Azure Blueprints を使用して複数のサブスクリプションのガバナンスを行う

100 XP

4 分

ここまでは、ガバナンスの決定を実装し、クラウド リソースのコンプライアンスを監視し、アクセスを制御して、重要なリソースが誤って削除されないようにするのに役立つ、Azure のいくつかの機能を調べてきました。

クラウド環境が 1 つのサブスクリプションに収まらないほど大きくなり始めたらどうなるでしょう。 これらの機能の構成を拡張して、新しいサブスクリプションのリソースに適用する必要があることを把握するには、どうすればよいでしょう。

新しいサブスクリプションごとに Azure Policy のような機能を構成する必要はなく、Azure Blueprints を使用することで、組織で必要なガバナンス ツールと標準の Azure リソースの反復可能なセットを定義できます。 このようにして、開発チームは新しい環境を迅速に構築してデプロイすることができます。新しい環境は組織のコンプライアンスに従って構築され、ネットワークなどの一連の組み込みコンポーネントが含まれていることがわかっているので、開発フェーズとデプロイ フェーズにかかる時間を短縮できます。

Azure Blueprints により、リソース テンプレートと次のようなさまざまな他の成果物のデプロイが調整されます。

- ロールの割り当て
- ポリシーの割り当て
- Azure Resource Manager テンプレート
- リソース グループ

Azure Blueprints の動作

編成されたクラウド技術拠点チームまたはクラウド カストディアン チームは、Azure Blueprints を使用して、ガバナンス プラクティスを組織全体に拡張することができます。

Azure Blueprints でのブループリントの実装には、次の 3 つのステップが含まれます。

1. Azure ブループリントを作成します。
2. ブループリントを割り当てます。
3. ブループリントの割り当てを追跡します。

Azure Blueprints では、ブループリント定義 (何をデプロイする "必要がある" か) とブループリント割り当て (何がデプロイ "された" か) の間の関係が維持されます。 言い換えると、Azure によって、リソースとそれが定義されているブループリントを関連付けるレコードが作成されます。 この結び付きを使用すると、デプロイを追跡して監査することができます。

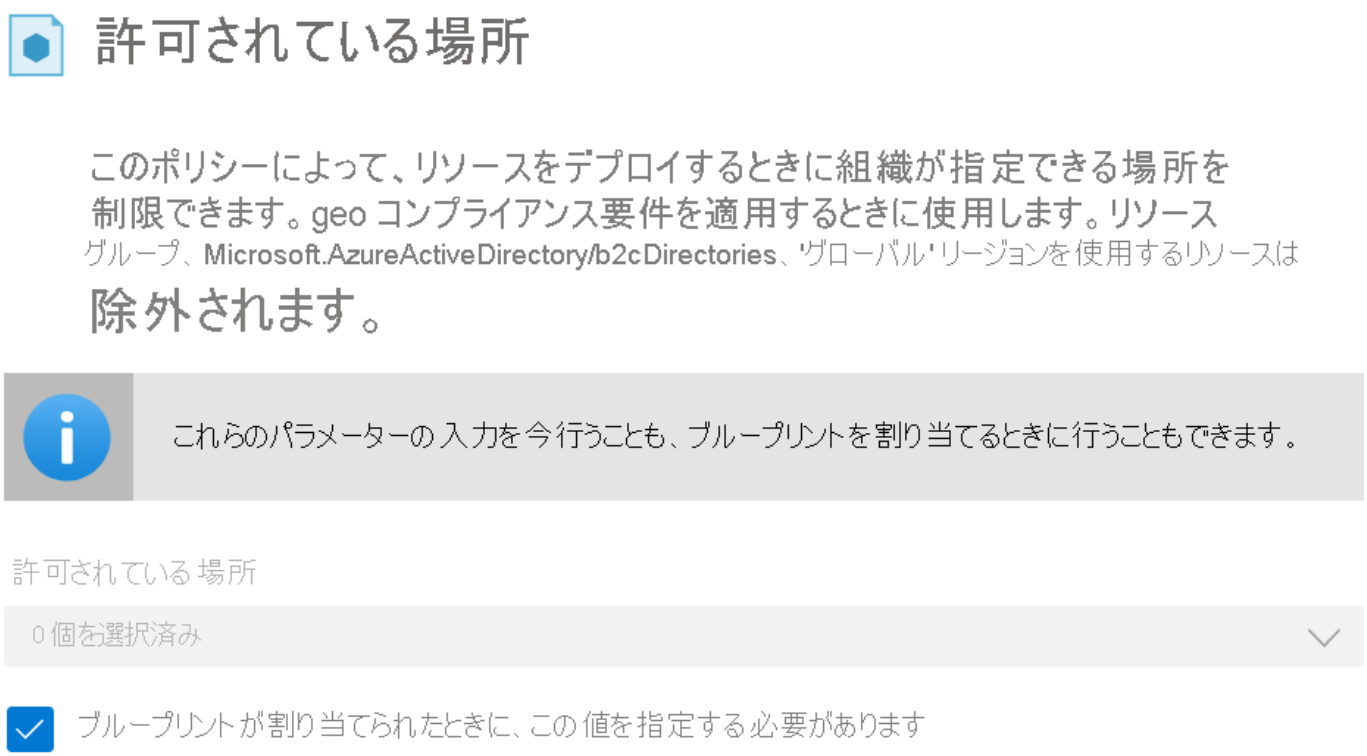
ブループリントもバージョン管理されています。 バージョン管理を使用すると、ブループリントへの変更を追跡してコメントすることができます。

ブループリント アーティファクトとは

ブループリントの定義の各コンポーネントは、"アーティファクト" と呼ばれます。

アーティファクトには、パラメーターがない場合があります。 たとえば、**SQL Server での脅威検出のデプロイ** ポリシーについては、それ以上の構成は必要ありません。

また、構成可能なパラメーターが 1 つ以上アーティファクトに含まれることもあります。 次のスクリーンショットでは、**許可されている場所** ポリシーを示します。 このポリシーには、許可される場所を指定するパラメーターが含まれます。



ブループリントの定義を作成するとき、またはブループリントの定義をスコープに割り当てるときに、パラメーターの値を指定できます。 これにより、標準のブループリントを 1 つ維持しながら、定義が割り当てられるスコープごとに関連する構成パラメーターを柔軟に指定できます。

Tailwind Traders による ISO 27001 へのコンプライアンスのための Azure Blueprints の使用方法

ISO 27001 は、国際標準化機構によって公開されている、IT システムのセキュリティに適用される標準です。 Tailwind Traders は、品質プロセスの一環として、この標準に準拠していることを認定しようと考えています。 Azure Blueprints には、ISO 27001 に関連する組み込みのブループリント定義がいくつかあります。

IT 管理者であるあなたは、**ISO 27001: 共有サービス ブループリント** の定義を調べることにします。 計画の概要を次に示します。

1. **PROD-MG** という名前の管理グループを定義します。

   管理グループを使用すると、複数の Azure サブスクリプションにまたがってアクセス、ポリシー、コンプライアンスを管理できることを思い出してください。 サブスクリプションが作成されるときに、すべての新しい Azure サブスクリプションがこの管理グループに追加されます。

2. ブループリント定義を **ISO 27001: 共有サービス ブループリント** テンプレートを基にして作成します。 その後、ブループリントを発行します。

3. ブループリントを **PROD-MG** 管理グループに割り当てます。

次の図では、テンプレートから ISO 27001 ブループリントを実行すると作成されるアーティファクトを示します。

ブループリントの作成

Data Lake Store アカウントにおける暗号化の強制	ポリシーの割り当て	なし
ストレージ アカウントの BLOB 暗号化を必須とする	ポリシーの割り当て	なし
成果物の追加...		
Log Analytics リソース グループ	リソース グループ	2 個中 2 個のパラメーターが入力されました
Log Analytics テンプレート	Azure Resource Manager テ...	4 個中 0 個のパラメーターが入力されました
成果物の追加...		
ネットワーク リソース グループ	リソース グループ	2 個中 2 個のパラメーターが入力されました
Azure Firewall テンプレート	Azure Resource Manager テ...	3 個中 0 個のパラメーターが入力されました
仮想ネットワークとルート テーブルのテンプレート	Azure Resource Manager テ...	9 個中 0 個のパラメーターが入力されました

ブループリントのテンプレートには、ポリシー割り当て、Resource Manager テンプレート、リソース グループが含まれていることがわかります。 このブループリントでは、**PROD-MG**管理グループ内の既存のサブスクリプションに、これらのアーティファクトがデプロイされます。 また、このブループリントでは、新しいサブスクリプションが作成されて管理グループに追加されるときにも、これらのアーティファクトがそれにデプロイされます。