Azure Policy を使用してリソースを制御および監査する

100 XP

5 分

ガバナンスとビジネスの要件を特定したら、リソースの準拠をどのようにして "維持する" ことができるでしょうか。 リソースの構成が変更された場合にアラートを受け取るにはどうすればよいでしょうか。

Azure のサービスである Azure Policy を使用すると、リソースを制御または監査するポリシーの作成、割り当て、管理を行うことができます。 これらのポリシーにより、リソースの構成にさまざまなルールと効果が適用されて、それらの構成は会社の標準に準拠した状態に保たれます。

Azure Policy でポリシーを定義する方法

Azure Policy を使用すると、個別のポリシーと、関連するポリシーのグループ ("イニシアティブ" と呼ばれます) の両方を定義できます。 Azure Policy によってリソースが評価され、作成したポリシーに準拠していないリソースが明示されます。 Azure Policy を使用すると、準拠していないリソースが作成されないようにすることもできます。

Azure Policy には、ストレージ、ネットワーク、コンピューティング、Security Center、監視などのカテゴリで使用できる組み込みのポリシーとイニシアティブの定義が多数用意されています。

たとえば、特定の Stock Keeping Unit (SKU) サイズの仮想マシン (VM) のみを環境で使用できるようにするポリシーを定義するとします。 このポリシーを有効にすると、新しい VM を作成するとき、または既存の VM のサイズを変更するときに、そのポリシーが適用されます。 Azure Policy では、環境内の現在の VM も評価されます。

場合によっては、準拠していないリソースや構成を Azure Policy で自動的に修復して、リソースの状態の整合性を保証することができます。 たとえば、特定のリソース グループ内のすべてのリソースにタグ **AppName** と値 "SpecialOrders" を付ける必要がある場合、それが削除されたら、Azure Policy で自動的にそのタグを再適用することができます。

また、アプリケーションのデプロイ前とデプロイ後のフェーズに適用される継続的インテグレーションおよび配信パイプラインのポリシーを適用することで、Azure Policy と Azure DevOps が統合されます。

Azure Policy の動作

Azure Policy でのポリシーの実装は、次の 3 つのステップで行います。

1. ポリシー定義を作成します。
2. 定義をリソースに割り当てます。
3. 評価の結果を確認します。

各ステップを詳しく調べてみましょう。

1.ポリシー定義を作成する

ポリシー定義では、評価対象と対処方法を表します。 たとえば、特定の Azure リージョンには VM がデプロイされないようにすることができます。 また、ストレージ アカウントを監査して、許可されたネットワークからの接続のみが受け入れられることを確認することもできます。

すべてのポリシー定義に、ポリシーが適用される条件があります。 また、ポリシー定義には、条件が満たされた場合に実行される付随する効果も含まれます。 次に、ポリシー定義の例をいくつか示します。

- **許可されている仮想マシン SKU**

  このポリシーでは、組織がデプロイできる一連の VM SKU を指定できます。

- **許可される場所**

  このポリシーでは、リソースをデプロイするときに組織が指定できる場所を制限できます。その効果は、地理的なコンプライアンス要件を適用するために使用されます。

- **サブスクリプションに対する書き込みアクセス許可を持つアカウントに対して MFA を有効にする必要がある**

  このポリシーでは、アカウントまたはリソースの侵害を防ぐため、書き込み権限を持つすべてのサブスクリプション アカウントで多要素認証 (MFA) を有効にする必要があります。

- **CORS で Web アプリケーションへのアクセスをすべてのリソースには許可しない**

  クロス オリジン リソース共有 (CORS) は、1 つのドメインの下で実行される Web アプリケーションが別のドメインのリソースにアクセスできるようにする HTTP 機能です。 セキュリティ上の理由から、最新の Web ブラウザーではクロスサイト スクリプティングが既定で制限されています。 このポリシーを使用すると、必要なドメインだけが Web アプリとの対話を許可されます。

- **システム更新プログラムをマシンにインストールする必要がある**

  このポリシーを使用すると、サーバーで不足しているセキュリティ システムの更新プログラムが Azure Security Center によって推奨されます。

2.定義をリソースに割り当てる

ポリシー定義を実装するには、リソースに定義を割り当てます。 "ポリシーの割り当て" は、特定のスコープ内で実行されるポリシー定義です。 このスコープには、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)、単一のサブスクリプション、またはリソース グループを指定できます。

ポリシーの割り当ては、そのスコープ内のすべての子リソースによって継承されます。 ポリシーがリソース グループに適用された場合、そのリソース グループ内のすべてのリソースにそのポリシーが適用されます。 ポリシーの割り当てから除外する必要がある特定の子リソースがある場合は、ポリシーの割り当てからサブスコープを除外できます。

3. 評価の結果を確認する

既存のリソースに対して条件が評価されると、各リソースは準拠または非準拠としてマークされます。 非準拠ポリシーの結果を確認し、必要なアクションを実行できます。

ポリシーの評価は、だいたい 1 時間に 1 回行われます。 ポリシー定義を変更し、ポリシーの割り当てを作成した場合、そのポリシーは 1 時間以内にリソースに対して評価されます。

Azure Policy のイニシアティブとは

Azure Policy のイニシアティブは、関連するポリシーを 1 つのセットにグループ化する手段です。 イニシアティブ定義には、大きな目標に対するコンプライアンスの状態を追跡するのに役立つすべてのポリシー定義が含まれます。

たとえば、Azure Policy には **Azure Security Center での監視を有効にする** という名前のイニシアティブが含まれています。 その目的は、すべての Azure リソースの種類に対して利用可能なすべてのセキュリティ推奨事項を Azure Security Center で監視することです。

このイニシアティブには、次のようなポリシー定義が含まれます。

- **暗号化されていない SQL データベースを Security Center で監視する**

  このポリシーでは、暗号化されていない SQL データベースとサーバーが監視されます。

- **OS の脆弱性を Security Center で監視する**

  このポリシーでは、構成されている OS 脆弱性ベースラインを満たしていないサーバーが監視されます。

- **Endpoint Protection の不足を Security Center で監視する**

  このポリシーでは、エンドポイント保護エージェントがインストールされていないサーバーが監視されます。

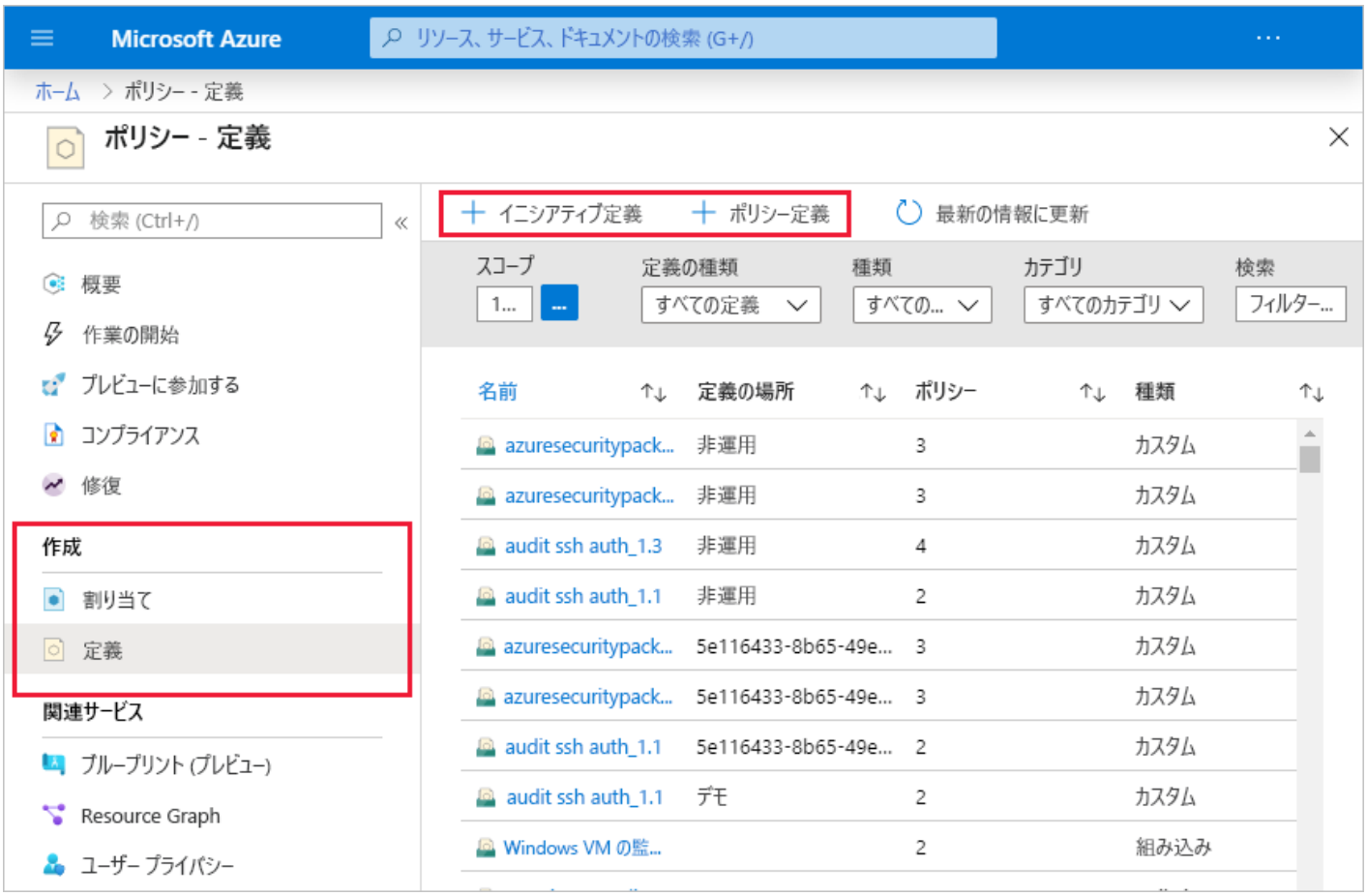
実際、**Azure Security Center での監視を有効にする** イニシアティブには、100 を超える個別のポリシー定義が含まれます。

Azure Policy には、HIPAA や ISO 27001 などの規制コンプライアンス標準をサポートするイニシアティブも含まれています。

イニシアティブを定義する方法

イニシアティブを定義するには、Azure portal またはコマンドライン ツールを使用します。 Azure portal では、Azure によって既に提供されている組み込みイニシアティブの一覧を検索できます。 独自のカスタム ポリシー定義を作成することもできます。

次の図は、Azure portal での Azure Policy イニシアティブの例を示したものです。



イニシアティブを割り当てる方法

ポリシーの割り当てと同様に、イニシアティブの割り当ては、管理グループ、サブスクリプション、またはリソース グループの特定のスコープに割り当てられたイニシアティブ定義です。

ポリシーが 1 つしかない場合でも、イニシアティブを使用すると時間の経過と共にポリシーの数を増やすことができます。 関連付けられたイニシアティブは割り当てられたままなので、リソースのポリシー割り当てを変更する必要なしに、ポリシーを簡単に追加したり削除したりできます。