Azure Key Vault を使用したシークレットの保存と管理

100 XP

3 分

Tailwind Traders は、クラウドでワークロードを作成するため、パスワード、暗号化キー、証明書などの機密情報を慎重に処理する必要があります。 アプリケーションが機能するためには、これらの情報を使用可能な状態にしておく必要がありますが、そのために承認されていないユーザーがアプリケーション データにアクセスできるようになる可能性があります。

Azure Key Vault は、アプリケーションのシークレットを中央の 1 か所に保存するための一元的なクラウド サービスです。 アクセス制御とログ記録の機能を提供することで、機密情報への安全なアクセスを提供します。

Azure Key Vault でできること

Azure Key Vault を使用して、次のことができます。

- **シークレットを管理する**

  トークン、パスワード、証明書、API キー、その他のシークレットを安全に保存し、それらへのアクセスを厳密に制御できます。

- **暗号化キーの管理**

  Key Vault をキー管理ソリューションとして使用できます。 Key Vault により、データの暗号化に使用される暗号化キーの作成と制御が簡単になります。

- **SSL/TLS 証明書の管理**

  Key Vault を使用すると、Azure リソースと内部リソースの両方でパブリックおよびプライベートの Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書をプロビジョニング、管理、デプロイすることができます。

- **ハードウェア セキュリティ モジュール (HSM) によってサポートされているシークレットの保存**

  これらのシークレットとキーは、ソフトウェアまたは FIPS 140-2 レベル 2 検証済み HSM で保護できます。

以下は、Key Vault でのテストに使用される証明書を示す例です。

このモジュールの後半で、Key Vault にシークレットを追加します。

Azure Key Vault を使用する利点とは

Key Vault を使用すると、次のような利点があります。

- **アプリケーション シークレットが一元管理される**

  アプリケーション シークレットの保存を一元管理することで、その配布を制御できます。また、シークレットが誤って漏洩する恐れが少なくなります。

- **シークレットとキーが安全に保存される**

  Azure では、業界標準のアルゴリズム、キーの長さ、HSM が使用されています。 Key Vault にアクセスするには、適切な認証と承認が必要です。

- **アクセス監視とアクセス制御**

  Key Vault を使用すると、アプリケーション シークレットへのアクセスを監視および制御できます。

- **簡単なアプリケーション シークレットの管理**

  Key Vault を使用すると、公開証明機関 (CA) からの証明書の登録と更新が簡単になります。リージョン内のコンテンツをスケールアップして複製し、標準の証明書管理ツールを使用することもできます。

- **その他の Azure サービスとの統合**

  Key Vault は、ストレージ アカウント、コンテナー レジストリ、イベント ハブなど、多くの Azure サービスと統合できます。 これらのサービスは、Key Vault に保存されているシークレットを安全に参照できます。