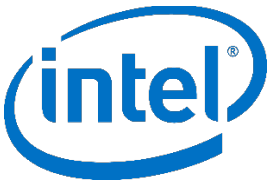


Intel® Endpoint Management Assistant (Intel® EMA)

Amazon Web Services* (AWS) 部署指南

英特尔® 版本 1.3.3

2020 年 10 月

法律免责声明

英特尔技术可能需要支持的硬件、软件或服务激活。

没有任何产品或组件能保证绝对安全。

您的成本和结果可能会有所不同。

本文档不代表英特尔公司或其他机构向任何人（明示或暗示、明确或隐含地）授予任何知识产权许可。

英特尔不承诺任何明示或暗示的担保，包括但不限于对适销性、特定用途适用性和不侵权的暗示担保，以及由履约过程、交易过程和贸易中使用引起的任何担保。

所描述的产品和服务可能包含可导致产品和服务与公布的技术规格有所偏离的瑕疵或误差（将被收入勘误表）。可应要求提供当前的勘误表。

英特尔技术特性和优势取决于系统配置，并可能需要支持的硬件、软件或服务激活。性能会因系统配置的不同而有所差异。没有任何计算机系统能保证绝对安全。英特尔对数据或系统丢失或被盗、以及因此而导致的任何其它损失不承担任何责任。请咨询您的系统制造商或零售商，也可访问 http://www.intel.com/technology/vpro 获取更多信息。

目录

1 简介

本文档介绍了将基础架构部署到 Amazon Web Services*（一种云计算平台），以支持一个或多个 Intel® Endpoint Management Assistant (Intel® EMA) 服务器实例的步骤。它适用于掌握了 IT 基础架构的中级到高级知识，但可能对云计算了解有限的 IT 管理员。

完整的云基础架构环境需要多个组件，因此我们建议您仔细阅读本指南以了解如何配置它们以协同工作。我们会在部署过程前提供每个组件的描述，并附带云提供商官方文档的链接，以在需要时提供更多信息。

1.1 云计算简介

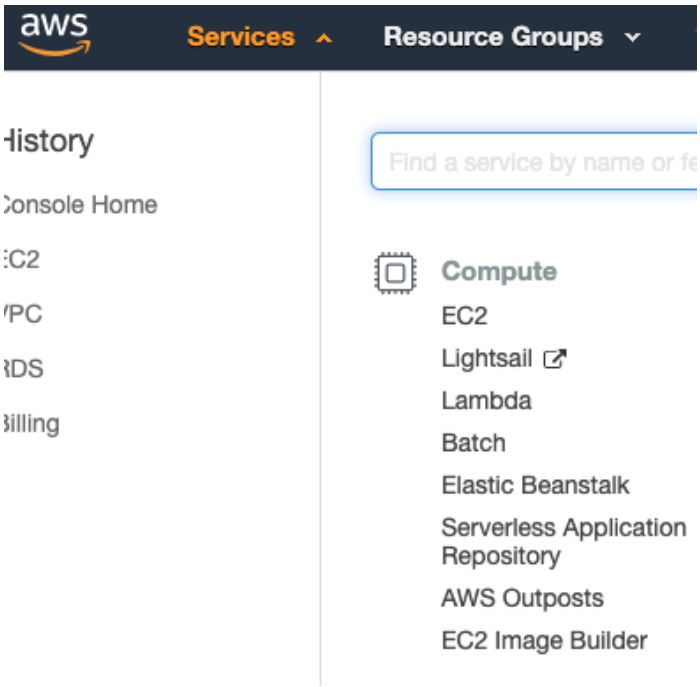
云计算采用即用即付的定价方式，通过互联网按需交付 IT 资源。您无需购买、拥有和维护物理数据中心和服务器，便可以从云提供商处按需访问技术服务，例如计算能力、存储和数据库。您可以只配置现在需要的资源，并随着业务需求的变化进行调整，以增加和减少资源。

大型的云提供商在全球都拥有数据中心，使您可以将资源部署到距离客户和最终用户更近的地理位置。

借助类似 Amazon Relational Database Service 的完全托管服务，您可以专注于数据，而云提供商则可以管理提供该服务的所有底层硬件和软件。借助在云中运行的虚拟机，您只需要管理来宾操作系统及其上安装的软件，而云提供商则管理底层硬件并尽量为您提供最佳的可靠性和可用性。

1.2 操作 AWS 管理控制台

1.2.1 服务

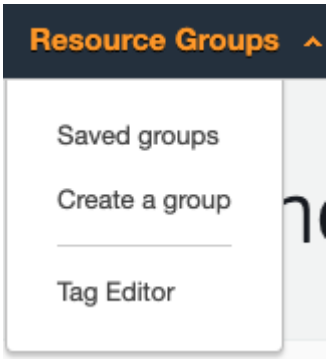


在 https://aws.amazon.com/console/ 登录 AWS 管理控制台，您将在屏幕的左上角看到 Services 菜单。

单击此按钮可打开 AWS 提供的所有服务的列表，按照 Compute，Storage，Database 等类别进行分类。

在部署本指南中的服务时，我们将提供说明来指导您进入此屏幕界面以选择适当的服务。

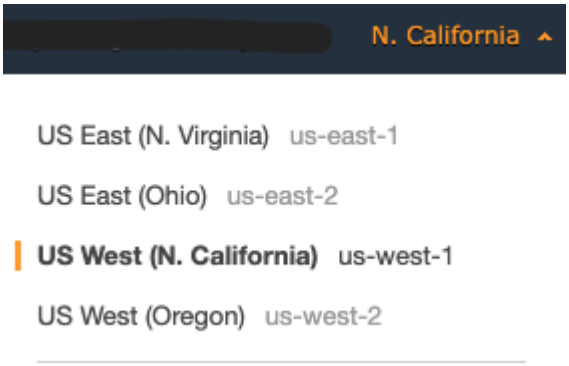
1.2.2 资源组



Services 旁边是 Resource Groups 菜单，您可以在其中创建或查看已创建的资源组。

通常，您将看到在当前区域中部署的所有资源，与部署者是谁或被部署资源属于哪个项目无关，因此使用资源组可以根据已附加到每个资源的自定义标签为您提供资源的筛选列表。

1.2.3 区域



在管理控制台的右上角，您将看到一个菜单，您必须在其中选择将要进行资源部署的区域。

您将只能看到为所选区域列出的资源。

每个 AWS 区域都包含多个不同的位置，称为可用区 (Availability Zone)。每个可用区均经过精心设计，可与其他可用区中的故障隔离开来。

1.3 标签和资源组

标签是自定义键值对，您可以将其分配给可以在 AWS 中部署的许多不同种类的资源。最好在创建资源时对资源添加标签，以使您能够更轻松地跟踪资源所有者、资源所属的项目、启用基于标签的资源组以及启用基于标签的账单报告。

在本指南中，我们将不使用标记或创建资源组，因为这会有多种不同的方法并会增加很多额外的步骤，但是您应该了解如果您想实施标记和资源分组策略，则可以使用这些方法。

有关使用标签的更多信息，请访问以下链接：
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

1.4 开始之前

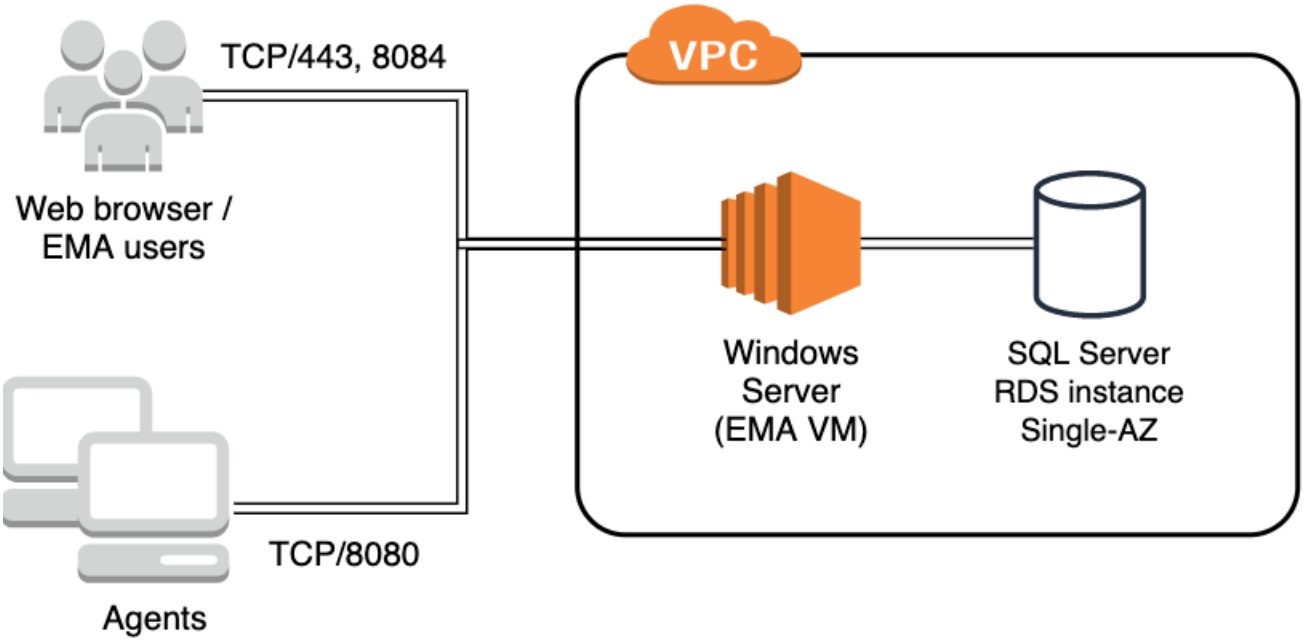
如果您的组织已经有 AWS 账户，则应要求云管理员授予您足够的访问权限，以便创建本指南中列出的所有资源。

如果您的组织没有 AWS 账户，或者您想对它进行个人评估，则可以转到 https://aws.amazon.com/console/ 并单击 **Create a Free Account** 按钮。

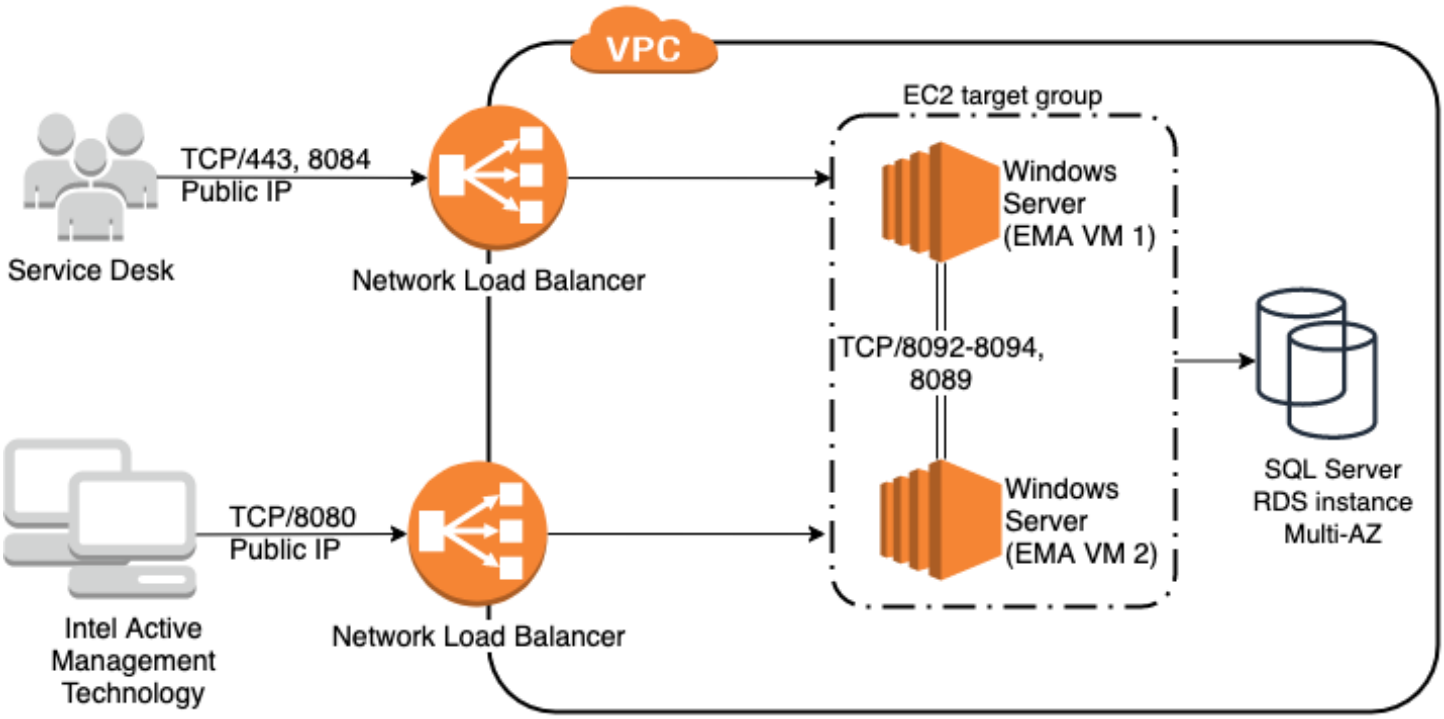
请与您的网络管理员联系，询问是否存在可供使用的首选的地 止空间。如果您已经建立了连接到云提供商的 VPN，或者将来要建立此类连接，则您应避免与企业网络重叠，以免出现路由问题。您还需要找出数据是通过哪个源 IP 地 止离开组织并到达云端的，以便仅允许受信任的网络通过互联网访问 Intel EMA 虚拟机。

2 高层级架构图

2.1 单服务器部署

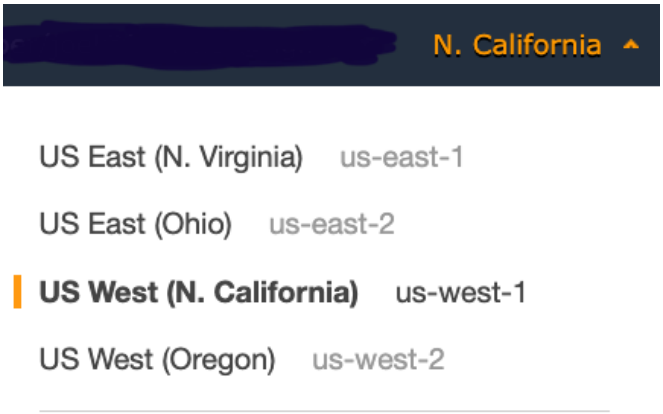


2.2 分布式服务器部署



3 选择部署区域

从右上角的区域菜单中，选择将要部署资源的区域。



4 网络部署

4.1 概述

为了让虚拟机能够彼此通信，也能与云提供商或与互联网通信，我们首先需要配置网络环境。虚拟私有云 (VPC) 是 AWS 中私有网络的主要构建基块，它与传统网络非常相似，但在 AWS 中它是虚拟化的。VPC 在逻辑上彼此隔离。

创建 VPC 时，您将需要提供自定义的私有 IP 地址空间。AWS 将在需要时从该地址空间为资源分配私有 IP 地址。建议避免使用与组织的其他网络范围重叠的地址空间，以免在网络通过 VPN 连接后产生路由冲突。如果您的公司已建立或将建立与云的私有 IP 连接，您应该咨询您的网络工程团队确定可用的 IP 地址块，避免路由冲突。

创建 VPC 后，我们还将创建子网。子网让您可以对 VPC 网络分段，将其一部分的地址空间分配给各个子网。我们的子网将位于所选区域内的两个单独的可用区 (AZ) 中，以便我们可以为数据库和 Intel EMA 应用程序提供更高的可用性。我们将创建公共子网和私有子网，根据资源是否需要使用公共 IP 地址直接访问互联网来使用。

默认情况下，AWS 防火墙不允许对我们的资源进行入站访问，因此网络部署的一部分将包括创建安全组，以实现与这些资源的网络通信。

为了减少虚拟机的攻击面，将不允许 RDP 通过 VPC 防火墙。相反，我们将使用 AWS Session Manager 来启用虚拟机的远程管理。此外，对于分布式服务器部署，所有虚拟机都不具有公共 IP 地址。

有关 VPC 的更多信息，请访问以下链接:
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html

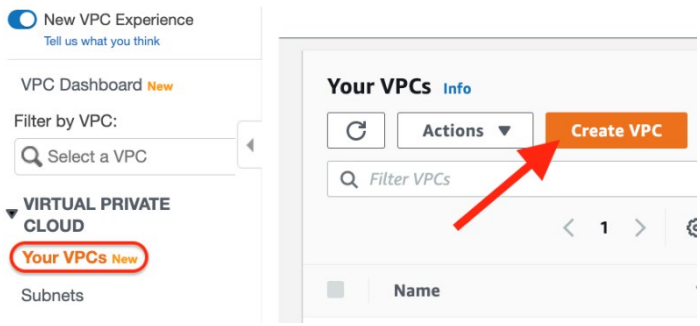
4.2 创建 VPC

如果您仅使用一个公共子网进行单服务器部署，则可以使用 VPC Wizard， 但是在这里，我们将手动创建所有网络组件，以更好地了解所需资源，因为该向导不足以进行分布式服务器部署。

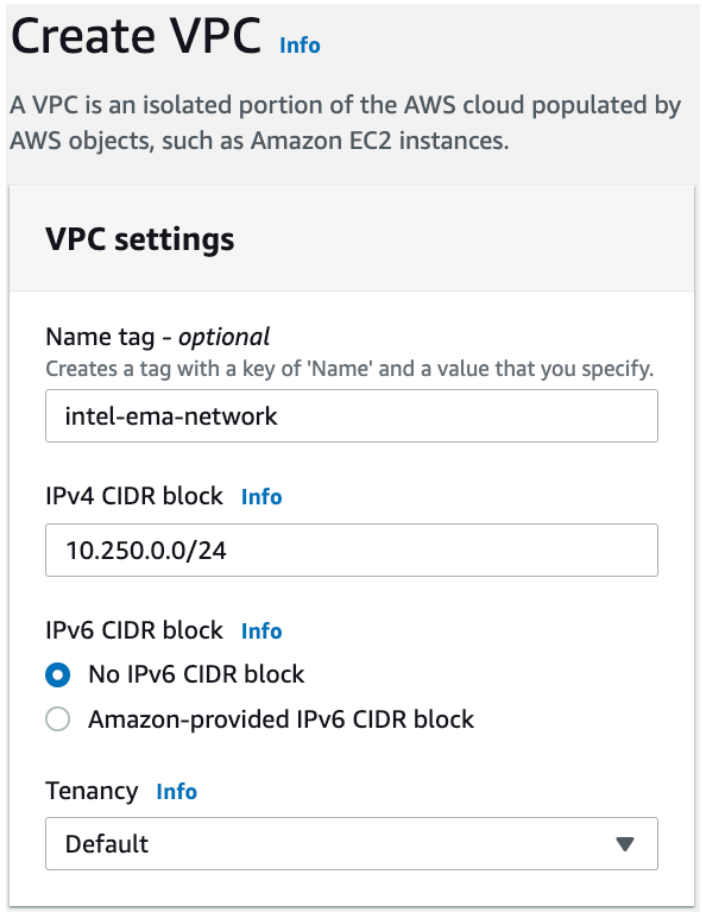
4.2.1 导航至 VPC 服务

	从 **Services** 菜单的 **Network & Content Delivery** 部分中，选择 **VPC**。

4.2.2 创建 VPC

	在 VPC 侧栏中，选择 **Your VPCs**。 单击 **Create VPC** 按钮。

4.2.3 配置 VPC 详细信息



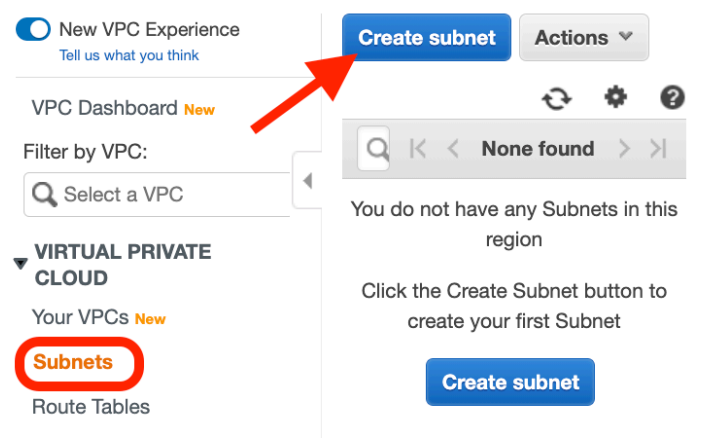
输入如下所示的网络详细信息

- **Name Tag**：输入 VPC 的唯一名称。
  示例：*intel-ema-network*
- **IPv4 CIDR block**：选择一个足以容纳您的子网的未使用网络。
  示例：*10.250.0.0/24*

单击 **Create VPC** 按钮

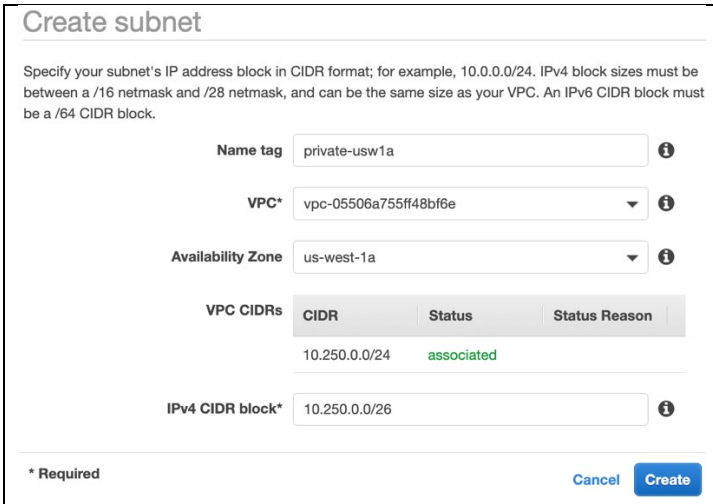
4.3 创建子网

4.3.1 导航至 Subnets 屏幕



在 VPC 侧栏中，选择 **Subnets**。

4.3.2 创建第一个私有子网



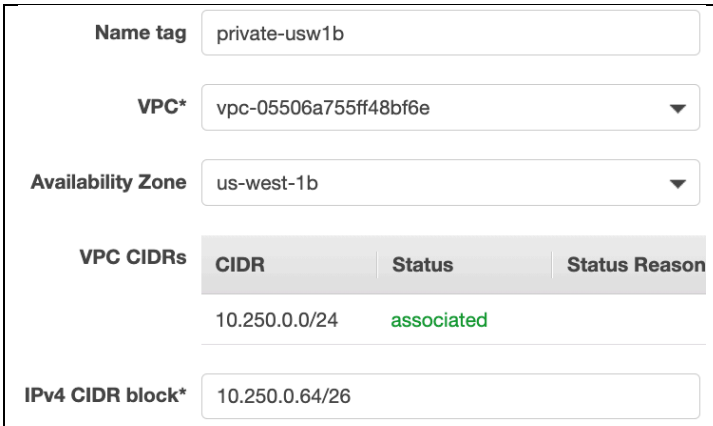
单击 **Create subnet** 按钮。

按如下所示配置子网：

- **Name tag**：提供唯一的子网名称。
  示例：*private-usw1a*
- **VPC**：选择先前创建的虚拟网络。
- **可用区**：在我们的设计中，我们希望使用两个不同的区，因此请在此处使用您的首选区。
  示例：*us-west-1a*
- **IPv4 CIDR block**：在 VPC 地 止空间内选择一个未使用的 IP 块。
  示例：*10.250.0.0/26*

单击 **Create** 按钮。

4.3.3 创建第二个私有子网



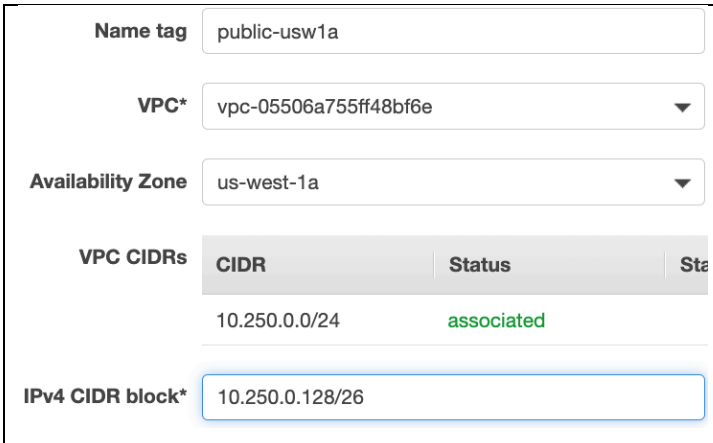
单击 **Create subnet** 按钮。

按如下所示配置子网：

- **Name tag**：提供唯一的子网名称。
  示例：*private-usw1b*
- **VPC**：选择先前创建的虚拟网络。
- **可用区**：在我们的设计中，我们希望使用两个不同的区，因此请在此处使用您的第二个区。
  示例：*us-west-1b*
- **IPv4 CIDR block**：在 VPC 地 止空间内选择一个未使用的 IP 块。
  示例：*10.250.0.64/26*

单击 **Create** 按钮。

4.3.4 创建第一个公共子网



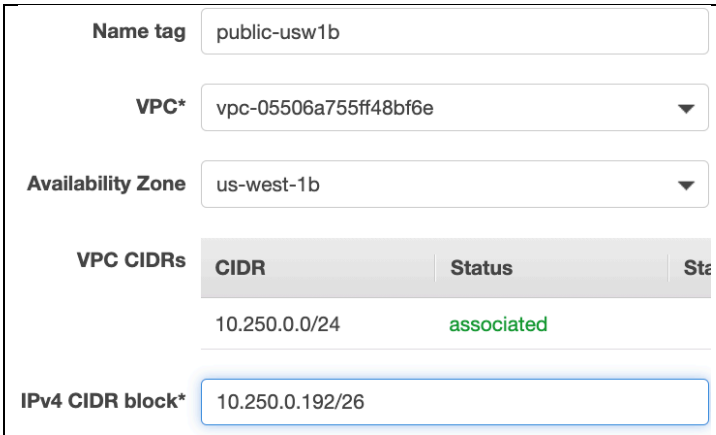
单击 **Create subnet** 按钮。

按如下所示配置子网：

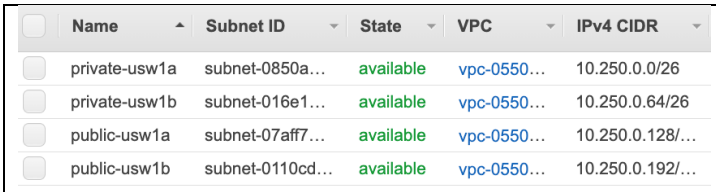
- **Name tag**：提供唯一的子网名称。
  示例：*public-usw1a*
- **VPC**：选择先前创建的虚拟网络。
- **可用区**：在我们的设计中，我们希望使用两个不同的区，因此请在此处使用您的首选区。
  示例：*us-west-1a*

	• **IPv4 CIDR block**：在 VPC 地 止空间内选择一个未使用的 IP 块。 示例： *10.250.0.128/26* 单击 **Create** 按钮。

4.3.5 创建第二个公共子网

	单击 **Create subnet** 按钮。 按如下所示配置子网： • **Name tag**：提供唯一的子网名称。 示例：*public-usw1b* • **VPC**：选择先前创建的虚拟网络。 • **可用区**：在我们的设计中，我们希望使用两个不同的区，因此请在此处使用您的第二个区。 示例：*us-west-1b* • **IPv4 CIDR block**：在 VPC 地 止空间内选择一个未使用的 IP 块。 示例： *10.250.0.196/26* 单击 **Create** 按钮

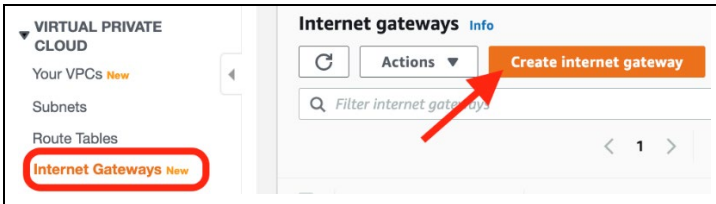
4.3.6 审查您的子网

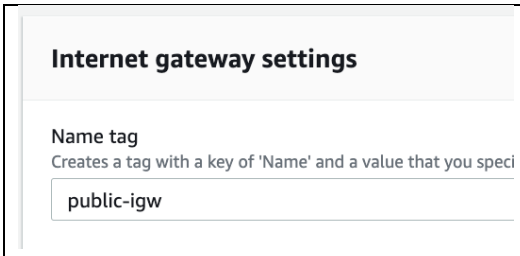
	审查您的子网列表。您现在应该已经创建了四个子网。

4.4 创建面向公共子网的互联网网关

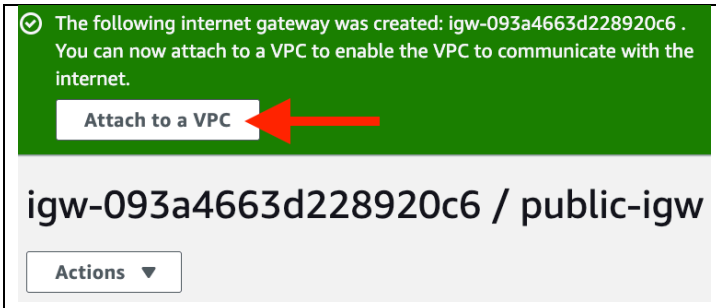
要将流量从公共子网导流到互联网，我们需要部署互联网网关并将其连接到 VPC。我们将在后面的部分中为其配置路由。

4.4.1 创建互联网网关

	在 VPC 侧栏中，选择 Internet Gateways。 单击 **Create Internet** gateway。 输入名称标签。示例：*public-igw* 单击屏幕底部的 **Create Internet gateway** 按钮以完成操作。

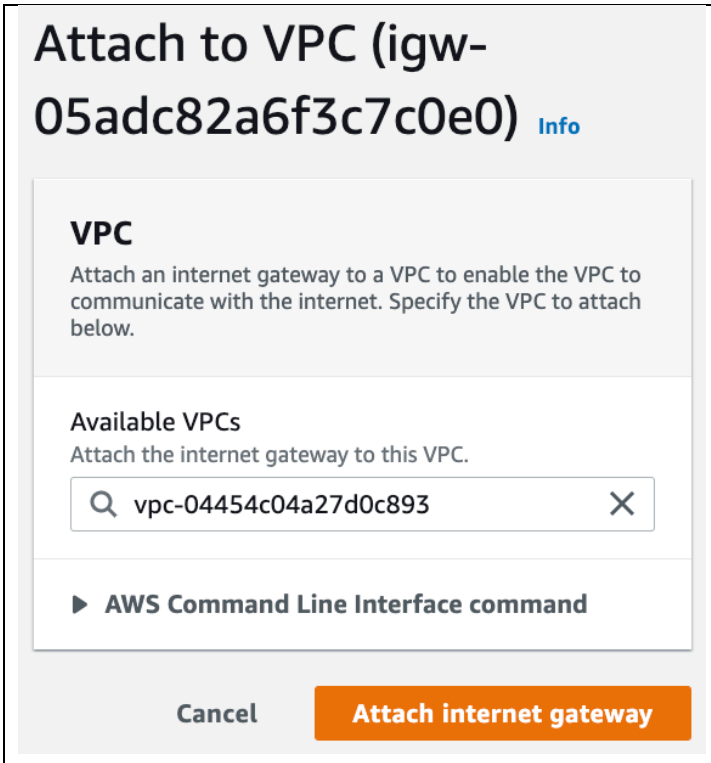


4.4.2 将 Internet Gateway 连接到 VPC



创建 Internet Gateway 后，系统将提示您将其连接到 VPC。单击指示的按钮。您也可以从 Actions 菜单执行此操作。

4.4.3 输入附件详细信息



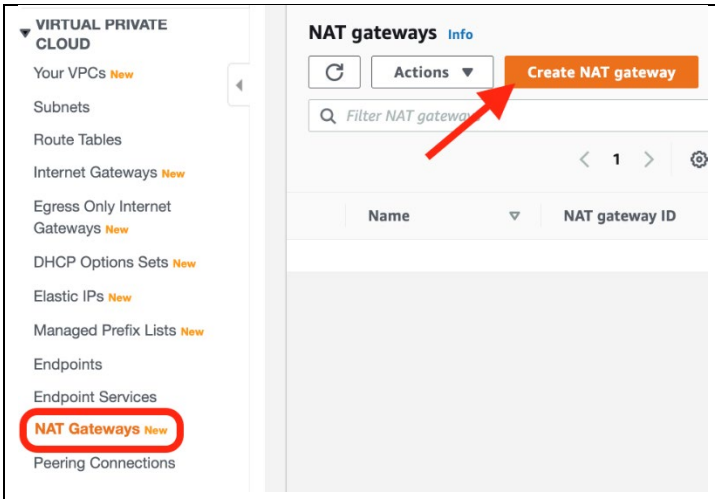
选择您之前创建的 VPC。

单击 **Attach internet gateway** 按钮。

4.5 创建面向私有子网的 NAT 网关

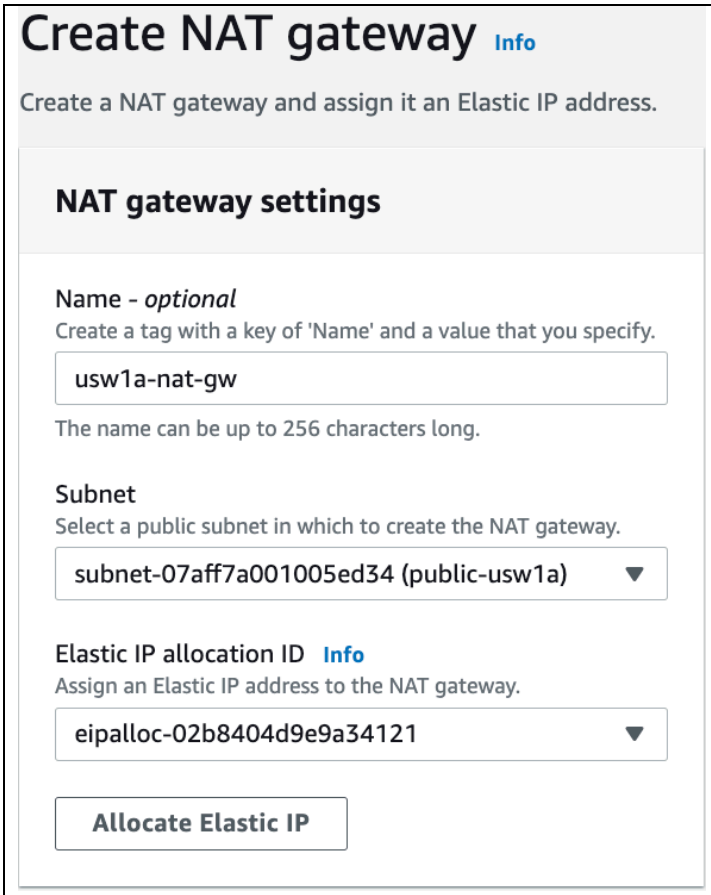
NAT 网关是一种区资源，该区中的资源可以将其用作出站互联网通讯的出口点。NAT 网关将执行地 止转换，并将流量转发到 VPC 中的互联网网关。我们将为我们的两个可用区各创建一个 NAT 网关，即便其中一个区域出现故障，我们也不会失去连接。

4.5.1 导航至 NAT 网关



在 VPC 侧栏中，选择 **NAT Gateways**。

4.5.2 创建第一个 NAT 网关



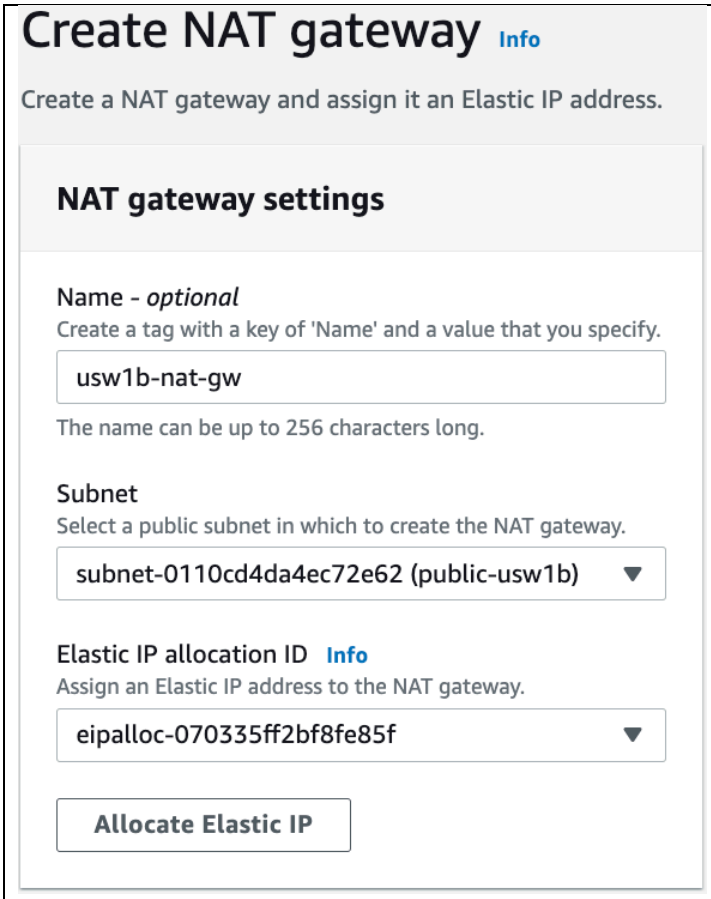
单击 **Create NAT gateway** 按钮。

按如下所示配置 NAT 网关设置：

- **Name**（可选）：输入网关的唯一名称。
  示例：*usw1a-nat-gw*
- **Subnet**：选择第一个公共子网。
  示例：*public-usw1a*
- **Elastic IP allocation ID**：单击 Allocate Elastic IP 按钮以自动填充此字段。

单击 **Create NAT gateway** 按钮以完成此操作。

4.5.3 创建第二个 NAT 网关



单击 **Create NAT gateway** 按钮。

按如下所示配置 NAT 网关设置：

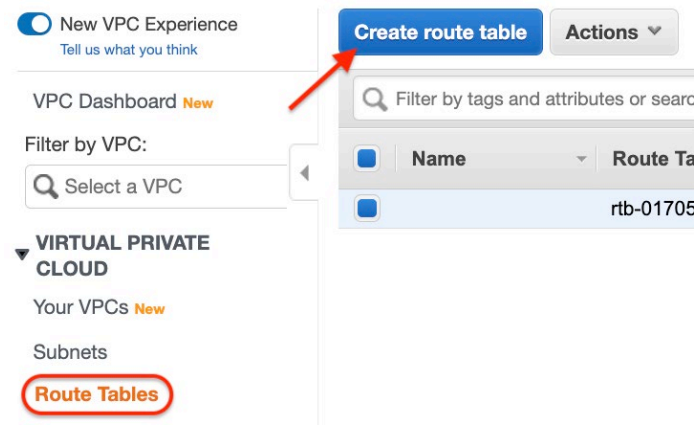
- **Name**（可选）：输入网关的唯一名称。
  示例：*usw1b-nat-gw*
- **Subnet**：选择第二个公共子网。
  示例：*public-usw1b*
- **Elastic IP allocation ID**：单击 Allocate Elastic IP 按钮以自动填充此字段。

单击 **Create NAT gateway** 按钮以完成此操作。

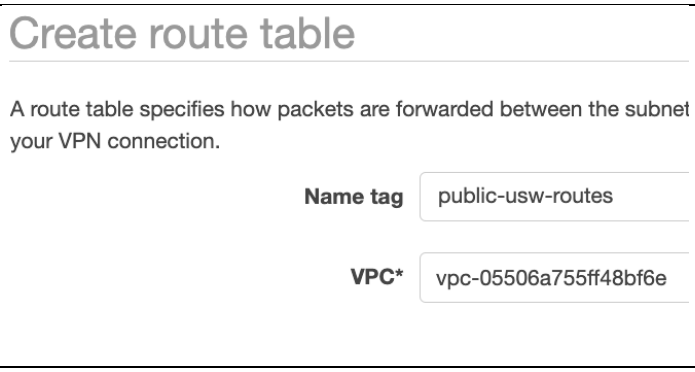
4.6 创建和配置路由表

路由表是一组路由规则，用于确定将网络流量定向到何处。VPC 已包含默认路由表，该默认路由表用于未与路由表明确关联的任何子网。我们将忽略它，并创建三个新的路由表，其中一个与我们的公共子网相关联，另外两个与我们的私有子网相关联。我们将默认路由添加到 NAT 网关和互联网网关。

4.6.1 导航至路由表



4.6.2 创建公共子网的路由表



单击 **Create route table** 按钮。

按如下所示配置路由表：

- **Name Tag**：输入路由表的唯一名称。
  示例：*public-usw-routes*
- **VPC**：选择先前创建的虚拟网络。

单击 **Create** 按钮。

单击 **Close** 按钮。

4.6.3 创建面向第一个私有子网的路由表

单击 **Create route table** 按钮。

按如下所示配置路由表：

- **Name Tag**：输入路由表的唯一名称。
  示例：*private-usw1a-routes*
- **VPC**：选择先前创建的虚拟网络。

单击 **Create** 按钮。

单击 **Close** 按钮。

4.6.4 创建面向第二个私有子网的路由表

单击 **Create route table** 按钮。

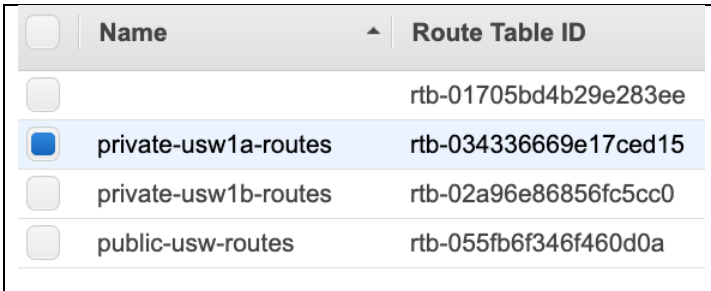
按如下所示配置路由表：

- **Name Tag**：输入路由表的唯一名称。
  示例：*private-usw1b-routes*
- **VPC**：选择先前创建的虚拟网络。

单击 **Create** 按钮。

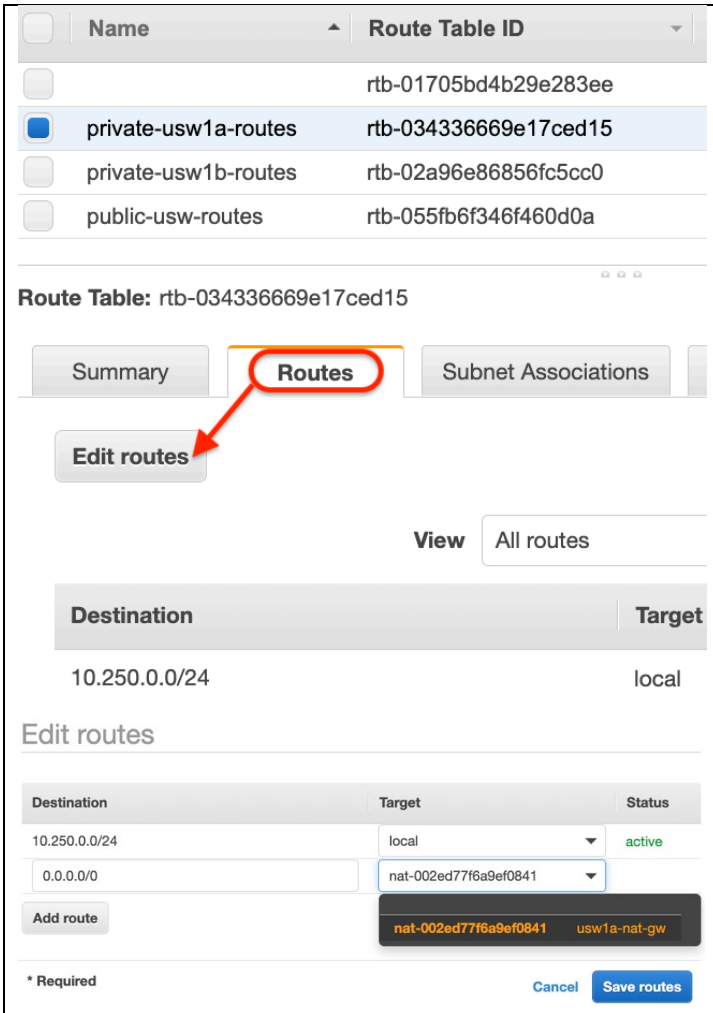
单击 **Close** 按钮。

4.6.5 审查路由表列表



验证路由表列表中是否包含三个新条目以及您为其所选的名称标签。

4.6.6 编辑面向第一个私有子网路由表的路由



选择面向第一个私有子网的路由表。
示例：*private-usw1a-routes*

选择列表下方的 **Routes** 标签。

单击 **Edit routes** 按钮。

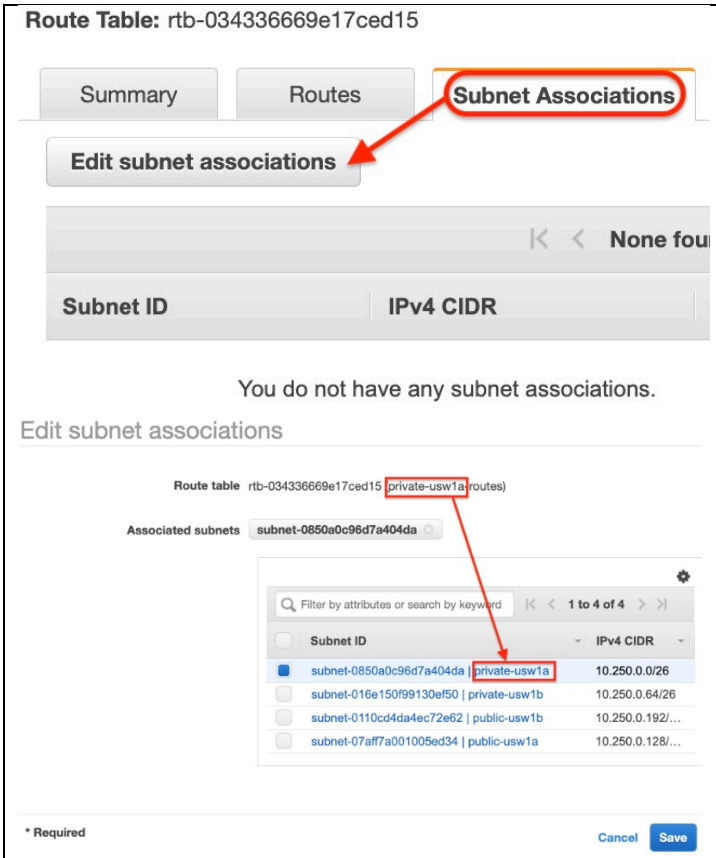
单击 **Add route** 按钮并设置以下值：

- **Destination**：*0.0.0.0/0*
- **Target**：选择部署到第一个可用区的 NAT 网关。
  示例：*usw1a-nat-gw*

单击 **Save routes** 按钮。

单击 **Close** 按钮。

4.6.7 编辑面向第一个私有子网路由表的子网关联



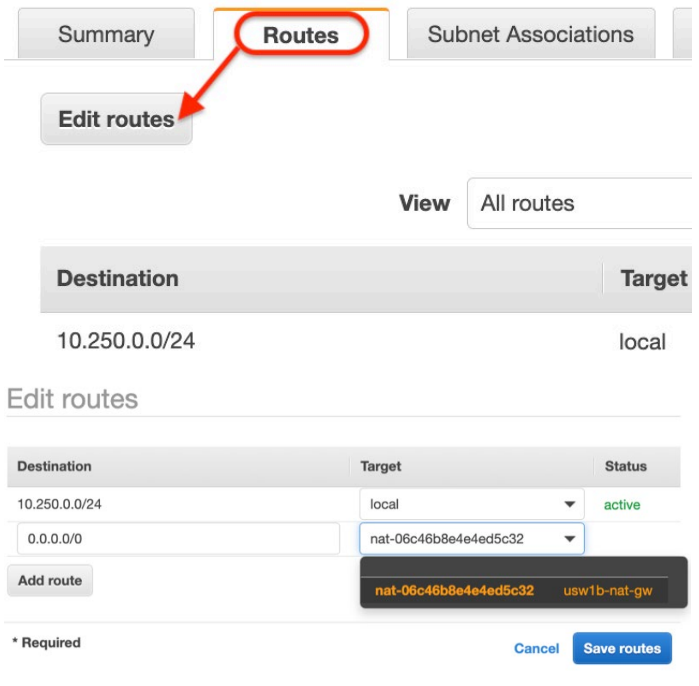
选择 **Subnet Associations** 选项卡。

单击 **Edit subnet associations** 按钮。

选择第一个私有子网以与此路由表进行关联。如果遵循本指南中的示例名称，则可以轻松地将路由表的名称与子网匹配。

单击 **Save** 按钮。

4.6.8 编辑面向第二个私有子网路由表的路由



选择面向第二个私有子网的路由表。
示例：*private-usw1b-routes*

选择列表下方的 **Routes** 标签。

单击 **Edit routes** 按钮。

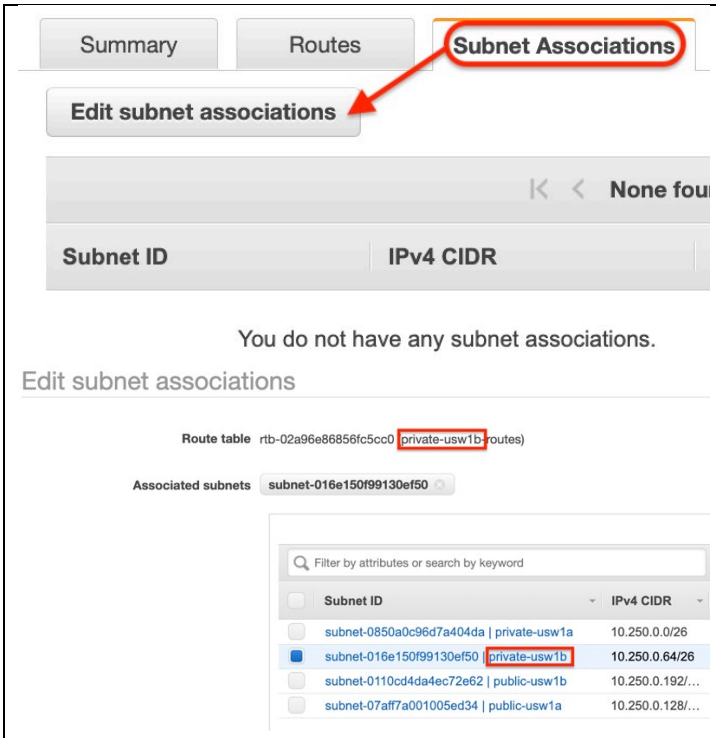
单击 **Add route** 按钮并设置以下值：

- **Destination**：*0.0.0.0/0*
- **Target**：选择部署到第二个可用区的 NAT 网关。
  示例：*usw1b-nat-gw*

单击 **Save routes** 按钮。

单击 **Close** 按钮。

4.6.9 编辑面向第二个私有子网路由表的子网关联



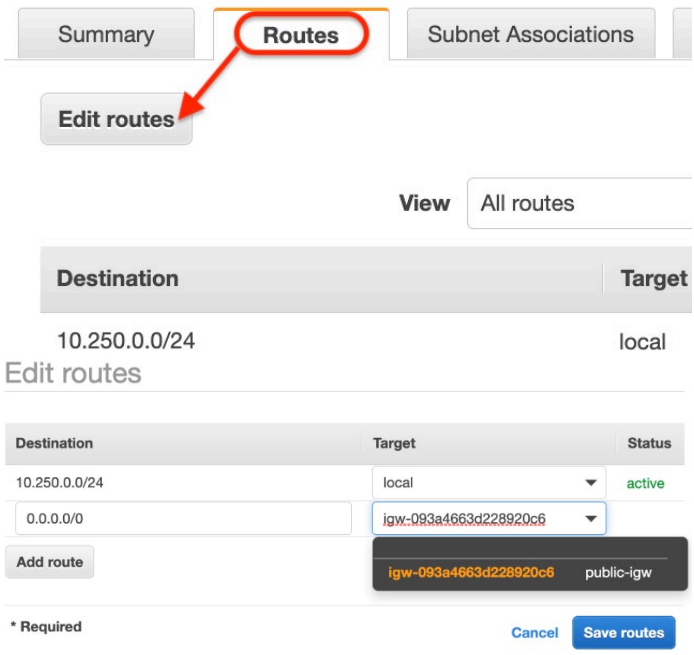
选择 **Subnet Associations** 选项卡。

单击 **Edit subnet associations** 按钮。

选择第二个私有子网以与此路由表进行关联。如果遵循本指南中的示例名称，则可以轻松地将路由表的名称与子网匹配。

单击 **Save** 按钮。

4.6.10 编辑面向第二个公共子网路由表的路由



选择面向公共子网的路由表。
示例：*public-usw-routes*

选择列表下方的 **Routes** 标签。

单击 **Edit routes** 按钮。

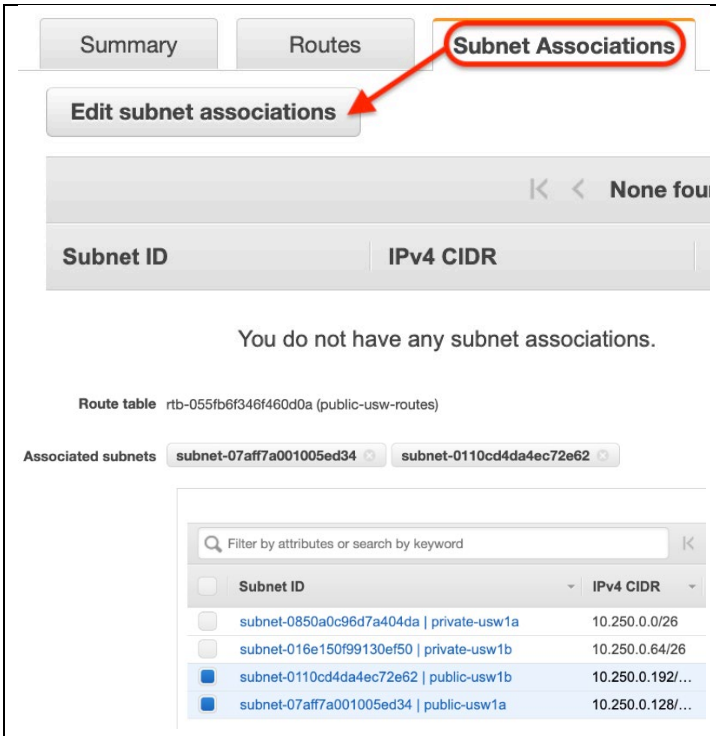
单击 **Add route** 按钮并设置以下值：

- **Destination**：*0.0.0.0/0*
- **Target**：选择您所部署的互联网网关。
  示例：*public-igw*

单击 **Save routes** 按钮。

单击 **Close** 按钮。

4.6.11 编辑面向第二个公共子网路由表的子网关联



选择 **Subnet Associations** 选项卡。

单击 **Edit subnet associations** 按钮。

选择两个公共子网以与此路由表进行关联。

单击 **Save** 按钮。

4.7 安全组

安全组充当虚拟机实例的虚拟防火墙，以控制传入和传出流量。稍后创建虚拟机时，我们将可以在其上附加一个或多个安全组。您可以随时修改安全组的规则。新规则和修改后的规则将自动应用于与安全组关联的所有实例。

创建安全组规则时，将指定来源和目标。这些可以表示为 IP 网络列表或安全组 ID。当您将安全组指定为规则的来源或目标时，该规则会影响与该安全组关联的所有实例。我们将在分布式服务器部署中使用此功能，以允许 Intel EMA 虚拟机之间的流量传输，而不必过于广泛，并允许私有网络中的所有流量传输，这遵循最小特权安全性最佳实践。

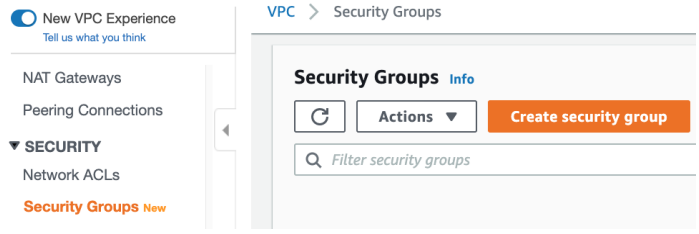
在以下过程中，我们将创建一个安全组来控制对 Intel EMA 虚拟机的访问，并创建一个单独的组来控制对数据库的访问。

有关 VPC 安全组的更多信息，请访问以下链接:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

4.7.1 创建面向虚拟机的安全组

注意：以下示例图像中的某些源地 止已被删除，因为它们特定于您自己的网络环境，因此不应逐字复制。您应该改用自己的受信任网络。

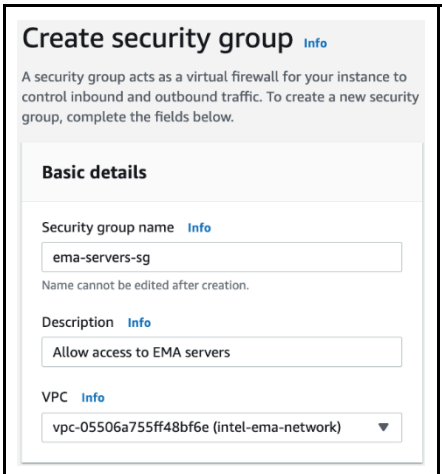
4.7.1.1 创建安全组



在 **VPC** 部分的侧栏中，选择 **Security Groups。**

单击 **Create security group** 按钮。

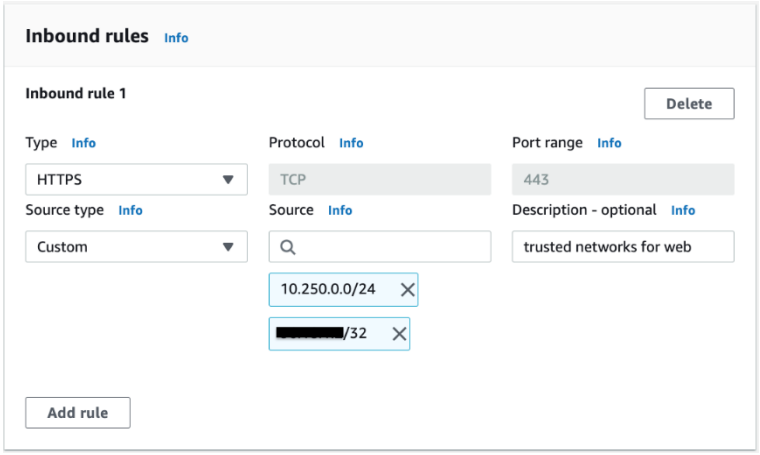
4.7.1.2 配置安全组基本详细信息



输入将允许访问 EMA 服务器的安全组的基本详细信息。

- **Security group name**：请输入唯一的名称。
  示例：*ema-server-sg*
- **Description**（可选）：输入安全组的说明。
  示例：*Allow access to EMA servers*
- **VPC**：选择您之前创建的 VPC。

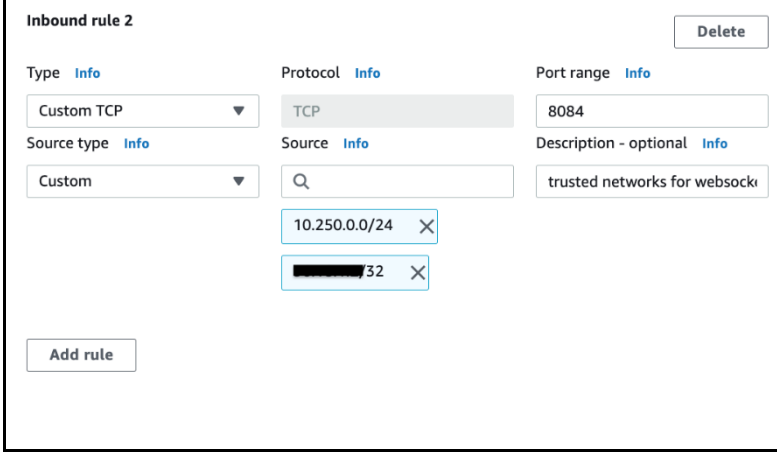
4.7.1.3 为 Web 流量添加入站规则



使用以下设置添加入站规则。

- **Type**: *HTTPS*
- **Description**: *Trusted network(s) for web*
- **Source**：输入 VPC CIDR 块以允许进行运行状况检查。
  示例：*10.250.0.0/24*
  您也可以输入允许访问 EMA Web UI 的其他网络，例如服务台流量源自的公共网络。

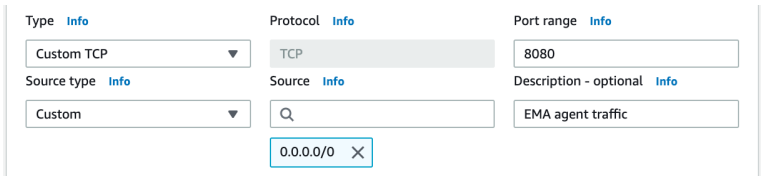
4.7.1.4 为 Websocket 流量添加入站规则



使用以下设置添加入站规则。

- **Type**: *Custom TCP*
- **Port range**: *8084*
- **Description**: *Trusted network(s) for websocket*
- **Source**：输入 VPC CIDR 块以允许进行运行状况检查。
  示例：*10.250.0.0/24*
  您也可以输入允许访问 EMA Web UI 的其他网络，例如服务台流量源自的公共网络。

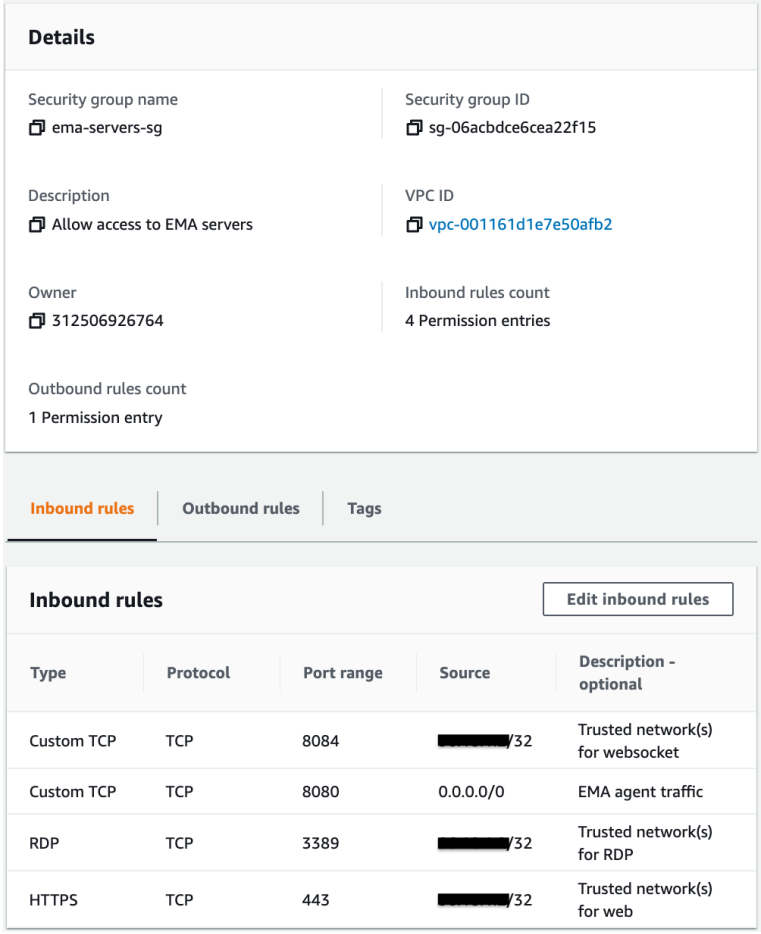
4.7.1.5 为集群流量添加入站规则



使用以下设置添加入站规则。

- **Type**: *Custom TCP*
- **Port range**: *8080*
- **Description**: *EMA agent traffic*
- **Source**: *0.0.0.0/0*

4.7.1.6 创建和审查



单击 **Create security group** 按钮以保存规则。

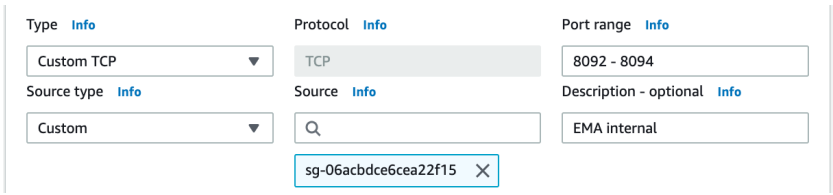
审查规则列表是否正确无误。

注意：我们将出站规则保留为默认规则，该规则允许所有出站流量传输。

4.7.2 更新安全组以允许 Intel EMA 虚拟机之间的流量传输（仅限分布式服务器）

现在，我们已经创建了 ema-server-sg 安全组，单击 **Edit inbound rules** 按钮，然后进行以下更改。

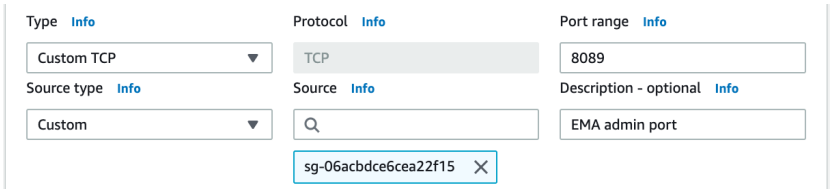
4.7.2.1 为端口 8092-8094 添加内部流量入站规则



使用以下设置添加入站规则。

- **Type**: C*ust*om TCP
- **Port range**:*8092-8094*
- **Description**: *EMA internal*
- **Source**：单击空白文本框，然后选择在上一步中创建的安全组的名称。

4.7.2.2 为端口 8089 添加内部流量入站规则



使用以下设置添加入站规则。

- **Type**: C*ust*om TCP
- **Port range**:*8089*
- **Description**: *EMA admin port*
- **Source**：单击空白文本框，然后选择在上一步中创建的安全组的名称。

4.7.2.3 保存并审查最终列表是否正确无误

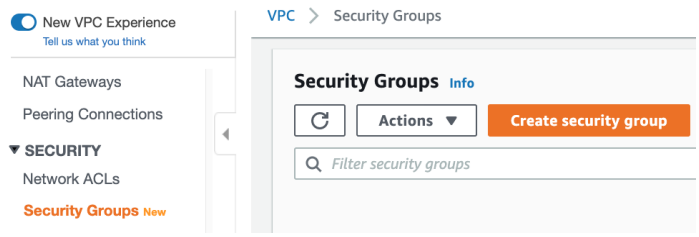
单击 **Save rules** 按钮。审查规则是否正确无误。

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 创建面向数据库的安全组

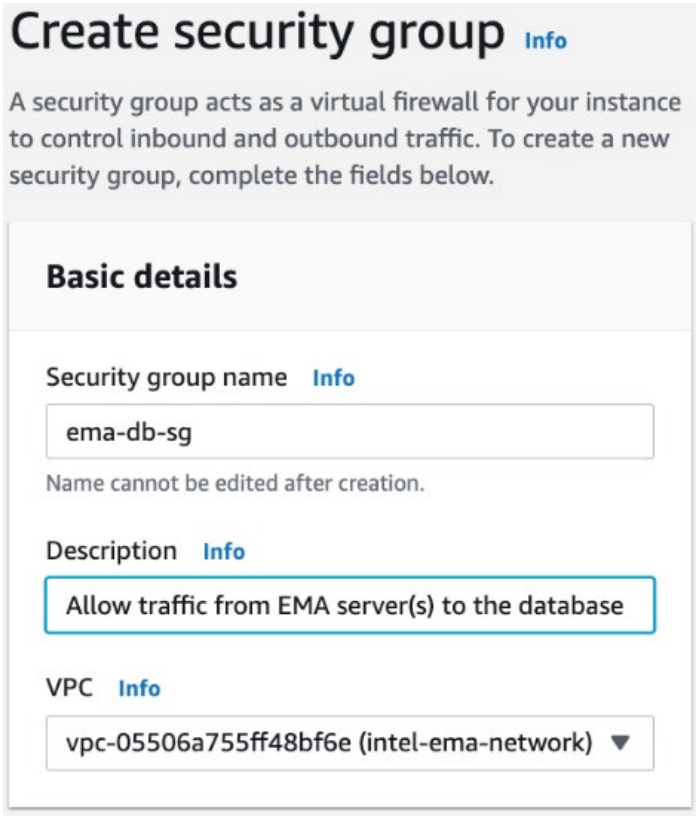
4.7.3.1 创建安全组



在 **VPC** 部分的侧栏中，选择 **Security Groups**。

单击 **Create security group** 按钮。

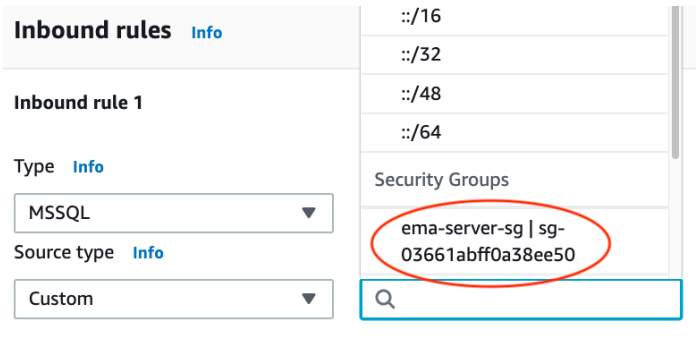
4.7.3.2 配置安全组基本详细信息



输入将允许访问 EMA 服务器的安全组的基本详细信息。

- **Security group name**：请输入唯一的名称。
  示例：*ema-db-sg*
- **Description**（可选）：输入安全组的说明。
  示例：*Allow traffic from EMA server(s) to the database*
- **VPC**：选择您之前创建的 VPC。

4.7.3.3 为 MSSQL 添加入站规则

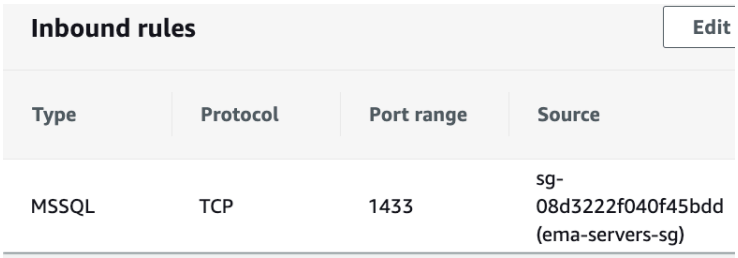


使用以下设置添加入站规则。

- **Type**: *MSSQL*
- **Source**：单击空白文本框，然后为之前创建的 EMA 服务器选择安全组。

4.7.3.4 创建和审查

单击 **Create security group** 按钮。审查规则列表是否正确无误。



5 虚拟机部署

5.1 概述

Amazon Elastic Compute Cloud* (Amazon EC2) 为您提供了计算虚拟化的灵活性，而无需购买和维护用以运行的物理硬件。但是，您仍然有责任维护来宾操作系统及其中运行的软件。

您将在创建时决定要分配给 EC2 实例的 CPU、内存和存储数量，但是您可以稍后增加这些配额，也可以减少 CPU 和内存数量，以便针对工作量优化虚拟机，从而降低成本。

EC2 使用 EC2 密钥对保护实例的登录安全（AWS 存储公钥，而您将私钥存储在安全的地方）。它可以预先创建，也可以在创建 EC2 实例时创建。您将需要私钥，以便为基于 Windows 的实例检索自动生成的管理员凭据。EC2 中可以有多个密钥对，但是您只能将一个实例与一个密钥对相关联，并且在实例创建后就不能对其进行更改。

创建实例时或之后的任何时间，可以通过附加一个或多个安全组来保护对 EC2 实例的网络访问。上一部分已经配置了我们所需的安全组。

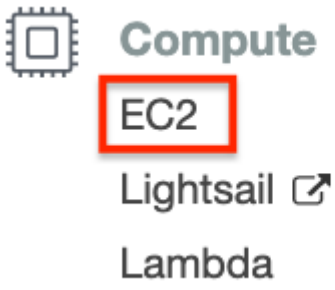
对于分布式服务器部署，下面的过程以及其他部分中包含其他步骤，您可以跳过这些步骤以进行单服务器部署。其中包括创建第二个虚拟机，将虚拟机与目标组关联，将目标组连接到负载均衡器，并配置负载均衡器转发规则。

有关 EC2 实例或密钥对的更多信息，请访问以下链接：
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-key-pairs.html

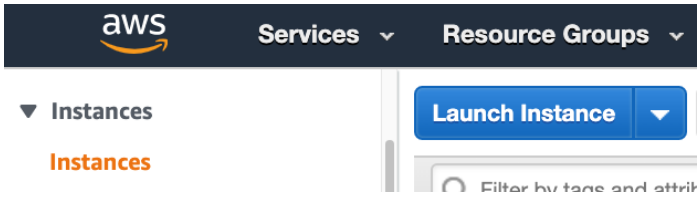
5.2 创建虚拟机

请按照以下过程使用最新的 Windows Server 映像为 Intel EMA 服务器创建 EC2 实例，并连接我们之前创建的安全组。

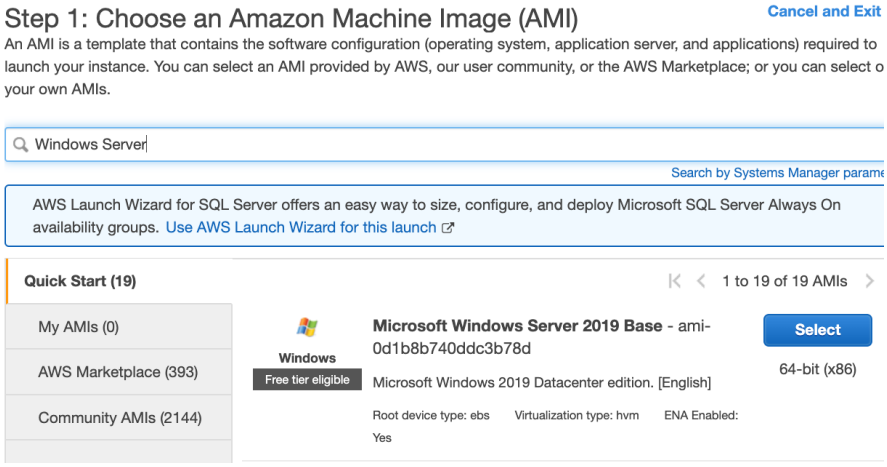
5.2.1 导航至 EC2 服务

	在 **Services** 菜单的 **Compute** 部分下，选择 **EC2**。

5.2.2 启动 EC2 实例

	在边栏上选择 **Instances**，然后单击 **Launch Instance** 按钮。

5.2.3 选择 Amazon Machine 映像

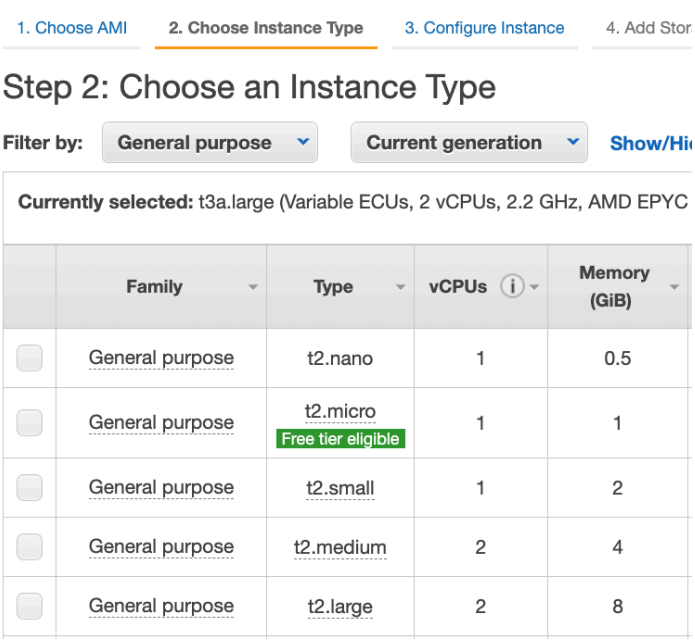


搜索 Intel EMA 支持的最新 Microsoft Windows* Server Base 映像。

有关支持的操作系统，请参阅《Intel® Endpoint Management Assistant Server 安装指南》。

单击 **Select** 按钮。

5.2.4 选择机器类型

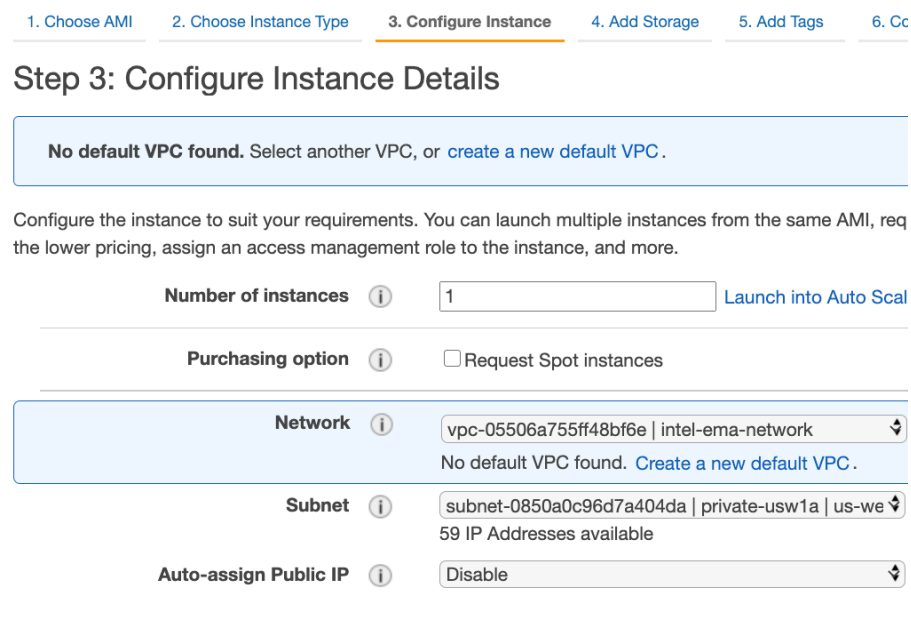


选择具有所需 CPU 和内存资源容量的机器类型。如果需要，您可以稍后在实例关闭电源时更改此设置。

有关系统要求，请参阅《Intel® Endpoint Management Assistant Server 安装指南》。

单击 **Next: Configure Instance Details** 按钮。

5.2.5 配置实例详细信息



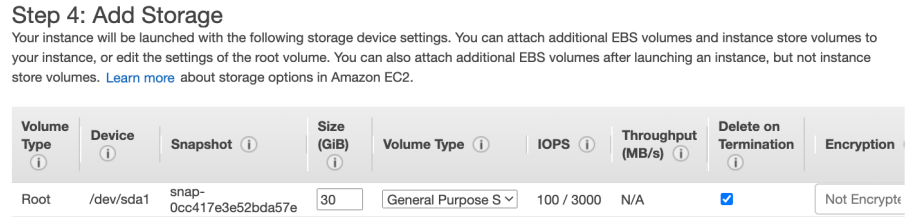
按如下配置实例详细信息：

- **Network: 设置**为之前创建的 VPC。
  示例：*intel-ema-network*
- **Subnet**：选择一个私有子网。
  示例：*private-usw1a*
- **Auto-assign Public IP**: *Disable*

此屏幕上的其余实例详细信息可默认保留。

单击 **Next: Add Storage** 按钮。

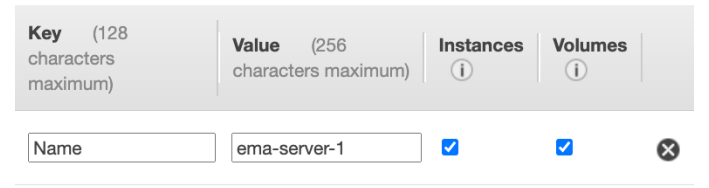
5.2.6 添加存储



除非您需要更多空间，否则存储设置可以保留为默认设置。有关系统要求，请参阅《Intel® Endpoint Management Assistant Server 安装指南》。

单击 **Next: Add Tags** 按钮。

5.2.7 添加标签

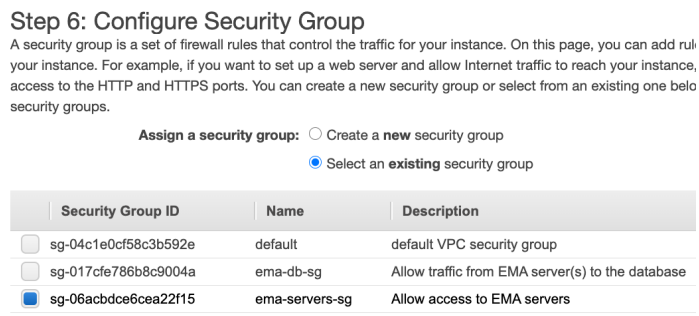


添加带有键 "Name" 和所需服务器名称的值的标签。

如之前在“简介”的“标签和资源组”部分所述，可以添加您希望帮助组织资源的任何其他自定义标签。

单击 **Next: Configure Security Group** 按钮。

5.2.8 配置安全组



将 **Assign a security group** 按钮设置为 *Select an existing security group*。

选择您之前为 Intel EMA 服务器创建的安全组。
示例： *ema-servers-sg*

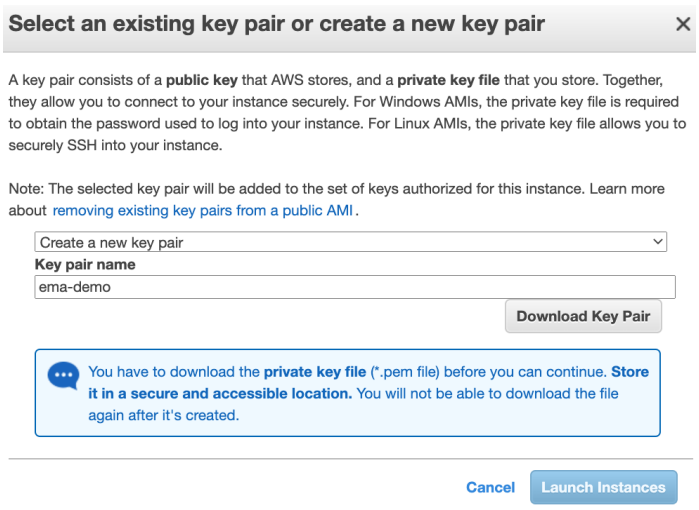
单击 **Next: Review and Launch** 按钮。

您可能会收到这样一条警告：由于安全组未打开端口 3389 (RDP)，您将无法连接到实例。您可以忽略该消息并继续，因为我们还有另一种访问虚拟机的方法。

5.2.9 审查实例启动

审查实例详细信息，然后单击 **Launch** 按钮。

5.2.10 选择一个 EC2 密钥对



系统将提示您选择现有的密钥对或创建新的密钥对。

从列表中选择适当的密钥对，或者使用该选项创建一个新的密钥对，然后单击 **Download Key Pair** 按钮将私钥文件保存到您的计算机。

如果选择使用现有的密钥对，则必须有权访问私钥文件。

单击 **Launch Instances** 按钮。

5.3 创建第二个 EC2 实例（仅分布式服务器）

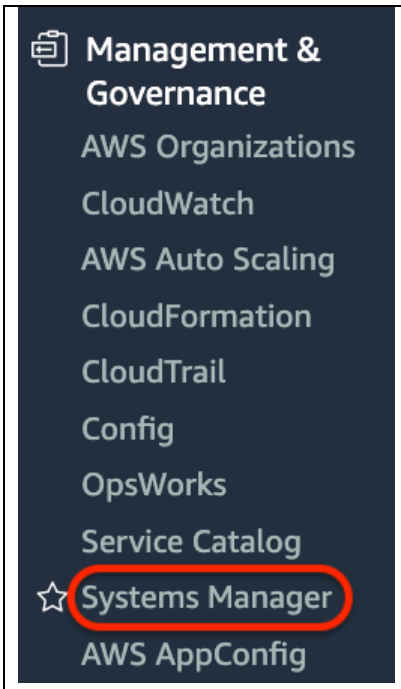
对于分布式服务器部署，请重复上述步骤以创建第二个 Intel EMA 服务器，选择其他子网并为其分配一个不同的 Name 标签，例如 *ema-server-2*。

6 配置 AWS Systems Manager（仅分布式服务器）

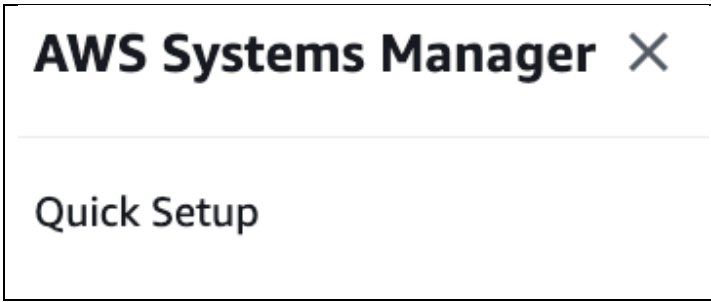
AWS Systems Manager 是一项服务，可让您更好地了解和控制 AWS 上的基础架构。我们需要启用它以使用 Session Manager 组件，该组件将使我们能够远程访问没有公共 IP 地址的虚拟机。

有关 Systems Manager 的更多信息，请访问以下链接：https://aws.amazon.com/systems-manager/

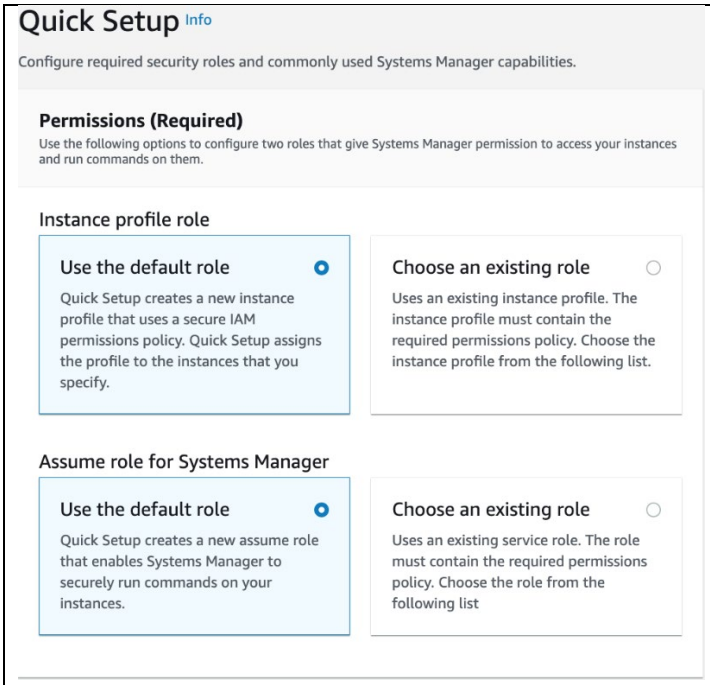
6.1 导航至 Systems Manager 服务

	在 Services 菜单的 Management & Governance 部分下，选择 Systems Manager。

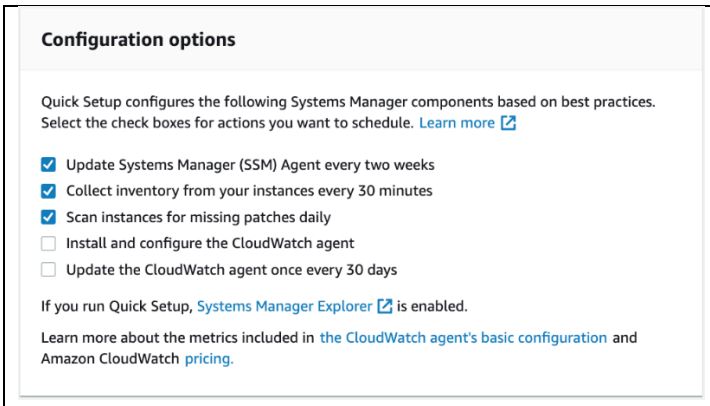
6.2 开始快速设置

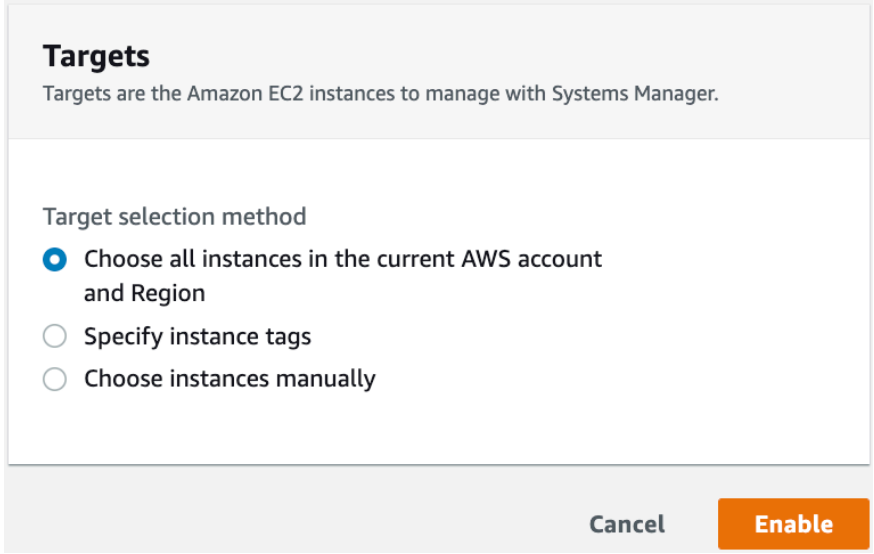
6.3 选择权限选项



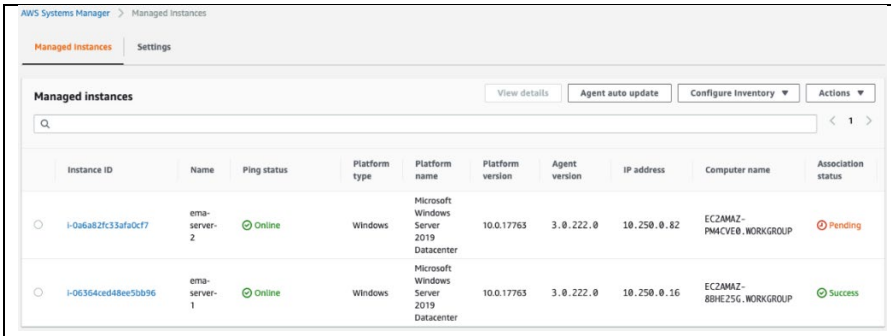
6.4 选择配置选项



6.5 选择目标



6.6 验证托管实例列表



从 Systems Manager 侧栏中，选择 Managed Instances。

首次运行快速设置后，虚拟机可能需要几分钟的时间才能显示在此列表中。

当您的虚拟机成功注册到 System Manager 后，您将在此处看到。

6.7 通过 Session Manager 登录到虚拟机

通过 AWS 控制台使用 Session Manager 只能使您连接到虚拟机上的 Powershell* 会话。为了与 RDP 连接，我们需要使用 AWS Command Line Interface (AWS CLI) 从本地命令行调用会话管理器，并传入一个选项以启用端口转发。

安装 AWS CLI 超出了本文档的范围。请参阅 https://aws.amazon.com/cli/ 以了解更多信息。

安装并配置 CLI 并在 AWS System Manager 中显示虚拟机之后，可以使用以下语法运行 CLI 命令：

```
aws ssm start-session --target <instanceId> --document-name AWS-
StartPortForwardingSession --parameters
"localPortNumber=55678,portNumber=3389"
```

将 <instanceId> 替换为希望连接的 EC2 实例 ID。示例：i-06364ced48ee5bb96

如果此命令成功，那么您将能够使用远程桌面客户端以您指定的 localPortNumber 连接到本地主机。然后，您可以使用该虚拟机的凭据登录。

7 Relational Database Service (RDS) 部署

AWS 具有名为 Amazon Relational Database Service (Amazon RDS) 的完全托管的平台即服务数据库引擎，该引擎可轻松在 AWS Cloud 中设置、操作和扩展关系数据库。它提供具有成本效益的、可调整大小的容量，并管理常见的数据库管理任务，包括备份、软件修补、自动故障检测和恢复。

Amazon RDS 的基本构建模块是数据库实例。数据库实例是 AWS Cloud 中的隔离数据库环境。您的数据库实例可以包含多个用户创建的数据库。您可以使用与独立数据库实例相同的工具和应用程序来访问数据库实例。数据库实例的计算和内存容量由其数据库实例类确定。您可以选择最能满足您需求的数据库实例。如果您的需求随时间变化，可以更改数据库实例。

由于我们的 VPC 是在不同可用区中的多个子网创建的，因此我们将能够使用称为多可用区部署的选项启动 RDS 实例。通过为我们的生产部署选择此选项，您的主数据库实例将自动同步复制到另一个可用区中的辅助备用数据库实例。这种方法有助于提供数据冗余和故障转移支持，消除 I/O 冻结，并最大程度地减少系统备份期间的延迟峰值。我们将创建一个数据库子网组，该组将通知 RDS 为此目的使用哪些可用区。

我们之前在本指南中创建的安全组将用于控制对 RDS 实例的访问，并且仅允许我们的 Intel EMA EC2 实例与其连接。

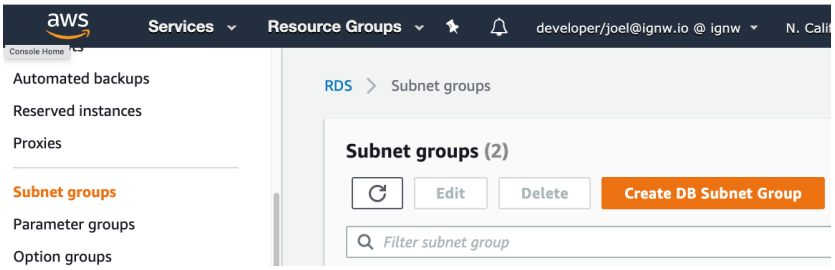
有关 RDS 的更多信息，请访问以下链接：
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

请按照以下过程创建 Relational Database Service (RDS) 实例，并附加先前创建的安全组，以允许从 Intel EMA EC2 实例到数据库的流量进入。

7.1 导航至 RDS 服务

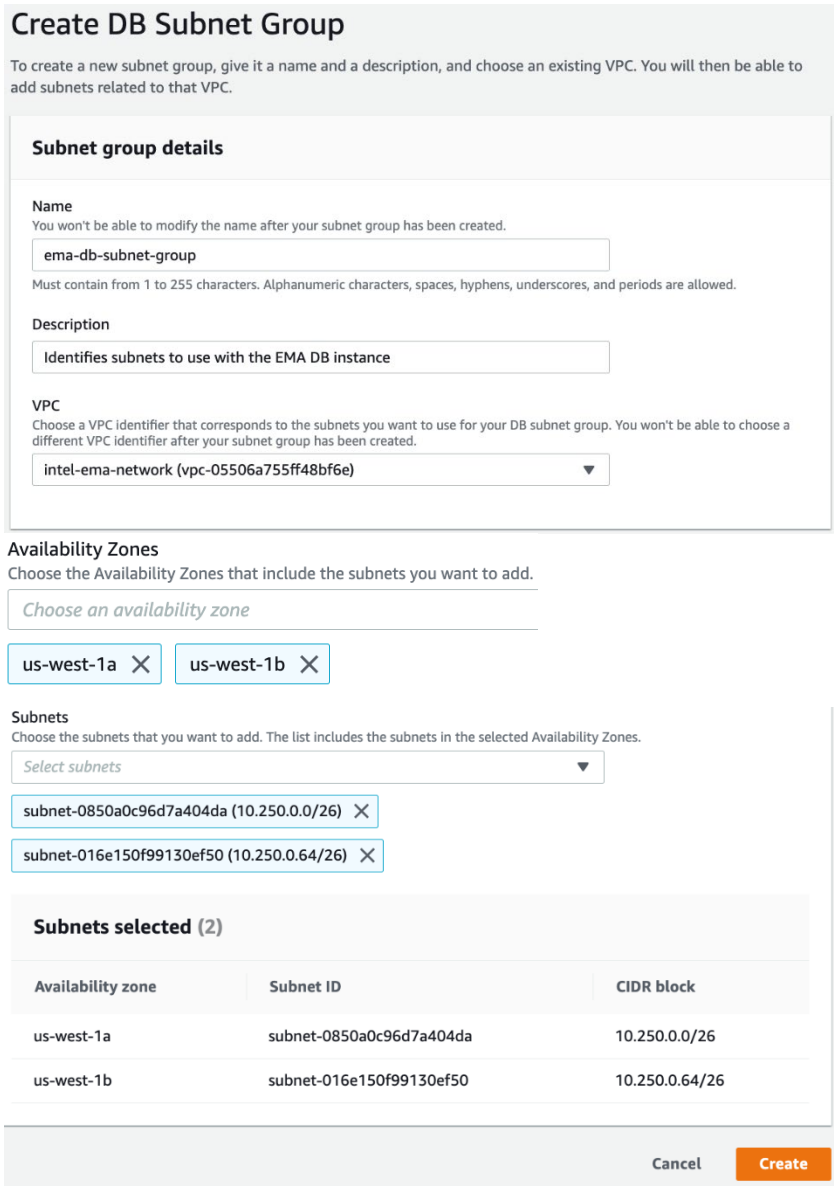
从 **Services** 菜单的 **Database** 下，选择 **RDS**。

7.2 创建数据库子网组



从 **RDS** 侧栏中，选择 **Subnet groups**，然后单击 **Create DB Subnet Group** 按钮。

7.2.1 子网组详细信息

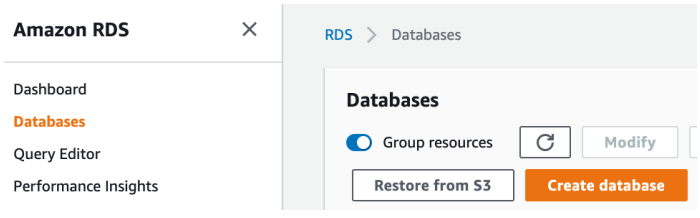


按如下所示输入子网组详细信息。

- **Name**：请输入唯一的名称。
  示例：*ema-db-subnet-group*
- **Description**（可选）
  示例：*Identifies subnets to use with the EMA DB instance*
- **VPC**：选择您之前创建的 VPC。
- **Availability Zones**：选择创建子网的两个区。
- **Subnets**：选择之前创建的两个私有子网。

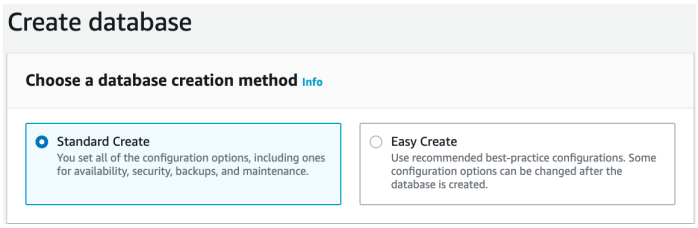
单击 **Create** 按钮。

7.3 创建数据库



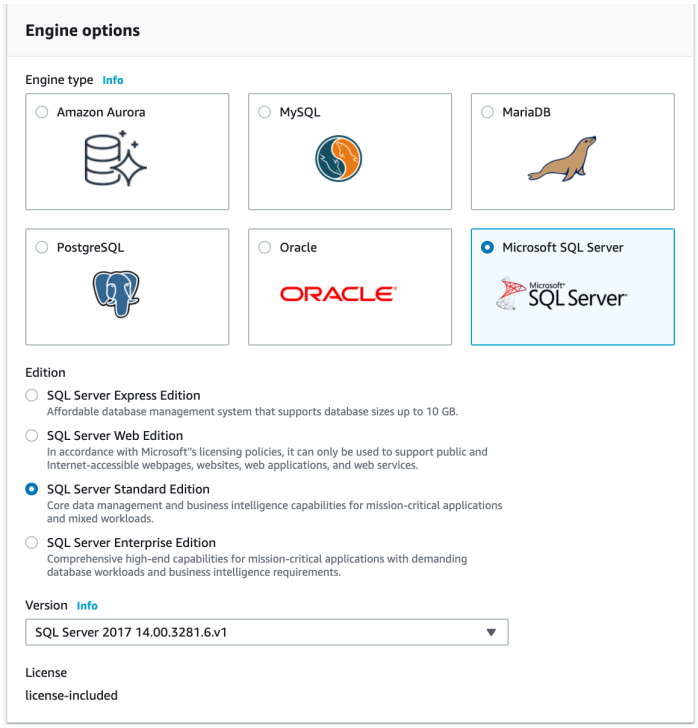
从 RDS 侧栏中，选择 Databases，然后单击 **Create database** 按钮。

7.3.1 选择数据库创建方法



选择 **Standard Create** 数据库创建方法。

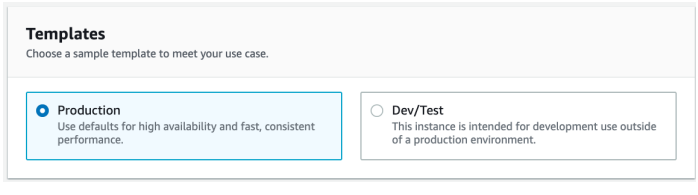
7.3.2 选择引擎类型和版本



选择 **Microsoft SQL Server** 引擎。

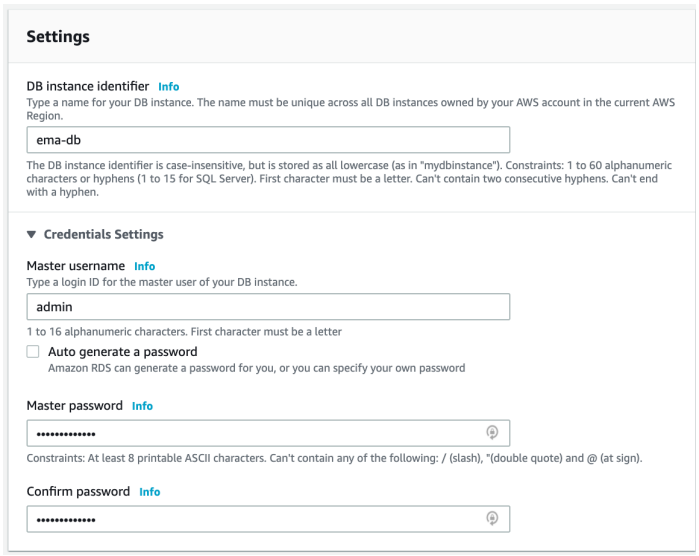
选择合适的 SQL Server 版本。就本文档而言，我们假设使用 SQL Server Standard Edition 进行生产部署。SQL Server Express Edition 可用于开发和测试以降低成本。

7.3.3 选择部署模板



在 Templates 部分选择 **Production**。

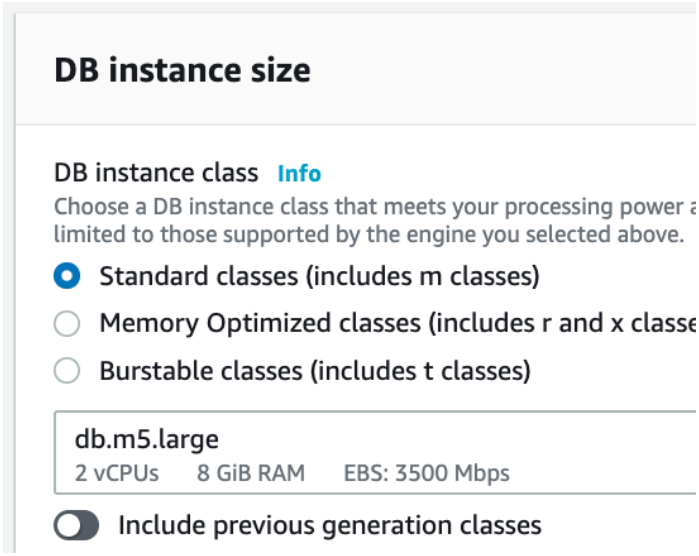
7.3.4 配置实例名称和主用户凭据



为数据库指定一个唯一的名称。
示例：*ema-db*

创建用户名和密码。

7.3.5 配置数据库实例大小

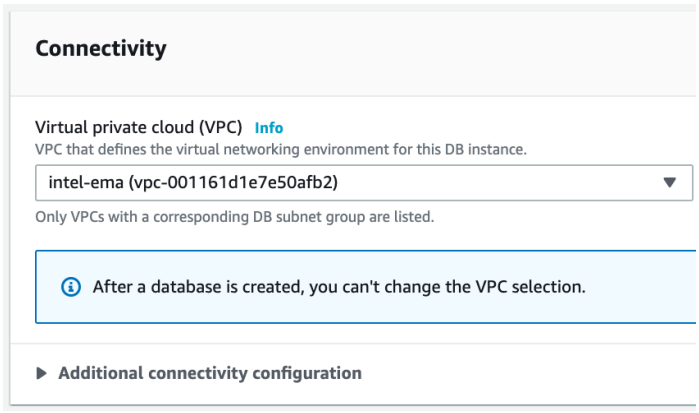


设置数据库实例类以提供足够的资源。
建议：*db.m5.large*

7.3.6 配置存储（可选）

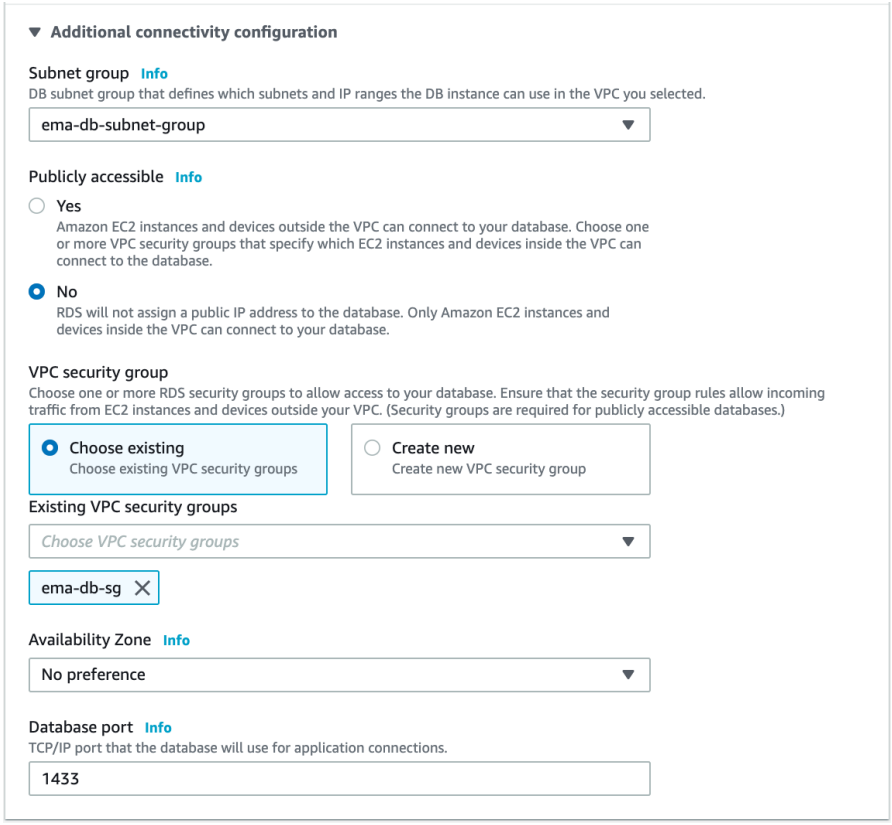
如您需要，可以增加分配的默认存储容量。我们将保留默认值。您仍然可以在之后增加存储容量。

7.3.7 配置连接性



在 **Connectivity** 中，选择先前创建的 VPC，然后展开 **Additional connectivity configuration** 部分。

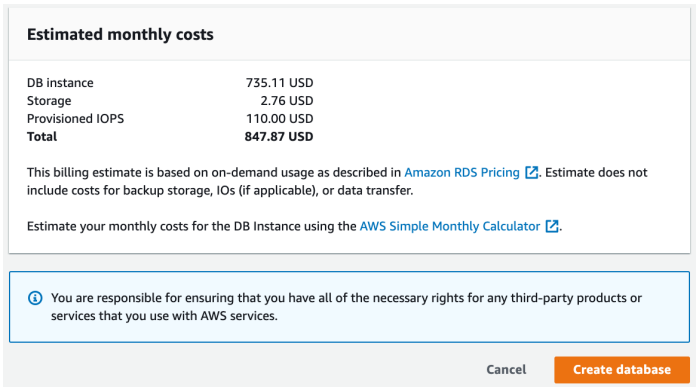
7.3.8 配置连接性 - 其他连接性配置



选择您之前创建的数据库子网组。

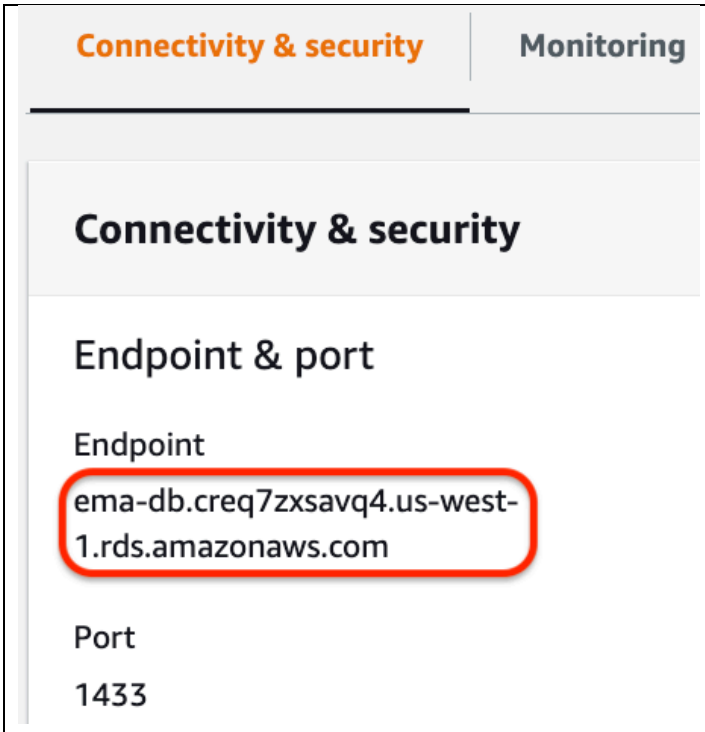
取消选择默认的 VPC 安全组，然后选择之前为数据库创建的现有安全组。

7.3.9 查看和创建



审查估计成本，然后单击 **Create database** 按钮。

7.4 获取数据库主机名



数据库完成部署后，详细信息页面将显示数据库主机名，您将在安装过程中使用该主机名来配置 Intel EMA 软件。

8 负载均衡器部署（仅限于分布式服务器）

8.1 概述

AWS Network Load Balancer 是第 4 层 (TCP) 负载均衡器，可在应用程序的多个实例之间分配用户流量。通过分散负载，负载平衡可降低应用程序负担过重、运行缓慢或无法工作的风险。负载均衡器收到连接请求后，会根据转发规则从关联的目标组中选择运行状况良好的目标，并将连接转发到该目标。

*侦听器*使用您配置的协议和端口检查来自客户端的连接请求，并将请求转发到目标组。

每个*目标组*使用您指定的协议和端口号将请求发送到一个或多个注册目标，例如 EC2 实例。您可以基于每个目标组配置运行状况检查。对目标组注册的所有目标执行运行状况检查，该目标组是在负载均衡器的侦听器规则中指定的。

我们将为我们部署的负载均衡器启用多个可用区，以便我们可以将流量引导至任一区中的目标。

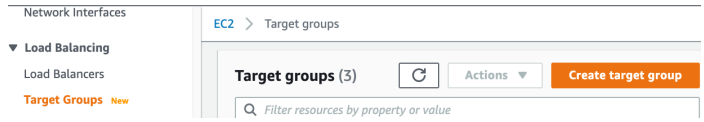
负载均衡器会有一个自动生成的主机名，该主机名将指向每个可用区中相关负载均衡器的面向公众的地 止。您将要创建一个别名为该主机名的 DNS CNAME 记录，以便使用您的自定义域来访问 Intel EMA 服务器。

还有其他负载均衡配置的可能性，本文档未涵盖。您应该向 IT 部门咨询可能需要实施的任何要求或实践。有关在 AWS 中进行负载均衡的更多信息，请访问以下链接：
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

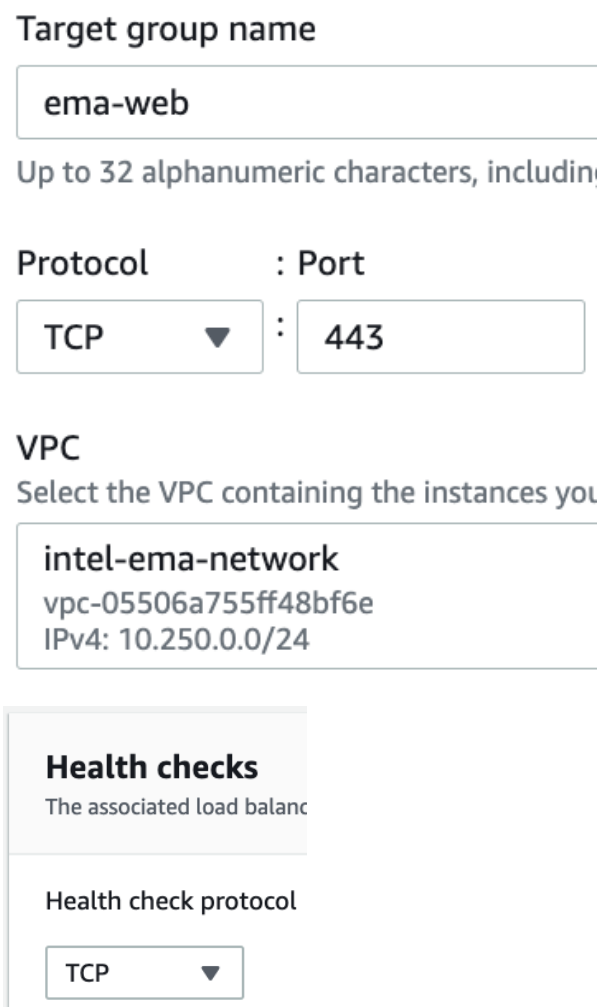
8.2 创建目标组

按照此过程为负载均衡器将要服务的每个 TCP 端口创建一个目标组，创建运行状况检查，并注册我们的虚拟机以接收每个目标组的流量。

8.2.1 创建目标组

	在 **EC2** 侧栏中的 **Load Balancing** 部分，选择 **Target Groups**。 单击 **Create target group** 按钮。

8.2.2 配置面向 TCP/443 的目标组

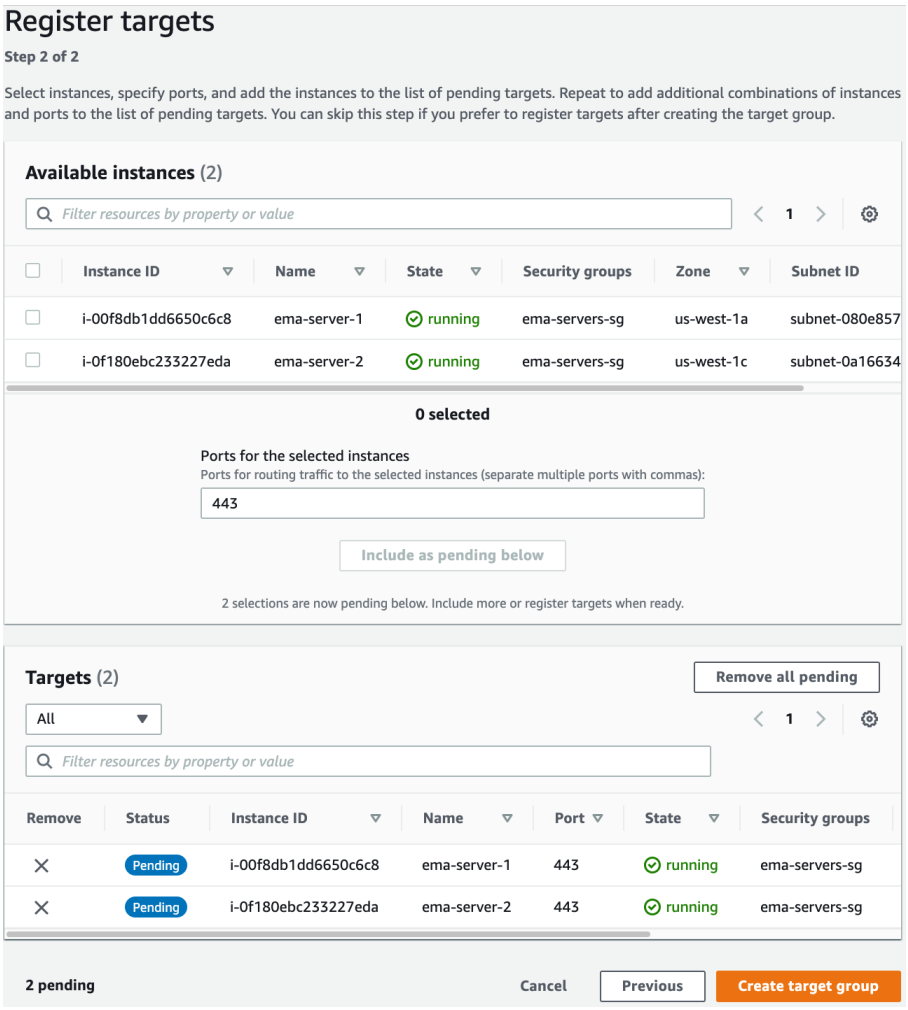


按如下所示配置目标组：

- **Target type**: *Instances*
- **Target group name**：请输入唯一的名称。
  示例：*ema-web*
- **Protocol**: *TCP*
- **Port**: *443*
- **VPC**：选择您之前创建的 VPC。
- **Health check protocol**: *TCP*

单击 **Next** 进入 **Register targets** 屏幕。

8.2.2.1 将两个 EC2 实例注册为目标



选择两个 EMA 虚拟机实例，然后单击 **Include as pending below** 按钮。

单击 **Create target group** 按钮。

8.2.3 创建/配置面向 TCP/8084 的目标

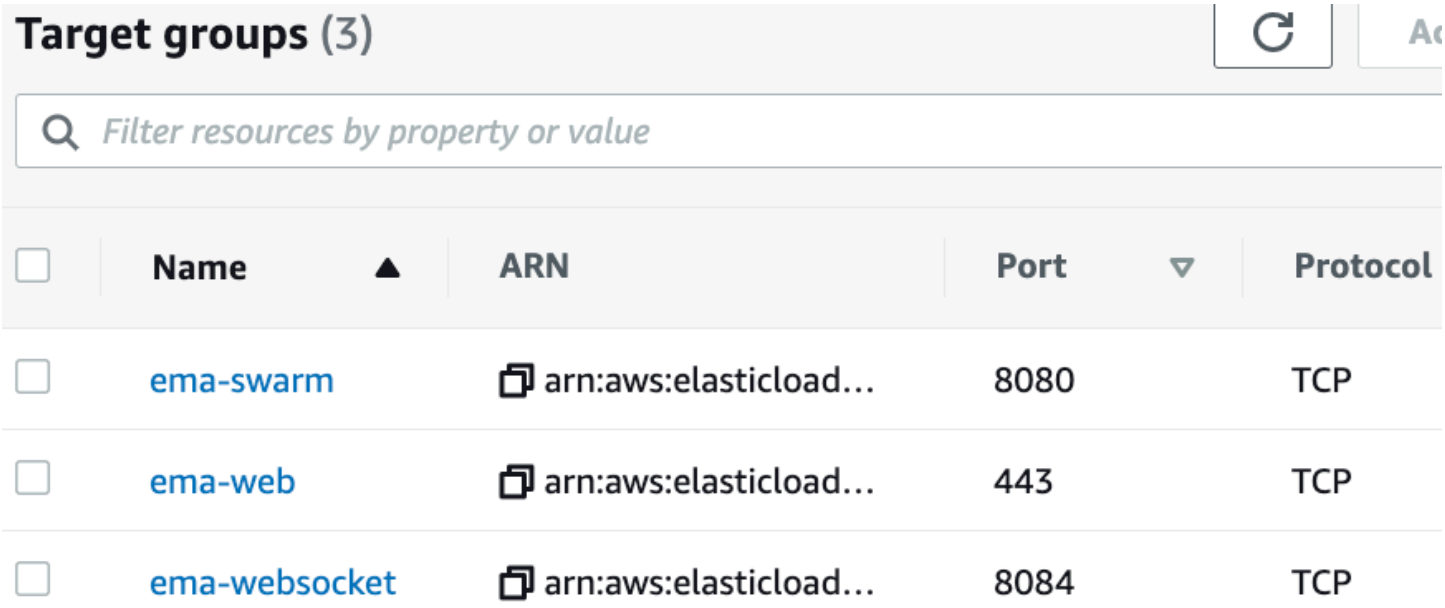
对面向 TCP/8084 名为“ema-websocket”的另一个目标组重复上述步骤。

8.2.4 配置面向 TCP/8080 的目标

对面向 TCP/8080 名为“ema-swarm”的另一个目标组重复上述步骤。

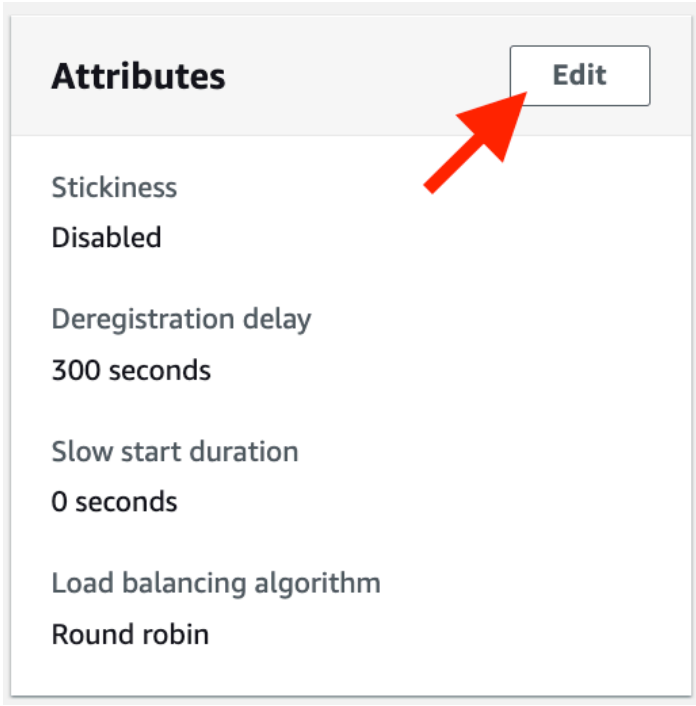
8.2.5 审查目标组

确定您已创建三个目标组。



8.2.6 为 TCP/443 目标组启用粘性

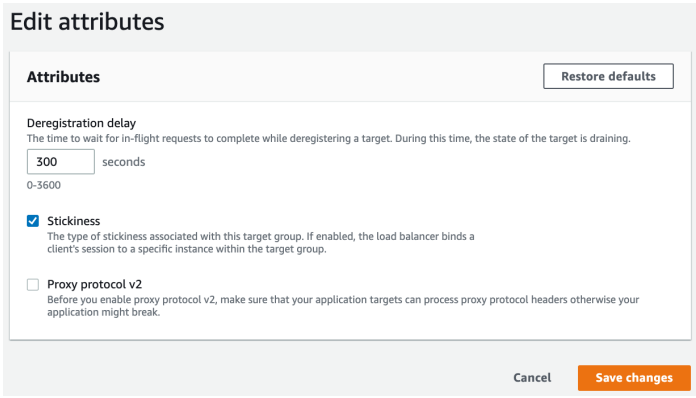
8.2.6.1 目标组详细信息



单击 *ema-web* 目标组名称以访问组详细信息屏幕。

在 **Attributes** 部分中，单击 **Edit** 按钮。

8.2.6.2 编辑属性



启用 **Stickiness** 标记。

单击 **Save changes** 按钮。

8.2.7 为 TCP/8084 目标组启用粘性

重复上述指示，为 ema-websocket (TCP/8084) 目标组启用粘性。

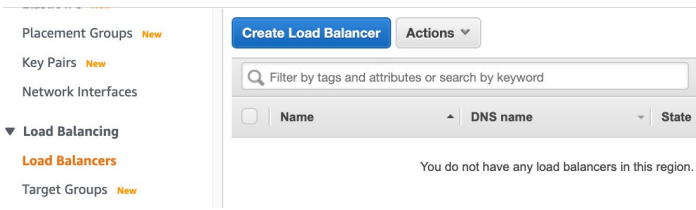
8.2.8 有关监视目标组运行状况的说明

在任何目标组中，您可以检查 **Targets** 和 **Monitoring** 选项卡以查看目标实例的运行状况检查状态。这些运行状况检查最初将失败，直至安装了 Intel EMA 软件。

8.3 创建面向网络流量的网络负载均衡器

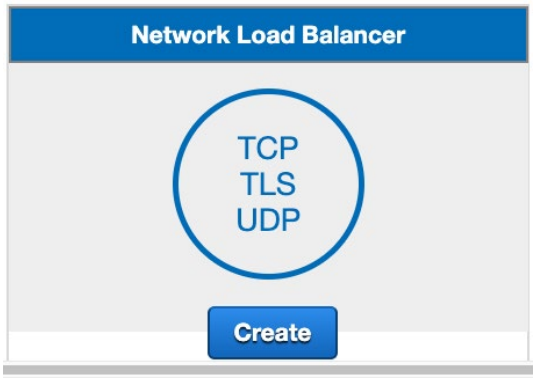
请按照以下过程创建网络负载均衡器，以将流量分配到正常的目标组。

8.3.1 创建负载均衡器



在 **EC2** 侧栏中的 **Load Balancing** 部分，选择 **Load Balancers**，然后单击 **Create Load Balancer**。

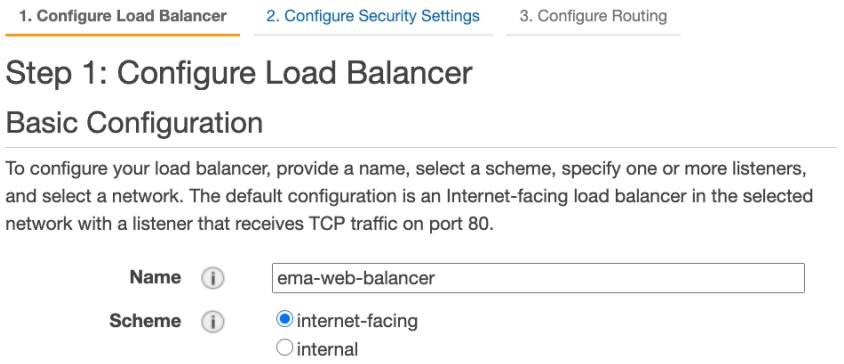
8.3.2 选择负载均衡器类型



单击 **Network Load Balancer** 标题下的 **Create** 按钮。

8.3.3 配置负载均衡器

8.3.3.1 基本配置



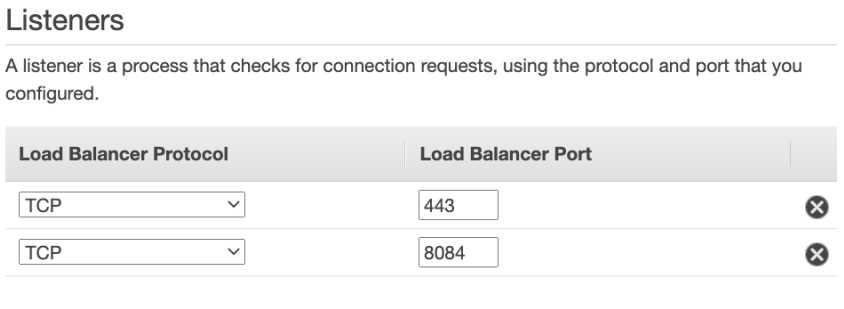
输入基本配置。

Name：请输入唯一的名称。
示例：*ema-web-balancer*

Scheme: internet-facing.
注意：如果您的组织具有一个带 AWS 的站点到站点 VPN，可以为您提供私有 IP 访问权限，则这可能是绑定到私有子网的内部负载均衡器。

对于本指南，我们假设没有此类访问权限，因此它将是绑定到公共子网的面向互联网的负载均衡器。

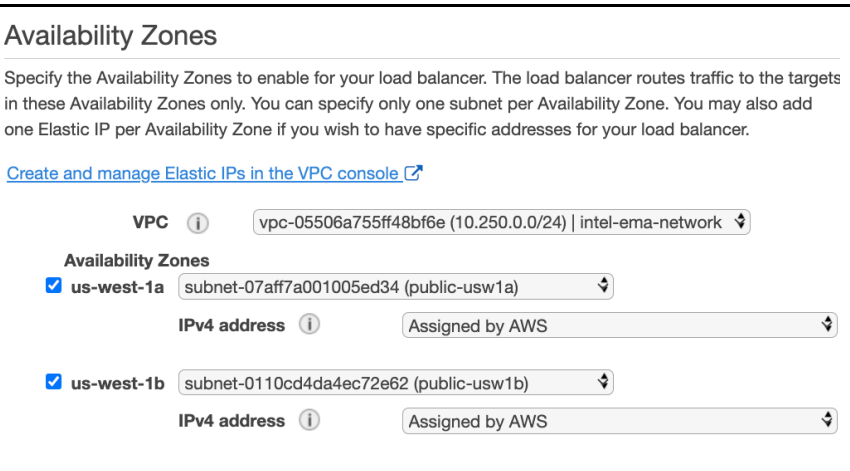
8.3.3.2 侦听器



在 **Listeners** 部分中，为这些协议和端口添加侦听器。

- *TCP 443*
- *TCP 8084*

8.3.3.3 可用区



按如下所示配置 **Availability Zones** 部分：

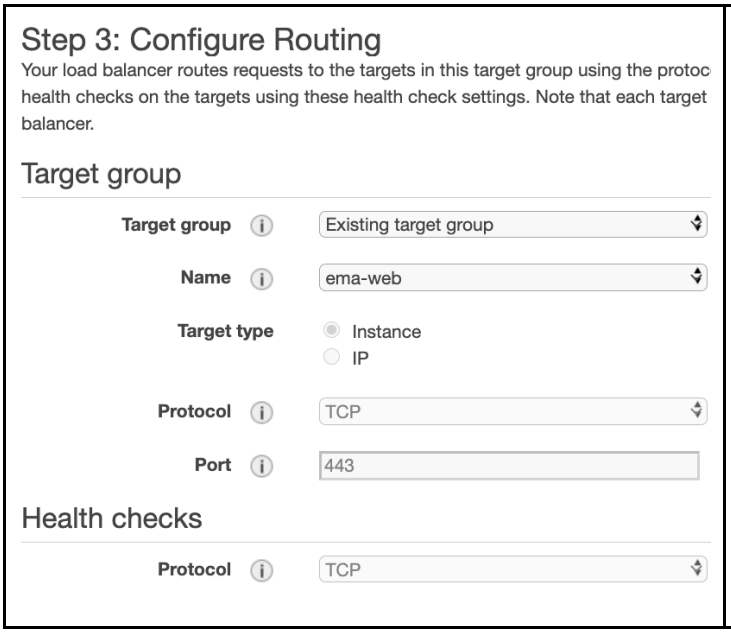
- **VPC**：选择您之前创建的 VPC。
- **Availability Zones**：启用两个可用区并选择两个公共子网。IPv4 address 应设置为 *Assigned by AWS*。

单击 **Next: Configure Security Settings** 按钮。

8.3.3.4 配置安全设置

在此步骤中，我们无需配置任何内容。单击 **Next: Configure Routing** 按钮。

8.3.3.5 配置路由

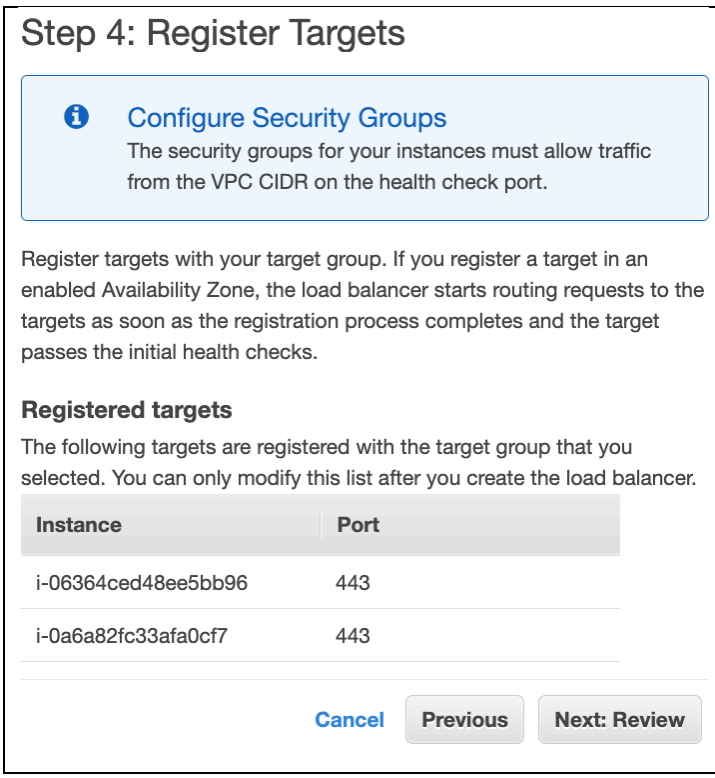


在 **Step 3: Configure Routing**，按如下所示配置 Target group。

- **Target group**: *Existing target group*
- **Name**: 选择您之前创建的 TCP/443 目标组的名称。
  示例： *ema-web*

单击 **Next: Register Targets** 按钮。

8.3.3.6 注册目标

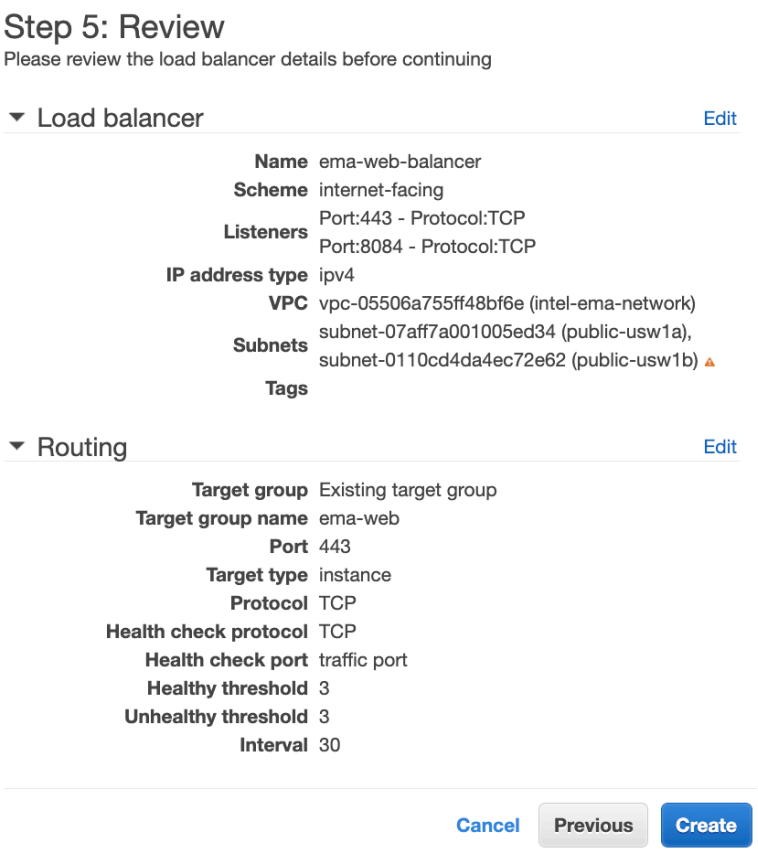


确认您看到两个所列实例为注册目标。

单击 **Next: Review** 按钮。

8.3.3.7 审阅

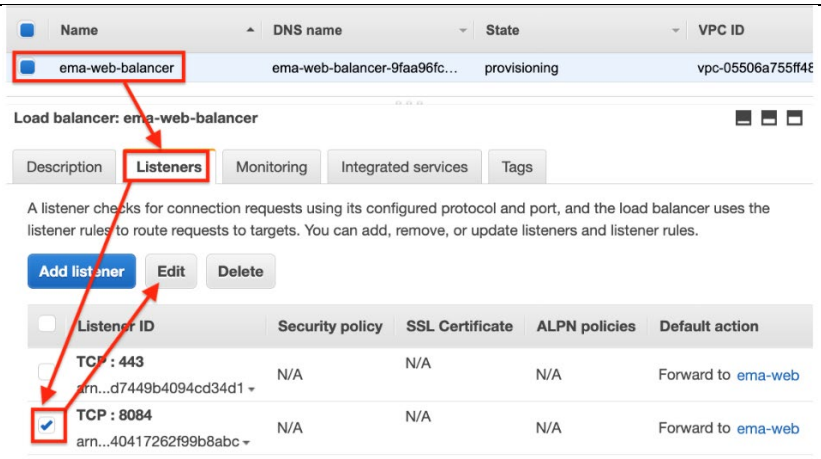
在 **Step 5: Review**，确认与此处提供的示例类似，然后单击 **Create** 按钮。



8.3.4 修复负载均衡器转发规则

转发目标对于端口 443 侦听器是正确的，但是我们现在需要编辑和更改端口 8084 的侦听器，以转发到正确的目标组。

8.3.4.1 编辑负载均衡器侦听器



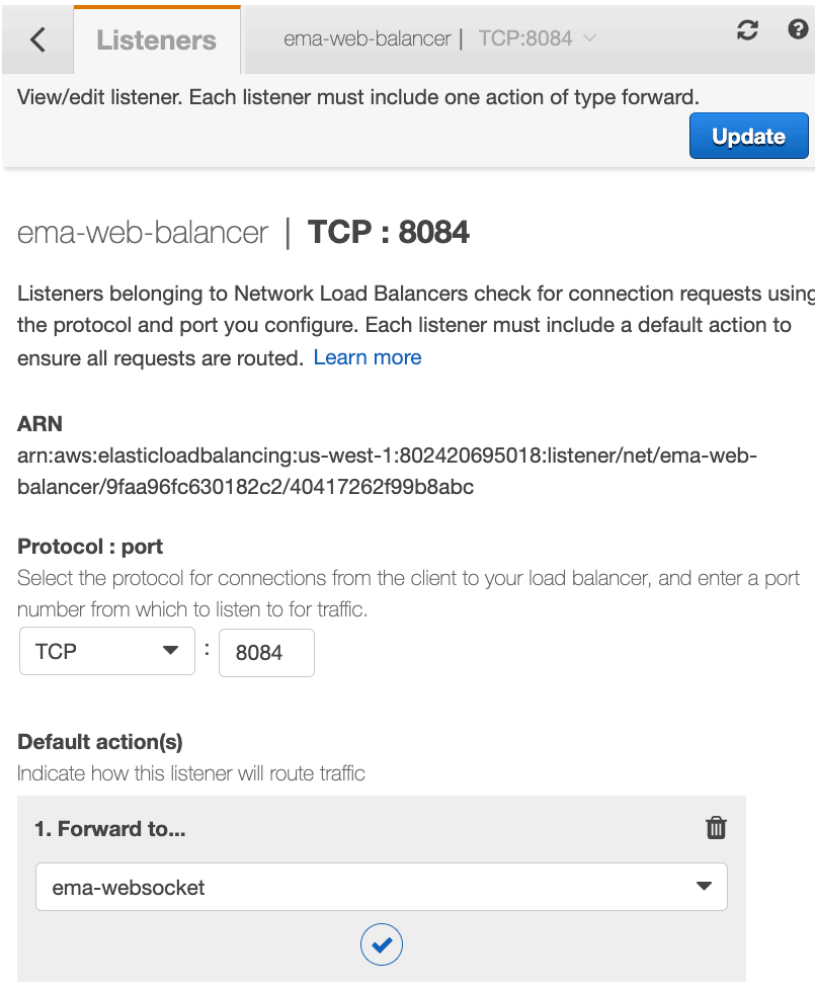
选择您所创建的负载均衡器。

选择 **Listeners** 选项卡。

选中 TCP/8084 侦听器旁边的复选框。

单击 **Edit** 按钮。

8.3.4.2 更新 TCP/8084 侦听器转发操作

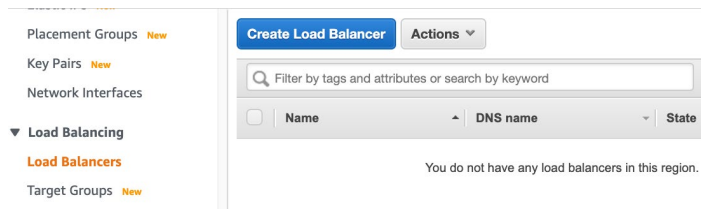


更改默认操作以转发到 websocket 侦听器。

单击 **Update** 按钮。

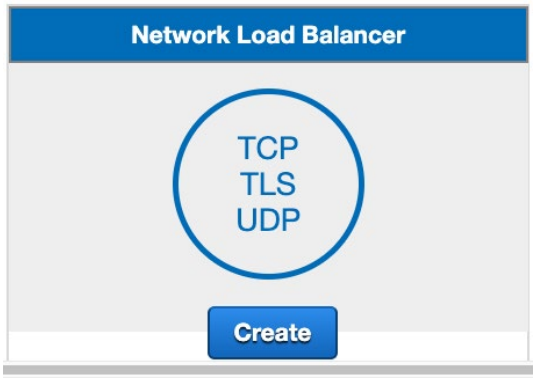
8.4 创建面向集群流量的网络负载均衡器

8.4.1 创建负载均衡器



在 **EC2** 侧栏中的 **Load Balancing** 部分，选择 **Load Balancers**，然后单击 **Create Load Balancer**。

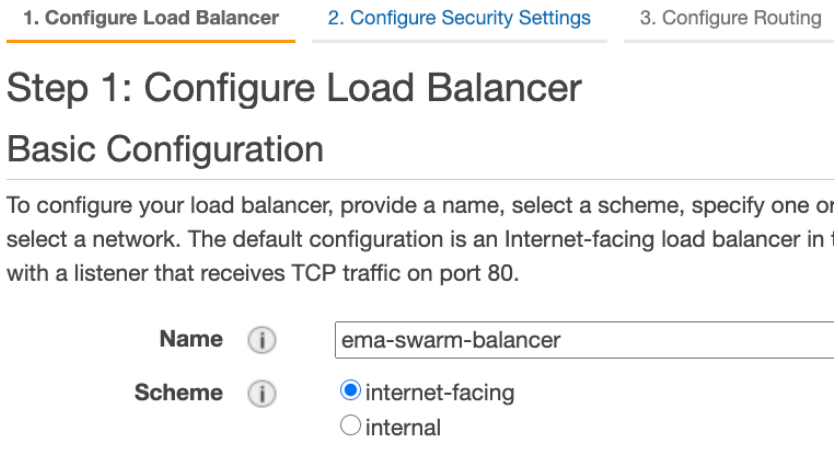
8.4.2 选择负载均衡器类型



单击 **Network Load Balancer** 标题下的 **Create** 按钮。

8.4.3 配置负载均衡器

8.4.3.1 基本配置

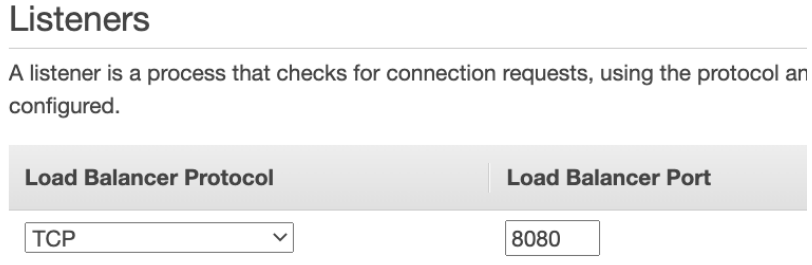


进入基本配置。

Name：请输入唯一的名称。
示例：*ema-swarm-balancer*

Scheme: internet-facing.

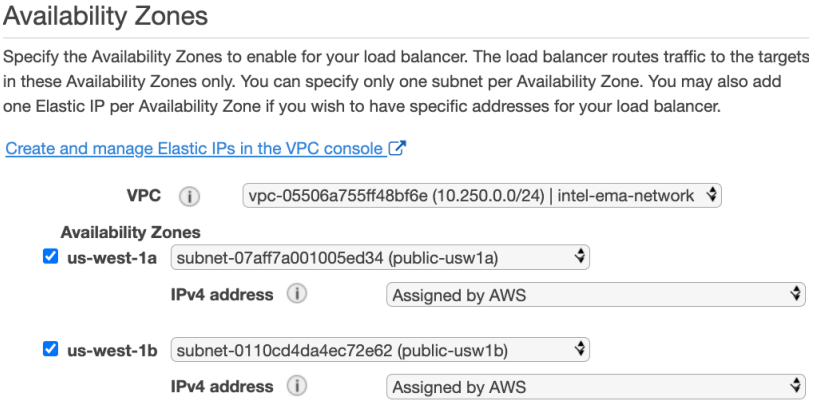
8.4.3.2 侦听器



在 **Listeners** 部分中，为这些协议和端口添加侦听器。

- *TCP 8080*

8.4.3.3 可用区



按如下所示配置 **Availability Zones** 部分：

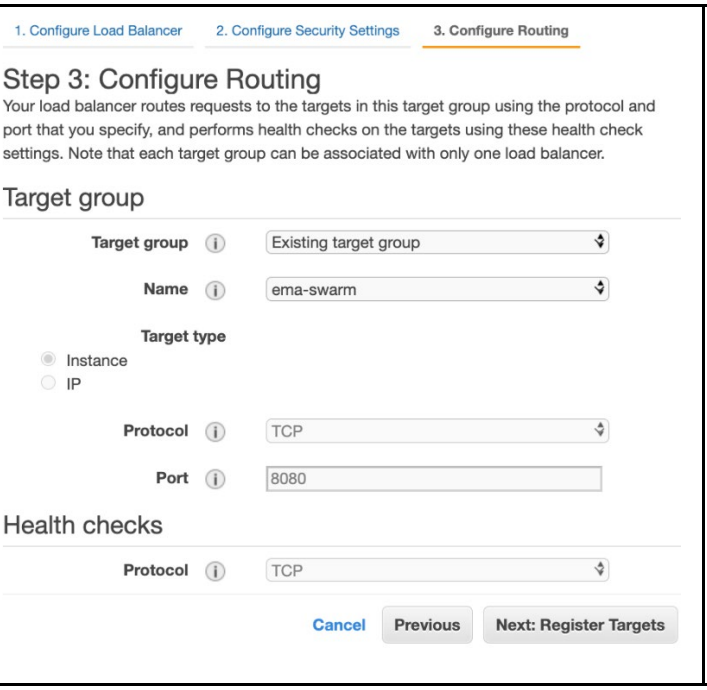
- **VPC**：选择您之前创建的 VPC。
- **Availability Zones**：启用两个可用区并选择两个公共子网。IPv4 address 应设置为 *Assigned by AWS*。

单击 **Next: Configure Security Settings** 按钮。

8.4.3.4 配置安全设置

在此步骤中，我们无需配置任何内容。单击 **Next: Configure Routing** 按钮。

8.4.3.5 配置路由



在 **Step 3: Configure Routing**，按如下所示配置 Target group。

- **Target group**: *Existing target group*
- **Name**: 选择您之前创建的 TCP/8080 目标组的名称。示例： *ema-swarm*

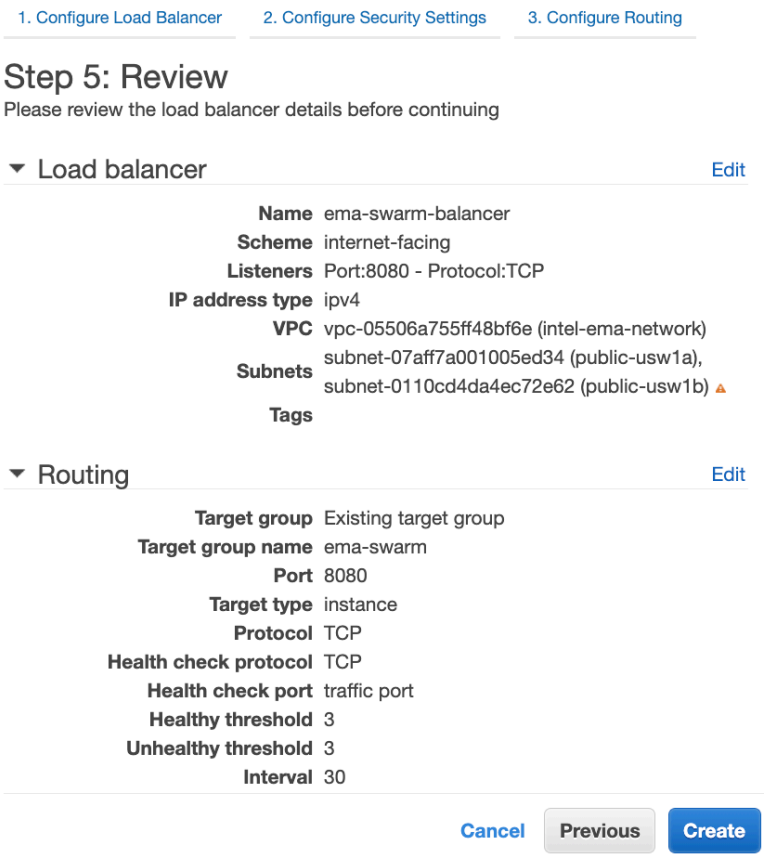
单击 **Next: Register Targets** 按钮。

8.4.3.6 注册目标

	确认您看到两个所列实例为注册目标。 单击 **Next: Review** 按钮。

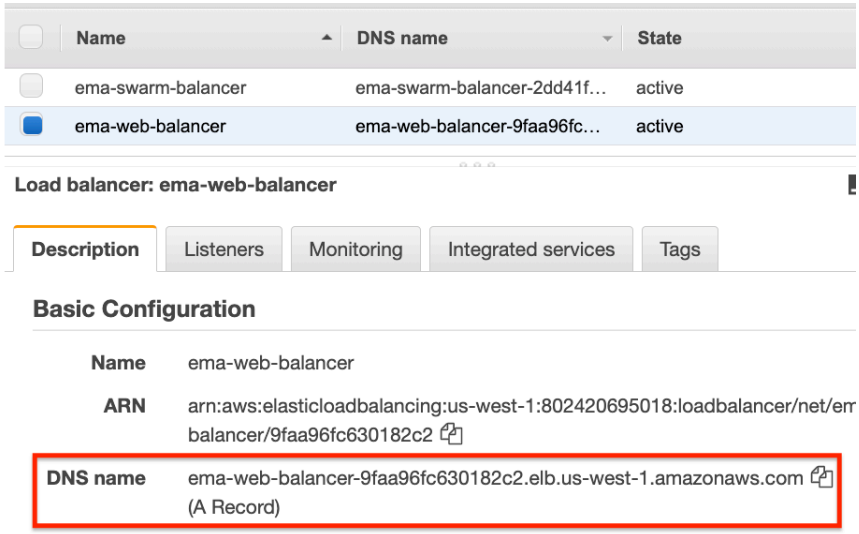
8.4.3.7 审阅

在 **Step 5: Review**，确认与此处提供的示例类似，然后单击 **Create** 按钮。



8.4.4 请注意负载均衡器 DNS 名称

返回到负载均衡器的 **Description** 选项卡，并记下 DNS 名称。您将要与 DNS 提供商一起为您的自定义域名创建 CNAME 记录，这样您就可以将您的 Intel EMA 集群流量引向负载均衡器。


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 附录 A – 有关 Active Directory* 集成的说明

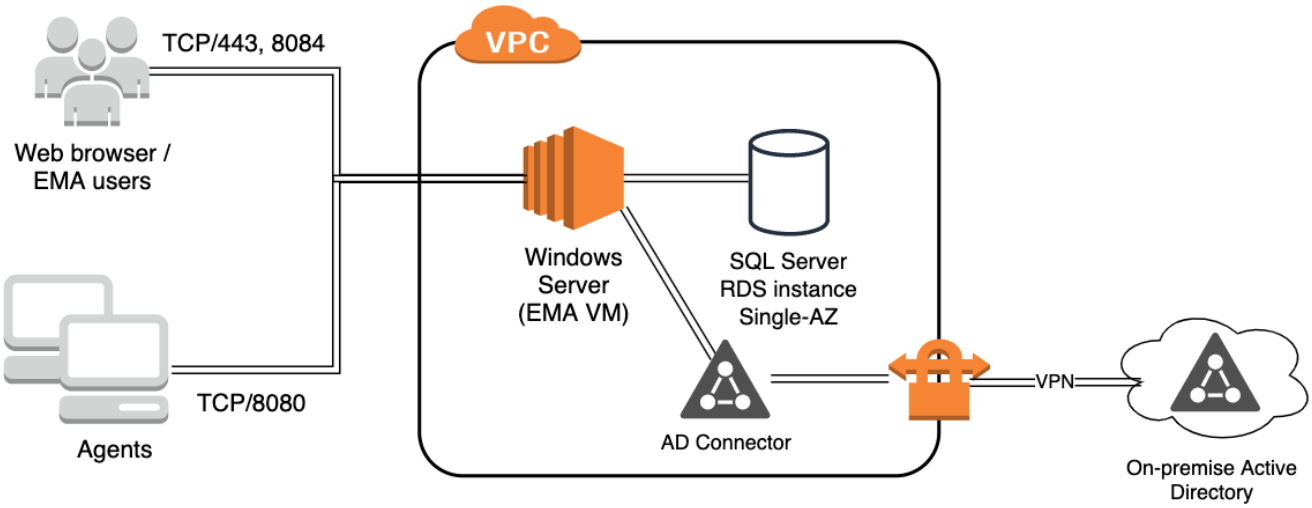
您可以通过多种方式将 Active Directory* 与 AWS 集成，以将您的虚拟机加入域并使用 AD 身份验证。由于组织的需求可能千差万别，因此本附录仅简要说明如何将现有的本地目录扩展到云以达成上述目的。云提供商会不定期修改和扩展他们的服务产品，因此在部署生产解决方案之前，您应该自行研究，了解哪些服务最适合您的业务。

有关 AWS 中 Active Directory 服务的更多信息，请访问以下链接：

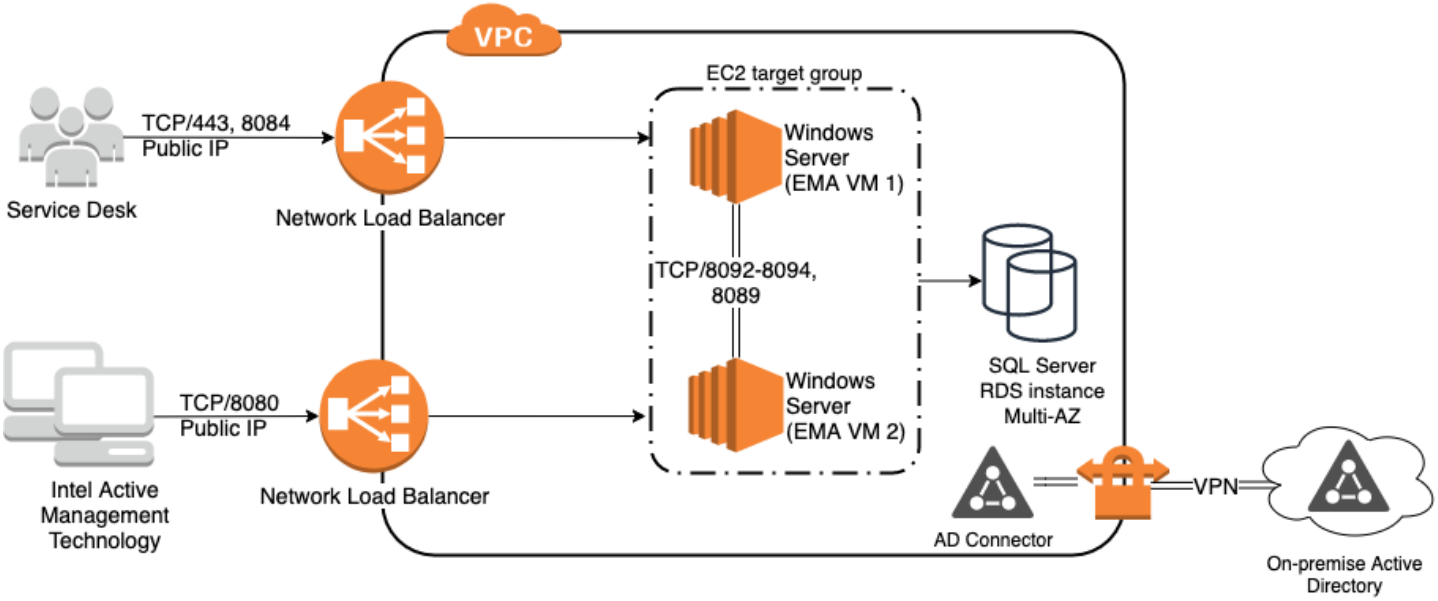
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.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

10 集成 Active Directory 的架构图

10.1 单服务器部署



10.2 分布式服务器部署



10.3 使用 AWS AD Connect 将 Active Directory 扩展到云

- ❏ 创建一个 VPN 以连接到您的本地网络，提供与域控制器的连接。
  - ❏ 创建一个客户网关来代表 VPN 的远程（本地）端。
  - ❏ 创建虚拟专用网关以在 VPN 和 VPC 之间提供路由。
  - ❏ 将虚拟专用网关连接至您的 VPC。
  - ❏ 创建一个 VPN 连接，选择新的客户网关和 VPG。

- ❏ 选择静态路由选项，然后输入可通过 VPN 连接使用的网络。这应该包括您的本地域控制器。
- ❏ 您可以让 Amazon 生成您的隧道地 止和密钥。

- ❏ 下载 VPN 连接配置以帮助配置另一端。
- ❏ 转到 VPC 路由表并启用路由传播，以便与 VPN 连接关联的路由可用于您的 VPC 网络。

- ❏ 创建一个 AD 连接器资源，作为本地 AD 的代理。
  - ❏ 选择 AD 连接器作为您的目录类型。
  - ❏ 选择适合您需要支持的对象数量的目录大小。
  - ❏ 选择您的 VPC 和两个不同的子网。
  - ❏ 输入您将连接到的本地目录的信息。
    - ❏ 请注意您需要一个服务帐户。下面的文档链接中对前提条件进行了充分说明。
- ❏ 创建一个 DHCP 选项集并将其与 VPC 关联，以便虚拟机将收到正确的 DNS 服务器和域名。
  - ❏ 提供 Active Directory 域名和 DNS 服务器。其他参数是可选的。
  - ❏ 前往您的 VPC 并将 DHCP 选项集与其关联。
- ❏ 在配置 EC2 虚拟机实例时，请使用“域加入”选项使虚拟机自动加入您的 AD 域。