Azure のロールベースのアクセス制御を使用してクラウド リソースへのアクセスを制御する

100 XP

4 分

複数の IT チームとエンジニアリング チームがある場合、クラウド環境内のリソースに対するアクセスをどのようにして制御できますか。 ユーザーには、自分の仕事を遂行するために必要な権限だけを、関連するリソースに対してだけ許可するのが、適切なセキュリティ プラクティスです。

各ユーザーの詳細なアクセス要件を定義し、新しいリソースが作成されたらアクセス要件を更新する代わりに、Azure では、Azure のロールベースのアクセス制御 (Azure RBAC) を使用してアクセスを制御できます。

Azure には、クラウド リソースに対する一般的なアクセス規則が記述された組み込みのロールが用意されています。 独自のロールを定義することもできます。 各ロールには、そのロールに関連する一連のアクセス許可が関連付けられています。 1 つ以上のロールに個人またはグループを割り当てると、関連付けられているすべてのアクセス許可が付与されます。

ロールベースのアクセス制御がリソースに適用される方法

ロールベースのアクセス制御は、このアクセスが適用されるリソースまたはリソースのセットである "スコープ" に対して適用されます。

次の図では、ロールとスコープの間の関係が示されています。

スコープには以下のものが含まれます。

- 管理グループ (複数のサブスクリプションのコレクション)。
- 1 つのサブスクリプション。
- リソース グループ。
- 1 つのリソース。

"オブザーバー"、"リソースを管理するユーザー"、"管理者"、"自動化されたプロセス" は、さまざまな各ロールに一般に割り当てられるユーザーまたはアカウントの種類を示しています。

親スコープでアクセス権を付与すると、それらのアクセス許可がすべての子スコープに継承されます。 次に例を示します。

- 管理グループのスコープでユーザーに所有者ロールを割り当てると、そのユーザーは、その管理グループ内にあるすべてのサブスクリプションのすべてのものを管理できます。
- 閲覧者ロールをサブスクリプションのスコープでグループに割り当てると、そのグループのメンバーは、そのサブスクリプション内にあるすべてのリソース グループとリソースを表示できます。
- リソース グループのスコープでアプリケーションに共同作成者ロールを割り当てると、そのアプリケーションは、そのリソース グループ内にあるすべての種類のリソースを管理できますが、サブスクリプション内の他のリソース グループは管理できません。

どのようなときに Azure RBAC を使用するか

次のことが必要なときは、Azure RBAC を使用します。

- あるユーザーにサブスクリプション内の VM の管理を許可し、別のユーザーに仮想ネットワークの管理を許可します。
- データベース管理者グループにサブスクリプション内の SQL データベースの管理を許可します。
- あるユーザーに、仮想マシン、Web サイト、サブネットなど、リソース グループ内のすべてのリソースの管理を許可します。
- あるアプリケーションに、リソース グループ内のすべてのリソースへのアクセスを許可します。

いくつかの例を示します。 すべての組み込みロールの一覧については、このモジュールの最後を参照してください。

Azure RBAC が適用される方法

Azure RBAC は、Azure Resource Manager を経由する Azure リソースに対して開始されるすべてのアクションに適用されます。 Resource Manager は、クラウド リソースを整理してセキュリティ保護する手段を提供する管理サービスです。

通常、Resource Manager にアクセスするには、Azure portal、Azure Cloud Shell、Azure PowerShell、Azure CLI を使用します。 Azure RBAC では、アプリケーション レベルまたはデータ レベルではアクセス許可は適用されません。 アプリケーションのセキュリティは、アプリケーションで処理する必要があります。

RBAC では、"許可モデル" が使用されます。 ロールを割り当てられると、RBAC によって読み取り、書き込み、削除などの特定のアクションの実行を "許可" されます。 1 つのロールの割り当て

によってあるリソース グループへの読み取りアクセス許可が付与されていて、別のロールの割り当てによって同じリソース グループへの書き込みアクセス許可が付与されている場合、ユーザーはそのリソース グループで読み取りと書き込みの両方のアクセス許可を持つことになります。

Azure RBAC が適用される対象

Azure RBAC は、個々のユーザーまたはグループに適用できます。 また、サービス プリンシパルやマネージド ID など、他の特別な ID の種類に Azure RBAC を適用することもできます。 これらの ID の種類は、Azure リソースへのアクセスを自動化するために、アプリケーションとサービスによって使用されます。

Tailwind Traders では、以下のチームが IT 環境全体の一部に関心を持っています。

- IT 管理者

  このチームは、オンプレミスとクラウドの両方におけるテクノロジ資産の最終的な所有権を持ちます。 チームは、すべてのリソースを完全に制御する必要があります。

- バックアップと障害復旧

  このチームは、定期的なバックアップの正常性を管理し、データまたはシステムの復旧を開始する役割を担います。

- コストと課金

  このチームの担当者は、テクノロジ関連の支出を追跡して報告します。 また、組織の内部予算も管理します。

- セキュリティ運用担当者

  このチームは、テクノロジ関連のセキュリティ インシデントをすべて監視して対応します。 チームは、ログ ファイルとセキュリティ アラートに継続的にアクセスする必要があります。

Azure RBAC のアクセス許可の管理方法

アクセス許可の管理は、Azure portal の **[アクセス制御 (IAM)]** ペインで行います。 このペインには、どのユーザーがどのスコープにアクセスでき、どのロールが適用されるかが表示されます。 また、アクセス許可の付与や削除も、このペインから行うことができます。

次のスクリーンショットでは、リソース グループに対する **[アクセス制御 (IAM)]** ペインの例を示します。 この例では、このリソース グループに対する **バックアップ オペレーター** ロールが Alain Charon に割り当てられています。


ホーム > リソース グループ > sales-projectforecast > アクセス制御 - ロールの割り当て
アクセス制御 - ロールの割り当て
sales-projectforecast
検索 (Ctrl+/)
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
追加
削除
ロール
更新
Helo
名前
名前または電子メールで検索する
種類
すべて
ロール
5 件選択済み
スコープ
すべてのスコープ
グループ化
ロール
8 個のアイテム (5 ユーザー、1 グループ、2 サービス プリンシパル)
名前
型
ロール
スコープ
バックアップ オペレーター
AC
Alain Charon
alain
ユーザー
バックアップ オペレーター
このリソース