Workforce Identity 連携と Microsoft Entra を使用して Power BI で Big Query データにアクセスする

リリースノート

このガイドでは、Microsoft Entra グループ内のユーザーが Workforce Identity 連携 (https://cloud.google.com/iam/docs/workforce-identity-federation?hl=ja)を使用して、Power BI の BigQuery データにアクセスできるようにする方法について説明します。

Microsoft Entra は ID プロバイダ（IdP）です。Microsoft Entra のグループ クレームは Google Cloudにマッピングされます。グループには、BigQuery データにアクセスするための Identity and Access Management（IAM）権限が付与されます。

このガイドでは、Power BI Desktop または Power BI Web の操作方法について説明します。

始める前に

1. Google Cloud 組織が設定されていることを確認します。
2. Google Cloud CLI をインストール (https://cloud.google.com/sdk/docs/install?hl=ja) します。 インストール後、次のコマンドを実行して Google Cloud CLI を初期化 (https://cloud.google.com/sdk/docs/initializing?hl=ja)します。

   ```
   gcloud init
   ```

   外部 ID プロバイダ（IdP）を使用している場合は、まずフェデレーション ID を使用して gcloud CLI にログイン (https://cloud.google.com/iam/docs/workforce-log-in-gcloud?hl=ja)する必要があります。

★ **注:** すでに gcloud CLI をインストールしている場合は、**`gcloud components update`** を実

行して、最新バージョンがインストールされていることを確認してください。

3. Microsoft Entra と Microsoft Graph にアクセスできる必要があります。
4. Power BI がセットアップされている必要があります。

費用

Workforce Identity 連携は、無料の機能として利用できます。ただし、Workforce Identity 連携の詳細な監査ロギングでは Cloud Logging が使用されます。Logging の料金については、Google Cloud Observability の料金 (https://cloud.google.com/stackdriver/pricing?hl=ja#logs-costs)をご覧ください。

必要なロール

このセクションでは、管理者とリソースに必要なロールについて説明します。

管理者のためのロール

Workforce Identity 連携の構成に必要な権限を取得するには、組織に対する IAM Workforce プール管理者 (https://cloud.google.com/iam/docs/roles-permissions/iam?hl=ja#iam.workforcePoolAdmin)（`roles/iam.workforcePoolAdmin`）の IAM ロールを付与するように管理者に依頼します。ロールの付与については、プロジェクト、フォルダ、組織へのアクセス権の管理 (https://cloud.google.com/iam/docs/granting-changing-revoking-access?hl=ja)をご覧ください。

必要な権限は、カスタムロール (https://cloud.google.com/iam/docs/creating-custom-roles?hl=ja)や他の事前定義ロール (https://cloud.google.com/iam/docs/roles-overview?hl=ja#predefined)から取得することもできます。

また、IAM オーナー（`roles/owner`）の基本ロールには ID 連携を構成する権限も含まれています。本番環境では基本ロールを付与すべきではありません。基本ロールは、開発環境またはテスト環境で付与してください。

フェデレーション ID のためのロール

Power BI は、トークン交換時に **userProject** パラメータを送信します。そのため、課金プロジェクトのフェデレーション ID に Service Usage ユーザー（**roles/serviceusage.serviceUsageConsumer**）ロールを付与するよう管理者に依頼する必要があります。

フェデレーション ID のグループにロールを付与するには、次のコマンドを実行します。

```
gcloud projects add-iam-policy-binding PROJECT_ID \
    --role="roles/serviceusage.serviceUsageConsumer" \
    --member="principalSet://iam.googleapis.com/locations/global/workforc
```

次のように置き換えます。

- ***PROJECT_ID***: 課金プロジェクト ID。
- ***WORKFORCE_POOL_ID***: Workforce Identity プールの ID。
- ***GROUP_ID***: グループ ID（例: **admin-group@altostrat.com**）。一般的なプリンシパル ID のリストについては、プリンシパル ID (https://cloud.google.com/iam/docs/principal-identifiers?hl=ja) をご覧ください。

Workforce Identity プールを作成する

このセクションでは、Workforce Identity プールの作成方法について説明します。Workforce Identity プール プロバイダは、このガイドの後半で作成します。

gcloudコンソール (#コンソール)
(#gcloud)

Workforce Identity プールを作成するには、次のコマンドを実行します。

```
gcloud iam workforce-pools create WORKFORCE_POOL_ID \
    --organization=ORGANIZATION_ID \
```

```
  --display-name="DISPLAY_NAME" \
  --description="DESCRIPTION" \
  --session-duration=SESSION_DURATION \
  --location=global
```

次のように置き換えます。

- ***WORKFORCE_POOL_ID***: Google Cloud Workforce プールを表す ID。ID の形式については、API ドキュメントのクエリ パラメータ (https://cloud.google.com/iam/docs/reference/rest/v1/locations.workforcePools.providers/create?hl=ja#query-parameters) セクションをご覧ください。
- ***ORGANIZATION_ID***: Workforce Identity プールの Google Cloud 組織の組織 ID。Workforce Identity プールは、組織内のすべてのプロジェクトとフォルダで使用できます。
- ***DISPLAY_NAME***: 省略可。Workforce Identity プールの表示名。
- ***DESCRIPTION***: 省略可。Workforce Identity プールの説明。
- ***SESSION_DURATION***: 省略可。セッション継続時間。s を付加した数値で表します（例: `3600s`）。セッション継続時間は、この Workforce プールの Google Cloud アクセス トークン、コンソール（連携） (https://cloud.google.com/iam/docs/workforce-identity-federation?hl=ja#console-federated) ログイン セッション、gcloud CLI ログイン セッションの有効期間を決定します。セッション継続時間のデフォルトは 1 時間（3,600 秒）です。セッション継続時間は 15 分（900 秒）～12 時間（43,200 秒）の範囲で指定する必要があります。

ヒント: **`gcloud iam workforce-pools create --help`** を実行して、このコマンド用にカスタマイズできる他のパラメータを見つけます。

新しい Microsoft Entra アプリを登録する

このセクションでは、Microsoft Azure Portal を使用して Microsoft Entra アプリを作

成する方法について説明します。

1. 新しい Microsoft Entra アプリケーションを登録します (https://learn.microsoft.com/en-us/azure/healthcare-apis/register-application#register-a-new-application)
   。
2. 登録した Microsoft Entra アプリケーションで、新しいクライアント シークレットを作成 (https://learn.microsoft.com/en-us/azure/healthcare-apis/register-application#certificates--secrets)
   します。クライアント シークレットは、メモしておいてください。
3. Microsoft Entra アプリケーションに API 権限を付与して、Active Directory のユーザーとグループの情報にアクセスできるようにします。Microsoft Graph API の権限を付与する手順は次のとおりです。
   a. アプリケーションで [**API 権限**] を選択します。
   b. [**構成されたアクセス許可**] で、[**アクセス許可の追加**] をクリックします。
   c. [**API のアクセス許可の要求**] ダイアログで、[**Microsoft Graph**] を選択します。
   d. [**アプリケーションのアクセス許可**] を選択します。
   e. [**アクセス許可の選択**] ダイアログで、次の操作を行います。
      i. 検索フィールドに「`User.ReadBasic.All`」と入力します。
      ii. **User.ReadBasic.All** をクリックします。
      iii. [**アクセス許可の追加**] をクリックします。
   f. [**API のアクセス許可の要求**] ダイアログで、[**Microsoft Graph**] を選択します。
   g. [**アプリケーションのアクセス許可**] を選択します。
   h. [**アクセス許可の選択**] ダイアログで、次の操作を行います。
      i. 検索フィールドに「`GroupMember.Read.All`」と入力します。
      ii. **GroupMember.Read.All** をクリックします。
      iii. [**アクセス許可の追加**] をクリックします。

i. [**構成されたアクセス許可**] で、[**管理者の同意の付与（ドメイン名）**] をクリックします。

j. 確認メッセージが表示されたら、[**はい**] をクリックします。

4. このガイドの後半で Workforce プール プロバイダを構成するために必要な値にアクセスするには、次の操作を行います。

   a. Microsoft Entra アプリケーションの [**概要**] ページに移動します。

   b. [**エンドポイント**] をクリックします。

   c. 次の値をメモします。

      - **クライアント ID:** このガイドの前半で登録した Microsoft Entra アプリの ID。
      - **クライアント シークレット:** このガイドの前半で生成したクライアント シークレット。
      - **テナント ID:** このガイドの前半で登録した Microsoft Entra アプリのテナント ID。
      - **発行元 URI:** OpenID Connect メタデータ ドキュメントの URI（`/.well-known/openid-configuration` は省略）。たとえば、OpenID Connect メタデータ ドキュメントの URL が `https://login.microsoftonline.com/d41ad248-019e-49e5-b3de-4bdfe1fapple/v2.0/.well-known/openid-configuration` の場合、発行元 URI は `https://login.microsoftonline.com/d41ad248-019e-49e5-b3de-4bdfe1fapple/v2.0/` になります。

Workforce Identity プール プロバイダを作成する

プロバイダを作成するには、次のコマンドを実行します。

```
gcloud iam workforce-pools providers create-oidc WORKFORCE_PROVIDER_ID
    --workforce-pool=WORKFORCE_POOL_ID \
    --location=global \
    --display-name=DISPLAY_NAME \
```

```
--issuer-uri=ISSUER_URI \
--client-id=https://analysis.windows.net/powerbi/connector/GoogleBig(
--attribute-mapping=ATTRIBUTE_MAPPING \
--web-sso-response-type=id-token \
--web-sso-assertion-claims-behavior=only-id-token-claims \
--extra-attributes-issuer-uri=APP_ISSUER_URI \
--extra-attributes-client-id=APP_CLIENT_ID \
--extra-attributes-client-secret-value=APP_CLIENT_SECRET \
--extra-attributes-type=EXTRA_GROUPS_TYPE \
--extra-attributes-filter=EXTRA_FILTER \
--detailed-audit-logging
```

次のように置き換えます。

- ***WORKFORCE_PROVIDER_ID***: 一意のプロバイダ ID。接頭辞 **gcp-** は予約されているため、プロバイダ ID では使用できません。
- ***WORKFORCE_POOL_ID***: IdP を接続する Workforce Identity プール ID。
- ***DISPLAY_NAME***: プロバイダのわかりやすい表示名（省略可）。
- ***ISSUER_URI***: 発行元 URI の値（**https://sts.windows.net/*TENANT_ID*** の形式）。***TENANT_ID*** の部分は、先ほどメモしたテナント ID で置き換えてください。
- ***ATTRIBUTE_MAPPING***: グループのマッピングと、必要な場合は Microsoft Entra のクレームからGoogle Cloud 属性に対応する、その他の属性マッピング（例: **google.groups=assertion.groups, google.subject=assertion.sub**）。このグループには、このガイドの後半で BigQuery データへのアクセス権が付与されます。

  詳細については、属性のマッピング (https://cloud.google.com/iam/docs/workforce-identity-federation?hl=ja#attribute-mapping) をご覧ください。
- ***APP_ISSUER_URI***: 先ほどメモした Microsoft Entra アプリケーションの発行元 URI。
- ***APP_CLIENT_ID***: 前述の発行元クライアント ID。
- ***APP_CLIENT_SECRET***: 先ほどメモした発行元のクライアント シークレット。
- ***EXTRA_GROUPS_TYPE***: グループ ID のタイプ。次のいずれかになります。

- `azure-ad-groups-mail`: グループのメールアドレスは IdP から取得されます（例: `admin-group@altostrat.com`）。
- `azure-ad-groups-id`: グループを表す UUID は IdP から取得されます（例: `abcdefgh-0123-0123-abcdef`）。

- ***EXTRA_FILTER***: IdP から渡される特定のアサーションをリクエストするために使用されるフィルタ。`--extra-attributes-type=azure-ad-groups-mail` を指定すると、IdP から渡されるユーザーのグループ クレームに対して `--extra-attributes-filter` のフィルタが実行されます。デフォルトでは、ユーザーに関連付けられているすべてのグループが取得されます。使用するグループは、メールとセキュリティが有効になっている必要があります。詳細については、$search クエリ パラメータを使用する (https://learn.microsoft.com/en-us/graph/search-query-parameter)をご覧ください。

★ **重要:** 取得できるグループは最大 999 個です。

次の例では、`gcp` で始まるユーザーのメールアドレスに関連付けられているグループをフィルタしています。

```
--extra-attributes-filter='"mail:gcp"'
```

次の例では、`gcp` で始まるメールアドレスと、`example` を含む **displayName** を持つユーザーに関連付けられているグループをフィルタしています。

```
--extra-attributes-filter='"mail:gcp" AND "displayName:example"'
```

- Workforce Identity 連携の詳細な監査ロギングでは、IdP から受信した情報が Logging に記録されます。詳細な監査ロギングは、Workforce Identity プール プロバイダの構成のトラブルシューティングに役立ちます。詳細な監査ロギングを使用して属性マッピング エラーのトラブルシューティングを行う方法については、一般的な属性マッピング エラー (https://cloud.google.com/iam/docs/troubleshooting-workforce-identity-federation?hl=ja#general-attribute-mapping-errors)

をご覧ください。Logging の料金については、Google Cloud Observability の料金 (https://cloud.google.com/stackdriver/pricing?hl=ja#logs-costs)をご覧ください。

Workforce Identity プール プロバイダの詳細な監査ロギングを無効にするには、**`gcloud iam workforce-pools providers create`** の実行時に **`--detailed-audit-logging`** フラグを省略します。詳細な監査ロギングを無効にするには、プロバイダを更新 (https://cloud.google.com/iam/docs/manage-workforce-identity-pools-providers?hl=ja#update-oidc-provider) することもできます。

IAM ポリシーを作成する

このセクションでは、BigQuery データが保存されているプロジェクトのマッピングされたグループに BigQuery データ閲覧者（**`roles/bigquery.dataViewer`**）ロールを付与する IAM 許可ポリシーを作成します。このポリシーにより、グループ内のすべての ID は、プロジェクトに保存されている BigQuery テーブルとビューのデータにアクセスできます。

ポリシーを作成するには、次のコマンドを実行します。

```
gcloud projects add-iam-policy-binding BIGQUERY_PROJECT_ID \
    --role="roles/bigquery.dataViewer" \
    --member="principalSet://iam.googleapis.com/locations/global/workforc
```

次のように置き換えます。

- ***`BIGQUERY_PROJECT_ID`***: BigQuery のデータとメタデータが保存されているプロジェクト ID。
- ***`WORKFORCE_POOL_ID`***: Workforce Identity プールの ID
- ***`GROUP_ID`***: グループ ID。Workforce Identity プール プロバイダの作成に使用された **`--extra-attributes-type`** の値によって異なります。
    - **`azure-ad-groups-mail`**: グループ ID はメールアドレスです（例: **`admin-group@altostrat.com`**）。

- `azure-ad-groups-id`: グループ ID はグループの UUID です（例: `abcdefgh-0123-0123-abcdef`）。

Power BI Desktop から BigQuery データにアクセスする

Power BI Desktop から BigQuery データにアクセスする手順は次のとおりです。

1. Power BI を開きます。
2. [**データを取得**] をクリックします。
3. [**データベース**] をクリックします。
4. データベースのリストで、[**Google BigQuery (Microsoft Entra ID) (Beta)**] を選択します。
5. [**接続**] をクリックします。
6. 次の必須フィールドに入力します。
   - **課金プロジェクト ID:** 課金プロジェクト ID。
   - **オーディエンス URI:** Google Cloud URI。形式は次のとおりです。

     ```
     //iam.googleapis.com/locations/global/workforcePools/WORKFORCE_
     ```

     次のように置き換えます。

     - *`WORKFORCE_POOL_ID`*: Workforce Identity プールの ID。
     - *`WORKFORCE_PROVIDER_ID`*: Workforce Identity プール プロバイダ ID。
7. [**OK**] をクリックします。
8. [**次へ**] をクリックします。
9. [**データの選択**] をクリックします。

ログインを求められた場合は、グループのメンバーである Microsoft Entra ID を使用してください。

以上の操作により、Power BI Desktop で BigQuery のデータを使用できるようになります。

Power BI Web から BigQuery データにアクセスする

Power BI Web から BigQuery データにアクセスする手順は次のとおりです。

1. Power BI Web に移動します。
2. [**Power Query**] をクリックして、新しいデータソースを追加します。
3. [**データを取得**] をクリックします。
4. リストで [**Google BigQuery (Microsoft Entra ID) (Beta)**] を見つけて選択します。
5. 次の必須フィールドに入力します。
    - **課金プロジェクト ID:** Google Cloud 課金プロジェクト
    - **オーディエンス URI:** オーディエンス URI の形式は次のとおりです。

      ```
      //iam.googleapis.com/locations/global/workforcePools/WORKFORCE_
      ```

      次のように置き換えます。

        - *WORKFORCE_POOL_ID*: Workforce Identity プールの ID
        - *WORKFORCE_PROVIDER_ID*: Workforce Identity プール プロバイダ ID
6. [**接続の資格情報**] > [**認証の種類**] をクリックします。
7. [**組織アカウント**] を選択します。
8. [**サインイン**] をクリックします。
9. [**次へ**] をクリックします。

10. **[データの選択]** をクリックします。

以上の操作により、Power BI Web で BigQuery のデータを使用できるようになります。

次のステップ

- Workforce Identity 連携ユーザーとそのデータを削除する。Workforce Identity 連携ユーザーとそのデータを削除する (https://cloud.google.com/iam/docs/workforce-delete-user-data?hl=ja)をご覧ください。
- Google Cloud プロダクトの Workload Identity 連携のサポートについて学習する。Identity 連携: サポート対象のプロダクトと制限事項 (https://cloud.google.com/iam/docs/federated-identity-supported-services?hl=ja)をご覧ください。

最終更新日 2025-08-23 UTC。