例如us-east-1。

e. 輸入要使用的預設輸出格式、或按* Enter *選取Json。

2. 建立儲存庫。

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

如果成功建立了儲存區、則會傳回儲存區的位置、如下列範例所示：

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

3. 上傳物件。

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

如果物件上傳成功、則會傳回Etag、這是物件資料的雜湊。

4. 列出儲存區的內容、以驗證物件是否已上傳。

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

5. 刪除物件。

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

6. 刪除儲存庫。

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

如何實作S3 REST API StorageGRID

用戶端應用程式可以使用S3 REST API呼叫來連線StorageGRID 至以建立、刪除和修改儲

存區、以及儲存和擷取物件。

- "衝突的用戶端要求"
- "一致性控管"
- "如何利用ILM規則來管理物件StorageGRID"
- "物件版本管理"
- "實作S3 REST API的建議"

衝突的用戶端要求

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

「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。

一致性控管

一致性控制可讓您在物件的可用度與不同儲存節點和站台之間的物件一致性之間（視應用程式需求而定）達成平衡。

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

如果您想要在不同的一致性層級執行物件作業、可以為每個儲存區或每個API作業指定一致性控制。

一致性控管

一致性控制項會影響StorageGRID 到物件所用的中繼資料如何在節點之間分佈、進而影響物件對用戶端要求的可用度。

您可以將桶或API作業的一致性控制設定為下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。

一致性控制	說明
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。符合Amazon S3一致性保證。 *附註：*如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請將一致性控制設為「可用」、除非您需要類似Amazon S3的一致性保證。
可用的（最終的頭端作業一致性）	其行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供一致的執行方式。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。不同於Amazon S3一致性保證、僅適用於頭端作業。

使用「全新寫入後的準備」和「可用」一致性控制

當執行者或Get作業使用「全新寫入後的讀取」一致性控制或Get作業時、StorageGRID 若使用「可用」一致性控制、則由下列多個步驟執行查詢：

- 它會先使用低一致性來查詢物件。
- 如果該查詢失敗、它會在次一一致性層級重複查詢、直到達到最高一致性層級「all」、這需要所有物件中繼資料複本都可用。

如果執行者或Get作業使用「全新寫入後的讀取」一致性控制、但物件不存在、則物件查詢將永遠達到「ALL」一致性層級。由於此一致性層級需要所有物件中繼資料複本都可供使用、因此如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。

除非您需要類似Amazon S3的一致性保證、否則您可以將一致性控制設定為「可用」、以避免發生上述錯誤。當營運者使用「可用」一致性控制時StorageGRID 、僅提供最終一致性。它不會重試失敗的作業、直到達到「all」一致性層級為止、因此不需要所有的物件中繼資料複本都可用。

指定**API**作業的一致性控制

若要設定個別API作業的一致性控制、作業必須支援一致性控制、而且您必須在要求標頭中指定一致性控制。此範例將Get物件作業的一致性控制設為「站台」。

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

您必須對「放置物件」和「取得物件」作業使用相同的一致性控制。

指定桶的一致性控制

若要設定桶的一致性控制、您可以使用StorageGRID 「用作桶」一致性要求和「取得桶」一致性要求。您也可以使用租戶管理程式或租戶管理API。

設定桶的一致性控制時、請注意下列事項：

- 設定區段的一致性控制可決定哪些一致性控制用於在區段或區段組態中的物件上執行S3作業。它不會影響儲存庫本身的作業。
- 個別API作業的一致性控制會覆寫貯體的一致性控制。
- 一般而言、儲存貯體應該使用預設的一致性控制：「全新寫入後的讀取」。 如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、將用戶端設定為針對每個API要求指定一致性控制。只能將貯體層級的一致性控制設定為最後的方法。

一致性控制與**ILM**規則如何互動、以影響資料保護

您選擇的一致性控制和ILM規則都會影響物件的保護方式。這些設定可以互動。

例如、儲存物件時所使用的一致性控制項會影響物件中繼資料的初始放置位置、而針對ILM規則所選取的擷取行為則會影響物件複本的初始放置位置。由於支援對象的中繼資料及其資料、因此需要同時存取才能滿足用戶端要求、因此針對一致性層級和擷取行為選擇相符的保護層級、可提供更好的初始資料保護、並提供更可預測的系統回應。StorageGRID

下列擷取行為適用於ILM規則：

- 嚴格：ILM規則中指定的所有複本都必須在成功傳回用戶端之前完成。
- 平衡：StorageGRID 在擷取時、會嘗試製作ILM規則中指定的所有複本；如果不可能、則會製作過渡複本、並將成功傳回給用戶端。ILM規則中指定的複本會盡可能製作。
- 雙重承諾：StorageGRID 此物件立即製作過渡複本、並讓用戶端恢復成功。在ILM規則中指定的複本會盡可能製作。

> 在選擇ILM規則的擷取行為之前、請先閱讀資訊生命週期管理物件管理說明中有關這些設定的完整說明。

一致性控制和**ILM**規則如何互動的範例

假設您有一個雙站台網格、其中包含下列ILM規則和下列一致性層級設定：

- * ILM規則*：建立兩個物件複本、一個在本機站台、一個在遠端站台。選取嚴格的擷取行為。
- 一致性層級：「'trong-globat'（物件中繼資料會立即發佈至所有站台）。

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

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

如果您改用相同的ILM規則和「站台」一致性層級、用戶端可能會在物件資料複寫到遠端站台之後、收到成功訊息、但物件中繼資料才會散佈到該站台。在此情況下、物件中繼資料的保護層級與物件資料的保護層級不符。如果在擷取後不久本機站台便會遺失、則物件中繼資料將會遺失。無法擷取物件。

一致性層級與ILM規則之間的相互關係可能相當複雜。如需協助、請聯絡NetApp。

相關資訊

"使用ILM管理物件"

"取得時段一致性要求"

"置入時段一致性要求"

如何利用**ILM**規則來管理物件**StorageGRID**

網格管理員會建立資訊生命週期管理（ILM）規則、以管理StorageGRID 從S3 REST API用戶端應用程式擷取到整個系統的物件資料。然後將這些規則新增至ILM原則、以決定物件資料的儲存方式和位置。

ILM設定決定物件的下列層面：

- 地理

  物件資料的位置、無論是StorageGRID 在更新系統（儲存資源池）或雲端儲存資源池中。

- 儲存等級

  用於儲存物件資料的儲存類型：例如Flash或旋轉式磁碟。

- 損失保護

  製作了多少份複本、以及建立的複本類型：複寫、銷毀編碼或兩者。

- 保留

  物件資料的管理方式、儲存位置、以及保護資料不受遺失的方式、都會隨時間而改變。

- 擷取期間的保護

  用於在擷取期間保護物件資料的方法：同步放置（使用擷取行為的平衡或嚴格選項）、或製作過渡複本（使用雙重提交選項）。

ILM規則可篩選及選取物件。對於使用S3擷取的物件、ILM規則可根據下列中繼資料來篩選物件：

- 租戶帳戶
- 儲存區名稱
- 擷取時間
- 金鑰
- 上次存取時間

根據預設、所有S3儲存區的上次存取時間更新都會停用。如果StorageGRID 您的支援系統包含使用「上次存取時間」選項的ILM規則、則必須針對該規則中指定的S3儲存區、啟用更新以達到上次存取時間。您可以使用租戶管理程式中的「放置時段上次存取時間」要求、「* S3 > Bucket >*設定上次存取時間」核取方塊、或使用租戶管理API來啟用上次存取時間更新。啟用上次存取時間更新時、請注意StorageGRID 、可能會降低不佳效能、尤其是在使用小型物件的系統中。

- 位置限制
- 物件大小
- 使用者中繼資料
- 物件標記

如需ILM的詳細資訊、請參閱資訊生命週期管理的物件管理說明。

相關資訊

"使用租戶帳戶"

"使用ILM管理物件"

"將時段放入上次存取時間要求"

物件版本管理

您可以使用版本管理功能來保留物件的多個版本、避免意外刪除物件、並可讓您擷取及還原物件的舊版。

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

物件版本管理可與StorageGRID 資訊的生命週期管理（ILM）或S3生命週期組態結合使用。您必須明確啟用每個儲存區的版本管理、才能開啟此儲存區功能。您儲存庫中的每個物件都會指派一個版本ID、由StorageGRID該系統產生。

不支援使用MFA（多因素驗證）刪除。

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

ILM與版本管理

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

對於啟用版本管理的儲存區中的S3物件、版本管理支援可讓您建立使用非目前時間做為參考時間的ILM規則。更新物件時、其舊版本會變成非最新版本。使用非目前時間篩選器可讓您建立原則、以降低舊版物件的儲存影響。

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

如需S3版本物件的ILM原則範例、請參閱使用資訊生命週期管理來管理物件的指示。

相關資訊

"使用ILM管理物件"

實作**S3 REST API**的建議

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

針對不存在物件的使用者提出建議

如果您的應用程式經常檢查某個物件是否存在於您預期該物件實際上不存在的路徑中、您應該使用「可用」一致性控制。例如、如果您的應用程式在放入之前就先前往某個位置、則應該使用「可用」一致性控制。

否則、如果執行頭作業找不到物件、當一個或多個儲存節點無法使用時、您可能會收到大量500個內部伺服器錯誤。

您可以使用「放置時段一致性」要求、為每個時段設定「可用」一致性控制、也可以在個別API作業的要求標頭中指定一致性控制。

物件金鑰建議

對於StorageGRID 在VMware 11.4或更新版本中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。例如、您現在可以將隨機值用於物件金鑰名稱的前四個字元。

對於StorageGRID 在更新版本早於《物件金鑰名稱》的版本中所建立的儲存區、請繼續遵循下列建議：

- 您不應使用隨機值做為物件金鑰的前四個字元。這與前AWS關於金鑰前置碼的建議不同。您應該改用非隨機、非唯一的前置詞、例如 `image`。
- 如果您遵循前一項AWS建議、在金鑰前置字元中使用隨機和獨特的字元、則應該在物件金鑰前置一個目錄名稱。也就是使用此格式：

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

  而非此格式：

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

「**range Reads**」建議

如果選擇*壓縮儲存的物件*選項（組態>*網格選項*）、S3用戶端應用程式應避免執行指定要傳回某個位元組範圍的Get物件作業。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮

物件讀取10 MB範圍的效率非常低。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

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

相關資訊

"一致性控管"

"置入時段一致性要求"

"管理StorageGRID"

S3 REST API支援的作業和限制

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

支援虛擬託管型要求和路徑型要求的支援。StorageGRID

- "驗證要求"
- "服務營運"
- "在貯體上作業"
- "在貯體上進行自訂作業"
- "物件上的作業"
- "多部份上傳作業"
- "錯誤回應"

日期處理

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

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

一般要求標頭

支援由_Simple Storage Service API Reference（簡易儲存服務API參考）定義的一般要求標頭、但有一個例外StorageGRID 。

要求標頭	實作
授權	完整支援AWS簽名版本2 支援AWS簽名版本4、但有下列例外： • SHA256值不會針對申請本文進行計算。使用者提交的值會在未經驗證的情況下接受、如同值一樣 `UNSIGNED-PAYLOAD` 已提供給 `x-amz-content-sha256` 標頭。
X-amz-security-token	未實作。退貨 `XNotImplemented`。

通用回應標頭

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

回應標頭	實作
X-amz-id-2	未使用

相關資訊

"Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"

驗證要求

支援使用S3 API驗證和匿名存取物件的功能。StorageGRID

S3 API支援驗證S3 API要求的簽名版本2和簽名版本4。

驗證的要求必須使用您的存取金鑰ID和秘密存取金鑰來簽署。

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

使用**HTTP**授權標頭

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

使用查詢參數

您可以使用查詢參數將驗證資訊新增至URL。這稱為URL預先簽署、可用來授予特定資源的暫時存取權。具有預先簽署URL的使用者不需要知道秘密存取金鑰、就能存取資源、讓您提供第三方受限的資源存取權。

服務營運

支援下列服務作業的支援。StorageGRID

營運	實作
取得服務	以所有Amazon S3 REST API行為來實作。
取得儲存使用量	「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。這是服務上的作業、其路徑為/和自訂查詢參數（`?x-ntap-sg-usage`）新增。
選項/	用戶端應用程式可能會發生問題 `OPTIONS /` 要求儲存節點上的S3連接埠、但不提供S3驗證認證、以判斷儲存節點是否可用。您可以使用此要求進行監控、或允許外部負載平衡器識別儲存節點何時當機。

相關資訊

"取得儲存使用量要求"

在貯體上作業

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

儲存區名稱限制遵循AWS US Standard地區限制、但您應該進一步限制它們使用DNS命名慣例、以支援S3虛擬託管型要求。

"Amazon Web Services（AWS）文件：儲存區限制與限制"

"S3要求的端點網域名稱"

Get Bucket（列出物件）和Get Bucket版本作業支援StorageGRID 一致性控管。

您可以檢查是否為個別的儲存區啟用或停用上次存取時間的更新。

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

營運	實作
刪除時段	以所有Amazon S3 REST API行為來實作。
刪除庫位檢查	此作業會刪除儲存區的CORS組態。
刪除時段加密	此作業會從儲存區刪除預設加密。現有的加密物件仍會保持加密狀態、但新增至儲存區的任何新物件都不會加密。
刪除時段生命週期	此作業會從儲存庫中刪除生命週期組態。
刪除庫位原則	此作業會刪除附加至儲存貯體的原則。

營運	實作
刪除時段複寫	此作業會刪除附加至儲存區的複寫組態。
刪除庫位標記	此作業使用 `tagging` SubResource可移除庫位中的所有標記。
Get Bucket（列出物件）、版本1和版本2	此作業會傳回某個儲存區中的部分或全部（最多1、000個）物件。物件的儲存類別可以有兩個值之一、即使物件是使用擷取的 `REDUCED_REDUNDANCY` 儲存類別選項： • `STANDARD`（表示物件儲存在儲存節點所組成的儲存資源池中）。 • `GLACIER`、表示物件已移至Cloud Storage Pool指定的外部儲存區。 如果儲存區包含大量具有相同前置碼的刪除金鑰、回應可能會包含部分金鑰 `CommonPrefixes` 不含金鑰。
取得Bucket ACL	此作業會傳回正面回應、並傳回貯體擁有者的ID、顯示名稱和權限、表示擁有者對該貯體具有完整存取權。
獲取庫位檢查器	此作業會傳回 `cors` 鏟斗組態。
取得Bucket加密	此作業會傳回儲存區的預設加密組態。
取得生命週期	此作業會傳回該儲存庫的生命週期組態。
取得理想位置	此作業會傳回使用設定的區域 `LocationConstraint` 置入庫位要求中的元素。如果庫位所在的區域是 `us-east-1`，則會傳回區域的空白字串。
取得庫存箱通知	此作業會傳回附加至儲存貯體的通知組態。
取得Bucket物件版本	此作業可透過鏟斗的讀取存取權限 `versions` 子資源會列出儲存區中所有物件版本的中繼資料。
取得庫存管理政策	此作業會傳回附加至庫位的原則。
取得庫位複寫	此作業會傳回附加至儲存區的複寫組態。
取得庫位標記	此作業使用 `tagging` SubResource可傳回某個儲存區的所有標記。

營運	實作
取得版本管理	此實作使用 `versioning` SubResource可傳回儲存區的版本管理狀態。傳回的版本管理狀態會指出儲存區是「未版本」、或儲存區是「已啟用」或「已待定」版本。
取得物件鎖定組態	此作業可決定是否為儲存區啟用S3物件鎖定。 "使用S3物件鎖定"
鏟斗	此作業會判斷儲存區是否存在、且您是否有權存取它。

營運	實作
放入鏟斗	此作業會建立新的儲存桶。建立貯體後、您就成為了貯體的擁有者。 • 庫位名稱必須符合下列規則： ◦ 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 ◦ 必須符合DNS規範。 ◦ 必須包含至少3個字元、且不得超過63個字元。 ◦ 可以是一或多個標籤的系列、相鄰的標籤以句點分隔。每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 ◦ 不得看起來像是文字格式的IP位址。 ◦ 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 • 根據預設、會在中建立儲存區 `us-east-1` 區域；不過、您可以使用 `LocationConstraint` 要求主體中的要求元素、以指定不同的區域。使用時 `LocationConstraint` 元素、您必須指定已使用Grid Manager或Grid Management API定義的區域確切名稱。如果您不知道應該使用的地區名稱、請聯絡系統管理員。附註：如果您的Pet Bucket要求使用StorageGRID 未在功能區中定義的區域、就會發生錯誤。 • 您可以加入 `x-amz-bucket-object-lock-enabled` 要求標頭以建立啟用S3物件鎖定的儲存區。 建立儲存區時、您必須啟用S3物件鎖定。建立儲存區之後、您無法新增或停用S3物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。 "使用S3物件鎖定"
放入庫位	此作業會設定儲存區的CORS組態、以便儲存區能夠處理跨來源要求。跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的S3儲存區 `images` 儲存圖形。設定的CORS組態 `images` 儲存庫、您可以讓該儲存庫中的影像顯示在網站上 `http://www.example.com`。

營運	實作
使用資源桶加密	此作業會設定現有儲存區的預設加密狀態。啟用桶層級加密時、任何新增至桶的新物件都會加密。StorageGRID支援使用StorageGRID管理的金鑰進行伺服器端加密。指定伺服器端加密組態規則時、請設定 `SSEAlgorithm` 參數至 `AES256`、且請勿使用 `KMSMasterKeyID` 參數。 如果物件上傳要求已指定加密（亦即、如果要求包含、則會忽略儲存區預設加密組態 `x-amz-server-side-encryption-*` 要求標頭）。
放入鏟斗生命週期	此作業會為儲存庫建立新的生命週期組態、或取代現有的生命週期組態。在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素： • 到期日（天數、日期） • 非目前版本過期（非目前日期） • 篩選器（前置、標記） • 狀態 • ID 不支援下列動作：StorageGRID • AbortIncompleteMultiPart上 傳 • ExpiredObjectDelete標記 • 移轉 若要瞭解儲存庫生命週期中的到期行動如何與ILM放置指示互動、請參閱資訊生命週期管理物件說明中的「ILM在物件生命週期內的運作方式」。 附註：鏟斗生命週期組態可搭配已啟用S3物件鎖定的鏟斗使用、但舊型符合標準的鏟斗不支援鏟斗生命週期組態。

營運	實作

放置時段通知	此作業會使用要求內文所含的通知組態XML來設定儲存區的通知。您應該瞭解下列實作詳細資料：
	
	• 支援簡單通知服務（SNS）主題作為目的地。StorageGRID不支援簡單佇列服務（SQS）或Amazon Lambda端點。
	• 通知的目的地必須指定為StorageGRID 一個端點的URN。端點可以使用租戶管理程式或租戶管理API來建立。
	
	端點必須存在、通知組態才能成功。如果端點不存在、則為 `400 Bad Request` 程式碼傳回錯誤 `InvalidArgument`。
	
	• 您無法設定下列事件類型的通知。這些事件類型*不支援*。
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• 從Suse傳送的事件通知StorageGRID 會使用標準Json格式、但不包含某些金鑰、而且會針對其他金鑰使用特定值、如下列清單所示：
	• 事件來源
	
	`sgws:s3`
	
	• * awsRegion *
	
	不含
	
	• * X-amz-id-2*
	
	不含
	
	• * arn*
	
	`urn:sgws:s3:::bucket_name`

資源桶政策	此作業會設定附加至庫位的原則。

營運	實作
放入資源桶複寫	此作業會使用StorageGRID 要求本文中提供的複寫組態XML、為儲存區設定「CloudMirror複寫」。對於CloudMirror複寫、您應該瞭解下列實作詳細資料： • 僅支援複寫組態的V1。StorageGRID這表示StorageGRID 、不支援使用 `Filter` 規則元素、並遵循刪除物件版本的V1慣例。如需詳細資訊、請參閱Amazon複寫組態文件。 • 儲存區複寫可在版本控制或未版本控制的儲存區上進行設定。 • 您可以在複寫組態XML的每個規則中指定不同的目的地儲存區。來源儲存區可複寫至多個目的地儲存區。 • 目的地貯體必須指定為StorageGRID 租戶管理程式或租戶管理API中指定的非功能性端點的URN。 複寫組態必須存在端點才能成功。如果端點不存在、則要求會以的形式失敗 `400 Bad Request`。錯誤訊息指出： `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • 您不需要指定 `Role` 在組態XML中。此值不供StorageGRID Some使用、如果提交、將會忽略此值。 • 如果您從組態XML中省略儲存類別、StorageGRID則無法使用 `STANDARD` 預設為儲存類別。 • 如果您從來源儲存區刪除物件、或是刪除來源儲存區本身、跨區域複寫行為如下： ◦ 如果您在複寫物件或儲存區之前先將其刪除、則不會複寫物件/儲存區、也不會通知您。 ◦ 如果您在複寫物件或儲存區之後將其刪除、StorageGRID 則針對跨區域複寫的V1、執行標準Amazon S3刪除行為。
置入庫位標記	此作業使用 `tagging` 子資源：新增或更新一組庫位的標記。新增庫位標記時、請注意下列限制： • 支援每個儲存區最多50個標籤的支援功能包括：StorageGRID • 與庫位關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元。 • 標記值長度最多可達256個UNICODE字元。 • 金鑰和值區分大小寫。

營運	實作
放入資源桶版本管理	此實作使用 `versioning` SubResource可設定現有儲存區的版本管理狀態。您可以使用下列其中一個值來設定版本設定狀態： • 已啟用：啟用儲存區中物件的版本管理。新增至儲存庫的所有物件都會收到唯一的版本ID。 • 暫停：停用儲存區中物件的版本設定。新增至儲存庫的所有物件都會收到版本ID `null`。

相關資訊

"Amazon Web Services（AWS）文件：跨區域複寫"

"一致性控管"

"取得時段上次存取時間要求"

"儲存庫和群組存取原則"

"使用S3物件鎖定"

"稽核記錄中追蹤的S3作業"

"使用ILM管理物件"

"使用租戶帳戶"

建立**S3**生命週期組態

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

本節的簡單範例說明S3生命週期組態如何控制從特定S3儲存區刪除（過期）特定物件的時間。本節範例僅供說明用途。如需建立S3生命週期組態的完整詳細資料、請參閱《Amazon簡易儲存服務開發人員指南》中的物件生命週期管理一節。請注意StorageGRID 、僅支援過期行動、不支援轉換行動。

"Amazon Simple Storage Service開發人員指南：物件生命週期管理"

什麼是生命週期組態

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

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

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

- ID

如果您將生命週期組態套用至貯體、則該貯體的生命週期設定一律會覆寫StorageGRID 「ILM」設定。使用儲存區的到期設定、而非ILM來決定是否要刪除或保留特定物件。StorageGRID

因此、即使ILM規則中的放置指示仍套用至物件、也可能從網格中移除物件。或者、即使物件的任何ILM放置指示失效、物件仍可能保留在網格上。如需詳細資訊、請參閱資訊生命週期管理物件說明中的「ILM在物件生命週期內的運作方式」。

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

支援使用下列庫位作業來管理生命週期組態：StorageGRID

- 刪除時段生命週期
- 取得生命週期
- 放入鏟斗生命週期

建立生命週期組態

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

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

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

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

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

將生命週期組態套用至儲存庫

建立生命週期組態檔案之後、您可以發出「放入庫位」生命週期要求、將其套用至庫位。

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

```
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至儲存庫、請發出「Get Bucket生命週期」要求。例如：

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

成功的回應會列出您剛套用的生命週期組態。

驗證目標是否適用庫位生命週期到期

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

> 因為儲存區生命週期會取代ILM `expiry-date` 顯示的是物件刪除的實際日期。如需詳細資訊、請參閱執行StorageGRID 支援的說明中的「如何決定物件保留」。

例如、此Put物件要求是在2020年6月22日發出、並在中放置物件 `testbucket` 鏟斗。

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

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

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

例如、此「標頭物件」要求是用來取得同一個物件在testBucket儲存區中的中繼資料。

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

成功回應包括物件的中繼資料、指出物件將在100天內過期、且符合規則2。

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

相關資訊

"在貯體上作業"

"使用ILM管理物件"

在貯體上進行自訂作業

支援將自訂儲存區作業新增至S3 REST API、並專供系統使用。StorageGRID

下表列出StorageGRID 支援的自訂儲存區作業。

營運	說明	以取得更多資訊
取得庫位一致性	傳回套用至特定儲存庫的一致性層級。	"取得時段一致性要求"
實現庫位一致性	設定套用至特定儲存庫的一致性層級。	"置入時段一致性要求"
取得時段上次存取時間	傳回是否為特定儲存區啟用或停用上次存取時間更新。	"取得時段上次存取時間要求"
將資源桶放在最後存取時間	可讓您啟用或停用特定儲存區的上次存取時間更新。	"將時段放入上次存取時間要求"
刪除時段中繼資料通知組態	刪除與特定儲存區相關聯的中繼資料通知組態XML。	"刪除時段中繼資料通知組態要求"

營運	說明	以取得更多資訊
取得Bucket中繼資料通知組態	傳回與特定儲存區相關聯的中繼資料通知組態XML。	"取得Bucket中繼資料通知組態要求"
放置時段中繼資料通知組態	設定區段的中繼資料通知服務。	"放置時段中繼資料通知組態要求"
為符合法規要求而進行資源庫修改	已過時且不受支援：您無法再建立啟用「符合性」的新儲存區。	"已過時：將資源桶要求修改以符合法規要求"
取得符合需求的產品	已過時但受支援：傳回現有舊版相容儲存區目前有效的法規遵循設定。	"已過時：Get Bucket Compliance要求"
符合資源需求	已過時但受支援：可讓您修改現有舊版相容儲存區的法規遵循設定。	"已過時：提出資源桶法規遵循要求"

相關資訊

"稽核記錄中追蹤的S3作業"

物件上的作業

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

- "使用S3物件鎖定"
- "使用伺服器端加密"
- "取得物件"
- "標頭物件"
- "POST物件還原"
- "放置物件"
- "放置物件-複製"

下列條件適用於所有物件作業：

- 物件上的所有作業均支援不一致的控制、但下列項目除外StorageGRID ：
  - 取得物件ACL
  - `OPTIONS /`
  - 將物件保留為合法
  - 保留物件
- 相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非S3用戶端何時開始運作。
- 所有物件均由庫位擁有者擁有、包括匿名使用者或其他帳戶所建立的物件。StorageGRID

- 透過StorageGRID Swift擷取至整個系統的資料物件無法透過S3存取。

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

營運	實作
刪除物件	多因素驗證（MFA）和回應標頭 `x-amz-mfa` 不受支援。 處理刪除物件要求時StorageGRID 、功能區會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在30秒內移除所有複本（例如、因為某個位置暫時無法使用）、StorageGRID 則將複本排入佇列以供移除、然後向用戶端指出成功。 版本管理 若要移除特定版本、申請者必須是貯體擁有者、並使用 `versionId` 子資源：使用此子資源會永久刪除版本。如果是 `versionId` 對應於刪除標記、即回應標頭 `x-amz-delete-marker` 傳回設定為 `true`。 • 如果刪除的物件不含 `versionId` 子資源在啟用版本的儲存區上、會產生刪除標記。。 `versionId` 刪除標記會使用傳回 `x-amz-version-id` 回應標頭和 `x-amz-delete-marker` 回應標頭會傳回設定為 `true`。 • 如果刪除的物件不含 `versionId` 子資源在版本暫停的儲存區上、會永久刪除現有的'null '版本或'null '刪除標記、並產生新的'null '刪除標記。。 `x-amz-delete-marker` 回應標頭會傳回設定為 `true`。 附註：在某些情況下、物件可能會有多個刪除標記。
刪除多個物件	多因素驗證（MFA）和回應標頭 `x-amz-mfa` 不受支援。 您可以在同一個要求訊息中刪除多個物件。
刪除物件標記	使用 `tagging` SubResource可移除物件的所有標記。以所有Amazon S3 REST API行為來實作。 版本管理 如果是 `versionId` 查詢參數未在要求中指定、此作業會刪除版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。

營運	實作
取得物件	"取得物件"
取得物件ACL	如果提供帳戶所需的存取認證資料、則作業會傳回正面回應、並傳回物件擁有者的ID、顯示名稱和權限、表示擁有者擁有物件的完整存取權。
取得物件合法持有	"使用S3物件鎖定"
取得物件保留	"使用S3物件鎖定"
取得物件標記	使用 `tagging` SubResource可傳回物件的所有標記。以所有Amazon S3 REST API行為來實作 版本管理 如果是 `versionId` 查詢參數未在要求中指定、此作業會傳回版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。
標頭物件	"標頭物件"
POST物件還原	"POST物件還原"
放置物件	"放置物件"
放置物件-複製	"放置物件-複製"
將物件保留為合法	"使用S3物件鎖定"
保留物件	"使用S3物件鎖定"

營運	實作
放置物件標記	使用 `tagging` SubResource可將一組標記新增至現有物件。以所有Amazon S3 REST API行為來實作 標記更新和擷取行為 當您使用「放置物件」標記來更新物件的標記時、StorageGRID 無法重新擷取物件。這表示不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。 這表示、如果ILM規則使用嚴格選項來擷取行為、則無法進行所需的物件放置（例如、因為新需要的位置無法使用）、則不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。 解決衝突 相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID VMware系統何時完成指定的要求、而非S3用戶端何時開始運作。 版本管理 如果是 `versionId` 查詢參數未在要求中指定、該作業會將標記新增至版本控制儲存區中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「MethodNotSupported」狀態 `x-amz-delete-marker` 回應標頭設定為 `true`。

相關資訊

"一致性控管"

"稽核記錄中追蹤的S3作業"

使用**S3**物件鎖定

如果StorageGRID 您的還原系統已啟用全域S3物件鎖定設定、您可以在啟用S3物件鎖定的情況下建立儲存區、然後針對您新增至該儲存區的每個物件版本、指定保留直到日期和合法保留設定。

S3物件鎖定可讓您指定物件層級的設定、以防止物件在固定時間內或無限期刪除或覆寫。

「S3物件鎖定」StorageGRID 功能提供單一保留模式、相當於Amazon S3法規遵循模式。依預設、受保護的物件版本無法由任何使用者覆寫或刪除。「S3物件鎖定」StorageGRID 功能不支援管理模式、也不允許具有特殊權限的使用者略過保留設定或刪除受保護的物件。

啟用儲存區的**S3**物件鎖定

如果StorageGRID 您的整個S3物件鎖定設定已啟用、則您可以在建立每個儲存區時、選擇性地啟用S3物件鎖定。您可以使用下列任一種方法：

- 使用租戶管理程式建立桶。

  "使用租戶帳戶"

- 使用「放入庫位」要求與一起建立庫位 `x-amz-bucket-object-lock_enabled` 要求標頭：

  "在貯體上作業"

建立儲存區之後、您無法新增或停用S3物件鎖定。S3物件鎖定需要儲存區版本管理、這會在您建立儲存區時自動啟用。

啟用S3物件鎖定的儲存區可包含具有和不具有S3物件鎖定設定的物件組合。由於不支援S3物件鎖定儲存區中物件的預設保留、因此不支援「放置物件鎖定組態」儲存區作業StorageGRID 。

判斷是否已啟用儲存區的**S3**物件鎖定

若要判斷是否已啟用S3物件鎖定、請使用「取得物件鎖定組態」要求。

"在貯體上作業"

使用**S3**物件鎖定設定建立物件

若要在將物件版本新增至已啟用S3物件鎖定的儲存區時、指定S3物件鎖定設定、請發出「放置物件」、「放置物件-複製」或啟動「多重組件上傳」要求。請使用下列要求標頭。

> 建立儲存區時、您必須啟用S3物件鎖定。建立儲存區之後、您無法新增或停用S3物件鎖定。

- `x-amz-object-lock-mode`必須符合法規要求（區分大小寫）。

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

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

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

如果您使用上述任一要求標頭、請注意下列限制：

- 。 `Content-MD5` 如有任何要求、則要求標頭為必填欄位 `x-amz-object-lock-*` 要求標頭出現在「放置

物件」要求中。 `Content-MD5` 不需要「放置物件-複製」或「啟動多重成分上傳」。

- 如果儲存區未啟用S3物件鎖定和 `x-amz-object-lock-*` 出現要求標頭、傳回400個錯誤要求（InvalidRequest）錯誤。
- 「放置物件」要求支援使用 `x-amz-storage-class: REDUCED_REDUNDANCY` 以符合AWS行為。然而、當物件被擷取至啟用S3物件鎖定的儲存區時StorageGRID 、則會一律執行雙重認可擷取。
- 後續的Get或HeadObject版本回應將包含標頭 `x-amz-object-lock-mode`、 `x-amz-object-lock-retain-until-date`和 `x-amz-object-lock-legal-hold`（如果已設定）以及要求傳送者是否正確 `s3:Get*` 權限：
- 如果在保留截止日期之前或在合法持有之前、後續的刪除物件版本或刪除物件版本要求將會失敗。

更新**S3**物件鎖定設定

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

- `PUT Object legal-hold`

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

- `PUT Object retention`
  - 模式值必須符合法規（區分大小寫）。
  - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許使用其他ISO 8601格式。
  - 如果物件版本有現有的截至日期保留、您只能增加。新的價值必須是未來的價值。

相關資訊

"使用ILM管理物件"

"使用租戶帳戶"

"放置物件"

"放置物件-複製"

"啟動多部份上傳"

"物件版本管理"

"Amazon簡易儲存服務使用者指南：使用S3物件鎖定"

使用伺服器端加密

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

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

- * SSE（使用StorageGRID管理金鑰的伺服器端加密）*：當您發出S3要求以儲存物件時StorageGRID 、用

唯一的金鑰來加密物件。當您發出S3要求以擷取物件時StorageGRID 、則會使用儲存的金鑰來解密物件。

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

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

  > 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

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

使用**SS**

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

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

下列物件作業可支援SSe要求標頭：

- 放置物件
- 放置物件-複製
- 啟動多部份上傳

使用**SSE-C**

若要使用您管理的唯一金鑰來加密物件、請使用三個要求標頭：

要求標頭	說明
`x-amz-server-side-encryption-customer-algorithm`	指定加密演算法。標頭值必須是 `AES256`。
`x-amz-server-side-encryption-customer-key`	指定將用於加密或解密物件的加密金鑰。金鑰的值必須是256位元、已編碼的base64。
`x-amz-server-side-encryption-customer-key-MD5`	根據RFC 1321指定加密金鑰的md5摘要、以確保傳輸加密金鑰時不會發生錯誤。md5摘要的值必須是以64編碼的128位元。

下列物件作業可支援SSE-C要求標頭：

- 取得物件
- 標頭物件
- 放置物件
- 放置物件-複製
- 啟動多部份上傳

- 上傳零件
- 上傳零件-複製

使用伺服器端加密搭配客戶提供的金鑰（**SSE-C**）時的考量

使用SSE-C之前、請注意下列考量事項：

- 您必須使用https。

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

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

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

- 如果已針對儲存區設定CloudMirror複寫、您就無法擷取SSE-C物件。擷取作業將會失敗。

相關資訊

"取得物件"

"標頭物件"

"放置物件"

"放置物件-複製"

"啟動多部份上傳"

"上傳零件"

"上傳零件-複製"

"Amazon S3開發人員指南：使用客戶提供的加密金鑰（SSE-C）、使用伺服器端加密來保護資料"

取得物件

您可以使用S3取得物件要求、從S3儲存區擷取物件。

不支援零件編號要求參數

。 `partNumber` 「取得物件要求」不支援「要求」參數。您無法執行GET要求、以擷取多個部分物件的特定部分。傳回501未實作錯誤、並顯示下列訊息：

```
GET Object by partNumber is not implemented
```

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件是以您提供的唯一金鑰加密、請使用所有三個標頭。

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

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

使用者中繼資料中的**UTF-8**字元

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

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`：

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

版本管理

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

取得雲端儲存池物件的行為

如果物件已儲存在Cloud Storage Pool中（請參閱管理物件的指示、並進行資訊生命週期管理）、則Get物件要求的行為取決於物件的狀態。如需詳細資訊、請參閱「標頭物件」。

> 如果物件儲存在雲端儲存資源池中、而且網格上也有一個或多個物件複本、則「Get Object（取得物件）」要求會先嘗試從網格擷取資料、然後再從雲端儲存資源池擷取資料。

物件狀態	**Get**物件的行為
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK` 系統會擷取物件複本。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK` 系統會擷取物件複本。

物件狀態	**Get**物件的行為
物件移轉至無法擷取的狀態	`403 Forbidden、 InvalidObjectState` 使用POST物件還原要求、將物件還原至可擷取的狀態。
正在從無法擷取的狀態還原的物件	`403 Forbidden、 InvalidObjectState` 等待POST物件還原要求完成。
物件已完全還原至雲端儲存資源池	`200 OK` 系統會擷取物件複本。

雲端儲存資源池中的多部份或分段物件

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

在這些情況下：

- Get Object要求可能會傳回部分資料、但會在傳輸中途停止。
- 隨後可能會傳回「Get Object」（取得物件）要求 `403 Forbidden`。

相關資訊

"使用伺服器端加密"

"使用ILM管理物件"

"POST物件還原"

"稽核記錄中追蹤的S3作業"

標頭物件

您可以使用S3頭物件要求從物件擷取中繼資料、而不傳回物件本身。如果物件儲存在Cloud Storage Pool中、您可以使用「標頭物件」來判斷物件的轉換狀態。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件使用您提供的唯一金鑰加密、請使用這三個標頭。

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

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

使用者中繼資料中的**UTF-8**字元

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

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`：

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

Cloud Storage Pool物件的回應標頭

如果物件儲存在Cloud Storage Pool中（請參閱使用資訊生命週期管理來管理物件的指示）、則會傳回下列回應標頭：

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

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

物件狀態	回應標頭物件
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK` （未傳回特殊回應標頭。）

Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	在物件轉換為無法擷取的狀態之前、其值為 `expiry-date` 設定為未來的某段時間。確切的轉換時間不受StorageGRID 此功能的控制。

物件狀態	回應標頭物件

物件已轉換為無法擷取的狀態、但網格上至少也有一個複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	的價值 `expiry-date` 設定為未來的某段時間。
	
	附註：如果網格上的複本無法使用（例如、儲存節點當機）、您必須發出物件後還原要求、以便從雲端儲存池還原複本、才能成功擷取物件。

物件移轉至無法擷取的狀態、而且網格上不存在複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`

正在從無法擷取的狀態還原的物件	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

物件已完全還原至雲端儲存資源池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	。 `expiry-date` 指出Cloud Storage Pool中的物件何時會傳回無法擷取的狀態。

雲端儲存資源池中的多部份或分段物件

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

版本管理

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

相關資訊

"使用伺服器端加密"

"使用ILM管理物件"

"POST物件還原"

"稽核記錄中追蹤的S3作業"

POST物件還原

您可以使用S3 POST物件還原要求來還原儲存在雲端儲存池中的物件。

支援的要求類型

僅支援POST物件還原要求以還原物件。StorageGRID它不支援 `SELECT` 還原類型。選取「要求傳回」 `XNotImplemented`。

版本管理

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

在**Cloud Storage Pool**物件上進行物件後還原的行為

如果物件儲存在Cloud Storage Pool中（請參閱使用資訊生命週期管理來管理物件的指示）、則根據物件的狀態、POST物件還原要求會出現下列行為。如需詳細資訊、請參閱「標頭物件」。

> 如果物件儲存在雲端儲存資源池中、而且網格上也存在物件的一或多個複本、就不需要發出物件後還原要求來還原物件。相反地、您可以使用「取得物件」要求、直接擷取本機複本。

物件狀態	**POST**物件還原的行為
物件擷取至StorageGRID 不受ILM評估、或物件不在雲端儲存資源池中	`403 Forbidden`、 `InvalidObjectState`
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK` 不會進行任何變更。 附註：在物件轉換為無法擷取的狀態之前、您無法變更物件 `expiry-date`。

物件狀態	**POST**物件還原的行為
物件移轉至無法擷取的狀態	`202 Accepted` 將物件的可擷取複本還原至Cloud Storage Pool、直到要求本文指定的天數。在此期間結束時、物件會返回無法擷取的狀態。 您也可以選擇使用 `Tier` 要求元素以決定還原工作完成所需的時間 (`Expedited`、 `Standard`或 `Bulk` ）。如果您未指定 `Tier`、 `Standard` 使用階層。 注意：如果物件已轉換為S3 Glacier Deep Archive、或是雲端儲存資源池使用Azure Blob儲存設備、則無法使用還原 `Expedited` 層級。傳回下列錯誤 `403 Forbidden`、 `InvalidTier`： `Retrieval option is not supported by this storage class`。
正在從無法擷取的狀態還原的物件	`409 Conflict`、 `RestoreAlreadyInProgress`
物件已完全還原至雲端儲存資源池	`200 OK` *附註：*如果物件已還原為可擷取的狀態、您可以變更物件 `expiry-date` 以新的值重新發出POST物件還原要求 `Days`。還原日期會根據申請時間而更新。

相關資訊

"使用ILM管理物件"

"標頭物件"

"稽核記錄中追蹤的S3作業"

放置物件

您可以使用S3放置物件要求、將物件新增至儲存區。

解決衝突

相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。

物件大小

支援高達5 TB大小的物件StorageGRID 。

使用者中繼資料大小

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

使用者中繼資料中的**UTF-8**字元

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

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

- 如果使用者定義的中繼資料包含轉義的UTF-8字元、則放置、放置物件複製、取得和標頭要求都會成功。
- 無法歸還StorageGRID `x-amz-missing-meta` 標頭：金鑰名稱或值的解譯值包含不可列印的字元。

物件標籤限制

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

物件擁有權

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

支援的要求標頭

支援下列要求標頭：

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

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

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

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

- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對。

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

```
x-amz-meta-<em>name</em>: <em>value</em>
```

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

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

的價值 `creation-time` 自1970年1月1日起算為秒數。

> ILM規則無法同時使用*使用者定義的建立時間*作為參考時間、以及用於擷取行為的平衡或嚴格選項。建立ILM規則時會傳回錯誤。

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

"使用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`

"S3 REST API支援的作業和限制"

不支援的要求標頭

不支援下列要求標頭：

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

儲存類別選項

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

如果符合擷取物件的ILM規則使用「擷取行為」的「嚴格」選項、則會使用 `x-amz-storage-class` 標頭沒有作用。

下列值可用於 x-amz-storage-class：

- STANDARD （預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估ILM時、StorageGRID會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、可能需要在不同位置建立新的物件複本、而且可能需要刪除初始的過渡複本。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 且無法立即製作規則中指定的所有複本、StorageGRID 則在不同的儲存節點上製作兩份臨時複本。

    如果StorageGRID 能夠立即建立ILM規則中指定的所有物件複本（同步放置） x-amz-storage-class 標頭沒有作用。
- REDUCED_REDUNDANCY
  - 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 則僅當系統無法立即製作規則中指定的所有複本時、才能製作單一的過渡複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID。 REDUCED_REDUNDANCY 當符合物件的ILM規則建立單一複寫複本時、最適合使用此選項。在此案例中、請使用 REDUCED_REDUNDANCY 免除在每次擷取作業中不必要地建立和刪除額外的物件複本。

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

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

指定 REDUCED_REDUNDANCY 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

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

要求伺服器端加密的標頭

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

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

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

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

版本管理

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

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

相關資訊

"使用ILM管理物件"

"在貯體上作業"

"稽核記錄中追蹤的S3作業"

"使用伺服器端加密"

"如何設定用戶端連線"

放置物件-複製

您可以使用「S3放置物件-複製」要求來建立S3中已儲存物件的複本。「放置物件」-「複製」作業與執行「取得」和「放置」相同。

解決衝突

相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。

物件大小

支援高達5 TB大小的物件StorageGRID 。

使用者中繼資料中的**UTF-8**字元

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

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

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

支援的要求標頭

支援下列要求標頭：

- `Content-Type`

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

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

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

  您可以指定 `REPLACE` 覆寫複製物件時的現有標記、或更新標記。

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

"使用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`

"要求伺服器端加密的標頭"

不支援的要求標頭

不支援下列要求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`

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

儲存類別選項

。 `x-amz-storage-class` 如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會支援要求標頭、並影響到所建立的物件複本數量。

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

在「放置物件-複製」中使用**x-amz-copy-**來源

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

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

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

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

要求伺服器端加密的標頭

如果您使用伺服器端加密、所提供的要求標頭取決於來源物件是否加密、以及您是否打算加密目標物件。

- 如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「放置物件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` 指定 `AES256`。
  - `x-amz-copy-source-server-side-encryption-customer-key` 指定您在建立來源物件時所提供的加密金鑰。
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的md5摘要。

- 如果您要使用您提供及管理的唯一金鑰來加密目標物件（複本）、請包含下列三個標頭：
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定目標物件的新加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新加密金鑰的md5摘要。

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

- 如果您想要使用StorageGRID 由支援對象（複本）的獨特金鑰來加密目標物件（複本）、請在「放置物件-複製」要求中加入此標頭：
  - `x-amz-server-side-encryption`

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

版本管理

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

相關資訊

"使用ILM管理物件"

"使用伺服器端加密"

"稽核記錄中追蹤的S3作業"

"放置物件"

多部份上傳作業

本節說明StorageGRID 此功能如何支援多部份上傳作業。

- "列出多部份上傳"
- "啟動多部份上傳"
- "上傳零件"
- "上傳零件-複製"
- "完成多部份上傳"

下列條件與附註適用於所有多重部分上傳作業：

- 您不應超過1、000次同時將多個部分上傳至單一儲存庫、因為針對該儲存庫列出多個部分上傳查詢的結果可能會傳回不完整的結果。
- 針對多個零件執行AWS大小限制。StorageGRIDS3用戶端必須遵循下列準則：

- 多部份上傳的每個部分必須介於5個mib（5、242,880位元組）和5 GiB（5、368,709,120位元組）之間。
- 最後一部分可小於5個mib（5、242,880位元組）。
- 一般而言、零件尺寸應盡量大。例如、對於100 GiB物件使用5 GiB的零件大小。由於每個零件都被視為獨特的物件、因此使用大尺寸的零件可減少StorageGRID 元資料負荷。
- 對於小於5 GiB的物件、請考慮改用非多部份上傳。

- 如果ILM規則使用嚴格或平衡的擷取行為、則會針對多部分物件的每個部分進行ILM評估、並在多部分上傳完成時、針對整個物件進行ILM評估。您應該瞭解這會如何影響物件和零件放置：
  - 如果在S3多部份上傳進行期間ILM發生變更、則當多部份上傳完成物件的部分時、可能無法符合目前的ILM需求。未正確放置的任何零件都會排入ILM重新評估佇列、稍後會移至正確位置。
  - 評估零件的ILM時StorageGRID 、會根據零件大小而非物件大小來篩選。這表示物件的部分可儲存在不符合整個物件ILM需求的位置。例如、如果規則指定所有10 GB或更大的物件都儲存在DC1、而所有較小的物件則儲存在DC2、則在10部分多部分上傳的每1 GB擷取部分、都會儲存在DC2。當針對整個物件評估ILM時、物件的所有部分都會移至DC1。
- 所有的多部份上傳作業都支援StorageGRID 不一致的控管功能。
- 視需要、您可以使用伺服器端加密來上傳多個部分。若要使用SSe（伺服器端加密搭配StorageGRID管理金鑰）、請加入 `x-amz-server-side-encryption` 僅在「初始化多重成分上傳」要求中顯示要求標頭。若要使用SSE-C（使用客戶提供的金鑰進行伺服器端加密）、您可以在「初始化多部份上傳」要求和後續每個「上傳零件」要求中、指定相同的三個加密金鑰要求標頭。

營運	實作
列出多個部分上傳	請參閱 "列出多個部分上傳"
啟動多部份上傳	請參閱 "啟動多部份上傳"
上傳零件	請參閱 "上傳零件"
上傳零件-複製	請參閱 "上傳零件-複製"
完成多部份上傳	請參閱 "完成多部份上傳"
中止多部份上傳	以所有Amazon S3 REST API行為來實作
列出零件	以所有Amazon S3 REST API行為來實作

相關資訊

"一致性控管"

"使用伺服器端加密"

列出多個部分上傳

「列出多部份上傳」作業會列出某個儲存庫正在進行的多部份上傳。

支援下列要求參數：

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

。 delimiter 不支援要求參數。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。當執行完整的「多部份上傳」作業時、即為建立物件的時間點（若適用、則為版本控制）。

啟動多部份上傳

「初始化多部份上傳」作業會針對物件啟動多部份上傳、並傳回上傳ID。

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

如果符合擷取物件的ILM規則使用「擷取行為」的「嚴格」選項、則會使用 x-amz-storage-class 標頭沒有作用。

下列值可用於 x-amz-storage-class：

- STANDARD （預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估ILM時、StorageGRID會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、可能需要在不同位置建立新的物件複本、而且可能需要刪除初始的過渡複本。
  - 平衡：如果ILM規則指定平衡選項、StorageGRID 且無法立即製作規則中指定的所有複本、StorageGRID 則在不同的儲存節點上製作兩份臨時複本。

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

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

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

料。

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

指定 `REDUCED_REDUNDANCY` 只會影響第一次擷取物件時所建立的複本數量。它不會影響使用中ILM原則評估物件時所製作的物件複本數量、也不會導致資料儲存在StorageGRID 較低層級的資料冗餘環境中。

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

支援下列要求標頭：

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

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

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

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

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

  的價值 `creation-time` 自1970年1月1日起算為秒數。

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

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

"使用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`

"S3 REST API支援的作業和限制"

如需StorageGRID 瞭解如何處理UTF-8字元的資訊、請參閱「放置物件」的文件。

要求伺服器端加密的標頭

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

- * SSE-*：如果您想要使用StorageGRID 由支援的唯一金鑰來加密物件、請在「初始化多部份上傳」要求中使用下列標頭。請勿在任何上傳零件要求中指定此標頭。
  - `x-amz-server-side-encryption`
- * SSE-C*：如果您想要使用您提供及管理的唯一金鑰來加密物件、請在「初始化多部份上傳」要求（以及後續的每個「上傳零件」要求）中使用這三個標頭。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的md5摘要。

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

不支援的要求標頭

不支援並傳回下列要求標頭 `XNotImplemented`

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

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

"使用ILM管理物件"

"使用伺服器端加密"

"放置物件"

上傳零件

「上傳零件」作業會上傳物件的多部份上傳中的零件。

支援的要求標頭

支援下列要求標頭：

- `Content-Length`
- `Content-MD5`

要求伺服器端加密的標頭

如果您為「初始化多重組件上傳」要求指定SSE-C加密、則您也必須在每個「上傳零件」要求中包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定您在「初始化多部份上傳」要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在「初始化多部份上傳」要求中提供的相同的MD5摘要。

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

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

相關資訊

"使用伺服器端加密"

上傳零件-複製

「上傳零件-複製」作業會將現有物件的資料複製為資料來源、藉此上傳物件的一部分。

「上傳零件-複製」作業會在所有Amazon S3 REST API行為下執行。

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

支援下列要求標頭：

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

要求伺服器端加密的標頭

如果您為「初始化多重成分上傳」要求指定SSE-C加密、則您也必須在每個「上傳成分-複製」要求中包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定您在「初始化多部份上傳」要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在「初始化多部份上傳」要求中提供的相同的MD5摘要。

如果來源物件是使用客戶提供的金鑰（SSE-C）加密、您必須在「上傳零件-複製」要求中包含下列三個標頭、以便解密物件、然後複製：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定在創建源對象時提供的加密密鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的md5摘要。

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

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行完整的「多重組件上傳」作業時、會建立物件（並在適用情況下建立版本）。

完成多部份上傳

完整的「多重零件上傳」作業會透過組裝先前上傳的零件、完成物件的多重部分上傳。

解決衝突

相互衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間、是根據StorageGRID 下列條件而定：當系統完成特定要求時、S3用戶端開始作業時、不會開啟。

物件大小

支援高達5 TB大小的物件StorageGRID 。

要求標頭

。 `x-amz-storage-class` 如果StorageGRID 相符的ILM規則指定「雙重認可」或「平衡」的擷取行為、則會支援要求標頭、並影響到所建立的物件複本數量。

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

版本管理

此作業會完成多部份上傳。如果已針對某個儲存區啟用版本管理、則會在完成多重部分上傳時建立物件版本。

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

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

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

複寫失敗、通知或中繼資料通知

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

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

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

相關資訊

"使用ILM管理物件"

錯誤回應

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

支援的**S3 API**錯誤代碼

名稱	**HTTP**狀態
ACCESSDENIED	403禁止
《標誌摘要》	400個錯誤要求
BuckketAlreadyEx分子	衝突
BucketNotEmpty	衝突

名稱	**HTTP**狀態
不完整正文	400個錯誤要求
內部錯誤	500內部伺服器錯誤
InvalidAccessKeyId	403禁止
InvalidArgument	400個錯誤要求
InvalidBucketName	400個錯誤要求
InvalidBucketState	衝突
InvalidDigest	400個錯誤要求
InvalidEncryptionAlgorithm錯誤	400個錯誤要求
InvalidPart	400個錯誤要求
InvalidPartOrder	400個錯誤要求
InvalidRang	無法滿足416個要求的範圍
InvalidRequest	400個錯誤要求
InvalidStorageClass	400個錯誤要求
InvalidTag	400個錯誤要求
InvalidURI	400個錯誤要求
KeyTooLong	400個錯誤要求
MalformedXML	400個錯誤要求
Metadata TooLarg	400個錯誤要求
方法未允許	不允許使用405方法
內容長度	需要411長度
MissingRequestBodyError	400個錯誤要求

名稱	**HTTP**狀態
MISingSecurityHeader	400個錯誤要求
NoSuchBucket	找不到404
NoSuchKey	找不到404
NoSuchUpload	找不到404
未實作	501未實作
NoSuchBucketPolicy	找不到404
ObjectLockConfiguration未找到錯誤	找不到404
預先條件失敗	412先決條件失敗
要求時間TooSkewed	403禁止
服務無法使用	503服務無法使用
簽名DoesNotMatch	403禁止
TooManyboo	400個錯誤要求
使用者KeyMustBeSpecified	400個錯誤要求

零點自訂錯誤代碼**StorageGRID**

名稱	說明	**HTTP**狀態
XBucketLifecycleNotSupported	不允許在符合舊版規範的儲存庫中進行貯體生命週期組態	400個錯誤要求
XBucketPolicyParseException	無法剖析收到的儲存區原則Json。	400個錯誤要求
XComplianceConflict	因為舊版規範設定而拒絕作業。	403禁止
XComplianceReducedRedundancyForbided	舊型符合標準的儲存區不允許減少備援	400個錯誤要求
XMaxBucketPolicyLengthExceed	您的原則超過允許的儲存區原則長度上限。	400個錯誤要求

名稱	說明	HTTP狀態
XMissingInternalRequestHeader	缺少內部要求的標頭。	400個錯誤要求
XNoSuchBucketCompliance	指定的儲存庫未啟用舊版法規遵循。	找不到404
XNotAcceptable	要求包含一或多個無法滿足的Accept標頭。	無法接受的406
XNotImplemed	您提供的要求暗示功能尚未實作。	501未實作

支援SS3 REST API作業StorageGRID

S3 REST API上新增了特定StorageGRID 於該系統的作業。

取得時段一致性要求

「Get Bucket一致性」要求可讓您決定套用至特定Bucket的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

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

申請範例

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

回應

在回應XML中、 `<Consistency>` 會傳回下列其中一個值：

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。

一致性控制	說明
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。符合Amazon S3一致性保證。 *附註：*如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請將一致性控制設為「可用」、除非您需要類似Amazon S3的一致性保證。
可用的（最終的頭端作業一致性）	其行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供一致的執行方式。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。不同於Amazon S3一致性保證、僅適用於頭端作業。

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

"一致性控管"

置入時段一致性要求

「放入庫位一致性」要求可讓您指定要套用至庫位執行作業的一致性層級。

預設的一致性控制項設定為保證新建立物件的寫入後讀取。

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

申請

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

一致性控制	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。符合Amazon S3一致性保證。 *附註：*如果您的應用程式在不存在的物件上使用標頭要求、如果一個或多個儲存節點無法使用、您可能會收到大量500個內部伺服器錯誤。若要避免這些錯誤、請將一致性控制設為「可用」、除非您需要類似Amazon S3的一致性保證。
可用的（最終的頭端作業一致性）	其行為與「全新寫入後的讀取」一致性層級相同、但最終只能提供一致的執行方式。如果儲存節點無法使用、則頭端作業的可用度比「全新寫入後的準備」高。不同於Amazon S3一致性保證、僅適用於頭端作業。

*附註：*一般而言、您應該使用「全新寫入後的讀取」一致性控制值。如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、將用戶端設定為針對每個API要求指定一致性控制。只能將貯體層級的一致性控制設定為最後的方法。

申請範例

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

相關資訊

"一致性控管"

取得時段上次存取時間要求

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

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

申請範例

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

回應範例

此範例顯示已針對儲存庫啟用上次存取時間更新。

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

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

將時段放入上次存取時間要求

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

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

> 從版本10.3開始StorageGRID 、所有新的儲存庫預設都會停用上次存取時間的更新。如果您有使用StorageGRID 舊版的更新程式建立的儲存區、而且想要符合新的預設行為、則必須明確停用這些舊版儲存區的上次存取時間更新。您可以使用租戶管理程式中的「放置時段上次存取時間」要求、「* S3 > Bucket >*變更上次存取設定」核取方塊、或「租戶管理API」、來啟用或停用上次存取時間的更新。

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

- 「取得物件」、「取得物件ACL」、「取得物件標記」和「標頭物件要求」不會更新上次存取時間。不會將物件新增至佇列、以進行資訊生命週期管理（ILM）評估。
- 放置物件：只更新中繼資料的複製和放置物件標記要求、也會更新上次存取時間。物件會新增至佇列以進行ILM評估。
- 如果來源儲存區的上次存取時間更新已停用、則「放置物件」-「複製要求」不會更新來源儲存區的上次存取時間。複製的物件不會新增至來源儲存區的ILM評估佇列。但是、對於目的地、「放置物件」-「複製要求」一律會更新上次存取時間。物件複本會新增至佇列以進行ILM評估。
- 完成多重成分上傳要求更新上次存取時間。完成的物件會新增至佇列以進行ILM評估。

申請範例

此範例可讓儲存區的上次存取時間達到。

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

此範例會停用儲存區的上次存取時間。

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

相關資訊

"使用租戶帳戶"

刪除時段中繼資料通知組態要求

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

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

申請範例

此範例顯示停用區段的搜尋整合服務。

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

取得**Bucket**中繼資料通知組態要求

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

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

申請範例

此要求會擷取名為的儲存區之中繼資料通知組態 `bucket`。

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

回應

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

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

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

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的

名稱	說明	必要
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的

名稱	說明	必要
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es` 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

回應範例

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

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

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

相關資訊

"使用租戶帳戶"

放置時段中繼資料通知組態要求

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

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

申請

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

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

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

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

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

下表說明中繼資料通知組態XML中的元素。

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

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es` 必須是第三個元素。 • URN必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

申請範例

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

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

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

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

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

<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>
```

相關資訊

"使用租戶帳戶"

由搜尋整合服務產生的JSON

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

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

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

中繼資料通知中包含的物件中繼資料

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

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

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

類型	項目名稱	說明
系統中繼資料	md5	物件雜湊
使用者中繼資料	中繼資料 *key:value*	物件的所有使用者中繼資料、做為金鑰值配對
標記	標記 *key:value*	為物件定義的所有物件標記、做為金鑰值配對

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

取得儲存使用量要求

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

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

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

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

申請範例

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

回應範例

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

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

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

版本管理

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

相關資訊

"一致性控管"

已過時的資源桶要求、適用於舊版法規遵循

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

法規遵循功能已過時

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

如果您先前已啟用「全域規範」設定、當您升級StorageGRID 至版本號為「版本5：11：5」時、全域「S3物件鎖定」設定會自動啟用。您不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、您可以視需要使用StorageGRID 「S3 REST API」來管理任何現有的符合舊規範的儲存庫。

"使用S3物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

已過時：將資源桶要求修改以符合法規要求

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

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

"使用S3物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您無法再建立啟用「法規遵循」的新庫位。如果您嘗試使用「置放桶」要求修改以符合法規要求、以建立新的「符合法規」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.
```

相關資訊

"使用ILM管理物件"

"使用租戶帳戶"

已過時：**Get Bucket Compliance**要求

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

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

"使用S3物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

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

申請範例

此範例要求可讓您決定名為的儲存區的法規遵循設定 `mybucket`。

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

回應範例

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

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

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

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。在取消合法持有之前、即使保留期間已過期、也無法刪除此儲存區中的物件。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

錯誤回應

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

相關資訊

"使用ILM管理物件"

"使用租戶帳戶"

已過時：提出資源桶法規遵循要求

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

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

"使用S3物件鎖定"

"使用ILM管理物件"

"NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

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

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

申請範例

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

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

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

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。 *注意：*當為RetentionPeriodMinute指定新值時、您必須指定等於或大於該儲存格目前保留期間的值。在桶的保留期間設定完成之後、您就無法減少該值、只能增加該值。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。在取消合法持有之前、即使保留期間已過期、也無法刪除此儲存區中的物件。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

法規遵循設定的一致性層級

當您更新S3儲存區的法規遵循設定、並提出「置放儲存區法規遵循」要求時StorageGRID 、即可嘗試更新整個網格的儲存區中繼資料。根據預設、StorageGRID 支援使用*強式全域*一致性層級、以保證所有資料中心站台及包含儲存庫中繼資料的所有儲存節點、在變更的法規遵循設定中、具有寫入後讀取一致性。

如果StorageGRID 由於某個站台的資料中心站台或多個儲存節點無法使用、導致無法達到*強式全域*一致性等級、則回應的HTTP狀態代碼為 `503 Service Unavailable.`

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

除非您是技術支援人員的指示、而且您不瞭解使用此層級可能造成的後果、否則請勿強迫*強站台*一致性層級以符合放置桶規範。

當一致性層級降至*強站台*時StorageGRID 、更新的法規遵循設定只有在站台內的用戶端要求才具有寫入後讀取一致性。這表示StorageGRID 在所有站台和儲存節點都可用之前、此儲存區的設定可能會暫時有多個不一致的設定。不一致的設定可能會導致非預期和非預期的行為。例如、如果您將儲存庫置於合法持有之下、而強制降低一致性層級、則儲存庫先前的法規遵循設定（即合法暫停）可能會繼續在某些資料中心站台上生效。因此、您認為合法保留的物件、可能會在保留期間到期時遭到刪除、使用者或自動刪除（如果已啟用）。

若要強制使用*強站台*一致性層級、請重新發出「Put Bucket Compliance」（放入儲存庫）要求、並附上 `Consistency-Control` HTTP要求標頭、如下所示：

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

錯誤回應

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

相關資訊

"已過時：將資源桶要求修改以符合法規要求"

"使用租戶帳戶"

"使用ILM管理物件"

儲存庫和群組存取原則

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

- 資源庫原則、使用「取得資源庫」原則設定、「放入資源庫」原則、以及刪除資源庫原則S3 API作業。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。

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。
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。

在主體元素中、除了設定匿名存取（將權限授予每個人）之外、不支援萬用字元。例如、您將萬用字元（*）設為主要值。

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

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。

相關資訊

"使用租戶帳戶"

原則的一致性控制設定

根據預設、您對群組原則所做的任何更新最終都是一致的。一旦群組原則一致、因為原則快取、變更可能需要額外15分鐘才能生效。根據預設、您對庫位原則所做的任何更新、最終也會保持一致。

您可以視需要變更庫位原則更新的一致性保證。例如、基於安全考量、您可能希望變更庫位原則、使其儘快生效。

在此情況下、您可以設定 `Consistency-Control` 請參閱「放入庫位」原則要求中的標頭、或使用「放入庫位一致性」要求。變更此要求的一致性控制時、您必須使用* all *值、以提供寫入後讀取一致性的最高保證。如果您在「放置時段一致性要求」的標頭中指定任何其他一致性控制值、則該要求將被拒絕。如果您為「放入庫位」原則要求指定任何其他值、則會忽略該值。當儲存區原則一致之後、由於原則快取、變更可能需要額外8秒的時間才能生效。

如果您將一致性層級設為*全部*、以強制新的儲存庫原則更快生效、請務必在完成時將儲存庫層級控制權設回其原始值。否則、所有未來的貯體要求都會使用* all*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"

  PPUT Bucket原則作業的HTTP要求本文必須以charset=utf-8進行編碼。

指定原則中的資源

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。

相關資訊

"在原則中指定變數"

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主體元素、因為群組被理解為主體。
- 在原則中、原則會以「主體」或「NotPrincipal」等元素表示、以排除原則。
- 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現在使用S3：PuttReplicationConfiguration權限來執行PPUT和DELETE Bucket複寫動作。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	放入鏟斗	
S3：刪除資源桶	刪除時段	
S3：刪除BucketMetadata通知	刪除時段中繼資料通知組態	是的
S3：刪除BucketPolicy	刪除庫位原則	
S3：刪除複製組態	刪除時段複寫	是的、請針對「放置」和「刪除」*分別設定權限
S3：GetBucketAcl	取得Bucket ACL	
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	獲取庫位檢查器	
S3：GetEncryptionConfiguration	取得Bucket加密	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：GetBucketLastAccessTime	取得時段上次存取時間	是的
S3：GetBucketLocation	取得理想位置	
S3：GetBucketMetadata通知	取得Bucket中繼資料通知組態	是的
S3：GetBucketNotification	取得庫存箱通知	
S3 ：GetBucketObjectLockConfiguration	取得物件鎖定組態	
S3：GetBucketPolicy	取得庫存管理政策	
S3：GetBucketting	取得庫位標記	
S3：GetBucketVersion	取得版本管理	
S3：Get生命 週期組態	取得生命週期	
S3：GetReplicationConfiguration	取得庫位複寫	
S3：ListAllMyb桶	• 取得服務 • 取得儲存使用量	是的、適用於取得儲存設備使用量
S3：清單庫	• Get Bucket（列出物件） • 鏟斗 • POST物件還原	
S3：listBucketMultiPartUploads	• 列出多個部分上傳 • POST物件還原	
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	• 刪除庫位檢查 • 放入庫位	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：PuttEncryptionConfiguration	• 刪除時段加密 • 使用資源桶加密	
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的
S3：PuttBucketNotification	放置時段通知	
S3：PuttBucketObjectLockConfiguration	將鏟斗放在一起 `x-amz-bucket-object-lock-enabled: true` 要求標頭（也需要S3：建立桶權限）	
S3：PuttBucketPolicy	資源桶政策	
S3：PuttBucketting	• 刪除庫位標記 • 置入庫位標記	
S3：PuttBucketVersion	放入資源桶版本管理	
S3：Putt升降 器組態	• 刪除時段生命週期 • 放入鏟斗生命週期	
S3：PuttReplicationConfiguration	放入資源桶複寫	是的、請針對「放置」和「刪除」*分別設定權限

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	• 中止多部份上傳 • POST物件還原	
S3：刪除物件	• 刪除物件 • 刪除多個物件 • POST物件還原	
S3：刪除ObjectTagging	刪除物件標記	

權限	**S3 REST API**作業	客製**StorageGRID** 化以供選擇
S3：刪除ObjectVersion標記	刪除物件標記（物件的特定版本）	
S3：刪除ObjectVersion	刪除物件（物件的特定版本）	
S3：GetObject	• 取得物件 • 標頭物件 • POST物件還原	
S3：GetObjectAcl	取得物件ACL	
S3：GetObjectLegalHold	取得物件合法持有	
S3：GetObjectRetention	取得物件保留	
S3：GetObjectTagging	取得物件標記	
S3：GetObjectVersion標記	取得物件標記（物件的特定版本）	
S3：GetObjectVersion	Get物件（物件的特定版本）	
S3：列出多個零件上傳零件	列出零件、POST物件還原	
S3：PuttObject	• 放置物件 • 放置物件-複製 • POST物件還原 • 啟動多部份上傳 • 完成多部份上傳 • 上傳零件 • 上傳零件-複製	
S3：PuttObjectLegalHold	將物件保留為合法	
S3：PuttObjectRetention	保留物件	
S3：PuttObjectTagging	放置物件標記	
S3：PuttObjectVersion標記	放置物件標記（物件的特定版本）	

權限	S3 REST API作業	客製StorageGRID 化以供選擇
S3：PuttOverwriteObject	• 放置物件 • 放置物件-複製 • 放置物件標記 • 刪除物件標記 • 完成多部份上傳	是的
S3：恢復物件	POST物件還原	

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：
    - 無法覆寫物件的資料、使用者定義的中繼資料或S3物件標記。
    - 任何進行中的擷取作業都會取消、並傳回錯誤。
    - 如果啟用S3版本管理、則「拒絕」設定可防止「放置物件標記」或「刪除物件標記」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、而且PuttOverwriteObject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、如果選中*防止用戶端修改*核取方塊（組態>*網格選項*）、該設定會覆寫「PuttoverriteObject」權限的設定。

相關資訊

"S3群組原則範例"

指定原則中的條件

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: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

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。

條件運算子	說明
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據「'true or假'」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

類別	適用的條件金鑰	說明
IP營運者	AWS：來源Ip	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` 由於無法確定標頭的有效性、因此會忽略標頭。
資源/身分識別	AWS：使用者名稱	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。

類別	適用的條件金鑰	說明
S3：清單儲存庫和 S3：listBucketVerions權限	S3：分隔符號	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的分隔符號參數。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：金鑰上限	會比較「Get Bucket」或「Get Bucket Object版本」要求中指定的最大金鑰參數。
S3：清單儲存庫和 S3：listBucketVerions權限	S3：前置碼	會比較「Get Bucket」或「Get Bucket Object versions」要求中指定的前置字元參數。

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**
原則授予非擁有者帳戶（包括匿名帳戶）放置物件的權限	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：

- 在Grid Manager中，轉到* Configuration（配置）> Grid Options（網格選項），然後選中 Prevent Client Modification（禁止客戶修改）複選框。
- 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。
  - 新增「允許放置物件」作業至S3原則。

> 若在S3原則中將刪除物件設為拒絕、則不會在存在「30天後歸零複本」等規則時、防止ILM刪除物件。

> 即使套用所有這些規則和原則、也無法防止並行寫入（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

"使用ILM管理物件"

"建立需要特殊處理的原則"

"如何利用ILM規則來管理物件StorageGRID"

"S3群組原則範例"

S3原則範例

請利用本節的範例、針對StorageGRID 庫位和群組建構不需執行的存取原則。

S3儲存區政策範例

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。

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
<em>file://policy.json</em>
```

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）都可以列出儲存區中的物件、並對儲存區中的所有物件執行「Get Object」（取得物件）作業。所有其他作業都將遭拒。請注意、此原則可能並不特別實用、因為除了帳戶根以外、沒有其他人擁有寫入儲存區的權限。

```
{
  "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、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「Get Object」（取得物件）作業、而只有屬於群組的使用者 `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/*"
    }
  ]
}
```

相關資訊

"在貯體上作業"

S3群組原則範例

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、因為它是內含的。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

使用租戶管理程式新增或編輯群組時、您可以選取建立群組原則的方式、以定義此群組中哪些S3存取權限成員

將擁有的群組原則、如下所示：

- 無**S3**存取：預設選項。此群組中的使用者沒有S3資源的存取權、除非使用資源桶原則授予存取權。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。
- 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。

  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）。

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：允許群組成員只能完整存取儲存庫中的「**'folder"**」

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}/*"
    }
  ]
}
```

相關資訊

"使用租戶帳戶"

"使用PuttOverwriteObject權限"

"一次寫入多讀（WORM）保護"

設定REST API的安全性

您應該檢閱針對REST API實作的安全措施、並瞭解如何保護系統安全。

如何為REST API提供安全性StorageGRID

您應該瞭解StorageGRID 什麼是讓此系統為REST API實作安全性、驗證和授權。

使用下列安全措施。StorageGRID

- 如果已針對負載平衡器端點設定HTTPS、則用戶端與負載平衡器服務的通訊會使用HTTPS。

  當您設定負載平衡器端點時、可以選擇啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

- 根據預設StorageGRID 、使用HTTPS與儲存節點進行用戶端通訊、並在閘道節點上使用CLB服務。

您可以選擇性地為這些連線啟用HTTP。例如、您可能想要使用HTTP進行測試或其他非正式作業用途。如StorageGRID 需詳細資訊、請參閱《關於管理功能的說明》。

CLB服務已過時。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。

安全性憑證與用戶端應用程式

用戶端可連線至閘道節點或管理節點上的負載平衡器服務、直接連線至儲存節點、或連線至閘道節點上的CLB服務。

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線至負載平衡器服務時、應用程式會使用針對用於建立連線的特定負載平衡器端點所設定的憑證來執行此作業。每個端點都有自己的憑證、可以是由網格管理員上傳的自訂伺服器憑證、也可以是網格管理員StorageGRID 在設定端點時產生的憑證。
- 當用戶端應用程式直接連線至儲存節點或閘道節點上的CLB服務時、它們會使用StorageGRID 安裝時（由系統憑證授權單位簽署）為儲存節點產生的系統產生伺服器憑證、 或是由網格管理員提供的單一自訂伺服器憑證。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

如StorageGRID 需設定負載平衡器端點的相關資訊、以及新增單一自訂伺服器憑證以供TLS連線直接連線至儲存節點或閘道節點上的CLB服務的相關指示、請參閱《for Administering》（管理功能）。

摘要

下表顯示S3和Swift REST API如何實作安全性問題：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證
用戶端驗證	• S3：S3帳戶（存取金鑰ID和秘密存取金鑰） • Swift：Swift帳戶（使用者名稱和密碼）
用戶端授權	• S3：貯體所有權及所有適用的存取控制原則 • Swift：系統管理員角色存取

相關資訊

"管理StorageGRID"

TLS程式庫支援的雜湊和加密演算法

支援一套有限的加密套件、用戶端應用程式可在建立傳輸層安全性（TLS）工作階段時使用。StorageGRID

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

不再支援SSLv3和TLS 1.1（或更早版本）。

支援的加密套件

TLS版本	加密套件的**IANA**名稱
1.2	TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
1.2	TLS_ECDHE_RSA_with _CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_with _AES-122_GCM_SHA256
1.3	TLS_AES-256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES-128_GCM_SHA256

已過時的加密套件

下列加密套件已過時。未來版本將會移除對這些密碼的支援。

IANA名稱
TLS_RSA_AT_AES-122_GCM_SHA256
TLS_RSA_AT_AES-256_GCM_SHA384

相關資訊

"如何設定用戶端連線"

監控與稽核作業

您可以檢視整個網格或特定節點的交易趨勢、來監控用戶端作業的工作負載和效率。您可以使用稽核訊息來監控用戶端作業和交易。

- "監控物件擷取和擷取速率"
- "存取及檢閱稽核記錄"

監控物件擷取和擷取速率

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

步驟

1. 使用支援的瀏覽器登入Grid Manager。
2. 在儀表板上、找到「傳輸協定作業」區段。

   本節概述StorageGRID 您的一套系統執行的用戶端作業數量。在過去兩分鐘內平均傳輸協定速率。

3. 選擇*節點*。
4. 在節點首頁（部署層級）中、按一下*負載平衡器*索引標籤。

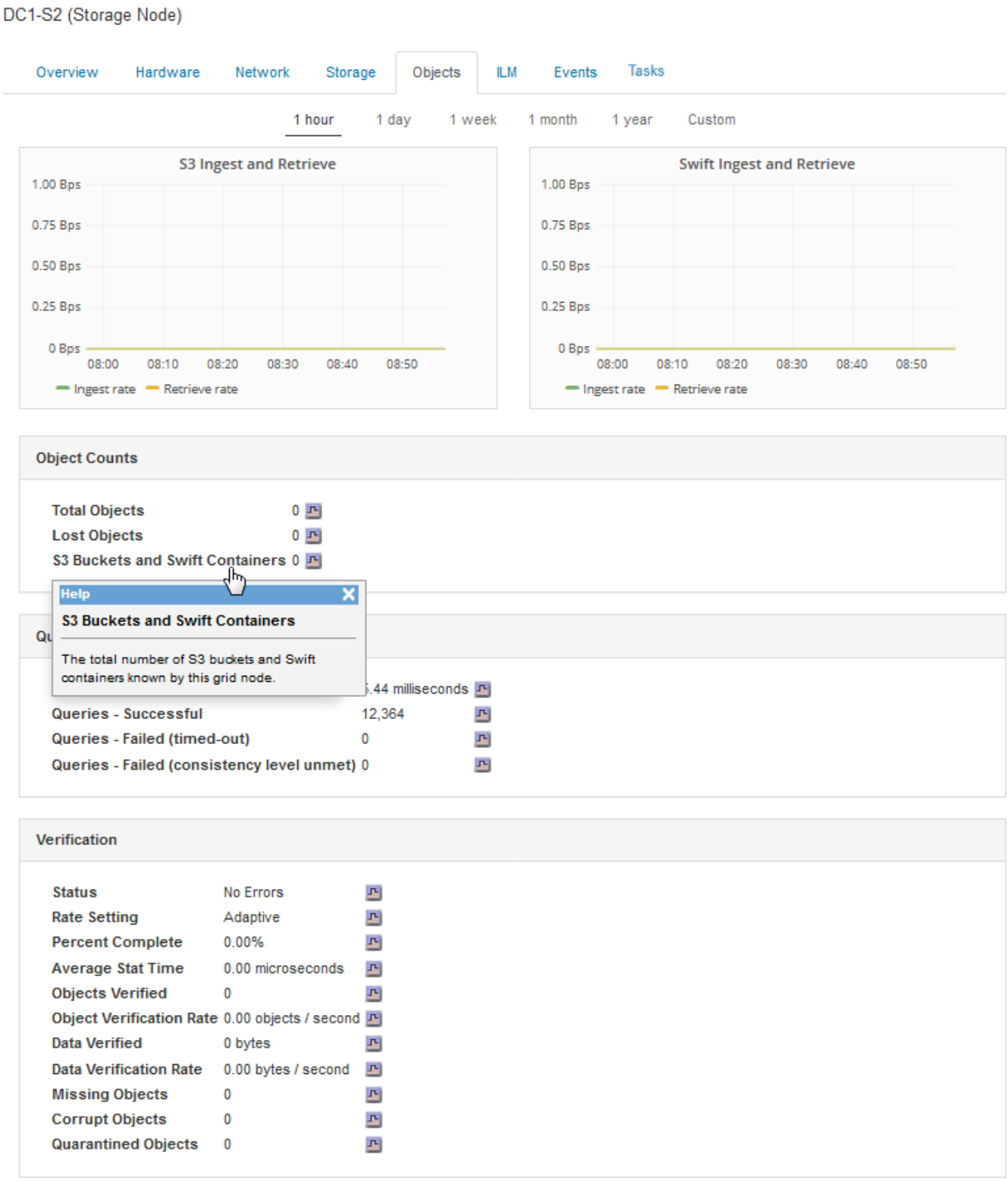
   這些圖表顯示了導向至網格內負載平衡器端點的所有用戶端流量趨勢。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

5. 在節點首頁（部署層級）中、按一下*物件*索引標籤。

   此圖表以StorageGRID 每秒位元組數和總位元組數顯示整個系統的擷取和擷取速率。您可以選擇以小時、天、週、月或年為單位的時間間隔、 您也可以套用自訂時間間隔。

6. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後按一下「物件」索引標籤。

   此圖表顯示此儲存節點的物件擷取和擷取速率。此索引標籤也包含物件計數、查詢和驗證的度量。您可以按一下標籤來查看這些度量的定義。



7. 如果您想要更詳細的資料：
   a. 選取*支援*>*工具*>*網格拓撲*。
   b. 選擇*站台_*>*總覽*>*主選項*。

      「API作業」區段會顯示整個網格的摘要資訊。

c. 選擇「儲存節點_」>「最大」>「用戶端應用程式_」>「總覽」>「主要」

「作業」區段會顯示所選儲存節點的摘要資訊。

存取及檢閱稽核記錄

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。稽核日誌中的API專屬稽核訊息可提供關鍵的安全性、作業和效能監控資料、協助您評估系統的健全狀況。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有 `Passwords.txt` 檔案：
- 您必須知道管理節點的IP位址。

關於這項工作

作用中的稽核記錄檔會命名為 `audit.log`和儲存在管理節點上。

一天只要儲存一次作用中的audit.log檔案、就會儲存一個新檔案 `audit.log` 檔案已啟動。儲存檔案的名稱會以格式指出儲存時間 *`yyyy-mm-dd.txt`*。

一天後、儲存的檔案會以壓縮格式重新命名 *`yyyy-mm-dd.txt.gz`*，保留原始日期。

此範例顯示使用中的 `audit.log` 檔案、前一天的檔案 (`2018-04-15.txt`）、以及前一天的壓縮檔案 (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

步驟

1. 登入管理節點：
   a. 輸入下列命令：+ `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
2. 移至包含稽核記錄檔的目錄：

   ```
   cd /var/local/audit/export
   ```

3. 視需要檢視目前或已儲存的稽核記錄檔。

稽核記錄中追蹤的**S3**作業

在不完整的稽核記錄中、會追蹤多項庫位作業和物件作業StorageGRID 。

稽核記錄中追蹤的庫位作業

- 刪除時段
- 刪除庫位標記
- 刪除多個物件
- Get Bucket（列出物件）
- 取得Bucket物件版本
- 取得庫位標記
- 鏟斗
- 放入鏟斗
- 符合資源需求
- 置入庫位標記
- 放入資源桶版本管理

稽核記錄中追蹤的物件作業

- 完成多部份上傳
- 上傳零件（ILM規則使用嚴格或平衡的擷取行為時）
- 上傳零件-複本（ILM規則使用嚴格或平衡的擷取行為時）
- 刪除物件
- 取得物件
- 標頭物件
- POST物件還原
- 放置物件
- 放置物件-複製

相關資訊

"在貯體上作業"

"物件上的作業"

作用中、閒置及並行HTTP連線的優點

如何設定HTTP連線、可能會影響StorageGRID 到整個系統的效能。組態會因HTTP連線為作用中或閒置狀態、或是您同時有多個連線而有所不同。

您可以找出下列類型HTTP連線的效能優勢：

- 閒置HTTP連線
- 作用中HTTP連線

- 並行HTTP連線

相關資訊

- "保持閒置HTTP連線開啟的優點"
- "作用中HTTP連線的優點"
- "並行HTTP連線的優點"
- "分隔HTTP連線集區以進行讀取和寫入作業"

保持閒置**HTTP**連線開啟的優點

即使用戶端應用程式閒置、您仍應保持HTTP連線開啟、以允許用戶端應用程式透過開放式連線執行後續交易。根據系統測量與整合體驗、您應將閒置的HTTP連線保持開啟狀態最長10分鐘。可能會自動關閉持續開啟和閒置超過10分鐘的HTTP連線。StorageGRID

開放式和閒置的HTTP連線提供下列優點：

- 縮短延遲時間、從StorageGRID 由整個過程中、由整個過程中的資訊系統判斷它必須執行HTTP交易到StorageGRID 整個系統能夠執行交易的時間

  縮短延遲是主要優勢、尤其是在建立TCP/IP和TLS連線所需的時間內。

- 使用先前執行的傳輸來初始化TCP/IP慢速啟動演算法、藉此提高資料傳輸率
- 即時通知多種故障情況、可中斷用戶端應用程式與StorageGRID 該系統之間的連線

判斷閒置連線開啟的時間長度、是在與現有連線相關的慢速啟動優點與內部系統資源連線的理想分配之間取得平衡。

作用中**HTTP**連線的優點

對於直接連線至儲存節點或閘道節點上的CLB服務（已過時）、您應該將作用中HTTP連線的持續時間限制在最長10分鐘內、即使HTTP連線持續執行交易。

判斷連線應保持開啟的最長時間、是在連線持續性的優點與連線至內部系統資源的理想分配之間取得平衡。

對於用戶端連線至儲存節點或CLB服務、限制作用中HTTP連線可提供下列優點：

- 在StorageGRID 整個支援過程中實現最佳負載平衡。

  使用CLB服務時、您應避免長時間使用的TCP/IP連線、以最佳化StorageGRID 整個VMware系統的負載平衡。您應該設定用戶端應用程式來追蹤每個HTTP連線的持續時間、並在設定時間後關閉HTTP連線、以便重新建立及重新平衡HTTP連線。

  CLB服務會在StorageGRID 用戶端應用程式建立HTTP連線時、平衡整個整個作業系統的負載。隨著時間推移、隨著負載平衡需求的變更、HTTP連線可能不再是最佳狀態。當用戶端應用程式為每筆交易建立獨立的HTTP連線時、系統會執行最佳負載平衡、但這會使持續連線所帶來的更多寶貴成果喪失價值。

  CLB服務已過時。

- 允許用戶端應用程式將HTTP交易導向具有可用空間的LDR服務。
- 可啟動維護程序。

  部分維護程序只會在所有進行中的HTTP連線完成後才會開始。

對於連接到負載平衡器服務的用戶端連線、限制開放連線的持續時間、有助於讓部分維護程序立即啟動。如果用戶端連線的持續時間不受限制、可能需要幾分鐘的時間才能自動終止作用中的連線。

並行**HTTP**連線的優點

您應該StorageGRID 將多個TCP/IP連線保持開放狀態、以允許平行處理、進而提升效能。最佳的平行連線數量取決於各種因素。

並行HTTP連線提供下列優點：

- 縮短延遲時間

  交易可以立即開始、而非等待其他交易完成。

- 提高處理量

  此系統可執行平行交易、並提高集合交易處理量。StorageGRID

用戶端應用程式應建立多個HTTP連線。當用戶端應用程式必須執行交易時、它可以選取並立即使用任何目前未處理交易的已建立連線。

在StorageGRID 效能開始降級之前、每個支援系統的拓撲在並行交易和連線方面都有不同的尖峰處理量。尖峰處理量取決於運算資源、網路資源、儲存資源和WAN連結等因素。此外、伺服器和服務的數量、StorageGRID 以及支援哪些應用程式、也是因素。

支援多種用戶端應用程式的系統。StorageGRID當您決定用戶端應用程式所使用的並行連線數目上限時、請謹記這一點。如果用戶端應用程式包含多個軟體實體、每個實體都會建立StorageGRID 與該系統的連線、您應該新增整個實體之間的所有連線。在下列情況下、您可能必須調整並行連線的最大數量：

- 此系統的拓撲會影響系統可支援的並行交易和連線數量上限。StorageGRID
- 在StorageGRID 頻寬有限的網路上與該系統互動的用戶端應用程式、可能必須降低並行度、以確保在合理的時間內完成個別交易。
- 當許多用戶端應用程式共用StorageGRID 該系統時、您可能必須減少並行處理的程度、以避免超出系統限制。

分隔**HTTP**連線集區以進行讀取和寫入作業

您可以使用不同的HTTP連線集區進行讀取和寫入作業、並控制每個集區的使用量。獨立的HTTP連線集區可讓您更有效地控制交易並平衡負載。

用戶端應用程式可建立擷取主導（讀取）或儲存主導（寫入）的負載。有了個別的HTTP連線集區、即可針對讀寫交易調整每個集區的專屬容量、以處理讀寫交易。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。