リソース ロックを使用して偶発的な変更を防ぐ

100 XP

3 分

リソース ロックを使用して、リソースが誤って削除または変更されるのを防ぐことができます。

Azure のロールベースのアクセス制御 (Azure RBAC) ポリシーが適用されていても、適切なレベルのアクセス権を持つユーザーが重要なクラウド リソースを削除するリスクがあります。 リソース ロックは、リソースを削除または変更してはならないことを通知する警告システムと考えることができます。

たとえば、Tailwind Traders では、IT 管理者が Azure で使用されていないリソースの定期的なクリーンアップを実行していました。 管理者は、使用されていないように見えるリソースを誤って削除しました。 しかし、これらのリソースは、季節のプロモーションに使用されるアプリケーションにとって重要なものでした。 リソース ロックを使用すると、今後この種のインシデントが発生するのをどのようにふせぐことができるのでしょうか。

リソース ロックを管理する方法

リソースロックは、Azure portal、PowerShell、Azure CLI、または Azure Resource Manager テンプレートから管理できます。

Azure portal でロックを表示、追加、または削除するには、Azure portal で任意のリソースの **[設定]** ペインの **[設定]** セクションに移動します。

次の例では、Azure portal からリソース ロックを追加する方法を示します。 次のパートでは、同様のリソース ロックを適用します。

使用できるロックのレベル

ロックは、サブスクリプション、リソース グループ、または個々のリソースに対して適用できます。 ロック レベルは **CanNotDelete** または **ReadOnly** に設定できます。

- **CanNotDelete** は、承認されたユーザーはリソースの読み取りと変更を行うことができますが、先にロックを削除しないとリソースを削除できないことを意味します。
- **ReadOnly** は、承認されたユーザーはリソースを読み取ることはできますが、リソースの削除または変更はできないことを意味します。 このロックの適用は、すべての承認されたユーザーを、Azure RBAC の **閲覧者** ロールによって付与されるアクセス許可に制限するのと似ています。

ロックされたリソースを削除または変更する方法

ロックは誤った変更を防ぐのに役立ちますが、それでも 2 ステップのプロセスに従って変更を行うことができます。

ロックされたリソースを変更するには、最初にロックを解除する必要があります。 ロックを解除した後は、実行するためのアクセス許可を持っているすべてのアクションを適用できます。 この追加のステップによりアクションを実行できますが、管理者が意図していない操作を実行するのを防ぐのに役立ちます。

リソース ロックは RBAC アクセス許可に関係なく適用されます。 自分がリソースの所有者であっても、ブロックされているアクティビティを実行するには先にロックを解除する必要があります。

リソース ロックと Azure Blueprints を組み合わせる

クラウド管理者がリソース ロックを誤って解除した場合はどうなるでしょう。 リソース ロックが解除されると、それに関連付けられているリソースを変更または削除できるようになります。

保護プロセスの堅牢性を高めるには、リソース ロックと Azure Blueprints を組み合わせることができます。 Azure Blueprints を使用すると、組織で必要とされる標準的な Azure リソースのセットを定義できます。 たとえば、特定のリソース ロックが存在していなければならないことを指定するブループリントを定義できます。 Azure Blueprints を使用すると、リソース ロックが解除された場合に、そのロックを自動的に置き換えることができます。

Azure Blueprints については、このモジュールで後ほどさらに学習します。