建立或修改存取原則聲明
ONTAP 9

NetApp
February 12, 2026

目錄

建立或修改存取原則聲明

瞭解 ONTAP S3 儲存區和物件儲存區伺服器原則

使用者和群組對S3資源的存取權是由儲存區和物件存放區伺服器原則所控制。如果您的使用者或群組數量不多、在庫位層級控制存取可能就足夠了、但如果您有許多使用者和群組、則更容易控制物件庫伺服器層級的存取。

將存取規則新增至預設的 ONTAP S3 儲存區原則

您可以將存取規則新增至預設的儲存區原則。其存取控制的範圍是包含貯體的範圍、因此當有單一貯體時、最適合使用此功能。

開始之前

已啟用 S3 的儲存 VM 必須已存在、其中包含 S3 伺服器和儲存區。

在授予權限之前、您必須先建立使用者或群組。

關於這項工作

您可以為新使用者和群組新增聲明、也可以修改現有聲明的屬性。如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket policy`資訊，請參閱。

使用者和群組權限可在建立儲存區時或稍後視需要授予。您也可以修改儲存區容量和QoS原則群組指派。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

步驟

1. 編輯儲存桶：按一下「儲存設備>儲存桶」、按一下所需的儲存桶、然後按一下「編輯」。 新增或修改權限時、您可以指定下列參數：
   - 主要：授予存取權的使用者或群組。
   - * effect*：允許或拒絕存取使用者或群組。
   - 動作：特定使用者或群組的儲存庫允許動作。
   - 資源：儲存區內已授予或拒絕存取的物件路徑和名稱。

     預設值*_bucketname_*和*_bucketname/_會授予儲存區中所有物件的存取權。您也可以授與單一物件的存取權、例如***_Bucketname/_** readme.txt*。
   - 條件（選用）：嘗試存取時會評估的運算式。例如、您可以指定允許或拒絕存取的IP位址清單。

> 從 ONTAP 9.14.1 開始、您可以在 * 資源 * 欄位中指定貯體原則的變數。這些變數是預留位置、在評估原則時會以關聯式值取代。例如、 If `${aws:username}` 會指定為原則的變數、然後此變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。

CLI

步驟

1. 在庫位政策中加入聲明：

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取
`-action`	您可以指定 `*` 表示所有動作、或是下列一或多個動作清單： `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, 和 `ListMultipartUploadParts`。
`-principal`	一或多個S3使用者或群組的清單。 • 最多可指定10個使用者或群組。 • 如果已指定 S3 群組、則該群組必須採用格式 `group/group_name`. • `*` 可以指定為公開存取、也就是說、無需存取金鑰和秘密金鑰即可存取。 • 如果未指定主體、則會授予儲存 VM 中的所有 S3 使用者存取權。

-resource	儲存區及其所包含的任何物件。萬用字元 * 和 ？可用於形成用於指定資源的規則運算式。對於資源、您可以在原則中指定變數。這些原則變數是預留位置、在評估原則時會以關聯式值取代。

您可以選擇性地指定文字字串做為的註解 -sid 選項。

範例

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定允許存取物件儲存區伺服器使用者使用者 1 的讀我資料夾。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定物件儲存區伺服器群組群組 1 的所有物件存取權。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

從 ONTAP 9.14.1 開始、您可以指定貯體原則的變數。以下範例為儲存 VM 建立伺服器儲存區原則聲明 svm1 和 bucket1`和指定 `${aws:username} 做為原則資源的變數。評估原則時、原則變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。例如、評估下列原則陳述時、${aws:username} 替換為執行 S3 作業的使用者。如果是使用者 user1 執行作業時、會授予該使用者存取權 bucket1 做為 bucket1/user1/*。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

建立或修改 ONTAP S3 物件存放區伺服器原則

您可以建立可套用至物件存放區中一或多個儲存區的原則。物件存放區伺服器原則可附加至使用者群組、因此可簡化跨多個資源區的資源存取管理。

開始之前

已啟用S3的SVM必須已存在S3伺服器和儲存區。

關於這項工作

您可以在物件儲存伺服器群組中指定預設或自訂原則、以在SVM層級啟用存取原則。原則只有在群組定義中指定之後才會生效。

使用物件儲存伺服器原則時、您可以在群組定義中指定主體（即使用者和群組）、而非在原則本身中指定主體。

有三種唯讀的預設原則可供存取ONTAP 不完整的S3資源：

- FullAccess
- NoS3 存取
- ReadOnlyAccess

您也可以建立新的自訂原則、然後為新使用者和群組新增陳述式、或是修改現有陳述式的屬性。如"指令參考資料ONTAP"需詳細 `vserver object-store-server policy`資訊，請參閱。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**建立或修改物件存放區伺服器原則

步驟

1. 編輯儲存 VM ：按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。
2. 新增使用者：按一下*原則*、然後按一下*新增*。
   a. 輸入原則名稱、然後從群組清單中選取。
   b. 選取現有的預設原則或新增原則。

      新增或修改群組原則時、您可以指定下列參數：

      - 群組：授予存取權的群組。
      - 效果：允許或拒絕存取一或多個群組。
      - 行動：特定群組的一個或多個儲存桶中允許的行動。
      - 資源：一或多個儲存區內的物件路徑和名稱、這些儲存區已授予或拒絕存取權限。 例如：
        - ***授予對儲存VM中所有儲存區的存取權。
        - * Bucketname*與* Bucketname/*可授予特定儲存區中所有物件的存取權。
        - * Bucketname/readme.txt*可讓您存取特定儲存區中的物件。
   c. 如有需要、請在現有原則中新增陳述式。

CLI

使用**CLI**建立或修改物件存放區伺服器原則

步驟

1. 建立物件儲存伺服器原則：

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. 建立原則聲明：

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取

`-action`	您可以指定 * 表示所有動作、或是下列一或多個動作清單： `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, 和 `ListMultipartUploadParts`。
`-resource`	儲存區及其所包含的任何物件。萬用字元 * 和 ? 可用於形成用於指定資源的規則運算式。

您可以選擇性地指定文字字串做為的註解 `-sid` 選項。

根據預設、新的對帳單會新增至對帳單清單的結尾、並依順序處理。稍後新增或修改說明時、您可以選擇修改說明 `-index` 設定以變更處理順序。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定外部目錄服務以進行 ONTAP S3 存取

從 ONTAP 9.14.1 開始、外部目錄的服務已與 ONTAP S3 物件儲存設備整合。這項整合可透過外部目錄服務簡化使用者和存取管理。

您可以為屬於外部目錄服務的使用者群組提供存取 ONTAP 物件儲存環境的權限。輕量型目錄存取傳輸協定（ LDAP ）是與 Active Directory 等目錄服務進行通訊的介面、可為身分識別與存取管理（ IAM ）提供資料庫和服務。若要提供存取權、您必須在 ONTAP S3 環境中設定 LDAP 群組。設定存取權限之後、群組成員就擁有 ONTAP S3 工作區的權限。有關 LDAP 的信息，請參見"了解如何在 ONTAP NFS SVM 上使用 LDAP 名稱服務"。

您也可以將 Active Directory 使用者群組設定為快速繫結模式、以便驗證使用者認證、並透過 LDAP 連線驗證協力廠商和開放原始碼 S3 應用程式。

開始之前

在設定 LDAP 群組及啟用群組存取的快速繫結模式之前、請先確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱。 "設定DNS服務"
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱。 "在 SVM 上安裝自簽名根 CA 憑證"
5. LDAP 用戶端在 SVM 上設定為啟用 TLS 。請參閱"為 ONTAP NFS 存取建立 LDAP 用戶端配置"和"將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯以獲取資訊"。

設定 S3 的 LDAP 存取

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

深入瞭解 ONTAP 命令參照中的連結： https://docs 。 NetApp 。 ONTAP - CLI/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^] 命令。

2. 使用建立物件儲存庫貯體原則聲明 `principal` 設定為您要授與存取權的 LDAP 群組：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

範例：下列範例建立的 Bucket 原則陳述式 `buck1`。原則允許 LDAP 群組存取 `group1` 至資源（貯體及其物件） `buck1`。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. 驗證 LDAP 群組中的使用者 `group1` 能夠從 S3 用戶端執行 S3 作業。

使用 LDAP 快速繫結模式進行驗證

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

深入瞭解 ONTAP 命令參照中的連結： https://docs 。 NetApp 。 ONTAP - CLI/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^] 命令。

2. 確保存取 S3 儲存貯體的 LDAP 使用者具有在儲存庫原則中定義的權限。如需詳細資訊、請參閱 "修改庫位原則"。
3. 確認 LDAP 群組中的使用者可以執行下列作業：
   a. 在 S3 用戶端上以下列格式設定存取金鑰：範例 "NTAPFASTBIND"： + base64 編碼（ LDAPUser:password ），結果就是 NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`這樣 `"NTAPFASTBIND" + base64-encode(user-name:password)

      S3 用戶端可能會提示輸入秘密金鑰。如果沒有秘密金鑰、則可以輸入至少 16 個字元的任何密碼。

   b. 從使用者具有權限的 S3 用戶端執行基本 S3 作業。

Base64 認證

ONTAP S3 的預設組態不包括 HTTP ，而且僅使用 HTTPS 和傳輸層安全性（ TLS ）連線。ONTAP 可以產生自我簽署的憑證，但建議的最佳做法是使用來自協力廠商憑證授權單位（ CA ）的憑證。使用 CA 憑證時，您會在用戶端應用程式和 ONTAP 物件存放區伺服器之間建立信任的關係。

請注意，使用 Base64 編碼的認證資料很容易解碼。使用 HTTPS 可防止中間人封包監聽器擷取編碼認證。

建立預先簽署的 URL 時，請勿使用 LDAP 快速連結模式進行驗證。驗證是以預先簽署的 URL 所包含的 Base64 存取金鑰為基礎。將向解碼 Base64 存取金鑰的任何人顯示使用者名稱和密碼。

驗證方法為 **nsswitch** ， **LDAP** 為啟用範例

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。

為 **Active Directory** 或 **SMB** 伺服器設定 **S3** 訪問

如果在 Bucket 原則聲明中指定的 nasgroup 或 nasgroup 的使用者沒有 UID 和 GID 集，則找不到這些屬性時，查詢會失敗。Active Directory 使用 SID ，而非 UID 。如果無法將 SID 項目對應至 UID ，則必須將必要資料帶到 ONTAP 。

若要這麼做，請使用"vserver Active Directory建立"，讓 SVM 可以透過 Active Directory 驗證，並取得必要的使用者和群組資訊。

或者，使用"建立Vserver CIFS"在 Active Directory 網域中建立 SMB 伺服器。

如果名稱伺服器和物件儲存使用不同的域名，則可能會遇到查找失敗的情況。為避免尋找失敗， NetApp建議使用 UPN 格式的受信任網域進行資源授權： `nasgroup/group@trusted_domain.com`受信任網域是指已新增至 SMB 伺服器受信任網域清單中的網域。了解如何"新增、刪除和修改首選信任域"在 SMB 伺服器清單中。

當驗證方法是網域且信任的網域是在 **Active Directory** 中設定時，會產生金鑰

將端點與以 UPN 格式指定的使用者一起使用 `s3/services/<svm_uuid>/users` 。範例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

> 將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。

當驗證方法為網域且沒有信任的網域時，請產生金鑰

當停用 LDAP 或非 POSIX 使用者尚未設定 UID 和 GID 時，就可以執行此動作。範例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

> 將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。如果沒有信任的網域，您只需要將選用的網域值（ @FQDN ）新增至使用者名稱。

讓 LDAP 或網域使用者產生自己的 ONTAP S3 存取金鑰

從 ONTAP 9.14.1 開始、身為 ONTAP 管理員、您可以建立自訂角色、並將其授予本機或網域群組或輕量型目錄存取傳輸協定（ LDAP ）群組、讓屬於這些群組的使用者能夠產生自己的存取權和機密金鑰、以供 S3 用戶端存取。

您必須在儲存 VM 上執行幾個組態步驟，才能建立自訂角色，並將其指派給啟動 API 以產生存取金鑰的使用者。

> 如果 LDAP 被停用，您可以"為ONTAP S3 存取設定外部目錄服務"允許使用者產生存取密鑰。

開始之前

請確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱。 "設定DNS服務"
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱。 "在 SVM 上安裝自簽

名根 CA 憑證"

5. LDAP 用戶端在儲存 VM 上設定為啟用 TLS 。請參閱。 "為 ONTAP NFS 存取建立 LDAP 用戶端配置"
6. 將用戶端組態與虛擬伺服器建立關聯。請參閱。 "將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯"如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。
7. 如果您使用的是資料儲存 VM 、請在 VM 上建立管理網路介面（ LIF ）、以及 LIF 的服務原則。深入瞭解 `network interface create`及 `network interface service-policy create` "指令參考資料ONTAP"。

設定使用者以產生存取金鑰

範例 **1.** 步驟

LDAP 用戶

1. 將 LDAP 指定為儲存 VM 的名稱服務資料庫 _ 、以用於群組和 LDAP 密碼：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch modify`資訊，請參閱。

2. 建立可存取 S3 使用者 REST API 端點的自訂角色：
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
在此範例中 `s3-role` 角色是針對儲存 VM 上的使用者所產生 `svm-1`，授予所有存取權限、讀取、建立及更新。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

如"指令參考資料ONTAP"需詳細 `security login rest-role create`資訊，請參閱。

3. 使用以下方式建立 LDAP 使用者群組 `security login`命令並新增用於存取 S3 使用者 REST API 端點的新自訂角色。詳細了解 `security login create`在"指令參考資料ONTAP" 。

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

在此範例中、是 LDAP 群組 `ldap-group-1` 是在中建立的 `svm-1`**以及自訂角色** `s3role` 新增至 IT 以存取 API 端點、並在快速繫結模式中啟用 LDAP 存取。

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

如需更多資訊、請參閱 "使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。

如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

將自訂角色新增至 LDAP 群組允許該群組中的使用者對ONTAP進行有限的訪問 `/api/protocols/s3/services/{svm.uuid}/users`端點。透過呼叫 API，LDAP 群組使用者可以產生自己的存取

金鑰和金鑰來存取 S3 用戶端。他們只能為自己產生密鑰，而不能為其他使用者產生密鑰。

網域用戶

1. 建立可以存取 S3 使用者 REST API 端點的自訂角色：

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

在此範例中， `s3-role`為儲存虛擬機器上的使用者產生角色 `svm-1` ，授予所有存取權限，即讀取、建立和更新。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

如"指令參考資料ONTAP"需詳細 `security login rest-role create`資訊，請參閱。

1. 使用以下方式建立網域使用者群組 `security login`命令並新增用於存取 S3 使用者 REST API 端點的新自訂角色。詳細了解 `security login create`在"指令參考資料ONTAP" 。

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   在此範例中，網域組 `domain\group1`創建於 `svm-1`以及自訂角色 `s3role`添加到其中以存取 API 端點。

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

將自訂角色新增至網域群組允許該群組中的使用者對ONTAP進行有限的訪問 `/api/protocols/s3/services/{svm.uuid}/users`端點。透過呼叫 API，網域組使用者可以產生自己的存取金鑰和金鑰來存取 S3 用戶端。他們只能為自己產生密鑰，而不能為其他使用者產生密鑰。

做為 S3 或 LDAP 使用者、產生您自己的存取金鑰

從 ONTAP 9.14.1 開始、如果您的系統管理員已授予您自行產生金鑰的角色、您就可以產生自己的存取權和秘密金鑰、以供存取 S3 用戶端。您只能使用下列 ONTAP REST API 端點自行產生金鑰。

建立 **S3** 使用者並產生金鑰

此 REST API 呼叫使用下列方法和端點。有關此端點的更多信息，請參閱參考 "API 文件" 。

HTTP方法	路徑
貼文	/api/protocols / s3/services / ｛ SVM.uuid ｝ / 使用者

對於網域用戶，請使用以下格式作為 S3 使用者名稱： `user@fqdn` ， 在哪裡 `fqdn`是域的完全限定域名。

Curl範例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

Json輸出範例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

為 **S3** 使用者重新產生金鑰

如果 S3 使用者已存在，您可以重新產生其存取金鑰和金鑰。此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
修補	/api/protocols/s3/services/{svm.uuid}/使用者/{名稱}

Curl範例

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

Json輸出範例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

版權資訊

商標資訊