

インテル® エンドポイント・マネジメント・アシスタント (インテル® EMA)

Microsoft* Azure* 向けデプロイメント・ガイド

免責条項

©2021 Intel Corporation. 無断での引用、転載を禁じます。

本ソフトウェアおよび関連資料は、インテルの著作権で保護された資料であり、それらの使用はユーザーに提供された明示ライセンス（以下「ライセンス」）に準拠します。ライセンスに別段の定めがない限り、本ソフトウェアまたは関連資料をインテルの事前の書面による許可なしに使用、変更、コピー、発行、配布、公開、送信することは禁止されています。

本ソフトウェアおよび関連資料は、ライセンスに明示的に規定された場合を除き、明示的と黙示的とを問わず一切の保証なく、現状のまま提供されます。

インテルのテクノロジーを使用するには、対応したハードウェア、ソフトウェア、またはサービスの有効化が必要となる場合があります。

絶対的なセキュリティを提供できる製品やコンポーネントはありません。

生じるコストおよび結果は異なる場合があります。

本資料は、（明示されているか否かにかかわらず、また禁反言によるとらずにかかわらず）いかなる知的財産権のライセンスも許諾するものではありません。

インテルは、明示されているか否かにかかわらず、いかなる保証もいたしません。ここにいう保証には、商品適格性、特定目的への適合性、および非侵害性の黙示の保証、ならびに履行の過程、取引の過程、または取引での使用から生じるあらゆる保証を含みますが、これらに限定されるわけではありません。

本書で説明されている製品とサービスには、エラッタと呼ばれる不具合が含まれている可能性があり、公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。絶対的なセキュリティを提供できるコンピューター・システムはありません。データやシステムの紛失や盗難など、これらの損失の結果生じたいかなる損害に対しても、インテルは責任を負いません。詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、<http://www.intel.com/technology/vpro> を参照してください。

Intel、インテル、Intel ロゴ、その他のインテルの名称やロゴは、Intel Corporation またはその子会社の商標です。その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。

目次

1 はじめに	1
1.1 クラウド・コンピューティングについて	1
1.2 Azure* コンソールの画面構成	1
1.2.1 Azure* ポータルメニュー	1
1.2.2 Azure* ポータルメニューの展開	1
1.2.3 名前によるサービスの検索	2
1.3 始める前に	2
2 アーキテクチャー概要図	3
2.1 シングル・サーバー・デプロイメント	3
2.2 分散サーバー・デプロイメント	3
3 リソースグループのデプロイメント	3
3.1 リソースグループの概要	3
3.2 リソースグループの作成	4
3.2.1 リソース・グループ・サービスの選択	4
3.2.2 リソースグループの追加	4
3.2.3 リソースグループの設定	5
3.2.4 確認と作成	5
4 ネットワークのデプロイメント	5
4.1 概要	5
4.2 仮想ネットワークの作成	6
4.2.1 仮想ネットワーク・サービスへの移動	6
4.2.2 仮想ネットワークの追加	6
4.2.3 仮想ネットワークの基本情報の設定	7
4.2.4 IPv4 アドレス空間の設定	7
4.2.5 インテル® EMA サーバー用サブネットの追加	8
4.2.6 Azure* Bastion の有効化	8
4.2.7 確認	8
4.3 アプリケーション・セキュリティ・グループ (ASG)	9
4.3.1 アプリケーション・セキュリティ・グループ・サービスへの移動	9
4.3.2 アプリケーション・セキュリティ・グループの追加	9
4.3.3 アプリケーション・セキュリティ・グループ (ASG) の設定	10
4.4 ネットワーク・セキュリティ・グループ	10
4.4.1 インテル® EMA サーバーサブネット用のネットワーク・セキュリティ・グループの作成	10
4.4.2 ネットワーク・セキュリティ・グループの設定	12
4.4.3 確認	17
4.4.4 ネットワーク・セキュリティ・グループのサブネットとの関連付け	17
4.4.5 Azure* Bastion サブネット用のネットワーク・セキュリティ・グループの作成	18
4.4.6 ネットワーク・セキュリティ・グループの設定	19
4.4.7 送信セキュリティ規則の設定	21
4.4.8 ネットワーク・セキュリティ・グループと Azure* Bastion サブネットとの関連付け	24
5 SQL Server* のデプロイメント	24
5.1 概要	24
5.2 SQL Server* の作成	25
5.2.1 新しい SQL Server* の追加	25
5.2.2 SQL Server* の基本情報の設定	26
5.2.3 SQL Server* ファイアウォールの設定	26
6 可用性セット(分散サーバーのみ)	27
6.1 可用性セットの作成	28

7	ロードバランサーのデプロイメント (分散サーバーのみ)	28
7.1	ロードバランサーの作成	28
7.1.1	ロード・バランサー・サービスへの移動	28
7.1.2	ロードバランサーの基本情報	29
7.2	ロードバランサー設定の更新	30
7.2.1	2 つ目のフロントエンド設定の追加	30
7.2.2	2 つ目のフロントエンドの設定	30
7.2.3	バックエンド・プールの追加	31
8	仮想マシンのデプロイメント	31
8.1	概要	31
8.2	仮想マシンの作成	32
8.2.1	VM の追加と基本情報の設定	32
8.2.2	ログファイル保存用のデータディスクの追加	33
8.2.3	VM のネットワーク・インターフェイスの設定	34
8.2.4	VM ロード・バランシング・オプションの設定 (分散サーバーのみ)	35
8.2.5	追加の仮想マシンの作成 (分散サーバーのみ)	35
8.2.6	仮想マシンとアプリケーション・セキュリティ・グループの関連付け	35
9	ロードバランサーの設定の続き (分散サーバーのみ)	36
9.1	正常性プローブの設定	36
9.1.1	Health Probes (正常性プローブ) 画面への移動	36
9.1.2	ウェブ・トラフィック用の正常性プローブの追加	36
9.1.3	Swarm トラフィック用の正常性プローブの追加	37
9.1.4	WebSocket トラフィック用の正常性プローブの追加	37
9.2	負荷分散規則の設定	38
9.2.1	Load Balancing Rules (負荷分散規則) 画面への移動	38
9.2.2	ウェブ・トラフィック用の規則の作成	39
9.2.3	WebSocket トラフィック用の規則の作成	40
9.2.4	Swarm トラフィック用の規則の作成	41
9.3	NAT バックエンド・トラフィック用の送信規則の作成	41
9.3.1	アウトバウンド規則の追加	42
9.3.2	アウトバウンド規則の設定	43
10	Azure* Bastion を使用した仮想マシンへの接続	44
11	付録 A - Active Directory* 統合に関する注記	45
11.1	Active Directory* 統合のアーキテクチャー概要図	45
11.1.1	シングル・サーバー・デプロイメント	45
11.1.2	分散サーバー・デプロイメント	45
11.2	Azure* AD Connect を使用した Active Directory* のクラウドへの拡張	46

1 はじめに

本資料は、1 つまたは複数のインテル® エンドポイント・マネジメント・アシスタント (インテル® EMA) サーバー・インスタンスをサポートするために必要なクラウド・コンピューティング・プラットフォームである、Microsoft* Azure* にインフラストラクチャーを導入する手順を説明します。対象読者は、IT インフラストラクチャーについて中級～上級レベルの知識を持つ IT 管理者で、必ずしもクラウド・コンピューティングに熟知している必要はありません。

クラウド・インフラストラクチャー環境を完成させるには、複数のコンポーネントが必要です。このガイドをよく読み、連携動作に必要な設定を理解することをお勧めします。各コンポーネントのデプロイ手順の前に、各コンポーネントの説明があります。詳しい情報を必要とする方向けに、公式のクラウド・プロバイダーの資料へのリンクも用意されています。

1.1 クラウド・コンピューティングについて

クラウド・コンピューティングとは、IT リソースをインターネットを介してオンデマンドで従量課金制で供給することです。物理的なデータセンターやサーバーを購入/所有して自身で保守管理する代わりに、クラウド・プロバイダーが提供する演算能力、ストレージ、データベースなどのテクノロジー・サービスに必要に応じてアクセスできます。現在必要な分のみをプロビジョニング可能で、その容量はビジネスの変化に応じて拡大することも縮小することも可能です。

大規模なクラウド・プロバイダーのデータセンターは世界中にあるため、顧客やエンドユーザーの住む場所の近くにリソースをデプロイできます。

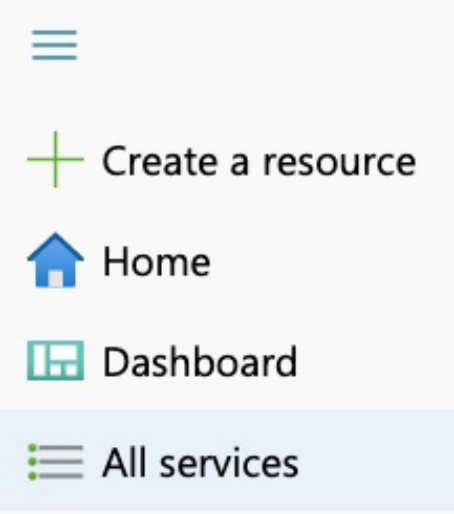
Azure* SQL Server* などのようなフルマネージド型のサービスでは、クラウド・プロバイダーがサービス提供の基盤となるハードウェアやソフトウェアをすべて管理してくれるので、自社のデータに専念できます。クラウド上で仮想マシンを実行する場合、ユーザーが自分で管理する必要があるのはゲスト・オペレーティング・システムとそこにインストールされたソフトウェアのみです。あとはクラウド・プロバイダーが基盤ハードウェアを管理し、最高の信頼性と可用性を提供するために尽力してくれます。

1.2 Azure* コンソールの画面構成

1.2.1 Azure* ポータルメニュー

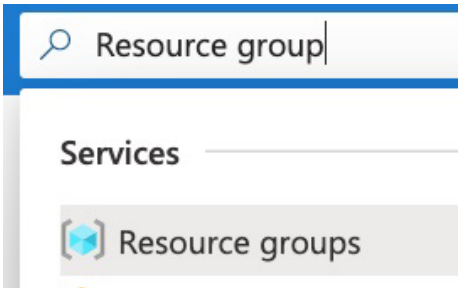
	Microsoft* Azure* のポータル (http://portal.azure.com/) にログインすると、左上隅にメニューアイコンが表示されます。
--	---

1.2.2 Azure* ポータルメニューの展開

	そのアイコンをクリックし、All services (すべてのサービス) を選択すると、サービスのリストが GENERAL (全般)、COMPUTE (計算)、NETWORKING (ネットワーキング)、SECURITY (セキュリティ) などの多くのカテゴリーに分かれて表示されます。 これは、組織に役立つ可能性のあるさまざまなカテゴリーで利用できるサービスを探すのに便利です。
--	--

GENERAL (17) ▾	
COMPUTE (35) ▾	
NETWORKING (29) ▴	
 Virtual networks	
 Load balancers	
 CDN profiles	

1.2.3 名前によるサービスの検索

	本ガイドでは、必要なサービスの名前をすでに知っているため、画面上部にある検索バーを使用してサービスを検索し、表示されるリストから選択します。 例えば、リソースグループを作成するには、検索バーに「Resource group (リソースグループ)」と入力し、その下の Services (サービス) カテゴリに表示された項目をクリックします。
--	---

1.3 始める前に

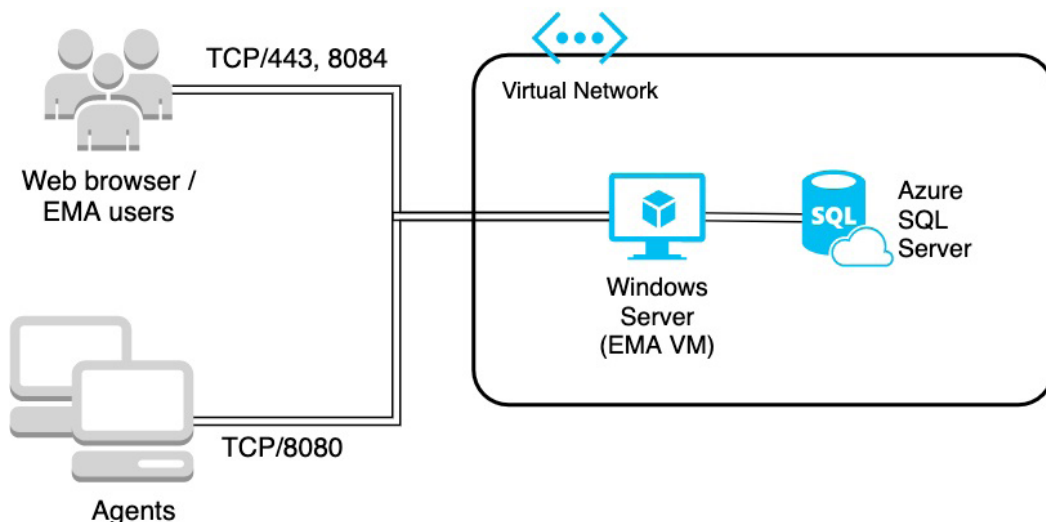
組織に既存の Azure* アカウントがある場合、クラウド管理者に依頼して、本ガイドに記載されたすべてのリソースを作成するのに十分なアクセス権を付与してもらう必要があります。

組織に既存の Azure* アカウントがない場合、または個人として評価する場合、<https://azure.microsoft.com/ja-jp/free/> にアクセスして無料アカウントをセットアップします。

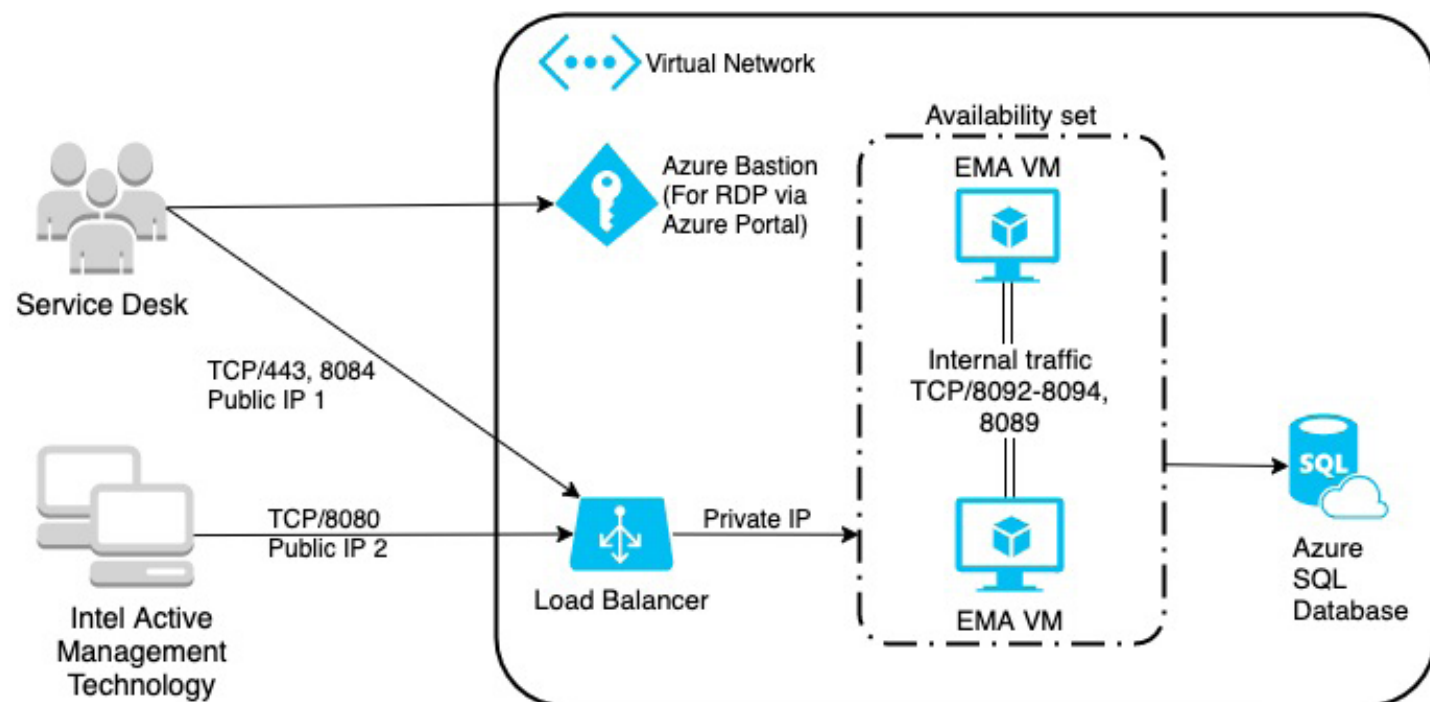
使用するアドレス空間があるか、ネットワーク管理者に確認します。クラウド・プロバイダーへの VPN がすでに確立している場合や将来的にその予定がある場合に、企業ネットワークとの重複を防ぎ、ルーティングの問題を防止できます。また、組織からクラウドにアクセスするトラフィックの送信元 IP アドレスについても確認が必要です。これにより、インターネットからの信頼できるネットワークのみをインテル® EMA の仮想マシンに許可することができます。

2 アーキテクチャー概要図

2.1 シングル・サーバー・デプロイメント



2.2 分散サーバー・デプロイメント



3 リソースグループのデプロイメント

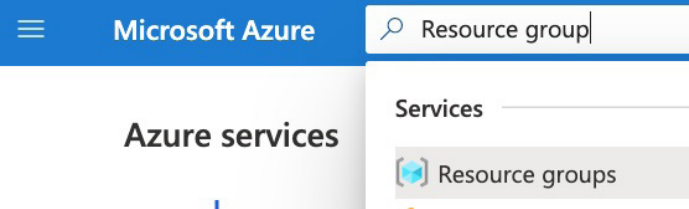
3.1 リソースグループの概要

リソースグループとは、Azure* ソリューションの関連するリソースを保持するコンテナです。リソースグループを使うことで、それらのリソースを1つのグループとして簡単にデプロイ、更新、削除できるようになります。また、グループ内のすべてのリソースに関する請求情報も簡単に確認できます。Azure* で何かをデプロイしようとする、必ず既存のリソースグループを選択するように求められます。そのため、まず、リソースグループの作成から始めましょう。

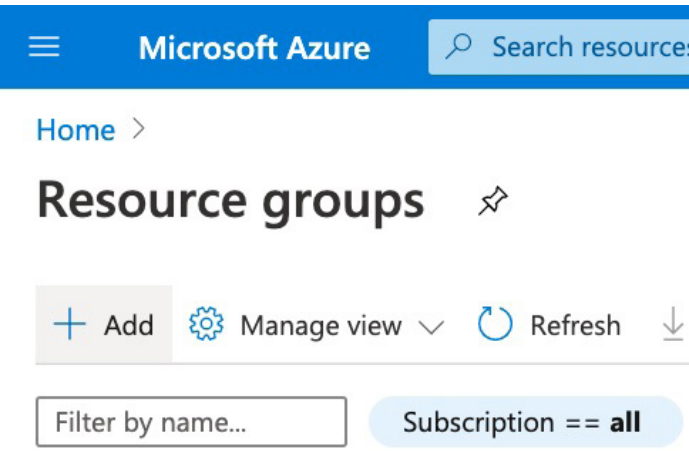
リソースグループの詳細については、以下のリンクを参照してください。 <https://docs.microsoft.com/ja-jp/azure/azure-resource-manager/management/manage-resource-groups-portal>

3.2 リソースグループの作成

3.2.1 リソース・グループ・サービスの選択

	画面上部の検索バーを使用して「 Resource groups (リソース グループ)」を検索し、表示されるリスト項目をクリックします。
--	---

3.2.2 リソースグループの追加

	Add (追加) ボタンをクリックします。
---	------------------------------

3.2.3 リソースグループの設定

Home > Resource groups >

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution, or only those resources that you want to allocate resources to resource groups based on what makes the most sense for your solution.

Project details

Subscription * ⓘ

Resource group * ⓘ intel-ema-resources

Resource details

Region * ⓘ (US) West US

基本情報を次のように入力します。

- **Resource group (リソース グループ)**: 一意のリソースグループ名を入力します。
例: intel-ema-resources
- **Region (リージョン)**: リソースをデプロイするリージョンを選択します。
例: (US) West US (米国西部)

注記: 他のリソースを作成するとき、リージョンの入力が求められる場合があります。デフォルト値はここで選択したリージョンになりますが、そうならない場合のために、本ガイドには適切なリージョンを設定するように指示があります。

3.2.4 確認と作成

1. **Review + create (確認と作成)** ボタンをクリックします。
2. 画面の情報を確認してから、**Create (作成)** ボタンをクリックします。

4 ネットワークのデプロイメント

4.1 概要

仮想マシンが、他の仮想マシン、クラウド・プロバイダー、またはインターネットと通信するには、まずネットワーク環境を構成する必要があります。Virtual Network は、Azure* に構築するプライベート・ネットワークの基本構成要素であり、Azure* 上に仮想化されているという点を除けば、従来のネットワークによく似ています。Virtual Network は他の Virtual Network と論理的に分離されています。

Virtual Network を作成するとき、カスタムのプライベート IP アドレス空間を提供する必要があります。Azure* は必要に応じて、このアドレス空間内のプライベート IP アドレスをリソースに割り当てます。ネットワークが VPN で接続されたときにルーティングの競合が発生しないよう、自組織のその他のネットワーク範囲と重複するアドレス空間の使用は避けることを推奨します。

Virtual Network を作成するとき、サブネットを少なくとも 1 つ作成する必要があります。サブネットを使用すると、仮想ネットワークのアドレス空間の一部を各サブネットに割り当てて仮想ネットワークをセグメント化できます。その後、Azure* リソースを特定のサブネットにデプロイできます。

インバウンド・トラフィックを許可および制御するため、ネットワーク・セキュリティ・グループを作成してサブネットに接続します。サブネットでサービス・エンドポイントを有効化することで、仮想マシンから SQL Server* へのトラフィックが許可されます。

ここでは、Azure* Bastion サービスを使用します。このサービスにより、仮想マシンの RDP ポートをインターネット上に公開することなく、Azure* Portal を介して仮想マシンへの RDP または SSH 接続を構成できます。

本セクションでデプロイするネットワーキング・リソースの詳細については、以下のリンクか、以降のセクションで紹介するその他のリンクを参照してください。

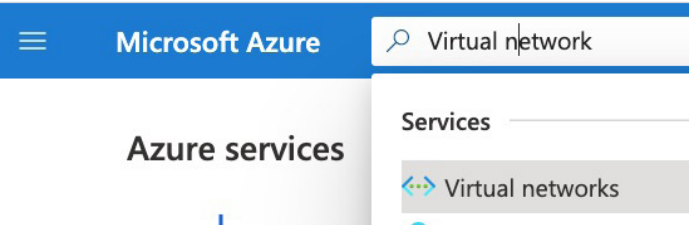
- Virtual Network : <https://docs.microsoft.com/ja-jp/azure/virtual-network/>
- 仮想ネットワーク (VNet) サービス・エンドポイント : <https://docs.microsoft.com/ja-jp/azure/virtual-network/virtual-network-service-endpoints-overview>

- Azure* Bastion : <https://docs.microsoft.com/ja-jp/azure/bastion/>

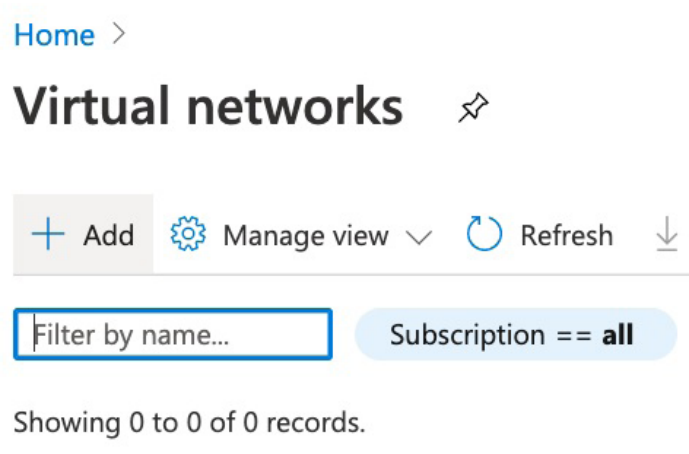
4.2 仮想ネットワークの作成

単一のサブネットに仮想ネットワークを作成する手順は次のとおりです。

4.2.1 仮想ネットワーク・サービスへの移動

	画面上部の検索バーを使用して「 Virtual networks (仮想ネットワーク) 」を検索し、表示されるリスト項目をクリックします。
--	--

4.2.2 仮想ネットワークの追加

	Add (追加) ボタンをクリックします。
---	------------------------------

4.2.3 仮想ネットワークの基本情報の設定

Home > Virtual networks > Create virtual network Basics IP Addresses Security Tags Review + create Azure Virtual Network (VNet) is the fundamental building block for your Azure resources, such as Azure Virtual Machines (VM), to securely communicate. VNet is similar to a traditional network that you'd operate in your data center. VNet benefits of Azure's infrastructure such as scale, availability, and isolation. Project details Subscription * ⓘ Resource group * ⓘ intel-ema-resources Create new Instance details Name * intel-ema-network Region * (US) West US	基本情報を次のように入力します。 • Resource group (リソース グループ) : 先ほど作成したリソースグループを選択します。 例 : <i>intel-ema-resources</i> • Name (名前) : 一意のリソースグループ名を入力します。 例 : <i>intel-ema-network</i> • Region (リージョン) : リソースのデプロイ先とするリージョンに設定されていることを確認します。 例 : <i>(US) West US</i> (米国西部) Next: IP Addresses (次へ : IP アドレス) ボタンをクリックして、次のステップへ進みます。
---	--

4.2.4 IPv4 アドレス空間の設定

Basics IP Addresses Security Tags Review + create The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24). IPv4 address space 10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses) 	ゴミ箱アイコンをクリックしてデフォルトのアドレス空間を削除し、新しい IPv4 アドレス空間を入力します。 例 : 10.250.0.0/24 自社にすでにクラウドへのプライベート IP 接続がある場合、または今後設定する可能性がある場合にルーティングの競合が発生しないよう、ネットワーク技術チームに相談して、利用可能な IP アドレスブロックを選択します。
--	--

4.2.5 インテル® EMA サーバー用サブネットの追加

Add subnet	
Subnet name * ema-servers	Add Subnet (サブネットの追加) ボタンをクリックし、次のようにサブネットを設定します。 Subnet name (サブネット名) : 一意のサブネット名を入力します。 例 : <i>ema-servers</i> Subnet address range (サブネット アドレス範囲) : 先ほど入力した IPv4 アドレス空間内の未使用のサブネットアドレス範囲を入力します。 例 : <i>10.250.0.0/26</i> Services (サービス) ドロップダウン・メニューから Microsoft.Sql を選択します。 Add (追加) ボタンをクリックしてサブネットを確定します。 Next: Security (次へ : セキュリティー) ボタンをクリックします。
Subnet address range * ⓘ 10.250.0.0/26 10.250.0.0 - 10.250.0.63 (59 + 5 Azure reserved addresses)	
SERVICE ENDPOINTS Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more Services ⓘ Microsoft.Sql	
Add Cancel	

4.2.6 Azure* Bastion の有効化

Basics IP Addresses Security Tags Review + create	
BastionHost ⓘ	☐ Disable ☒ Enable
Bastion name *	EmaBastion
AzureBastionSubnet address space *	10.250.0.64/26 10.250.0.64 - 10.250.0.127 (64 addresses)
Public IP address *	(New) EmaBastion Create new
DDoS Protection Standard ⓘ	☒ Disable ☐ Enable
Firewall ⓘ	☒ Disable ☐ Enable

4.2.7 確認

Review + create (確認と作成) ボタンをクリックします。

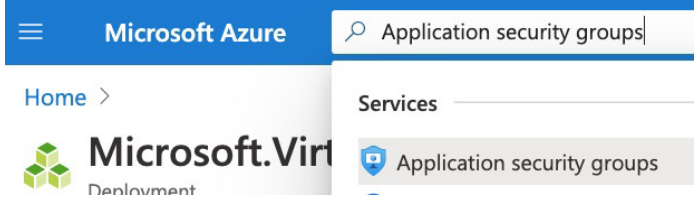
画面に表示されたネットワークの詳細を確認してから、**Create (作成)** ボタンをクリックします。

4.3 アプリケーション・セキュリティ・グループ (ASG)

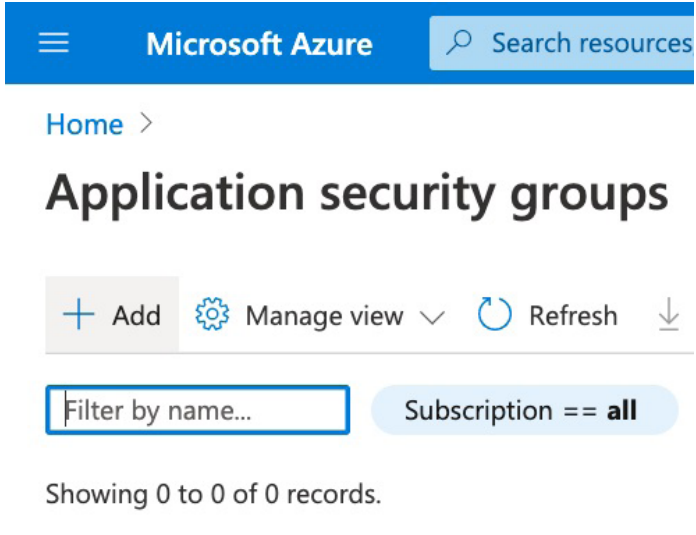
ASG は、ファイアウォール規則の対象を仮想マシンに設定する(「ネットワーク・セキュリティ・グループ」のセクションで後述)のを簡単にする、仮想マシンに適用可能な特別なタグのようなものです。その準備として、以下の手順で ASG を作成します。

アプリケーション・セキュリティ・グループの詳細については、以下のリンクを参照してください。<https://docs.microsoft.com/ja-jp/azure/virtual-network/security-overview#application-security-groups>

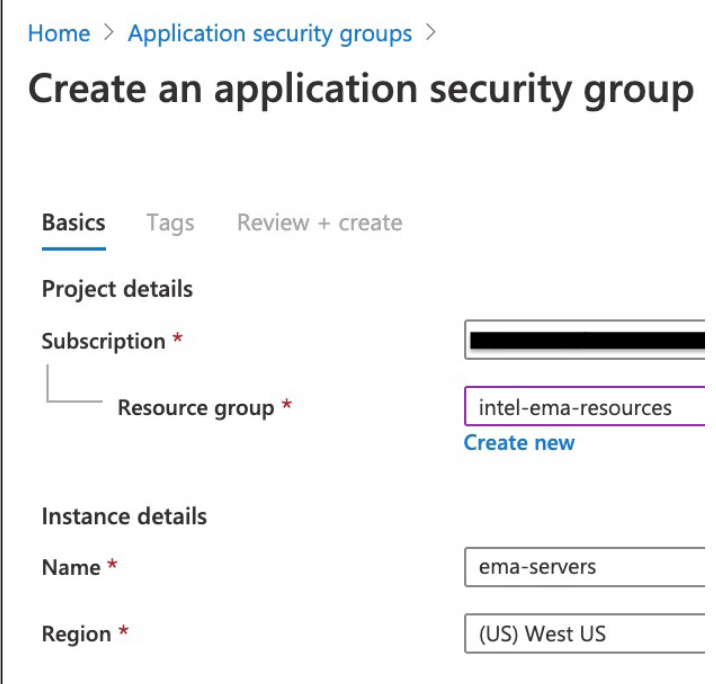
4.3.1 アプリケーション・セキュリティ・グループ・サービスへの移動

	画面上部の検索バーを使用して「Application security groups (アプリケーション・セキュリティ・グループ)」を検索し、表示されるリスト項目をクリックします。
--	---

4.3.2 アプリケーション・セキュリティ・グループの追加

	Add (追加) ボタンをクリックします。
---	------------------------------

4.3.3 アプリケーション・セキュリティ・グループ (ASG) の設定

	基本情報を次のように入力します。 • Resource group (リソース グループ) : 先ほど作成したリソースグループを選択します。 • Name (名前) : 一意の ASG 名を入力します。 例 : <i>ema-servers</i> • Region (リージョン) : リソースのデプロイ先とするリージョンに設定されていることを確認します。 Review + create (確認と作成) ボタンをクリックします。 画面の情報を確認してから、Create (作成) ボタンをクリックします。
--	--

4.4 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 (NSG) には、何種類かの Azure* リソースとの送受信ネットワーク・トラフィックを拒否または許可するセキュリティ規則が含まれます。各規則について、送信元と送信先、ポート、プロトコルを指定できます。

NSG を作成すると、Azure* に既定の規則のセットが含まれます。これらの既定の規則は削除できませんが、非常に低い優先順位を持つため、通常、必要に応じて優先順位の高い規則によってオーバーライドできます。既定の規則は次のとおりです。

AllowVNetInBound : 仮想ネットワーク内のリソース間のすべてのトラフィックを許可します。

AllowAzureLoadBalancerInBound : Azure* Load Balancer から仮想ネットワークへのすべてのトラフィックを許可します。

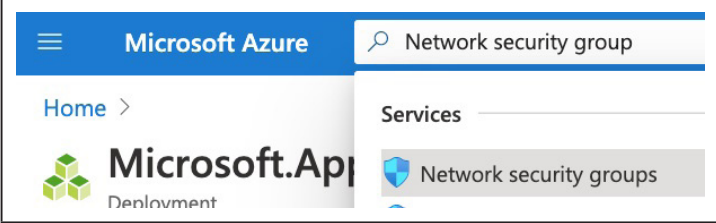
DenyAllInbound : 任意のソースから任意のソースへのすべてのインバウンド・トラフィックを拒否します。

このセクションでは、NSG を作成し、インテル® EMA 仮想マシンへのトラフィックを許可するために必要な規則をすべて追加します。また、Azure* Bastion サブネットへの必要なトラフィックを許可するための 2 つ目の NSG を作成します。

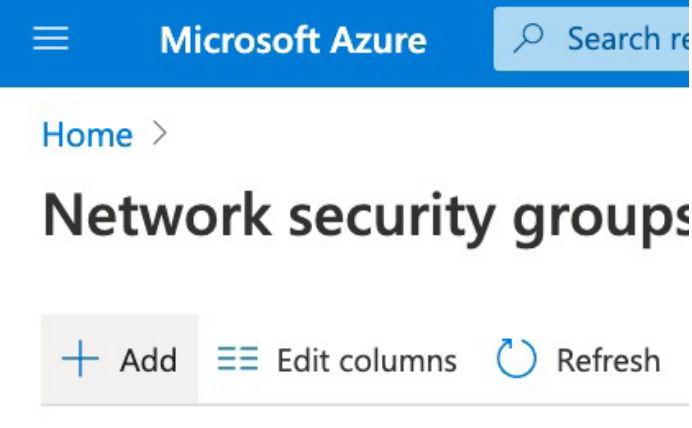
ネットワーク・セキュリティ・グループの詳細については、以下のリンクを参照してください。 <https://docs.microsoft.com/ja-jp/azure/virtual-network/security-overview>

4.4.1 インテル® EMA サーバーサブネット用のネットワーク・セキュリティ・グループの作成

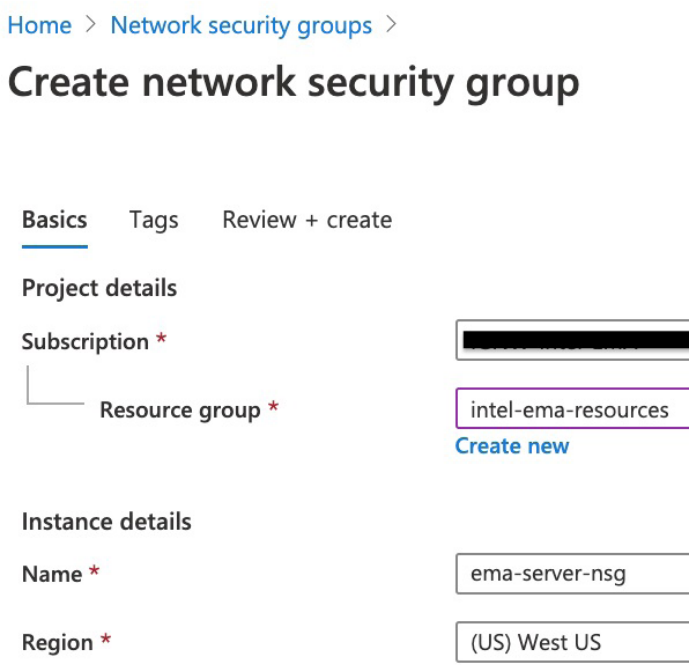
4.4.1.1 ネットワーク・セキュリティ・グループ・サービスへの移動

	画面上部の検索バーを使用して「Network security groups (ネットワーク・セキュリティ・グループ)」を検索し、表示されるリスト項目をクリックします。
--	--

4.4.1.2 ネットワーク・セキュリティ・グループの追加

	Add (追加) ボタンをクリックします。
--	-------------------------------------

4.4.1.3 ネットワーク・セキュリティ・グループ (NSG) の基本情報の設定

	基本情報を次のように入力します。 • Resource group (リソース グループ) : 先ほど作成したリソースグループを選択します。 • Name (名前) : 一意の NSG 名を入力します。 例 : <i>ema-server-nsg</i> • Region (リージョン) : リソースのデプロイ先とするリージョンに設定されていることを確認します。 Review + create (確認と作成) ボタンをクリックします。 画面に表示されたネットワークの詳細を確認してから、Create (作成) ボタンをクリックします。 デプロイ成功のポップアップ・メッセージが表示されたら、Go To Resource (リソースに移動) ボタンをクリックします。
---	--

4.4.2 ネットワーク・セキュリティ・グループの設定

4.4.2.1 受信セキュリティ規則への移動

Home > Network security groups >

ema-server-nsg | Inbound security rules

Network security group

Search (Cmd+/) << + Add Default rules Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Priority	Name	Port
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBala...	Any
65500	DenyAllInBound	Any

ネットワーク・セキュリティ・グループのサイドバーの **Settings(設定)** で、**Inbound security rules (受信セキュリティ規則)** を選択します。

注記: 以下の手順で各規則を作成後、Azure* が優先順位を正しく自動インクリメントできるよう、規則の作成が完了してリストに表示されるまで待機してください。

4.4.2.2 RDP 規則の作成

 **Add inbound security rule**
ema-server-nsg

 Basic

Source * ⓘ

Source IP addresses/CIDR ranges * ⓘ

Add your own trusted network in the field above

Source port ranges * ⓘ

Destination * ⓘ

Destination application security group * ⓘ

Destination port ranges * ⓘ

Protocol *

Any **TCP** UDP ICMP

Action *

Allow Deny

Priority * ⓘ

Name *

Description

Add

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)** : IP Addresses (IP アドレス)
- **Source IP addresses/CIDR ranges (ソース IP アドレス /CIDR 範囲)** : 仮想ネットワーク作成時に定義した Azure* Bastion サブネットの CIDR 範囲を入力します。
例 : 10.250.0.64/26
- **Source port ranges (ソース ポート範囲)** : *
- **Destination (宛先)** : Application security group (アプリケーションのセキュリティ・グループ)
- **Destination application security group (宛先アプリケーションのセキュリティ・グループ)** : ema-servers (または指定した任意の名前)
- **Destination port ranges (宛先ポート範囲)** : 3389
- **Protocol (プロトコル)** : TCP
- **Action (操作)** : Allow (許可)
- **Priority (優先順位)** : 自動で割り当てられた値を使用します。
- **Name (名前)** : 一意の規則名を入力します。
例 : RDP
- **Description (説明)** : インテル® EMA サーバーへの信頼できるソースからの RDP を許可する

完了したら、画面下部の **Add (追加)** ボタンをクリックします。

4.4.2.3 ウェブ・トラフィック規則の作成



Add inbound security rule

ema-server-nsg

Basic

Source *

IP Addresses

Source IP addresses/CIDR ranges *

10.0.0.0/24 or 2001:1234::/64

Add your own trusted network here

Source port ranges *

*

Destination *

Application security group

Destination application security group *

ema-servers

Destination port ranges *

443,8084

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority *

110

Name *

web

Description

Allow web traffic from trusted sources to EMA servers

Add

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)** : IP Addresses (IP アドレス)
- **Source IP addresses/CIDR ranges (ソース IP アドレス/ CIDR 範囲)** : インターネットからインテル® EMA ウェブ・インターフェイスにアクセスすることが許可される、信頼できるネットワークを入力します。制限が不要な場合、Source (ソース) を Any (任意) に設定することもできます。
- **Source port ranges (ソース ポート範囲)** : *
- **Destination (宛先)** : Application security group (アプリケーションのセキュリティ・グループ)
- **Destination application security group (宛先アプリケーションのセキュリティ・グループ)** : ema-servers (または指定した任意の名前)
- **Destination port ranges (宛先ポート範囲)** : 443,8084
- **Protocol (プロトコル)** : TCP
- **Action (操作)** : Allow (許可)
- **Priority (優先順位)** : 自動で割り当てられた値を使用します。
- **Name (名前)** : 一意の規則名を入力します。
例 : web
- **Description (説明)** : インテル® EMA サーバーへの信頼できるソースからのウェブ・トラフィックを許可する

完了したら、画面下部の **Add (追加)** ボタンをクリックします。

4.4.2.4 Swarm トラフィック規則の作成



Add inbound security rule

ema-server-nsg

 Basic

Source * ⓘ

Source port ranges * ⓘ

Destination * ⓘ

Destination application security group * ⓘ

Destination port ranges * ⓘ

Protocol *

☐ Any ☒ TCP ☐ UDP ☐ ICMP

Action *

☒ Allow ☐ Deny

Priority * ⓘ

Name *

Description

Add

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)** : Any (任意)
- **Source port ranges (ソース ポート範囲)** : *
- **Destination (宛先)** : Application security group (アプリケーションのセキュリティ・グループ)
- **Destination application security group (宛先アプリケーションのセキュリティ・グループ)** : ema-servers (または指定した任意の名前)
- **Destination port ranges (宛先ポート範囲)** : 8080
- **Protocol (プロトコル)** : TCP
- **Action (操作)** : Allow (許可)
- **Priority (優先順位)** : 自動で割り当てられた値を使用します。
- **Name (名前)** : 一意の規則名を入力します。
例 : swarm
- **Description (説明)** : 任意のソースからインテル® EMA サーバーへの Swarm トラフィックを許可する

完了したら、画面下部の **Add (追加)** ボタンをクリックします。

4.4.2.5 内部トラフィック規則の追加 (分散サーバーのみ)



Add inbound security rule

ema-server-nsg

Basic

Source * ⓘ

Application security group

Source application security group * ⓘ

ema-servers

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

ema-servers

Destination port ranges * ⓘ

8092-8094,8089

Protocol *

Any

TCP

UDP

ICMP

Action *

Allow

Deny

Priority * ⓘ

130

Name *

ema_internal

Description

Allow internal communication between EMA servers

Add

分散サーバー・アーキテクチャをデプロイする場合、次の手順に従います。そうでない場合は省略できます。

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)**: *Application security group* (アプリケーションのセキュリティ・グループ)
- **Source application security group (ソース アプリケーションのセキュリティ・グループ)**: *ema-servers* (または指定した任意の名前)
- **Source port ranges (ソース ポート範囲)**: *
- **Destination (宛先)**: *Application security group* (アプリケーションのセキュリティ・グループ)
- **Destination application security group (宛先アプリケーションのセキュリティ・グループ)**: *ema-servers* (または指定した任意の名前)
- **Destination port ranges (宛先ポート範囲)**: 8092-8094,8089
- **Protocol (プロトコル)**: *TCP*
- **Action (操作)**: *Allow* (許可)
- **Priority (優先順位)**: 自動で割り当てられた値を使用します。
- **Name (名前)**: 一意の名前を入力します。
例: *ema_internal*
- **Description (説明)**: インテル® EMA サーバー間の内部通信を許可する

完了したら、画面下部の **Add (追加)** ボタンをクリックします。

4.4.3 確認

完了すると、以下の図に示すような表が表示されます。

注記：ema_internal 規則が存在するのは、分散サーバー・アーキテクチャーをデプロイする場合のみです。

+ Add

Default rules

Refresh

Priority	Name	Port	Protocol	Source	Destination
100	RDP	3389	TCP	10.250.0.64/26	ema-servers
110	web	443,8084	TCP		ema-servers
120	swarm	8080	TCP	Any	ema-servers
130	ema_internal	8092-8094,8089	TCP	ema-servers	ema-servers
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

4.4.4 ネットワーク・セキュリティ・グループのサブネットとの関連付け

4.4.4.1 ネットワーク・セキュリティ・グループのサブネット関連付けへの移動

Home > Network security groups >

ema-server-nsg | Subnets

Network security group

+ Associate

Name

No results.

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

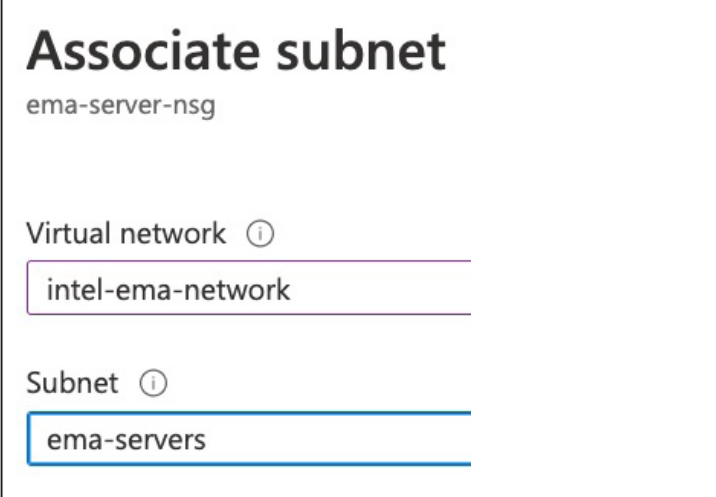
Outbound security rules

Network interfaces

Subnets

ネットワーク・セキュリティ・グループのサイドバーの **Settings (設定)** で **Subnets (サブネット)** を選択してから、**Associate (関連付け)** ボタンをクリックします。

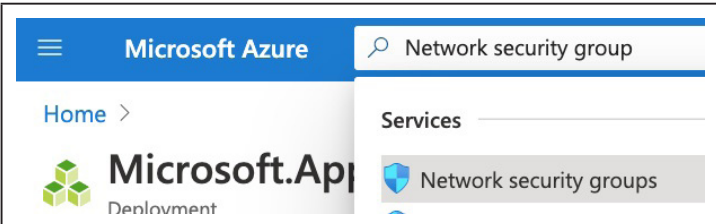
4.4.4.2 ネットワーク・セキュリティ・グループとサブネットの関連付け

	先ほどインテル® EMA サーバー用に作成したサブネットを選択し、 OK をクリックします。
--	---

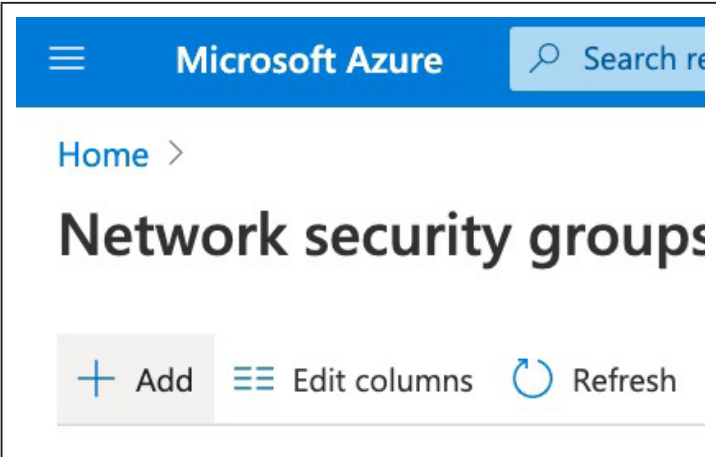
4.4.5 Azure* Bastion サブネット用のネットワーク・セキュリティ・グループの作成

参考 : <https://docs.microsoft.com/ja-jp/azure/bastion/bastion-nsg>

4.4.5.1 ネットワーク・セキュリティ・グループ・サービスへの移動

	画面上部の検索バーを使用して「 Network security groups (ネットワーク・セキュリティ・グループ) 」を検索し、表示されるリスト項目をクリックします。
---	---

4.4.5.2 ネットワーク・セキュリティ・グループの追加

	Add (追加) ボタンをクリックします。
--	------------------------------

4.4.5.3 ネットワーク・セキュリティ・グループの基本情報の設定

Create network security group

Basics Tags Review + create

Project details

Subscription * IGNW-Intel-EMA

Resource group * intel-ema-resources
[Create new](#)

Instance details

Name * ema-bastion-nsg

Region * (US) West US

基本情報を次のように入力します。

- **Resource group (リソース グループ)**: 先ほど作成したリソースグループを選択します。
- **Name (名前)**: 一意の名前を入力します。
例: `ema-bastion-nsg`
- **Region (リージョン)**: リソースのデプロイ先とするリージョンに設定されていることを確認します。

Review + create (確認と作成) ボタンをクリックします。

画面に表示されたネットワークの詳細を確認してから、**Create (作成)** ボタンをクリックします。

デプロイ成功のポップアップ・メッセージが表示されたら、**Go To Resource (リソースに移動)** ボタンをクリックします。

4.4.6 ネットワーク・セキュリティ・グループの設定

4.4.6.1 受信セキュリティ規則への移動

ema-bastion-nsg | Inbound security rules

Network security group

Search (Cmd+ /) << + Add Default rules Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

Inbound security rules Outbound security rules

Priority	Name
65000	AllowVnetIn
65001	AllowAzureIn
65500	DenyAllInBo

ネットワーク・セキュリティ・グループのサイドバーの **Settings (設定)** で、**Inbound security rules (受信セキュリティ規則)** を選択します。

注記: 以下の手順で各規則を作成後、Azure* が優先順位を正しく自動インクリメントできるよう、規則の作成が完了してリストに表示されるまで待機してください。

4.4.6.2 Azure* Bastion への HTTPS を許可する規則の作成

 **Add inbound security rule**

ema-bastion-nsg

 Basic

Source * ⓘ

Service Tag

Source service tag * ⓘ

Internet 

Source port ranges * ⓘ

*

Destination * ⓘ

Any

Destination port ranges * ⓘ

443

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

AllowHttpsInbound

Description

Allow HTTPS to Azure Bastion

Add

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)** : *Service Tag* (サービス タグ)
- **Source service tag (ソース・サービス・タグ)** : *Internet* (インターネット)
- **Source port ranges (ソース・ポート範囲)** : *
- **Destination (宛先)** : *Any* (任意)
- **Destination port ranges (宛先ポート範囲)** : 443
- **Protocol (プロトコル)** : *TCP*
- **Action (操作)** : *Allow* (許可)
- **Priority (優先順位)** : 自動で割り当てられた値を使用します。
- **Name (名前)** : 一意の名前を入力します。
例 : *AllowHttpsInbound*
- **Description (説明)** : Azure* Bastion への HTTPS を許可する

画面下部の **Add (追加)** ボタンをクリックします。

4.4.6.3 Gateway Manager から Azure* Bastion への接続を許可する規則の作成

 Add inbound security rule ema-bastion-nsg  Basic Source * ⓘ Service Tag Source service tag * ⓘ GatewayManager Source port ranges * ⓘ * Destination * ⓘ Any Destination port ranges * ⓘ 443 Protocol * Any TCP UDP ICMP Action * Allow Deny Priority * ⓘ 110 Name * AllowGatewayManagerInbound Description Allow control plane traffic to Azure Bastion Add	画面の上の方にある Add (追加) ボタンをクリックし、以下のように規則を設定します。 • Source (ソース) : <i>Service Tag</i> (サービス タグ) • Source service tag (ソース・サービス・タグ) : <i>GatewayManager</i> • Source port ranges (ソース・ポート範囲) : * • Destination (宛先) : <i>Any</i> (任意) • Destination port ranges (宛先ポート範囲) : 443 • Protocol (プロトコル) : <i>TCP</i> • Action (操作) : <i>Allow</i> (許可) • Priority (優先順位) : 自動で割り当てられた値を使用します。 • Name (名前) : 一意の名前を入力します。 例 : <i>AllowGatewayManagerInbound</i> • Description (説明) : Azure* Bastion へのコントロール・プレーン・トラフィックを許可する 画面下部の Add (追加) ボタンをクリックします。
---	---

4.4.7 送信セキュリティ規則の設定

Settings  Inbound security rules  Outbound security rules	サイドバーの Inbound Security rules (受信セキュリティ規則) の下にある Outbound security rules (送信セキュリティ規則) をクリックします。
---	---

4.4.7.1 仮想ネットワークへの SSH/RDP エグレス・トラフィックの有効化

 **Add outbound security rule**
ema-bastion-nsg

 Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Service Tag

Destination service tag ⓘ

VirtualNetwork

Destination port ranges * ⓘ

22,3389

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

AllowRdpOutbound

Description

Allow SSH and RDP connections from Azure Bastion to our vi

Add

画面の上の方にある **Add (追加)** ボタンをクリックし、以下のように規則を設定します。

- **Source (ソース)** : Any (任意)
- **Source port ranges (ソース ポート範囲)** : *
- **Destination (宛先)** : Service Tag (サービス タグ)
- **Destination service tag (宛先サービス タグ)** : VirtualNetwork
- **Destination port ranges (宛先ポート範囲)** : 22,3389
- **注記**: いずれかのポートが不要な場合でも、Azure* Bastion では両方のポートを有効にする必要があります。
- **Protocol (プロトコル)** : Any (任意)
- **Action (操作)** : Allow (許可)
- **Priority (優先順位)** : 自動で割り当てられた値を使用します。
- **Name (名前)** : 一意の名前を入力します。
例 : AllowGatewayManagerInbound
- **Description (説明)** : Azure* Bastionk から仮想ネットワークへの RDP 接続を許可する

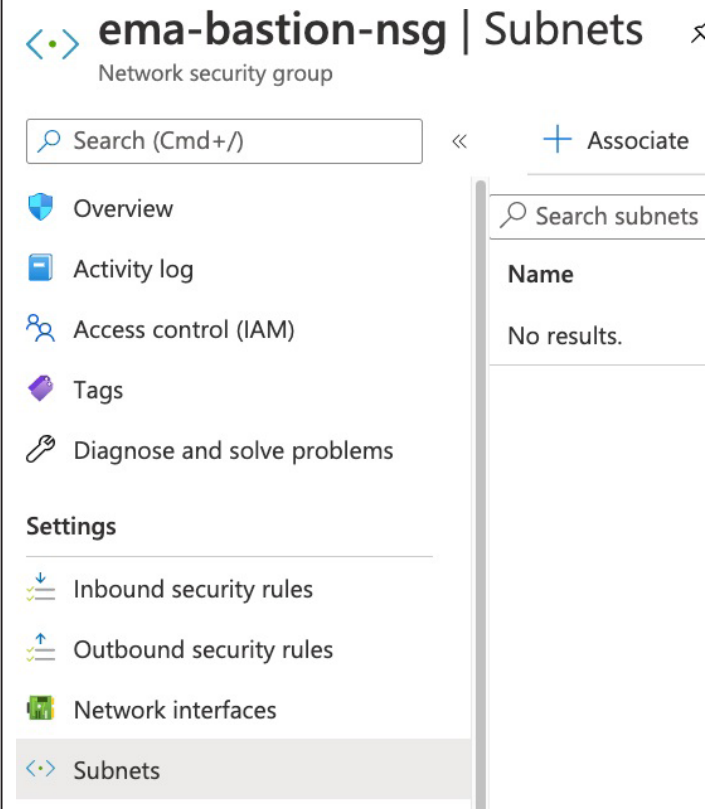
画面下部の **Add (追加)** ボタンをクリックします。

4.4.7.2 Azure* サービスへのエグレスの有効化

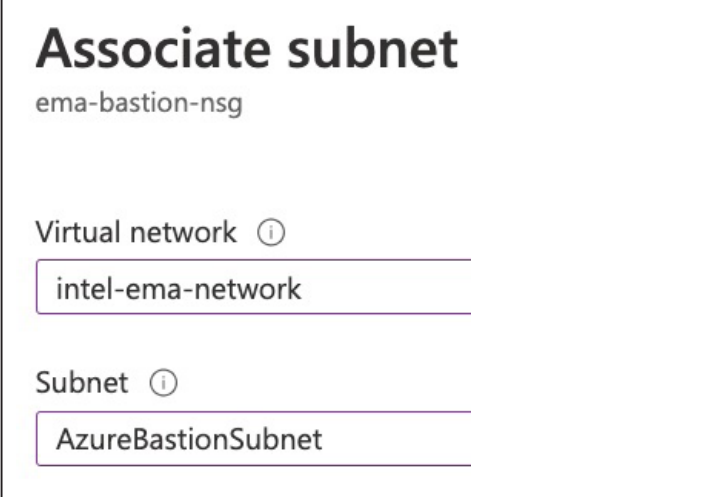
 Add outbound security rule ema-bastion-nsg  Basic Source * ⓘ Any Source port ranges * ⓘ * Destination * ⓘ Service Tag Destination service tag ⓘ AzureCloud Destination port ranges * ⓘ 443 Protocol * Any TCP UDP ICMP Action * Allow Deny Priority * ⓘ 110 Name * AllowAzureCloudOutbound Description Add	画面の上の方にある Add (追加) ボタンをクリックし、以下のように規則を設定します。 • Source (ソース) : Any (任意) • Source port ranges (ソース ポート範囲) : * • Destination (宛先) : Service Tag (サービス タグ) • Destination service tag (宛先サービス タグ) : AzureCloud • Destination port ranges (宛先ポート範囲) : 443 • Protocol (プロトコル) : TCP • Action (操作) : Allow (許可) • Priority (優先順位) : 自動で割り当てられた値を使用します。 • Name (名前) : 一意の名前を入力します。 例 : AllowAzureCloudOutbound • Description (説明) : Azure* Bastion がパブリック Azure* サービス・エンドポイントに接続することを許可する 画面下部の Add (追加) ボタンをクリックします。
---	--

4.4.8 ネットワーク・セキュリティ・グループと Azure* Bastion サブネットとの関連付け

4.4.8.1 ネットワーク・セキュリティ・グループのサブネット関連付けへの移動

	ネットワーク・セキュリティ・グループのサイドバーの Settings (設定) で Subnets (サブネット) を選択してから、Associate (関連付け) ボタンをクリックします。
---	---

4.4.8.2 ネットワーク・セキュリティ・グループとサブネットの関連付け

	先ほどインテル® EMA サーバー用に作成したサブネットを選択し、OK をクリックします。
--	---

5 SQL Server* のデプロイメント

5.1 概要

Azure* には、フルマネージド型の Platform-as-a-Service (PaaS) データベース・エンジンがあります。これは次の 2 つのコンポーネントで構成されています。

- 論理 SQL Server*。これには DNS ホスト名が関連付けられます。
- 1 つまたは複数の SQL Database。スケーラビリティと性能を向上するために個別に構成できます。

マネージド型のサービスであることから、ユーザーが手間をかけることなく、最新安定バージョンの SQL Server* データベース・エンジン上で 99.99% の可用性でデータベースを実行し続けるために必要なほとんどのデータベース管理作業（アップグレード、パッチ適用、バックアップ、モニタリングなど）が Azure* によって行われます。Standard 高可用性モデルと、Premium 高可用性モデルがあります。

SQL Database を使うと、[仮想コア \(vCore\) ベースの購入モデル](#)と [DTU ベースの購入モデル](#)の 2 つの異なる購入モデルの中で、簡単に性能を定義し、スケーリングできます。

- [仮想コア \(vCore\) ベースの購入モデル](#)では、vCore の数、メモリー容量、ストレージ容量および速度を選択できます。
- [DTU ベースの購入モデル](#)は、コンピューティング・リソース、メモリーリソース、I/O リソースの組み合わせを、データベース・ワークロードの負荷レベルに対応する 3 つのサービス階層で提供します。

これは、事前に論理 SQL Server* を作成しておくだけで、インテル® EMA サーバーで使用できます。SQL Database は、インテル® EMA のインストール・プロセス中に動的に作成されます。インストール・プロセスが完了した後、Azure* 管理コンソールに戻ってデータベースの設定を確認し、必要に応じて調整できます。

Azure* SQL Server*、SQL Database、高可用性モデルの詳細については、以下のリンクを参照してください。

<https://docs.microsoft.com/ja-jp/azure/azure-sql/>

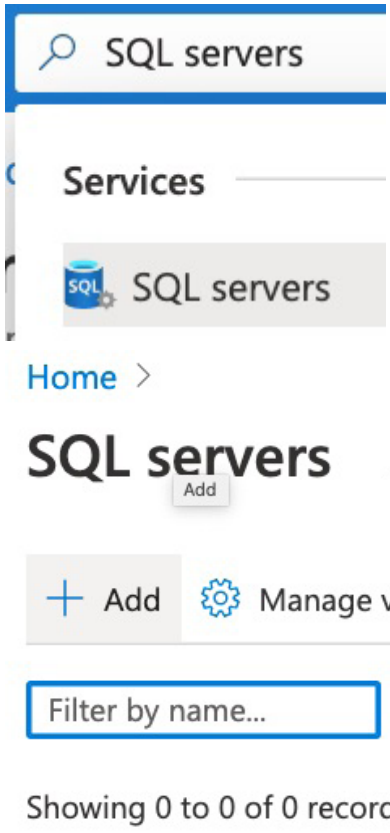
<https://docs.microsoft.com/ja-jp/azure/azure-sql/database/>

<https://docs.microsoft.com/ja-jp/azure/azure-sql/database/high-availability-sla>

5.2 SQL Server* の作成

Azure* SQL Server* を作成し、仮想マシンサブネットからのアクセスを有効にする手順は次のとおりです。

5.2.1 新しい SQL Server* の追加

	画面上部の検索バーを使用して「SQL servers」を検索し、表示されるリスト項目をクリックします。 Add (追加) ボタンをクリックします。
--	--

5.2.2 SQL Server* の基本情報の設定

Home > SQL servers >

Create SQL Database Server

Microsoft

Basics Networking Additional settings Tags Review + create

SQL database server is a logical container for managing databases and elastic pools. Complete the Basic tab, then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Server details

Enter required settings for this server, including providing a name and location.

Server name * ✓
.database.windows.net

Location * ✓

Administrator account

Server admin login * ✓

Password * ✓

Confirm password * ✓

[Review + create](#) [Next : Networking >](#)

基本情報を次のように入力します。

- **Resource group (リソース グループ)** : 先ほど作成したリソースグループを選択します。
- **Server name (サーバー名)** : グローバルで一意的な名前を入力します。
例 : *ema-demo*
注記 : ここで選択した名前にサフィックス「.database.windows.net」を付けたものが、インテル® EMA のインストール・プロセス中にデータベースにアクセスするために使用できる DNS 名になります。
- **Location (場所)** : リソースのデプロイ先とするリージョンに設定されていることを確認します。
- 管理者アカウントのユーザー名とパスワードを入力します。

Review + create (確認と作成) ボタンをクリックします。

画面上の情報を確認し、**Create (作成)** ボタンをクリックし、作成が完了したらリソースに移動します。

5.2.3 SQL Server* ファイアウォールの設定

ema-demo | Firewa

SQL server

Search (Cmd+/) <<

Security

- Advanced data security
- Auditing
- Firewalls and virtual networks**
- Private endpoint connections
- Transparent data encryption

SQL Server* のサイドバーの **Security(セキュリティ)** セクションで、**Firewalls and virtual networks(ファイアウォールと仮想ネットワーク)** を選択します。

Connections from the VNET/Subnet specified below provides access to all databases in ema-demo.

Virtual networks

+ Add existing virtual network
+ Create new virtual network

Rule name	Virtual network	Subnet
No vnet rules for this server.		

右側のウィンドウを下にスクロールし、**Add existing virtual network (既存の仮想ネットワークを追加)** をクリックします。

5.2.3.1 規則の命名と既存ネットワークおよびサブネットの選択

Create/Update

virtual network rule

Name *

allow-ema-servers

provide vnet rule name

Subscription *

Virtual network *

intel-ema-network

Subnet name / Address prefix *

ema-servers / 10.250.0.0/26

Virtual network	Service endpoint stat...
intel-ema-network/e...	Enabled

仮想ネットワークの規則の詳細を次のように入力します。

- **Name (名前)**: 一意の名前を入力します。
例: `allow-ema-servers`
- **Virtual network (仮想ネットワーク)**: 先ほど作成した仮想ネットワークが選択されていることを確認します。
- **Subnet name / Address prefix (サブネット名/アドレス・プレフィックス)**: 先ほど作成したサブネットが選択されていることを確認します。

OK ボタンをクリックします。

6 可用性セット (分散サーバーのみ)

可用性セットとは、仮想マシンの論理的なグループ分けです。仮想マシンが複数の物理サーバー、コンピューティング・ラック、ストレージ単位、ネットワーク・スイッチにわたって確実に実行されるように Azure* に指示します。その目的は、ハードウェアまたはソフトウェア障害が発生しても、影響を受けるのは VM のサブネットのみで、ソリューション全体は稼働状態を保つことです。

可用性セットを作成する手順は次のとおりです。ここで作成した可用性セットは、後で VM を作成するときに割り当てることができます。

シングルサーバーのみをデプロイする場合、このセクションは省略できます。

可用性セットの詳細については、以下のリンクを参照してください。 <https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/tutorial-availability-sets>

Azure* 向けインテル® EMA ウェブ・デプロイメント・ガイド – 2020 年 10 月

27

6.1 可用性セットの作成

- 画面上部の検索バーを使用して「Availability sets (可用性セット)」を検索し、表示されるリスト項目をクリックします。
- Add (追加)** ボタンをクリックします。
- 基本情報を次のように入力します。
 - Resource group (リソース グループ)**: 先ほど作成したリソースグループを選択します。
 - Name (名前)**: 一意の名前を入力します。
例: ema-servers
 - Region (リージョン)**: リソースのデプロイ先とするリージョンに設定されていることを確認します。
- Review + create (確認と作成)** ボタンをクリックします。
- 画面の情報を確認してから、**Create (作成)** ボタンをクリックします。

7 ロードバランサーのデプロイメント (分散サーバーのみ)

Azure* Load Balancer は、第 4 層 (TCP) ロードバランサーで、ユーザー・トラフィックをアプリケーションの複数のインスタンスに分散させます。ロード・バランシングは、負荷を分散させることで、アプリケーションに過剰な負荷がかかったり、低速化したり、機能しなくなるリスクを緩和します。ロードバランサーの正常性プローブが各 VM の指定されたポートをモニタリングし、稼働状態の VM にのみトラフィックを分配します。

ここではまず、フロントエンド設定のみを定義したロードバランサーを作成します。後で仮想マシンを作成するときに、仮想マシンをロードバランサーのバックエンドに接続します。ロードバランサーでは、ウェブ・トラフィックと Swarm トラフィック用に個別のフロントエンド IP アドレスを持ちます。

VM をロードバランサーに接続した後、ロードバランサーの設定に戻り、ヘルスチェックと転送ルールをセットアップし、受信トラフィックを適切なバックエンド VM ポートに向けます。

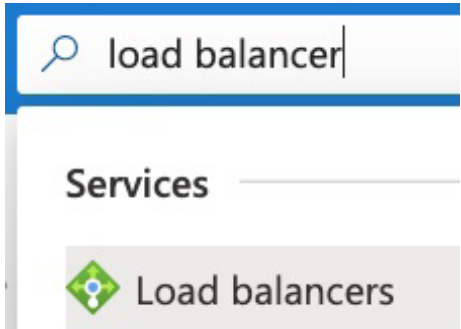
シングルサーバーのみをデプロイする場合、このセクションは省略できます。

Windows* VM 間のロード・バランシングの詳細については、以下のリンクを参照してください。

<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/tutorial-load-balancer>

7.1 ロードバランサーの作成

7.1.1 ロード・バランサー・サービスへの移動

	画面上部の検索バーを使用して「Load balancers (ロードバランサー)」を検索し、表示されるリスト項目をクリックします。
--	--

7.1.2 ロードバランサーの基本情報

Create load balancer

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers use a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *
Resource group *
intel-ema-resources
[Create new](#)

Instance details

Name *
ema-load-balancer
Region *
(US) West US
Type * ⓘ
☐ Internal ☒ Public
SKU * ⓘ
☐ Basic ☒ Standard

Public IP address

Public IP address * ⓘ
Public IP address name *
ema-load-balancer-ip
Public IP address SKU
Standard
Assignment
☐ Dynamic ☒ Static
Add a public IPv6 address ⓘ
 No Yes

Standard Load Balancer is secure by default. This means Network Security Groups (NSGs) are used to explicitly permit and whitelist allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource. Please configure an NSG to ensure communication if needed. For outbound communication, an explicit outbound rule is needed. [Learn more about outbound connectivity](#)

Add (追加) ボタンをクリックします。

基本情報を次のように入力します。

- **Resource group (リソース グループ)** : 先ほど作成したリソースグループを選択します。
- **Name (名前)** : 一意の名前を入力します。
例 : *ema-load-balancer*
- **Region (リージョン)** : リソースのデプロイ先とするリージョンに設定されていることを確認します。
- **Type (タイプ)** : *Public* (パブリック)
- **SKU** : *Standard* (標準)
- **Public IP address (パブリック IP アドレス)** : *Create new* (新規作成)
- **Public IP address name (パブリック IP アドレス名)** :
ema-web-lb-ip

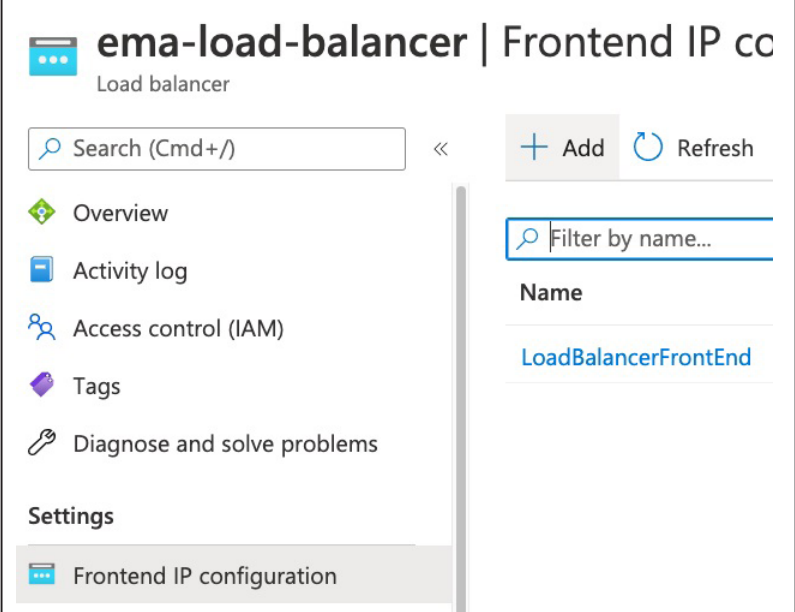
Review + create (確認と作成) ボタンをクリックします。

画面の情報を確認してから、**Create (作成)** ボタンをクリックします。

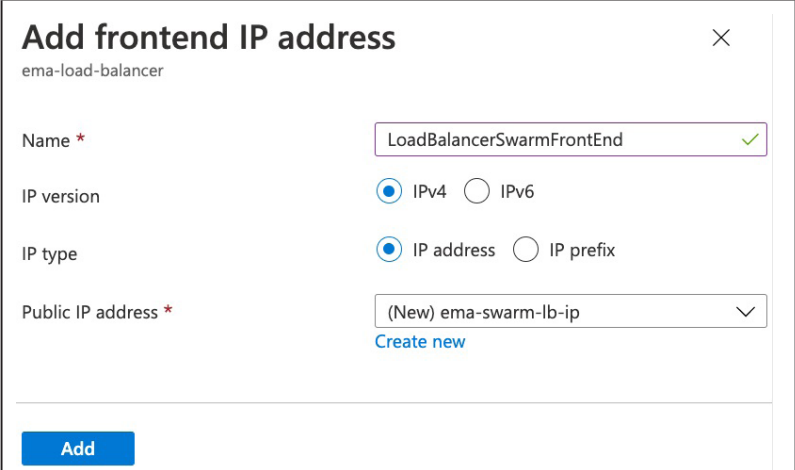
デプロイが完了したら、**Go to Resource (リソースに移動)** ボタンをクリックします。

7.2 ロードバランサー設定の更新

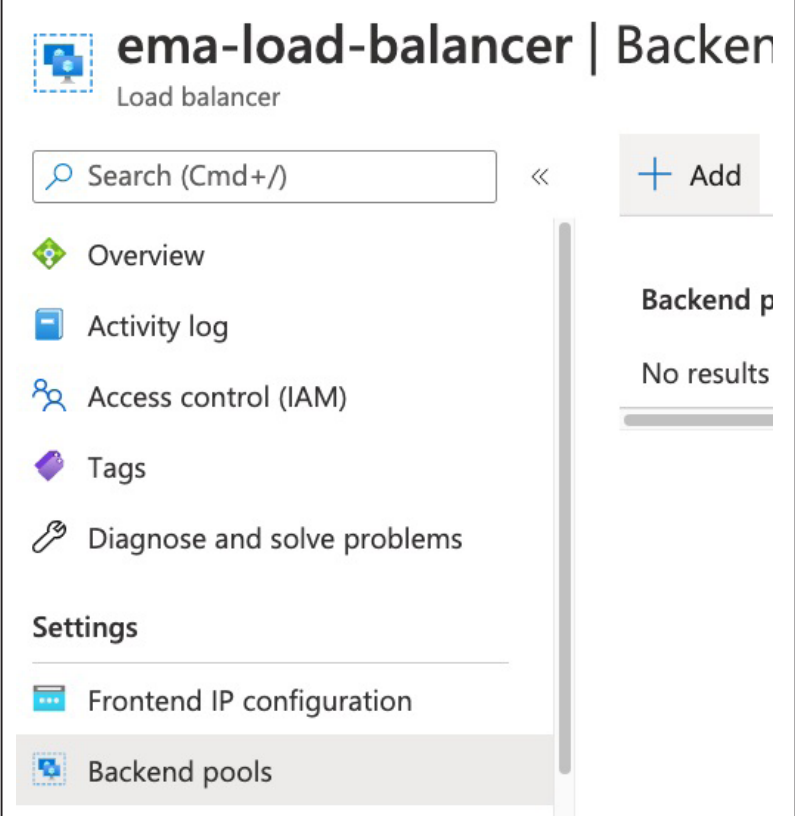
7.2.1 2 回目のフロントエンド設定の追加

	サイドバーの Settings (設定) で、Frontend IP Configuration (フロントエンド IP 構成) をクリックします。 Add (追加) ボタンをクリックします。
--	---

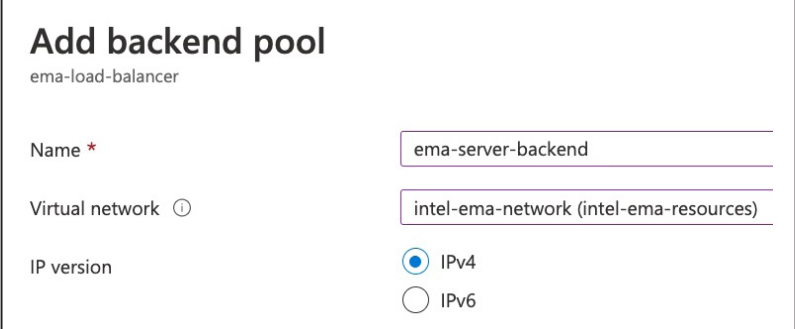
7.2.2 2 回目のフロントエンドの設定

	フロントエンドの一意の名前を入力します。 例 : <i>LoadBalancerSwarmFrontEnd</i> Public IP address (パブリック IP アドレス) では、Create new (新規作成) リンクをクリックし、IP アドレスに名前を付けます。 例 : <i>ema-swarm-lb-ip</i> Add (追加) ボタンをクリックします。
--	---

7.2.3 バックエンド・プールの追加

	サイドバーの Settings (設定) で、Backend pools (バックエンド・プール) をクリックします。 Add (追加) ボタンをクリックします。
---	--

バックエンド・プールの設定

	一意のバックエンド・プール名を入力します。 例 : <i>ema-server-backend</i> 既存の仮想ネットワークを選択します。 Add (追加) ボタンをクリックします。 このバックエンド・プールは、仮想マシン作成時に選択肢として表示されます。
--	--

8 仮想マシンのデプロイメント

8.1 概要

Azure* 仮想マシン (VM) は、物理的ハードウェアを購入、保守する手間なく、柔軟性の高い仮想化コンピューティングを提供します。ただし、ゲスト・オペレーティング・システムとそこで実行されるソフトウェアの管理については、ユーザーの責任です。

VM に割り当てる CPU、メモリー、ストレージの量は、インスタンスの作成時にユーザーが決定しますが、いずれも後から増減できます。CPU やメモリーを削減してワークロード用の VM を最適化してコストを削減することもできます。

分散サーバー・デプロイメントでは、以下の手順に追加のステップがあります。シングル・サーバー・デプロイメントの場合、これらのステップは省略できます。これには、2 つ目の VM の作成、VM と可用性セットの関連付け、VM のロードバランサーへの接続が含まれます。

Windows* ベースの仮想マシンの詳細については、以下のリンクを参照してください。

<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/>

<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/overview>

8.2 仮想マシンの作成

8.2.1 VM の追加と基本情報の設定

Create a virtual machine

×

Basics Disks Networking Management Advanced Tags ...

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
[Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

intel-ema-resources
[Create new](#)

Instance details

Virtual machine name * ⓘ

ema-server-1 ✓

Region * ⓘ

(US) West US

Availability options ⓘ

Availability set

Availability set * ⓘ

ema-servers
[Create new](#)

Image * ⓘ

Windows Server 2019 Datacenter
[Browse all public and private images](#)

Azure Spot instance ⓘ

☐ Yes ☒ No

Size * ⓘ

Standard_E2sv3 - 2 vcpus, 16 GiB memory...
[Select size](#)

Administrator account

Username * ⓘ

ema ✓

Password * ⓘ

..... ✓

Confirm password * ⓘ

..... ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

☒ None ☐ Allow selected ports

画面上部の検索バーを使用して「Virtual machines (仮想マシン)」を検索し、表示されるリスト項目をクリックします。

Add (追加) ボタンをクリックします。

VM の基本情報を次のように設定します。

- **Resource group (リソース グループ)** : 先ほど作成したリソースグループを選択します。
- **Name (名前)** : 一意の名前を入力します。
例 : `ema-server-1`
- **Region (リージョン)** : リソースのデプロイ先とするリージョンに設定されていることを確認します。
- **Availability options (可用性オプション)** :
(シングルサーバーのみ) *No infrastructure redundancy required* (インフラストラクチャー冗長は必要ありません)
(分散サーバーのみ) *Availability set* (可用性セット)
- **Availability set (可用性セット) (分散サーバーのみ)** : 先ほど作成した可用性セットを選択します。
- **Image (イメージ)** : サポートされる最新の Windows Server* イメージを選択します。
- **Size (サイズ)** : マシンサイズを選択します。
推奨値 : *Standard_E2sv3 - 2 vcpus, 16 GiB memory*
(Standard_E2sv3 - 2 個の vCPU、16 GiB メモリー)
- **Azure Spot instance (Azure* スポット・インスタンス)** : *No* (いいえ)
- **Administrator account (管理者アカウント)** の情報を入力します。
- **Public inbound ports (パブリック受信ポート)** : *None* (なし)

Next: Disks (次へ : ディスク) ボタンをクリックします。

8.2.2 ログファイル保存用のデータディスクの追加

8.2.2.1 新しいディスクの作成と接続

Basics

Disks

Networking

Management

Advanced

Tags

Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ Premium SSD ▼

Encryption type * (Default) Encryption at-rest with a platform-managed key ▼

Enable Ultra Disk compatibility ⓘ ☐ Yes ☒ No

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				

Create and attach a new disk (新しいディスクを作成して接続する) リンクをクリックします。

8.2.2.2 新しいディスクの詳細設定

Home > Virtual machines > Create a virtual machine >

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name * ema-server-1_logs ✓

Source type * ⓘ None (empty disk) ▼

Size * ⓘ 256 GiB
Standard HDD
[Change size](#)

Encryption type * (Default) Encryption at-rest with a platform-managed k... ▼

Enable shared disk ☐ Yes ☒ No
Shared disk not available for the selected size.

OK

ディスクの詳細を以下のように設定します。

- **Name (名前)** : デフォルトの名前をそのまま使用するか、一意のディスク名を入力します。
- **Source type (ソース タイプ)** : None (empty disk) (なし (空のディスク))
- **Size (サイズ)** : **Change size (サイズの変更)** リンクをクリックし、ディスクのタイプとディスクのサイズを設定します。256 GiB の標準 HDD を推奨します。
- **Encryption type (暗号化の種類)** : Default (既定)

OK ボタンをクリックします。

8.2.2.3 データディスクの項目の確認

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
0	ema-server-1_logs	256	Standard HDD	Read-only

[Create and attach a new disk](#) [Attach an existing disk](#)

▼ **Advanced**

[Review + create](#) [< Previous](#) [Next : Networking >](#)

データディスクの情報を確認してから、**Next: Networking (次へ : ネットワーク)** ボタンをクリックします。

注記: VM が起動した後、Windows* のディスク管理ユーティリティを使用してストレージディスクを初期化、フォーマット、およびマウントする必要があります。

8.2.3 VM のネットワーク・インターフェイスの設定

Basics Disks **Networking** Management Advanced ...

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ intel-ema-network
[Create new](#)

Subnet * ⓘ ema-servers (10.250.0.0/26)
[Manage subnet configuration](#)

Public IP ⓘ None
[Create new](#)

NIC network security group ⓘ ☒ None ☐ Basic ☐ Advanced

Networking (ネットワーク) を選択し、ネットワーク・インターフェイスを次のように設定します。

- **Virtual network (仮想ネットワーク)**: 先ほど作成した VPC を選択します。
- **Subnet (サブネット)**: 先ほど作成したサブネットが選択されていることを確認します。
- **Public IP (パブリック IP)**: None (なし)
- **NIC network security group (NIC ネットワーク・セキュリティ・グループ)**: None (なし)

シングル・サーバー・デプロイメントの場合、**Review + create (確認および作成)** ボタンをクリックし、画面上の情報を確認してから、**Create (作成)** ボタンをクリックします。

分散サーバー・デプロイメントの場合、続けて次のステップのネットワーク設定に進みます。

8.2.4 VM ロード・バランシング・オプションの設定 (分散サーバーのみ)

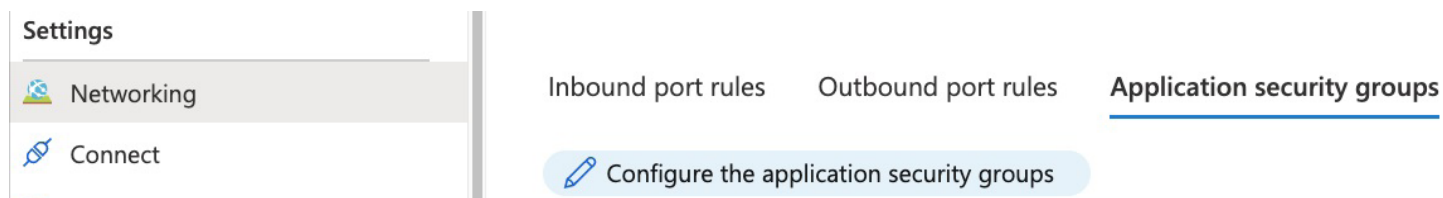
Load balancing You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more Place this virtual machine behind an existing load balancing solution? ☒ Yes ☐ No Load balancing settings • Application Gateway is an HTTP/HTTPS web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. Learn more about Application Gateway • Azure Load Balancer supports all TCP/UDP network traffic, port-forwarding, and outbound flows. Learn more about Azure Load Balancer Load balancing options * ⓘ Azure load balancer ▼ Select a load balancer * ⓘ ema-load-balancer ▼ Select a backend pool * ⓘ ema-server-backend ▼ Create new	Networking (ネットワーク) 画面の下半分にある Load balancing (負荷分散) を設定します。 • Place this virtual machine behind an existing load balancing solution (この仮想マシンを既存の負荷分散ソリューションの後ろに配置しますか?) : Yes (はい) • Load balancing options (負荷分散のオプション) : <i>Azure load balancer</i> (Azure* Load Balancer) • Select a load balancer (ロード バランサーを選択する) : 先ほど作成したロードバランサーを選択します。 • Select a backend pool (バックエンド・プールを選択する) : 先ほど作成したバックエンド・プールを選択します。 Review + create (確認および作成) ボタンをクリックし、画面上の情報を確認してから、Create (作成) ボタンをクリックして VM の作成を完了します。
---	--

8.2.5 追加の仮想マシンの作成 (分散サーバーのみ)

分散サーバー・デプロイメントでは、前述した手順に従って、少なくとも 1 つの追加 VM を作成します。

8.2.6 仮想マシンとアプリケーション・セキュリティ・グループの関連付け

作成した各 VM について、サイドバーの **Settings (設定)** カテゴリで **Networking (ネットワーク)** を選択し、**Application security groups (アプリケーション・セキュリティ・グループ)** タブを選択し、**Configure the application security groups (アプリケーション・セキュリティ・グループの設定)** をクリックします。

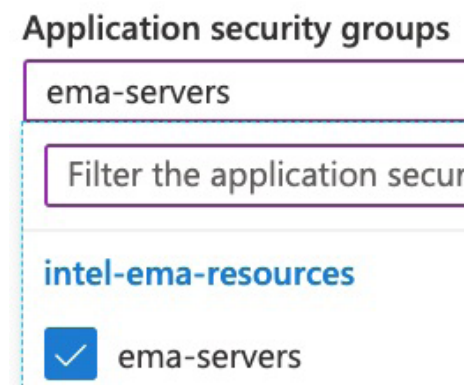


Settings

Networking Inbound port rules Outbound port rules Application security groups

Connect [Configure the application security groups](#)

先ほど作成したアプリケーション・セキュリティ・グループを選択します。



Application security groups

ema-servers

Filter the application security groups

intel-ema-resources

☒ ema-servers

9 ロードバランサーの設定の続き (分散サーバーのみ)

仮想マシンの作成が完了したら、ロードバランサーの設定に戻り、ヘルスチェックと転送ルールをセットアップし、受信トラフィックを適切なバックエンド VM ポートに向けます。

9.1 正常性プローブの設定

9.1.1 Health Probes (正常性プローブ) 画面への移動

	画面上部の検索バーを使用して「Load balancers (ロードバランサー)」を検索し、表示されるリスト項目をクリックします。 先ほど作成したロードバランサーをクリックします。 サイドバーの Settings (設定) で、Health probes (正常性プローブ) をクリックします。
--	--

9.1.2 ウェブ・トラフィック用の正常性プローブの追加

	Add (追加) ボタンをクリックし、正常性プローブを以下のように設定します。 • Name (名前) : 一意の名前を入力します。 例 : <i>ema-https</i> • Protocol (プロトコル) : <i>TCP</i> • Port (ポート) : <i>443</i> OK ボタンをクリックします。
--	--

9.1.3 Swarm トラフィック用の正常性プローブの追加

Add health probe ema-load-balancer Name * ema-swarm Protocol ⓘ	Add (追加) ボタンをクリックし、正常性プローブを以下のように設定します。 • Name (名前): 一意の名前を入力します。 例: <i>ema-swarm</i> • Protocol (プロトコル): <i>TCP</i> • Port (ポート): <i>8080</i> OK ボタンをクリックします。
TCP Port * ⓘ	
8080 Interval * ⓘ	
5 Unhealthy threshold * ⓘ	
2	

9.1.4 WebSocket トラフィック用の正常性プローブの追加

Add health probe ema-load-balancer Name * ema-websocket Protocol ⓘ	Add (追加) ボタンをクリックし、正常性プローブを以下のように設定します。 • Name (名前): 一意の名前を入力します。 例: <i>ema-websocket</i> • Protocol (プロトコル): <i>TCP</i> • Port (ポート): <i>8084</i> OK ボタンをクリックします。
TCP Port * ⓘ	
8084 Interval * ⓘ	
5 Unhealthy threshold * ⓘ	
2	

9.2 負荷分散規則の設定

9.2.1 Load Balancing Rules (負荷分散規則) 画面への移動

ema-load-balancer | Load balancing rules

Load balancer

Search (Cmd+ /) << + Add

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Search load balancing rules

Name	↑↓	Load balance
No results.		

ローダーバランサーの詳細画面のサイドバーから **Load balancing rules (負荷分散規則)** を選択します。

9.2.2 ウェブ・トラフィック用の規則の作成

ema-https

ema-load-balancer

Save

Discard

Delete

Name *

ema-https

IP Version *

IPv4

IPv6

Frontend IP address * ⓘ

13.83.98.18 (LoadBalancerFrontEnd)

Protocol

TCP

UDP

Port *

443

Backend port * ⓘ

443

Backend pool ⓘ

ema-server-backend (2 virtual machines)

Health probe ⓘ

ema-https (TCP:443)

Session persistence ⓘ

Client IP

Idle timeout (minutes) ⓘ

30

TCP reset

Disabled

Enabled

Floating IP ⓘ

Disabled

Outbound source network address translation (SNAT) ⓘ

Outbound and inbound use the same IP. SNAT port exhaustion may occur.

(Recommended) Use outbound rules to provide backend pool members access to the internet.

[Learn more](#)

Add (追加) ボタンをクリックし、規則を以下のように設定します。

- **Name (名前)** : *ema-https*
- **Frontend IP address (フロントエンド IP アドレス)** : ウェブ・トラフィックに使用されるロード・バランサー・フロントエンドを選択します。
例 : *LoadBalancerFrontEnd*
- **Protocol (プロトコル)** : *TCP*
- **Port (ポート)** : *443*
- **Backend Port (バックエンド・ポート)** : *443*
- **Backend pool (バックエンド・プール)** : 先ほど作成したバックエンド・プールを選択します。
例 : *ema-server-backend*
- **Health probe (正常性プローブ)** : 先ほど作成したポート 443 の正常性プローブを選択します。
例 : *ema-https*
- **Session persistence (セッション永続化)** : *Client IP* (クライアント IP)
- **Idle timeout (minutes) (アイドル・タイムアウト (分))** : 最大値 (30) に設定します
- **TCP reset (TCP リセット)** : *Enabled* (有効)
- **Outbound source network address translation (アウトバウンド送信元ネットワーク・アドレス変換 (SNAT))** : *Use outbound rules to provide backend pool members access to the internet.* (アウトバウンド規則を使用してバックエンド・プール・メンバーにインターネットへのアクセスを提供する)

OK ボタンをクリックします。

9.2.3 WebSocket トラフィック用の規則の作成

ema-websocket

ema-load-balancer

Save

Discard

Delete

Name *

ema-websocket

IP Version *

IPv4

IPv6

Frontend IP address * ⓘ

13.83.98.18 (LoadBalancerFrontEnd)

Protocol

TCP

UDP

Port *

8084

Backend port * ⓘ

8084

Backend pool ⓘ

ema-server-backend (2 virtual machines)

Health probe ⓘ

ema-websocket (TCP:8084)

Session persistence ⓘ

Client IP

Idle timeout (minutes) ⓘ

30

TCP reset

Disabled

Enabled

Floating IP ⓘ

Disabled

Outbound source network address translation (SNAT) ⓘ

Outbound and inbound use the same IP. SNAT port exhaustion may occur.

(Recommended) Use outbound rules to provide backend pool members access to the internet.
[Learn more](#)

Add (追加) ボタンをクリックし、規則を以下のように設定します。

- **Name (名前)** : *ema-websocket*
- **Frontend IP address (フロントエンド IP アドレス)** : ウェブ・トラフィックに使用されるロード・バランサー・フロントエンドを選択します。
例 : *LoadBalancerFrontEnd*
- **Protocol (プロトコル)** : *TCP*
- **Port (ポート)** : *8084*
- **Backend Port (バックエンド・ポート)** : *8084*
- **Backend pool (バックエンド・プール)** : 先ほど作成したバックエンド・プールを選択します。
例 : *ema-server-backend*
- **Health probe (正常性プローブ)** : 先ほど作成したポート 8084 の正常性プローブを選択します。
例 : *ema-websocket*
- **Session persistence (セッション永続化)** : *Client IP* (クライアント IP)
- **Idle timeout (minutes) (アイドル・タイムアウト (分))** : 最大値 (30) に設定します
- **TCP reset (TCP リセット)** : *Enabled* (有効)
- **Outbound source network address translation (アウトバウンド送信元ネットワーク・アドレス変換 (SNAT))** : *Use outbound rules to provide backend pool members access to the internet.* (アウトバウンド規則を使用してバックエンド・プール・メンバーにインターネットへのアクセスを提供する)

OK ボタンをクリックします。

9.2.4 Swarm トラフィック用の規則の作成

ema-swarm

ema-load-balancer

Save

Discard

Delete

Name *

ema-swarm

IP Version *

IPv4

IPv6

Frontend IP address * ⓘ

13.88.132.106 (LoadBalancerSwarmFrontEnd)

Protocol

TCP

UDP

Port *

8080

Backend port * ⓘ

8080

Backend pool ⓘ

ema-server-backend (2 virtual machines)

Health probe ⓘ

ema-swarm (TCP:8080)

Session persistence ⓘ

None

Idle timeout (minutes) ⓘ

30

TCP reset

Disabled

Enabled

Floating IP ⓘ

Disabled

Outbound source network address translation (SNAT) ⓘ

Outbound and inbound use the same IP. SNAT port exhaustion may occur.

(Recommended) Use outbound rules to provide backend pool members access to the internet.

Add (追加) ボタンをクリックし、規則を以下のように設定します。

- **名前 (Name)** : *ema-swarm*
- **Frontend IP address (フロントエンド IP アドレス)** : 最初のロードバランサー設定時に Swarm トラフィック用に作成したフロントエンドを選択します。
例 : *LoadBalancerSwarmFrontEnd*
- **Protocol (プロトコル)** : *TCP*
- **Port (ポート)** : *8080*
- **Backend Port (バックエンド・ポート)** : *8080*
- **Backend pool (バックエンド・プール)** : 先ほど作成したバックエンド・プールを選択します。
例 : *ema-server-backend*
- **Health probe (正常性プローブ)** : 先ほど作成したポート 8080 の正常性プローブを選択します。
例 : *ema-swarm*
- **Session persistence (セッション永続化)** : *None* (なし)
- **Idle timeout (minutes) (アイドル・タイムアウト (分))** : 最大値 (30) に設定します
- **TCP reset (TCP リセット)** : *Enabled* (有効)
- **Outbound source network address translation (アウトバウンド送信元ネットワーク・アドレス変換 (SNAT))** : *Use outbound rules to provide backend pool members access to the internet.* (アウトバウンド規則を使用してバックエンド・プール・メンバーにインターネットへのアクセスを提供する)

OK ボタンをクリックします。

9.3 NAT バックエンド・トラフィック用の送信規則の作成

仮想マシンはパブリック IP アドレスを持たないため、インターネットに向けたアウトバウンド・トラフィックにソース・ネットワーク・アドレス変換 (SNAT) を使用する必要があります。Azure* NAT ゲートウェイをデプロイしなくても、フロントエンド IP アドレスをアウトバウンド・トラフィック用のソース IP アドレスとして使用することで、すでに作成したロードバランサーがこの機能を提供できます。

このトピックの詳細については、以下のリンクを参照してください。 <https://docs.microsoft.com/ja-jp/azure/load-balancer/load-balancer-outbound-connections>

9.3.1 アウトバウンド規則の追加

ema-load-balancer | Outbound rules

Load balancer

Search (Cmd+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Outbound rules

+ Add

Refresh

Use outbound rules to configure virtual machines in the backend must be standard and the front address. [Learn more about out](#)

Filter by name...

Frontend IP address == all

Name	Frontend IP address
Add a rule to get started	

ロードバランサー画面のサイドバーの **Settings (設定)** セクションで、**Outbound rules (アウトバウンド規則)** をクリックします。

Add (追加) ボタンをクリックします。

9.3.2 アウトバウンド規則の設定

Add outbound rule

ema-load-balancer

Name *

Frontend IP address *
[Create new](#)

Protocol ☒ All ☐ TCP ☐ UDP

Idle timeout (minutes) Max: 30

TCP Reset ☒ Enabled ☐ Disabled

Backend pool *
[Create new](#)

Port allocation

Azure automatically assigns the number of outbound ports to use for source network address translation (SNAT) based on the number of frontend IP addresses and backend pool instances.
[Learn more about outbound connectivity](#)

Port allocation

Outbound ports

Choose by *

Ports per instance

Frontend IPs

Maximum number of backend instances

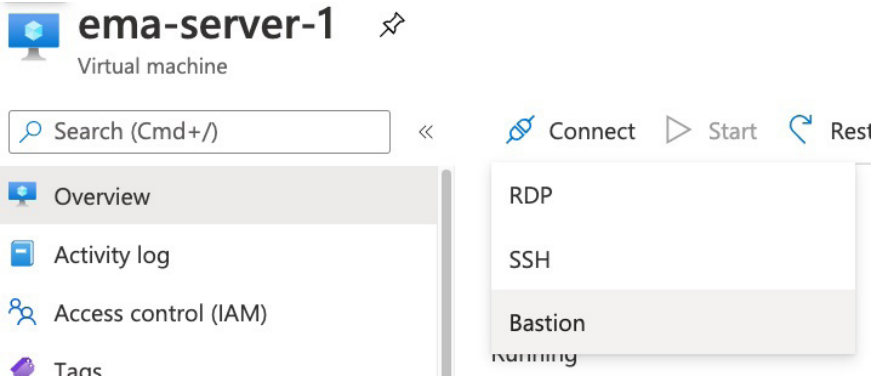
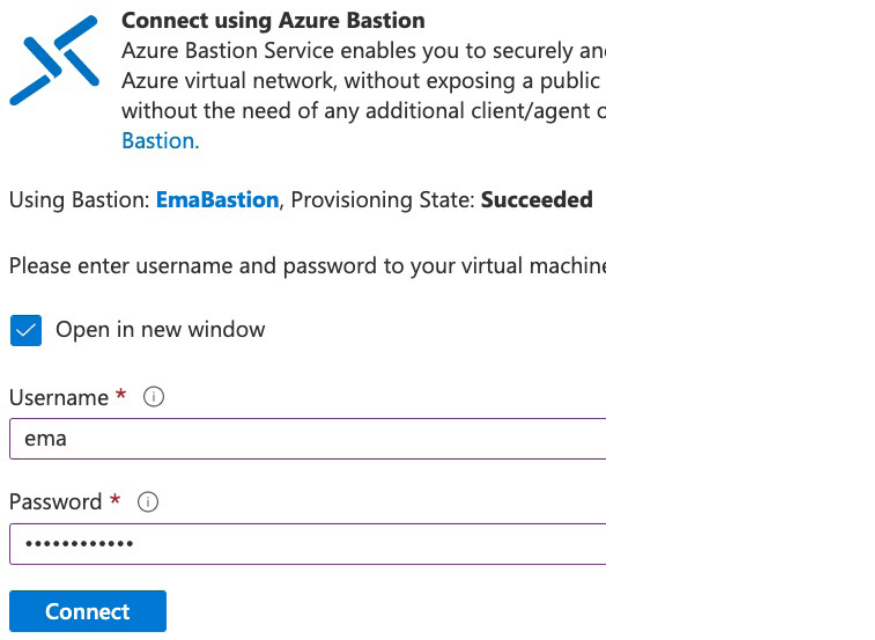
[Add](#)

アウトバウンド規則を以下のように設定します。

- **Name (名前)** : 一意の名前を入力します。
例 : *ema-server-outbound*
- **Frontend IP address (フロントエンド IP アドレス)** : ドロップダウン・メニューから利用可能なすべての IP アドレスを選択します。
- **Protocol (プロトコル)** : *All* (すべて)
- **TCP Reset (TCP リセット)** : *Enabled* (有効)
- **Backend Pool (バックエンド・プール)** : 先ほど作成したバックエンド・プールを選択します。
例 : *ema-server-backend*
- **Port allocation (ポートの割り当て)** : *Manually choose number of outbound ports* (送信ポートの数を手動で選択する)
- **Outbound ports Choose by (送信ポート選択基準)** : *Maximum number of backend instances* (バックエンド・インスタンスの最大数)
- **Maximum number of backend instances (バックエンド・インスタンスの最大数)** : 各フロントエンド IP アドレスごとに、64,000 個のポートが SNAT に使用可能です。ここで数を選択すると、ポートのプールの総数がその数で割られ、各バックエンド・インスタンスが等しい数のポートを利用できるようになります。このデプロイメント・ガイドでは、2 つの VM をデプロイすることを想定しているため、必要な場合に VM を 1 つ追加できる余地を残して 3 と入力します。

Add (追加) ボタンをクリックします。

10 Azure* Bastion を使用した仮想マシンへの接続

	任意の仮想マシンにログインするには、VM の Overview (概要) 画面に移動し、Connect (接続) ボタンをクリックし、Bastion を選択します。
	Use Bastion (Bastion を使用する) ボタンをクリックします。
	VM の資格情報を入力し、Connect (接続) ボタンをクリックします。 ブラウザーのウィンドウが開き、その VM への RDP セッションが表示されます。

11 付録 A - Active Directory* 統合に関する注記

仮想マシンをドメインに参加させ、AD 認証を使用できるようにするために、Active Directory* と Microsoft* Azure* を統合する方法は複数あります。組織のニーズは多種多様なため、本付録では、既存のオンプレミス・ディレクトリーをこの目的でクラウドに拡張するためのいくつかのヒントを提供します。クラウド・プロバイダーは、時折、提供サービスを変更します。そのため、本稼働用のソリューションをデプロイする前に、ビジネスに最も適したソリューションを確認する必要があります。詳細情報へのリンクを以下に示します。

「[Azure* Active Directory* のドキュメント](#)」

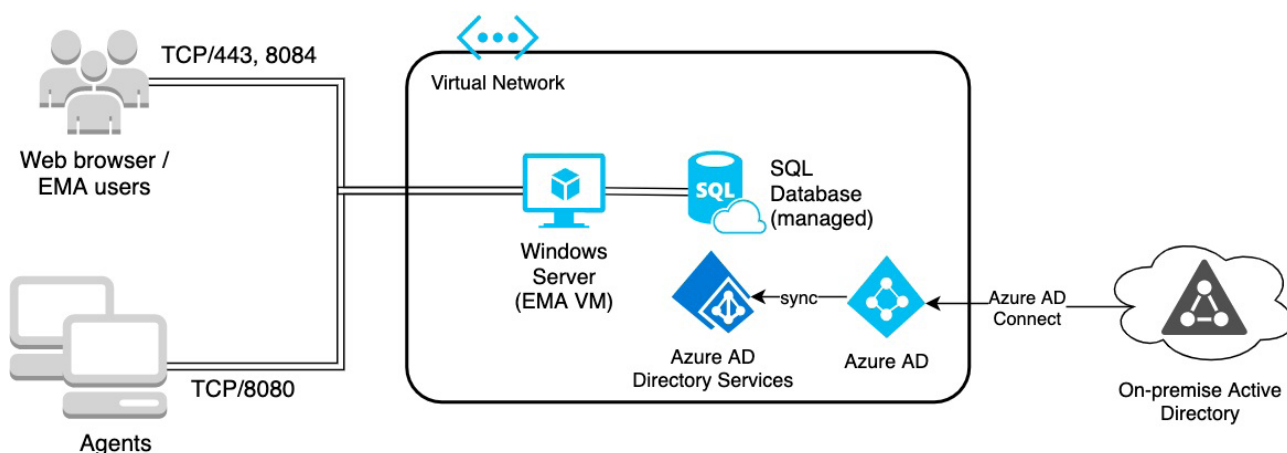
「[Azure* AD Domain Services のドキュメント](#)」

「[Azure* の Active Directory* ベースのサービスを比較する](#)」

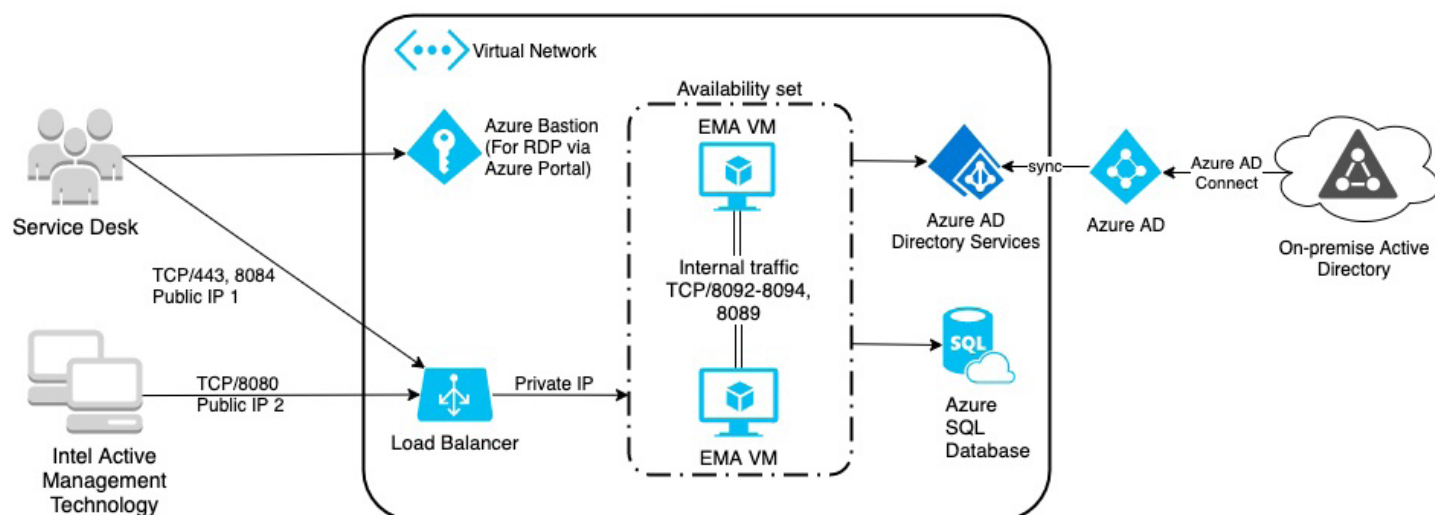
「[Azure* AD Connect 同期：同期を理解してカスタマイズする](#)」

11.1 Active Directory* 統合のアーキテクチャー概要図

11.1.1 シングル・サーバー・デプロイメント



11.1.2 分散サーバー・デプロイメント



11.2 Azure* AD Connect を使用した Active Directory* のクラウドへの拡張

- ❑ Azure* AD Directory Services (AADDs) リソースをデプロイして、仮想マシンを AD ドメインに参加させます。
 - ❑ このプロセスにおいて、AADDs 専用のサブネットを作成する必要があります。
 - ❑ Azure* Active Directory* から、このマネージドドメインの管理者権限を持つユーザーを追加します。
 - ❑ セットアップが完了するまでに 1 時間以上かかることがあります。セットアップが完了したら、AD DS サーバー IP アドレスを使用するように、仮想ネットワークの DNS サーバー設定を更新します。
- ❑ AD Connect をオンプレミス環境にデプロイし、ユーザーおよびパスワードハッシュを Azure* Active Directory* に同期します。
 - ❑ 組織のネットワーク上のドメインに参加済みのサーバーに、AD Connect ソフトウェアをダウンロードし、インストールします。
 - ❑ Express Settings (簡単設定) を使います。
 - ❑ Azure* AD と Azure* AD DS の資格情報を入力します。
 - ❑ ドメイン名が、あらかじめ Azure* AD に追加および検証されたカスタムドメインに一致することを確認します。
 - ❑ 設定が完了したら、30 分後にバックグラウンドが同期されます。動作の詳細な仕組みについては、Microsoft の資料を参照してください。
 - ❑ Azure* AD Connect のダウンロード場所 : [Microsoft* Azure* AD Connect を Microsoft* 公式ダウンロード・センターからダウンロード](#)
 - ❑ Azure* AD Connect の前提条件 : 「[Azure* AD Connect : 前提条件とハードウェア](#)」
- ❑ このインフラストラクチャーが完成した後、以下のリンクの指示に従って、ドメインに VM を参加させることができます。
「[Azure* Active Directory* Domain Services のマネージドドメインに Windows Server* 仮想マシンを参加させる](#)」