

Azure Virtual Network の設定

100 XP

7 分

Azure portal、ローカル コンピューター上の Azure PowerShell、または Azure Cloud Shell から Azure Virtual Network インスタンスを作成して構成できます。

仮想ネットワークの作成

Azure 仮想ネットワークを作成するときに、基本的な設定をいくつか構成します。複数のサブネット、分散型サービス拒否 (DDoS) の保護、サービス エンドポイントなど、高度な設定を構成することができます。

[ホーム](#) > [仮想ネットワーク](#) >

仮想ネットワークの作成

基本 IP アドレス セキュリティ タグ 確認と 作成

Azure Virtual Network (VNet) は、Azure 内のプライベート ネットワークの基本的な構成要素です。VNet により、Azure Virtual Machines (VM) などのさまざまな種類の Azure リソースが、他の Azure リソース、インターネット、およびオンプレミスのネットワークと安全に通信することができます。VNet は、自社のデータ センターで運用する従来のネットワークと似ていますが、スケール、可用性、分離性など、

Azure のインフラストラクチャのさらなる利点を提供します。仮想ネットワークの詳細

プロジェクトの詳細

サブスクリプション ⓘ

Learn AIRS - Microsoft Azure 社内従量課金プラン



リソース グループ ⓘ

読み込み中...

[新規作成](#)

インスタンスの詳細

名前 *

リージョン

読み込み中...

基本的な仮想ネットワークに対して次の設定を構成します。

- **ネットワーク名**

ネットワーク名は、サブスクリプション内で一意である必要がありますが、グローバルに一意である必要はありません。覚えやすく、他の仮想ネットワークと区別しやすい、説明的な名前を付けます。

- **アドレス空間**

仮想ネットワークを設定するときに、クラスレス ドメイン間ルーティング (CIDR) 形式で内部のアドレス空間を定義します。このアドレス空間は、サブスクリプション内と接続する他のネットワーク内で固有である必要があります。

最初の仮想ネットワークに 10.0.0.0/24 のアドレス空間を選択したとします。このアドレス空間に定義されるアドレスは、10.0.0.1 から 10.0.0.254 の範囲になります。次に、2 つ目の仮想ネットワークを作成して、10.0.0.0/8 のアドレス空間を選択します。このアドレス空間に定義されるアドレスは、10.0.0.1 から 10.255.255.254 の範囲になります。一部のアドレスが重複しており、それらを 2 つの仮想ネットワークで使用することはできません。

ただし、10.0.0.1 から 10.0.255.254 までの範囲のアドレスを持つ 10.0.0.0/16 と、10.1.0.1 から 10.1.255.254 までの範囲のアドレスを持つ 10.1.0.0/16 は使用できます。アドレスの重複がないため、これらのアドレス空間を仮想ネットワークに割り当てることができます。

注意

仮想ネットワークを作成した後で、アドレス空間を追加できます。

• サブスクリプション

このオプションは、選択するサブスクリプションが複数ある場合にのみ適用されます。

• リソース グループ

他の Azure リソースと同様、仮想ネットワークはリソース グループ内に配置する必要があります。既存のリソース グループを選択するか、新しいリソース グループを作成できます。

• 場所

仮想ネットワークを配置する場所を選択します。

• サブネット

各仮想ネットワークのアドレス範囲内で、仮想ネットワークのアドレス空間をパーティション分割するサブネットを、1 つまたは複数作成できます。サブネット間のルーティングは、既定のトラフィックのルーティングに依存します。カスタム ルートを定義することもできます。または、すべての仮想ネットワークのアドレス範囲を含むサブネットを 1 つ定義できます。

注意

サブネット名の先頭は文字または数字、末尾は文字、数字、またはアンダースコアでなければなりません。文字、数字、アンダースコア、ピリオド、およびハイフンのみを含めることができます。

• DDoS Protection

Basic または Standard のいずれかの DDoS 保護を選択できます。Standard DDoS Protection はプレミアム サービスです。Standard の DDoS 保護の詳細については、「Azure DDoS Protection Standard の概要」を参照してください。

- **サービス エンドポイント**

ここで、サービス エンドポイントを有効にします。その後、有効にする Azure サービス エンドポイントを一覧から選択します。オプションには、Azure Cosmos DB、Azure Service Bus、Azure Key Vault などが含まれます。

これらの設定を構成したら、**[作成]** を選択します。

追加設定の定義

仮想ネットワークを作成したら、追加設定を定義できます。次に例を示します。

- **ネットワーク セキュリティ グループ**

ネットワーク セキュリティ グループのセキュリティ規則を使用して、仮想ネットワーク サブネットとネットワーク インターフェイスに出入りできるネットワーク トラフィックの種類をフィルター処理できます。ネットワーク セキュリティ グループは個別に作成します。その後、それを仮想ネットワークに関連付けます。

- **ルート テーブル**

Azure では、Azure 仮想ネットワークのサブネットごとにルート テーブルが自動的に作成され、既定のシステム ルートがテーブルに追加されます。カスタム ルート テーブルを追加して、仮想ネットワーク間のトラフィックを変更できます。

また、サービス エンドポイントを修正することもできます。

既定値
RFD-vnet

保存 破棄 削除 更新

★ アドレス範囲 (CIDR ブロック) ⓘ

10.0.0.0/24

10.0.0.0 - 10.0.0.255 (256 個のアドレス)

使用可能なアドレス ⓘ

250

ネットワーク セキュリティ グループ

なし >

ルート テーブル

なし >

ユーザー

ユーザーの管理 >

サービス エンドポイント

サービス ⓘ

選択済み 0

仮想ネットワークを構成する

仮想ネットワークを作成した後、Azure portal の **[仮想ネットワーク]** ウィンドウで追加設定を変更できます。または、PowerShell コマンドや Cloud Shell のコマンドを使用して変更を加えることもできます。

9

検索 (Ctrl+F)

<<

(+> 概要

🔒 アクティビティ ログ

👤 アクセス制御 (IAM)

🏷️ タグ

✖️ 問題の診断と解決

設定

<-> アドレス空間

🖨️ 接続済みのデバイス

(+> サブネット

🛡️ DDoS Protection

📦 ファイアウォール (プレビュー)

🌐 WWW DNS サーバー

↔️ ピアリング

🌐 サービスエンドポイント

📊 プロパティ

🔒 ロック

🔄 Automation スクリプト

監視

👁️ 接続モニター

🗺️ ダイアグラム

サポートと トラブルシューティング

🔧 接続のトラブルシューティング

💬 新しいサポート リクエスト

🔄 更新 移動 🗑️ 削除

リソース グループ (変更)
ATS_RG1

場所
米国西部

サブスクリプション (変更)
Technologists_A
サブスクリプション ID
601d2f24-5767-4e46-ae20-f72192cc4cc8

タグ (変更)
タグを追加するにはここをクリック

アドレス空間
10.1.0.0/16
DNS サーバー
Azure 提供の DNS サービス

⌵

接続済みのデバイス

🔍 接続デバイスの検索

デバイス	↑↓ 種類	14 IP アドレス	↑↓ サブネット
結果がありません。			

その後、サブウィンドウで追加設定の確認と変更を行うことができます。設定は次のとおりです。

- **アドレス空間:**初期定義にさらにアドレス空間を追加できます。
- **接続デバイス:**仮想ネットワークを使用してコンピューターを接続します。
- **サブネット:** さらにサブネットを追加できます。
- **ピアリング:**ピアリング配置で仮想ネットワークをリンクします。

仮想ネットワークの監視とトラブルシューティングを行うこともできます。または、自動化スクリプトを作成して、現在の仮想ネットワークを生成できます。

仮想ネットワークは、Azure 内のエンティティを接続するための強力なメカニズムであり、自由に構成することができます。Azure リソースを相互に接続したり、またはオンプレミスのリソースに接続したりできます。ネットワークトラフィックの分離、フィルター処理、およびルーティングを実行できます。Azure では、必要と思われる場所のセキュリティを強化できます。