演習 - Azure Key Vault でパスワードを管理する

100 XP

5 分

このモジュールでは、サンドボックスを完了する必要があります。 **サンドボックス**で無料リソースにアクセスできます。 お客様の個人のサブスクリプションに対する課金は行われません。 サンドボックスを使用できるのは、Microsoft Learn のトレーニングを完了するためだけです。 その他の目的で利用することは禁止されており、サンドボックスに永久にアクセスできなくなる可能性があります。

サインインしてサンドボックスをアクティブにする

この演習では、Azure Key Vault にパスワードを追加します。 パスワードは、保護する必要がある機密情報の例です。 その後、Azure Key Vault からパスワードを読み取って、パスワードがアクセス可能であることを確認します。

実際には、Azure Key Vault にシークレットを追加し、Azure Key Vault からシークレットを読み取るには、いくつかの方法があります。 Azure portal、Azure CLI、または Azure PowerShell を使用できます。 好みのプログラミング言語を使用して、アプリケーションから必要なシークレットに安全にアクセスすることもできます。

ここでは、Azure portal を使用して Key Vault 内にシークレットを作成します。 その後、ポータルおよび Azure Cloud Shell の Azure CLI からシークレットにアクセスします。

Azure CLI は、コマンド ラインまたはスクリプトから Azure リソースを操作するための手段です。 Cloud Shell は、Azure リソースを開発および管理するための、ブラウザー ベースのシェル環境です。 Cloud Shell は、クラウド上で動作する対話型コンソールと考えてください。

Key Vault を作成します

1. Azure portal にアクセスします。
2. Azure portal のメニューまたは **ホーム** ページで、**[リソースの作成]** を選択します。
3. 検索バーに「**Key Vault**」と入力し、結果から **[Key Vault]** を選択します。
4. **[Key Vault]** ウィンドウで、**[作成]** を選択します。 **[キー コンテナーの作成]** ウィンドウが表示されます。
5. **[基本]** タブで、各設定に対して次の値を入力します。

注意

NNN は一連の数字に置き換えます。 こうすると、キー コンテナーの名前が確実に一意になります。

設定	値
プロジェクトの詳細	
サブスクリプション	**コンシェルジェ サブスクリプション**
リソース グループ	**[サンドボックス リソース グループ名]**
インスタンスの詳細	
キー コンテナー名	**my-keyvault-NNN**

その他の設定は、既定値のままにしておきます。

6. **[確認および作成]** を選択し、検証に成功したら **[作成]** を選択します。

   デプロイが正常に完了するまで待ちます。

7. **[リソースに移動]** を選択します。

8. キー コンテナーの詳細を確認します。

   たとえば、**[Vault URI](コンテナー URI)** フィールドには、アプリケーションで REST API からコンテナーにアクセスするために使用できる URI が表示されます。

   my-keyvault-321 という名前のキー コンテナーの例を次に示します。

9. 省略可能なステップとして、左側のメニュー ウィンドウの **[設定]** で、他の機能をいくつか調べることができます。

   これらは最初は空ですが、ここにはキー、シークレット、証明書を格納できる場所があります。

   注意

   このコンテナーへのアクセスが許可されているのは、ご自分の Azure サブスクリプションだけです。 **[設定]** の **[アクセス ポリシー]** 機能を使用して、コンテナーへのアクセス

を構成できます。

キー コンテナーにパスワードを追加する

1. 左側のメニュー ウィンドウの [**設定**] で、[**シークレット**] を選択します。 ご利用のキー コンテナーのウィンドウが表示されます。

2. 上部のメニュー バーで、[**生成/インポート**] を選択します。 [**シークレットの作成**] ウィンドウが表示されます。

3. 各設定に対して次の値を入力します。

設定	値
Upload options	[**手動**]
Name	**MyPassword**
値	**hVFkk96**

その他の設定は、既定値のままにしておきます。 アクティベーションの日付や有効期限などのプロパティを指定できることに注目してください。 シークレットへのアクセスを無効にすることもできます。

4. [**作成**] を選択します。

パスワードを表示する

ここでは、キー コンテナーからパスワードに 2 回アクセスします。 まず、Azure portal からアクセスします。 次に、Azure CLI からアクセスします。

1. [Key Vault] **または** [**シークレット**] ウィンドウから、[MyPassword] を選択します。 [MyPassword] **または** [**バージョン**] ウィンドウが表示されます。 現在のバージョンが有効になっていることがわかります。

2. 現在のバージョンを選択します。 [**シークレットのバージョン**] ウィンドウが表示されます。

   [**シークレット識別子**] の下に、アプリケーションでシークレットにアクセスするために使用できる URI が表示されます。 承認されたアプリケーションのみがこのシークレットにアクセスできることを思い出してください。

3. [**シークレット値の表示**] を選択します。

4. Cloud Shell から、次のコマンドを実行します。

注意

Azure CLI に慣れていない場合は、指示どおりに入力してください。

Azure CLI コピー

```
az keyvault secret show \
  --name MyPassword \
  --vault-name $(az keyvault list --query [0].name --output tsv) \
  --query value \
  --output tsv
```

出力にパスワードが表示されます。

出力 コピー

```
hVFkk96
```

良くできました この時点で、アプリケーションで使用するために安全に保存されたパスワード シークレットがキー コンテナーに含まれています。

クリーンアップ

このモジュールを完了したら、サンド ボックスは、リソースを自動的にクリーンアップします。

独自のサブスクリプションを使用している場合は、プロジェクトの最後に、作成したリソースがまだ必要かどうかを確認してください。 リソースを実行したままにすると、お金がかかる場合があります。 リソースを個別に削除するか、リソース グループを削除してリソースのセット全体を削除することができます。