



# 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)

アマゾン ウェブ サービス \*(AWS\*) 向けデプロイメント・ガイド

---

インテル® バージョン 1.3.3

2020 年 10 月

## 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、明示的と默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ー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よらずにかかわらず）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、および非侵害性の默示の保証、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ー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 AWS* マネジメント・コンソールの画面構成.....	1
1.2.1 Services (サービス) .....	1
1.2.2 リソースグループ .....	2
1.2.3 リージョン .....	2
1.3 タグとリソースグループ .....	2
1.4 始める前に.....	2
2アーキテクチャ概要図 .....	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デプロイメント・リージョンの選択.....	4
4ネットワークのデプロイメント .....	5
4.1 概要.....	5
4.2 VPC の作成.....	5
4.2.1 VPC サービスへの移動.....	5
4.2.2 VPC の作成 .....	6
4.2.3 VPC の詳細の設定.....	6
4.3 サブネットの作成 .....	7
4.3.1 Subnets (サブネット) 画面への移動 .....	7
4.3.2 1つ目のプライベート・サブネットの作成 .....	7
4.3.3 2つ目のプライベート・サブネットの作成 .....	7
4.3.4 1つ目のパブリックサブネットの作成 .....	8
4.3.5 2つ目のパブリックサブネットの作成 .....	8
4.3.6 サブネットの確認 .....	8
4.4 パブリックサブネット用インターネット・ゲートウェイの作成 .....	9
4.4.1 インターネット・ゲートウェイの作成 .....	9
4.4.2 VPC へのインターネット・ゲートウェイのアタッチ .....	9
4.4.3 アタッチの詳細の入力 .....	10
4.5 プライベート・サブネットの NAT ゲートウェイの作成 .....	10
4.5.1 NAT ゲートウェイへの移動 .....	10
4.5.2 1つ目の NAT ゲートウェイの作成 .....	11
4.5.3 2つ目の NAT ゲートウェイの作成 .....	12
4.6 ルートテーブルの作成と設定 .....	12
4.6.1 ルートテーブルへの移動 .....	12
4.6.2 パブリックサブネット用ルートテーブルの作成 .....	13
4.6.3 1つ目のプライベート・サブネット用ルートテーブルの作成 .....	13
4.6.4 2つ目のプライベート・サブネット用ルートテーブルの作成 .....	13
4.6.5 ルートテーブルのリストの確認 .....	13
4.6.6 1つ目のプライベート・サブネット用ルートテーブルのルートの編集 .....	14
4.6.7 1つ目のプライベート・サブネット用ルートテーブルのサブネット関連付けを編集 .....	15
4.6.8 2つ目のプライベート・サブネット用ルートテーブルのルートの編集 .....	16
4.6.9 2つ目のプライベート・サブネット用ルートテーブルのサブネット関連付けを編集 .....	16
4.6.10 パブリックサブネット用ルートテーブルのルートの編集 .....	17
4.6.11 パブリックサブネット用ルートテーブルのサブネットの関連付けを編集 .....	17
4.7 セキュリティー・グループ .....	18
4.7.1 VM 用のセキュリティー・グループの作成 .....	18
4.7.2 セキュリティー・グループを更新し、インテル® EMA VM 間のトラフィックを許可 (分散サーバーのみ) .....	20
4.7.3 データベース用のセキュリティー・グループの作成 .....	21

<b>5 仮想マシンのデプロイメント .....</b>	<b>23</b>
5.1 概要.....	23
5.2 仮想マシンの作成.....	23
5.2.1 EC2* サービスへの移動.....	23
5.2.2 EC2* インスタンスの起動.....	23
5.2.3 Amazon マシンイメージ (AMI) の選択.....	24
5.2.4 マシンタイプの選択.....	24
5.2.5 インスタンスの詳細の設定.....	25
5.2.6 ストレージの追加.....	25
5.2.7 タグの追加.....	25
5.2.8 セキュリティー・グループの設定.....	26
5.2.9 インスタンスの起動の確認.....	26
5.2.10 EC2* キーペアの選択.....	26
5.3 2つ目の EC2* インスタンスの作成 (分散サーバーのみ) .....	26
<b>6 AWS* System Manager の設定 (分散サーバーのみ) .....</b>	<b>27</b>
6.1 Systems Manager サービスへの移動.....	27
6.2 Quick Setup (高速セットアップ) の開始 .....	27
6.3 Permissions (アクセス許可) オプションの選択 .....	28
6.4 Configurations (設定) オプションの選択 .....	28
6.5 Targets (ターゲット) の選択 .....	29
6.6 Managed Instances (マネージド・インスタンス) のリストの確認 .....	29
6.7 Session Manager による仮想マシンへのログイン .....	29
<b>7 Relational Database Service (RDS) のデプロイメント .....</b>	<b>30</b>
7.1 RDS サービスへの移動.....	30
7.2 データベース・サブネット・グループの作成.....	30
7.2.1 サブネットグループの詳細.....	31
7.3 データベースの作成 .....	31
7.3.1 データベース作成方法の選択.....	32
7.3.2 エンジンタイプとエディションの選択 .....	32
7.3.3 デプロイメント・テンプレートの選択 .....	32
7.3.4 インスタンス名とマスターユーザー資格情報の設定 .....	33
7.3.5 DB インスタンス・サイズの設定 .....	33
7.3.6 ストレージの設定 (オプション) .....	33
7.3.7 接続の設定 .....	34
7.3.8 接続の設定 - Additional Connectivity Configuration (追加の接続設定) .....	34
7.3.9 確認と作成 .....	35
7.4 データベースのホスト名の取得 .....	35
<b>8 ロードバランサーのデプロイメント (分散サーバーのみ) .....</b>	<b>36</b>
8.1 概要.....	36
8.2 ターゲットグループの作成 .....	36
8.2.1 ターゲットグループの作成 .....	36
8.2.2 TCP/443 用のターゲットグループの設定 .....	37
8.2.3 TCP/8084 用のターゲットの作成/設定 .....	38
8.2.4 TCP/8080 用のターゲットの設定 .....	38
8.2.5 ターゲットグループの確認 .....	39
8.2.6 TCP/443 ターゲットグループでのスティックィネスの有効化 .....	39
8.2.7 TCP/8084 ターゲットグループでのスティックィネスの有効化 .....	40
8.2.8 ターゲットグループのヘルス・モニタリングに関する注記 .....	40
8.3 ウェブ・トラフィック用のネットワーク・ロード・バランサーの作成 .....	40
8.3.1 ロードバランサーの作成 .....	40
8.3.2 ロードバランサーのタイプの選択 .....	40
8.3.3 ロードバランサーの設定 .....	41
8.3.4 ロードバランサー転送ルールの修正 .....	43

8.4 Swarm トラフィック用のネットワーク・ロード・バランサーの作成 .....	45
8.4.1 ロードバランサーの作成.....	45
8.4.2 ロードバランサーのタイプの選択.....	45
8.4.3 ロードバランサーの設定.....	45
8.4.4 ロードバランサーの DNS 名の記録.....	47
<b>9 付録 A - Active Directory* 統合に関する注記.....</b>	<b>49</b>
<b>10 Active Directory* 統合のアーキテクチャ図 .....</b>	<b>50</b>
10.1 シングル・サーバー・デプロイメント.....	50
10.2 分散サーバー・デプロイメント.....	50
10.3 AWS* AD Connector を使用した Active Directory* のクラウドへの拡張 .....	50

# 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、Amazon ウェブ サービス\* 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/所有して自分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。

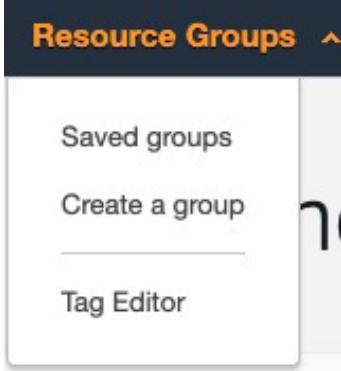
Amazon Relational Database Service\* などのようなフルマネージド型のサービスでは、クラウド・プロバイダーがサービス提供の基盤となるハードウェアやソフトウェアをすべて管理してくれるので、自社のデータに専念できます。クラウド上で仮想マシンを実行する場合、ユーザーが自分で管理する必要があるのはゲスト・オペレーティング・システムとそこにインストールされたソフトウェアのみです。あとはクラウド・プロバイダーが基盤ハードウェアを管理し、最高の信頼性と可用性を提供するために尽力してくれます。

## 1.2 AWS\* マネジメント・コンソールの画面構成

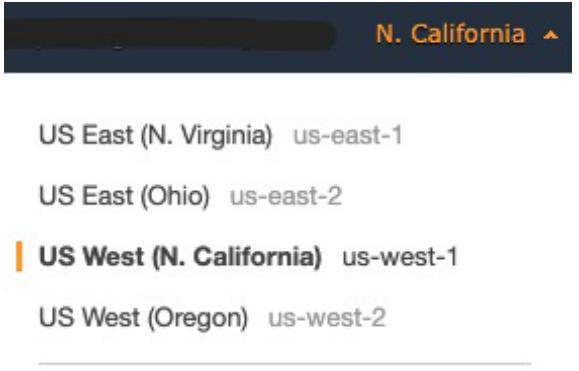
### 1.2.1 Services(サービス)

aws		Services ▾	Resource Groups ▾	AWS* マネジメント・コンソール <a href="https://aws.amazon.com/console/">https://aws.amazon.com/console/</a> にログインすると、画面の左上に Services (サービス) メニューが表示されます。
History	Console Home	Find a service by name or feature	Compute EC2 Lightsail ▾ Lambda Batch Elastic Beanstalk Serverless Application Repository AWS Outposts EC2 Image Builder	これをクリックすると、AWS* が提供するすべてのサービスのリストが、Compute (演算)、Storage (ストレージ)、Database (データベース) などのカテゴリー別に表示されます。  本ガイドでサービスをデプロイする際、この画面を開いて適切なサービスを選択するように指示があります。

## 1.2.2 リソースグループ

	<p>Services(サービス)の次は、Resource Groups(リソースグループ)メニューです。ここでは、リソースグループを作成したり、作成したリソースグループを確認できます。</p> <p>通常、デプロイしたユーザーと所属するプロジェクトを問わず、現在のリージョンにデプロイされたすべてのリソースが表示されます。そのため、リソースグループを使うことで、各リソースに付加したカスタムタグに基づいて絞り込まれたリソースリストを表示できます。</p>
--	--

## 1.2.3 リージョン

	<p>マネジメント・コンソールの右上にあるメニューで、リソースをデプロイするリージョンを選択する必要があります。</p> <p>選択したリージョンに関するリソースのみをリストで表示できます。</p>
---	---

各 AWS\* リージョンには、アベイラビリティー・ゾーン、略して AZ と呼ばれる複数の独立した場所があります。各アベイラビリティー・ゾーンは、他のアベイラビリティー・ゾーンの障害の影響を受けないように、分離して設計されています。

## 1.3 タグとリソースグループ

タグとは、AWS\* にデプロイ可能な多くの異なる種類のリソースにユーザーが割り当てることができる、カスタムのキーと値のペアです。お勧めの方法はリソース作成時にタグを付けることで、リソースの所有者、所属するプロジェクトの把握が容易になり、タグベースのリソースグループや、タグベースの請求レポートを使用できるようになります。

タグやリソースグループの作成については非常に多くのやり方が存在し手順が煩雑になるため、本ガイドでは扱いませんが、タグ付けとリソースのグループ化ストラテジーを導入する場合に、このような機能が存在することを覚えておいてください。

タグの使用の詳細については、以下のリンクを参照してください。

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

## 1.4 始める前に

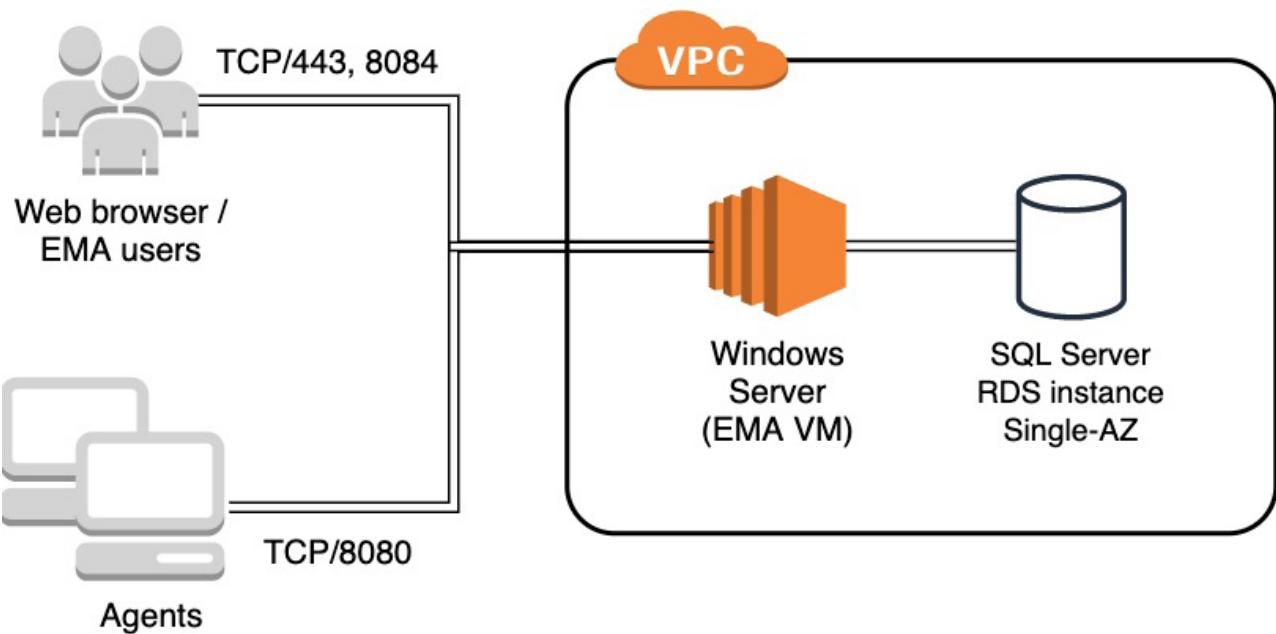
組織に既存の AWS\* アカウントがある場合、クラウド管理者に依頼して、本ガイドに記載されたすべてのリソースを作成するのに十分なアクセス権を付与してもらう必要があります。

組織に既存の AWS\* 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://aws.amazon.com/console/> にアクセスして **Create a Free Account (今すぐ無料サインアップ)** ボタンをクリックします。

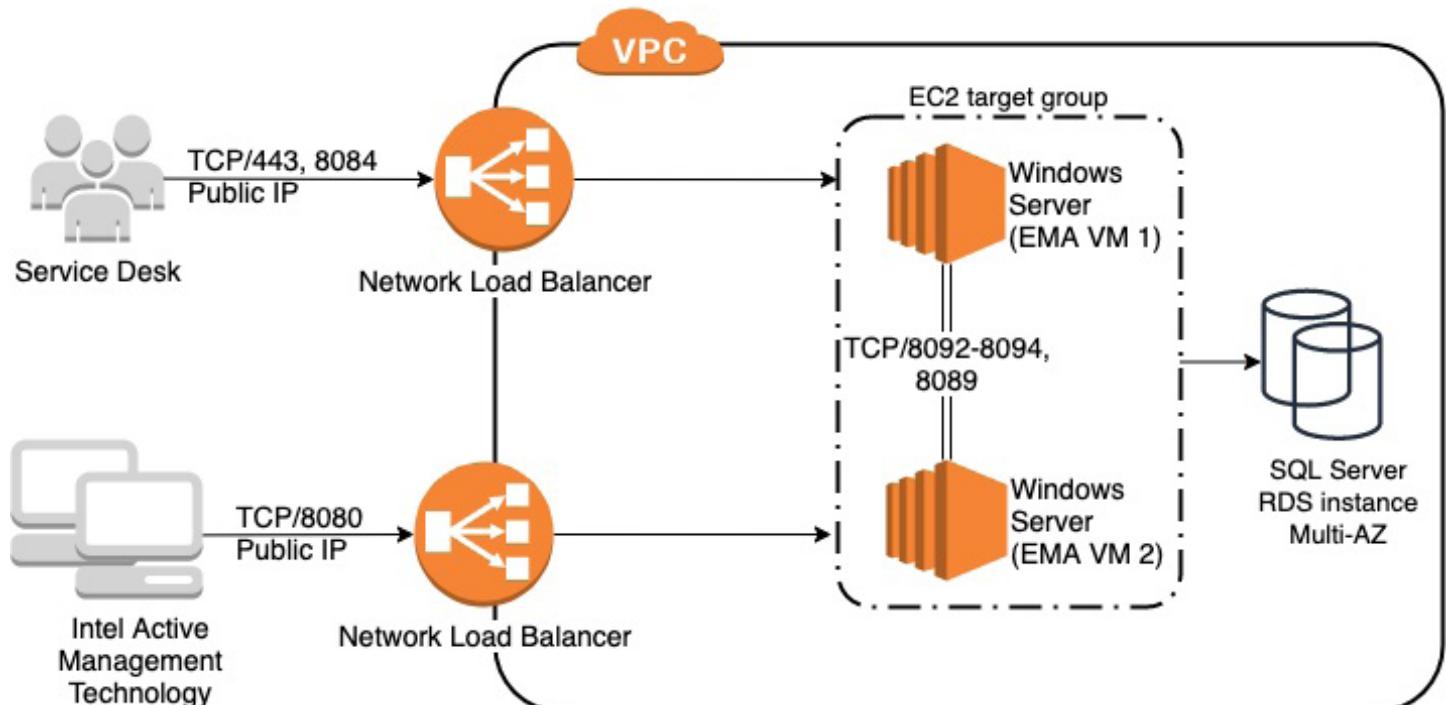
使用すべきアドレス空間があるか、ネットワーク管理者に確認します。クラウド・プロバイダーへの VPN がすでに確立している場合や将来的にその予定がある場合に、企業ネットワークとの重複を防ぎ、ルーティングの問題を防止できます。また、組織からクラウドにアクセスするトラフィックの送信元 IP アドレスについても確認が必要です。これにより、インターネットからの信頼できるネットワークのみをインテル® EMA の仮想マシンに許可することができます。

## 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 デプロイメント・リージョンの選択

右上のリージョンメニューから、リソースをデプロイするリージョンを選択します。



US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

**US West (N. California) us-west-1**

US West (Oregon) us-west-2

---

## 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 Private Cloud (VPC) は、AWS\* 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、AWS\* 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。VPC は他の VPC と論理的に分離されています。

VPC 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。AWS\* 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。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特定します。

VPC を作成した後、サブネットを作成します。サブネットを使用すると、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 VPC ネットワークをセグメント化できます。サブネットは、選択されたリージョン内の 2 つの別々のアベイラビリティー・ゾーン (AZ) で動作します。これにより、データベースとインテル® EMA アプリケーションの可用性が向上されます。そのリソースにパブリック IP アドレスによる直接のインターネット・アクセスが必要かどうかに応じて、パブリックサブネットとプライベート・サブネットの両方を作成します。

デフォルトでは、AWS\* ファイアウォールはリソースに対するインバウンド・アクセスを一切許可しません。そのため、ネットワークのデプロイメントの一環として、これらのリソースへのネットワーク通信を可能にするためにセキュリティー・グループの作成を行います。

仮想マシンの攻撃対象領域を小さくするため、VPC ファイアウォールを介した RDP は許可されません。その代わりに、AWS\* Session Manager(セッション・マネージャー)を使用して、VM のリモート管理を実現します。また、分散サーバー・デプロイメントでは、仮想マシンはパブリック IP アドレスを持ちません。

VPC 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.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html>

### 4.2 VPC の作成

パブリックサブネットが 1 つのみのシングル・サーバー・デプロイメントしか行わない場合は VPC ウィザードを使用できますが、分散サーバー・デプロイメントではウィザードでは不十分です。そのため、ここではすべてのネットワーク・コンポーネントを手動で作成して、必要な設定が明確に分かるようにします。

#### 4.2.1 VPC サービスへの移動

 Networking & Content Delivery  CloudFront	Services(サービス) メニューで、Network & Content Delivery(ネットワーキング & コンテンツ配信) の VPC を選択します。
---	---

## 4.2.2 VPC の作成

VPC のサイドバーから **Your VPCs (あなたの VPC)** を選択します。  
**Create VPC (VPC を作成)** ボタンをクリックします。

## 4.2.3 VPC の詳細の設定

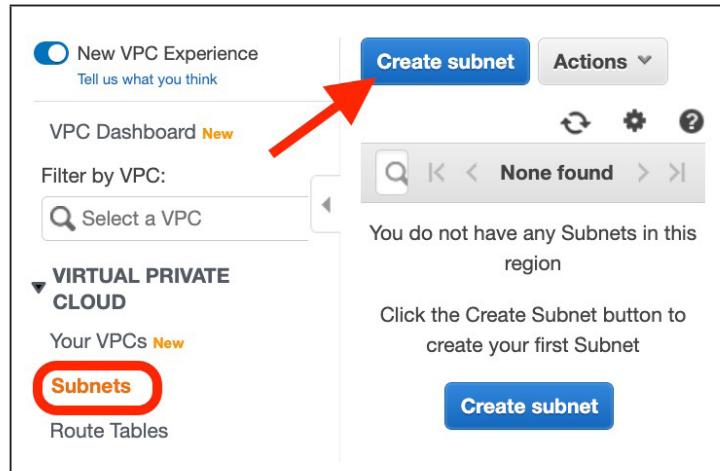
ネットワークの詳細情報を次のように入力します。

- Name Tag (Name タグ)**: 一意の VPC 名を入力します。  
例 : *intel-ema-network*
- IPv4 CIDR block (IPv4 CIDR ブロック)**: サブネットを含めるのに十分な大きさを持つ未使用のネットワークを選択します。  
例 : *10.250.0.0/24*

**Create VPC (VPC を作成)** ボタンをクリックします。

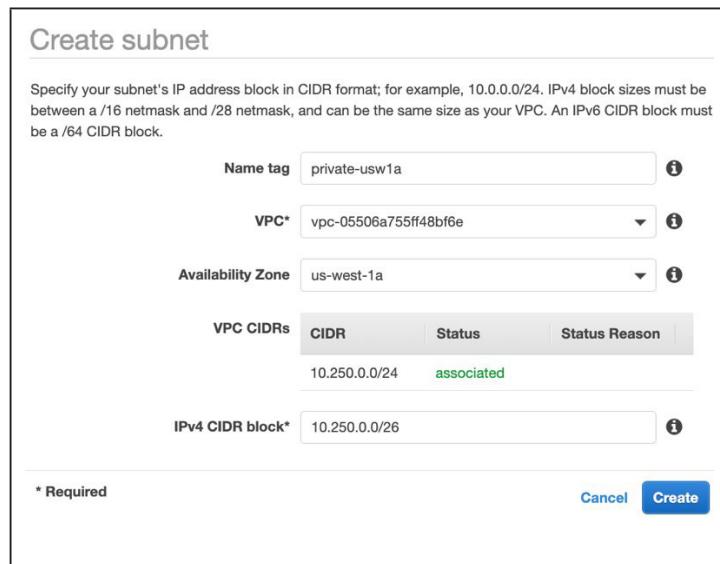
## 4.3 サブネットの作成

### 4.3.1 Subnets(サブネット)画面への移動



VPC のサイドバーから **Subnets(サブネット)** を選択します。

### 4.3.2 1つ目のプライベート・サブネットの作成

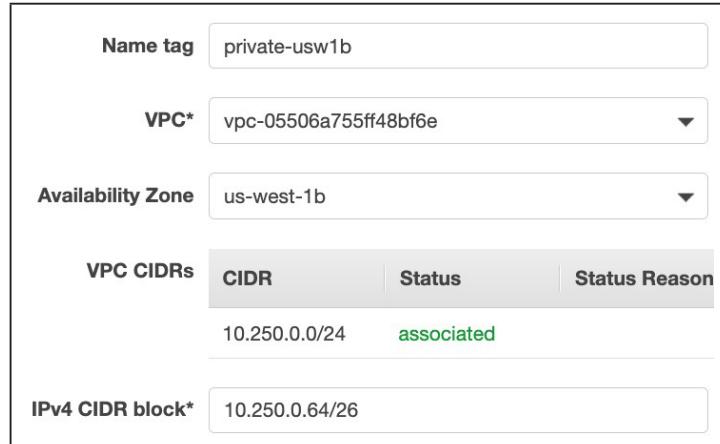


**Create subnet (サブネットを作成)** ボタンをクリックします。サブネットを以下のように設定します。

- Name tag (Name タグ)** : 一意のサブネット名を指定します。  
例 : *private-usw1a*
- VPC** : 先ほど作成した仮想ネットワークを選択します。
- Availability Zone (アベイラビリティー・ゾーン)** : 今回の設計では 2 つの個別のゾーンを使用するため、1 つ目に選択したゾーンをここで使用します。  
例 : *us-west-1a*
- IPv4 CIDR block (IPv4 CIDR ブロック)** : VPC アドレス空間内の未使用の IP ブロックを選択します。  
例 : *10.250.0.0/26*

**Create (作成)** ボタンをクリックします。

### 4.3.3 2つ目のプライベート・サブネットの作成



**Create subnet (サブネットを作成)** ボタンをクリックします。

サブネットを以下のように設定します。

- Name tag (Name タグ)** : 一意のサブネット名を指定します。  
例 : *private-usw1b*
- VPC** : 先ほど作成した仮想ネットワークを選択します。
- Availability Zone (アベイラビリティー・ゾーン)** : 今回の設計では 2 つの個別のゾーンを使用するため、2 つ目に選択したゾーンをここで使用します。  
例 : *us-west-1b*

	<ul style="list-style-type: none"> <li><b>IPv4 CIDR block (IPv4 CIDR ブロック)</b>: VPC アドレス空間内の未使用的 IP ブロックを選択します。 例 : 10.250.0.64/26</li> </ul> <p>Create (作成) ボタンをクリックします。</p>
--	---

#### 4.3.4 1つ目のパブリックサブネットの作成

<p>Name tag <input type="text" value="public-usw1a"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1a"/></p> <table border="1"> <thead> <tr> <th>VPC CIDRs</th><th>CIDR</th><th>Status</th><th>Sta</th></tr> </thead> <tbody> <tr> <td></td><td>10.250.0.0/24</td><td>associated</td><td></td></tr> </tbody> </table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.128/26"/></p>	VPC CIDRs	CIDR	Status	Sta		10.250.0.0/24	associated		<p>Create subnet (サブネットを作成) ボタンをクリックします。</p> <p>サブネットを以下のように設定します。</p> <ul style="list-style-type: none"> <li><b>Name tag (Name タグ)</b>: 一意のサブネット名を指定します。 例 : <i>public-usw1a</i></li> <li><b>VPC</b>: 先ほど作成した仮想ネットワークを選択します。</li> <li><b>Availability Zone (アベイラビリティー・ゾーン)</b>: 今回の設計では 2 つの個別のゾーンを使用するため、1 つ目に選択したゾーンをここで使用します。 例 : <i>us-west-1a</i></li> <li><b>IPv4 CIDR block (IPv4 CIDR ブロック)</b>: VPC アドレス空間内の未使用的 IP ブロックを選択します。 例 : 10.250.0.128/26</li> </ul> <p>Create (作成) ボタンをクリックします。</p>
VPC CIDRs	CIDR	Status	Sta						
	10.250.0.0/24	associated							

#### 4.3.5 2つ目のパブリックサブネットの作成

<p>Name tag <input type="text" value="public-usw1b"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1b"/></p> <table border="1"> <thead> <tr> <th>VPC CIDRs</th><th>CIDR</th><th>Status</th><th>Sta</th></tr> </thead> <tbody> <tr> <td></td><td>10.250.0.0/24</td><td>associated</td><td></td></tr> </tbody> </table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.192/26"/></p>	VPC CIDRs	CIDR	Status	Sta		10.250.0.0/24	associated		<p>Create subnet (サブネットを作成) ボタンをクリックします。</p> <p>サブネットを以下のように設定します。</p> <ul style="list-style-type: none"> <li><b>Name tag (Name タグ)</b>: 一意のサブネット名を指定します。 例 : <i>private-usw1b</i></li> <li><b>VPC</b>: 先ほど作成した仮想ネットワークを選択します。</li> <li><b>Availability Zone (アベイラビリティー・ゾーン)</b>: 今回の設計では 2 つの個別のゾーンを使用するため、2 つ目に選択したゾーンをここで使用します。 例 : <i>us-west-1b</i></li> <li><b>IPv4 CIDR block (IPv4 CIDR ブロック)</b>: VPC アドレス空間内の未使用的 IP ブロックを選択します。 例 : 10.250.0.192/26</li> </ul> <p>Create (作成) ボタンをクリックします。</p>
VPC CIDRs	CIDR	Status	Sta						
	10.250.0.0/24	associated							

#### 4.3.6 サブネットの確認

	Name	Subnet ID	State	VPC	IPv4 CIDR	
<input type="checkbox"/>	private-usw1a	subnet-0850a...	available	vpc-0550...	10.250.0.0/26	
<input type="checkbox"/>	private-usw1b	subnet-016e1...	available	vpc-0550...	10.250.0.64/26	
<input type="checkbox"/>	public-usw1a	subnet-07aff7...	available	vpc-0550...	10.250.0.128/...	
<input type="checkbox"/>	public-usw1b	subnet-0110cd...	available	vpc-0550...	10.250.0.192/...	

## 4.4 パブリックサブネット用インターネット・ゲートウェイの作成

パブリックサブネットからインターネットにトラフィックをルーティングするため、インターネット・ゲートウェイをデプロイして VPC にアタッチする必要があります。ルーティングの設定は後のセクションで行います。

### 4.4.1 インターネット・ゲートウェイの作成

The screenshot shows the AWS VPC console. On the left sidebar, 'Internet Gateways' is selected. In the main area, the 'Internet gateways' section is displayed with a 'Create internet gateway' button highlighted by a red arrow. Below this, the 'Internet gateway settings' section shows a 'Name tag' input field containing 'public-igw'. A red box highlights the 'public-igw' text.

VPC のサイドバーから **Internet Gateways (インターネット・ゲートウェイ)** を選択します。

**Create Internet gateway (インターネット・ゲートウェイの作成)** をクリックします。

Name タグを入力します。例 : *public-igw*

画面下部にある **Create Internet gateway (インターネット・ゲートウェイの作成)** ボタンをクリックして完了します。

### 4.4.2 VPC へのインターネット・ゲートウェイのアタッチ

The screenshot shows the details of the created internet gateway 'igw-093a4663d228920c6 / public-igw'. A green box highlights the message: 'The following internet gateway was created: igw-093a4663d228920c6 . You can now attach to a VPC to enable the VPC to communicate with the internet.' Below this, the 'Attach to a VPC' button is highlighted by a red arrow. At the bottom, there is an 'Actions' menu.

The following internet gateway was created: igw-093a4663d228920c6 . You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

igw-093a4663d228920c6 / public-igw

Actions ▾

インターネット・ゲートウェイが作成されると、VPC にアタッチすることを促すプロンプトが表示されます。表示されたボタンをクリックします。Actions (アクション) メニューからも同じ操作が可能です。

#### 4.4.3 アタッチの詳細の入力

先ほど作成した VPC を選択します。

Attach internet gateway (インターネット・ゲートウェイのアタッチ) ボタンをクリックします。

#### 4.5 プライベート・サブネットの NAT ゲートウェイの作成

NAT ゲートウェイは、リソースがアウトバウンド・インターネット・トラフィックの送信ポイントとしてゾーン内で使用できるゾーンリソースです。NAT ゲートウェイはアドレス変換を実行し、トラフィックを VPC 内のインターネット・ゲートウェイに転送します。ここでは、1 つがダウンしても接続が保たれるよう、2 つのアベイラビリティー・ゾーンに対して 1 つずつ作成します。

##### 4.5.1 NAT ゲートウェイへの移動

VPC のサイドバーから **NAT Gateways (NAT ゲートウェイ)** を選択します。

## 4.5.2 1つ目のNAT ゲートウェイの作成

<p><b>Create NAT gateway</b> <small>Info</small></p> <p>Create a NAT gateway and assign it an Elastic IP address.</p> <p><b>NAT gateway settings</b></p> <p><b>Name - optional</b> Create a tag with a key of 'Name' and a value that you specify. <input type="text" value="usw1a-nat-gw"/> The name can be up to 256 characters long.</p> <p><b>Subnet</b> Select a public subnet in which to create the NAT gateway. <input type="text" value="subnet-07aff7a001005ed34 (public-usw1a)"/></p> <p><b>Elastic IP allocation ID</b> <small>Info</small> Assign an Elastic IP address to the NAT gateway. <input type="text" value="eipalloc-02b8404d9e9a34121"/></p> <p><b>Allocate Elastic IP</b></p>	<p><b>Create NAT gateway (NAT ゲートウェイの作成)</b> ボタンをクリックします。</p> <p>NAT ゲートウェイを以下のように設定します。</p> <ul style="list-style-type: none"><li>• <b>Name (オプション)</b> : 一意のゲートウェイ名を入力します。 例 : <i>usw1a-nat-gw</i></li><li>• <b>Subnet (サブネット)</b> : 1つ目のパブリックサブネットを選択します。 例 : <i>public-usw1a</i></li><li>• <b>Elastic IP allocation ID (Elastic IP 割り当て ID)</b> : Allocate Elastic IP (Elastic IP を割り当て) ボタンをクリックすると、このフィールドに値が自動で表示されます。</li></ul> <p><b>Create NAT gateway (NAT ゲートウェイの作成)</b> ボタンをクリックして完了します。</p>
--	---

#### 4.5.3 2つ目のNAT ゲートウェイの作成

### Create NAT gateway Info

Create a NAT gateway and assign it an Elastic IP address.

#### NAT gateway settings

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.  
  
The name can be up to 256 characters long.

**Subnet**  
Select a public subnet in which to create the NAT gateway.

**Elastic IP allocation ID Info**  
Assign an Elastic IP address to the NAT gateway.

**Allocate Elastic IP**

**Create NAT gateway (NAT ゲートウェイの作成)** ボタンをクリックします。

NAT ゲートウェイを以下のように設定します。

- **Name (オプション)** : 一意のゲートウェイ名を入力します。  
例 : usw1b-nat-gw
- **Subnet (サブネット)** : 2つ目のパブリックサブネットを選択します。  
例 : public-usw1b
- **Elastic IP allocation ID (Elastic IP 割り当て ID)** : Allocate Elastic IP (Elastic IP を割り当てる) ボタンをクリックすると、このフィールドに値が自動で表示されます。

**Create NAT gateway (NAT ゲートウェイの作成)** ボタンをクリックして完了します。

## 4.6 ルートテーブルの作成と設定

ルートテーブルとは、ネットワーク・トライフィックの宛先を決定するために使用される、「ルート」と呼ばれる規則の集まりです。VPC には、ルートテーブルと明示的に関連付けされていない任意のサブネットで使用されるデフォルトのルートテーブルが最初から含まれています。ここではそれを無視し、新しいルートテーブルを 3 つ作成します。うち 1 つはパブリックサブネットに関連付け、2 つはプライベート・サブネットに関連付けます。NAT ゲートウェイとインターネット・ゲートウェイにデフォルトのルートを追加します。

### 4.6.1 ルートテーブルへの移動

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with 'New VPC Experience' and a 'Route Tables' button highlighted with a red oval. The main area has a 'Create route table' button at the top, which is also highlighted with a red arrow. Below it is a search bar and a table listing route tables, with one entry 'rtb-01705' visible.

## 4.6.2 パブリックサブネット用ルートテーブルの作成

<b>Create route table</b>	<p>Create route table (ルートテーブルを作成) ボタンをクリックします。</p> <p>ルートテーブルを以下のように設定します。</p> <ul style="list-style-type: none"><li>• <b>Name tag (Name タグ)</b> : 一意のルートテーブル名を入力します。 例 : <i>public-usw-routes</i></li><li>• <b>VPC</b> : 先ほど作成した仮想ネットワークを選択します。</li></ul> <p><b>Create (作成)</b> ボタンをクリックします。</p> <p><b>Close (閉じる)</b> ボタンをクリックします。</p>
---------------------------	---

## 4.6.3 1つ目のプライベート・サブネット用ルートテーブルの作成

<b>Name tag</b> <input type="text" value="private-usw1a-routes"/>	<p>Create route table (ルートテーブルを作成) ボタンをクリックします。</p> <p>ルートテーブルを以下のように設定します。</p> <ul style="list-style-type: none"><li>• <b>Name tag (Name タグ)</b> : 一意のルートテーブル名を入力します。 例 : <i>private-usw1a-routes</i></li><li>• <b>VPC</b> : 先ほど作成した仮想ネットワークを選択します。</li></ul> <p><b>Create (作成)</b> ボタンをクリックします。</p> <p><b>Close (閉じる)</b> ボタンをクリックします。</p>
---	--

## 4.6.4 2つ目のプライベート・サブネット用ルートテーブルの作成

<b>Name tag</b> <input type="text" value="private-usw1b-routes"/>	<p>Create route table (ルートテーブルを作成) ボタンをクリックします。</p> <p>ルートテーブルを以下のように設定します。</p> <ul style="list-style-type: none"><li>• <b>Name tag (Name タグ)</b> : 一意のルートテーブル名を入力します。 例 : <i>private-usw1b-routes</i></li><li>• <b>VPC</b> : 先ほど作成した仮想ネットワークを選択します。</li></ul> <p><b>Create (作成)</b> ボタンをクリックします。</p> <p><b>Close (閉じる)</b> ボタンをクリックします。</p>
---	--

## 4.6.5 ルートテーブルのリストの確認

<input type="checkbox"/>	Name	Route Table ID	
<input type="checkbox"/>		rtb-01705bd4b29e283ee	
<input checked="" type="checkbox"/>	private-usw1a-routes	rtb-034336669e17ced15	ルートテーブルのリストに、先ほど選択した Name タグを持つ新しいエントリーが 3 つあることを確認します。
<input type="checkbox"/>	private-usw1b-routes	rtb-02a96e86856fc5cc0	
<input type="checkbox"/>	public-usw-routes	rtb-055fb6f346f460d0a	

#### 4.6.6 1つ目のプライベート・サブネット用ルートテーブルのルートの編集

Name	Route Table ID	操作
private-usw1a-routes	rtb-034336669e17ced15	1つ目のプライベート・サブネット用ルートテーブルを選択します。 例 : private-usw1a-routes リストの下にある <b>Routes (ルート)</b> タブを選択します。 <b>Edit routes (ルートを編集)</b> ボタンをクリックします。 <b>Add route (ルートを追加)</b> ボタンをクリックして、以下の値を設定します。 <ul style="list-style-type: none"><li>• <b>Destination (送信先)</b> : 0.0.0.0/0</li><li>• <b>Target (ターゲット)</b> : 1つ目のアベイラビリティー・ゾーンにデプロイした NAT ゲートウェイを選択します。 例 : usw1a-nat-gw</li></ul> <b>Save routes (ルートを保存)</b> ボタンをクリックします。 <b>Close (閉じる)</b> ボタンをクリックします。
private-usw1b-routes	rtb-02a96e86856fc5cc0	
public-usw-routes	rtb-055fb6f346f460d0a	

Route Table: rtb-034336669e17ced15

Summary Routes Subnet Associations

Edit routes

View All routes

Destination	Target
10.250.0.0/24	local

Edit routes

Destination	Target	Status
10.250.0.0/24	local	active
0.0.0.0/0	nat-002ed77f6a9ef0841	

Add route

\* Required Cancel Save routes

#### 4.6.7 1つ目のプライベート・サブネット用ルートテーブルのサブネット関連付けを編集

Route Table: rtb-034336669e17ced15

Summary    Routes    **Subnet Associations**

**Edit subnet associations**

None found

Subnet ID	IPv4 CIDR
You do not have any subnet associations.	

Edit subnet associations

Route table rtb-034336669e17ced15

Associated subnets **subnet-0850a0c96d7a404da**

Subnet ID	IPv4 CIDR
subnet-0850a0c96d7a404da   <b>private-usw1a</b>	10.250.0.0/26
subnet-016e150f99130ef50   private-usw1b	10.250.0.64/26
subnet-0110cd4da4ec72e62   public-usw1b	10.250.0.192/26
subnet-07aff7a001005ed34   public-usw1a	10.250.0.128/26

\* Required

Cancel **Save**

**Subnet Associations (サブネット関連付け) タブ**を選択します。

**Edit subnet associations (サブネットの関連付けを編集)**ボタンをクリックします。

このルートテーブルと関連付ける1つ目のプライベート・サブネットを選択します。このガイドの名前をそのまま使用した場合、ルートテーブル名とサブネットの対応が簡単に分かります。

**Save (保存)**ボタンをクリックします。

#### 4.6.8 2つ目のプライベート・サブネット用ルートテーブルのルートの編集

<p>Summary      <b>Routes</b>      Subnet Associations</p> <p><b>Edit routes</b></p> <p>View      All routes</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Destination</th> <th style="text-align: left;">Target</th> <th style="text-align: left;">Status</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>local</td> <td>active</td> </tr> <tr> <td colspan="3"> <b>Edit routes</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Destination</th> <th style="text-align: left;">Target</th> <th style="text-align: left;">Status</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>local</td> <td>active</td> </tr> <tr> <td>0.0.0.0/0</td> <td>nat-06c46b8e4e4ed5c32</td> <td>active</td> </tr> <tr> <td colspan="3"> <input type="button" value="Add route"/> </td> </tr> <tr> <td colspan="3"> <small>* Required</small> </td> </tr> <tr> <td colspan="2"> <small>Cancel</small> </td> <td> <input type="button" value="Save routes"/> </td> </tr> </tbody> </table> </td> </tr> </tbody> </table>	Destination	Target	Status	10.250.0.0/24	local	active	<b>Edit routes</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Destination</th> <th style="text-align: left;">Target</th> <th style="text-align: left;">Status</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>local</td> <td>active</td> </tr> <tr> <td>0.0.0.0/0</td> <td>nat-06c46b8e4e4ed5c32</td> <td>active</td> </tr> <tr> <td colspan="3"> <input type="button" value="Add route"/> </td> </tr> <tr> <td colspan="3"> <small>* Required</small> </td> </tr> <tr> <td colspan="2"> <small>Cancel</small> </td> <td> <input type="button" value="Save routes"/> </td> </tr> </tbody> </table>			Destination	Target	Status	10.250.0.0/24	local	active	0.0.0.0/0	nat-06c46b8e4e4ed5c32	active	<input type="button" value="Add route"/>			<small>* Required</small>			<small>Cancel</small>		<input type="button" value="Save routes"/>	<p>2つ目のプライベート・サブネット用ルートテーブルを選択します。 例 : <i>private-usw1b-routes</i></p> <p>リストの下にある <b>Routes (ルート)</b> タブを選択します。</p> <p><b>Edit routes (ルートを編集)</b> ボタンをクリックします。</p> <p><b>Add route (ルートを追加)</b> ボタンをクリックして、以下の値を設定します。</p> <ul style="list-style-type: none"> <li>• <b>Destination (送信先)</b> : <i>0.0.0.0/0</i></li> <li>• <b>Target (ターゲット)</b> : 2つ目のアベイラビリティー・ゾーンにデプロイした NAT ゲートウェイを選択します。 例 : <i>usw1b-nat-gw</i></li> </ul> <p><b>Save routes (ルートを保存)</b> ボタンをクリックします。</p> <p><b>Close (閉じる)</b> ボタンをクリックします。</p>
Destination	Target	Status																										
10.250.0.0/24	local	active																										
<b>Edit routes</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Destination</th> <th style="text-align: left;">Target</th> <th style="text-align: left;">Status</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>local</td> <td>active</td> </tr> <tr> <td>0.0.0.0/0</td> <td>nat-06c46b8e4e4ed5c32</td> <td>active</td> </tr> <tr> <td colspan="3"> <input type="button" value="Add route"/> </td> </tr> <tr> <td colspan="3"> <small>* Required</small> </td> </tr> <tr> <td colspan="2"> <small>Cancel</small> </td> <td> <input type="button" value="Save routes"/> </td> </tr> </tbody> </table>			Destination	Target	Status	10.250.0.0/24	local	active	0.0.0.0/0	nat-06c46b8e4e4ed5c32	active	<input type="button" value="Add route"/>			<small>* Required</small>			<small>Cancel</small>		<input type="button" value="Save routes"/>								
Destination	Target	Status																										
10.250.0.0/24	local	active																										
0.0.0.0/0	nat-06c46b8e4e4ed5c32	active																										
<input type="button" value="Add route"/>																												
<small>* Required</small>																												
<small>Cancel</small>		<input type="button" value="Save routes"/>																										

#### 4.6.9 2つ目のプライベート・サブネット用ルートテーブルのサブネット関連付けを編集

<p>Summary      Routes      <b>Subnet Associations</b></p> <p><b>Edit subnet associations</b></p> <p>K    None found</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Subnet ID</th> <th style="text-align: left;">IPv4 CIDR</th> </tr> </thead> <tbody> <tr> <td colspan="2">You do not have any subnet associations.</td> </tr> </tbody> </table> <p><b>Edit subnet associations</b></p> <p>Route table rtb-02a96e86856fc5cc0 <b>private-usw1b-routes</b></p> <p>Associated subnets <b>subnet-016e150f99130ef50</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3"> <input type="text"/> Filter by attributes or search by keyword         </th> </tr> <tr> <th style="text-align: left;">Subnet ID</th> <th style="text-align: left;">IPv4 CIDR</th> <th style="text-align: left;"></th> </tr> </thead> <tbody> <tr> <td>subnet-0850a0c96d7a404da</td> <td>10.250.0.0/26</td> <td></td> </tr> <tr> <td><b>subnet-016e150f99130ef50   private-usw1b</b></td> <td><b>10.250.0.64/26</b></td> <td></td> </tr> <tr> <td>subnet-0110cd4da4ec72e62</td> <td>10.250.0.192/...</td> <td></td> </tr> <tr> <td>subnet-07aff7a001005ed34</td> <td>10.250.0.128/...</td> <td></td> </tr> </tbody> </table>	Subnet ID	IPv4 CIDR	You do not have any subnet associations.		<input type="text"/> Filter by attributes or search by keyword			Subnet ID	IPv4 CIDR		subnet-0850a0c96d7a404da	10.250.0.0/26		<b>subnet-016e150f99130ef50   private-usw1b</b>	<b>10.250.0.64/26</b>		subnet-0110cd4da4ec72e62	10.250.0.192/...		subnet-07aff7a001005ed34	10.250.0.128/...		<p><b>Subnet Associations (サブネット関連付け)</b> タブを選択します。</p> <p><b>Edit subnet associations (サブネットの関連付けを編集)</b> ボタンをクリックします。</p> <p>このルートテーブルと関連付ける 2つ目のプライベート・サブネットを選択します。このガイドの名前をそのまま使用した場合、ルートテーブル名とサブネットの対応が簡単に分かります。</p> <p><b>Save (保存)</b> ボタンをクリックします。</p>
Subnet ID	IPv4 CIDR																						
You do not have any subnet associations.																							
<input type="text"/> Filter by attributes or search by keyword																							
Subnet ID	IPv4 CIDR																						
subnet-0850a0c96d7a404da	10.250.0.0/26																						
<b>subnet-016e150f99130ef50   private-usw1b</b>	<b>10.250.0.64/26</b>																						
subnet-0110cd4da4ec72e62	10.250.0.192/...																						
subnet-07aff7a001005ed34	10.250.0.128/...																						

#### 4.6.10 パブリックサブネット用ルートテーブルのルートの編集

Summary    **Routes**    Subnet Associations

**Edit routes** Save routes

View All routes

Destination	Target
10.250.0.0/24	local

Destination Target Status

10.250.0.0/24 local active

Add route

\* Required    Cancel    Save routes

パブリックサブネット用ルートテーブルを選択します。  
例 : `public-usw-routes`

リストの下にある **Routes (ルート)** タブを選択します。

**Edit routes (ルートを編集)** ボタンをクリックします。

**Add route (ルートを追加)** ボタンをクリックして、以下の値を設定します。

- **Destination (送信先)** : `0.0.0.0/0`
- **Target (ターゲット)** : 先ほどデプロイしたインターネット・ゲートウェイを選択します。  
例 : `public-igw`

**Save routes (ルートを保存)** ボタンをクリックします。

**Close (閉じる)** ボタンをクリックします。

#### 4.6.11 パブリックサブネット用ルートテーブルのサブネットの関連付けを編集

Summary    Routes    **Subnet Associations**

**Edit subnet associations** Save

None found

Subnet ID	IPv4 CIDR
You do not have any subnet associations.	

Route table rtb-055fb6f346f460d0a (public-usw-routes)

Associated subnets `subnet-07aff7a001005ed34` `subnet-0110cd4da4ec72e62`

Subnet ID	IPv4 CIDR
<input type="checkbox"/> <code>subnet-0850a0c96d7a404da</code>   private-usw1a	<code>10.250.0.0/26</code>
<input type="checkbox"/> <code>subnet-016e150f99130ef50</code>   private-usw1b	<code>10.250.0.64/26</code>
<input checked="" type="checkbox"/> <code>subnet-0110cd4da4ec72e62</code>   public-usw1b	<code>10.250.0.192/...</code>
<input checked="" type="checkbox"/> <code>subnet-07aff7a001005ed34</code>   public-usw1a	<code>10.250.0.128/...</code>

Subnet Associations (サブネット関連付け) タブを選択します。

**Edit subnet associations (サブネットの関連付けを編集)** ボタンをクリックします。

このルートテーブルと関連付ける、両方のパブリックサブネットを選択します。

**Save (保存)** ボタンをクリックします。

## 4.7 セキュリティー・グループ

セキュリティー・グループは、仮想マシン・インスタンスに対する仮想ファイアウォールとして機能し、インバウンド・トラフィックとアウトバウンド・トラフィックをコントロールします。後で VM を作成するときに、1つまたは複数のセキュリティー・グループを VM に割り当てられます。セキュリティー・グループのルールはいつでも変更できます。変更後の新ルールは、そのセキュリティー・グループに関連付けられたすべてのインスタンスに自動的に適用されます。

セキュリティー・グループのルールを作成するとき、送信元と送信先を指定します。これらは IP ネットワークのリストか、セキュリティー・グループ ID として表現できます。セキュリティー・グループを送信元または送信先として指定した場合、ルールはそのセキュリティー・グループに関連付けられたすべてのインスタンスに影響します。この機能は分散サーバー・デプロイメントにおいて、プライベート・ネットワーク内のあらゆるトラフィックを広く許可しそうなく、インテル® EMA VM 間のトラフィックを許可するために使用されます。これは最小権限の原則のセキュリティー・ベスト・プラクティスに基づきます。

以下の手順では、インテル® EMA VM へのアクセスを制御するセキュリティー・グループを作成します。また、データベースへのアクセスを制御する別のグループも作成します。

VPC のセキュリティー・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.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

### 4.7.1 VM 用のセキュリティー・グループの作成

注記：以下の例の図の一部の送信元アドレスは加工されています。これらは各自のネットワーク環境に対して固有の設定であるため、そのままコピーしてはなりません。独自の信頼できるネットワークを使用してください。

#### 4.7.1.1 セキュリティー・グループの作成

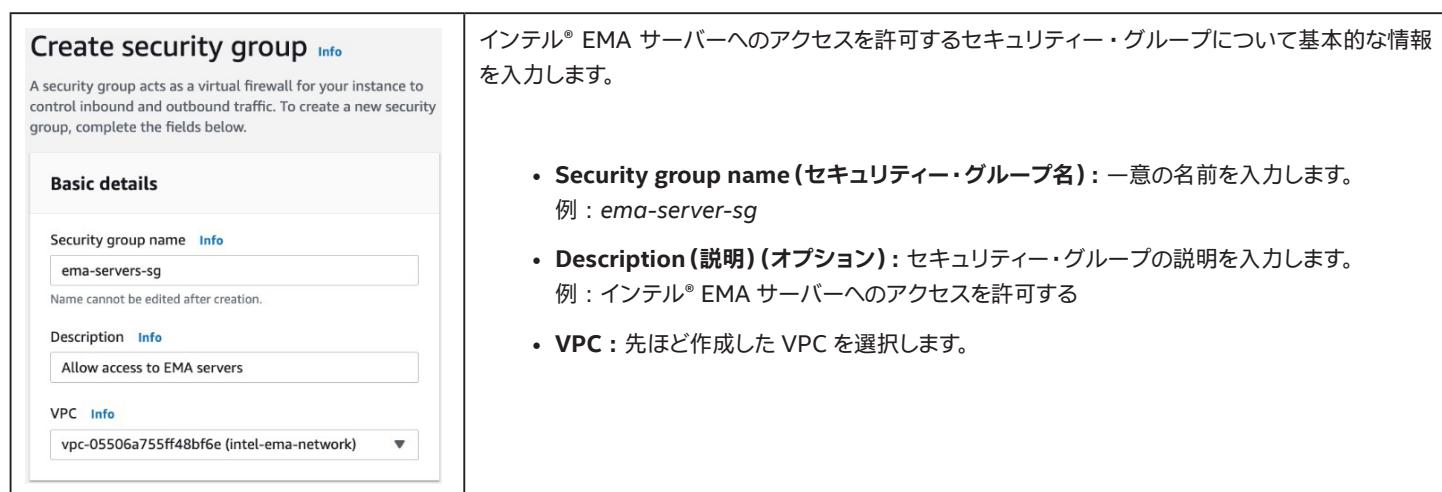


The screenshot shows the AWS VPC console. On the left sidebar, under the 'SECURITY' section, 'Security Groups' is selected. In the main content area, the 'Security Groups' page is displayed with the title 'Security Groups'. Below the title, there is a 'Create security group' button. The right side of the page contains descriptive text about creating a security group.

**VPC セクションのサイドバーから Security Groups (セキュリティー・グループ) を選択します。**

**Create security group (セキュリティー・グループを作成) ボタンをクリックします。**

#### 4.7.1.2 セキュリティー・グループの基本情報の設定



The screenshot shows the 'Create security group' configuration page. It includes sections for 'Basic details' (Security group name: ema-servers-sg, Description: Allow access to EMA servers), 'VPC' (VPC: vpc-05506a755ff48bf6e (intel-ema-network)), and a note about the security group acting as a virtual firewall. To the right, there is a list of configuration steps.

インテル® EMA サーバーへのアクセスを許可するセキュリティー・グループについて基本的な情報を入力します。

- Security group name (セキュリティー・グループ名)**: 一意の名前を入力します。  
例 : ema-server-sg
- Description (説明) (オプション)**: セキュリティー・グループの説明を入力します。  
例 : インテル® EMA サーバーへのアクセスを許可する
- VPC**: 先ほど作成した VPC を選択します。

#### 4.7.1.3 ウェブ・トラフィック用のインバウンド・ルールの追加

Inbound rules [Info](#)

Inbound rule 1

Type [Info](#) Protocol [Info](#) Port range [Info](#)

HTTPS [▼](#) TCP 443

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Custom [▼](#)  trusted networks for web

10.250.0.0/24 [X](#)  
 [X](#)

Add rule

以下の設定を持つインバウンド・ルールを追加します。

- Type (タイプ) : HTTPS**
- Description (説明) :** ウェブ用の信頼できるネットワーク
- Source (送信元) :** ヘルスチェックを許可する VPC CIDR ブロックを入力します。  
例 : 10.250.0.0/24  
インテル® EMA web UIへのアクセスが許可される追加のネットワークを入力することもできます(サービスデスクからのトラフィックの送信元であるパブリック・ネットワークなど)。

#### 4.7.1.4 WebSocket トラフィック用のインバウンド・ルールの追加

Inbound rule 2

Type [Info](#) Protocol [Info](#) Port range [Info](#)

Custom TCP [▼](#) TCP 8084

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Custom [▼](#)  trusted networks for websocket

10.250.0.0/24 [X](#)  
 [X](#)

Add rule

以下の設定を持つインバウンド・ルールを追加します。

- Type (タイプ) : Custom TCP (カスタム TCP)**
- Port range (ポート範囲) : 8084**
- Description (説明) :** WebSocket 用の信頼できるネットワーク
- Source (送信元) :** ヘルスチェックを許可する VPC CIDR ブロックを入力します。  
例 : 10.250.0.0/24  
インテル® EMA web UIへのアクセスが許可される追加のネットワークを入力することもできます(サービスデスクからのトラフィックの送信元であるパブリック・ネットワークなど)。

#### 4.7.1.5 Swarm トラフィック用のインバウンド・ルールの追加

Type [Info](#) Protocol [Info](#) Port range [Info](#)

Custom TCP [▼](#) TCP 8080

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Custom [▼](#)  EMA agent traffic

0.0.0.0/0 [X](#)

以下の設定を持つインバウンド・ルールを追加します。

- Type (タイプ) : Custom TCP (カスタム TCP)**
- Port range (ポート範囲) : 8080**
- Description (説明) :** インテル® EMA エージェントのトラフィック
- Source (送信元) : 0.0.0.0/0**

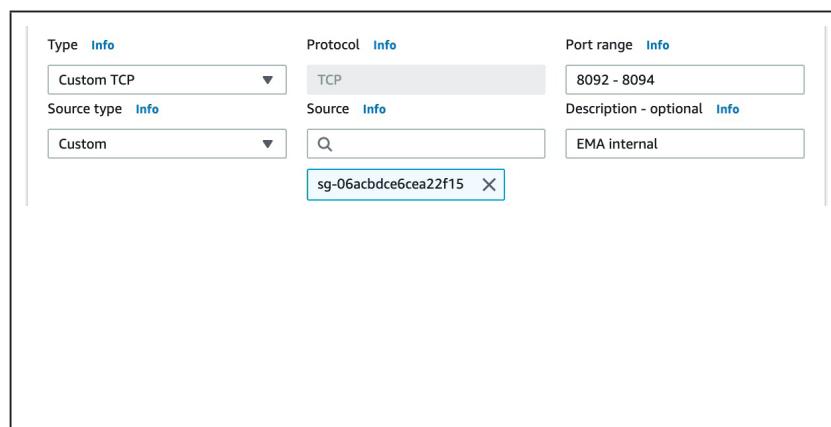
#### 4.7.1.6 作成と確認

<b>Details</b>	<p>Create security group(セキュリティー・グループを作成)ボタンをクリックし、ルールを保存します。</p> <p>ルールリストが正しいか確認します。</p> <p>注記：ここではアウトバウンド・ルールはデフォルトのルール(すべてのアウトバウンド・トラフィックを許可)のままにしました。</p>																														
<table border="1"><tr><td>Security group name ema-servers-sg</td><td>Security group ID sg-06acbdce6cea22f15</td></tr><tr><td>Description Allow access to EMA servers</td><td>VPC ID vpc-001161d1e7e50afb2</td></tr><tr><td>Owner 312506926764</td><td>Inbound rules count 4 Permission entries</td></tr><tr><td>Outbound rules count 1 Permission entry</td><td></td></tr></table>	Security group name ema-servers-sg	Security group ID sg-06acbdce6cea22f15	Description Allow access to EMA servers	VPC ID vpc-001161d1e7e50afb2	Owner 312506926764	Inbound rules count 4 Permission entries	Outbound rules count 1 Permission entry																								
Security group name ema-servers-sg	Security group ID sg-06acbdce6cea22f15																														
Description Allow access to EMA servers	VPC ID vpc-001161d1e7e50afb2																														
Owner 312506926764	Inbound rules count 4 Permission entries																														
Outbound rules count 1 Permission entry																															
<b>Inbound rules</b> <b>Outbound rules</b> <b>Tags</b>																															
<table border="1"><thead><tr><th colspan="5">Inbound rules</th></tr><tr><th>Type</th><th>Protocol</th><th>Port range</th><th>Source</th><th>Description - optional</th></tr></thead><tbody><tr><td>Custom TCP</td><td>TCP</td><td>8084</td><td>[REDACTED]/32</td><td>Trusted network(s) for websocket</td></tr><tr><td>Custom TCP</td><td>TCP</td><td>8080</td><td>0.0.0.0/0</td><td>EMA agent traffic</td></tr><tr><td>RDP</td><td>TCP</td><td>3389</td><td>[REDACTED]/32</td><td>Trusted network(s) for RDP</td></tr><tr><td>HTTPS</td><td>TCP</td><td>443</td><td>[REDACTED]/32</td><td>Trusted network(s) for web</td></tr></tbody></table>	Inbound rules					Type	Protocol	Port range	Source	Description - optional	Custom TCP	TCP	8084	[REDACTED]/32	Trusted network(s) for websocket	Custom TCP	TCP	8080	0.0.0.0/0	EMA agent traffic	RDP	TCP	3389	[REDACTED]/32	Trusted network(s) for RDP	HTTPS	TCP	443	[REDACTED]/32	Trusted network(s) for web	
Inbound rules																															
Type	Protocol	Port range	Source	Description - optional																											
Custom TCP	TCP	8084	[REDACTED]/32	Trusted network(s) for websocket																											
Custom TCP	TCP	8080	0.0.0.0/0	EMA agent traffic																											
RDP	TCP	3389	[REDACTED]/32	Trusted network(s) for RDP																											
HTTPS	TCP	443	[REDACTED]/32	Trusted network(s) for web																											

#### 4.7.2 セキュリティー・グループを更新し、インテル® EMA VM 間のトラフィックを許可(分散サーバーのみ)

ema-server-sg セキュリティー・グループを作成したところで、Edit inbound rules(インバウンド・ルールを編集)ボタンをクリックし、以下のように変更します。

##### 4.7.2.1 ポート 8092 ~ 8094 に対する内部トラフィック用のインバウンド・ルールの追加

	以下の設定を持つインバウンド・ルールを追加します。
	<ul style="list-style-type: none"><li><b>Type (タイプ)</b> : Custom TCP (カスタム TCP)</li><li><b>Port range (ポート範囲)</b> : 8092-8094</li><li><b>Description (説明)</b> : インテル® EMA 内部</li><li><b>Source (送信元)</b> : 空のテキストボックスをクリックし、前の手順で作成したセキュリティー・グループの名前を選択します。</li></ul>

#### 4.7.2.2 ポート 8089 に対する内部トラフィック用インバウンド・ルールの作成

以下 の 設定 を 持つ インバウンド・ルール を 追加 し ます。

- Type (タイプ)** : Custom TCP (カスタム TCP)
- Port range (ポート範囲)** : 8089
- Description (説明)** : インテル® EMA 管理ポート
- Source (送信元)** : 空のテキストボックスをクリックし、前の手順で作成したセキュリティー・グループの名前を選択します。

#### 4.7.2.3 保存し、最終的なリストが正しいか確認します。

Save rules (ルールを保存) ボタンをクリックします。ルールが正しいか確認します。

Inbound rules					Edit inbound rules
Type	Protocol	Port range	Source	Description - optional	
Custom TCP	TCP	8084	10.250.0.0/24	trusted networks for websocket	
Custom TCP	TCP	8084	[REDACTED]/32	trusted networks for websocket	
Custom TCP	TCP	8080	0.0.0.0/0	EMA agent traffic	
Custom TCP	TCP	8089	sg-08d3222f040f45bdd (ema-servers-sg)	EMA admin port	
Custom TCP	TCP	8092 - 8094	sg-08d3222f040f45bdd (ema-servers-sg)	EMA internal	
HTTPS	TCP	443	10.250.0.0/24	trusted networks for web	
HTTPS	TCP	443	[REDACTED]/32	trusted networks for web	

#### 4.7.3 データベース用のセキュリティー・グループの作成

##### 4.7.3.1 セキュリティー・グループの作成

VPC セクション の サイドバー から **Security Groups (セキュリティー・グループ)** を 選択 し ます。

Create security group (セキュリティー・グループを作成) ボタンを クリック し ます。

#### 4.7.3.2 セキュリティー・グループの基本情報の設定

**Create security group** [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name [Info](#)  
ema-db-sg  
Name cannot be edited after creation.

Description [Info](#)  
Allow traffic from EMA server(s) to the database

VPC [Info](#)  
vpc-05506a755ff48bf6e (intel-ema-network) ▾

インテル® EMA サーバーへのアクセスを許可するセキュリティー・グループについて基本的な情報を入力します。

- Security group name (セキュリティー・グループ名)**: 一意の名前を入力します。  
例 : ema-db-sg
- Description (説明) (オプション)**: セキュリティー・グループの説明を入力します。  
例 : インテル® EMA サーバーからデータベースへのトライアックの許可
- VPC**: 先ほど作成した VPC を選択します。

#### 4.7.3.3 MSSQL 用のインバウンド・ルールの追加

**Inbound rules** [Info](#)

**Inbound rule 1**

Type [Info](#)  
MSSQL

Source type [Info](#)  
Custom

Port range  
::/16  
::/32  
::/48  
::/64

Security Groups  
ema-server-sg | sg-03661abff0a38ee50

以下の設定を持つインバウンド・ルールを追加します。

- Type (タイプ)**: MSSQL
- Source (送信元)**: 空のテキストボックスをクリックし、先ほど作成したインテル® EMA サーバー用セキュリティー・グループを選択します。

#### 4.7.3.4 作成と確認

Create security group (セキュリティー・グループを作成) ボタンをクリックします。ルールリストが正しいか確認します。

Inbound rules				Edit
Type	Protocol	Port range	Source	
MSSQL	TCP	1433	sg-08d3222f040f45bdd (ema-servers-sg)	

# 5 仮想マシンのデプロイメント

## 5.1 概要

Amazon Elastic Compute Cloud\* (Amazon EC2\*) 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。

EC2\* インスタンスに割り当てる 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カロード用の VM を最適化してコストを削減することもできます。

EC2\* は EC2\* キーペアを使用してインスタンスへのログインを保護します (AWS\* では公開鍵を保管し、ユーザーは秘密鍵を安全な場所に保管します)。これは、事前に作成しておくことも、EC2\* インスタンスの作成時に作成することもできます。Windows\* ベースのインスタンスで自動生成された管理者資格情報を取得するには、秘密鍵が必要です。EC2\* では複数のキーペアを持つことができますが、インスタンスに関連付けることができるのは 1 つだけ、インスタンス作成後に変更することはできません。

EC2\* インスタンスへのネットワーク・アクセスのセキュリティーは、インスタンス作成時またはその後の任意の時点において、1 つまたは複数のセキュリティー・グループをアタッチすることで保護されます。ここで必要なセキュリティー・グループは、前章すでに作成しました。

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。該当するステップには、2 つ目の VM の作成、ターゲットグループへの VM の関連付け、ターゲットグループのロードバランサーへのアタッチ、ロードバランサー転送ルールの設定があります。

EC2\* インスタンスやキーペアの詳細については、以下のリンクを参照してください。

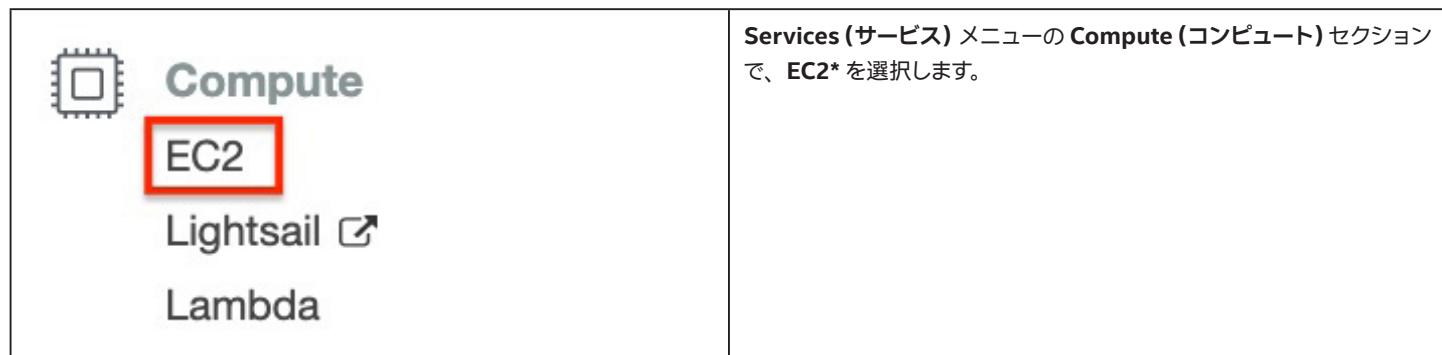
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html>

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-key-pairs.html>

## 5.2 仮想マシンの作成

最新の Windows Server\* イメージを使用してインテル® EMA サーバー用の EC2\* インスタンスを作成し、先ほど作成したセキュリティー・グループをアタッチする手順は以下のとおりです。

### 5.2.1 EC2\* サービスへの移動



### 5.2.2 EC2\* インスタンスの起動



### 5.2.3 Amazon マシンイメージ(AMI)の選択

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select your own AMIs.

Search: Windows Server

AWS Launch Wizard for SQL Server offers an easy way to size, configure, and deploy Microsoft SQL Server Always On availability groups. [Use AWS Launch Wizard for this launch](#)

Quick Start (19)

My AMIs (0)

AWS Marketplace (393)

Community AMIs (2144)

Windows

Microsoft Windows Server 2019 Base - ami-0d1b8b740ddc3b78d

Select

Free tier eligible

Microsoft Windows 2019 Datacenter edition. [English]

64-bit (x86)

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

1 to 19 of 19 AMIs

インテル® EMA でサポートされる最新の Microsoft\* Windows Server\* のベースイメージを検索します。

サポートされるオペレーティング・システムの一覧については、インテル® エンドポイント・マネジメント・アシスタント・サーバー・インストール・ガイドを参照してください。

Select (選択) ボタンをクリックします。

### 5.2.4 マシンタイプの選択

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage

Step 2: Choose an Instance Type

Filter by: General purpose Current generation Show/Hide

Currently selected: t3a.large (Variable ECUs, 2 vCPUs, 2.2 GHz, AMD EPYC)

	Family	Type	vCPUs	Memory (GiB)
	General purpose	t2.nano	1	0.5
	General purpose	t2.micro	1	1
	General purpose	t2.small	1	2
	General purpose	t2.medium	2	4
	General purpose	t2.large	2	8

必要な CPU およびメモリリソースを持つマシンタイプを選択します。マシンタイプは、必要に応じて、インスタンスをオフにしたときに変更できます。

システム要件については、インテル® エンドポイント・マネジメント・アシスタント・サーバー・インストール・ガイドを参照してください。

Next: Configure Instance Details (次へ：インスタンスの詳細を設定する) ボタンをクリックします。

## 5.2.5 インスタンスの詳細の設定

1. Choose AMI    2. Choose Instance Type    **3. Configure Instance**    4. Add Storage    5. Add Tags    6. Create

### Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request lower pricing, assign an access management role to the instance, and more.

Number of instances: 1    [Launch into Auto Scaling](#)

Purchasing option:  Request Spot instances

Network: vpc-05506a755ff48bf6e | intel-ema-network  
No default VPC found. [Create a new default VPC](#).

Subnet: subnet-0850a0c96d7a404da | private-usw1a | us-west-2a  
59 IP Addresses available

Auto-assign Public IP: Disable

インスタンスの詳細を以下のように設定します。

- Network (ネットワーク)**: 先ほど作成した VPC に設定します。  
例 : *intel-ema-network*
- Subnet (サブネット)**: プライベート・サブネットの 1 つを選択します。  
例 : *private-usw1a*
- Auto-assign Public IP (パブリック IP を自動割り当てる)**: *Disable* (無効)

インスタンスの詳細のその他の項目はデフォルトのままで構いません。

**Next: Add Storage (次へ:ストレージを追加する)** ボタンをクリックします。

## 5.2.6 ストレージの追加

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0cc417e3e52bda57e	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

より大きなスペースが必要でない限り、ストレージ設定はデフォルトのままで構いません。システム要件については、インテル® エンドポイント・マネジメント・アシスタント・サーバー・インストール・ガイドを参照してください。

**Next: Add Tags (次へ: タグを追加する)** ボタンをクリックします。

## 5.2.7 タグの追加

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.  
A copy of a tag can be applied to volumes, instances or both.  
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	ema-server-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key (キー) に「Name」、Value (値) に目的のサーバー名を指定したタグを追加します。

「はじめに」の「タグとリソースグループ」セクションで説明したとおり、リソースの整理に役立つ任意のカスタムタグを追加できます。

**Next: Configure Security Group (次へ: セキュリティ・グループを設定する)** ボタンをクリックします。

## 5.2.8 セキュリティー・グループの設定

<p><b>Step 6: Configure Security Group</b></p> <p>A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below.</p> <p>Assign a security group: <input type="radio"/> Create a new security group <input checked="" type="radio"/> Select an existing security group</p> <table border="1"><thead><tr><th>Security Group ID</th><th>Name</th><th>Description</th></tr></thead><tbody><tr><td>sg-04c1e0cf58c3b592e</td><td>default</td><td>default VPC security group</td></tr><tr><td>sg-017cfe786b8c9004a</td><td>ema-db-sg</td><td>Allow traffic from EMA server(s) to the database</td></tr><tr><td>sg-06acbdce6cea22f15</td><td>ema-servers-sg</td><td>Allow access to EMA servers</td></tr></tbody></table>	Security Group ID	Name	Description	sg-04c1e0cf58c3b592e	default	default VPC security group	sg-017cfe786b8c9004a	ema-db-sg	Allow traffic from EMA server(s) to the database	sg-06acbdce6cea22f15	ema-servers-sg	Allow access to EMA servers	<p><b>Assign a security group (セキュリティー・グループを割り当てる)</b> ラジオボタンを選択し、既存のセキュリティー・グループを選択します。</p> <p>先ほどインテル® EMA サーバー用に作成したセキュリティー・グループを選択します。例：ema-servers-sg</p> <p><b>Next: Review and Launch (次へ：確認して起動する)</b> ボタンをクリックします。</p> <p>セキュリティー・グループのポート 3389 (RDP) が開放されていないためインスタンスの接続できないという警告が表示される場合があります。ここでは仮想マシンにアクセスする別の方法があるため、このメッセージは無視して続行します。</p>
Security Group ID	Name	Description											
sg-04c1e0cf58c3b592e	default	default VPC security group											
sg-017cfe786b8c9004a	ema-db-sg	Allow traffic from EMA server(s) to the database											
sg-06acbdce6cea22f15	ema-servers-sg	Allow access to EMA servers											

## 5.2.9 インスタンスの起動の確認

インスタンスの詳細を確認してから、**Launch (起動)** ボタンをクリックします。

## 5.2.10 EC2\* キーペアの選択

<p>Select an existing key pair or create a new key pair</p> <p>A key pair consists of a <b>public key</b> that AWS stores, and a <b>private key file</b> that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.</p> <p>Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about <a href="#">removing existing key pairs from a public AMI</a>.</p> <p>Create a new key pair Key pair name ema-demo Download Key Pair</p> <p>You have to download the <b>private key file</b> (*.pem file) before you can continue. <b>Store it in a secure and accessible location.</b> You will not be able to download the file again after it's created.</p> <p>Cancel Launch Instances</p>	<p>既存のキーペアを選択するか、新しいキーペアを作成するよう促されます。</p> <p>リストから適切なキーペアを選択するか、<b>Create a new key pair (新しいキーペアを作成する)</b> を選択して、<b>Download Key Pair (キーペアをダウンロード)</b> ボタンをクリックし、ローカルのコンピューター上に秘密鍵ファイルを保存します。</p> <p>既存のキーペアを使用することを選択した場合、その秘密鍵ファイルにアクセスできることが必要です。</p> <p><b>Launch Instances (インスタンスを起動)</b> ボタンをクリックします。</p>
---	--

## 5.3 2つ目の EC2\* インスタンスの作成(分散サーバーのみ)

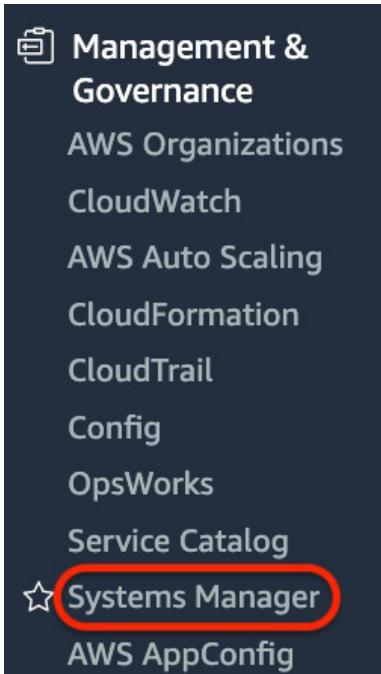
分散サーバー・デプロイメントでは、2つ目のインテル® EMA サーバーを作成するため、前の手順を繰り返します。ただし、前回とは別のサブネットを選択し、別の Name タグ (ema-server-2 など) を指定します。

## 6 AWS\* System Manager の設定(分散サーバーのみ)

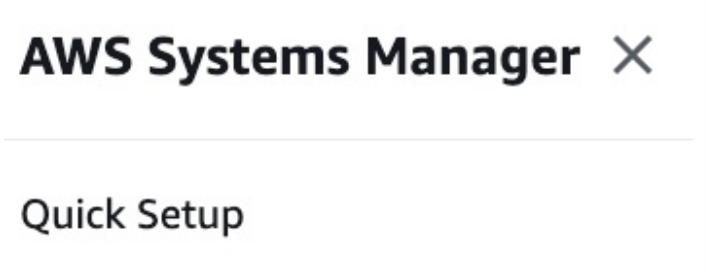
AWS\* System Manager とは、AWS\* 上のインフラストラクチャーの可視性を高め、コントロールしやすくしてくれるサービスです。セッション・マネージャー・コンポーネントを使用してパブリック IP アドレスを持たない VM へのリモートアクセスを実現するには、これを有効化する必要があります。

Systems Manager の詳細については、以下のリンクを参照してください。<https://aws.amazon.com/systems-manager/>

### 6.1 Systems Manager サービスへの移動

	Services(サービス)メニューの Management & Governance(管理とガバナンス) セクションで、 <b>Systems Manager</b> を選択します。
---	--

### 6.2 Quick Setup(高速セットアップ)の開始

	
--	--

## 6.3 Permissions (アクセス許可) オプションの選択

**Quick Setup** Info

Configure required security roles and commonly used Systems Manager capabilities.

**Permissions (Required)**

Use the following options to configure two roles that give Systems Manager permission to access your instances and run commands on them.

**Instance profile role**

Use the default role       Choose an existing role

Quick Setup creates a new instance profile that uses a secure IAM permissions policy. Quick Setup assigns the profile to the instances that you specify.

Use the default role       Choose an existing role

Uses an existing instance profile. The instance profile must contain the required permissions policy. Choose the instance profile from the following list.

**Assume role for Systems Manager**

Use the default role       Choose an existing role

Quick Setup creates a new assume role that enables Systems Manager to securely run commands on your instances.

Use the default role       Choose an existing role

Uses an existing service role. The role must contain the required permissions policy. Choose the role from the following list

## 6.4 Configurations (設定) オプションの選択

**Configuration options**

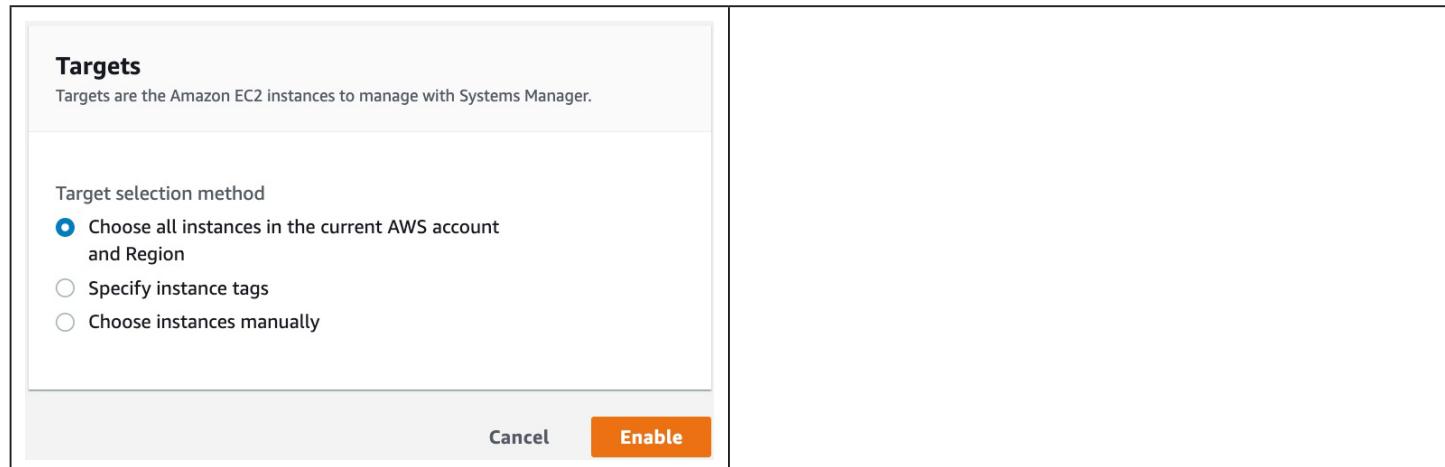
Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

Update Systems Manager (SSM) Agent every two weeks  
 Collect inventory from your instances every 30 minutes  
 Scan instances for missing patches daily  
 Install and configure the CloudWatch agent  
 Update the CloudWatch agent once every 30 days

If you run Quick Setup, [Systems Manager Explorer](#) is enabled.

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and [Amazon CloudWatch pricing](#).

## 6.5 Targets(ターゲット)の選択



## 6.6 Managed Instances(マネージド・インスタンス)のリストの確認

The screenshot shows the 'Managed Instances' list in the AWS Systems Manager console. It displays two instances: 'ema-server-2' and 'ema-server-1'. The 'ema-server-2' row shows an 'Association status' of 'Pending'. The 'ema-server-1' row shows an 'Association status' of 'Success'. Other columns include Instance ID, Name, Ping status, Platform type, Platform name, Platform version, Agent version, IP address, Computer name, and Actions.

Instance ID	Name	Ping status	Platform type	Platform name	Platform version	Agent version	IP address	Computer name	Association status
i-0a6a82fc35afa0cf7	ema-server-2	Online	Windows	Microsoft Windows Server 2019 Datacenter	10.0.17763	3.0.222.0	10.250.0.82	EC2AMAZ-PM4CVE0.WORKGROUP	Pending
i-06364ced48ee5bb96	ema-server-1	Online	Windows	Microsoft Windows Server 2019 Datacenter	10.0.17763	3.0.222.0	10.250.0.16	EC2AMAZ-8BHE25G.WORKGROUP	Success

## 6.7 Session Managerによる仮想マシンへのログイン

AWS\* のコンソール経由で Session Manager を使用する場合、VM 上の Powershell セッションにのみ接続できます。RDP で接続するには、ローカルのコマンドラインから AWS\* Command Line Interface (CLI) を使用し、ポート転送を有効化するオプションを渡して Session Manager を呼び出す必要があります。

本ガイドでは、AWS\* CLI のインストールについては説明しません。詳細については、<https://aws.amazon.com/cli/> を参照してください。

CLI がインストール済みかつ構成済みで、VM が AWS\* System Manager に表示されている場合、以下のシンタックスで CLI コマンドを実行できます。

```
aws ssm start-session --target <インスタンス ID> --document-name AWS-StartPortForwardingSession --parameters "localPortNumber=55678,portNumber=3389"
```

<インスタンス ID> を接続先の EC2\* インスタンスの ID に置き換えます。例：i-06364ced48ee5bb96

このコマンドが正常に動作した場合、リモート・デスクトップ・クライアントを使用して、指定した localPortNumber のローカルホストに接続できます。そして、その VM の資格情報を使用してログインできます。

## 7 Relational Database Service (RDS) のデプロイメント

AWS\* には、Amazon Relational Database Service\* (Amazon RDS\*) と呼ばれるフルマネージド型の Platform-as-a-Service データベース・エンジンがあり、AWS\* クラウド上のリレーショナル・データベースのセットアップ、オペレーション、スケールを簡単に実行できます。コスト効率に優れたサイズ変更可能なキャパシティーが提供されるだけでなく、バックアップ、ソフトウェアのパッチ適用、自動障害検出、リカバリーなどの一般的なデータベース管理タスクが管理されます。

Amazon RDS\* の基本構成要素は DB インスタンスです。DB インスタンスとは、AWS\* のクラウド上の分離されたデータベース環境です。DB インスタンスには、ユーザーが作成した複数のデータベースを含めることができます。DB インスタンスには、スタンダードアロンのデータベース・インスタンスに使用するのと同じツールとアプリケーションを使用してアクセスできます。DB インスタンスの演算およびメモリー容量は、DB インスタンス・クラスによって決まります。ニーズに最も合致する DB インスタンスを選択できます。時間が経ってニーズが変化した場合、DB インスタンスを変更できます。

今回は、異なるアベイラビリティー・ゾーン内の複数のサブネットに VPC を作成したため、マルチ AZ 配置というオプションを使用して RDS インスタンスを起動できます。本番環境でこのオプションを選択することで、プライマリーの DB インスタンスが、異なるアベイラビリティー・ゾーンにあるセカンダリーの予備 DB インスタンスに自動的に同期され、複製されます。このアプローチにより、データの冗長性とフェイルオーバーをサポートし、I/O フリーズを解消し、システム・バックアップ中のレイテンシー・スペイクを最小限に抑えられます。この目的で使用するアベイラビリティー・ゾーンを RDS に通知する、データベース・サブネット・グループを作成します。

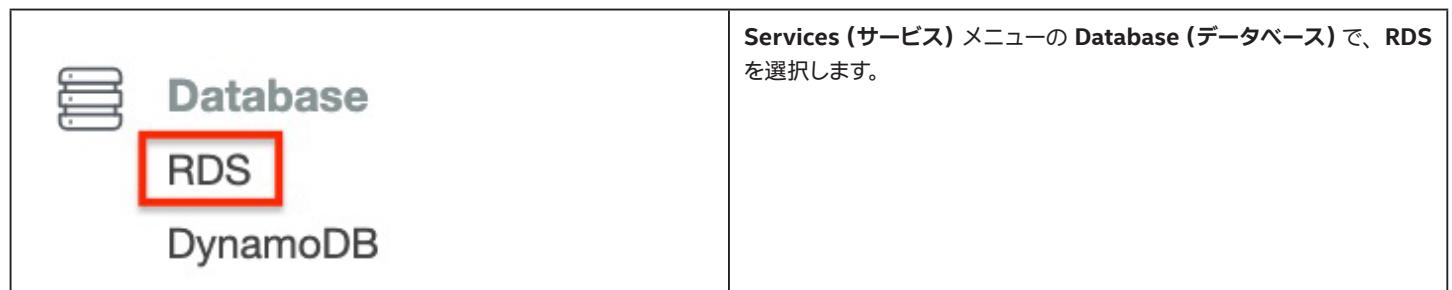
RDS インスタンスをコントロールし、インテル® EMA EC2\* インスタンスのみに接続を許可するには、本ガイドの前のセクションで作成したセキュリティー・グループを使用します。

RDS 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.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

Relational Database Service (RDS) インスタンスを作成し、前に作成したセキュリティー・グループをアタッチしてインテル® EMA EC2\* インスタンスからのデータベースへのトラフィックを許可するには、以下の手順に従います。

### 7.1 RDS サービスへの移動



Services (サービス) メニューの Database (データベース) で、RDS を選択します。

### 7.2 データベース・サブネット・グループの作成



RDS サイドバーから Subnet groups (サブネットグループ) を選択し、Create DB Subnet Group (DB サブネットグループを作成) ボタンをクリックします。

## 7.2.1 サブネットグループの詳細

### Create DB Subnet Group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

**Subnet group details**

**Name**  
You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

**Description**

**VPC**  
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

**Availability Zones**  
Choose the Availability Zones that include the subnets you want to add.

**Choose an availability zone**

**Subnets**  
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

**Select subnets**

**Subnets selected (2)**

Availability zone	Subnet ID	CIDR block
us-west-1a	subnet-0850a0c96d7a404da	10.250.0.0/26
us-west-1b	subnet-016e150f99130ef50	10.250.0.64/26

サブネットグループの詳細情報を以下のように入力します。

- **Name (名前)**: 一意の名前を入力します。  
例 : ema-db-subnet-group
- **Description (説明) (オプション)**  
例: インテル® EMA DB インスタンスで使用するサブネットを指定します。
- **VPC**: 先ほど作成した VPC を選択します。
- **Availability Zone (アベイラビリティー・ゾーン)**: サブネットを作成した両方のゾーンを選択します。
- **Subnets (サブネット)**: 先ほど作成した両方のプライベート・サブネットを選択します。

**Create (作成)** ボタンをクリックします。

## 7.3 データベースの作成

**Amazon RDS**

RDS > Databases

**Databases**

Group resources

RDS サイドバーから Databases (データベース) を選択し、**Create database (データベースを作成)** ボタンをクリックします。

### 7.3.1 データベース作成方法の選択

<p>Create database</p> <p>Choose a database creation method <a href="#">Info</a></p> <p><input checked="" type="radio"/> Standard Create You set all of the configuration options, including ones for availability, security, backups, and maintenance.</p> <p><input type="radio"/> Easy Create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.</p>	データベース作成方法として <b>Standard Create (標準作成)</b> を選択します。
---	---

### 7.3.2 エンジンタイプとエディションの選択

<p>Engine options</p> <p>Engine type <a href="#">Info</a></p> <p><input type="radio"/> Amazon Aurora</p> <p><input type="radio"/> MySQL</p> <p><input type="radio"/> MariaDB</p> <p><input type="radio"/> PostgreSQL</p> <p><input type="radio"/> Oracle</p> <p><input checked="" type="radio"/> Microsoft SQL Server</p> <p>Microsoft SQL Server エンジンを選択します。</p> <p>適切な SQL サーバー・エディションを選択します。本ガイドの目的上、本番環境では SQL Server* Standard Edition が使用されているものと仮定します。デプロイおよびテスト目的には、コスト削減のために SQL Server* Express Edition を使用できます。</p> <p>Edition</p> <p><input type="radio"/> SQL Server Express Edition Affordable database management system that supports database sizes up to 10 GB.</p> <p><input type="radio"/> SQL Server Web Edition In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.</p> <p><input checked="" type="radio"/> SQL Server Standard Edition Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.</p> <p><input type="radio"/> SQL Server Enterprise Edition Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.</p> <p>Version <a href="#">Info</a></p> <p>SQL Server 2017 14.00.3281.6.v1</p> <p>License</p> <p>license-included</p>	
--	--

### 7.3.3 デプロイメント・テンプレートの選択

<p>Templates</p> <p>Choose a sample template to meet your use case.</p> <p><input checked="" type="radio"/> Production Use defaults for high availability and fast, consistent performance.</p> <p><input type="radio"/> Dev/Test This instance is intended for development use outside of a production environment.</p>	Templates (テンプレート) で、 <b>Production (本番稼働用)</b> を選択します。
--	---

### 7.3.4 インスタンス名とマスターユーザー資格情報の設定

<p><b>Settings</b></p> <p><b>DB instance identifier</b> <a href="#">Info</a> Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region. <input type="text" value="ema-db"/></p> <p>The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.</p> <p><b>Credentials Settings</b></p> <p><b>Master username</b> <a href="#">Info</a> Type a login ID for the master user of your DB instance. <input type="text" value="admin"/></p> <p>1 to 16 alphanumeric characters. First character must be a letter <input type="checkbox"/> <b>Auto generate a password</b> Amazon RDS can generate a password for you, or you can specify your own password</p> <p><b>Master password</b> <a href="#">Info</a> <input type="password" value="*****"/> ⓘ Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).</p> <p><b>Confirm password</b> <a href="#">Info</a> <input type="password" value="*****"/> ⓘ</p>	<p>データベースに一意の名前を付けます。 例 : ema-db</p> <p>ユーザー名とパスワードの作成</p>
---	--

### 7.3.5 DB インスタンス・サイズの設定

<p><b>DB instance size</b></p> <p><b>DB instance class</b> <a href="#">Info</a> Choose a DB instance class that meets your processing power requirements, limited to those supported by the engine you selected above.</p> <p><input checked="" type="radio"/> <b>Standard classes (includes m classes)</b></p> <p><input type="radio"/> <b>Memory Optimized classes (includes r and x classes)</b></p> <p><input type="radio"/> <b>Burstable classes (includes t classes)</b></p> <p><b>db.m5.large</b> 2 vCPUs    8 GiB RAM    EBS: 3500 Mbps</p> <p><input checked="" type="checkbox"/> <b>Include previous generation classes</b></p>	<p>適切なリソースが提供されるよう、DB インスタンス・クラスを設定します。 推奨 : db.m5.large</p>
---	--

### 7.3.6 ストレージの設定(オプション)

割り当てられたデフォルトのストレージ容量を、必要に応じて増加させることができます。ここではデフォルトのままにします。ストレージ容量は後から増加させることができます。

## 7.3.7 接続の設定

<p><b>Connectivity</b></p> <p><b>Virtual private cloud (VPC) <small>Info</small></b> VPC that defines the virtual networking environment for this DB instance.</p> <p>intel-ema (vpc-001161d1e7e50afb2)</p> <p>Only VPCs with a corresponding DB subnet group are listed.</p> <p><small>(i) After a database is created, you can't change the VPC selection.</small></p> <p>▶ Additional connectivity configuration</p>	<p><b>Connectivity (接続)</b> で、前に作成した VPC を選択し、<b>Additional connectivity configuration(追加の接続設定)</b>セクションを展開します。</p>
---	---

## 7.3.8 接続の設定 - Additional Connectivity Configuration (追加の接続設定)

<p>▼ Additional connectivity configuration</p> <p><b>Subnet group <small>Info</small></b> DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.</p> <p>ema-db-subnet-group</p> <p><b>Publicly accessible <small>Info</small></b></p> <p><input type="radio"/> Yes Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.</p> <p><input checked="" type="radio"/> No RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.</p> <p><b>VPC security group</b> Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)</p> <p><input checked="" type="radio"/> Choose existing Choose existing VPC security groups</p> <p><input type="radio"/> Create new Create new VPC security group</p> <p>Existing VPC security groups</p> <p>Choose VPC security groups</p> <p>ema-db-sg X</p> <p><b>Availability Zone <small>Info</small></b></p> <p>No preference</p> <p><b>Database port <small>Info</small></b> TCP/IP port that the database will use for application connections.</p> <p>1433</p>	<p>先ほど作成したデータベース・サブネット・グループを選択します。</p> <p>デフォルトの VPC セキュリティー・グループの選択を解除し、先ほどデータベース用に作成した既存のセキュリティー・グループを選択します。</p>
--	--

### 7.3.9 確認と作成

<p><b>Estimated monthly costs</b></p> <table><tr><td>DB instance</td><td>735.11 USD</td></tr><tr><td>Storage</td><td>2.76 USD</td></tr><tr><td>Provisioned IOPS</td><td>110.00 USD</td></tr><tr><td><b>Total</b></td><td><b>847.87 USD</b></td></tr></table> <p>This billing estimate is based on on-demand usage as described in <a href="#">Amazon RDS Pricing</a>. Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.</p> <p>Estimate your monthly costs for the DB Instance using the <a href="#">AWS Simple Monthly Calculator</a>.</p> <p><small>ⓘ You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.</small></p>	DB instance	735.11 USD	Storage	2.76 USD	Provisioned IOPS	110.00 USD	<b>Total</b>	<b>847.87 USD</b>	<p>コスト見積もりを確認し、<b>Create database (データベースを作成)</b>ボタンをクリックします。</p>
DB instance	735.11 USD								
Storage	2.76 USD								
Provisioned IOPS	110.00 USD								
<b>Total</b>	<b>847.87 USD</b>								
<p>Cancel</p>	<p><b>Create database</b></p>								

### 7.4 データベースのホスト名の取得

Connectivity & security	Monitoring
<p><b>Connectivity &amp; security</b></p> <p>Endpoint &amp; port</p> <p>Endpoint</p> <p>ema-db.creq7zxsavq4.us-west-1.rds.amazonaws.com</p> <p>Port</p> <p>1433</p>	<p>データベースのデプロイが完了すると、詳細ページにデータベースのホスト名が表示されます。これは、インテル® EMA ソフトウェアのインストール中に設定に使用されます。</p>

# 8 ロードバランサーのデプロイメント(分散サーバーのみ)

## 8.1 概要

AWS\* ネットワーク・ロード・バランサーは、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。ロードバランサーが接続要求を受信すると、転送ルールに従い、関連付けられたターゲットグループからステータスの良好なターゲットを選択し、接続をターゲットに転送します。

リスナーは、ユーザーが設定したプロトコルおよびポートを使用して、クライアントからの接続要求をチェックし、ターゲットグループに要求を転送します。

各ターゲットグループは、ユーザーが設定したプロトコルおよびポート番号を使用して、EC2\* インスタンスなどの 1 つまたは複数の登録済みターゲットに要求をルーティングします。ターゲットグループごとにヘルスチェックを設定可能です。ヘルスチェックは、ロードバランサーのリスナールールに指定されたターゲットグループに登録されたすべてのターゲットに対して実行されます。

ここでは、どちらのアベイラビリティー・ゾーンでもトラフィックをターゲットにルーティングできるように、デプロイしたロードバランサーに対して複数のアベイラビリティー・ゾーンを有効化します。

ロードバランサーには、各 AZ 内の関連するロードバランサーの外部公開されたアドレスをポイントするホスト名が自動生成されます。インテル® EMA サーバーにアクセスするカスタムのドメインを使用するため、このホスト名をエイリアスする DNS CNAME レコードを作成する必要があります。

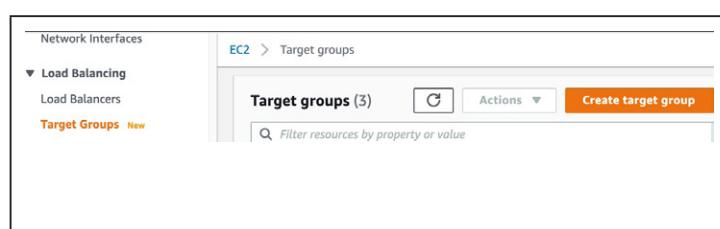
本資料に記載する以外にも、ロード・バランシングに関して可能な設定があります。順守すべき要件やプラクティスについて、IT 部門と相談する必要があります。AWS\* におけるロード・バランシングの詳細については、以下のリンクを参照してください。

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

## 8.2 ターゲットグループの作成

ロードバランサーがサービスを提供する各 TCP ポートに対してターゲットグループを作成し、ヘルスチェックを作成し、各ターゲットグループのトラフィックを受信するよう仮想マシンを登録する手順は次のとおりです。

### 8.2.1 ターゲットグループの作成

	<p><b>EC2*</b> サイドバーの <b>Load Balancing (ロード・バランシング)</b> で、<b>Target Groups (ターゲットグループ)</b> を選択します。</p> <p><b>Create target group (ターゲットグループを作成)</b> ボタンをクリックします。</p>
--	---

## 8.2.2 TCP/443 用のターゲットグループの設定

<p><b>Target group name</b></p> <p>ema-web</p> <p>Up to 32 alphanumeric characters, including underscores.</p> <p><b>Protocol</b> : Port</p> <p>TCP ▼ : 443</p> <p><b>VPC</b></p> <p>Select the VPC containing the instances you want to register.</p> <p>intel-ema-network vpc-05506a755ff48bf6e IPv4: 10.250.0.0/24</p> <p><b>Health checks</b></p> <p>The associated load balancer.</p> <p>Health check protocol</p> <p>TCP ▼</p>	<p>ターゲットグループを以下のように設定します。</p> <ul style="list-style-type: none"><li>• <b>Target type (ターゲットタイプ)</b> : Instances (インスタンス)</li><li>• <b>Target group name (ターゲットグループ名)</b> : 一意の名前を入力します。 例 : ema-web</li><li>• <b>Protocol (プロトコル)</b> : TCP</li><li>• <b>Port (ポート)</b> : 443</li><li>• <b>VPC</b> : 先ほど作成した VPC を選択します。</li><li>• <b>Health check protocol (ヘルスチェック・プロトコル)</b> : TCP</li></ul> <p>Next(次へ)をクリックして Register targets(ターゲットの登録)画面に進みます。</p>
--	---

### 8.2.2.1 両方の EC2\* インスタンスのターゲットとしての登録

**Register targets**

Step 2 of 2

Select instances, specify ports, and add the instances to the list of pending targets. Repeat to add additional combinations of instances and ports to the list of pending targets. You can skip this step if you prefer to register targets after creating the target group.

**Available instances (2)**

Instance ID	Name	State	Security groups	Zone	Subnet ID
i-00f8db1dd6650c6c8	ema-server-1	running	ema-servers-sg	us-west-1a	subnet-080e857
i-0f180ebc233227eda	ema-server-2	running	ema-servers-sg	us-west-1c	subnet-0a16634

0 selected

**Ports for the selected instances**  
Ports for routing traffic to the selected instances (separate multiple ports with commas):  
443

**Targets (2)**

Remove	Status	Instance ID	Name	Port	State	Security groups
X	Pending	i-00f8db1dd6650c6c8	ema-server-1	443	running	ema-servers-sg
X	Pending	i-0f180ebc233227eda	ema-server-2	443	running	ema-servers-sg

2 pending

Cancel Previous Create target group

両方のインテル® EMA VM インスタンスを選択し、**Include as pending below(以下に pending 状態として含める)** ボタンをクリックします。

**Create target group (ターゲットグループを作成)** ボタンをクリックします。

### 8.2.3 TCP/8084 用のターゲットの作成/設定

上記の手順を繰り返し、TCP/8084 用に「ema-websocket」という名前の別のターゲットグループを設定します。

### 8.2.4 TCP/8080 用のターゲットの設定

上記の手順を繰り返し、TCP/8080 用に「ema-swarm」という名前の別のターゲットグループを設定します。

## 8.2.5 ターゲットグループの確認

3つのターゲットグループが作成されたことを確認します。

Target groups (3)					
	Name	ARN	Port	Protocol	C A
<input type="checkbox"/>	ema-swarm	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/ema-swarm/53f34a1234567890	8080	TCP	
<input type="checkbox"/>	ema-web	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/ema-web/53f34a1234567890	443	TCP	
<input type="checkbox"/>	ema-websocket	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/ema-websocket/53f34a1234567890	8084	TCP	

## 8.2.6 TCP/443 ターゲットグループでのスティッキーネスの有効化

### 8.2.6.1 ターゲットグループの詳細

Attributes	
Stickiness	
Disabled	
Deregistration delay	
300 seconds	
Slow start duration	
0 seconds	
Load balancing algorithm	
Round robin	

ema-web ターゲットグループ名をクリックし、Group details (グループの詳細) 画面にアクセスします。

Attributes (属性) セクションで、Edit (編集) ボタンをクリックします。



### 8.2.6.2 属性の編集

<p>Edit attributes</p> <p>Attributes</p> <p>Deregistration delay The time to wait for in-flight requests to complete while deregistering a target. During this time, the state of the target is draining. <input type="text" value="300"/> seconds 0-3600</p> <p><input checked="" type="checkbox"/> Stickiness The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to a specific instance within the target group.</p> <p><input type="checkbox"/> Proxy protocol v2 Before you enable proxy protocol v2, make sure that your application targets can process proxy protocol headers otherwise your application might break.</p> <p>Cancel <span style="background-color: orange; color: white; padding: 2px 10px;">Save changes</span></p>	<p>Stickiness (ステイッキーネス) フラグを有効にします。</p> <p>Save changes (変更を保存) ボタンをクリックします。</p>
---	---

### 8.2.7 TCP/8084 ターゲットグループでのステイッキーネスの有効化

ema-websocket (TCP/8084) ターゲットグループについても、ステイッキーネス有効化の手順を繰り返します。

### 8.2.8 ターゲットグループのヘルス・モニタリングに関する注記

どのターゲットグループでも、Targets (ターゲット) タブと Monitoring (モニタリング) タブをチェックすることで、ターゲット・インスタンスのヘルスチェック・ステータスを確認できます。これらのヘルスチェックは、最初、インテル® EMA ソフトウェアがインストールされるまでは失敗します。

## 8.3 ウェブ・トラフィック用のネットワーク・ロード・バランサーの作成

トラフィックをステータスが良好なターゲットグループに分散させるためにネットワーク・ロード・バランサーを作成する手順は次のとおりです。

### 8.3.1 ロードバランサーの作成

<p>Placement Groups <a href="#">New</a></p> <p>Key Pairs <a href="#">New</a></p> <p>Network Interfaces</p> <p>▼ Load Balancing</p> <p><a href="#">Load Balancers</a></p> <p>Target Groups <a href="#">New</a></p>	<p>Create Load Balancer Actions ▾</p> <p>Filter by tags and attributes or search by keyword</p> <p>Name DNS name State</p> <p>You do not have any load balancers in this region.</p>	<p>EC2* サイドバーの Load Balancing (ロード・バランシング) で、Load Balancers (ロードバランサー) を選択し、Create Load Balancer (ロードバランサーを作成) をクリックします。</p>
---	--	--

### 8.3.2 ロードバランサーのタイプの選択

<p>Network Load Balancer</p> <p>TCP TLS UDP</p> <p>Create</p>	<p>Network Load Balancer (ネットワーク・ロード・バランサー) の見出しの下にある Create (作成) ボタンをクリックします。</p>
---	--

## 8.3.3 ロードバランサーの設定

### 8.3.3.1 基本設定

<p>1. Configure Load Balancer    2. Configure Security Settings    3. Configure Routing</p> <p><b>Step 1: Configure Load Balancer</b></p> <p><b>Basic Configuration</b></p> <p>To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.</p> <p>Name: ema-web-balancer</p> <p>Scheme: internet-facing</p>	<p>基本設定を入力します。</p> <p><b>Name (名前)</b>: 一意の名前を入力します。 例: ema-web-balancer</p> <p><b>Scheme (スキーム)</b>: internet-facing (インターネット公開)) 注記: 組織に AWS* によるサイト間の VPN が導入されており、プライベート IP アクセスが可能な場合、プライベート・サブネットにバインドされた内部ロードバランサーにすることもできます。</p> <p>本ガイドでは、そのようなアクセスがないことを想定しているため、パブリックサブネットにバインドされた、インターネット公開用のロードバランサーになります。</p>
--	---

### 8.3.3.2 リスナー

<p><b>Listeners</b></p> <p>A listener is a process that checks for connection requests, using the protocol and port that you configured.</p> <table border="1"><thead><tr><th>Load Balancer Protocol</th><th>Load Balancer Port</th></tr></thead><tbody><tr><td>TCP</td><td>443</td></tr><tr><td>TCP</td><td>8084</td></tr></tbody></table>	Load Balancer Protocol	Load Balancer Port	TCP	443	TCP	8084	<p><b>Listeners (リスナー)</b> セクションで、以下のプロトコルおよびポートについてリスナーを追加します。</p> <ul style="list-style-type: none"><li>TCP 443</li><li>TCP 8084</li></ul>
Load Balancer Protocol	Load Balancer Port						
TCP	443						
TCP	8084						

### 8.3.3.3 アベイラビリティ・ゾーン

<p><b>Availability Zones</b></p> <p>Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.</p> <p><a href="#">Create and manage Elastic IPs in the VPC console</a></p> <p>VPC: vpc-05506a755ff48bf6e (10.250.0.0/24)   intel-ema-network</p> <p>Availability Zones:</p> <ul style="list-style-type: none"><li>us-west-1a: subnet-07aff7a001005ed34 (public-usw1a)</li><li>us-west-1b: subnet-0110cd4da4ec72e62 (public-usw1b)</li></ul> <p>IPv4 address: Assigned by AWS</p>	<p><b>Availability Zone (アベイラビリティ・ゾーン)</b>を次のように設定します。</p> <ul style="list-style-type: none"><li><b>VPC</b>: 先ほど作成した VPC を選択します。</li><li><b>Availability Zone (アベイラビリティ・ゾーン)</b>: 両方のアベイラビリティ・ゾーンを有効にし、両方のパブリックサブネットを選択します。IPv4 アドレスは <b>Assigned by AWS (AWS*によって割り当て)</b> に設定します。</li></ul> <p><b>Next: Configure Security Settings (次へ: セキュリティ設定をする)</b> ボタンをクリックします。</p>
--	--

### 8.3.3.4 セキュリティ設定

このステップで行う設定はありません。 **Next: Configure Routing (次へ: ルーティングを設定する)** ボタンをクリックします。

### 8.3.3.5 ルーティングの設定

#### Step 3: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol health checks on the targets using these health check settings. Note that each target balancer.

##### Target group

Target group	<input type="button" value="i"/> Existing target group
Name	<input type="text" value="ema-web"/>
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP
Protocol	<input type="button" value="i"/> TCP
Port	<input type="text" value="443"/>

Step 3: Configure Routing (ステップ 3 : ルーティングの設定)で、Target group (ターゲットグループ) を以下のように設定します。

- **Target group (ターゲットグループ)**: 既存のターゲットグループ
- **Name (名前)**: 先ほど作成した TCP/443 ターゲットグループの名前を選択します。  
例 : ema-web

Next: Register Targets (次へ : ターゲットを登録する) ボタンをクリックします。

##### Health checks

Protocol	<input type="button" value="i"/> TCP
----------	--------------------------------------

### 8.3.3.6 ターゲットの登録

#### Step 4: Register Targets

##### Configure Security Groups

The security groups for your instances must allow traffic from the VPC CIDR on the health check port.

登録済みのターゲットとして 2 つのインスタンスがリストされていることを確認します。

Next: Review (次へ : 確認) ボタンをクリックします。

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

##### Registered targets

The following targets are registered with the target group that you selected. You can only modify this list after you create the load balancer.

Instance	Port
i-06364ced48ee5bb96	443
i-0a6a82fc33afa0cf7	443

[Cancel](#) [Previous](#) [Next: Review](#)

### 8.3.3.7 確認

Step 5: Review (ステップ 5 : 確認) で、以下に示すサンプルと似たような結果になっていることを確認し、Create (作成) ボタンをクリックします。

#### Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer Edit

**Name** ema-web-balancer  
**Scheme** internet-facing  
**Listeners** Port:443 - Protocol:TCP  
Port:8084 - Protocol:TCP  
**IP address type** ipv4  
**VPC** vpc-05506a755ff48bf6e (intel-ema-network)  
**Subnets** subnet-07aff7a001005ed34 (public-usw1a),  
subnet-0110cd4da4ec72e62 (public-usw1b) ▲  
**Tags**

▼ Routing Edit

**Target group** Existing target group  
**Target group name** ema-web  
**Port** 443  
**Target type** instance  
**Protocol** TCP  
**Health check protocol** TCP  
**Health check port** traffic port  
**Healthy threshold** 3  
**Unhealthy threshold** 3  
**Interval** 30

Cancel Previous Create

### 8.3.4 ロードバランサー転送ルールの修正

ポート 443 リスナーの転送ターゲットは正しいですが、正しいターゲットグループに転送するためにポート 8084 のリスナーを編集、変更する必要があります。

### 8.3.4.1 ロード・バランサー・リスナーの編集

作成したロードバランサーを選択します。

**Listeners (リスナー)** タブを選択します。

TCP/8084 リスナーの横のチェックボックスをオンにします。

**Edit (編集)** ボタンをクリックします。

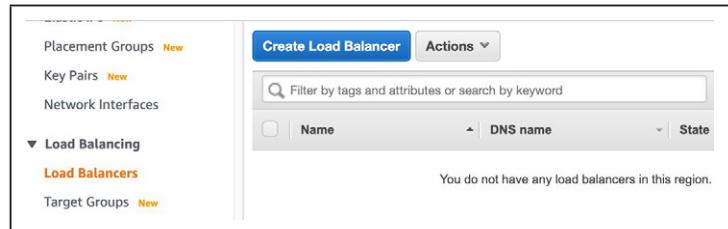
### 8.3.4.2 TCP/8084 リスナー転送アクションを更新します。

WebSocket リスナーに転送するよう、デフォルトのアクションを変更します。

**Update (更新)** ボタンをクリックします。

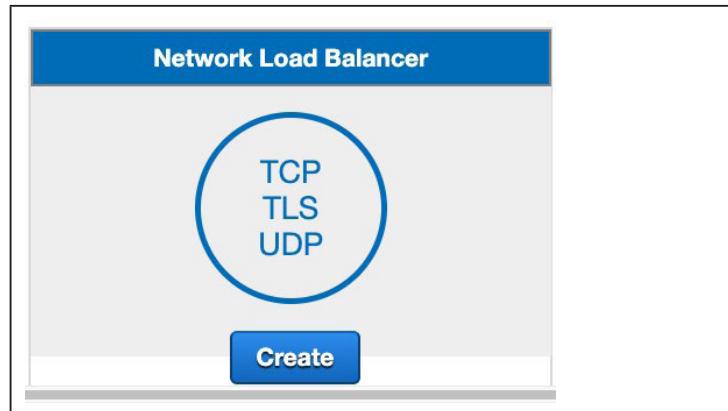
## 8.4 Swarm トラフィック用のネットワーク・ロード・バランサーの作成

### 8.4.1 ロードバランサーの作成



EC2\* サイドバーの **Load Balancing (ロード・バランシング)** で、**Load Balancers (ロードバランサー)** を選択し、**Create Load Balancer (ロードバランサーを作成)** をクリックします。

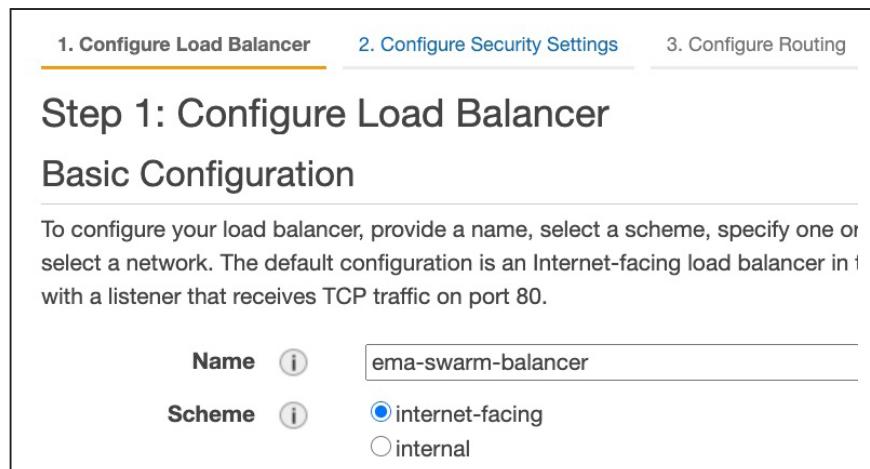
### 8.4.2 ロードバランサーのタイプの選択



**Network Load Balancer** (ネットワーク・ロード・バランサー) の見出しの下にある **Create (作成)** ボタンをクリックします。

### 8.4.3 ロードバランサーの設定

#### 8.4.3.1 基本設定



1. Configure Load Balancer    2. Configure Security Settings    3. Configure Routing

**Step 1: Configure Load Balancer**

**Basic Configuration**

To configure your load balancer, provide a name, select a scheme, specify one or select a network. The default configuration is an Internet-facing load balancer in with a listener that receives TCP traffic on port 80.

**Name**  **Scheme**  internet-facing

基本設定を入力します。  
**Name (名前)**: 一意の名前を入力します。  
例 : ema-swarm-balancer  
**Scheme (スキーム)**: internet-facing (インターネット公開)

#### 8.4.3.2 リスナー

<h3>Listeners</h3> <p>A listener is a process that checks for connection requests, using the protocol and port you specify.</p> <table border="1"><tr><td>Load Balancer Protocol</td><td>Load Balancer Port</td></tr><tr><td>TCP</td><td>8080</td></tr></table>	Load Balancer Protocol	Load Balancer Port	TCP	8080	<p>Listeners (リスナー) セクションで、以下のプロトコルおよびポートについてリスナーを追加します。</p> <ul style="list-style-type: none"><li>TCP 8080</li></ul>
Load Balancer Protocol	Load Balancer Port				
TCP	8080				

#### 8.4.3.3 アベイラビリティ・ゾーン

<h3>Availability Zones</h3> <p>Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.</p> <p><a href="#">Create and manage Elastic IPs in the VPC console</a></p> <table border="1"><tr><td>VPC</td><td>vpc-05506a755ff48bf6e (10.250.0.0/24)   intel-ema-network</td></tr><tr><td>Availability Zones</td><td><input checked="" type="checkbox"/> us-west-1a subnet-07aff7a001005ed34 (public-usw1a)</td></tr><tr><td>IPv4 address</td><td>Assigned by AWS</td></tr><tr><td><input checked="" type="checkbox"/> us-west-1b subnet-0110cd4da4ec72e62 (public-usw1b)</td><td></td></tr><tr><td>IPv4 address</td><td>Assigned by AWS</td></tr></table>	VPC	vpc-05506a755ff48bf6e (10.250.0.0/24)   intel-ema-network	Availability Zones	<input checked="" type="checkbox"/> us-west-1a subnet-07aff7a001005ed34 (public-usw1a)	IPv4 address	Assigned by AWS	<input checked="" type="checkbox"/> us-west-1b subnet-0110cd4da4ec72e62 (public-usw1b)		IPv4 address	Assigned by AWS	<p>Availability Zone (アベイラビリティ・ゾーン) を次のように設定します。</p> <ul style="list-style-type: none"><li><b>VPC</b> : 先ほど作成した VPC を選択します。</li><li><b>Availability Zone (アベイラビリティ・ゾーン)</b> : 両方のアベイラビリティ・ゾーンを有効にし、両方のパブリックサブネットを選択します。IPv4 アドレスは <b>Assigned by AWS (AWS*によって割り当て)</b> に設定します。</li></ul> <p>Next: Configure Security Settings (次へ: セキュリティ設定をする) ボタンをクリックします。</p>
VPC	vpc-05506a755ff48bf6e (10.250.0.0/24)   intel-ema-network										
Availability Zones	<input checked="" type="checkbox"/> us-west-1a subnet-07aff7a001005ed34 (public-usw1a)										
IPv4 address	Assigned by AWS										
<input checked="" type="checkbox"/> us-west-1b subnet-0110cd4da4ec72e62 (public-usw1b)											
IPv4 address	Assigned by AWS										

#### 8.4.3.4 セキュリティ設定

このステップで行う設定はありません。Next: Configure Routing (次へ: ルーティングを設定する) ボタンをクリックします。

#### 8.4.3.5 ルーティングの設定

<p>1. Configure Load Balancer    2. Configure Security Settings    3. Configure Routing</p> <p><b>Step 3: Configure Routing</b></p> <p>Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.</p> <p><b>Target group</b></p> <table border="1"><tr><td>Target group</td><td>Existing target group</td></tr><tr><td>Name</td><td>ema-swarm</td></tr><tr><td>Target type</td><td><input checked="" type="radio"/> Instance <input type="radio"/> IP</td></tr><tr><td>Protocol</td><td>TCP</td></tr><tr><td>Port</td><td>8080</td></tr></table> <p><b>Health checks</b></p> <table border="1"><tr><td>Protocol</td><td>TCP</td></tr></table> <p><b>Cancel</b>   <b>Previous</b>   <b>Next: Register Targets</b></p>	Target group	Existing target group	Name	ema-swarm	Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP	Protocol	TCP	Port	8080	Protocol	TCP	<p><b>Step 3: Configure Routing (ステップ 3: ルーティングの設定)</b> で、Target group (ターゲットグループ) を以下のように設定します。</p> <ul style="list-style-type: none"><li><b>Target group (ターゲットグループ)</b>: 既存のターゲットグループ</li><li><b>Name (名前)</b>: 先ほど作成した TCP/8080 ターゲットグループの名前を選択します。 例: ema-swarm</li></ul> <p>Next: Register Targets (次へ: ターゲットを登録する) ボタンをクリックします。</p>
Target group	Existing target group												
Name	ema-swarm												
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP												
Protocol	TCP												
Port	8080												
Protocol	TCP												

#### 8.4.3.6 ターゲットの登録

	<p>登録済みのターゲットとして 2 つのインスタンスがリストされていることを確認します。</p> <p><b>Next: Review (次へ : 確認)</b> ボタンをクリックします。</p>
--	---

#### 8.4.3.7 確認

Step 5: Review (ステップ 5 : 確認) で、以下に示すサンプルと似たような結果になっていることを確認し、**Create (作成)** ボタンをクリックします。

1. Configure Load Balancer    2. Configure Security Settings    3. Configure Routing

#### Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer Edit

Name ema-swarm-balancer  
Scheme internet-facing  
Listeners Port:8080 - Protocol:TCP  
IP address type ipv4  
VPC vpc-05506a755ff48bf6e (intel-ema-network)  
Subnets subnet-07aff7a001005ed34 (public-usw1a), subnet-0110cd4da4ec72e62 (public-usw1b) ▲  
Tags

▼ Routing Edit

Target group Existing target group  
Target group name ema-swarm  
Port 8080  
Target type instance  
Protocol TCP  
Health check protocol TCP  
Health check port traffic port  
Healthy threshold 3  
Unhealthy threshold 3  
Interval 30

[Cancel](#) [Previous](#) Create

#### 8.4.4 ロードバランサーの DNS 名の記録

ロードバランサーの **Description (説明)** タブに戻り、DNS 名をメモします。インテル® EMA ウェブ・トラフィックおよび Swarm トラフィックをロードバランサーに転送するため、DNS プロバイダーにカスタムのドメイン名について CNAME レコードを作成できます。

The screenshot shows the AWS Elastic Load Balancing console. At the top, there is a table listing two load balancers:

Name	DNS name	State
ema-swarm-balancer	ema-swarm-balancer-2dd41f...	active
<b>ema-web-balancer</b>	<b>ema-web-balancer-9faa96fc...</b>	active

Below the table, the title "Load balancer: ema-web-balancer" is displayed. Underneath it, there are tabs: Description (selected), Listeners, Monitoring, Integrated services, and Tags.

The "Basic Configuration" section contains the following details:

- Name:** ema-web-balancer
- ARN:** arn:aws:elasticloadbalancing:us-west-1:802420695018:loadbalancer/net/ema-web-balancer/9faa96fc630182c2
- DNS name:** ema-web-balancer-9faa96fc630182c2.elb.us-west-1.amazonaws.com (A Record)

## 9 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 AWS\* 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。

AWS\* での Active Directory\* サービスの詳細については、以下のリンクを参照してください。

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what\\_is.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html)

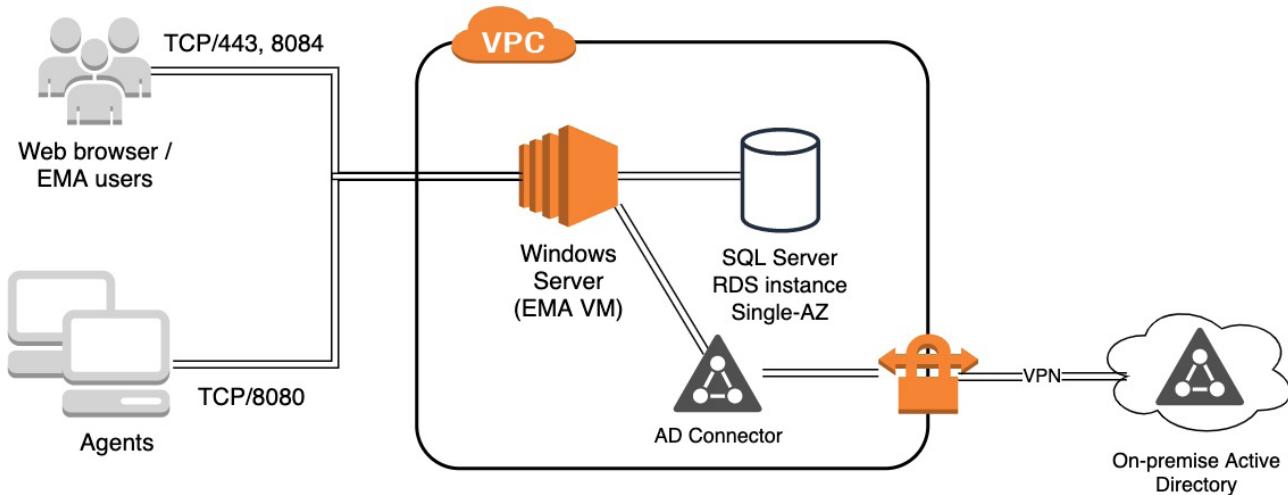
<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory\\_ad\\_connector.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html)

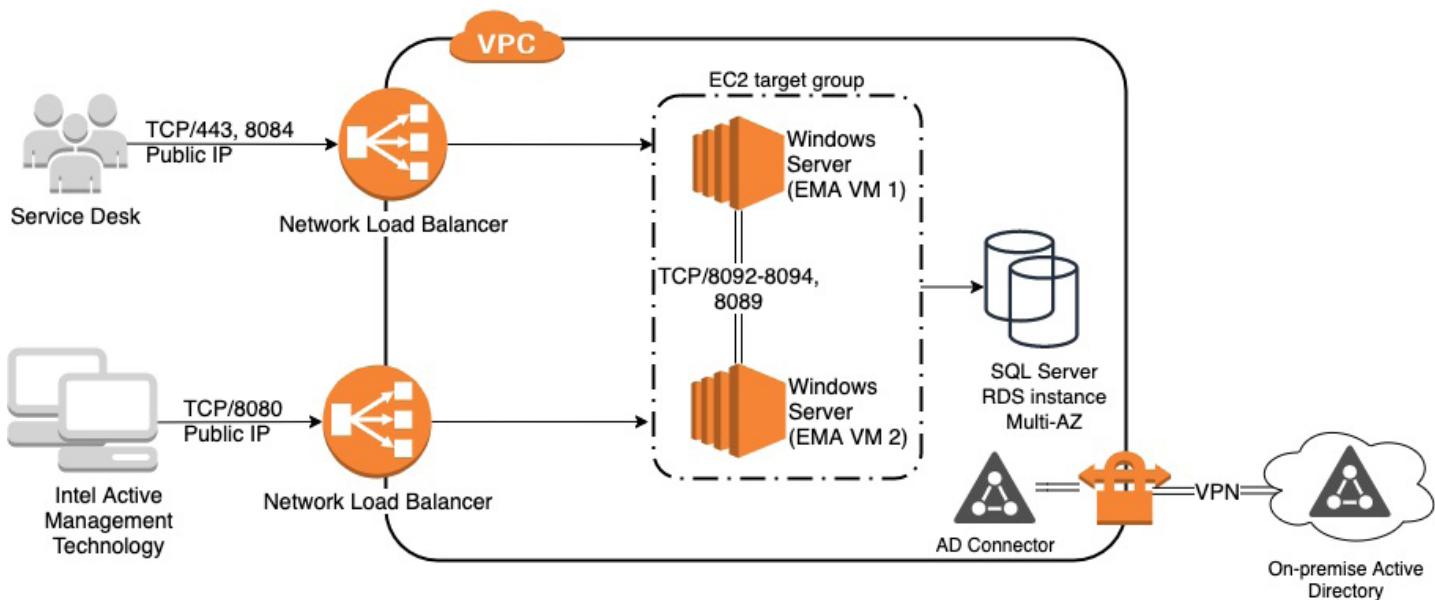
[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq\\_connector.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.html) [https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad\\_connector\\_best\\_practices.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html)

## 10 Active Directory\* 統合のアーキテクチャー図

### 10.1 シングル・サーバー・デプロイメント



### 10.2 分散サーバー・デプロイメント



### 10.3 AWS\* AD Connector を使用した Active Directory\* のクラウドへの拡張

- VPN を作成してオンプレミス・ネットワークに接続し、ドメイン・コントローラーへの接続を提供します。
  - VPN のリモート（オンプレミス）エンドを表すカスタマー・ゲートウェイを作成します。
  - VPN と VPC 間でルーティングを提供する仮想プライベート・ゲートウェイを作成します。
  - 仮想プライベート・ゲートウェイを VPC にアタッチします。
  - 新しいカスタマー・ゲートウェイと VPG を選択して、VPN 接続を作成します。

- 静的ルーティング・オプションを選択し、VPN 接続で利用できるネットワークを入力します。これには、オンプレミスのドメイン・コントローラーを含めます。
  - トンネルアドレスおよびキーは Amazon で生成できます。
- 他方の側の設定に役立てるため、VPN 接続設定をダウンロードします。
- VPC ルートテーブルを確認し、Route Propagation (ルート伝達) を有効にします。これにより、VPN 接続に関連付けられたルートが VPC ネットワークで使用できるようになります。
- オンプレミス AD のプロキシーとして働く AD Connector リソースを作成します。
  - AD Connector をディレクトリー・タイプとして選択します。
  - サポートする必要のあるオブジェクト数に適したディレクトリー・サイズを選択します。
  - VPC と 2 つの異なるサブネットを選択します。
  - 接続先のオンプレミス・ディレクトリーの情報を入力します。
    - サービスアカウントが必要なことに注意してください。
- DHCP オプションのセットを作成し、VPC と関連付け、仮想マシンが正しい DNS サーバーおよびドメイン名を受け取れるようにします。
  - Active Directory\* ドメイン名と DNS サーバーを提供します。その他のパラメーターは任意です。
  - VPC に移動し、DHCP オプションセットと関連付けます。
- EC2\* 仮想マシン・インスタンスを設定するとき、ドメイン参加のオプションを使用して、VM が自動的に AD ドメインに参加するようにします。