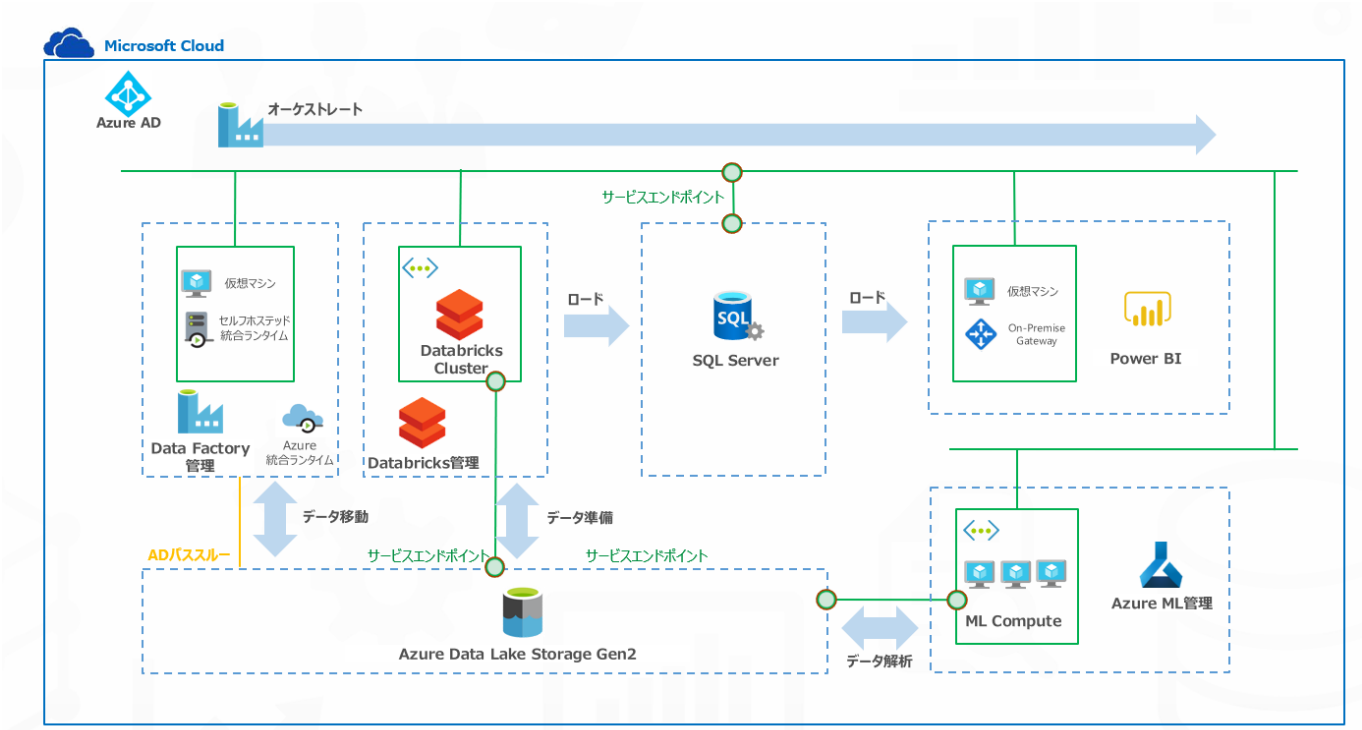
環境構築手順

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。

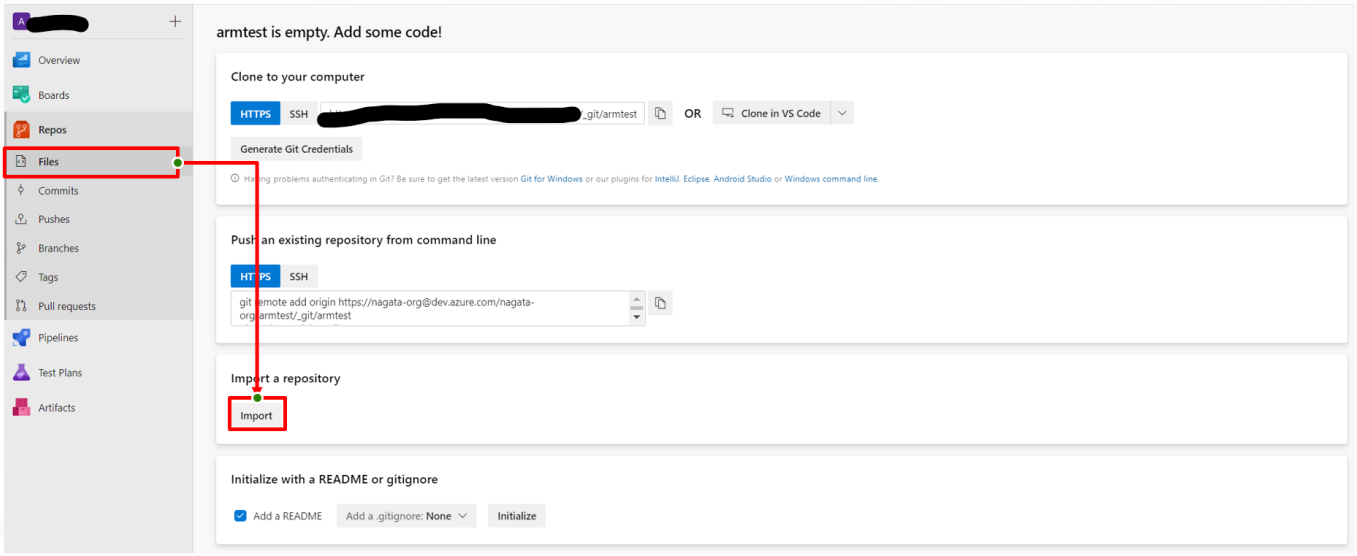
1. Azure DevOps Servicesの構成

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。

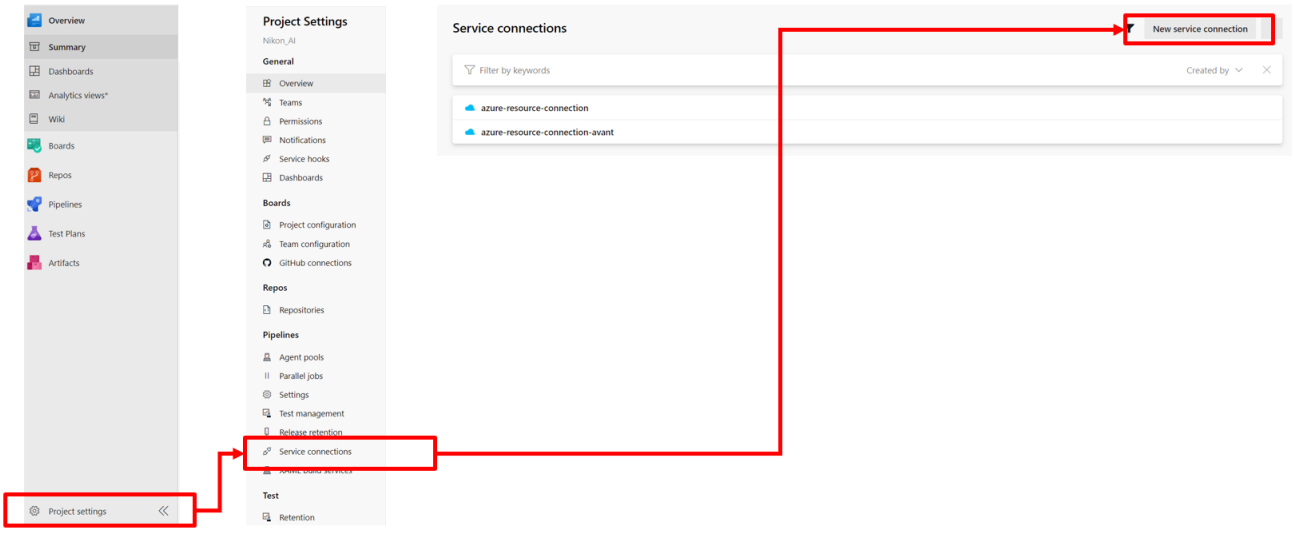


インポートのための設定をして、「Import」を選択します。
正常終了するとコードがインポートされます。

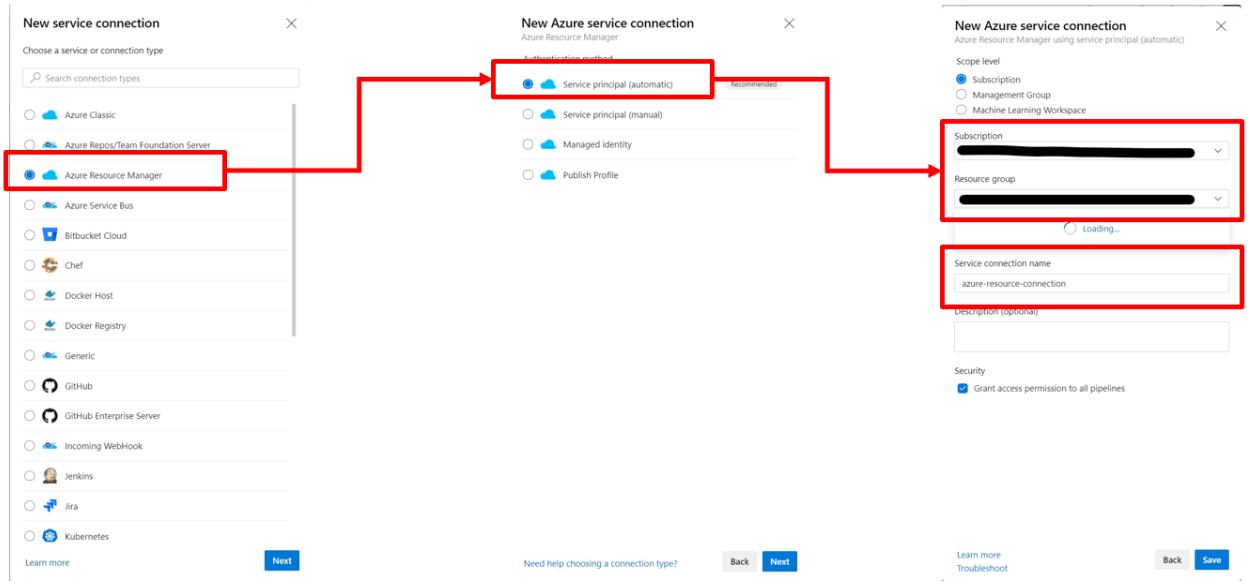
項目	設定値	備考
Repository type	Git	
Clone URL	講師からお伝えします	
Requires Authentication	チェックします	
User Name	空白	
Password / PAT	講師からお伝えします	

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。

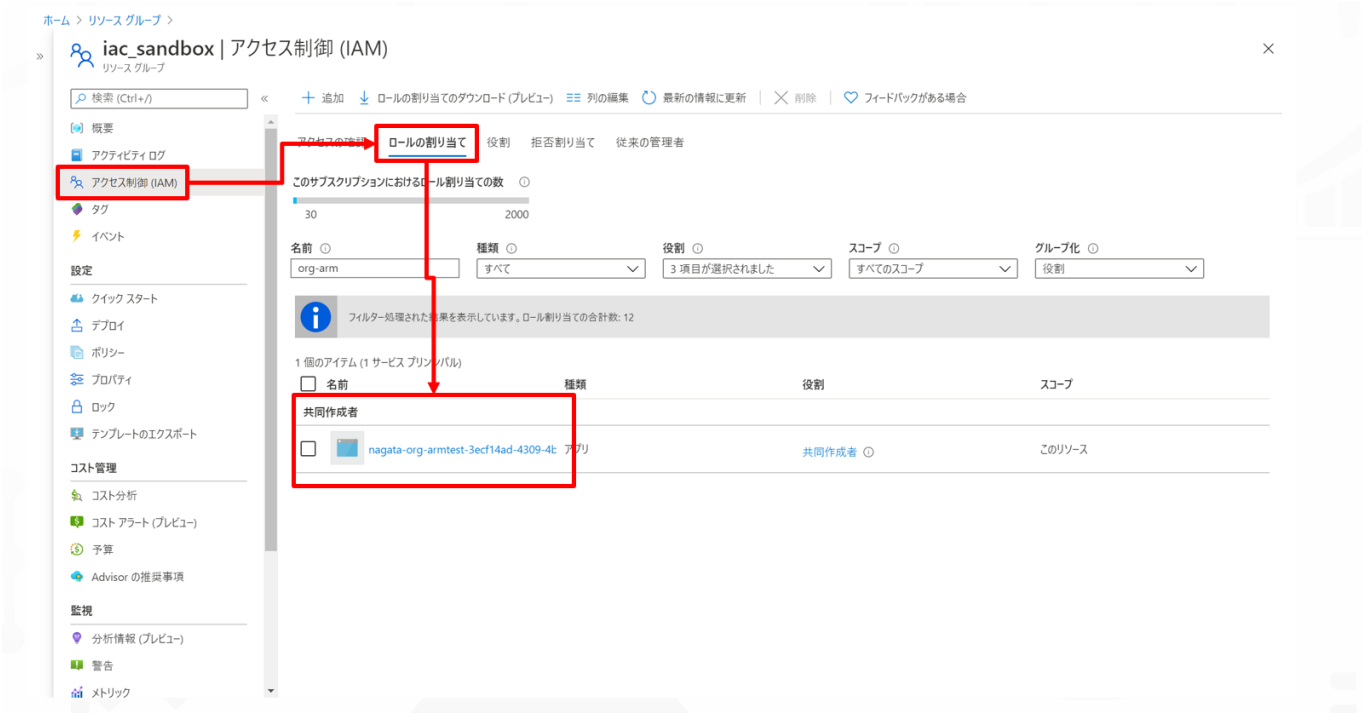


デプロイ対象のリソースグループ、サブスクリプションを指定し、名称を「**azure-resource-connection**」に設定し、「save」を選択します。



4. サービスプリンシパルの権限を所有者に変更

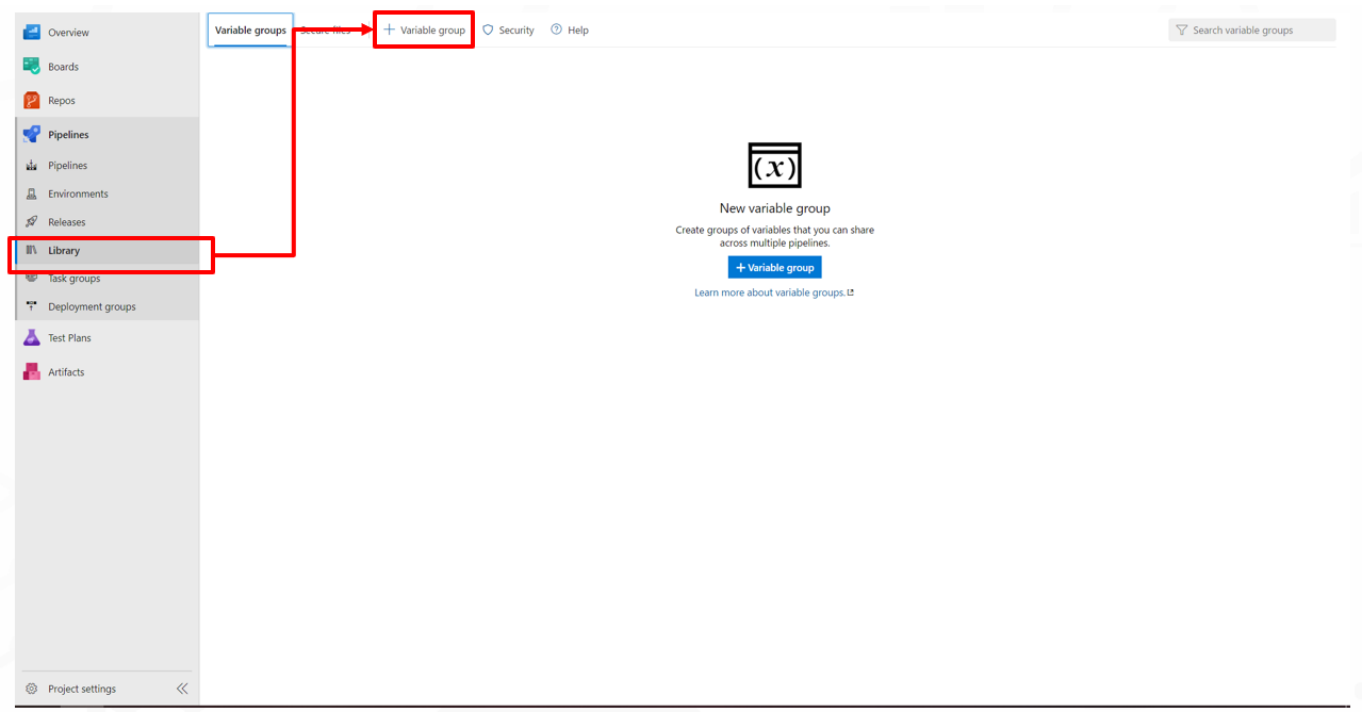
Azure Portalに移動して、リソースグループの共同作成者にDevOpsプロジェクトの名称ではじまるサービスプリンシパルが登録されていることを確認します。



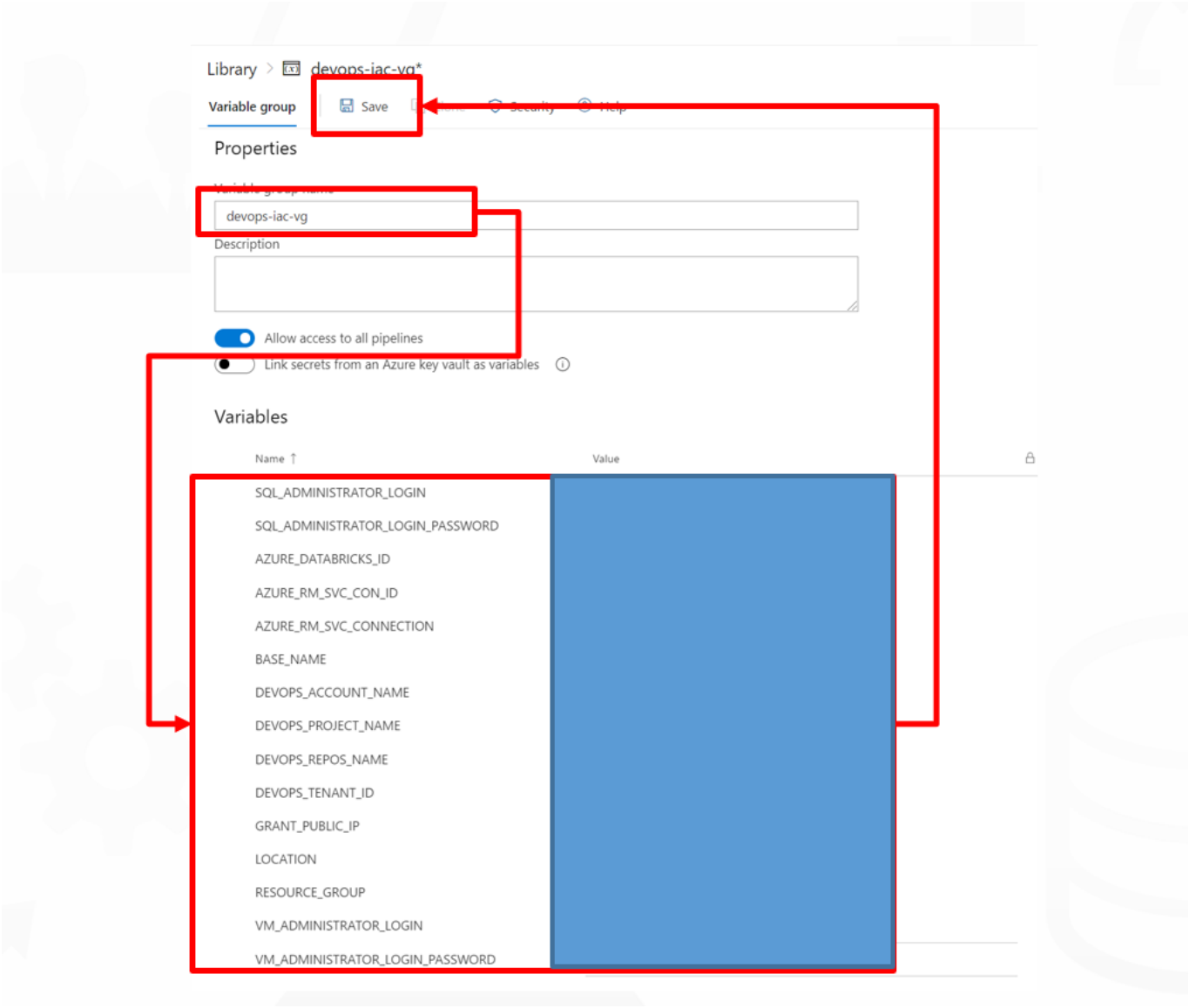
[追加]ボタンから、対象のサービスプリンシパルを所有者に登録します。

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。

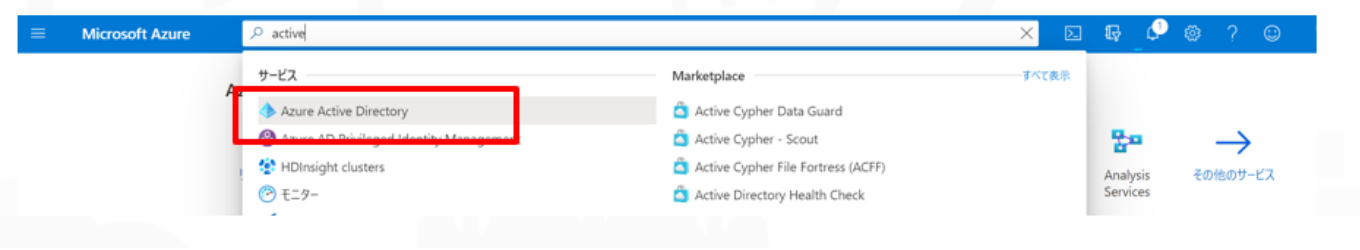


変数名	設定値	備考
SQL_ADMINISTRATOR_LOGIN	任意	Azure SQLの管理者ID
SQL_ADMINISTRATOR_LOGIN_PASSWORD	任意	AzureSQLの管理者パスワード 8文字以上
AZURE_DATABRICKS_ID	(要確認)	Databricksのテナント内プリンシパルID。確認方法は後述
AZURE_RM_SVC_CON_ID	(要確認)	Azure DevOpsサービス接続のプリンシパルID。確認方法は後述
AZURE_RM_SVC_CONNECTION	azure-resource-connection	変更不可
BASE_NAME	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

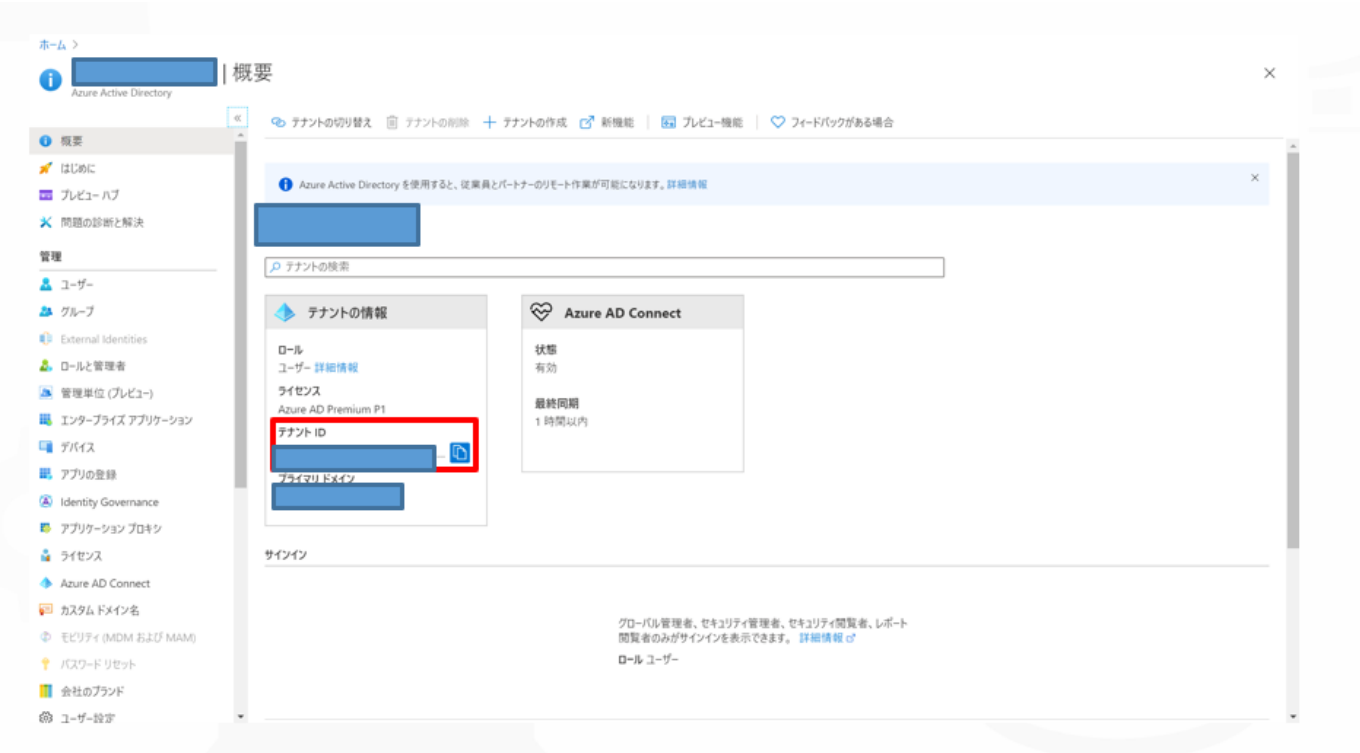
変数名	設定値	備考
DEVOPS_REPOS_NAME	(要確認)	作成したDevOpsRepos名。既定では、プロジェクト名と同様
DEVOPS_TENANT_ID	(要確認)	Azure DevOpsの組織を作成したテナントID。確認方法は後述
GRANT_PUBLIC_IP	任意	許可対象のGlobal IP ※複数ある場合は、環境構築後に設定
LOCATION	japaneast	東日本を指定
RESOURCE_GROUP	任意	デプロイ対象のリソースグループ名
VM_ADMINISTRATOR_LOGIN	任意	Azure VMのの管理者ID
VM_ADMINISTRATOR_LOGIN_PASSWORD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

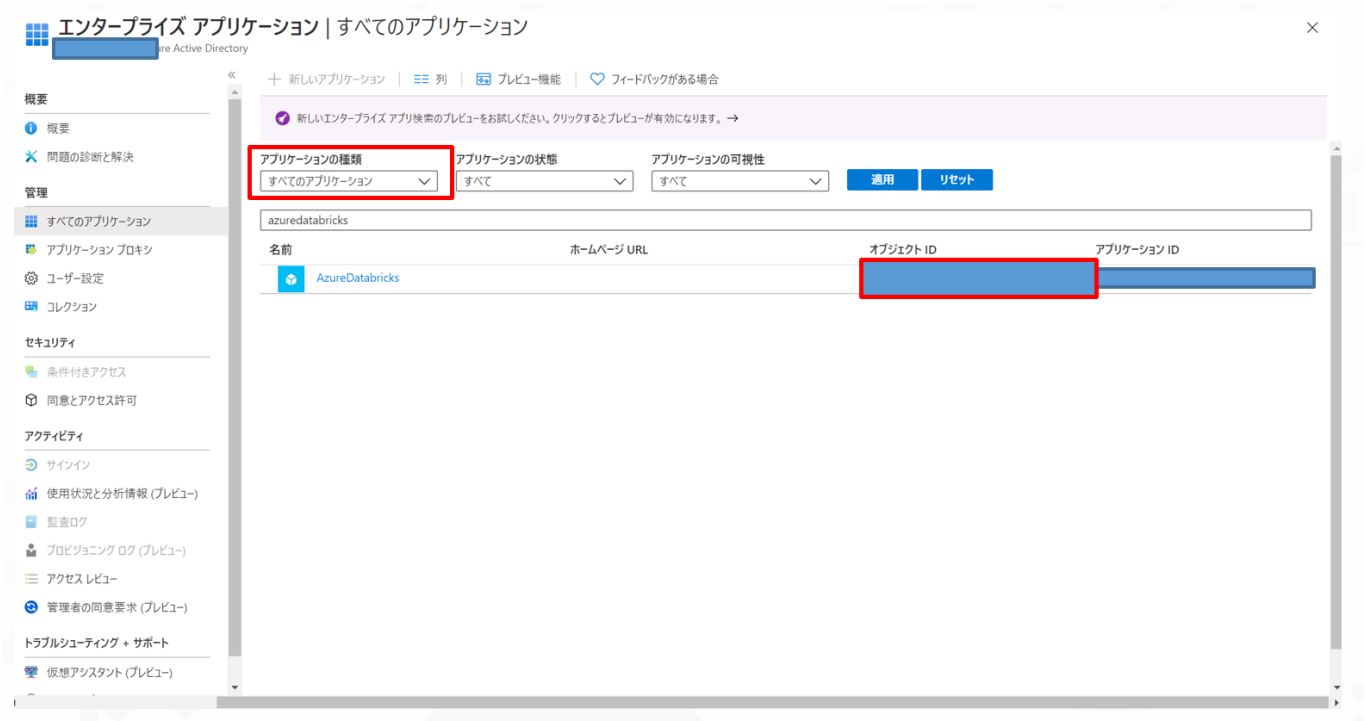
Azure Portalに移動して、ActiveDirectoryを検索します。



テナントIDは概要ページに記載されています。

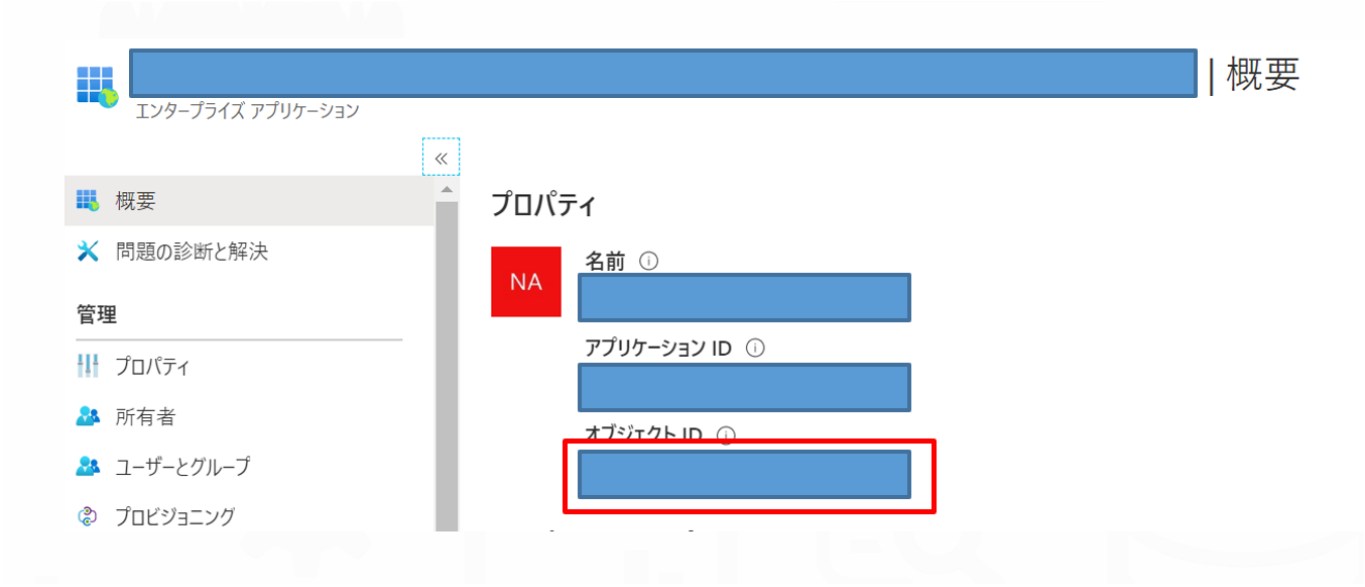


「エンタープライズアプリケーション」タブに移動して、アプリケーションの種類を **「全てのアプリケーション」** に変更したうえで「AzureDatabricks」を選択すると、オブジェクトIDが表示されます。



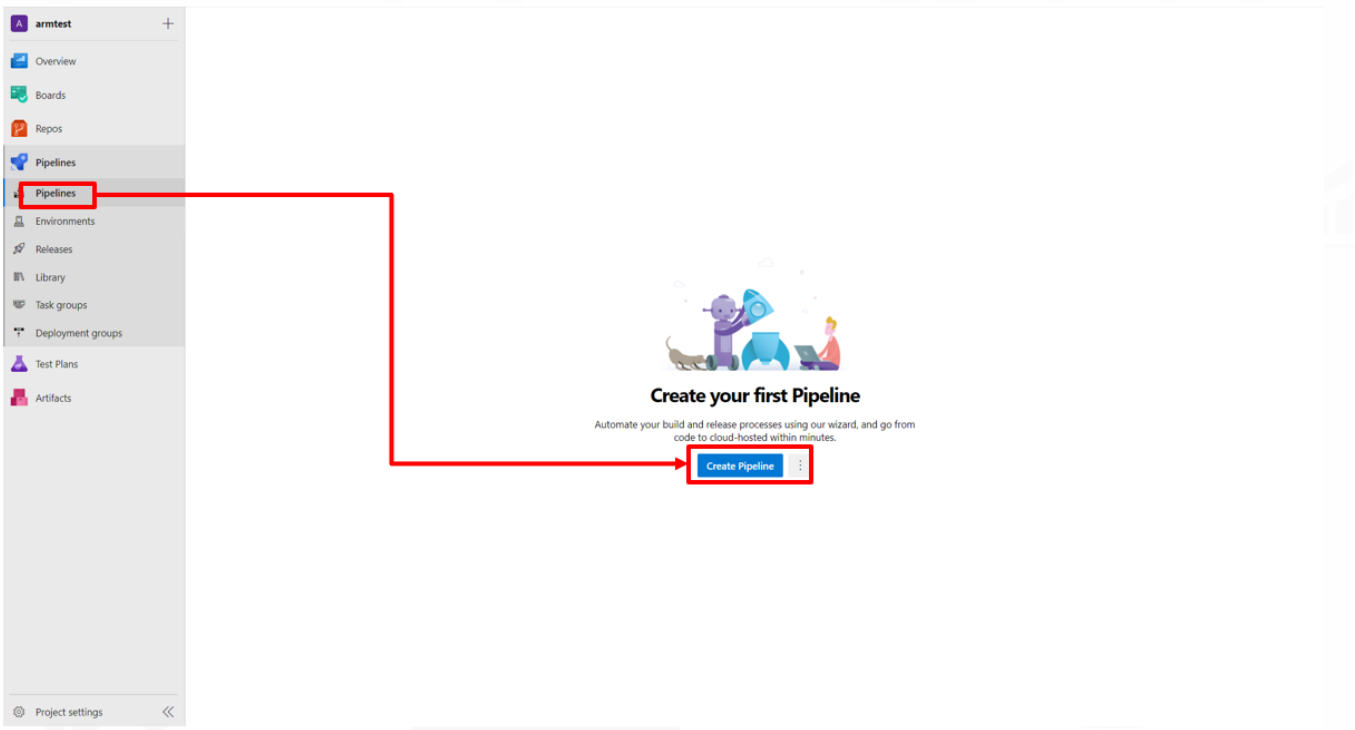
Azure DevOpsサービス接続のプリンシパルIDの確認方法

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。

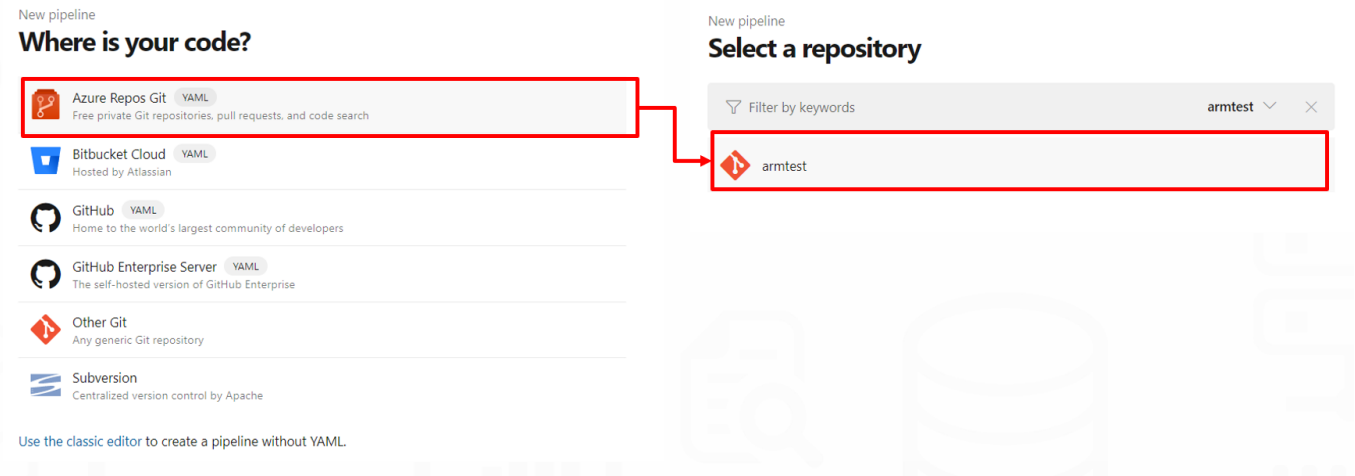


6. Pipeline読み込み,実行

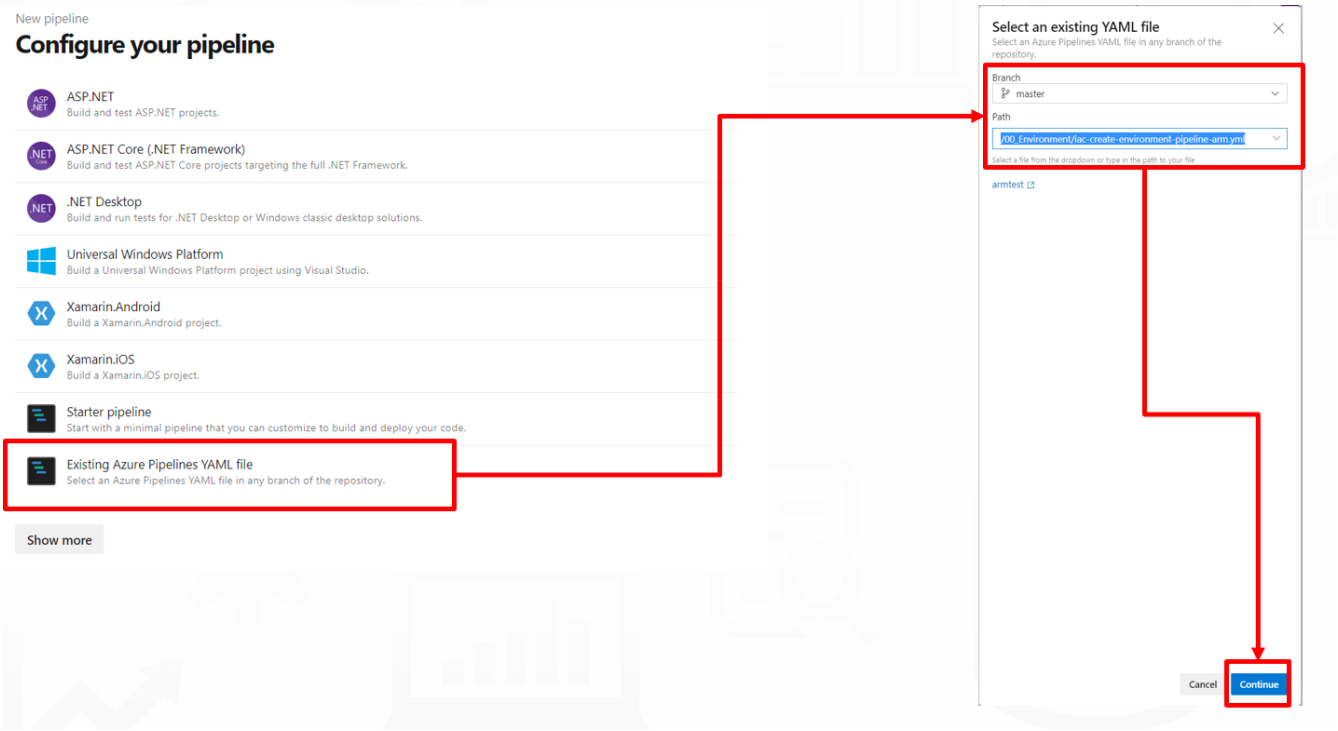
DevOpsに戻り、Pipelineの作成を行います。



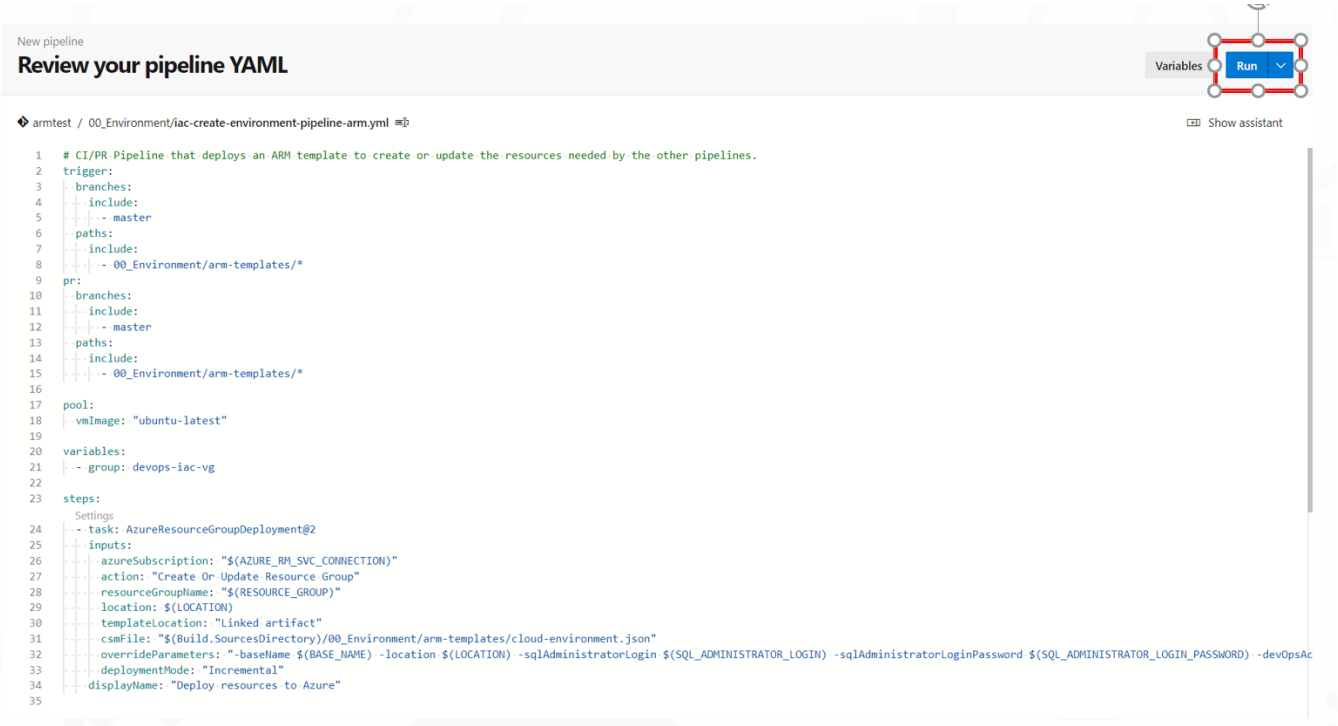
「Azure Repos Git」→「<repository名>」の順に選択します。



「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。



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上の、SQL Serverのリソースに移動します。

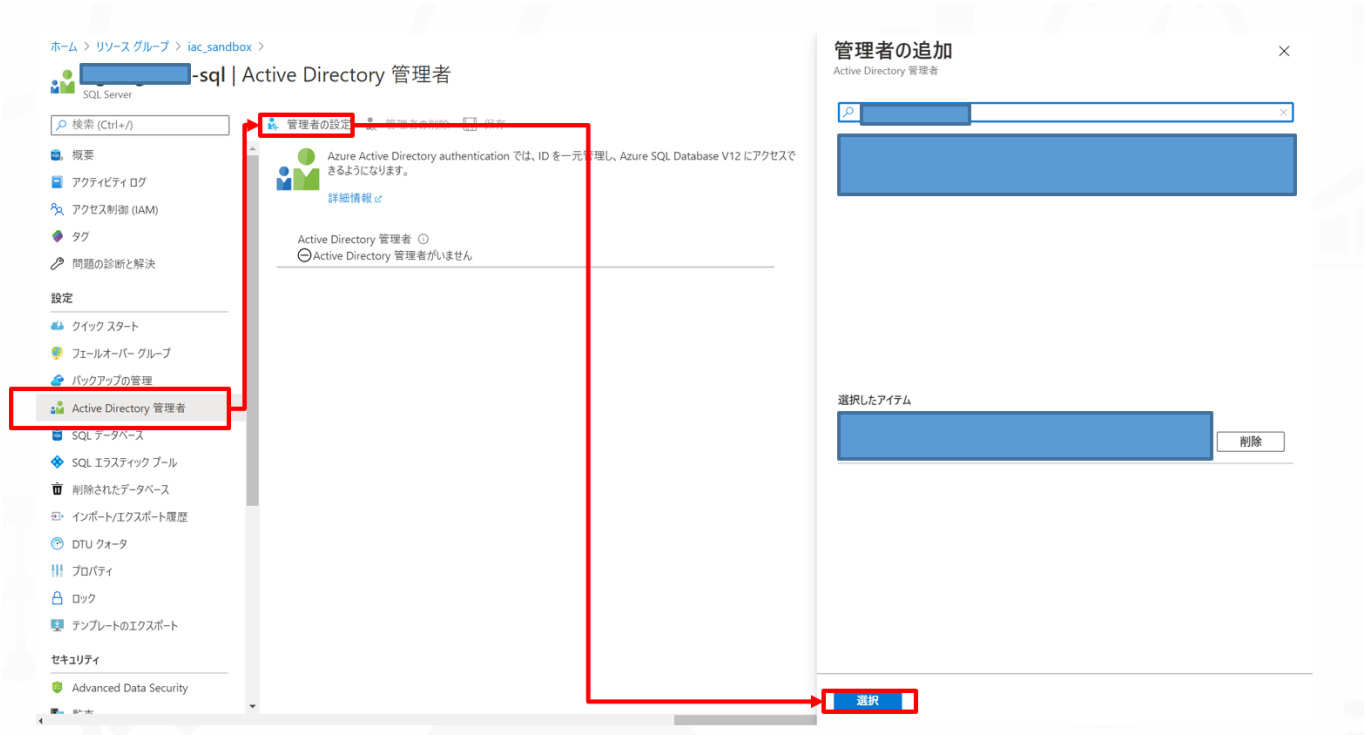
「ファイアウォール設定の表示」をクリックします。

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。

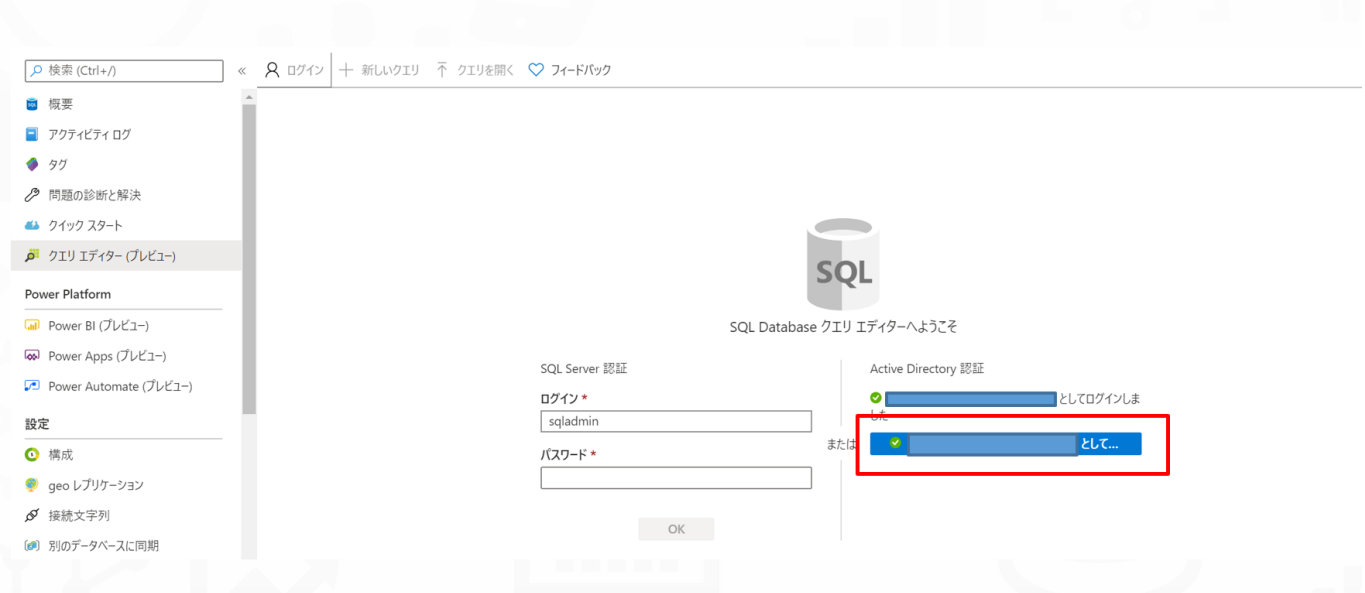


保存をクリックします。

3. DataFactoryリソースへの権限付与

Databaseのリソースに移動します。

「クエリエディター」に移動して、AD認証でログインします。



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

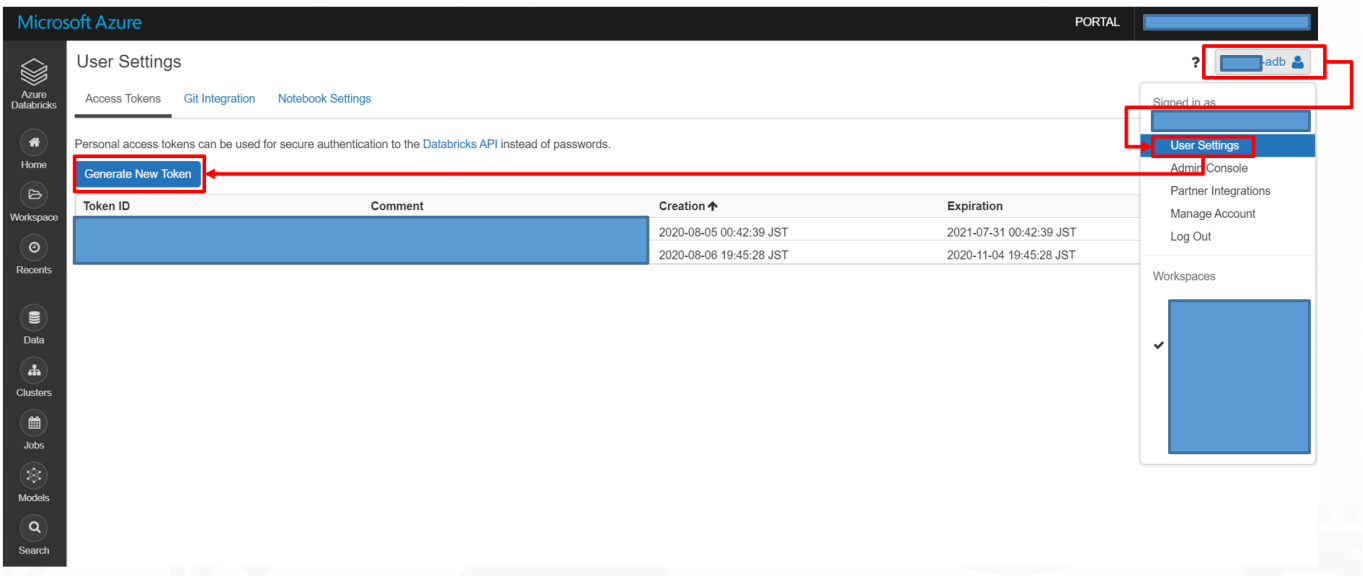
Databricksの設定手順概要

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

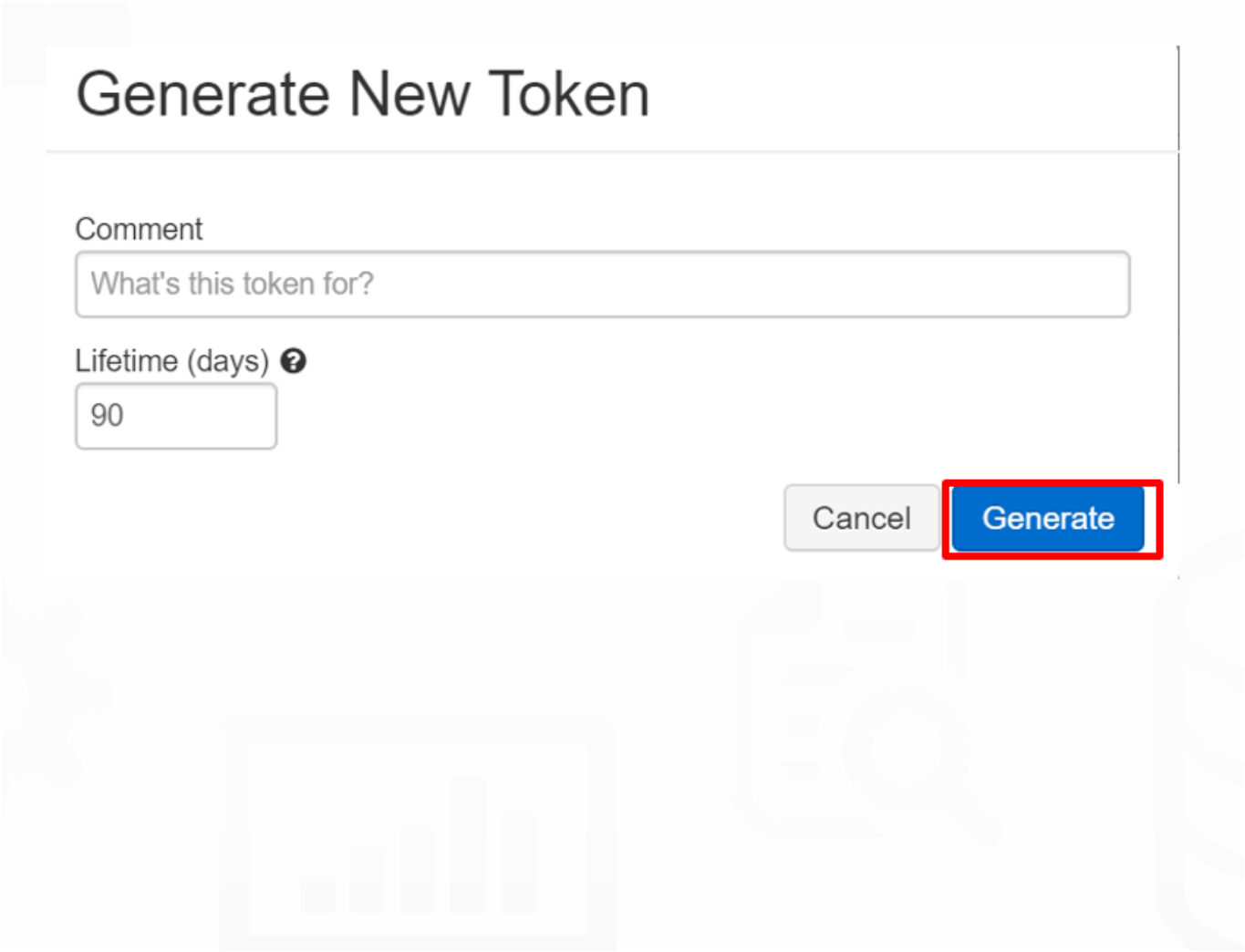
1. PAT(Private Access Token)の作成

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。



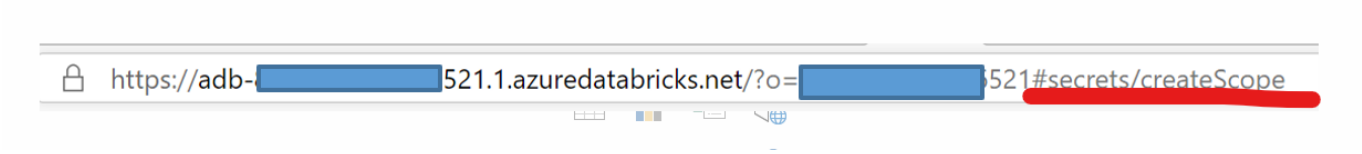
コメントと利用期限を設定し、「Generate」をクリックします。
表示されたPATは後の手順で利用するのでメモしてください。


Generate New Token
Comment
What's this token for?
Lifetime (days)
90
Cancel
Generate

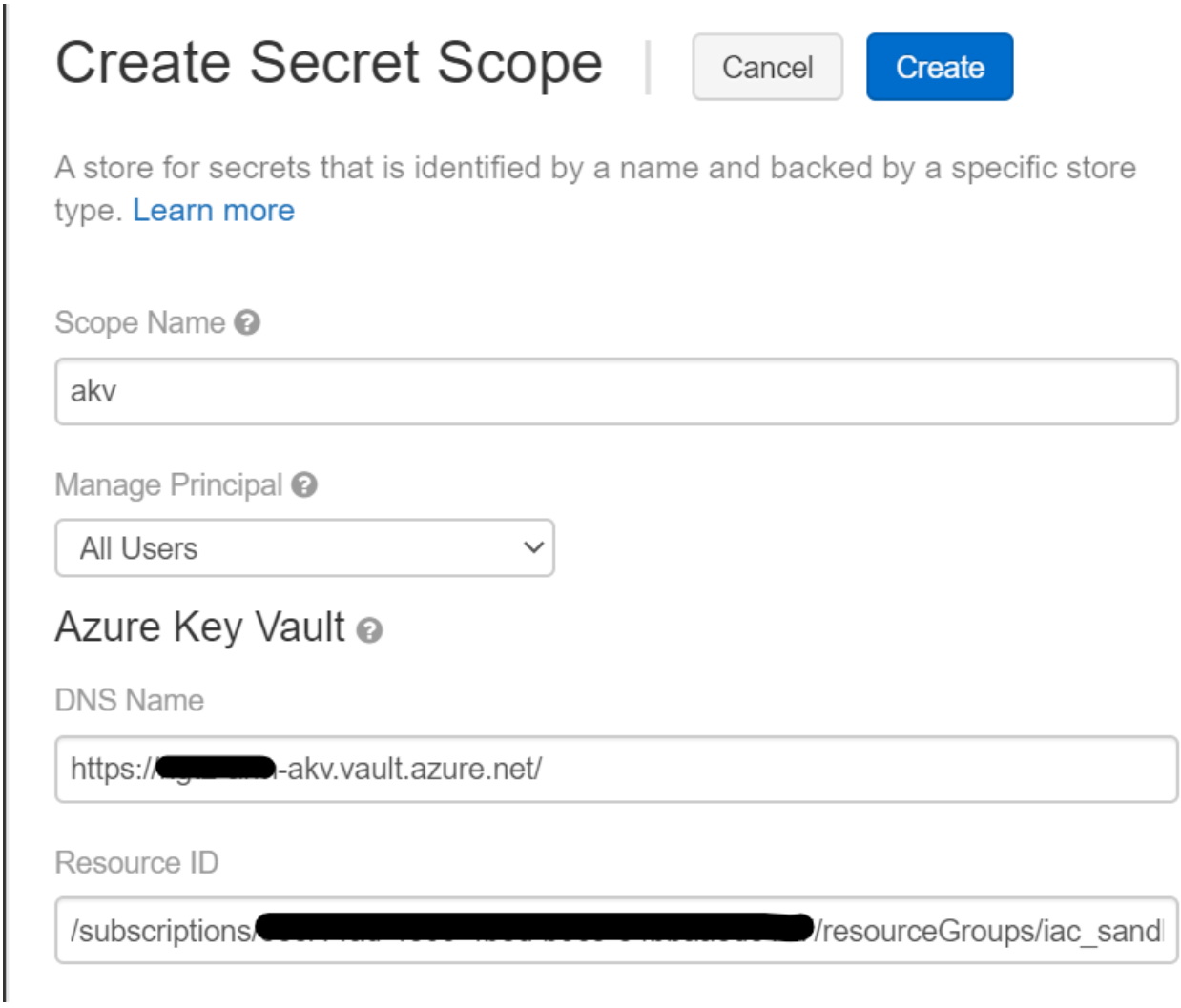
2. Scope作成

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。

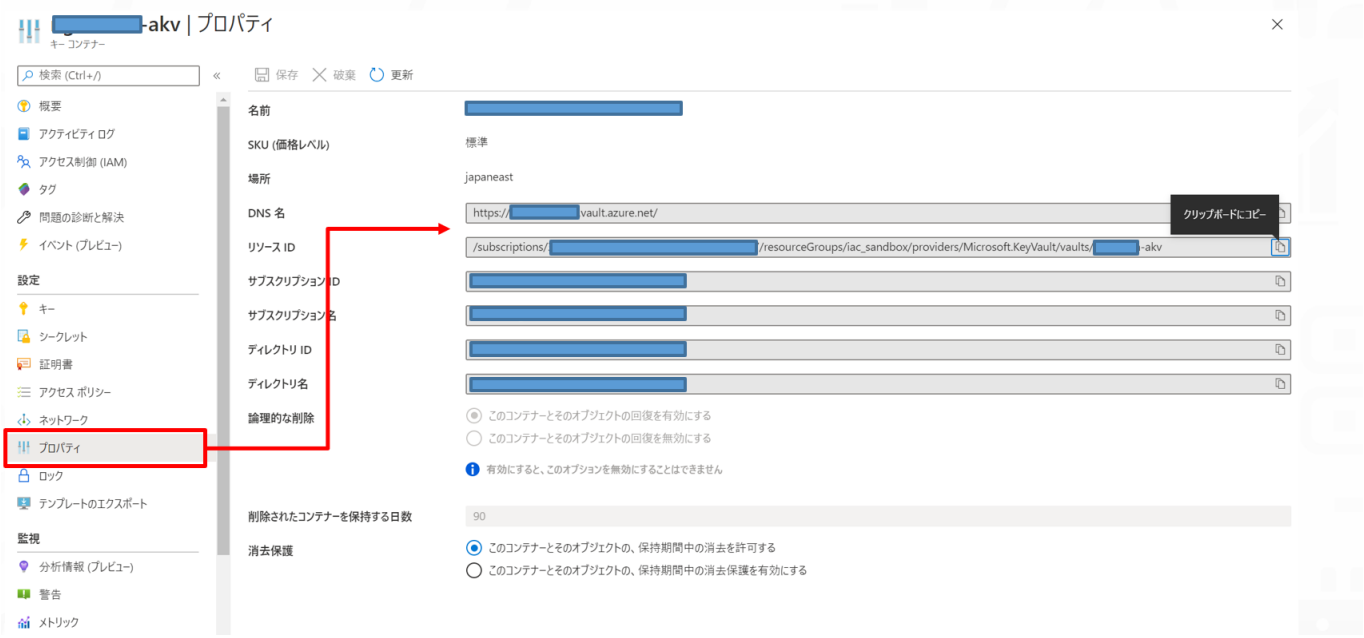


)

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
Resouce 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。

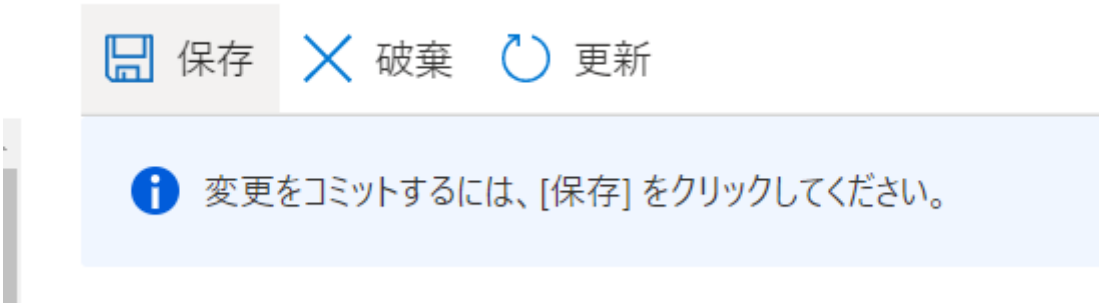


> 注意
> 本テンプレートではKey Vaultは**2つ作成されます（Azure ML用、その他用）** AZure ML専用のリソースには ***-aml-kv*** と付与されているため、その他用である末尾が ***-akv*** となっているリソースを選択してください。

3. KeyvaultSecretの登録

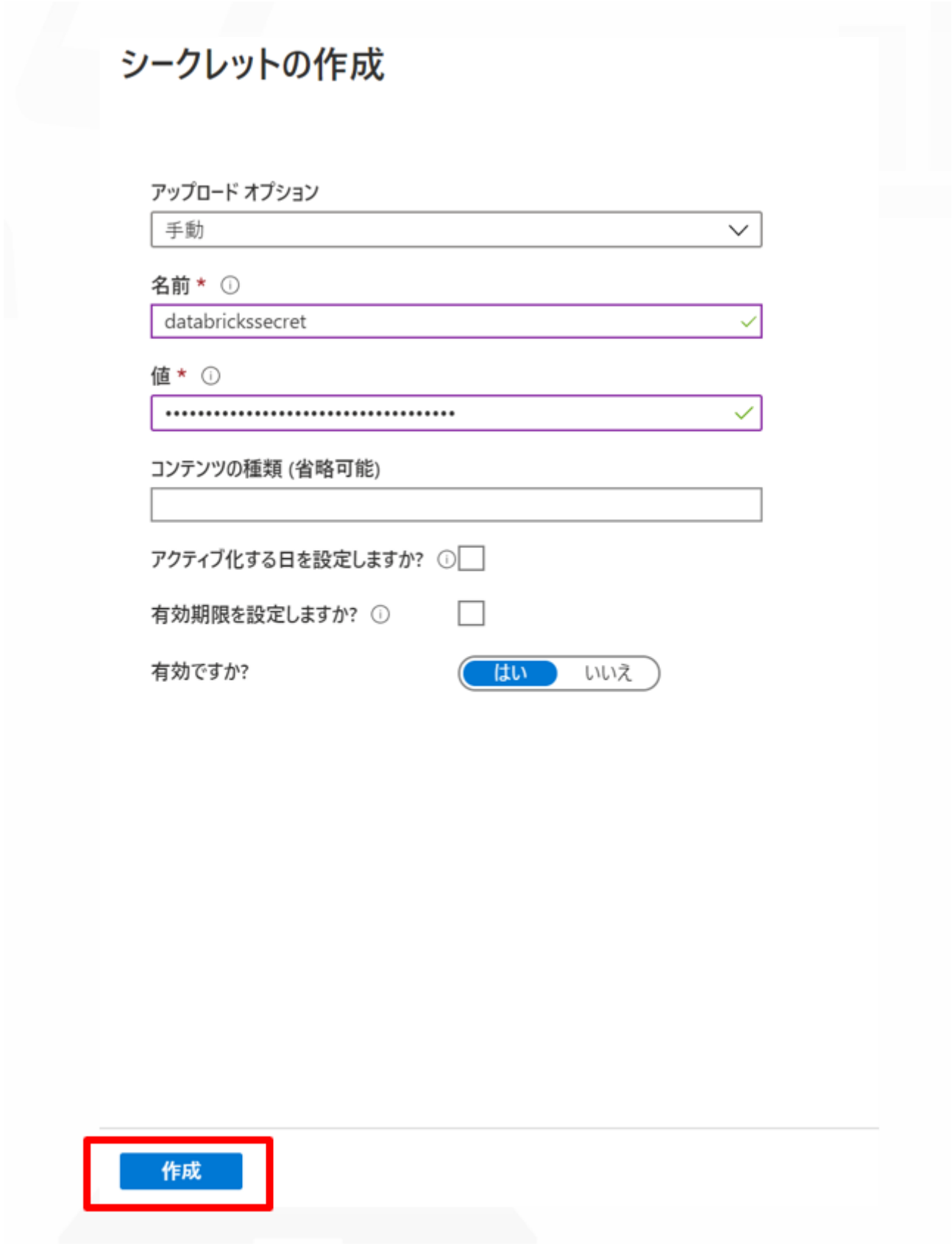
Key Vaultのリソースで、アクセスポリシーを追加します。「アクセスポリシー」→「アクセスポリシーの追加」に移動し、「キー、シークレット、および証明書の管理」を選択の上、「プリンシパルの選択」で自身を選択して、「追加」をクリックします。

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。



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>	
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