Azure Active Directory とは

100 XP

5 分

ここでは、Azure Active Directory (Azure AD) で ID サービスを提供し、Microsoft クラウド アプリケーションとユーザーが開発したクラウド アプリケーションの両方にユーザーがサインインしてアクセスできるようにする方法について説明します。 また、Azure AD でシングル サインオン (SSO) がサポートされる仕組みについても説明します。

Tailwind Traders は既に Active Directory を使用して、オンプレミス環境をセキュリティで保護しています。 この会社は、ユーザーがクラウド内のアプリケーションとデータへのアクセス時に異なるユーザー名とパスワードを記憶して使用しなければならない状況は望んでいません。 会社は既存の Active Directory インスタンスをクラウドの ID サービスと統合して、ユーザーのシームレスなエクスペリエンスを実現できるでしょうか?

まず、Azure AD と Active Directory を比較してみましょう。

Azure AD と Active Directory の違いは何でしょうか?

Active Directory は Azure AD に関連していますが、いくつかの重要な違いがあります。

Microsoft は Windows 2000 で Active Directory を導入し、ユーザーごとに 1 つの ID を使用して、複数のオンプレミスのインフラストラクチャ コンポーネントとシステムを管理する機能を組織に提供しました。

オンプレミス環境の場合、Windows Server で実行される Active Directory は、自分の組織によって管理される ID およびアクセスの管理サービスを提供します。 Azure AD は、Microsoft のクラウドベースの ID およびアクセスの管理サービスです。 Azure AD では、ユーザーが ID アカウントを制御しますが、サービスがグローバルに利用可能であることを Microsoft が保証します。 Active Directory を使用したことがある場合は、Azure AD にすぐに慣れることができるでしょう。

オンプレミスで Active Directory を使用して ID をセキュリティ保護する場合、Microsoft はサインインの試行を監視しません。 Active Directory を Azure AD と接続すると、Microsoft が追加費用なしで疑わしいサインインの試行を検出することによってお客様の環境が保護されます。 たとえば、Azure AD は、予期しない場所または不明なデバイスからのサインインの試行を検出できます。

Azure AD の利用者

Azure AD は次のユーザーを対象としています。

- **IT 管理者**

  管理者は Azure AD を使用すると、ビジネス要件に基づいてアプリケーションとリソースへのアクセスを制御することができます。

- **アプリ開発者**

  開発者は Azure AD を使用すると、作成するアプリケーションに機能を追加するときに標準ベースのアプローチを利用できます (アプリに SSO 機能を追加したり、アプリがユーザーの既存の資格情報を使用できるようにしたりするなど)。

- **ユーザー**

  ユーザーは自分の ID を管理できます。 たとえば、セルフサービスによるパスワードのリセットでは、IT 管理者やヘルプ デスクに連絡しなくても、ユーザーが自分のパスワードを変更またはリセットすることができます。

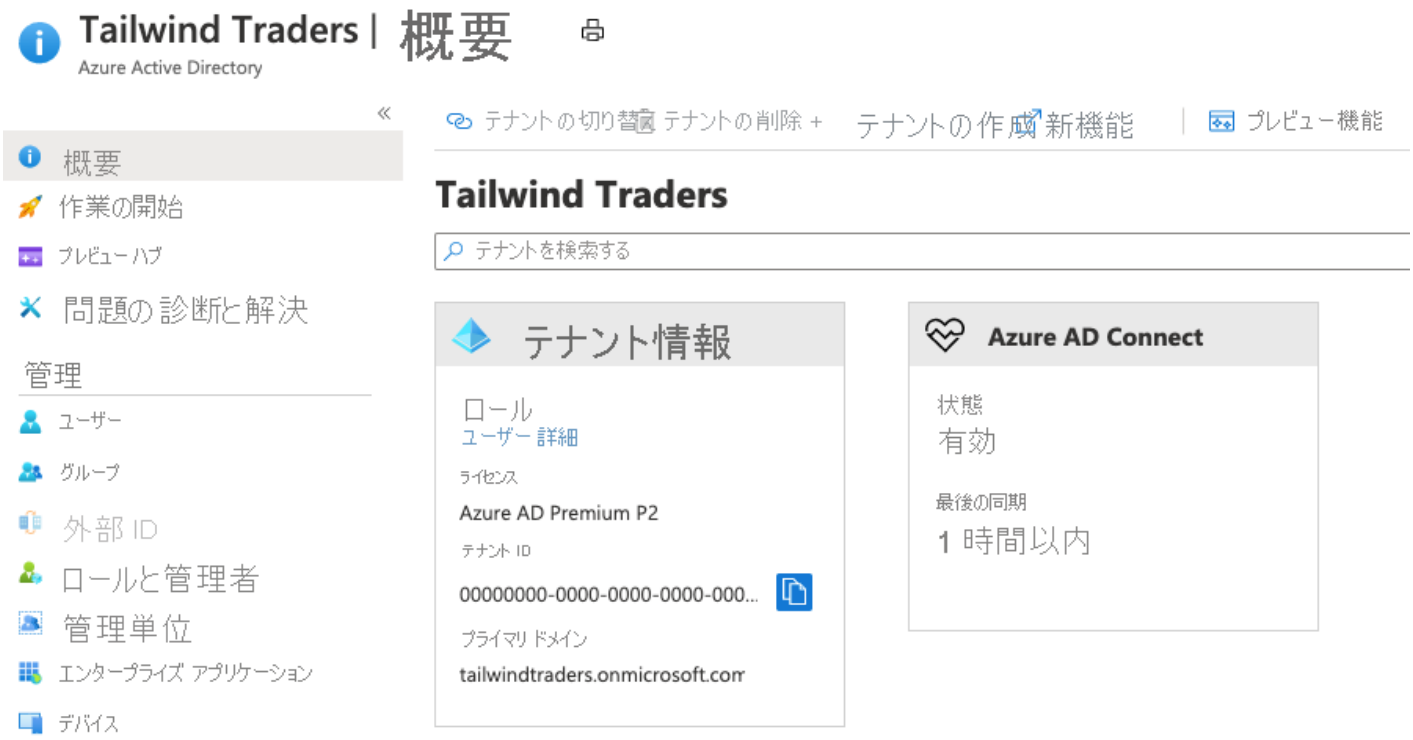
- **オンライン サービスのサブスクライバー**

  Microsoft 365、Microsoft Office 365、Azure、および Microsoft Dynamics CRM Online のサブスクライバーは、既に Azure AD を使用しています。

  テナント は組織を表します。 テナントは通常、他のテナントから分離され、独自の ID を持ちます。

  Microsoft 365、Office 365、Azure、および Dynamics CRM Online の各テナントは、自動的に Azure AD テナントになります。

次に、IT 管理者が Active Directory を操作するときに Azure portal で確認できる情報のスクリーンショットを示します。



Azure AD はどのようなサービスを提供していますか?

Azure AD は、次のようなサービスを提供しています。

- **認証**

  これには、アプリケーションとリソースにアクセスするための ID の確認が含まれます。 また、セルフサービスによるパスワードのリセット、多要素認証、禁止されているパスワードのカスタム リスト、スマート ロックアウト サービスなどの機能も提供されます。

- **シングル サインオン**

  SSO を使用すると、ユーザーは 1 つのユーザー名と 1 つのパスワードを記憶するだけで複数のアプリケーションにアクセスできるようになります。 単一の ID がユーザーに関連付けられているため、セキュリティ モデルが単純化されます。 ユーザーがロールを変更したか、退職したときに、アクセス変更がその ID に関連付けられ、アカウントを変更したり、無効にしたりするために必要な労力が大幅に減少します。

- **アプリケーション管理**

  Azure AD を使用すると、クラウドとオンプレミスのアプリを管理できます。 アプリケーション プロキシ、SaaS アプリ、マイ アプリ ポータル ("アクセス パネル" とも呼ばれる)、シングル サインオンなどの機能を使用すると、ユーザー エクスペリエンスを向上させることができます。

- **デバイス管理**

  個々のユーザーのアカウントと共に、Azure AD はデバイスの登録をサポートしています。 登録により、Microsoft Intune などのツールを使用してデバイスを管理できるようになります。 また、デバイスベースの条件付きアクセス ポリシーで、要求元のユーザー アカウントに関係なく、既知のデバイスからのアクセスのみに制限することもできます。

どのような種類のリソースを Azure AD でセキュリティ保護することができますか?

Azure AD を使用すると、ユーザーは外部リソースと内部リソースの両方にアクセスできます。

外部リソースには、Microsoft Office 365、Azure portal、およびその他の数千のサービスとしてのソフトウェア (SaaS) アプリケーションが含まれる可能性があります。

社内リソースには、組織内で開発されたクラウド アプリケーションに加えて、企業のネットワークとイントラネット上のアプリが含まれる可能性があります。

シングル サインオンとは

シングル サインオンを使用すると、ユーザーは 1 回サインインするだけで、その資格情報を使用して、さまざまなプロバイダーからの複数のリソースやアプリケーションにアクセスできます。

ID が多くなると、覚えておく必要があり、また変更する必要があるパスワードが増えることになります。 パスワード ポリシーはアプリケーションによって異なる場合があります。 複雑さの要件が増えるほど、ユーザーにとってパスワードを覚えておくことが一層困難になります。 ユーザーが管理する必要があるパスワードが多くなればなるほど、資格情報に関するセキュリティ インシデントのリスクが高まります。

これらすべての ID を管理するプロセスについて考えてみてください。 ヘルプ デスクにはさらに負担がかかります。アカウントのロックアウトやパスワードのリセット要求に対応する必要があるためです。 ユーザーが退職した場合、その ID をすべて追跡し、無効になっていることを確認することが困難である可能性があります。 ID を見落とした場合、除外しておくべきアクセスが許可される恐れがあります。

SSO の場合、ユーザーは 1 つの ID と 1 つのパスワードを覚えておくだけで済みます。 アプリケーション間でのアクセスはユーザーに関連付けられている単一の ID に許可され、セキュリティ モデルが簡素化されます。 ユーザーがロールを変更したり組織から脱退したりするとき、アクセスは 1 つの ID に関連付けられています。 この変更により、アカウントの変更や無効化に必要な労力が大幅に軽減されます。 アカウントに SSO を使用すると、ユーザーが自分の ID を簡単に管理できるようになり、セキュリティ機能が向上します。

Azure AD で SSO を有効にする方法については、このモジュールの最後にあるリソースを参照してください。

Active Directory を Azure AD と接続するにはどうすればよいですか?

Active Directory を Azure AD に接続すると、一貫性のある ID エクスペリエンスをユーザーに提供できます。

既存の Active Directory インストールを Azure AD に接続するには、いくつかの方法があります。おそらく、最も一般的な方法は Azure AD Connect を使用することです。

Azure AD Connect では、オンプレミスの Active Directory と Azure AD の間でユーザー ID が同期されます。 Azure AD Connect では両方の ID システム間で変更が同期されます。これにより、両方のシステムで SSO、多要素認証、セルフサービスによるパスワードのリセットなどの機能を使用できるようになります。 セルフサービスによるパスワードのリセットでは、ユーザーが既知の侵害されたパスワードを使用することが防止されます。

次の図は、オンプレミスの Active Directory と Azure AD の間で Azure AD Connect がどのように適合しているかを示しています。

Tailwind Traders では既存の Active Directory インスタンスが Azure AD と統合されるため、組織全体で一貫性のあるアクセス モデルが作成されます。 これにより、さまざまなアプリケーションへのサインイン、ユーザー ID の変更と制御の管理、および異常なアクセス試行の監視とブロックの機能が大幅に簡素化されます。