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

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。

目次

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、アマゾン 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

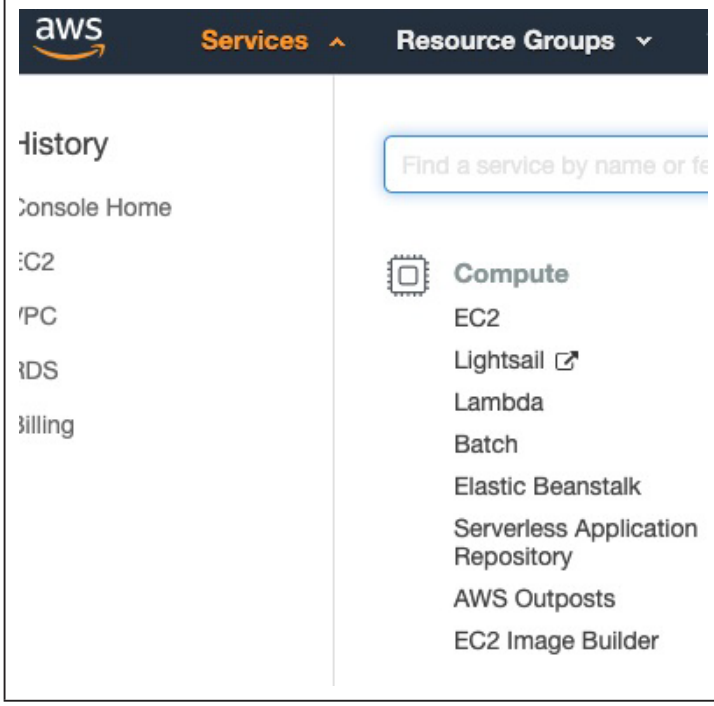
クラウド・コンピューティングとは、IT リソースをインターネットを介してオンデマンドで従量課金制で供給することです。物理的なデータセンターやサーバーを購入/所有して自身で保守管理する代わりに、クラウド・プロバイダーが提供する演算能力、ストレージ、データベースなどのテクノロジー・サービスに必要に応じてアクセスできます。現在必要な分のみをプロビジョニング可能で、その容量はビジネスの変化に応じて拡大することも縮小することも可能です。

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。

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)

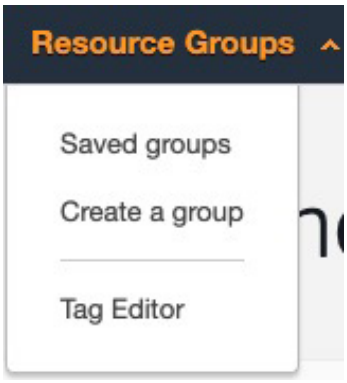


AWS* マネジメント・コンソール https://aws.amazon.com/console/ にログインすると、画面の左上に Services (サービス) メニューが表示されます。

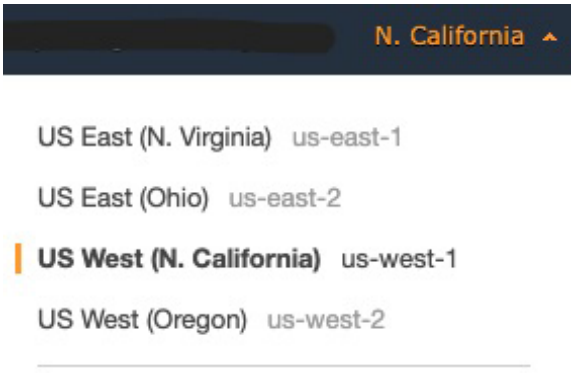
これをクリックすると、AWS* が提供するすべてのサービスのリストが、Compute (演算)、Storage (ストレージ)、Database (データベース) などのカテゴリー別に表示されます。

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

	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。 通常、デプロイしたユーザーや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。

1.2.3 リージョン

	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。 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。

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

1.4 始める前に

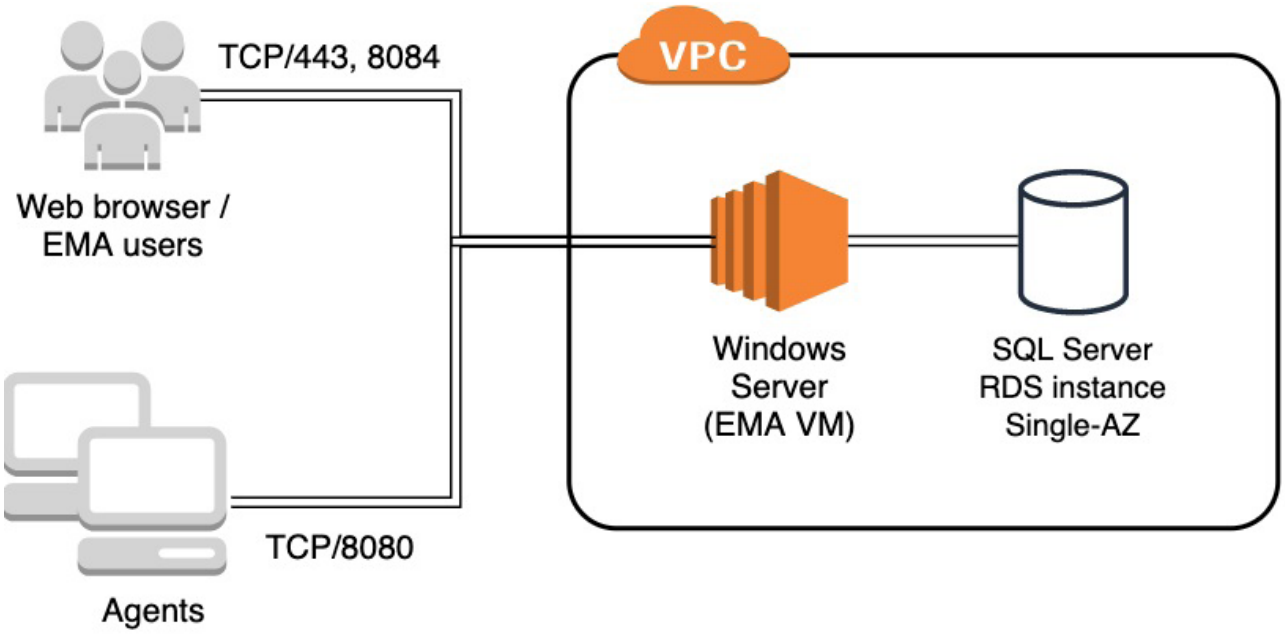
組織に既存の AWS* アカウントがある場合、クラウド管理者に依頼して、本ガイドに記載されたすべてのリソースを作成するのに十分なアクセス権を付与してもらう必要があります。

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。

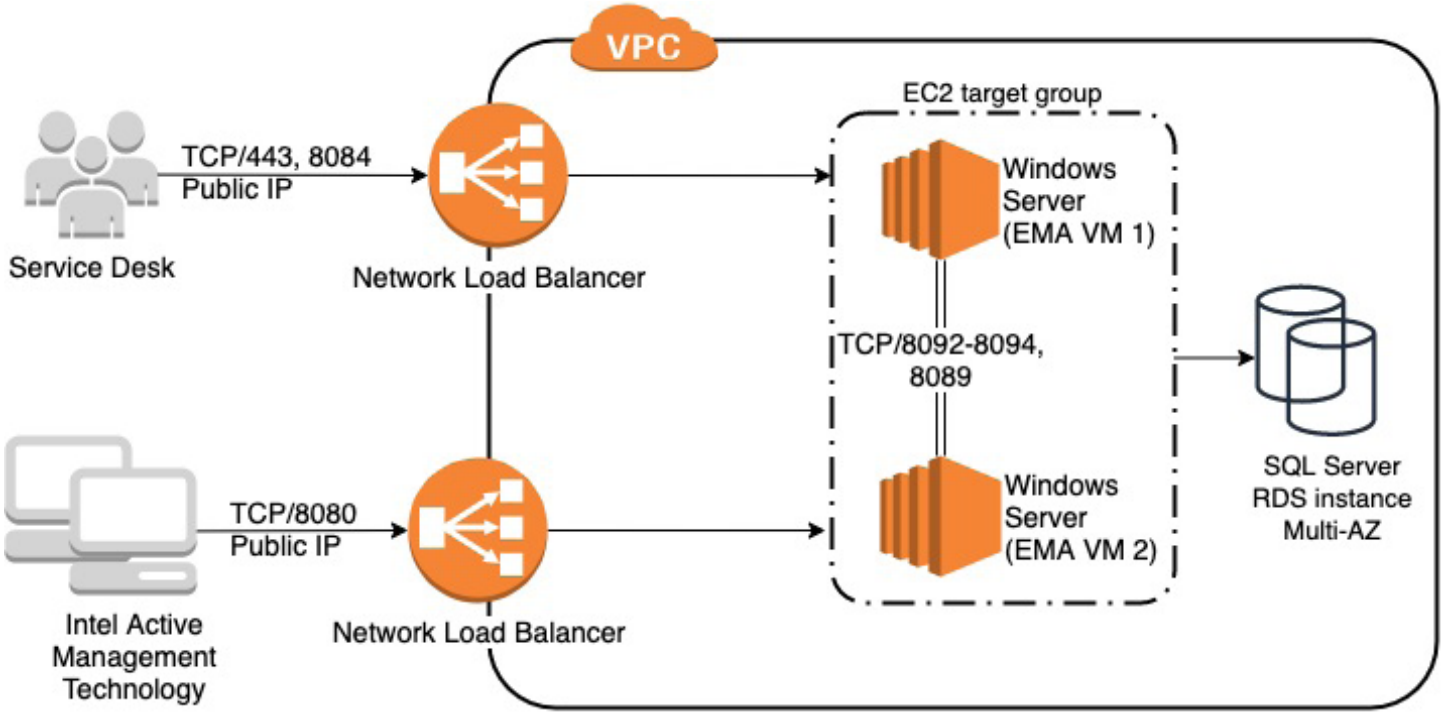
使用すべきアドレス空間があるか、ネットワーク管理者に確認します。クラウド・プロバイダーへの VPN がすでに確立している場合や将来的にその予定がある場合に、企業ネットワークとの重複を防ぎ、ルーティングの問題を防止できます。また、組織からクラウドにアクセスするトラフィックの送信元 IP アドレスについても確認が必要です。これにより、インターネットからの信頼できるネットワークのみをインテル® EMA の仮想マシンに許可することができます。

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

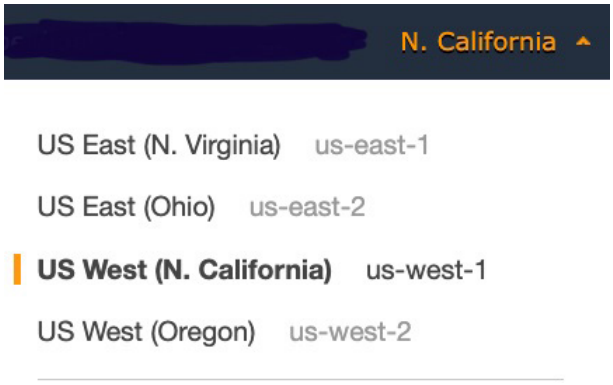


2.2 分散サーバー・デプロイメント



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。



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

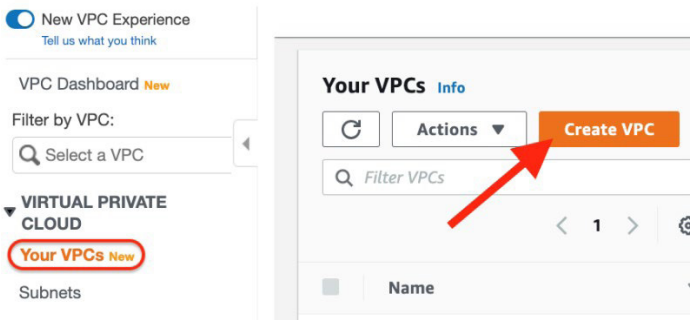
4.2 VPC の作成

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

	**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。

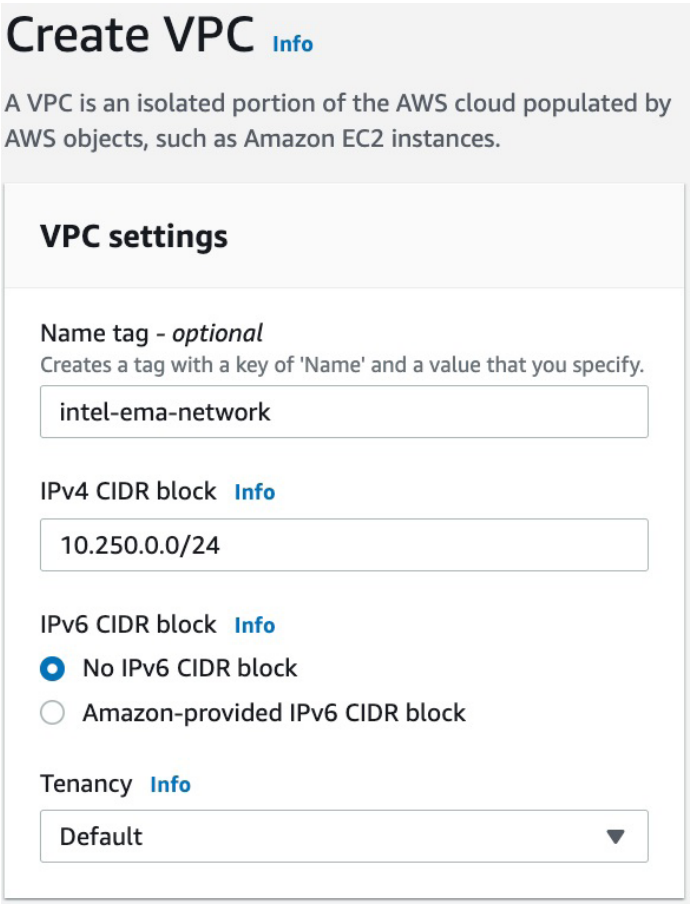
4.2.2 VPC の作成



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



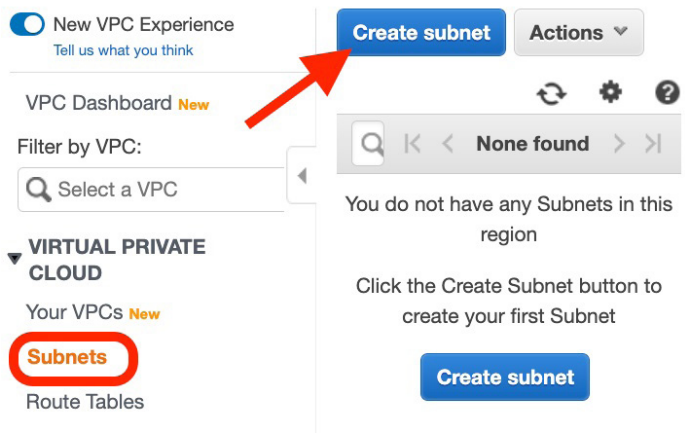
ネットワークの詳細情報を次のように入力します。

- **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。

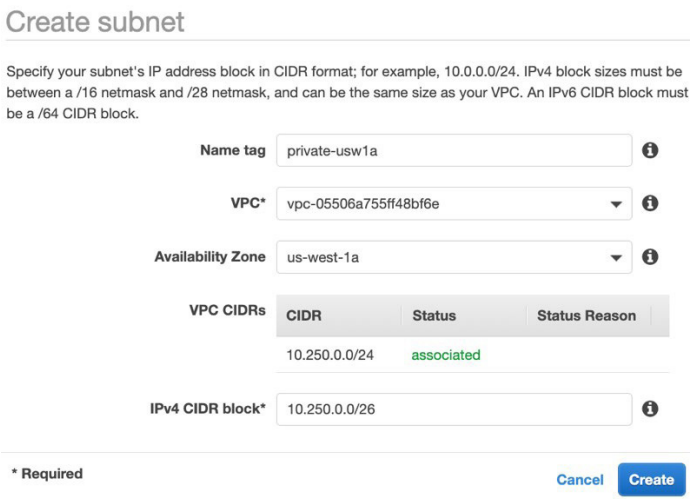
4.3 サブネットの作成

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

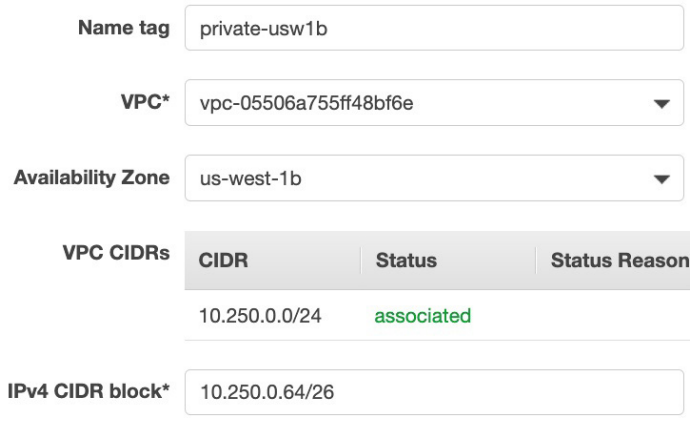


Create subnet（サブネットを作成）ボタンをクリックします。サブネットを以下のように設定します。

- **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



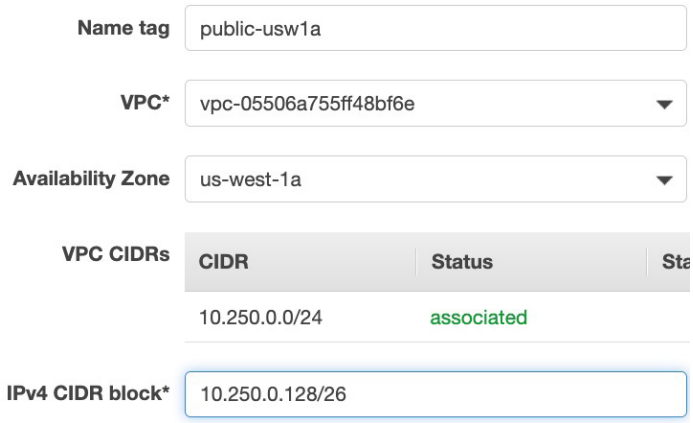
Create subnet（サブネットを作成）ボタンをクリックします。

サブネットを以下のように設定します。

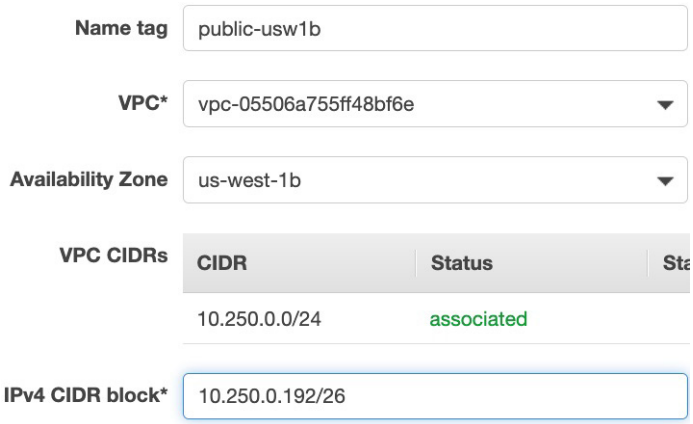
- **Name tag（Name タグ）：**一意のサブネット名を指定します。
  例：*private-usw1b*
- **VPC：**先ほど作成した仮想ネットワークを選択します。
- **Availability Zone（アベイラビリティー・ゾーン）：**今回の設計では 2 つの個別のゾーンを使用するため、2 つ目に選択したゾーンをここで使用します。
  例：*us-west-1b*

	• **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 : *10.250.0.64/26* **Create (作成)** ボタンをクリックします。

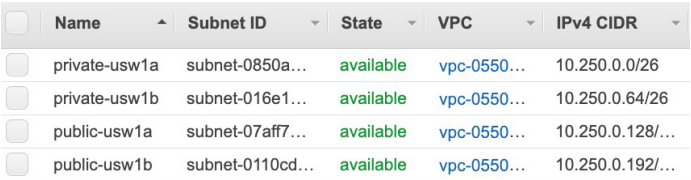
4.3.4 1 つ目のパブリックサブネットの作成

	**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 : *public-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 : *10.250.0.128/26* **Create (作成)** ボタンをクリックします。

4.3.5 2 つ目のパブリックサブネットの作成

	**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* • **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 : *10.250.0.196/26* **Create (作成)** ボタンをクリックします。

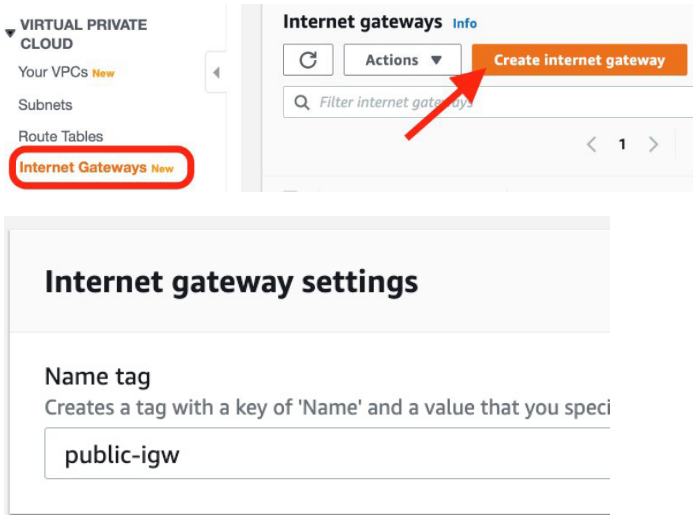
4.3.6 サブネットの確認

	サブネットのリストを確認します。4 つのサブネットが作成されているはずです。

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



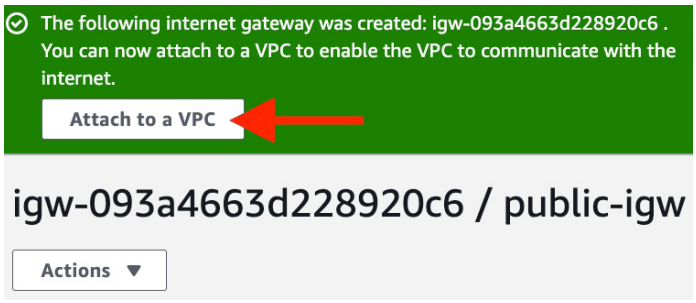
VPC のサイドバーから **Internet Gateways (インターネット・ゲートウェイ)** を選択します。

Create Internet gatway (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*

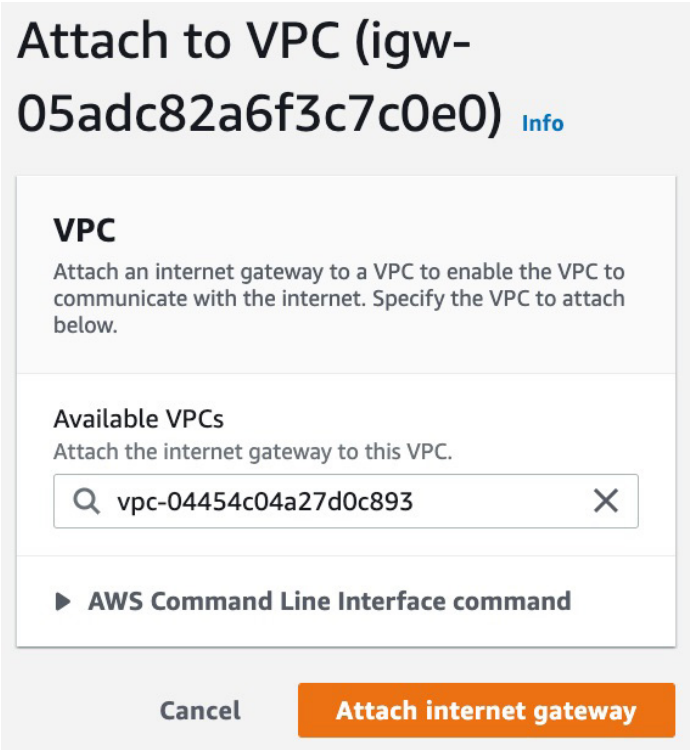
画面下部にある **Create Internet gateway (インターネット・ゲートウェイの作成)** ボタンをクリックして完了します。

4.4.2　VPC へのインターネット・ゲートウェイのアタッチ



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



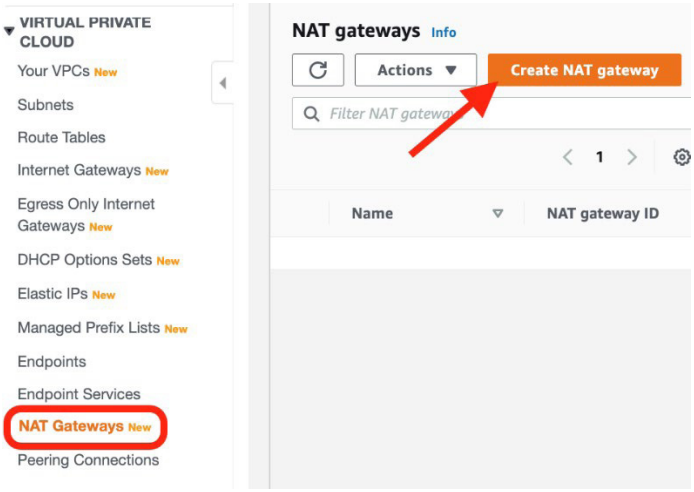
先ほど作成した VPC を選択します。

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

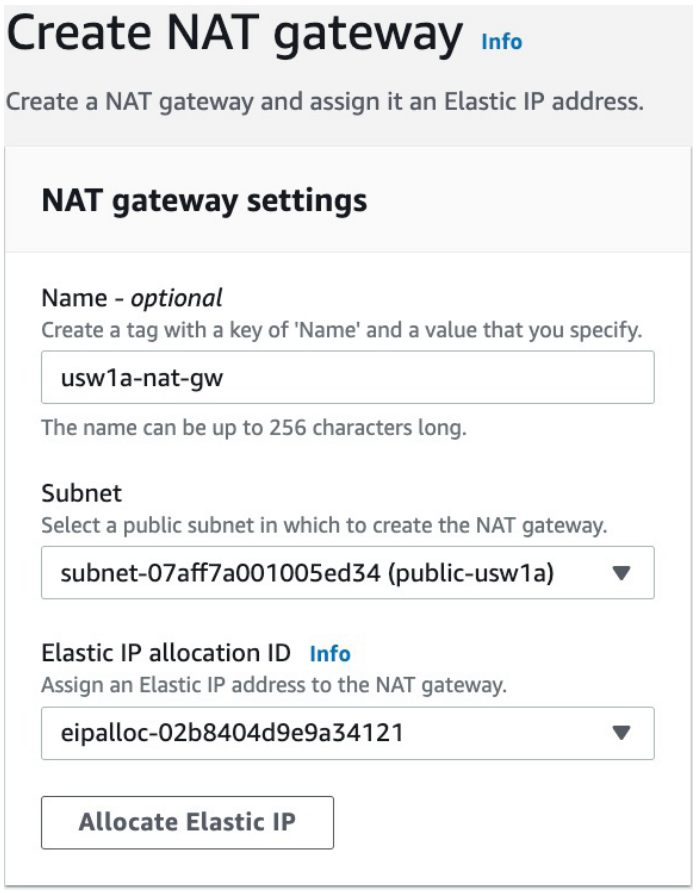
NAT ゲートウェイは、リソースがアウトバウンド・インターネット・トラフィックの送信ポイントとしてゾーン内で使用できるゾーンリソースです。NAT ゲートウェイはアドレス変換を実行し、トラフィックを VPC 内のインターネット・ゲートウェイに転送します。ここでは、1 つがダウンしても接続が保たれるよう、2 つのアベイラビリティー・ゾーンに対して 1 つずつ作成します。

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



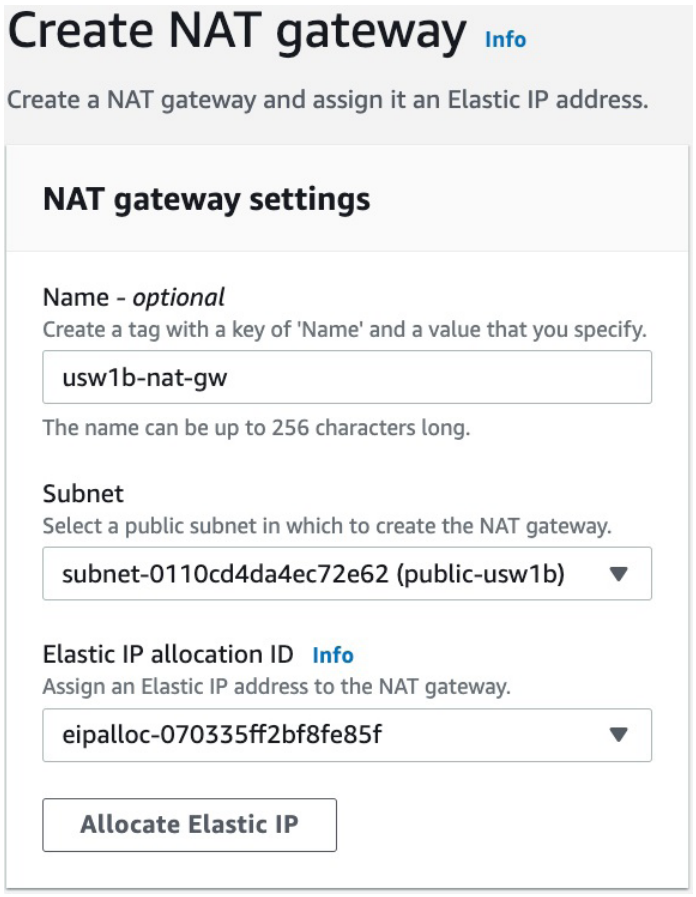
Create NAT gateway（NAT ゲートウェイの作成）ボタンをクリックします。

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：*usw1a-nat-gw*
- **Subnet（サブネット）：**1 つ目のパブリックサブネットを選択します。
  例：*public-usw1a*
- **Elastic IP allocation ID（Elastic IP 割り当て ID）：**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。

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。

4.5.3　2 つ目の NAT ゲートウェイの作成



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。

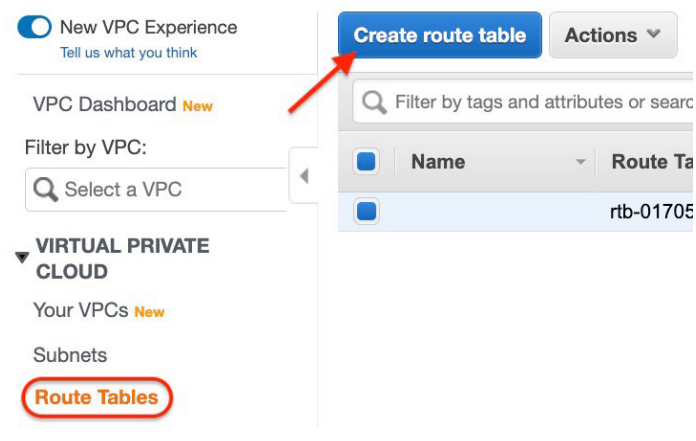
- **Name**（オプション）：一意のゲートウェイ名を入力します。
  例：*usw1b-nat-gw*
- **Subnet（サブネット）：**2 つ目のパブリックサブネットを選択します。
  例：*public-usw1b*
- **Elastic IP allocation ID（Elastic IP 割り当て ID）：**Allocate Elastic IP（Elastic IP を割り当て）ボタンをクリックすると、このフィールドに値が自動で表示されます。

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



4.6.2　パブリックサブネット用ルートテーブルの作成

Create route table（ルートテーブルを作成）ボタンをクリックします。

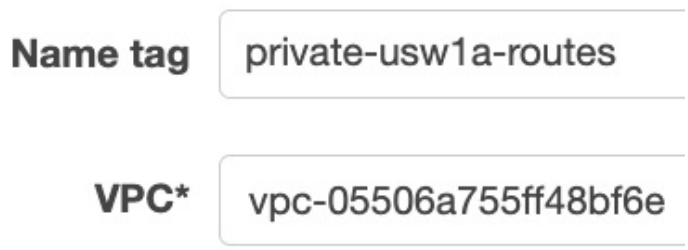
ルートテーブルを以下のように設定します。

- **Name tag（Name タグ）：**一意のルートテーブル名を入力します。
  例：*public-usw-routes*
- **VPC：**先ほど作成した仮想ネットワークを選択します。

Create（作成）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。

4.6.3　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



Create route table（ルートテーブルを作成）ボタンをクリックします。

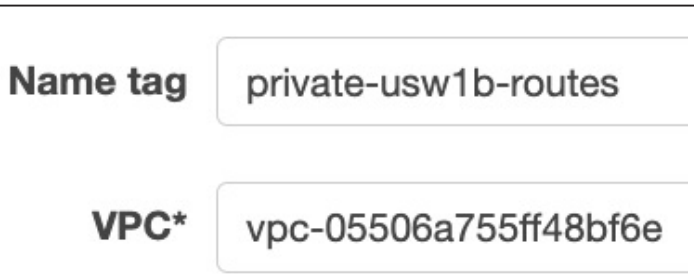
ルートテーブルを以下のように設定します。

- **Name tag（Name タグ）：**一意のルートテーブル名を入力します。
  例：*private-usw1a-routes*
- **VPC：**先ほど作成した仮想ネットワークを選択します。

Create（作成）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。

4.6.4　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



Create route table（ルートテーブルを作成）ボタンをクリックします。

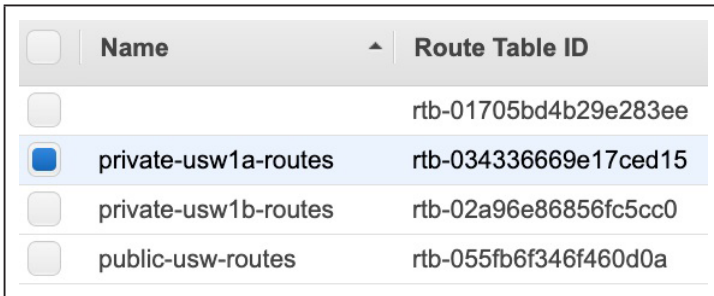
ルートテーブルを以下のように設定します。

- **Name tag（Name タグ）：**一意のルートテーブル名を入力します。
  例：*private-usw1b-routes*
- **VPC：**先ほど作成した仮想ネットワークを選択します。

Create（作成）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。

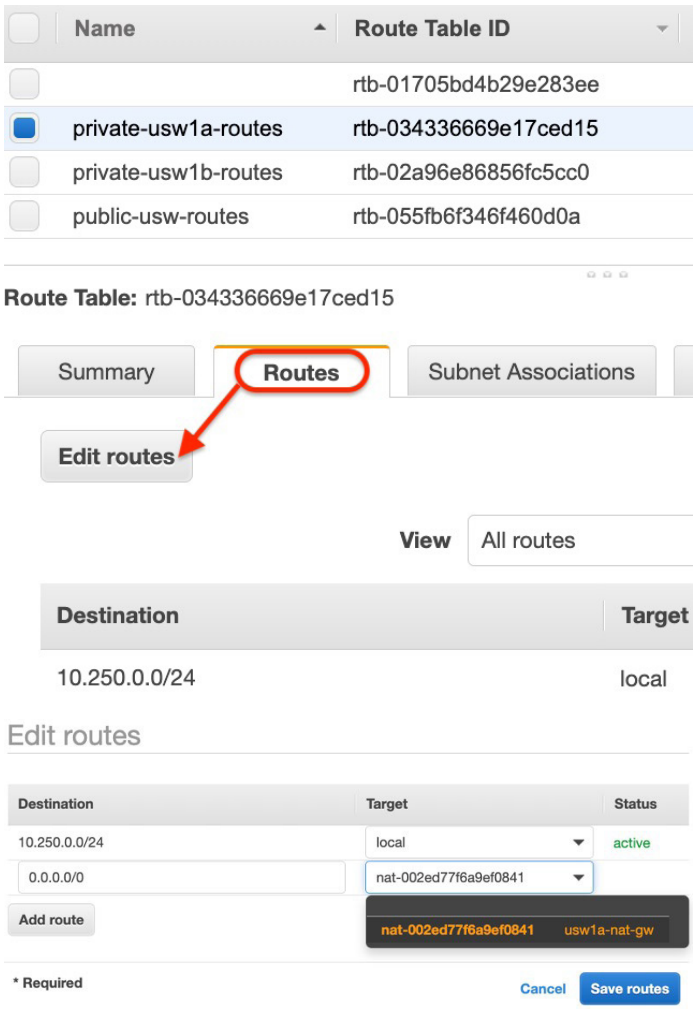
4.6.5　ルートテーブルのリストの確認



Name	Route Table ID
	rtb-01705bd4b29e283ee
private-usw1a-routes	rtb-034336669e17ced15
private-usw1b-routes	rtb-02a96e86856fc5cc0
public-usw-routes	rtb-055fb6f346f460d0a

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。

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



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 **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。

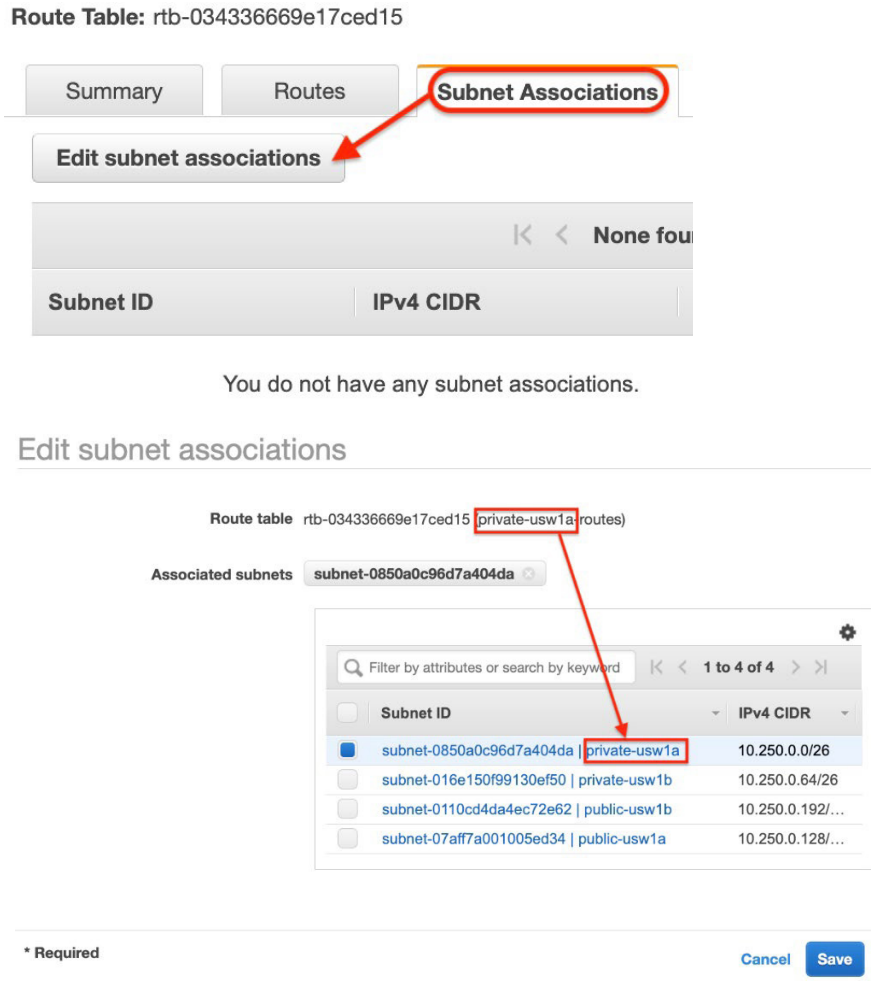
Add route（ルートを追加） ボタンをクリックして、以下の値を設定します。

- **Destination（送信先）：** *0.0.0.0/0*
- **Target（ターゲット）：** 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*

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。

4.6.7　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



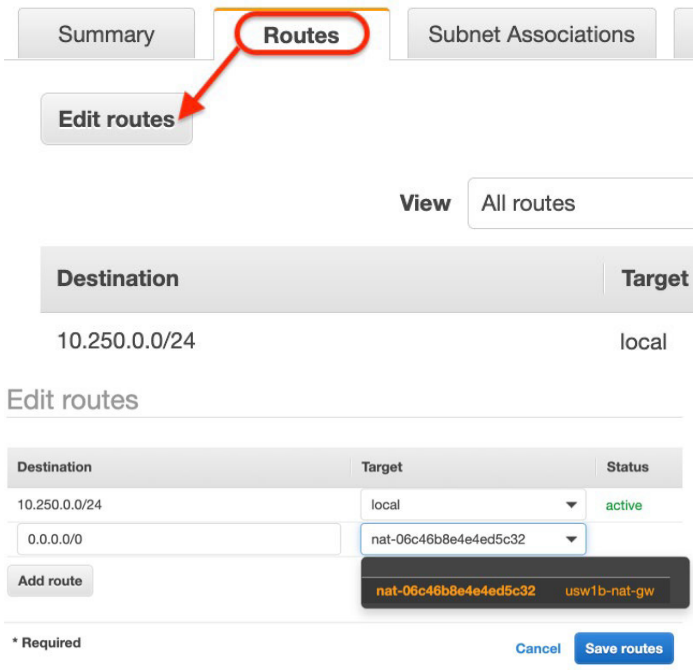
Subnet Associations（サブネット関連付け）タブを選択します。

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



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：*private-usw1b-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。

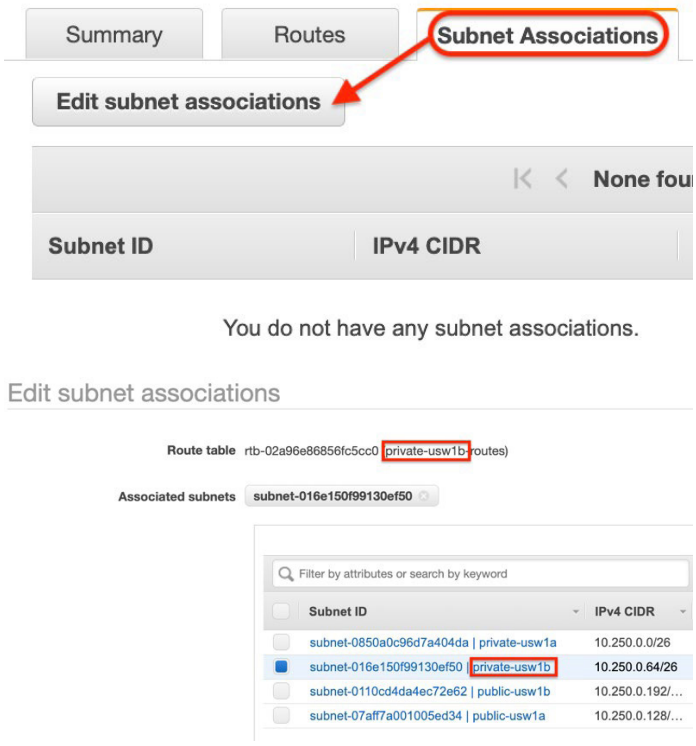
Add route（ルートを追加）ボタンをクリックして、以下の値を設定します。

- **Destination（送信先）：** *0.0.0.0/0*
- **Target（ターゲット）：** 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：*usw1b-nat-gw*

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。

4.6.9　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



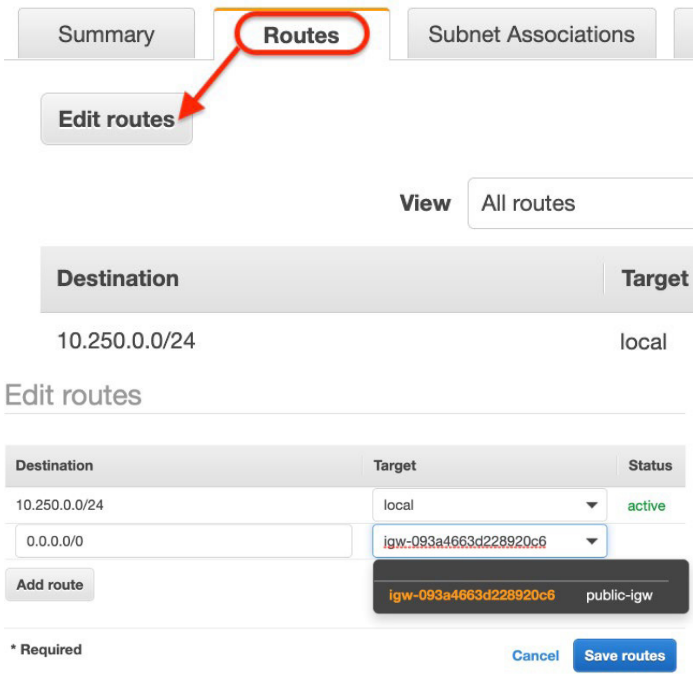
Subnet Associations（サブネット関連付け）タブを選択します。

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 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。

Save（保存）ボタンをクリックします。

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



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。

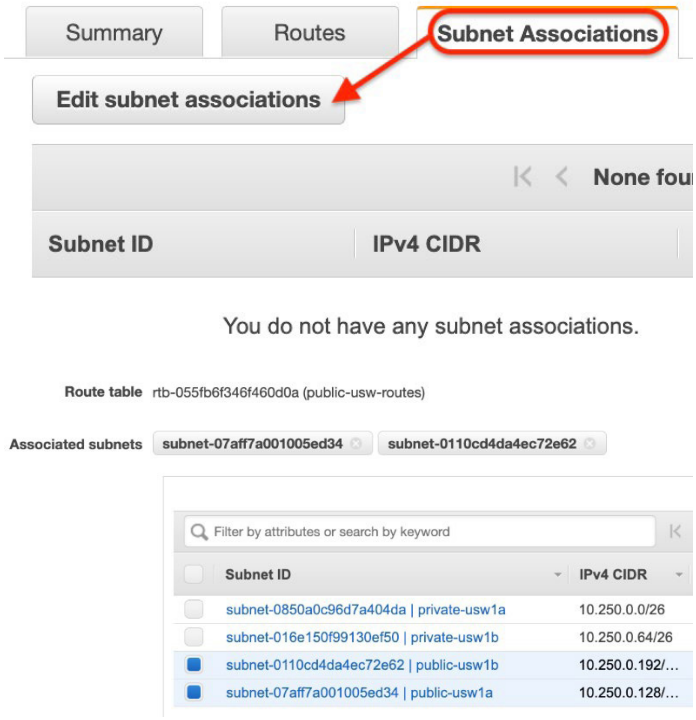
Add route（ルートを追加） ボタンをクリックして、以下の値を設定します。

- **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



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すぎることなく、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。

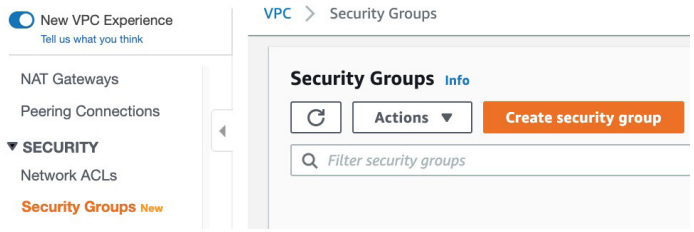
以下の手順では、インテル® EMA VM へのアクセスを制御するセキュリティー・グループを作成します。また、データベースへのアクセスを制御する別のグループも作成す。

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

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。

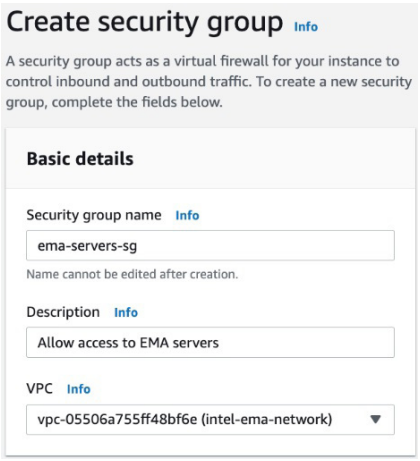
4.7.1.1 セキュリティー・グループの作成



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。

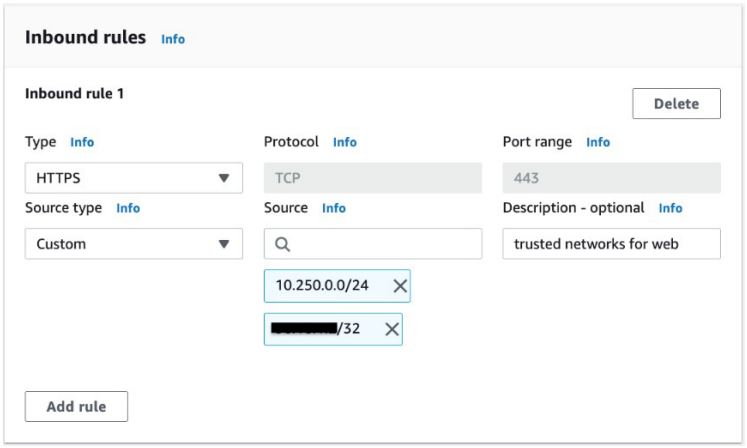
4.7.1.2 セキュリティー・グループの基本情報の設定



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。

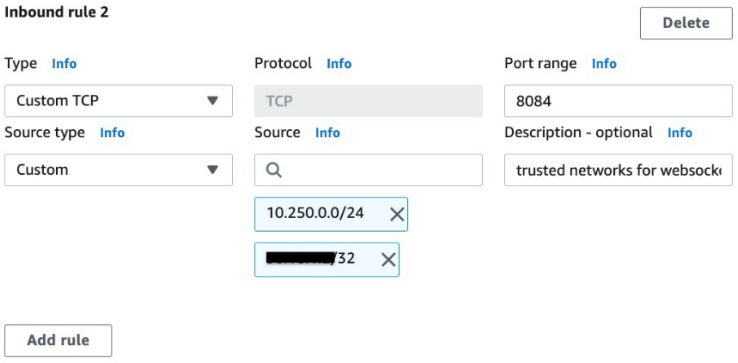
4.7.1.3 ウェブ・トラフィック用のインバウンド・ルールの追加



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）。

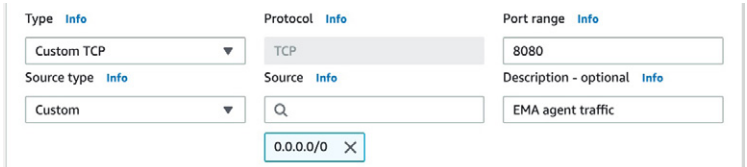
4.7.1.4 WebSocket トラフィック用のインバウンド・ルールの追加



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）。

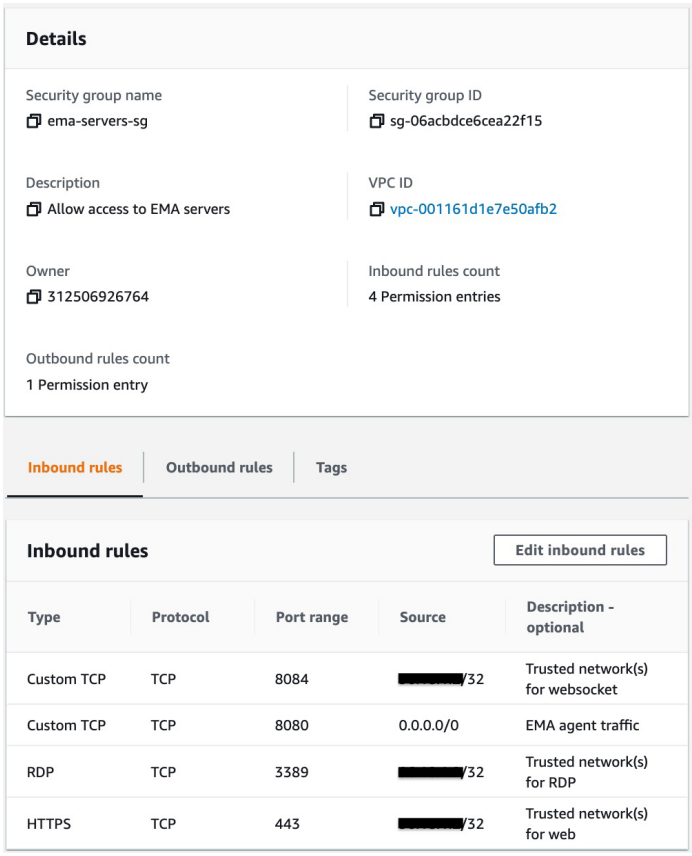
4.7.1.5 Swarm トラフィック用のインバウンド・ルールの追加



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



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。

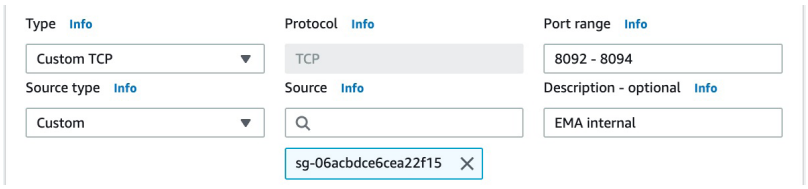
ルールリストが正しいか確認します。

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。

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。

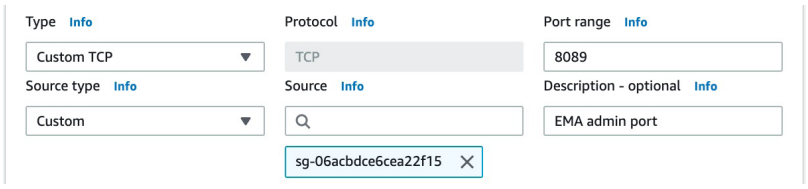
4.7.2.1 ポート 8092 ~ 8094 に対する内部トラフィック用のインバウンド・ルールの追加



以下の設定を持つインバウンド・ルールを追加します。

- **Type (タイプ) :** *Custom TCP* (カスタム TCP)
- **Port range (ポート範囲) :** *8092-8094*
- **Description (説明) :** インテル® EMA 内部
- **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。

4.7.2.2 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。

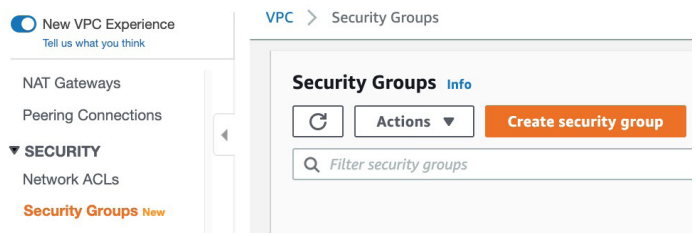
Save rules (ルールを保存) ボタンをクリックします。ルールが正しいか確認します。

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

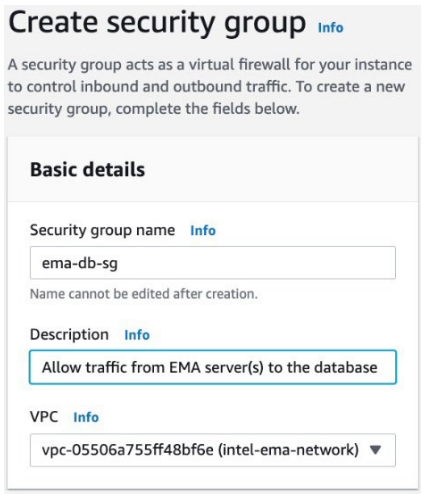
4.7.3.1 セキュリティー・グループの作成



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。

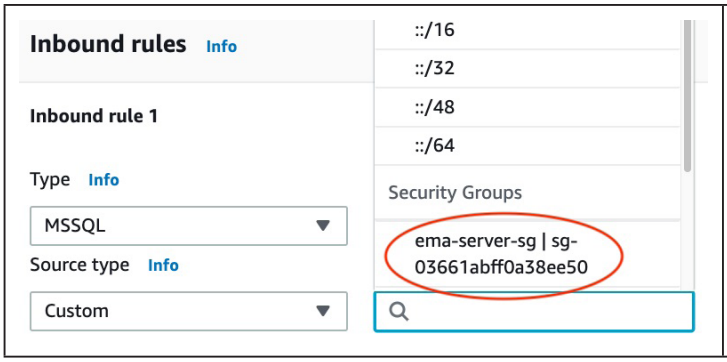
4.7.3.2 セキュリティー・グループの基本情報の設定



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フィックの許可
- **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



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。

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。

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 つだけで、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、前章で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

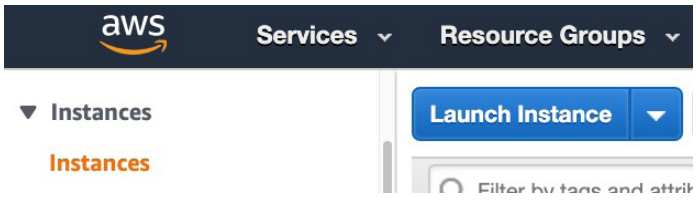
5.2 仮想マシンの作成

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

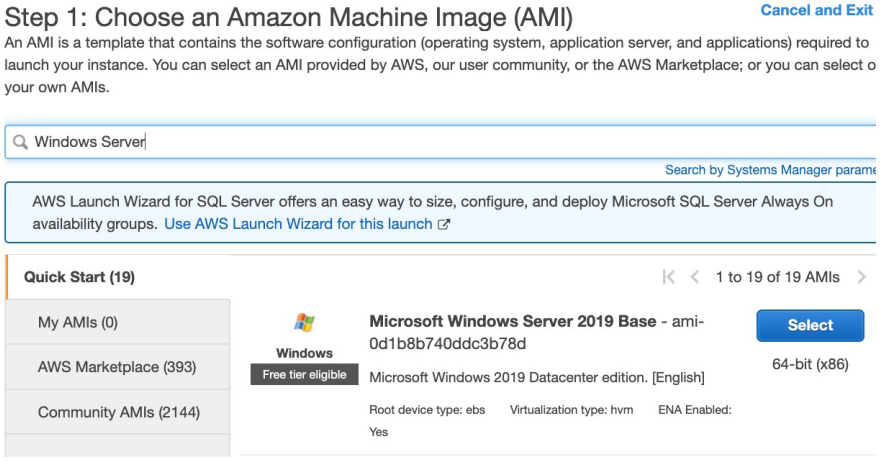
Services (サービス) メニューの **Compute (コンピュート)** セクションで、**EC2*** を選択します。

5.2.2 EC2* インスタンスの起動



サイドバーで **Instances (インスタンス)** を選択し、**Launch Instance (インスタンスを起動)** ボタンをクリックします。

5.2.3 Amazon マシンイメージ(AMI)の選択

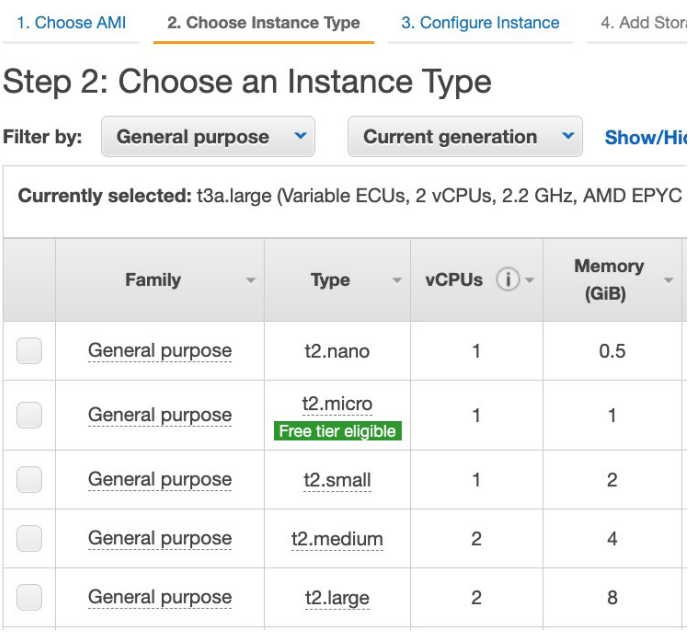


インテル® EMA でサポートされる最新の Microsoft* Windows Server* のベースイメージを検索します。

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

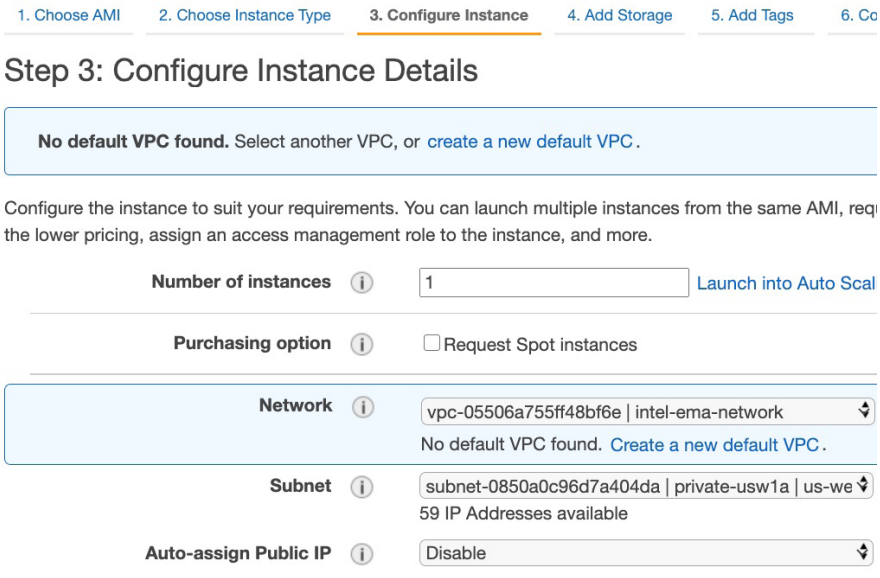


必要な CPU およびメモリーリソースを持つマシンタイプを選択します。マシンタイプは、必要に応じて、インスタンスをオフにしたときに変更できます。

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



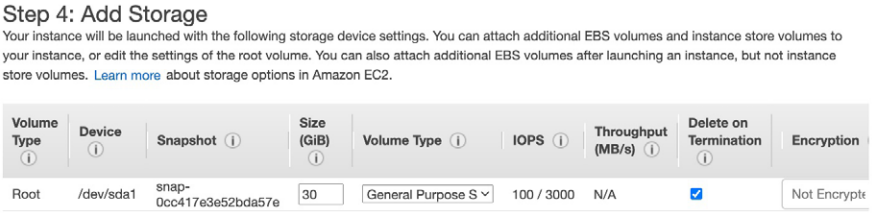
インスタンスの詳細を以下のように設定します。

- **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）：** *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。

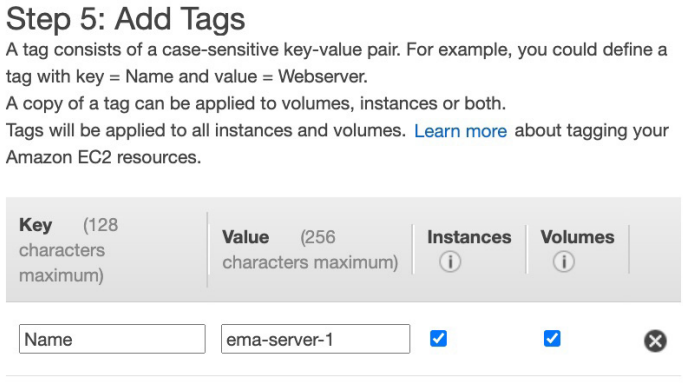
5.2.6 ストレージの追加



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

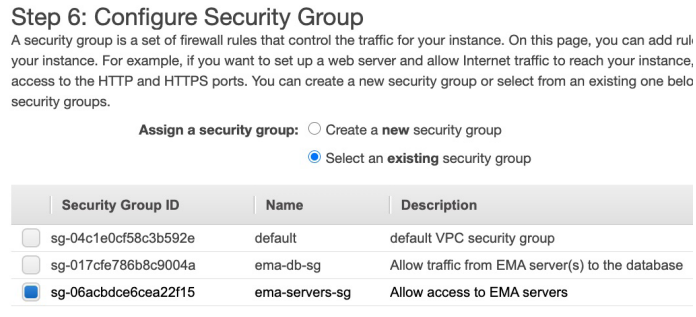


Key（キー）に「Name」、Value（値）に目的のサーバー名を指定したタグを追加します。

「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：セキュリティー・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



Assign a security group (セキュリティー・グループを割り当てる) 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。

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*

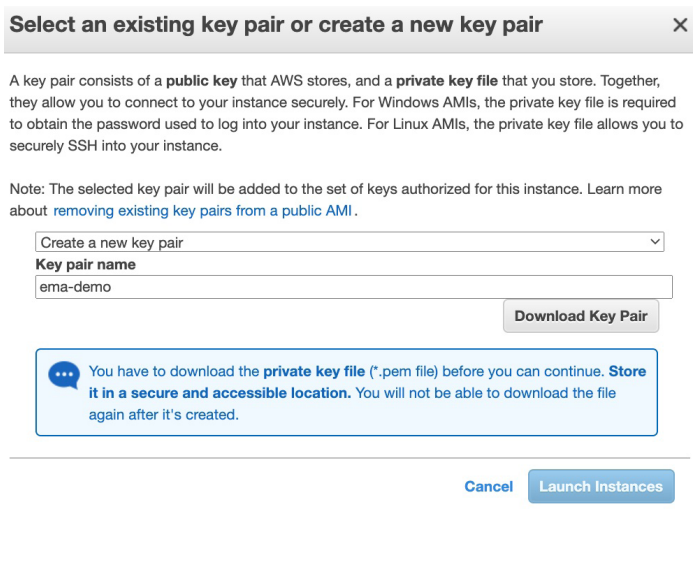
Next: Review and Launch (次へ：確認して起動する) ボタンをクリックします。

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。

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



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。

リストから適切なキーペアを選択するか、**Create a new key pair (新しいキーペアを作成する)** を選択して、**Download Key Pair (キーペアをダウンロード)** 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。

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。

Launch Instances (インスタンスを起動) ボタンをクリックします。

5.3 2 つ目の EC2* インスタンスの作成 (分散サーバーのみ)

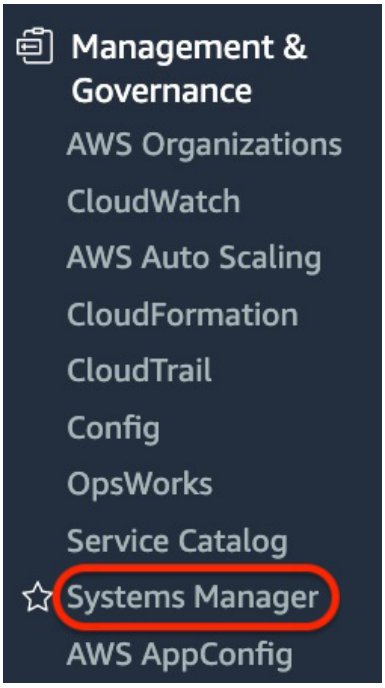
分散サーバー・デプロイメントでは、2 つ目のインテル® EMA サーバーを作成するため、前の手順を繰り返します。ただし、前回とは別のサブネットを選択し、別の Name タグ (*ema-server-2* など) を指定します。

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/

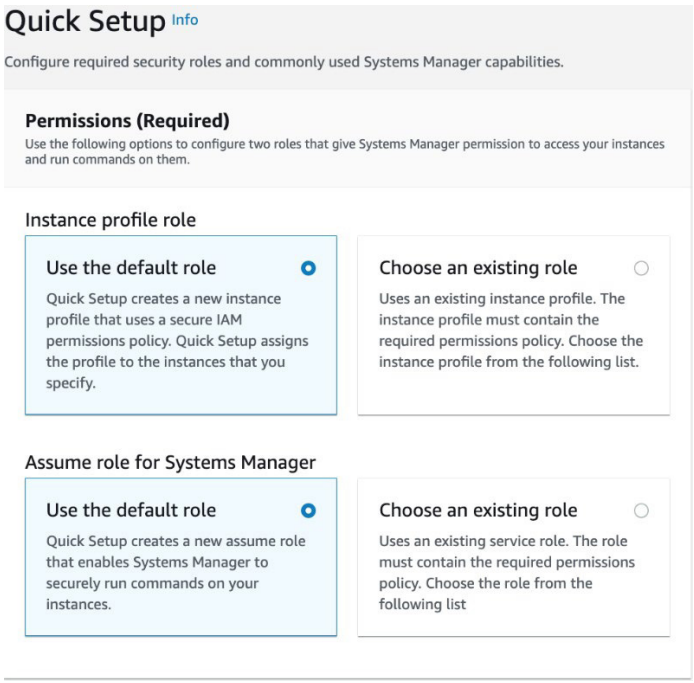
6.1 Systems Manager サービスへの移動

	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、**Systems Manager** を選択します。

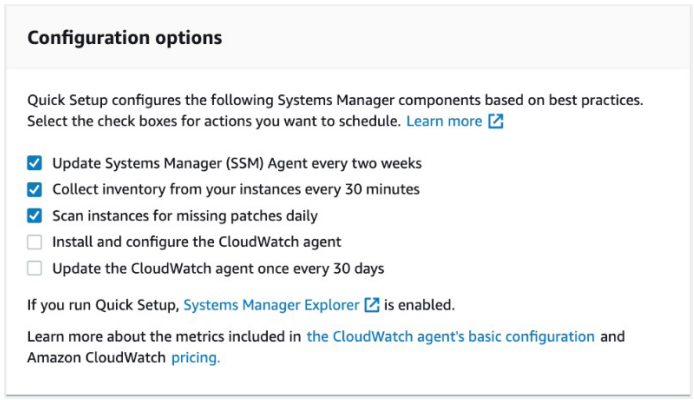
6.2 Quick Setup (高速セットアップ) の開始

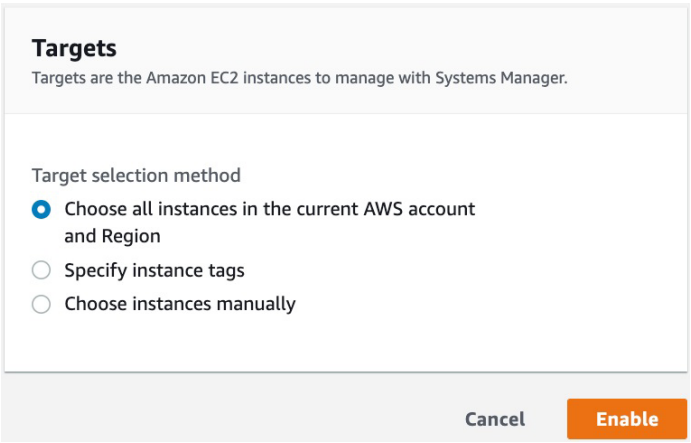
6.3 Permissions（アクセス許可）オプションの選択



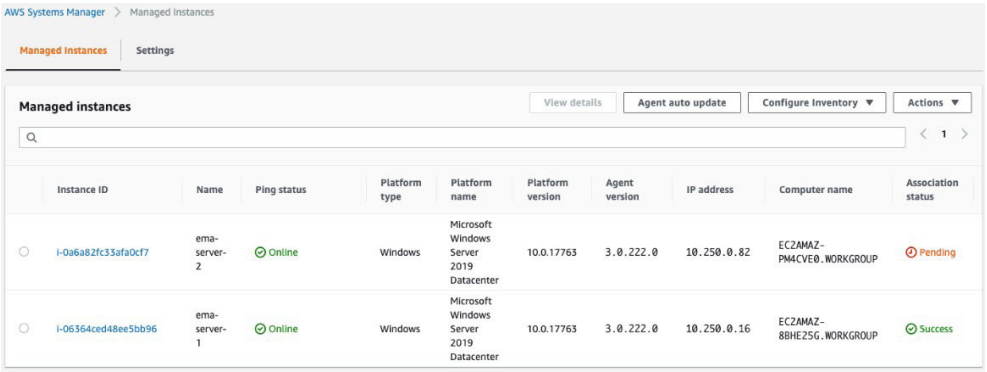
6.4 Configurations（設定）オプションの選択



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



Systems Manager のサイドバーから **Managed Instances（マネージド・インスタンス）**を選択します。

高速セットアップを初めて実行した後は、リストに仮想マシンが表示されるまで数分かかることがあります。

VM の System Manager への登録が正常に完了すると、このリストに表示されます。

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・スパ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。

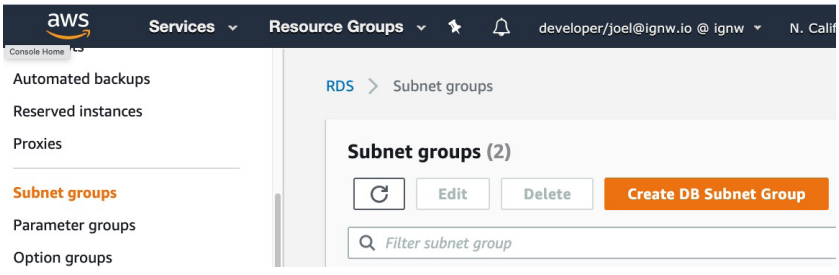
RDS の詳細については、以下のリンクを参照してください。
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

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

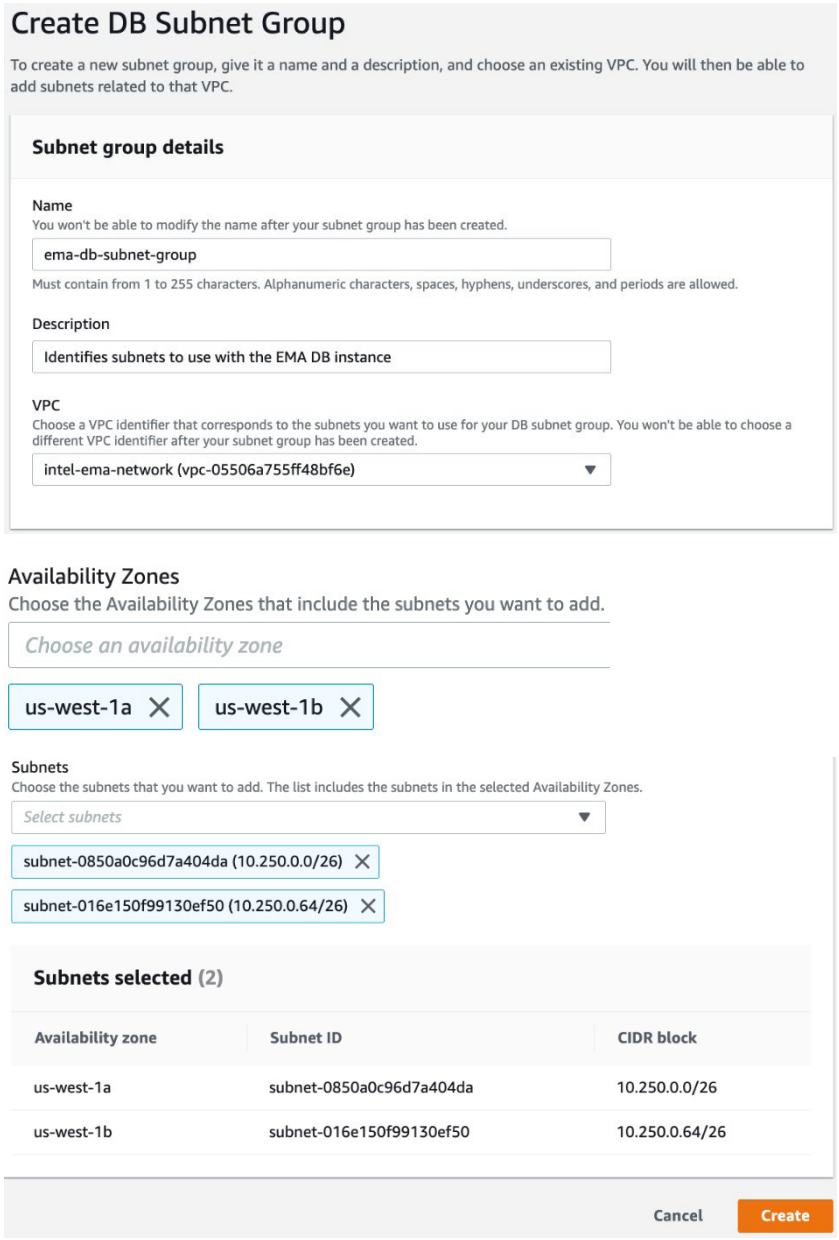
Services (サービス) メニューの **Database (データベース)** で、**RDS** を選択します。

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

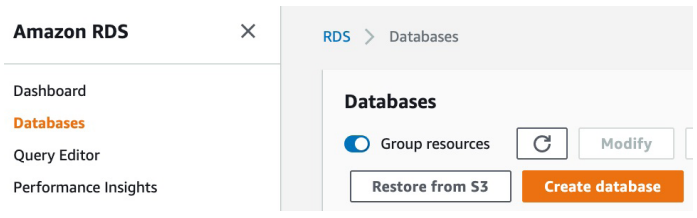


サブネットグループの詳細情報を以下のように入力します。

- **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。

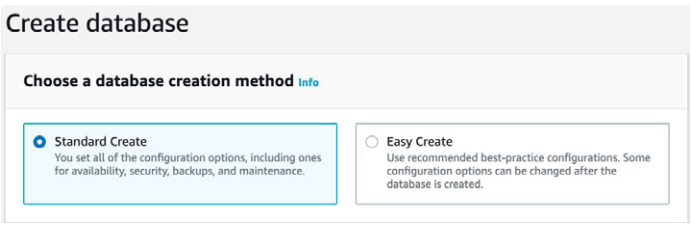
Create（作成）ボタンをクリックします。

7.3 データベースの作成



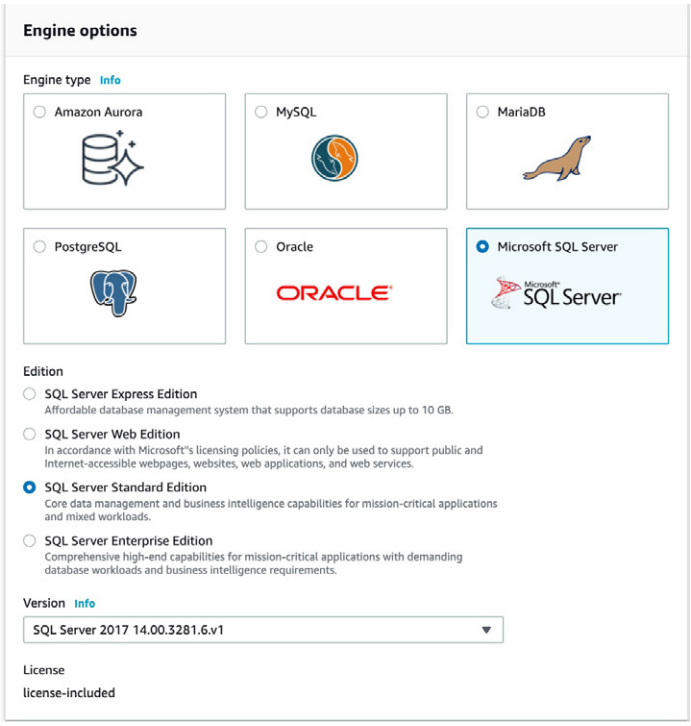
RDS サイドバーから Databases（データベース）を選択し、**Create database（データベースを作成）**ボタンをクリックします。

7.3.1 データベース作成方法の選択



データベース作成方法として **Standard Create（標準作成）**を選択します。

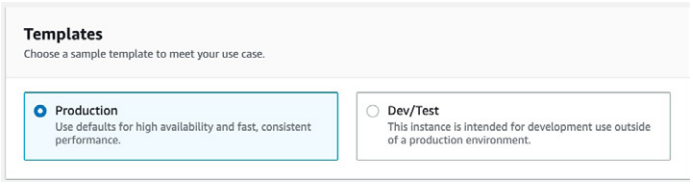
7.3.2 エンジンタイプとエディションの選択



Microsoft* SQL Server* エンジンを選択します。

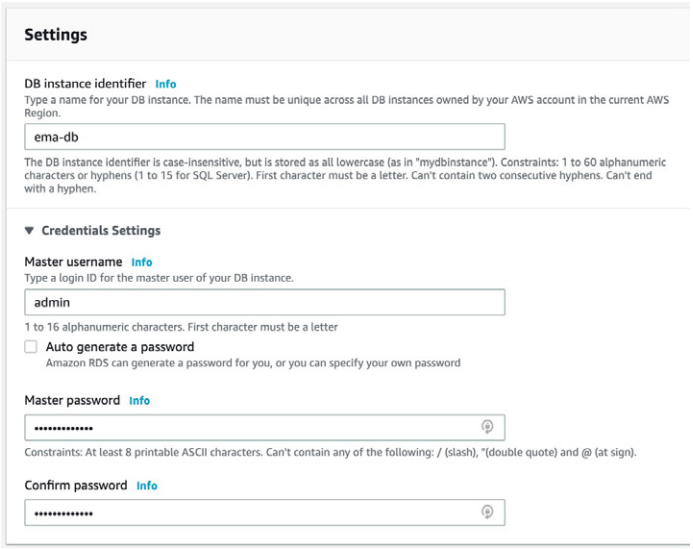
適切な SQL サーバー・エディションを選択します。本ガイドの目的上、本番環境では SQL Server* Standard Edition が使用されているものと仮定します。デプロイおよびテスト目的には、コスト削減のために SQL Server* Express Edition を使用できます。

7.3.3 デプロイメント・テンプレートの選択



Templates（テンプレート）で、**Production（本番稼働用）**を選択します。

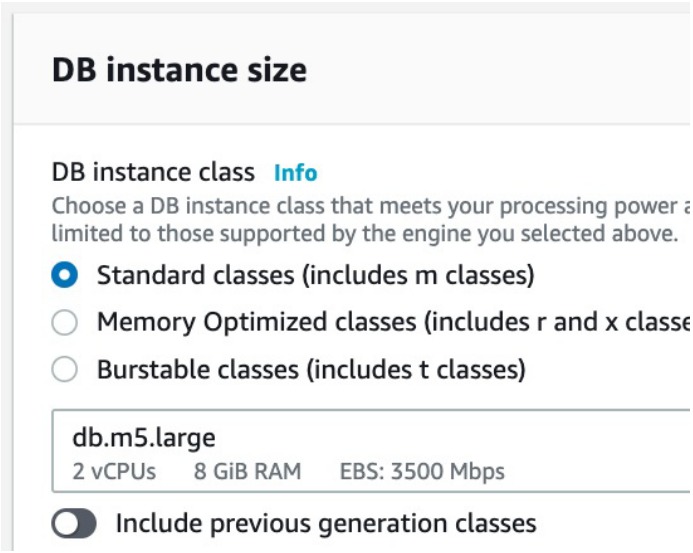
7.3.4　インスタンス名とマスターユーザー資格情報の設定



データベースに一意の名前を付けます。
例：*ema-db*

ユーザー名とパスワードの作成

7.3.5　DB インスタンス・サイズの設定

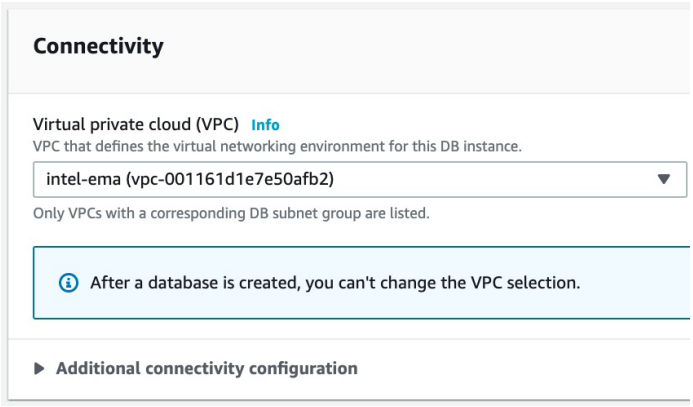


適切なリソースが提供されるよう、DB インスタンス・クラスを設定します。
推奨：*db.m5.large*

7.3.6　ストレージの設定 (オプション)

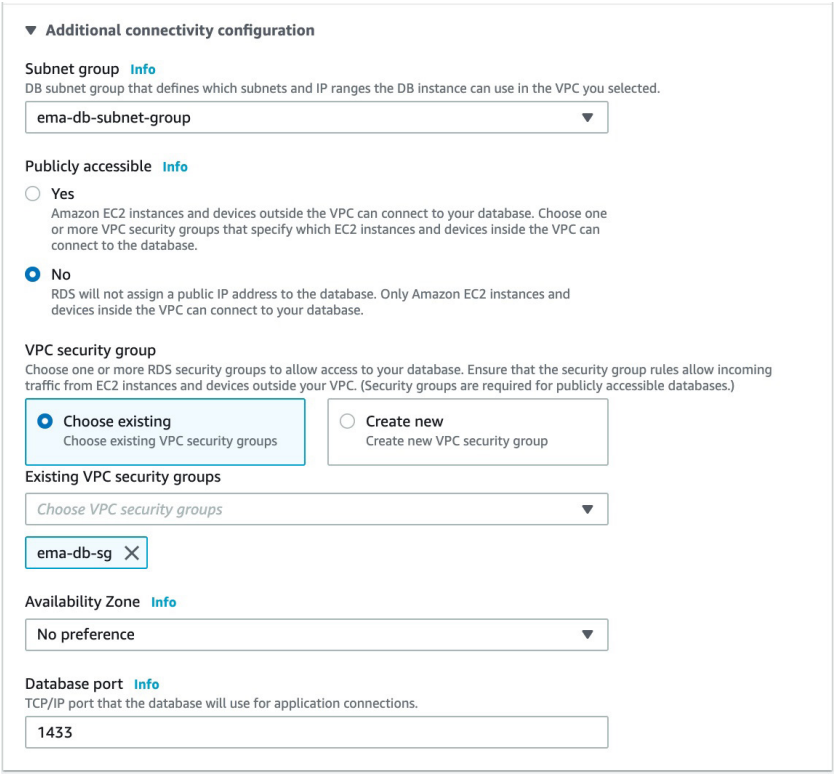
割り当てられたデフォルトのストレージ容量を、必要に応じて増加させることができます。ここではデフォルトのままにします。ストレージ容量は後から増加させることができます。

7.3.7 接続の設定



Connectivity (接続) で、前に作成した VPC を選択し、**Additional connectivity configuration(追加の接続設定)**セクションを展開します。

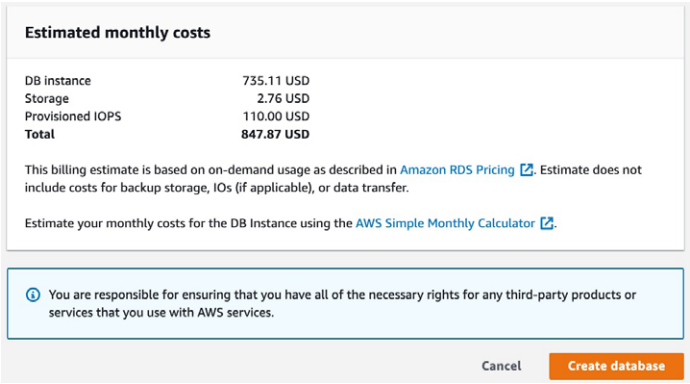
7.3.8 接続の設定 - Additional Connectivity Configuration (追加の接続設定)



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。

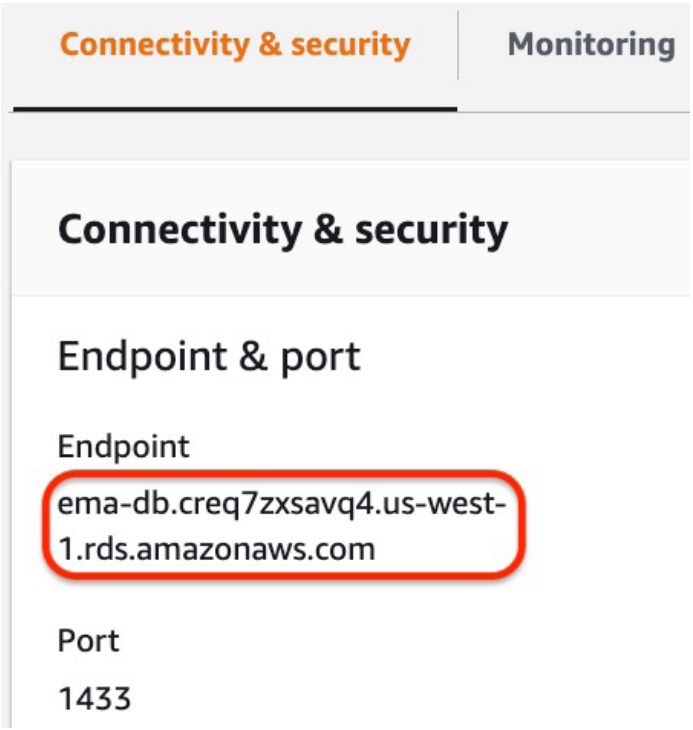
デフォルトの VPC セキュリティー・グループの選択を解除し、先ほどデータベース用に作成した既存のセキュリティー・グループを選択します。

7.3.9 確認と作成



コスト見積もりを確認し、**Create database (データベースを作成)** ボタンをクリックします。

7.4 データベースのホスト名の取得



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。

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。

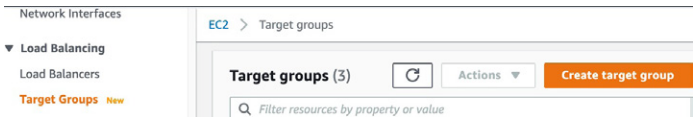
ロードバランサーには、各 AZ 内の関連するロードバランサーの外部公開されたアドレスをポイントするホスト名が自動生成されます。インテル® EMA サーバーにアクセスするカスタムのドメインを使用するため、このホスト名をエイリアスする DNS CNAME レコードを作成する必要があります。

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

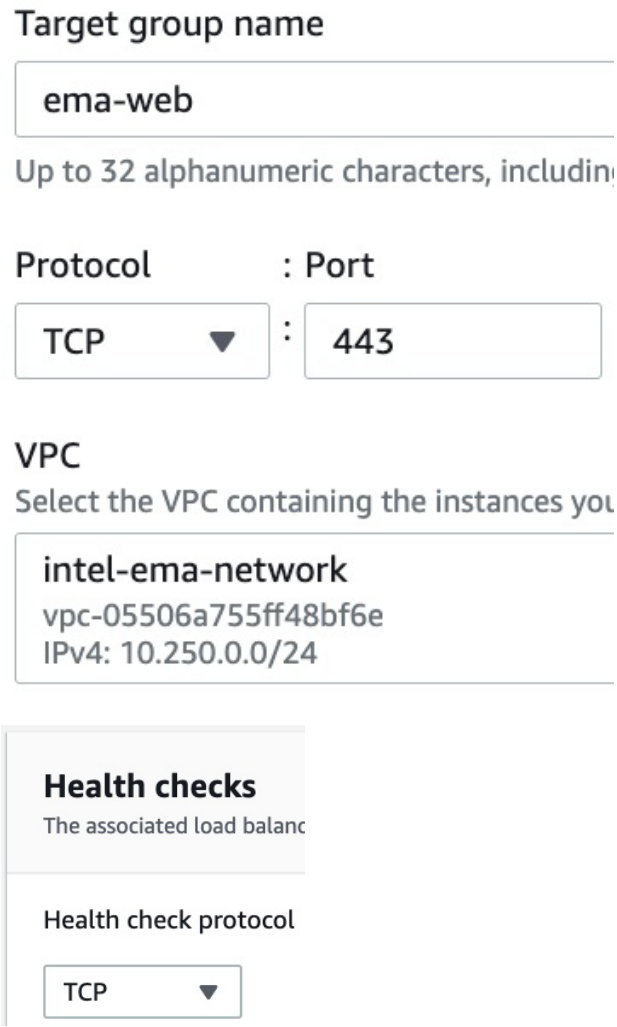
8.2 ターゲットグループの作成

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

	**EC2*** サイドバーの **Load Balancing (ロード・バランシング)** で、**Target Groups (ターゲットグループ)** を選択します。 **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。

8.2.2 TCP/443 用のターゲットグループの設定

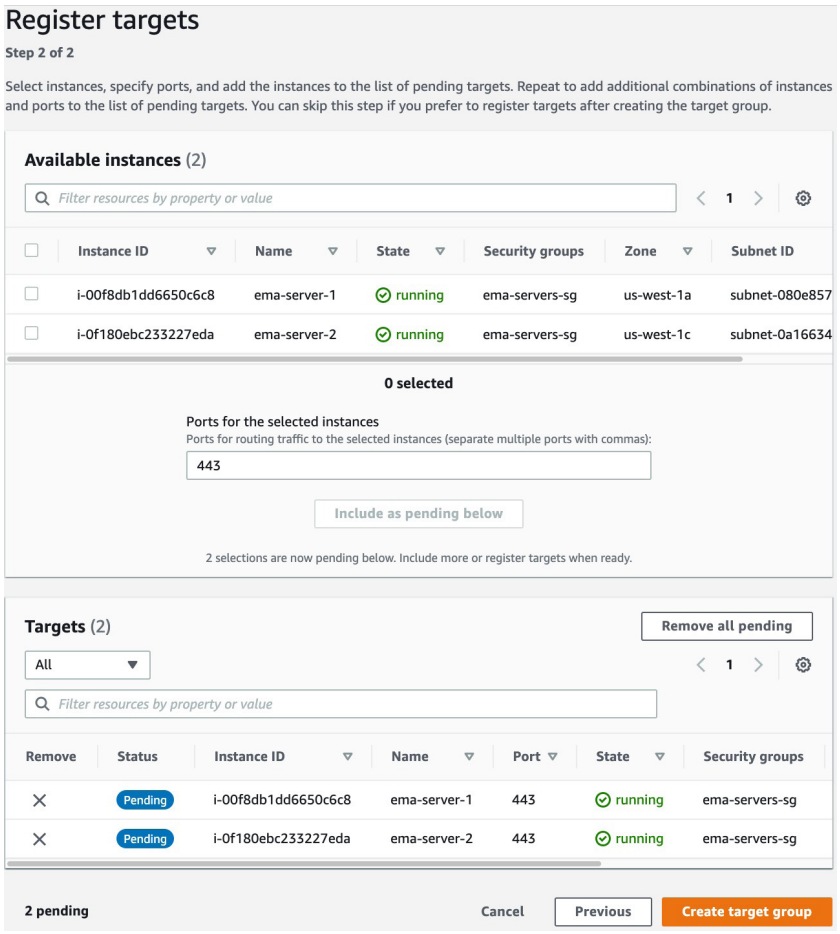


ターゲットグループを以下のように設定します。

- **Target type（ターゲットタイプ）：** *Instances*（インスタンス）
- **Target group name（ターゲットグループ名）：** 一意の名前を入力します。
  例：*ema-web*
- **Protocol（プロトコル）：** *TCP*
- **Port（ポート）：** *443*
- **VPC：** 先ほど作成した VPC を選択します。
- **Health check protocol（ヘルスチェック・プロトコル）：** *TCP*

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。

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



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

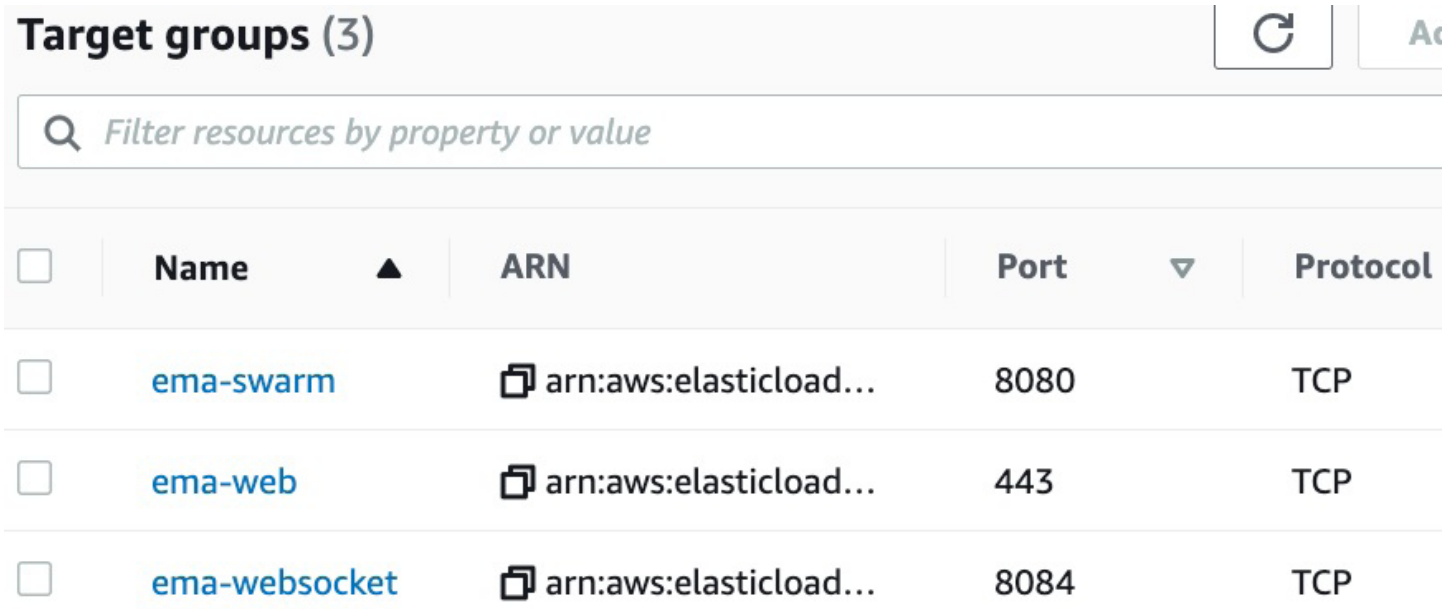
上記の手順を繰り返し、TCP/8084 用に「ema-websocket」という名前の別のターゲットグループを設定します。

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。

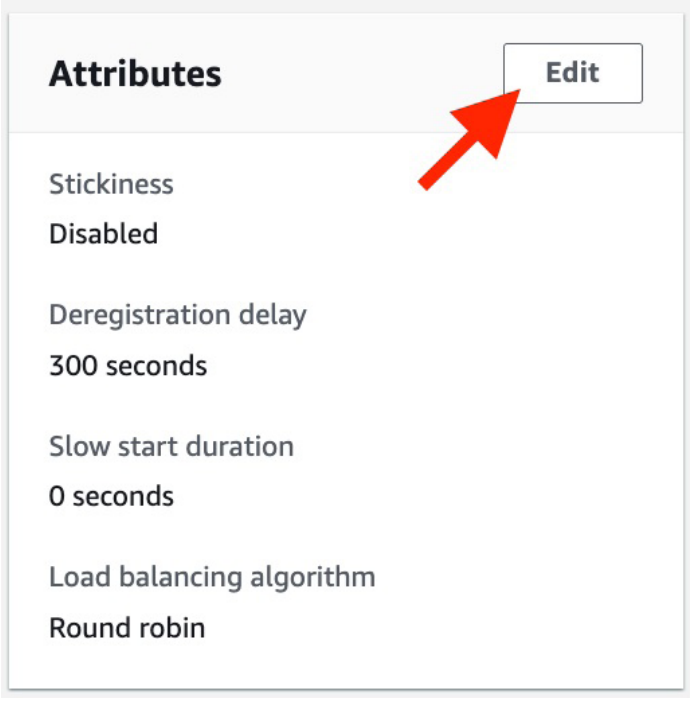
8.2.5 ターゲットグループの確認

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。



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

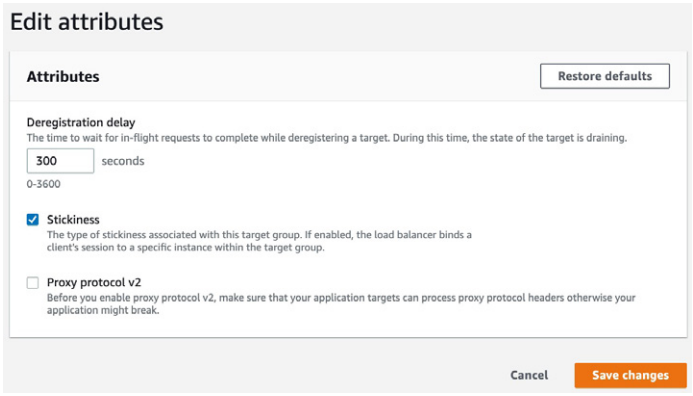
8.2.6.1 ターゲットグループの詳細



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



Stickiness（スティッキーネス）フラグを有効にします。

Save changes（変更を保存）ボタンをクリックします。

8.2.7 TCP/8084 ターゲットグループでのスティ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、スティッキーネス有効化の手順を繰り返します。

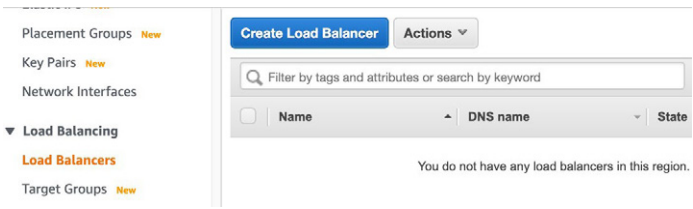
8.2.8 ターゲットグループのヘルス・モニタリングに関する注記

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

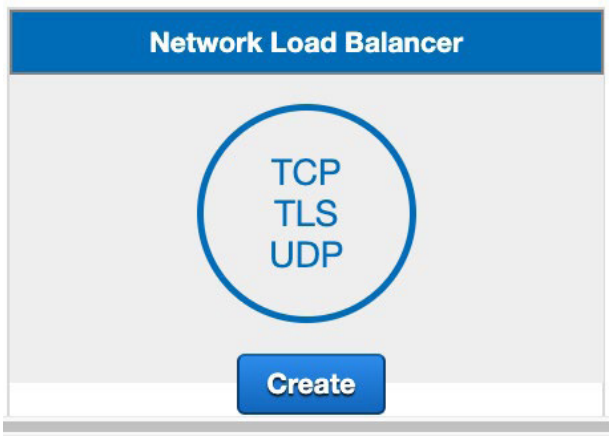
トラフィックをステータスが良好なターゲットグループに分散させるためにネットワーク・ロード・バランサーを作成する手順は次のとおりです。

8.3.1 ロードバランサーの作成



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。

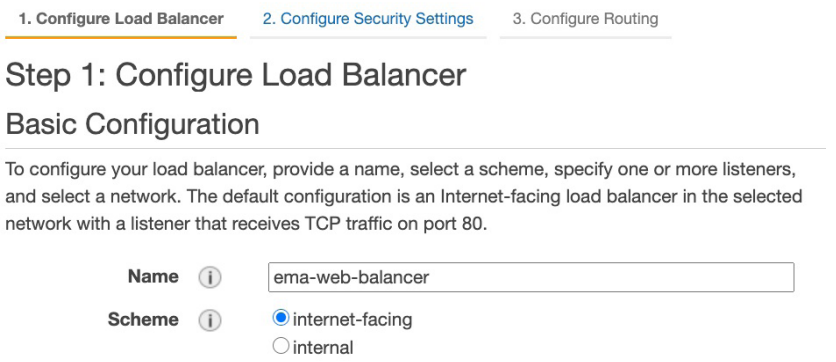
8.3.2 ロードバランサーのタイプの選択



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。

8.3.3 ロードバランサーの設定

8.3.3.1 基本設定



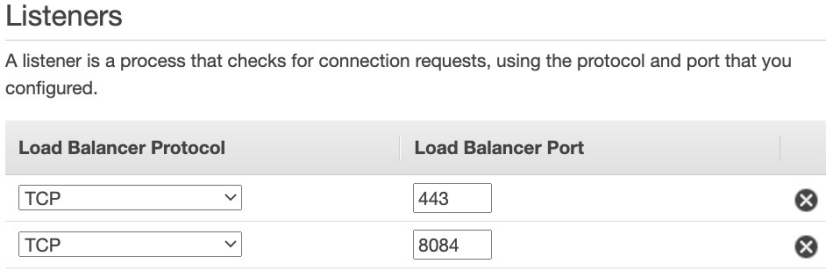
基本設定を入力します。

Name（名前）： 一意の名前を入力します。
例：*ema-web-balancer*

Scheme（スキーム： 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。

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。

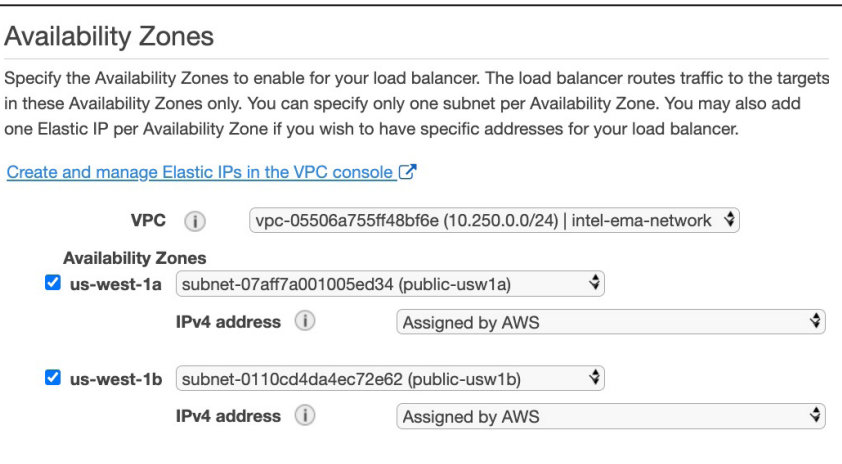
8.3.3.2 リスナー



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。

- *TCP 443*
- *TCP 8084*

8.3.3.3 アベイラビリティー・ゾーン



Availability Zone（アベイラビリティー・ゾーン） を次のように設定します。

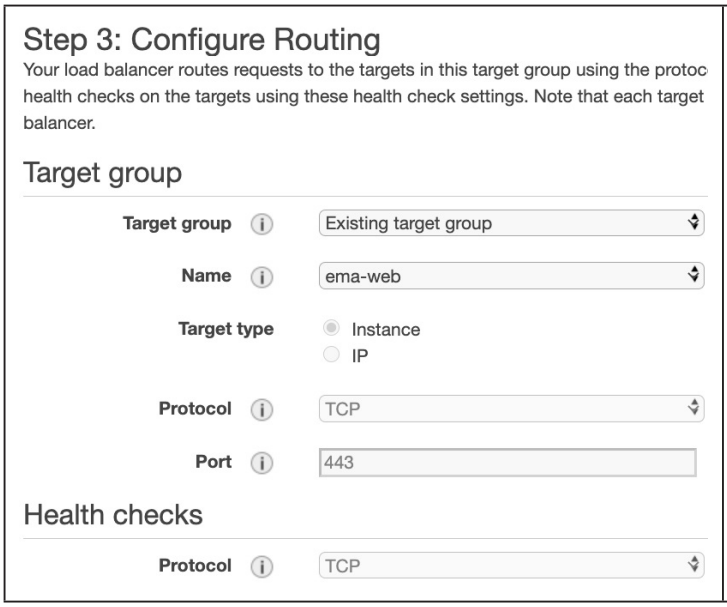
- **VPC：** 先ほど作成した VPC を選択します。
- **Availability Zone（アベイラビリティー・ゾーン）：** 両方のアベイラビリティー・ゾーンを有効にし、両方のパブリックサブネットを選択します。IPv4 アドレスは ***Assigned by AWS*（AWS* によって割り当て）** に設定します。

Next: Configure Security Settings（次へ：セキュリティー設定をする） ボタンをクリックします。

8.3.3.4 セキュリティー設定

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

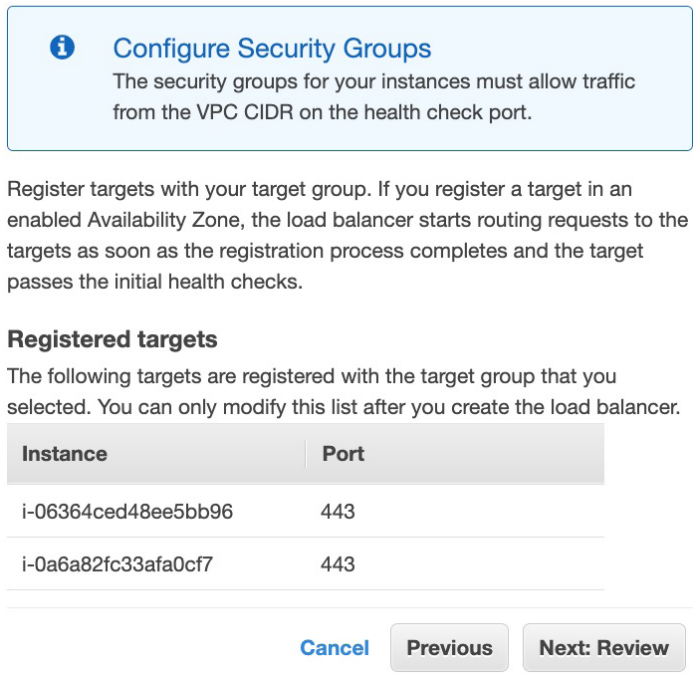


Step 3: Configure Routing（ステップ 3：ルーティングの設定）で、Target group（ターゲットグループ）を以下のように設定します。

- **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。

8.3.3.6 ターゲットの登録

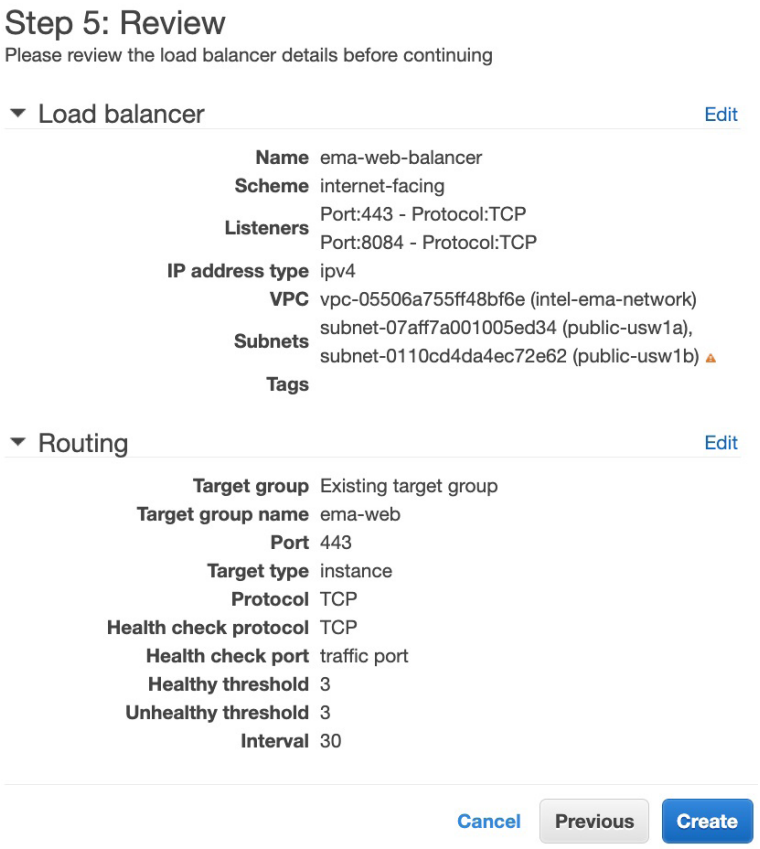


登録済みのターゲットとして 2 つのインスタンスがリストされていることを確認します。

Next: Review（次へ：確認）ボタンをクリックします。

8.3.3.7 確認

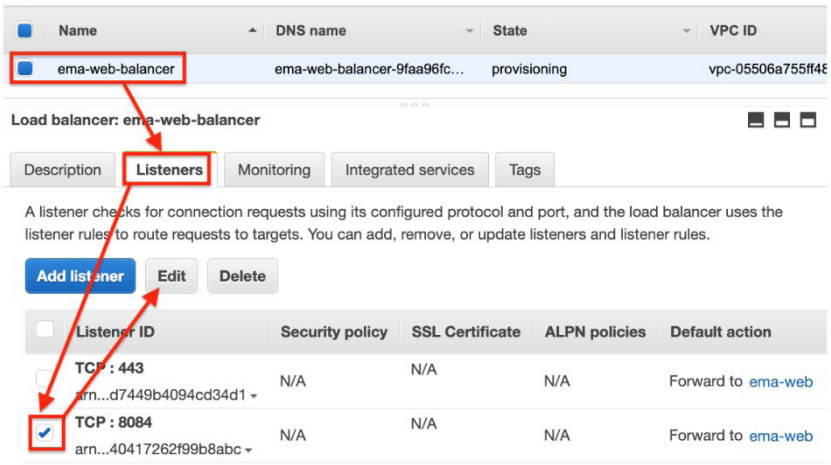
Step 5: Review（ステップ 5：確認）で、以下に示すサンプルと似たような結果になっていることを確認し、**Create（作成）**ボタンをクリックします。



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



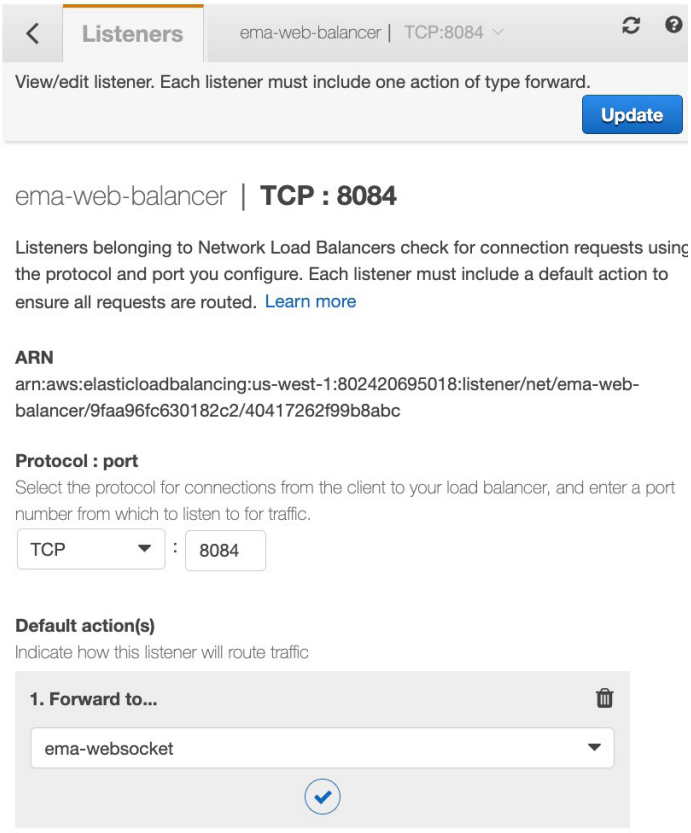
作成したロードバランサーを選択します。

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。

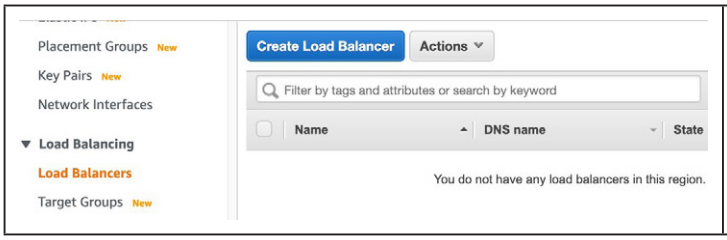


WebSocket リスナーに転送するよう、デフォルトのアクションを変更します。

Update（更新）ボタンをクリックします。

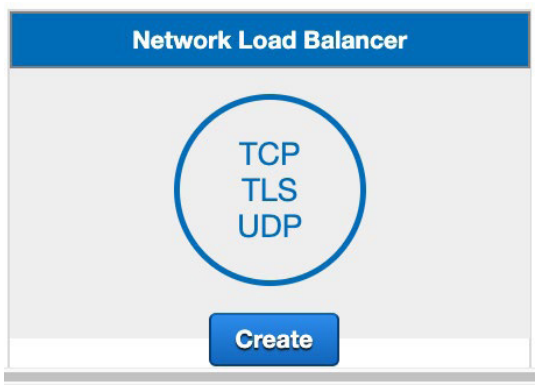
8.4 Swarm トラフィック用のネットワーク・ロード・バランサーの作成

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。

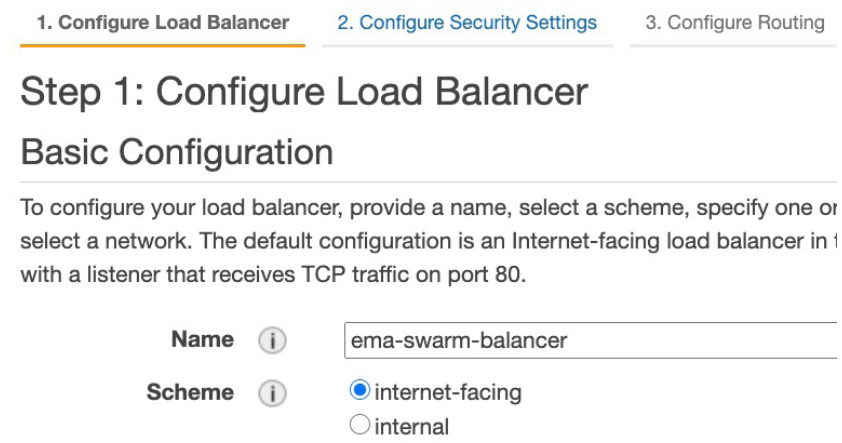
8.4.2 ロードバランサーのタイプの選択



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

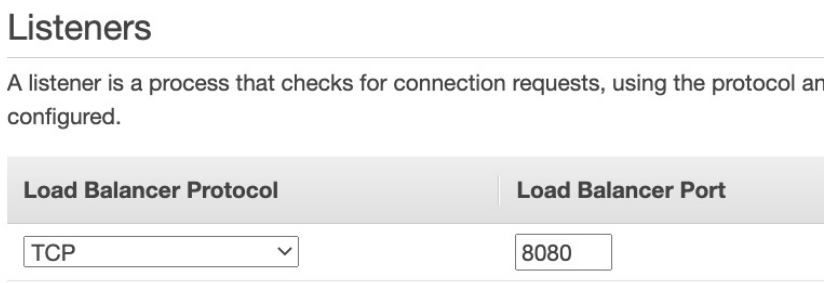


基本設定を入力します。

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）

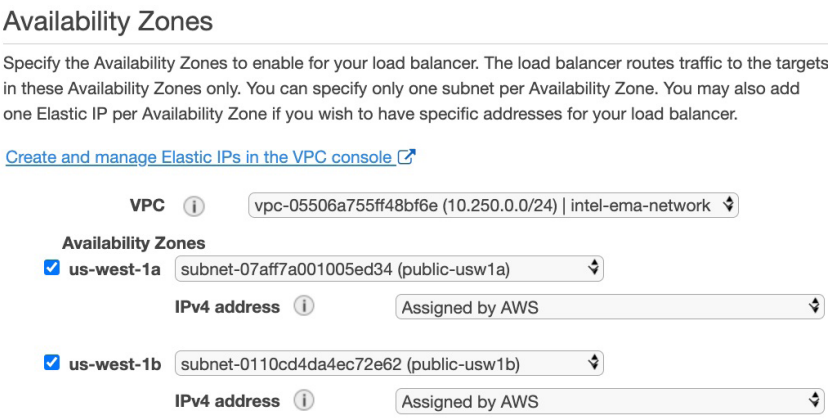
8.4.3.2 リスナー



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。

- *TCP 8080*

8.4.3.3 アベイラビリティー・ゾーン



Availability Zone（アベイラビリティー・ゾーン）を次のように設定します。

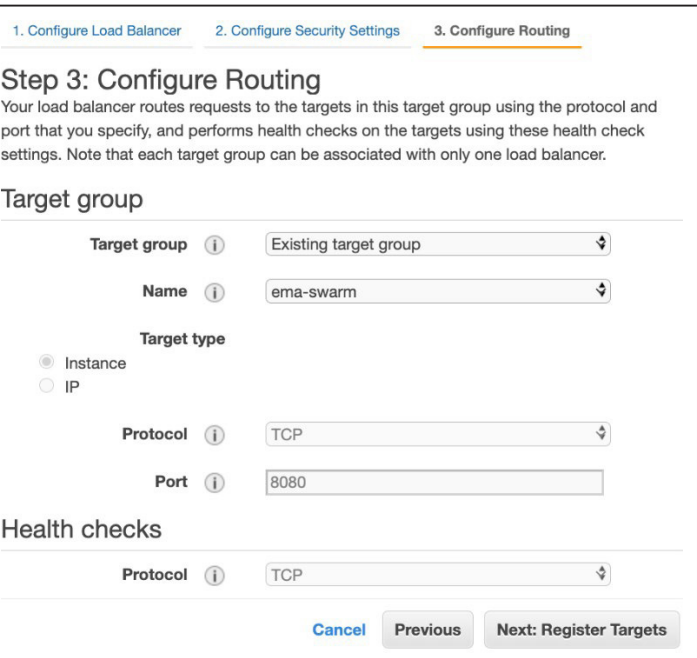
- **VPC：**先ほど作成した VPC を選択します。
- **Availability Zone（アベイラビリティー・ゾーン）：**両方のアベイラビリティー・ゾーンを有効にし、両方のパブリックサブネットを選択します。IPv4 アドレスは ***Assigned by AWS*（AWS* によって割り当て）**に設定します。

Next: Configure Security Settings（次へ：セキュリティー設定をする）ボタンをクリックします。

8.4.3.4 セキュリティー設定

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



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/8080 ターゲットグループの名前を選択します。
  例：*ema-swarm*

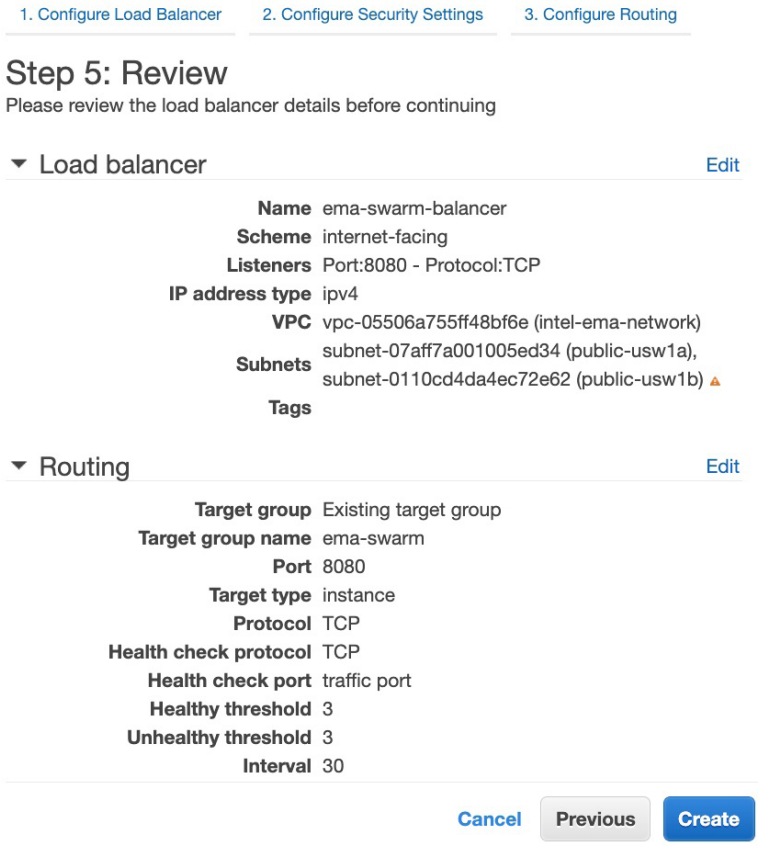
Next: Register Targets（次へ：ターゲットを登録する）ボタンをクリックします。

8.4.3.6 ターゲットの登録

	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。

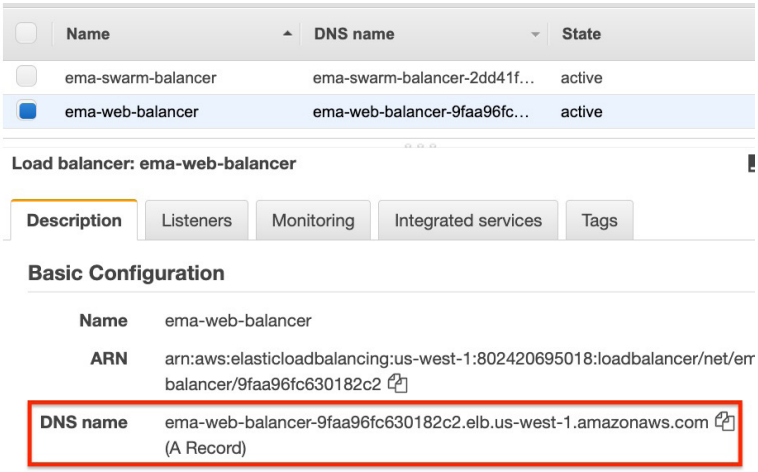
8.4.3.7 確認

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。



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。


Name
DNS name
State
ema-swarm-balancer
ema-swarm-balancer-2dd41f…
active
ema-web-balancer
ema-web-balancer-9faa96fc…
active
Load balancer: ema-web-balancer
Description
Listeners
Monitoring
Integrated services
Tags
Basic Configuration
Name
ema-web-balancer
ARN
arn:aws:elasticloadbalancing:us-west-1:802420695018:loadbalancer/net/em
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

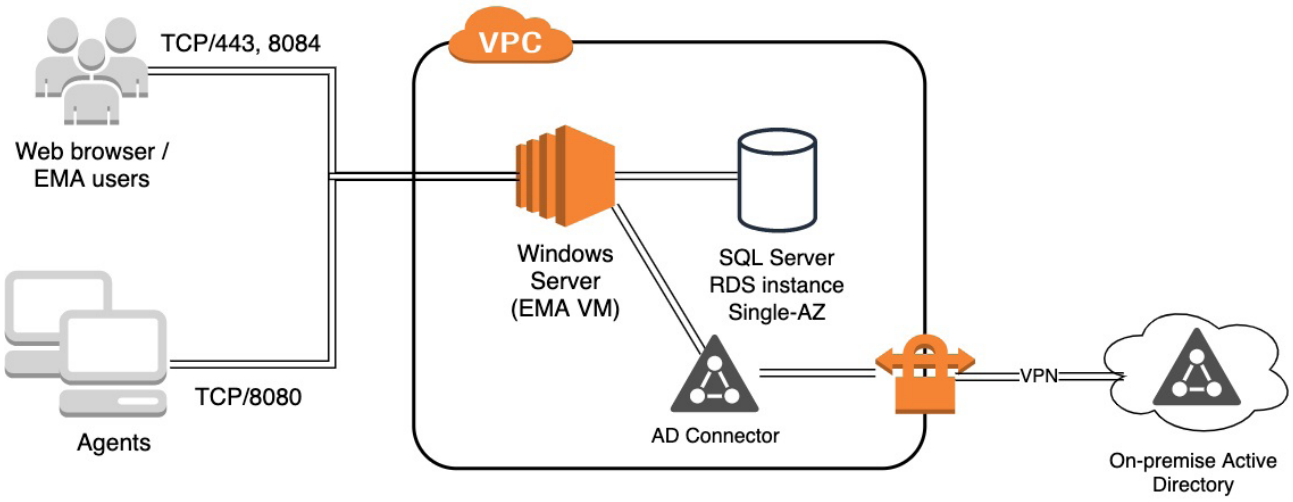
仮想マシンをドメインに参加させ、AD 認証を使用できるようにするために、Active Directory* と AWS* を統合する方法は複数あります。組織のニーズは多種多様なため、本付録では、既存のオンプレミス・ディレクトリーをこの目的でクラウドに拡張するためのいくつかのヒントを提供します。クラウド・プロバイダーは、時折、提供サービスを変更します。そのため、本稼働用のソリューションをデプロイする前に、ビジネスに最も適したソリューションを確認する必要があります。

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。

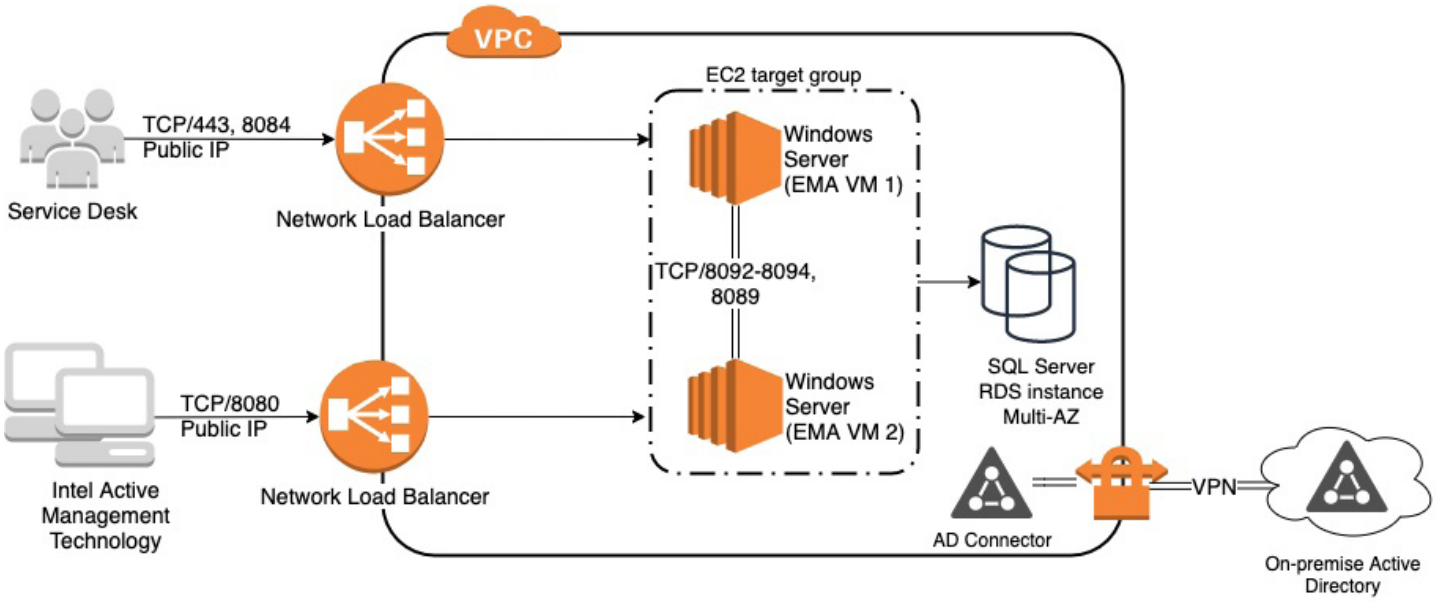
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.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。