外部の橋本 Corp を使用するようにデータブローカーを設定するバックアップ

Cloud Manager

Ben Cammett
July 11, 2021

目次

外部の橋本 **Corp** を使用するようにデータブローカーを設定する バックアップ

Amazon S3 、 Azure 、または Google Cloud のクレデンシャルが必要な同期関係を作成する場合は、 Cloud Sync のユーザインターフェイスまたは API を使用してそれらのクレデンシャルを指定する必要があります。別の方法として、データブローカーをセットアップして、外部の橋本社ボールトから直接クレデンシャル（または *secrets*）にアクセスする方法もあります。

この機能は、 Cloud Sync API を使用し、 Amazon S3 、 Azure 、または Google Cloud のクレデンシャルを必要とする同期関係をサポートします。

ボルトを準備します

URL　を設定して、データブローカーにクレデンシャルを提供するようにヴォールトを準備します。ボールトのシークレットの URL は、 *creds_* で終わる必要があります。

データブローカーを準備

データブローカーのローカル構成ファイルを変更し、外部ボルトからクレデンシャルを取得するようにデータブローカーを準備します。

API を使用して同期関係を作成してください

すべての設定が完了したら、　API　呼び出しを送信して、ヴォールトを使用してシークレットを取得する同期関係を作成できます。

ヴォールトを準備しています

ボールトのシークレットに Cloud Sync の URL を指定する必要があります。URL を設定してボールトを準備します。作成する同期関係の各ソースとターゲットのクレデンシャルへの URL を設定する必要があります。

URL は次のように設定する必要があります。

「 /<path>/<RequestID>/<endpoint-protocol> creds 」を指定します

パス
: シークレットへのプレフィックスパス。この値は、お客様に固有の任意の値にすることができます。

リクエスト **ID**
: 生成する必要があるリクエスト ID 。同期関係を作成するときは、 API POST 要求のいずれかのヘッダーに ID を指定する必要があります。

エンドポイントプロトコル
: 定義されている次のいずれかのプロトコル "v2 以降の関係に関するドキュメント"： S3 、 Azure 、 GCP （それぞれ大文字で入力する必要があります）。

Creds （作成）
: URL の末尾は *creds*. にする必要があります。

例

次の例は、シークレットへの URL を示しています。

ソースクレデンシャルの完全な **URL** とパスの例

この例のように、プレフィックスパスは */my-path/all-secrets/* で、要求 ID は _hb312vdasr2_ で 、ソースエンドポイントは S3 です。

ターゲットクレデンシャルの完全な **URL** とパスの例

プレフィックスパスは */my-path/all-secrets/* 、要求 ID は *n32hcbnejk2*、 ターゲットエンドポイントは Azure です。

データブローカーの準備

データブローカーのローカル構成ファイルを変更し、外部ボルトからクレデンシャルを取得するようにデータブローカーを準備します。

手順

1. SSH をデータブローカーに接続
2. /opt/netapp/databroker/config にある local.json ファイルを編集します。
3. enable を * true * に設定し、 _external-m積分 .hashicorp_as の下に config パラメータフィールドを設定します。

有効

- 有効な値は、 true または false です
- type ：ブール値
- デフォルト値： false
- true ：データブローカーは、社内の外部の橋本社から機密情報を入手します
- false ：データブローカーのクレデンシャルがローカルボールトに格納されます

URL

- 文字列を入力します
- 値：外部ボルトの URL

パス

- 文字列を入力します
- 値：クレデンシャルを使用してシークレットへのプレフィックスパスを指定します

拒否 **-** 承認されていません

- データブローカーで権限のないことを拒否するかどうかを指定します 外部ボールト
- type ：ブール値
- デフォルト： false

auth-method を指定します

- データブローカーが外部ボルトのクレデンシャルにアクセスする際に使用する認証方式
- 文字列を入力します
- 有効な値は「 AWS- IAM 」 / 「 role-app 」 / 「 GCP-IAM 」です。

ロール名

- 文字列を入力します
- ロール名（ AWS- IAM または GCP-IAM を使用している場合）

Secretd&rootid

- タイプ： string （ app-role を使用する場合）

ネームスペース

- 文字列を入力します
- ネームスペース（必要に応じて X-Vault - 名前空間ヘッダー）

AWS ロール認証の例

```
{
        "external-integrations": {
                "hashicorp": {
                        "enabled": true,
                        "url": "https://example.vault.com:8200",
                        "path": ""my-path/all-secrets",
                        "reject-unauthorized": false,
                        "auth-method": "aws-role",
                        "aws-role": {
                                "role-name": "my-role"
                        }
                }
        }
}
```

GCP - IAM 認証の例

```
{
"external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": http://ip-10-20-30-55.ec2.internal:8200,
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
"gcp-iam": {
          "role-name": "my-iam-role"
      }
    }
  }
}
```

GCP - IAM 認証を使用する場合に権限を設定します

_GCP-AM_authentication メソッドを使用している場合、データブローカーには次の GCP 権限が必要です。

```
- iam.serviceAccounts.signJwt
```

"データブローカーの GCP 権限要件の詳細については、こちらをご覧ください"。

ヴォールトのシークレットを使用して、新しい同期関係を作成します

すべての設定が完了したら、 API 呼び出しを送信して、ヴォールトを使用してシークレットを取得する同期関係を作成できます。

Cloud Sync REST API を使用して関係をポストします。

```
Headers:
Authorization: Bearer <user-token>
Content-Type: application/json
x-account-id: <accountid>
x-netapp-external-request-id-src: request ID as part of path for source
credentials
x-netapp-external-request-id-trg: request ID as part of path for target
credentials
Body: post relationship v2 body
```

- ユーザトークンと Cloud Central アカウント ID を取得するには、 "のドキュメントのこのページを参照してください"。
- 投稿関係の本文を作成するには、 "relationships-v2 API 呼び出しを参照してください"。

例

POST 要求の例：

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik…"
Body:
{
"dataBrokerId": "5e6e111d578dtyuu1555sa60",
"source": {
        "protocol": "s3",
        "s3": {
                "provider": "sgws",
                "host": "1.1.1.1",
                "port": "443",
                "bucket": "my-source"
     },
"target": {
        "protocol": "s3",
        "s3": {
                "bucket": "my-target-bucket"
        }
    }
}
```