aws

建立防護機制並監控預先簽章URLs

AWS 方案指引

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 建立防護機制並監控預先簽章URLs

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

建立防護機制並監控預先簽章URLs

Ryan Baker，Amazon Web Services (AWS)

2025 年 8 月 (文件歷史記錄)

安全性是 AWS Well-Architected Framework 中所有公司和關鍵支柱的重要考量。身為安全工程師，您需要實作符合組織控制需求的管理護欄。在 AWS Well-Architected Framework 中，護欄會定義限制活動的邊界。

本指南提供使用預先簽章 URLs 與 Amazon Simple Storage Service (Amazon S3) 物件搭配使用。預先簽章URLs 允許有權存取有效登入資料的使用者或應用程式產生預先簽署的請求，並在定義的過期時間之前接受這些請求。預先簽章 URLs 的常見使用案例是透過共用這些請求來擴展對物件或資源的存取。共用預先簽章請求是由有權執行特定請求的系統或使用者產生，然後可以傳送給其他系統或使用者，以擴展執行相同請求的能力。

在本指南中，您將學習：

- 預先簽章 URLs的概念
- 預先簽章 URLs的使用案例
- 建議和選用的護欄
- 監控選項
- AWS 服務 如何使用預先簽章 URLs的範例

目標對象

本指南面向負責在 AWS 雲端中實作安全控制的架構師和安全工程師。

目標

身為安全工程師，您想要了解解決方案建置器如何實作安全性，以及最終使用者的存取類型。本指南涵蓋一種存取類型，預先簽章URLs，通常與 Amazon S3 搭配使用。預先簽章URLs 為建置器提供可有效橋接身分驗證機制的選項。

在 Amazon S3 中，預先簽章URLs 代表唯一的請求類別。安全工程師可以監控和管理這些請求，以確保僅在適當且必要的情況下使用它們。本指南的目標是協助安全工程師提供這種類型的高階監督。

閱讀本指南後，您應該了解什麼是預先簽章的 URL、通常使用的時間，以及使用它的動機。

先決條件

如果您的公司尚未定義安全政策、控制目標或標準，如在 AWS 上實作安全控制指南所述，建議您先完成這些控管任務，再繼續本指南。

開始之前，您也應該熟悉控制和監控的建議和選用最佳實務。如需詳細資訊，請參閱：

- 服務控制政策 (AWS Organizations 文件）
- 資源控制政策 (AWS Organizations 文件）
- Amazon S3 的儲存貯體政策 (Amazon S3 文件）
- 使用伺服器存取記錄來記錄請求 (Amazon S3 文件）
- 使用 記錄 Amazon S3 API 呼叫 AWS CloudTrail (Amazon S3 文件）

預先簽章URLs 概觀

預先簽章的 URL 是一種 HTTP 請求，由 AWS Identity and Access Management (IAM) 服務識別。這類請求與所有其他 AWS 請求的差異在於 X-Amz-Expires 查詢參數。如同其他已驗證的請求，預先簽章的 URL 請求包含簽章。對於預先簽章的 URL 請求，此簽章會在 中傳輸`X-Amz-Signature`。簽章使用 Signature 第 4 版密碼編譯操作來編碼所有其他請求參數。

> **備註**
>
> - Signature 第 2 版目前正在淘汰，但有些版本仍然支援。 AWS 區域本指南適用於 Signature 第 4 版簽署。
> - 接收服務可以處理未簽署的標頭，但該選項的支援有限且具有目標性，符合最佳實務。除非另有說明，否則假設必須簽署所有標頭，才能接受請求。

`X-Amz-Expires` 參數允許將簽章處理為有效，且與編碼日期時間的偏差較大。仍會評估簽章有效性 的其他層面。 如果是暫時的，則簽署憑證在處理簽章時不得過期。簽署憑證必須連接到在處理時具有足夠授權的 IAM 主體。

預先簽章URLs 是預先簽章請求的子集

預先簽章的 URL 不是未來簽署請求的唯一方法。Amazon S3 也支援 POST 請求，這些請求通常也會預先簽章。預先簽章的 POST 簽章允許上傳符合已簽章政策，且具有內嵌在該政策中的過期日期。

請求的簽章可以是未來的日期，雖然這不常見。 只要基礎登入資料有效，簽章演算法就不會禁止未來的日期。 不過，在它們的有效時間時段之前，這些請求都無法成功處理，這使得未來日期對大多數使用案例來說是不切實際的。

預先簽章的請求允許什麼？

預先簽章的請求只能允許用於簽署請求的登入資料所允許的動作。如果登入資料隱含或明確拒絕預先簽章請求指定的動作，則傳送預先簽章請求時會遭到拒絕。這適用於下列項目：

- 與登入資料相關聯的工作階段政策
- 與登入資料相關聯之主體相關聯的身分型政策
- 影響工作階段或主體的資源政策
- 影響工作階段或主體的服務控制政策
- 影響工作階段或主體的資源控制政策

使用預先簽章請求的動機

身為安全工程師，您應該了解什麼會促使解決方案建置器使用預先簽章URLs。 了解必要項目和選用項目可協助您與解決方案建置器通訊。動機可能包括下列項目：

- 支援非 IAM 身分驗證機制，同時受益於 Amazon S3 中的可擴展性。核心動機是直接與 Amazon S3 通訊，以受益於此服務提供的內建可擴展性。如果沒有此直接通訊，解決方案將需要支援在 PutObject 和 GetObject 呼叫中重新傳輸位元組的負載。根據總負載，此需求會增加解決方案建置器可能想要避免的擴展挑戰。

  其他直接與 Amazon S3 通訊的方法，例如在 URLs 外部使用臨時登入資料 AWS Security Token Service (AWS STS) 或 Signature 第 4 版簽章，可能不適用於您的使用案例。Amazon S3 透過 AWS 登入資料識別使用者，而預先簽章的請求則假設透過 AWS 登入資料以外的機制進行識別。消除此差異，同時維持資料的直接通訊可透過預先簽章的請求實現。
- 受益於瀏覽器對 URLs 的原生理解。瀏覽器會了解 URLs，而 AWS STS 登入資料和 Signature 第 4 版簽章則不會。這在與瀏覽器型解決方案整合時很有幫助。替代解決方案需要更多程式碼、將更多記憶體用於大型檔案，並且可能會受到惡意軟體和病毒掃描器等延伸模組的不同處理。

與臨時 AWS STS 登入資料的比較

暫時登入資料類似於預先簽章的請求。 它們都會過期，允許存取範圍，並且通常用於將非 IAM 登入資料橋接到需要 AWS 登入資料的用量。

您可以緊密地將臨時 AWS STS 憑證範圍限定為單一 S3 物件和動作，但這可能會導致擴展挑戰，因為 AWS STS APIs具有限制。（如需詳細資訊，請參閱 AWS re：Post 網站上的文章如何解決 IAM 和 的 API 限流或「超過速率」錯誤 AWS STS。）此外，每個產生的登入資料都需要 AWS STS API 呼叫，這會增加延遲和可能影響彈性的新相依性。 臨時 AWS STS 登入資料也具有最短 15 分鐘的過期時間，而預先簽章的請求可以支援較短的持續時間。(60 秒在適當的條件下是可行的。)

與僅簽章解決方案的比較

預先簽章請求的唯一固有秘密元件是其簽章第 4 版簽章。 如果用戶端知道請求的其他詳細資訊，並提供符合這些詳細資訊的有效簽章，則可以傳送有效的請求。如果沒有有效的簽章，就無法。

預先簽章URLs 和僅簽章解決方案在密碼編譯上類似。不過，僅限簽章的解決方案具有實際優勢，例如能夠使用 HTTP 標頭而非查詢字串參數來傳輸簽章（請參閱記錄互動和緩解章節)。 管理員也應考慮查詢字串更常被視為中繼資料，而標頭則較不常被視為中繼資料。

另一方面， AWS SDKs 對直接產生和使用簽章的支援較少。建置僅限簽章的解決方案需要更多自訂程式碼。從實際的角度來看，使用程式庫而非自訂安全程式碼是一般最佳實務，因此僅限簽章解決方案的程式碼需要額外的審查。

僅簽章解決方案不會使用`X-Amz-Expires`查詢字串，也不會提供明確的有效期間。IAM 會管理沒有明確過期時間之簽章的隱含有效期間。這些隱含期間不會發佈。它們通常不會變更，但以安全為考量進行管理，因此您不應倚賴有效期間。明確控制過期日期與讓 IAM 管理過期之間 存在權衡。

身為管理員，您可能偏好純簽章解決方案。不過，從實際意義上來說，您需要支援建置的解決方案。

識別預先簽署的請求

識別使用預先簽署 URL 的要求

Amazon S3 提供兩種內建機制，用於監控請求層級的使用情況：Amazon S3 伺服器存取日誌和 AWS CloudTrail 資料事件。 這兩種機制都可以識別預先簽署的 URL 用法。

若要篩選預先簽署 URL 使用情況的記錄檔，您可以使用驗證類型。對於伺服器存取日誌，請檢查「身份驗證類型」欄位，在 Amazon A thena 表格中定義時，該欄位通常稱為 authtype。對於 CloudTrail，請AuthenticationMethod在`additionalEventData`欄位中檢查。在這兩種情況下，使用預先簽署 URL 的要求的欄位值都是`QueryString`，而`AuthHeader`大多數其他要求的值則為。

`QueryString`使用情況並不總是與預先簽署的 URL 相關聯。若要將搜尋限制為僅使用預先簽署的 URL，請尋找包含查詢字串參數`X-Amz-Expires`的要求。對於伺服器存取記錄檔，請檢查要求 URI，並尋找查詢字串中具有`X-Amz-Expires`參數的要求。 對於 CloudTrail，檢查`requestParameters`元素的`X-Amz-Expires`元素。

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

下列 Athena 查詢會套用此篩選器：

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

對於 AWS CloudTrail Lake，下列查詢會套用此篩選器：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

識別其他類型的預先簽署請求

POST 請求也具有唯一的身份驗證類型`HtmlForm`，在 Amazon S3 伺服器存取日誌和 CloudTrail. 此驗證類型較不常見，因此您可能無法在環境中找到這些要求。

下列 Athena 查詢會套用篩選器`HtmlForm`：

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

對於 CloudTrail Lake，下列查詢會套用篩選條件：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

識別請求模式

您可以使用上一節中討論的技巧來尋找預先簽署的要求。但是，為了使該數據有用，您需要查找模式。查詢的簡單TOP 10結果可能會提供深入分析，但如果這還不夠，請使用下表中的分組選項。

分組選項	伺服器存取記錄	CloudTrail湖	Description
使用者代理	`GROUP BY useragent`	`GROUP BY userAgent`	此分組選項可幫助您找到請求的來源和目的。用戶代理是用戶提供的，並且作為身份驗證或授權機制不可靠。但是，如果您正在尋找模式，它可能會顯示很多信息，因為大多數客戶端使用至少部分人類可讀的唯一字符串。
要求者	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	此分組選項可協助尋找簽署請求的 IAM 主體。如果您的目標是封鎖這些要求或為現有要求建立例外狀況，這些查詢會針對此目的提供足夠的資訊。當您按照 IAM 最佳實務使用角色時，該角色具有明確識別

分組選項	伺服器存取記錄	CloudTrail湖	Description
			的擁有者，您可以使用這些資訊來瞭解更多資訊。

分組選項	伺服器存取記錄	CloudTrail湖	Description
來源 IP 位址	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	在到達 Amazon S3 之前，此選項會按最後一個網路翻譯躍點進行分組。 • 如果流量通過 NAT 閘道，這將是 NAT 閘道位址。 • 如果流量通過網際網路閘道，這將是將流量傳送到網際網路閘道的公用 IP 位址。 • 如果流量來自外部 AWS，這將是與來源相關聯的公共互聯網地址。 • 如果它經過閘道虛擬私人雲端 (VPC) 端點，這將是 VPC 中執行個體的 IP 位址。 • 如果它通過公用虛擬界面 (VIF)，這將是請求者的內部部署 IP 或任何中介，例如僅公開其 IP 位址的 Proxy 伺服器或防火牆。

分組選項	伺服器存取記錄	CloudTrail湖	Description
			• 如果它經過介面 VPC 端點，這可能是 VPC 中執行個體的 IP 位址。它也可以是來自其他 VPC 或內部部署網路的 IP 位址。與公用 VIF 一樣，這可能是任何中介人的 IP 位址。 如果您的目標是強加網路控制，則此資料非常有用。您可能必須將此選項與諸如`endpoint`（用於服務器訪問日誌）或`vpcEndpointId`（用於 CloudTrail Lake）之類的數據結合使用以澄清來源，因為不同的網絡可能會複製私有 IP 地址。
S3 儲存貯體名稱	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	此分組選項有助於尋找收到請求的值區。這可協助您識別例外狀況的需求。

使用預先簽章請求的最佳實務

本節討論使用安全工程師應考慮的預先簽章請求的最佳實務。這些準則包括：

- 基礎最佳實務，這是每個組織應遵循的實務。
- 其他護欄，這是您應該考慮的實務，但可能會決定實作部分或例外狀況。這些旨在提供更深入的控制和防禦，但應與整體複雜性平衡。
- 記錄互動，這可能是由您或客戶在共同責任模型中的責任一部分的裝置或服務所造成。本節包含預防措施，以限制可透過日誌存取的資訊。

基礎最佳實務

其他 AWS API 請求的有效控制的一般最佳實務也適用於預先簽章的請求。本節會檢閱兩個最相關的實務：最低權限和資料周邊。這些實務可建立其他實務延伸的控制深度。

套用最低權限準則

一般而言，限制使用預先簽章請求的第一步是限制對 Amazon S3 的存取。預先簽章的 URL 無法提供未授予產生預先簽章 URL 之簽章的委託人之資源的存取權。也無法以未授予該委託人的方式提供資源的存取權。因此，套用最佳實務來授予這些委託人最低權限是有效的護欄。

建立預先簽章 URL 的程序是一種演算法操作，以用於產生簽章的已發佈標準（簽章第 4 版）為基礎。因此，您無法限制產生預先簽章URLs。不過，為了相關，預先簽章的 URL 必須是有效的，並提供 資源的存取權，因此預先簽章的 URL 的有效性也是有效的護欄。

如需最低權限的詳細資訊，請參閱 AWS Well-Architected Framework 安全支柱中的授予最低權限存取權。

實作資料周邊

最低權限的延伸是維護符合組織需求的資料周邊。預先簽章URLs 與資料周邊相容。 如同其他請求，預先簽章的 URL 請求的有效性會在請求時間進行評估。如果網路、資源、角色工作階段和主體的屬性變更，則會在接收請求時使用 方法進行評估。

例如，假設在 Amazon Elastic Kubernetes Service (Amazon EKS) 容器中執行的服務簽署請求。請求稍後會從連線至網際網路的使用者個人電腦系統傳送。在此情況下，aws：SourceIp 條件會從使用者的個人系統評估請求的可見公有 IP 地址，而不是 Amazon EKS 容器中的服務 IP 地址。

同樣地，如果主體或資源的標籤在傳送請求之前發生變更，則更新而非原始值將透過 aws：PrincipalTag/tag-key 和 aws：ResourceTag/tag-key 條件套用至請求。

其他護欄

當解決方案建置者和使用者適當使用預先簽章的請求時，它們會提供安全機制，讓使用者存取資料。此外，產生預先簽章請求的能力不會為委託人提供他們尚未擁有的存取權。

在這種情況下，是否需要額外的控制？ 其他控制項的理由並非基於需要拒絕存取，而是提供監控功能、核准用量和設定界限，以及降低使用者錯誤的風險。透過這種方式，您可以協助確保用量是適當且必要的。

下列護欄可協助您實現此目標。在啟用這些控制項之前，您可能想要透過識別預先簽章的請求來判斷現有的用量。此識別可協助您準備護欄對現有用量的影響，或視需要規劃例外狀況。

s3：signatureAge 的護欄

預先簽章請求的一個定義特徵是它們描述過期時間。請求的簽章包含日期。此日期會以預先簽章 URLs 的`X-Amz-Date`查詢字串參數傳輸，並以預先簽章 POST 的日期或 x-amz-date 標頭傳輸。

Amazon S3 提供條件金鑰 s3：signatureAge，可用來限制簽署日期與請求有效過期之間的最長時間。此條件永遠不會增加有效期間，但可以減少有效期間。

在下列政策中，`s3:signatureAge`條件索引鍵會將預先簽章的請求限制為 15 分鐘的有效時間。下列範例全都使用 15 分鐘，將有效性限制為與標準簽署支援類似的時間範圍。

政策的第二個陳述式拒絕任何 Signature 第 2 版存取。此版本的簽署通訊協定已被取代，但在某些 中仍然支援 AWS 區域。我們建議您在完全棄用之前明確封鎖它。

您可以套用下列政策做為 AWS Organizations 服務控制政策 (SCP)。只要簽章產生和用量之間的時間少於 15 分鐘，使用者仍然可以使用預先簽章的請求並部署相依於這些請求的解決方案。視實作而定，此限制可能沒有任何影響、可能導致解決方案無法使用，或可能導致偶爾重試的失敗。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

例外狀況

如果解決方案在過期前需要較長的時間，因此受到上述政策的影響，建議您提供核准例外狀況的方法。若要避免在 SCP 中列舉例外狀況，請使用 aws：PrincipalTag，如下列政策所示，以可擴展的方式管理例外狀況。其他 AWS 範例，例如 AWS 資料周邊政策範例，請使用此策略。

如果您使用 實作例外狀況政策`aws:PrincipalTag`，則必須控制在委託人上設定標籤的存取權。此類型的標籤可以直接來自委託人，並且可以由 SCP 控制，如控制可以設定哪些標籤值的這個範例所示。此類型的標籤也可以來自工作階段標籤，這些標籤是由身分提供者 (IdP) 或使用 時所設定 AWS STS。控制對 的存取`aws:PrincipalTag`是一個複雜的主題。不過，具有屬性型存取控制 (ABAC) 使用經驗的組織，將擁有經驗和控制項，可`aws:PrincipalTag`針對此使用案例適當使用 。

在下列範例中， `aws:PrincipalTag`條件會建立例外狀況，以允許任何已指派具名標籤 (`long-presigned-allowed`) 且設定為 的委託人`true`。在此情況下，不會套用對簽章存留期的限制。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

儲存貯體政策

您可以使用政策將儲存貯體政策套用至所有或選取的儲存貯體，如下列範例所示。與 SCP 不同，儲存貯體政策也會以服務主體用量為目標。附錄 A 不會記錄預先簽章請求的任何預期服務主體用量，但如果您想要實作控制項來證明該限制，下列政策會提供該控制項。此外，與 SCP 不同，儲存貯體政策可以套用至您管理帳戶中的主體。

ABAC 型例外狀況在儲存貯體政策中的運作方式與 SCP 相同。儲存貯體政策的目標可能是適用於組織外部的委託人，因此 ABAC 例外狀況應限於適用 ABAC 控制的委託人。

在下列範例中，第一個陳述式中的 `aws:PrincipalTag`條件會為已指派具名標籤 (`long-presigned-allowed`) 且設定為 的委託人建立例外狀況`true`。在此情況下，不會套用對簽章存留期的限制。第二個陳述式會將此限制套用至組織外部 AWS 擁有儲存貯體的所有委託人。第二個陳述式的範圍應與 ABAC 控制項相符，以設定主體的具名標籤。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
```

```
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

資源控制政策

您可以使用資源控制政策 (RCPs) 大規模將政策套用至儲存貯體。與 SCPs和與儲存貯體政策不同，RCPs不會以服務主體用量為目標。RCPs會影響任何帳戶中的非服務主體，但不會影響管理帳戶中的資源。如需詳細資訊，請參閱 AWS Organizations 文件。

如同儲存貯體政策，如果您使用 `aws:PrincipalTags`為委託人建立例外狀況，請記住標記委託人的 ABAC 控制範圍。

下列 RCP 會將組織中所有 S3 儲存貯體的預先簽章 URL 用量限制為 15 分鐘。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
```

```
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true",
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

s3：authType 的護欄

預先簽章URLs 使用查詢字串身分驗證，而預先簽章POSTs 一律使用 POST 身分驗證。Amazon S3 支援透過 s3：authType 條件金鑰根據身分驗證類型拒絕請求。 REST-QUERY-STRING 是查詢字串s3:authType的值，而 POST是 POST s3:authType的值。

您可以套用下列政策做為 SCP。政策使用 s3:authType只允許以標頭為基礎的身分驗證。它也會設定 方法，為個別使用者或角色提供例外狀況。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

根據身分驗證類型拒絕請求會影響使用拒絕身分驗證類型的任何解決方案或功能。例如，拒絕REST-QUERY-STRING可防止使用者從 Amazon S3 主控台執行上傳或下載。如果您希望使用者使用 Amazon S3 主控台，請勿使用此護欄，或對使用者進行例外處理。另一方面，如果您不希望使用者使用 Amazon S3 主控台，您可以拒絕 REST-QUERY-STRING 使用者。

也許您已經拒絕使用者直接存取 Amazon S3 資源。在這種情況下，身分驗證類型的護欄是多餘的。不過，s3:authType拒絕陳述式提供defense-in-depth公用程式，因為拒絕直接存取的實作通常跨越許多控制陳述式，有些則例外。

用於工作負載的角色通常不需要存取查詢字串或POST身分驗證。例外狀況是支援使用預先簽章請求之服務的角色。您可以為這些角色建立特定例外狀況。

您也可以使用如下所示的政策，將儲存貯體政策套用至所有或選取的儲存貯體：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
```

```
}
```

此儲存貯體政策具有拒絕使用 CopyObject 和 UploadPartCopy APIs 進行跨區域複製的效果。Amazon S3 複寫不受影響，因為它不依賴這些 APIs。

如果您想要使用儲存貯體政策，例如上述政策，但仍支援跨區域 CopyObject 或 UploadPartCopy API，請新增 的條件，`aws:ViaAWSService`如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

結合預先簽章的護欄和其他護欄的例外狀況

如果您不打算將護欄一般套用到您的使用者和角色，建議您將其套用到其他常見護欄的例外狀況，因此這些例外狀況不支援預先簽章的請求。

如果您有網路限制，但允許外部合作夥伴的例外狀況或特殊使用案例，您應該在套用這些例外狀況時封鎖查詢字串或`POST`身分驗證，除非特別將其識別為必要。

s3：signatureAge 的限制

管理員會發現`s3:signatureAge`更完整地了解 的影響非常有用。每個已簽署的請求都包含 `X-Amz-Date`，這應該表示目前的時間。此值由用戶端填入，並請求 signer. AWS rejects 認為具有無效時間的

請求。不過，簽署者可以在未來的時間預先產生簽章。如果傳送時間過早，Amazon S3 會拒絕指定未來時間的請求。不過，如果請求在登入簽章之前不會傳送，則可以更早產生並稍後傳送簽章。

s3:signatureAge 只會針對預先簽章的請求限制簽章X-Amz-Date中 的最長存留期。 即使過期時間超過指定的存留期，或X-Amz-ExpiresPOST政策已宣告有效， 仍會拒絕請求。 s3:signatureAge不會變更未包含明確過期的請求的有效期間。它也不會控制用戶端用於簽章X-Amz-Date的 值。

如果系統時鐘錯誤，或用戶端刻意提出未來日期請求，簽署時間可能不是產生簽章的時間。 這會限制s3:signatureAge控制解決方案的程度。產生簽章時使用目前時間的解決方案會以預期的方式受到限制：簽章在 中指定的毫秒數內仍然有效s3:signatureAge。不使用目前時間 的解決方案會有不同的限制。其中一個限制是用來簽署簽章的登入資料仍然有效。身為管理員，您可以控制發行的臨時登入資料的最大有效性。 您可以允許登入資料有效長達 36 小時，或將有效性限制為低至 15 分鐘。臨時登入資料 過期不取決於 的值X-Amz-Date。

永久登入資料沒有此限制。 僅使用臨時登入資料是最佳實務，您可以明確撤銷任何永久登入資料，這也會使根據該登入資料的任何簽章失效。

雖然 s3:signatureAge 是以毫秒為單位進行測量，但即使您有良好的同步時鐘和低延遲用量，也無法將其設定為少於 60 秒。低於 60 秒 的設定具有拒絕有效請求的風險。如果您預期簽章產生和請求提交之間的延遲，或時鐘同步問題，您應該在 的管理中考慮這些問題s3:signatureAge。

大規模鎖定儲存貯體

SCPs和 RCPs可以使用 aws:PrincipalTag 為使用者進行例外狀況。您無法在儲存貯體上使用標籤來透過 aws:ResourceTag– 僅物件標籤來控制存取。 為您要套用此控制項的每個物件新增標籤通常無法擴展。

適合許多使用案例的解決方案是在帳戶層級套用政策和例外狀況，方法是變更 SCP 或 RCP 套用的帳戶，或使用 aws：ResourceAccount、aws：ResourceOrgPaths 或 aws：ResourceOrgID。例如，SCP 或 RCP 可能會套用至一組生產帳戶。

另一個解決方案是使用自訂 AWS Config 規則來實作偵測性控制或回應式控制。目標是讓每個儲存貯體都包含具有適當護欄的儲存貯體政策。除了測試儲存貯體政策的內容之外，自訂 AWS Config 規則還可以從儲存貯體擷取標籤，如果儲存貯體標記了特定值，則從規則中排除儲存貯體。如果該規則未通過其合規檢查，則可以將儲存貯體標記為不合規，或叫用修復，將護欄新增至儲存貯體的政策。

> **Note**
>
> 您無法限制 PutBucketTagging 請求的標籤內容。若要維持對儲存貯體標籤方式的控制，您必須限制對 PutBucketTagging和 DeleteBucketTagging 的存取。

記錄互動和緩解措施

預先簽章的 URL 包含簽章，可在過期前的期間內用來執行其簽署的特定 API 操作。它應該被視為臨時存取憑證。只有需要知道的一方才能保持簽章的私密性。在大多數環境中，這是傳送請求的用戶端和接收請求的伺服器。將簽章作為直接 HTTPS 工作階段的一部分來傳送簽章會維護其私有性質，因為只有 HTTPS 工作階段的參與者才能查看傳輸簽章的 URI。

對於預先簽章URLs，簽章會傳輸為`X-Amz-Signature`查詢字串參數。查詢字串參數是 URI 的元件。風險是用戶端可以記錄 URI 和簽章。用戶端可以存取整個 HTTP 請求，並可記錄請求、資料和標頭的任何部分（包括身分驗證標頭）。不過，這是較不常見的慣例。URI 記錄比較常見，在存取記錄等情況下是必要的。在記錄 URIs之前，用戶端應使用修訂或遮罩來移除簽章。

在某些環境中，使用者允許中介裝置（代理）取得其 HTTPS 工作階段的可見性。啟用代理需要對用戶端系統進行高層級的特權存取，因為它們需要組態和信任的憑證。在用戶端中介環境的本機內容中安裝代理組態和信任的憑證，可允許非常高層級的權限。因此，應嚴格控制對這類中介裝置的存取。

中介裝置的用途通常是封鎖不需要的輸出，並追蹤其他輸出。因此，這類中介裝置通常會記錄請求。雖然中介裝置可以像用戶端一樣記錄任何內容、標頭和資料（所有內容都非常敏感），但他們更常記錄 URIs，例如包含`X-Amz-Signature`查詢字串參數的 URI。

緩解措施

我們建議 URI 記錄會修訂`X-Amz-Signature`查詢字串參數、修訂整個查詢字串，或將資訊視為高度機密，就像直接存取中介伺服器一樣。雖然強烈建議這些保護，但預先簽章URLs 過期的事實可降低日誌暴露的風險，只要暴露時間延遲到足以讓簽章過期的時間。

Amazon S3 也會看到簽章，且必須妥善處理。Amazon S3 伺服器存取日誌包含請求 URI`X-Amz-Signature`，但會依建議修改 。為 Amazon S3 記錄 CloudTrail 資料事件時也是如此。 您可以使用自訂資料識別符設定 Amazon CloudWatch Logs 來遮罩資料。 https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL-custom-data-identifiers.html

下列規則表達式符合 URI 中顯示的 `X-Amz-Signature` ：

```
X-Amz-Signature=[a-f0-9]{64}
```

以下規則表達式新增分組模式，以識別要更具體取代的文字：

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

如果您有如下的存取日誌項目：

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

第一個規則表達式會將存取日誌項目轉譯為：

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

在支援非擷取群組的系統上，第二個規則表達式會將存取日誌項目轉譯為：

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

常見問答集

是否可以多次使用預先簽章的請求？ 這是安全風險嗎？

是，預先簽章請求中的簽章可以多次使用。這是否為安全風險是情境式問題。存取 AWS 服務的其他方法也允許重複。具有 AWS 登入資料的使用者或工作負載可以將許多請求傳送至 AWS 服務，而這些請求中的任何一個都可能是重複的。

如果您的使用案例只需要執行一次，您應該實作其他機制來強制執行單次使用。單次使用不是預先簽章請求的功能。身為安全工程師，您應該檢閱使用案例和實作，但在許多情況下，多次使用將適合可接受的使用。

預期使用者以外的人員是否可以使用預先簽章的請求？

預先簽章請求中的簽章可由擁有該請求的任何人傳送。只有在它通過其他形式的驗證，例如資料周邊控制時，才會接受它。如果簽章已過期、簽署憑證已過期，或簽署憑證無法存取請求的資源，則會拒絕請求。

對於使用 驗證的其他方法也是如此 AWS 服務。不當共用的登入資料允許不當存取。核心最佳實務是僅與預期對象共用登入資料和簽章。如果您無法信任目標對象保護私有資料的安全，也無法與他人共用，這將破壞任何形式的身分驗證。

授權使用者是否可以使用預先簽章的請求來竊取資料？

保護資料需要強大的動作。為預期目的啟用存取，同時維護資料周邊需要全方位的方法。 最低權限存取、資料周邊控制，以及僅使用臨時存取登入資料，都是適用於保護資料的一般最佳實務。適當使用這些控制項也會限制使用者透過其產生的預先簽章請求執行動作的能力。

這是因為預先簽章請求提供的存取權是授予登入資料的存取子集，該登入資料用於簽署請求。在這種情況下，適用於存取資料的最佳實務通常適用於預先簽章的請求，但預先簽章的請求不會建立新的資料存取。

- 過期上限僅限於簽署憑證的過期。 如果撤銷簽署憑證，根據憑證的簽章將不再有效。
- 如果與簽署憑證相關聯的 IAM 主體許可不包含執行與預先簽章請求相關聯的動作，則調用預先簽章請求會導致「存取遭拒」回應。 回應取決於調用時的目前許可狀態，這與產生預先簽章請求簽章的時間無關。

- 委託人的屬性會根據與簽署憑證相關聯的委託人進行評估。
- 角色工作階段的屬性會根據與簽署憑證相關聯的角色工作階段進行評估。
- 網路的屬性會根據接收請求的方式進行評估，就像一般請求一樣。

在這種情況下，與預先簽章請求相關的風險檢查僅限於使用與使用者登入資料不同的登入資料進行簽署的區域，並提供不屬於使用者主體的存取。此檢查應套用至服務的設計、工作負載或代表使用者產生簽章的解決方案，而非預先簽章的請求功能本身。

如果我懷疑有人以未經授權的方式共用，是否可以拒絕來自預先簽章 URL 的存取？

是。這需要使 URL 登入的登入資料失效。有多種方法可以完成此操作：

- 從登入資料所屬的 IAM 主體移除許可。如果該 IAM 主體不再能夠存取 URL 簽署的資源和操作，則 URL 無法執行該操作。這會影響來自該 IAM 主體的所有相符使用。
- 如果用來簽署 URL 的登入資料是臨時 AWS STS 登入資料，您可以撤銷在 IAM 主體特定時間之前發行的臨時登入資料的工作階段許可。根據使用案例，可能有其他有效的工作階段在正常過期時間之前失效，但新工作階段不會受到影響。撤銷工作階段許可也會使使用與這些工作階段相關聯的登入資料所簽署的任何 URLs 失效，但與新工作階段相關聯的新 URLs 不會受到影響。
- 如果用來簽署 URL 的登入資料是永久登入資料，請停用存取金鑰。這會影響與這些登入資料相關的所有用量。

資源

Amazon S3 文件

- 驗證請求（AWS 簽名版本 4）
- 驗證要求：使用查詢參數 (AWS 簽章版本 4)
- 驗證請求：使用 POST 進行瀏覽器上傳（AWS 簽名版本 4）
- Amazon S3 簽名版本 4 身份驗證特定政策金鑰
- 使用預先簽署的 URL

其他參考

- 在 AWS 上建立資料周邊 (AWS 白皮書)
- SEC03-BP02 授予最低權限訪問權限（架構AWS 良好的框架，安全性支柱）
- SEC03-BP05 為您的組織定義許可護欄（架構AWS 良好的框架，安全性支柱）

附錄 A： AWS 服務 如何使用預先簽章URLs

此附錄提供使用預先簽章 URLs AWS 服務 和 功能的相關資訊。此資訊有兩種用途：

- 為實作控制項的安全工程師提供這些控制項可能影響的資訊。
- 建立此風險可能與 URL 記錄互動相關的情況意識。

> **Important**
>
> 此附錄不提供預先簽章 URLs 的完整清單 AWS 服務 或其使用方式。它也不涵蓋自訂或第三方解決方案。

Amazon S3 主控台

主體：主控台使用者

預設過期時間：5 分鐘

> **免責聲明**
>
> 本節記錄 Amazon S3 console. AWS console 行為的目前行為可能會有所變更，恕不另行通知。

Amazon S3 主控台支援下載和上傳物件。 下載使用過期時間為 300 秒 (5 分鐘） 的預先簽章 URL。 URL 是由對 的請求產生`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`。

該請求會在使用者按一下下載按鈕時啟動，因此 URL 不會預先產生或傳送至用戶端，直到發生明確的下載請求為止。

上傳類似，但主控台會傳送兩個請求：`OPTIONS`做為預檢 CORS 檢查，以及 PUT。 這兩個請求都使用相同的簽章。

用於簽署的登入資料是與目前登入使用者相關聯的臨時登入資料。取得這些臨時登入資料的方法 詳細資訊超出本指南的範圍。

Amazon S3 Object Lambda

主體：存取點呼叫者

預設過期時間：61 秒

> **Note**
>
> 自 2025 年 11 月 7 日起，S3 Object Lambda 僅適用於目前正在使用該服務的現有客戶，以及 select AWS Partner Network (APN) 合作夥伴。對於類似 S3 Object Lambda 的功能，請在此處進一步了解 – Amazon S3 Object Lambda 可用性變更。

Amazon S3 Object Lambda 使用 AWS Lambda 函數自動處理和轉換從 Amazon S3 擷取的資料。當 S3 Object Lambda 叫用函數時，該函數會收到預先簽章的 URL (`inputS3Url`)，可用來從支援的存取點下載原始物件。

這些預先簽章URLs 會針對支援的 Amazon S3 存取點簽署，該存取點會在您設定 S3 Object Lambda 時提供。（這與 Object Lambda 存取點不同。）與其使用繫結至 Lambda 函數的角色，URL 是使用原始發起人的身分來簽署的，而該使用者的許可在使用 URL 時將套用。如果 URL 中有已簽章的標頭，Lambda 函數必須在對 Amazon S3 的呼叫中包含這些標頭。

傳回的預先簽章 URL 的過期時間為 61 秒（比 S3 Object Lambda 函數的最長持續時間多一秒）。產生的 URL 只能與支援的存取點搭配使用。S3 Object Lambda 存取點的發起人需要能夠存取此存取點。您可以使用條件 限制對 S3 Object Lambda 內容的存取`"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]`。當該條件連接到支援的存取點或儲存貯體時，使用者無法直接存取支援的存取點或儲存貯體。

此方法的值是，不需要將 Lambda 函數存取權授予 S3 儲存貯體或存取點。與 Lambda 函數相關聯的角色將需要 WriteGetObjectResponse 的許可，但不需要 GetObject 的許可。

當 S3 Object Lambda 產生預先簽章URLs 時，不會新增網路限制，因此 URL 可以在 Lambda 函數之外使用。不過，對 S3 Object Lambda 發起人施加的任何限制仍然適用。例如，如果您的 Lambda 函數在 VPC 中執行，且您將發起人限制為使用 VPC 端點，則擁有預先簽章 URL 的任何人都需要能夠透過該 VPC 端點傳送。 此限制也適用於 SourceIp 和 VpcSourceIp。

> **Note**
>
> 若要在 VPC 中使用 S3 Object Lambda 函數，VPC 必須具有公有 S3 端點的路由，才能呼叫 WriteGetObjectResponse。 這並不表示使用 VPC 端點的需求不適用於從儲存貯體擷取資料的請求。

AWS Lambda 跨區域 CopyObject

委託人：AWS 內部

預設過期時間：3600 秒

當您使用 CopyObject 或 UploadPartCopy API 進行複製時 AWS 區域，Amazon S3 會在內部使用預先簽章URLs。這些 APIs可以直接從 SDKs或 AWS CLI 命令 `aws s3api copy-object`和 呼叫`aws s3api upload-part`。這些 APIs 不會用於 Amazon S3 複寫，但當來源和目的地是 S3 儲存貯體時， 和 `aws s3 sync`命令會使用這些 AWS CLI `aws s3 cp` API。它們也受到各種 AWS SDKs 中的`TransferManager`實作支援。

AWS Lambda GetFunction

Principal： AWS internal

預設過期時間：10 分鐘

AWS Lambda 會將使用者版本存放在 Lambda 團隊擁有的 S3 儲存貯體中， 在產生部署到 Lambda 容器的資產之前。當您想要存取函數的程式碼 時， 您呼叫 GetFunction API。 此 API 會以 回應`Code.Location`， 其中包含 10 分鐘內有效的預先簽章 URL （此過期時間是目前行為而非已發佈的合約）。 如果您不想要程式碼， 您可以使用 GetFunctionConfiguration、GetFunctionConcurrency、 和 ListTags，以擷取 傳回的其他資料`GetFunction`。

傳回的 URL 不會使用目前登入使用者的登入資料簽署，而是由 Lambda 代表使用者簽署。因此，套用至目前登入使用者或使用者臨時工作階段登入資料的條件金鑰 （例如 `aws:SourceIP`) 不適用於產生的 URL。無論條件金鑰僅套用至 GetFunction，或套用至使用者或工作階段的所有 AWS API 用量，都是如此。

Lambda 主控台也會使用 GetFunction 及其傳回的預先簽章 URL。 主控台會使用與目前登入使用者相關聯的臨時登入資料來呼叫 GetFunction。取得這些臨時登入資料的詳細資訊超出本文件的範圍。

Amazon ECR

Principal： AWS internal

預設過期時間：1 小時

Amazon Elastic Container Registry (Amazon ECR) 提供 GetDownloadUrlForLayer API，傳回一個預先簽章的 URL，有效期為一小時，並支援從 Amazon ECR 映像下載單一層。不過，Amazon ECR 代理會使用此操作，使用者通常不會使用此操作來提取和推送映像。

Amazon Redshift Spectrum

委託人：透過 傳遞給 CREATE EXTERNAL SCHEMA 的角色 `IAM_ROLE`

預設過期時間：1 小時

Amazon Redshift Spectrum 在內部使用預先簽章URLs，並禁止對儲存貯體和 Amazon Redshift 角色組合的限制，這會限制預先簽章URLs。 您可以使用 16 分鐘`s3:signatureAge`的值，但非常低的值不可靠。您可以使用的最小值取決於查詢的時間和大小。雖然低於 16 分鐘的值適用於許多案例，但它需要測試。角色可以且應該限制為僅供 Redshift Spectrum 使用，Redshift Spectrum 不會公開其產生的 URLs，因此可以減輕較低過期值的典型理由。

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio 支援兩個 API 動作：CreatePresignedDomainUrl 和 CreatePresignedNotebookInstanceUrl。不過，這些 APIs 與 Signature 第 4 版預先簽章的 URL 功能無關。這些 APIs會建立使用 `authToken` 參數的 URL，但不支援任何標準 Signature 第 4 版查詢參數。

`authToken` 是不同的機制，但與預先簽章URLs 相似。它以查詢字串參數的形式傳送，並支援 5 分鐘的過期時間。

SageMaker AI 支援網路限制。如果您對`sagemaker:CreatePresignedDomainUrl`動作施加限制，該動作會同時套用到呼叫 CreatePresignedDomainUrl 和使用產生的 URL。如果 URL 從有效網路產生，然後由非有效網路傳送，則產生 URL 的 API 呼叫會成功，但傳送 URL 的請求會失敗。CreatePresignedNotebookInstanceUrl 和 `sagemaker:CreatePresignedNotebookInstanceUrl`動作也是如此。

如需詳細資訊，請參閱 SageMaker AI 文件。

附錄 B：預先簽章 URLs的控制項如何影響 AWS 服務

此附錄說明 AWS 服務 使用預先簽章 URLs 與本指南先前所述的控制項之間的互動，如附錄 A 所述。

s3：signatureAge 的護欄

Amazon S3 主控台不會因為`s3:signatureAge`條件索引鍵設定的 5 分鐘最大過期而中斷。當您選擇下載按鈕並套用自己的 5 分鐘過期時間時， Amazon S3 主控台會產生預先簽章URLs。少於 2 分鐘的最長持續時間可能會根據時鐘同步和延遲產生隨機失敗。

Amazon S3 Object Lambda 使用 61 秒的過期時間，因此在 61 秒以上的`s3:signatureAge`值上設定條件不會造成任何中斷。較短的持續時間可能較不可靠，並可能導致間歇性故障。

Amazon S3 跨區域 CopyObject 不會因最長過期 5 分鐘而中斷。不過，較短的持續時間可能會根據時鐘同步和延遲產生隨機失敗。

在 中 AWS Lambda，GetFunction 提供客戶帳戶外部物件的 URL，因此客戶政策不會影響產生的 URLs。

Amazon Redshift Spectrum 已經過 16 分鐘`s3:signatureAge`條件測試。不過，較短的持續時間可能會導致中斷。

不使用網路限制時的 s3：authType 護欄

Amazon S3 主控台通常受`s3:authType`護欄影響。主控台會根據本機網路組態路由至 Amazon S3。 如果本機網路路由至 Amazon S3 的方式是網路限制允許的方式，Amazon S3 主控台仍會運作。 不過，如果透過代理或公有網際網路以不允許的方式路由，則會封鎖用量。 不過，封鎖用量可能是此政策的意圖。

如果 Lambda 函數未連接到適當的 VPC，Amazon S3 Object Lambda 會受到影響。在此組態 中，VPC 必須具有 NAT 閘道，而不是存取 S3 儲存貯 體，而是呼叫 WriteGetObjectResponse。

如果將此護欄套用至儲存貯體政策，而沒有建議的例外狀況，則 Amazon S3 跨區域 CopyObject 會中斷`aws:viaAWSService`。

除非使用增強型 VPC `s3:authType` 路由，否則 Amazon Redshift Spectrum 會受到護欄影響。目前，Redshift Spectrum 僅支援使用無伺服器叢集的增強型 VPC 路由，不支援佈建叢集。

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
更新和說明	在其他護欄區段中，新增了RCPs和釐清的例外狀況。	2025 年 8 月 8 日
初次出版	—	2024 年 7 月 23 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。