

# 環境構築手順

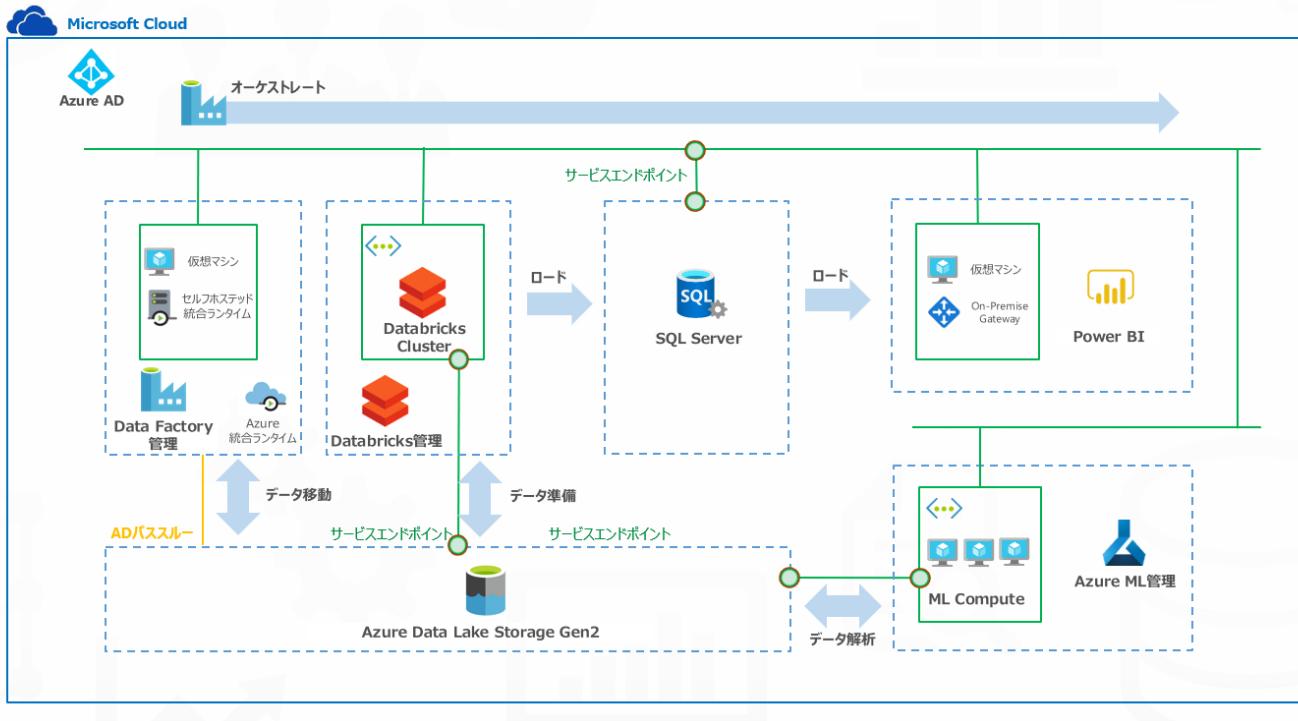
---

- 環境構築手順
  - 概要
  - 環境のデプロイ
    - 環境のデプロイ手順概要
    - 前提条件
    - 1. Azure DevOps Servicesの構成
    - 2. コードのインポート
    - 3. サービスコネクションの構成
    - 4. サービスプリンシパルの権限を所有者に変更
    - 5. パイプラインの変数グループを作成する
      - DatabricksID、テナントIDの確認方法
      - Azure DevOpsサービス接続のプリンシパルIDの確認方法
    - 6. Pipeline読み込み,実行
  - リソース設定 - Azure SQL
    - Azure SQL設定手順概要
    - 1. IPアドレスの追加
    - 2. AD管理者の設定
    - 3. DataFactoryリソースへの権限付与
  - 4 Databricksの設定
    - Databricksの設定手順概要
    - 1. PAT/Private Access Token)の作成
    - 2. Scope作成
      - Azure Key VaultのDNS名、リソースIDの確認方法
    - 3. KeyvaultSecretの登録
  - 確認
  - 次のステップ

## 概要

Azure分析基盤を迅速に構築します。

このテンプレートでは、Vnetの利用を前提にしており、一般的なセキュリティベースラインをパスすることを想定しています。



## 環境のデプロイ

AzureリソースのデプロイにはARMテンプレートを利用します。

DevOpsパイプラインを構成し、環境構築パイプラインを設定・実行します。

### 環境のデプロイ手順概要

1. Azure DevOps Servicesの構成
2. コードのインポート
3. サービスコネクションの構成
4. サービスプリンシパルの権限を所有者に変更
5. パイプラインの変数グループを作成する
6. Pipeline読み込み, 実行

### 前提条件

- 作業者はサブスクリプション所有者である必要があります。

## 1. Azure DevOps Servicesの構成

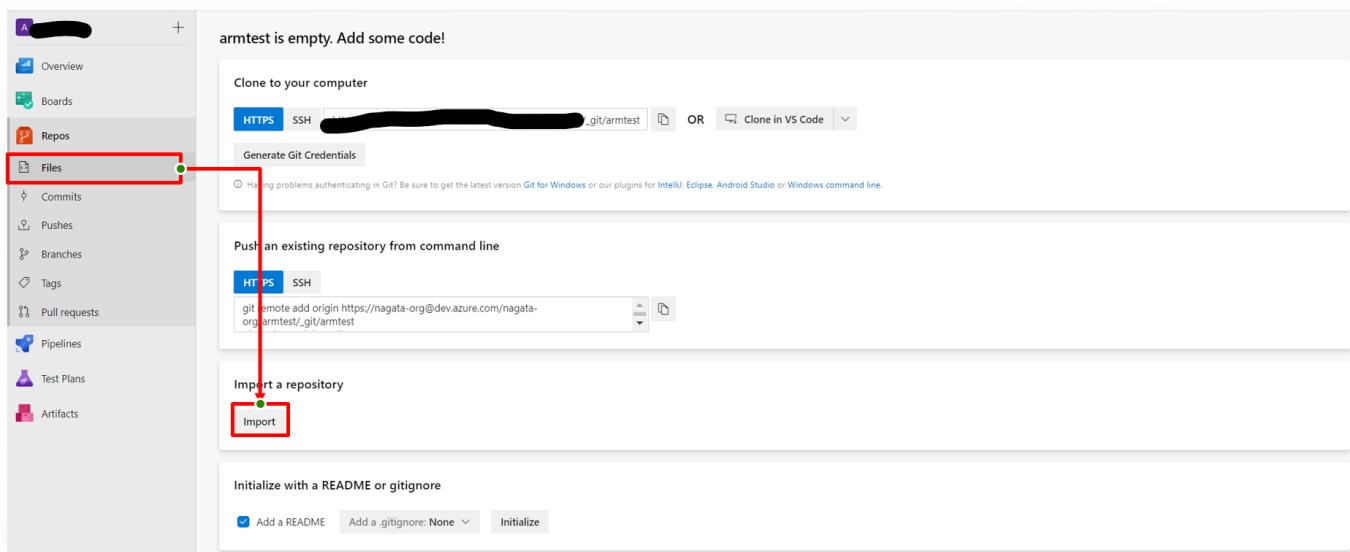
Azure DevOpsを利用していくつかのパイプラインを実行します。

Azure DevOps 組織をまだ持っていない場合は、「[クイックスタート: 組織またはプロジェクトコレクションを作成する](#)」の手順に従って作成します。

組織を構成したあとは、「[Azure DevOps および TFS でのプロジェクトの作成](#)」のガイドを使用して新しいプロジェクトを作成します。

## 2. コードのインポート

作成したDevOpsにサインインして、リポジトリのインポート画面に移動します。



The screenshot shows the 'Import a repository' page in Azure DevOps. On the left, there's a sidebar with various options like Overview, Boards, Repos, Files (which is highlighted with a red box), Commits, Pushes, Branches, Tags, Pull requests, Pipelines, Test Plans, and Artifacts. The main content area has three main sections: 'Clone to your computer' (with HTTPS and SSH options), 'Push an existing repository from command line' (with HTTPS and SSH options), and 'Import a repository'. In the 'Import a repository' section, the 'Import' button is also highlighted with a red box. At the bottom, there are checkboxes for 'Add a README' and 'Add a .gitignore: None', and a 'Initialize' button.

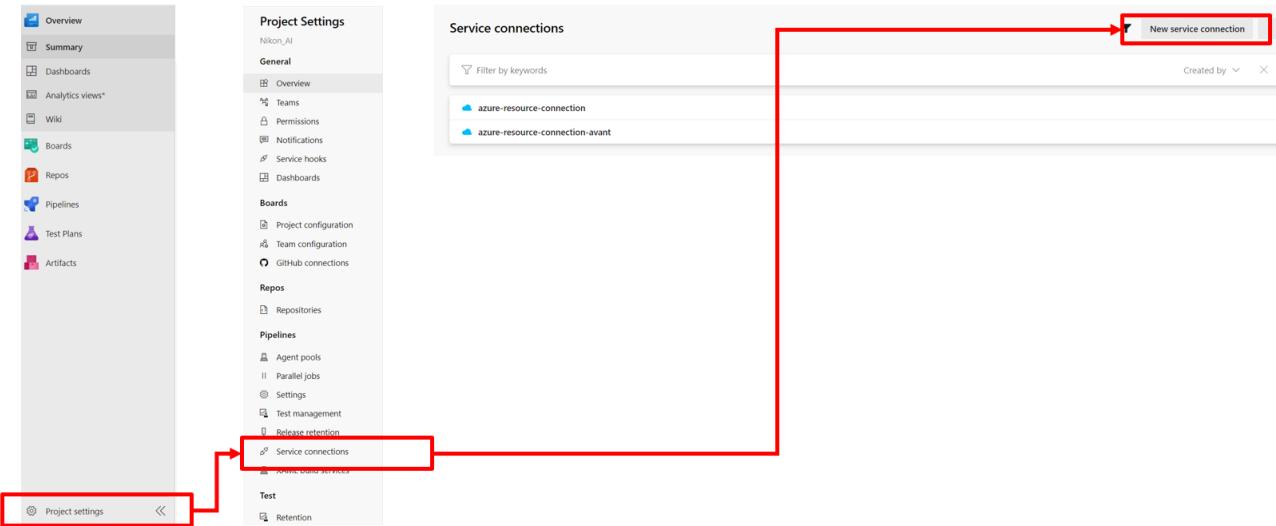
インポートのための設定をして、「Import」を選択します。

正常終了するとコードがインポートされます。

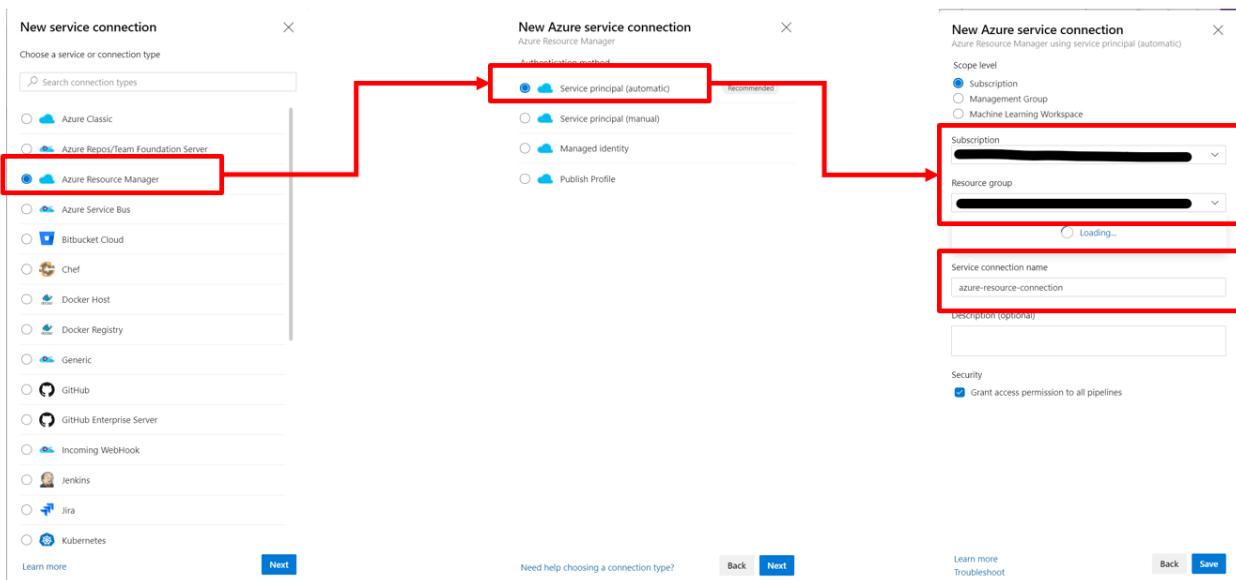
| 項目                      | 設定値        | 備考 |
|-------------------------|------------|----|
| Repository type         | Git        |    |
| Clone URL               | 講師からお伝えします |    |
| Requires Authentication | チェックします    |    |
| User Name               | 空白         |    |
| Password / PAT          | 講師からお伝えします |    |

### 3. サービスコネクションの構成

Azure DevOpsのサービスコネクション作成画面に移動します。



デプロイ対象のリソースグループ、サブスクリプションを指定し、名称を「**azure-resource-connection**」に設定し、「save」を選択します。



## 4. サービスプリンシパルの権限を所有者に変更

Azure Portalに移動して、リソースグループの共同作成者にDevOpsプロジェクトの名称ではじまるサービスプリンシパルが登録されていることを確認します。

ホーム > リソース グループ > iac\_sandbox | アクセス制御 (IAM)

概要 アクティビティ ログ アクセス制御 (IAM) タグ イベント 設定 クイック スタート デプロイ ポリシー プロバイダー ロック テンプレート のエクスポート コスト 管理 コスト 分析 コスト アラート (プレビュー) 予算 Advisor の推奨事項 監視 分析情報 (プレビュー) 警告 メトリック

アカウントの活動 ロールの割り当て 役割 拒否割り当て 従来の管理者

このサブスクリプションにおけるロール割り当ての数: 30 2000

名前: org-arm 種類: すべて 役割: 3 項目が選択されました スコープ: すべてのスコープ グループ化: 役割

**1 個のアイテム (1 サービス プリンシパル)**

| 名前  | 種類    | 役割 | スコープ   |
|---|-------|----|--------|
| <input type="checkbox"/> nagata-org-armtest-3ecf14ad-4309-4b8d-b9c3-84bb... アプリ | 共同作成者 |    | このリソース |

[追加]ボタンから、対象のサービスプリンシパルを所有者に登録します。

ス制御 (IAM)

+ 追加 ロールの割り当てのダウンロード (プレビュー) 列の編集 最新の情報に更新 削除 フィードバックがある場合

ロールの割り当ての追加

役割: 所有者 アクセスの割り当て先: Azure AD のユーザー、グループ、サービス プリンシパル 選択: nagata-org-arm...

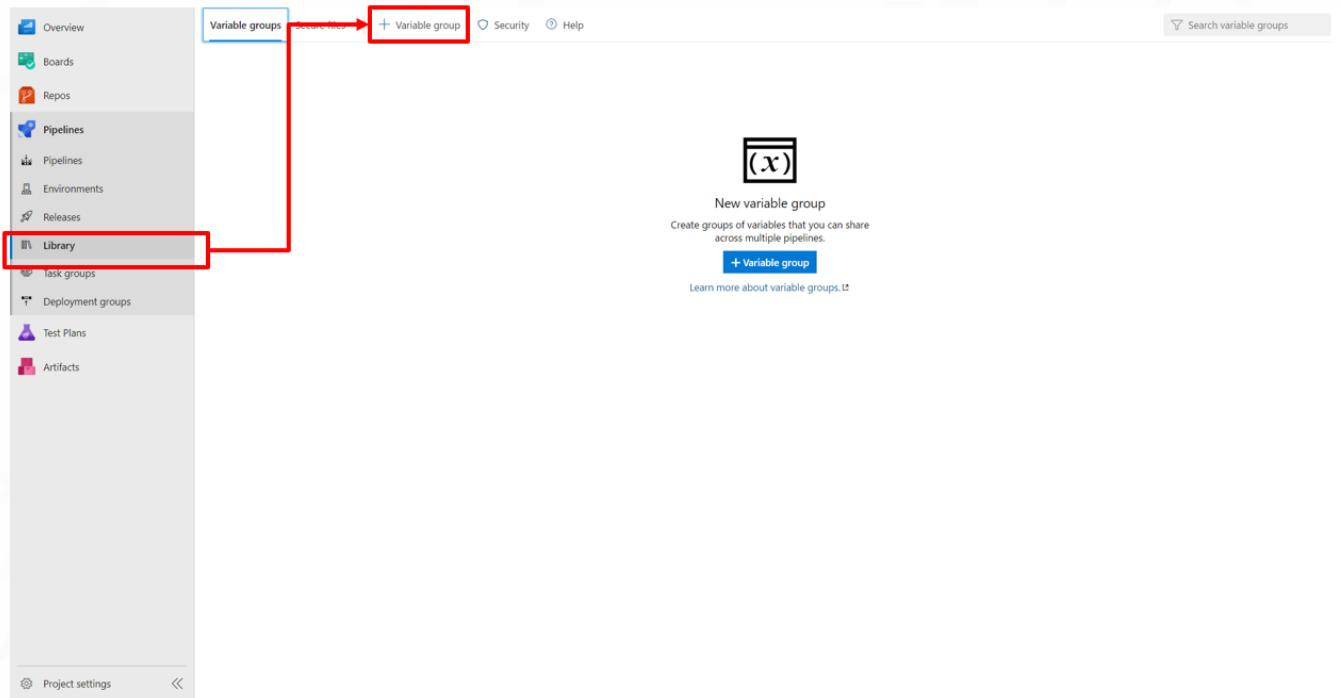
選択したメンバー: メンバーが選択されていません。このロールに割り当てるメンバーを 1 人以上検索してこのリストに対して追加してください。

RBAC の詳細

保存 破棄

## 5. パイプラインの変数グループを作成する

「ライブラリ」タブから変数グループの作成をします。



名称を「**devops-iac-vg**」としたうえで変数内容を設定し、「save」をクリックします。

Library > devops-iac-vg\*

**Variable group**

Name: devops-iac-vg

Description:

Allow access to all pipelines

Link secrets from an Azure key vault as variables

**Variables**

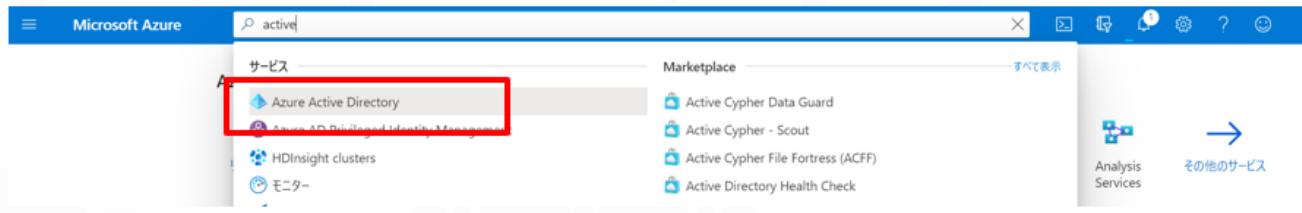
| Name ↑                           | Value |
|----------------------------------|-------|
| SQL_ADMINISTRATOR_LOGIN          |       |
| SQL_ADMINISTRATOR_LOGIN_PASSWORD |       |
| AZURE_DATABRICKS_ID              |       |
| AZURE_RM_SVC_CON_ID              |       |
| AZURE_RM_SVC_CONNECTION          |       |
| BASE_NAME                        |       |
| DEVOPS_ACCOUNT_NAME              |       |
| DEVOPS_PROJECT_NAME              |       |
| DEVOPS_REPOS_NAME                |       |
| DEVOPS_TENANT_ID                 |       |
| GRANT_PUBLIC_IP                  |       |
| LOCATION                         |       |
| RESOURCE_GROUP                   |       |
| VM_ADMINISTRATOR_LOGIN           |       |
| VM_ADMINISTRATOR_LOGIN_PASSWORD  |       |

| 変数名                              | 設定値                       | 備考                                      |
|----------------------------------|---------------------------|---|
| SQL_ADMINISTRATOR_LOGIN          | 任意                        | Azure SQLの管理者ID                         |
| SQL_ADMINISTRATOR_LOGIN_PASSWORD | 任意                        | AzureSQLの管理者パスワード 8文字以上                 |
| AZURE_DATABRICKS_ID              | (要確認)                     | Databricksのテナント内プリンシパルID。確認方法は後述        |
| AZURE_RM_SVC_CON_ID              | (要確認)                     | Azure DevOpsサービス接続のプリンシパルID。確認方法は後述     |
| AZURE_RM_SVC_CONNECTION          | azure-resource-connection | 変更不可                                    |
| BASE_NAME                        | 例 : dev-viz               | 小文字英字7文字以内。各リソースの接頭辞となります。一意となる必要があります。 |
| DEVOPS_ACCOUNT_NAME              | (要確認)                     | 作成したDevOps組織名                           |
| DEVOPS_PROJECT_NAME              | (要確認)                     | 作成したDevOpsプロジェクト名                       |

| 変数名                             | 設定値       | 備考                                 |
|---------------------------------|-----------|------------------------------------|
| DEVOPS_REPOS_NAME               | (要確認)     | 作成したDevOpsRepos名。既定では、プロジェクト名と同様   |
| DEVOPS_TENANT_ID                | (要確認)     | Azure DevOpsの組織を作成したテナントID。確認方法は後述 |
| GRANT_PUBLIC_IP                 | 任意        | 許可対象のGlobal IP ※複数ある場合は、環境構築後に設定   |
| LOCATION                        | japaneast | 東日本を指定                             |
| RESOURCE_GROUP                  | 任意        | デプロイ対象のリソースグループ名                   |
| VM_ADMINISTRATOR_LOGIN          | 任意        | Azure VMの管理者ID                     |
| VM_ADMINISTRATOR_LOGIN_PASSWORD | 任意        | Azure VMの管理者パスワード 英数字大小含む12文字以上    |

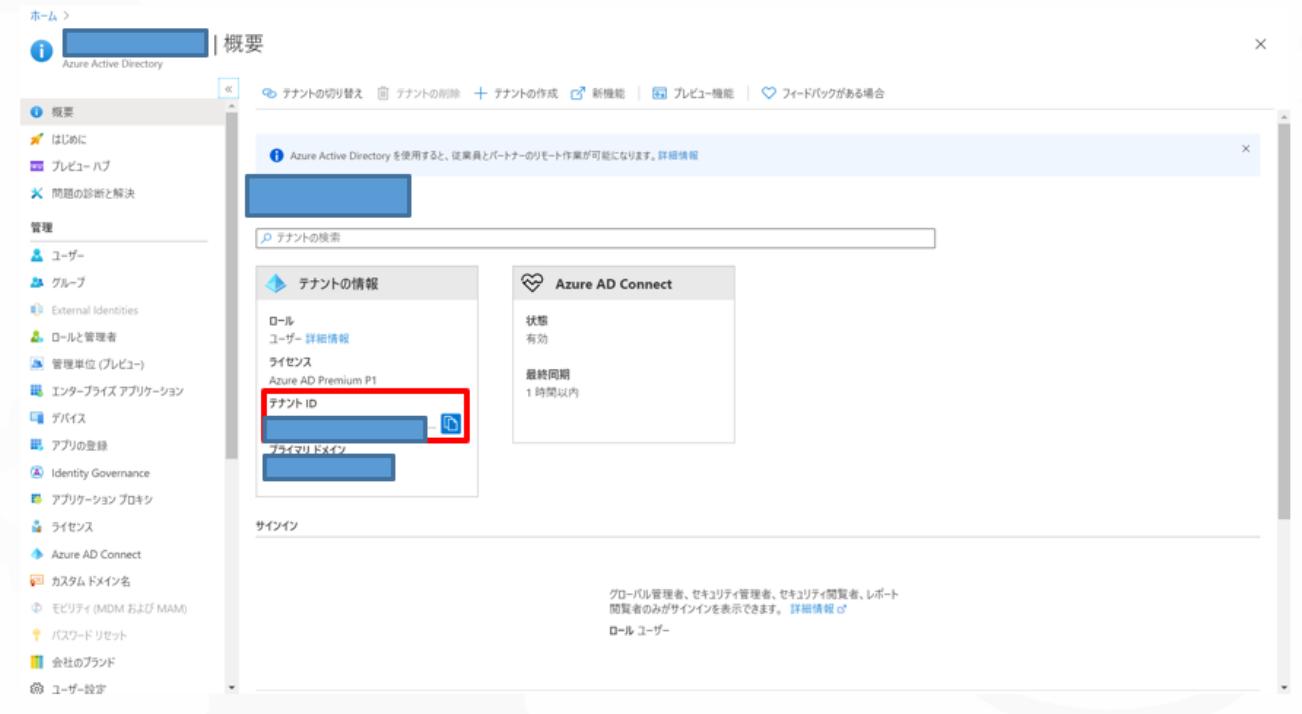
## DatabricksID、テナントIDの確認方法

Azure Portalに移動して、ActiveDirectoryを検索します。



The screenshot shows the Microsoft Azure portal's search interface. A search bar at the top contains the text "active". Below it, a list of services is displayed under the heading "サービス". The "Azure Active Directory" service is highlighted with a red box. Other listed services include "Azure AD Premium Identity Management", "HDInsight clusters", and "モニター". To the right, there's a "Marketplace" section with links to "Active Cypher Data Guard", "Active Cypher - Scout", "Active Cypher File Fortress (ACFF)", and "Active Directory Health Check". There are also icons for "Analysis Services" and a link to "その他のサービス".

テナントIDは概要ページに記載されています。



The screenshot shows the "Azure Active Directory" overview page. On the left, a sidebar menu includes "概要", "はじめに", "プレビュー ハブ", "問題の診断と解決", "管理" (with sub-options like "ユーザー", "グループ", etc.), and "サインイン". The main content area has tabs for "テナントの切り替え", "テナントの削除", "+ テナントの作成", "新機能", "プレビュー機能", and "フィードバックがある場合". A message box says "Azure Active Directory を使用すると、従業員とパートナーのリモート作業が可能になります。詳細情報". Below this is a search bar labeled "テナントの検索". The central panel is titled "テナントの情報" and shows "ロール" (User - 詳細情報), "ライセンス" (Azure AD Premium P1), and the "テナント ID" field, which is highlighted with a red box. To the right, there's a "Azure AD Connect" section showing "状態" (有効) and "最終同期" (1時間以内). At the bottom, there's a "サインイン" section with a note about global administrators, security managers, and report readers.

「エンタープライズアプリケーション」タブに移動して、アプリケーションの種類を「全てのアプリケーション」に変更したうえで「AzureDatabricks」を選択すると、オブジェクトIDが表示されます。

The screenshot shows the Azure Active Directory Enterprise Application Overview page. The left sidebar includes sections for Overview, Troubleshoot, Management (Applications, Users & Groups, Projections), Security (Conditional Access, Consent & Access Requests), Activity (Sign-in, Usage & Analytics, Audit Log, Project Log, Access Review, Manager Approval Request, Troubleshooting + Support, Virtual Assistant), and Help & Support. The main area displays a table for applications, with a row for 'azuredatabricks' highlighted by a red box. The columns include Name (AzureDatabricks), Home Page URL, Object ID (redacted), and Application ID (redacted). At the top, there are filters for Application Type (All Applications selected), Status (All selected), and Visibility (All selected), along with 'Apply' and 'Reset' buttons.

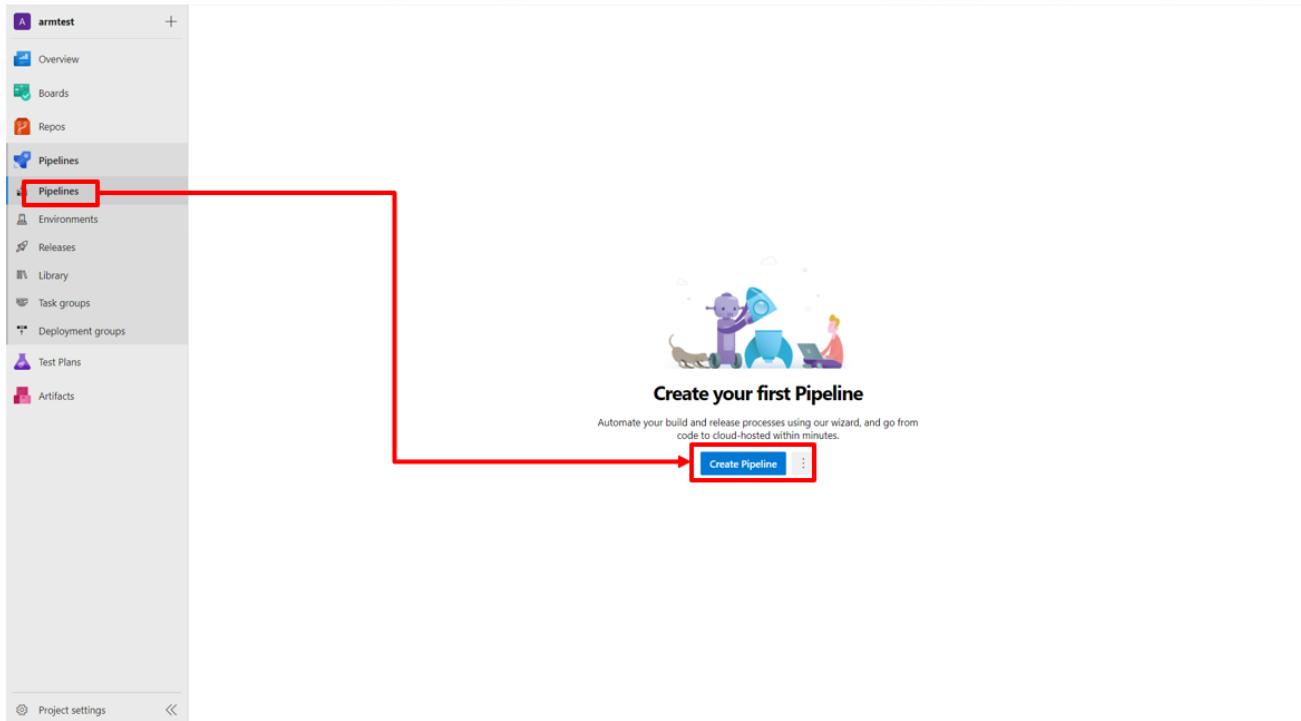
## Azure DevOpsサービス接続のプリンシパルIDの確認方法

リソースグループのアクセス制御(RBAC)画面から、サービスプリンシパルをクリックし、概要画面で確認可能です。

The screenshot shows the Azure RBAC Overview page. The left sidebar includes sections for Overview, Troubleshoot, Management (Properties, Owners, Users & Groups, Projections), and Help & Support. The main area displays a table for service principals, with a row for 'NA' highlighted by a red box. The columns include Name (NA), Application ID (redacted), and Object ID (redacted). The 'Properties' tab is selected in the sidebar.

## 6. Pipeline読み込み, 実行

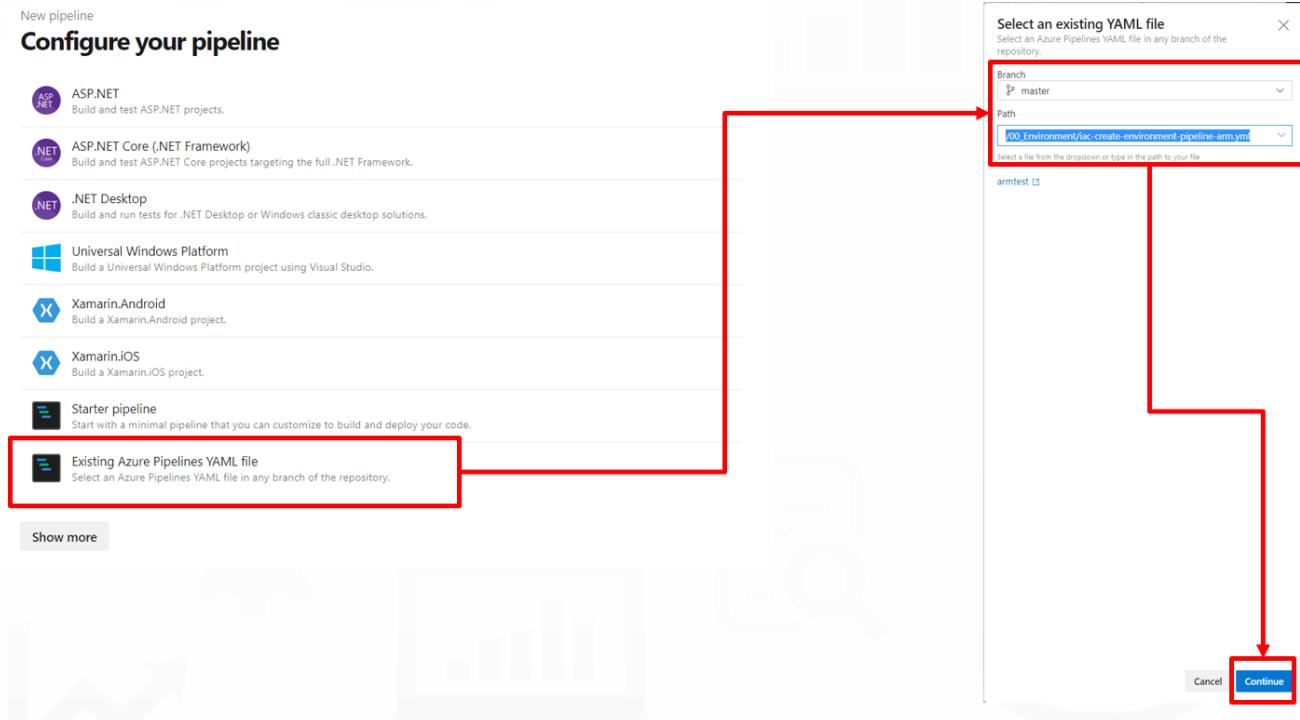
DevOpsに戻り、Pipelineの作成を行います。



「Azure Repos Git」 → 「<repository名>」の順に選択します。

The image contains two side-by-side screenshots. The left screenshot shows the 'Where is your code?' step of the 'New pipeline' wizard. It lists several options: 'Azure Repos Git' (selected), 'Bitbucket Cloud', 'GitHub', 'GitHub Enterprise Server', 'Other Git', and 'Subversion'. A red box surrounds the 'Azure Repos Git' option. The right screenshot shows the 'Select a repository' step. It displays a list of repositories with a search bar at the top. One repository, 'armtest', is selected and highlighted with a red box. A red arrow points from the 'armtest' repository in the second screenshot back to the 'Azure Repos Git' option in the first screenshot.

「Existing Azure Pipelines YAML file」 → 「/00\_Environment/iac-create-environment-pipeline-arm.yml」の順に選択します。



YAMLファイルの内容が表示されるので、「RUN」をクリックします。

```

New pipeline
Review your pipeline YAML

00_Environment / iac-create-environment-pipeline-arm.yml

1 # CI/PR Pipeline that deploys an ARM template to create or update the resources needed by the other pipelines.
2 trigger:
3   branches:
4     - include:
5       - master
6   paths:
7     - include:
8       - 00_Environment/arm-templates/*
9 pr:
10   branches:
11     - include:
12       - master
13   paths:
14     - include:
15       - 00_Environment/arm-templates/*
16 pool:
17   vmImage: "ubuntu-latest"
18 variables:
19   - group: devops-iac-vg
20 steps:
21   - task: AzureResourceGroupDeployment@2
22     settings:
23       inputs:
24         azureSubscription: "$(AZURE_RM_SVC_CONNECTION)"
25         action: "Create Or Update Resource Group"
26         resourceGroupName: "$(RESOURCE_GROUP)"
27         location: "$(LOCATION)"
28         templateLocation: "Linked artifact"
29         csmFile: "$(Build.SourcesDirectory)/00_Environment/arm-templates/cloud-environment.json"
30         overrideParameters: "-baseName $(BASE_NAME) -location $(LOCATION) -sqlAdministratorLogin $(SQL_ADMINISTRATOR_LOGIN) -sqlAdministratorLoginPassword $(SQL_ADMINISTRATOR_LOGIN_PASSWORD) -devOpsAc"
31         deploymentMode: "Incremental"
32         displayName: "Deploy resources to Azure"
33
34
35
  
```

Variables Run Show assistant

## リソース設定 - Azure SQL

Azure SQLの設定を行います。

### Azure SQL設定手順概要

1. IPアドレスの追加
2. ad管理者の設定
3. adfリソース追加

## 1. IPアドレスの追加

Azure Portal上での、SQL Serverのリソースに移動します。



sql | 種類 == (すべて) × 場所 == (すべて) × フィルターの追加

3件中 1 ~ 3 件のレコードを表示しています。  非表示の型の表示 ⓘ

名前 ↑↓ 場所 ↑↓

SQL Server 東日本 ...

sql-sandbox

「ファイアウォール設定の表示」をクリックします。



リソース グループ ([変更](#)) : iac\_sandbox

状態 : 利用可能

サーバー管理者 : sqladmin

ファイアウォールと仮想ネット... : [ファイアウォール設定の表示](#)

クライアントIPのリストに必要なIPアドレスが記載されていることを確認して、不足していれば追加の上、保存します。

### 補足

IPアドレスの設定はSQL ServerのリソースをARMテンプレートとしてエクスポートして、該当箇所を cloud-environment.json に反映することで、同様の設定が再現できます。

## 2. AD管理者の設定

「Active Directory管理者」→「管理者の設定」に移動して、ユーザorグループを選択します。



保存をクリックします。



### 3. DataFactoryリソースへの権限付与

Databaseのリソースに移動します。

Azure portal search results for 'db'. The search bar shows 'db'. The results list shows one item: 'db (sql...-sqldb) SQL データベース'. The 'SQL データベース' part is highlighted with a red box.

「クエリエディター」に移動して、AD認証でログインします。

クエリエディター (プレビュー) のスクリーンショット。左側のナビゲーションメニューでは 'クエリエディター (プレビュー)' が選択されています。右側には SQL データベースの認証オプションが表示されています。赤い枠で囲まれた部分は Active Directory 認証の 'としてログインします' ボタンです。

以下のスクリプトを実行します。※リソース名は適宜変更してください。

```
-- sql  
CREATE USER [DataFactoryのリソース名] FROM EXTERNAL PROVIDER;  
ALTER ROLE [db_owner] ADD MEMBER [DataFactoryのリソース名];
```

## 4 Databricksの設定

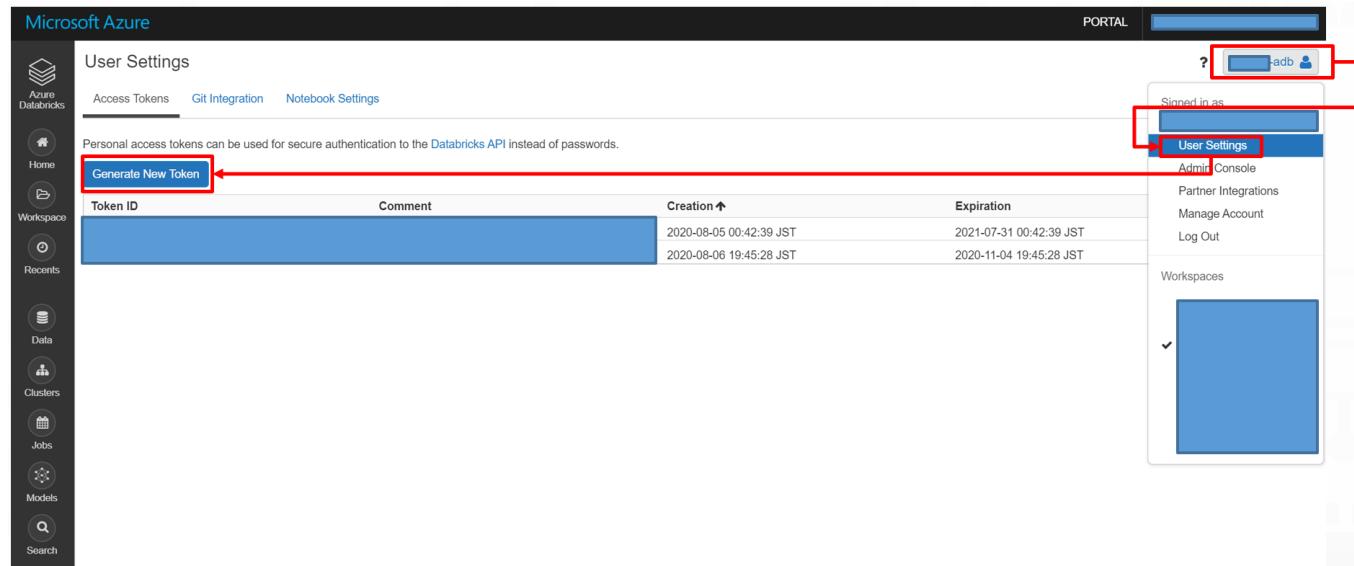
### Databricksの設定手順概要

1. PAT(Private Access Token)の作成
2. Scope作成
3. KeyvaultSecretの登録

## 1. PAT(Private Access Token)の作成

PATを利用して、他のシステムに権限を委任して各種の操作が可能になります。※PATの権限は発行者に基づきます。

Databricksのリソースに移動して、「Workspaceの起動」から、ワークスペースにログインします。  
ログイン後、以下の図のように画面を選択し、「Generate New Token」をクリックします。



コメントと利用期限を設定し、「Generate」をクリックします。  
表示されたPATは後の手順で利用するのでメモしてください。

# Generate New Token

Comment

What's this token for?

Lifetime (days) ?

90

Cancel

Generate

## 2. Scope作成

DatabricksのURLに「#secrets/createScope」を追加して移動します。

例：



以下のように設定して、「Create」をクリックします。

Create Secret Scope | [Cancel](#) [Create](#)

A store for secrets that is identified by a name and backed by a specific store type. [Learn more](#)

Scope Name ?

Manage Principal ?

Azure Key Vault ?

DNS Name

Resource ID

)

| 項目               | 設定値       | 備考                             |
|------------------|-----------|--------------------------------|
| Scope Name       | akv       | Notebookで利用するものとあわせてください       |
| Manage Principal | All Users | 適宜変更可能                         |
| DNS Name         |           | Azure Key VaultのDNS名。確認方法は後述   |
| Resource ID      |           | Azure Key VaultのリソースID。確認方法は後述 |

### Azure Key VaultのDNS名、リソースIDの確認方法

Key Vaultのリソースに移動し、プロパティをクリックすることで確認可能です。

The screenshot shows the 'Properties' tab of a Key Vault resource named 'aml-akv'. The 'Resource ID' field contains the URL: `https://[REDACTED]vault.azure.net/`. A red arrow points from the left margin to the 'Resource ID' field. To the right of the URL is a 'Copy to clipboard' button.

Key Vault Properties - aml-akv | プロパティ

概要

SKU (価格レベル) 標準

場所 japaneast

DNS 名 https://[REDACTED]vault.azure.net/

リソース ID /subscriptions/[REDACTED]/resourceGroups/iac\_sandbox/providers/Microsoft.KeyVault/vaults/[REDACTED]-akv

サブスクリプション ID [REDACTED]

サブスクリプション名 [REDACTED]

ディレクトリ ID [REDACTED]

ディレクトリ名 [REDACTED]

論理的な削除

このコンテナーとそのオブジェクトの回復を有効にする

このコンテナーとそのオブジェクトの回復を無効にする

削除されたコンテナーを保持する日数 90

削除保護

このコンテナーとそのオブジェクトの、保持期間中の消去を許可する

このコンテナーとそのオブジェクトの、保持期間中の削除保護を有効にする

プロパティ

ロック

テンプレートのエクスポート

監視

分析情報 (レビュー)

警告

メトリック

### 注意

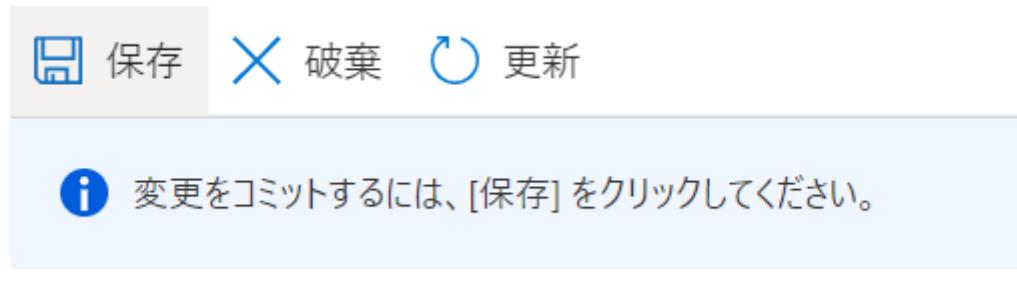
本テンプレートではKey Vaultは**2つ作成されます（Azure ML用、その他用）** AZure ML専用のリソースには **-aml-kv** と付与されているため、その他用である末尾が **-akv** となっているリソースを選択してください。

### 3. KeyvaultSecretの登録

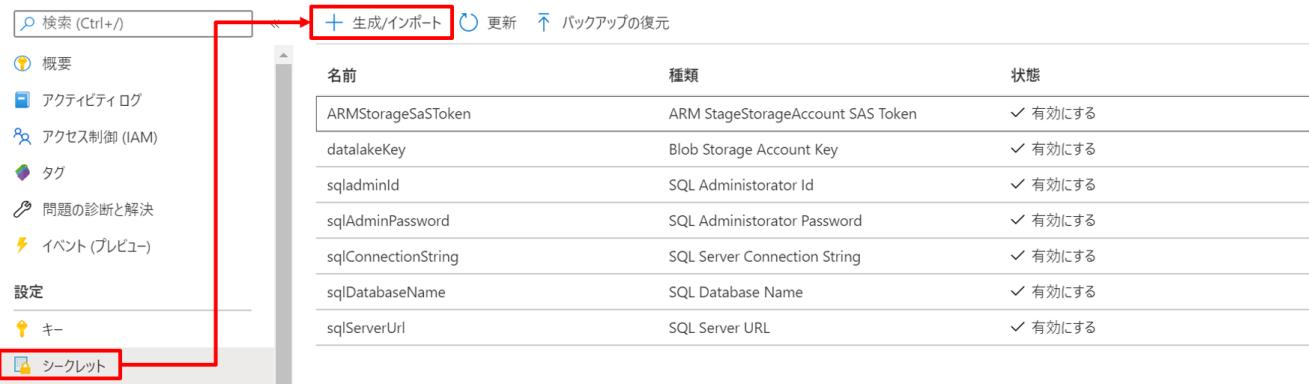
Key Vaultのリソースで、アクセスポリシーを追加します。「アクセスポリシー」→「アクセスポリシーの追加」に移動し、「キー、シークレット、および証明書の管理」を選択の上、「プリンシパルの選択」で自身を選択して、「追加」をクリックします。



追加後、保存します。



次に、シークレットの作成画面に移動して、「生成/インポート」をクリックします。



内容を設定して、作成します。

## シークレットの作成

### アップロード オプション

手動



名前 \* ⓘ

databrickssecret



値 \* ⓘ

.....



コンテンツの種類 (省略可能)

アクティブ化する日を設定しますか? ⓘ

有効期限を設定しますか? ⓘ

有効ですか?

はい

いいえ

作成

| 項目           | 設定値              | 備考                         |
|--------------|------------------|----------------------------|
| アップロード オプション | 手動               | 既定設定                       |
| 名前           | databrickssecret | DataFactoryで利用されているため、変更不可 |

| 項目                | 設定値            | 備考 |
|-------------------|----------------|----|
| 値                 | <PATを貼り付け<br>> |    |
| コンテンツの種類          | 任意の値           |    |
| アクティブ化する日を設定しますか？ | チェックしない        | 既定 |
| 有効期限を設定しますか？      | チェックしない        | 既定 |
| 有効ですか？            | はい             | 既定 |

## 確認

Data Factoryの作成画面から、Linked Service、およびSelf-hosted IRの接続が正常であることが確認できます。

## 次のステップ

[Azure SQL DBプロジェクトのデプロイ](#)