Intel® Endpoint Management Assistant (Intel® EMA)

Guia de implantação para Amazon Web Services* (AWS)

Intel® Versão 1.3.3

Outubro de 2020

Isenção de responsabilidade legal

As tecnologias Intel podem exigir ativação de hardware, software específico ou de serviços.

Nenhum produto ou componente pode ser totalmente seguro.

Os custos e resultados podem variar.

Este documento não concede nenhuma licença (expressa ou implícita, por impedimento ou de outra forma) para quaisquer direitos de propriedade intelectual.

A Intel renuncia a todas as garantias expressas ou implícitas, incluindo, sem limitação, as garantias implícitas de comercialização, adequação a um fim específico e não violação, bem como as garantias decorrentes do curso de desempenho, curso de negociação ou do uso no comércio.

Os produtos e os serviços descritos podem conter incorreções ou erros conhecidos como errata, que podem ocasionar desvios das especificações publicadas. Erratas caracterizadas atualizadas estão disponíveis mediante solicitação.

Os recursos e benefícios das tecnologias Intel dependem da configuração do sistema e podem exigir hardware habilitado, software ou ativação de serviços. O desempenho varia de acordo com a configuração do sistema. Nenhum sistema de computador pode ser totalmente seguro. A Intel não assume responsabilidade por perda e roubo de dados ou sistemas ou qualquer outro dano resultante. Consulte o fabricante ou revendedor do seu sistema ou saiba mais em http://www.intel.com/technology/vpro.

Sumário

1 Introdução 1

1.1 Sobre a computação em nuvem 1
1.2 Navegação no console de gerenciamento da AWS 1
1.2.1 Serviços 1
1.2.2 Grupos de recursos 2
1.2.3 Regiões 2
1.3 Tags e Grupos de recursos 2
1.4 Antes de começar 2

2 Diagramas de arquitetura de alto nível 3

2.1 Implantação de servidor único 3
2.2 Implantação de servidor distribuído 3

3 Selecione a região de implantação 4

4 Implantação de rede 5

4.1 Visão geral 5
4.2 Crie uma VPC 5
4.2.1 Acesse o serviço da VPC 5
4.2.2 Crie uma VPC 6
4.2.3 Configure os detalhes da VPC 6
4.3 Criar sub-redes 7
4.3.1 Acesse a tela de sub-redes 7
4.3.2 Crie a primeira sub-rede privada 7
4.3.3 Crie a segunda sub-rede privada 7
4.3.4 Crie a primeira sub-rede pública 8
4.3.5 Crie a segunda sub-rede pública 8
4.3.6 Analise suas sub-redes 9
4.4 Criar um gateway de internet para as sub-redes públicas 9
4.4.1 Crie gateways de Internet 9
4.4.2 Anexe o gateway de Internet à VPC 9
4.4.3 Insira os detalhes de anexo 10
4.5 Criar gateways NAT para as sub-redes privadas 10
4.5.1 Acesse os gateways NAT 10
4.5.2 Crie o primeiro gateway NAT 11
4.5.3 Crie o segundo gateway NAT 12
4.6 Criar e configurar tabelas de roteamento 12
4.6.1 Acesse as tabelas de roteamento 12
4.6.2 Crie uma tabela de roteamento para sub-redes públicas 13
4.6.3 Crie uma tabela de roteamento para a primeira sub-rede privada 13
4.6.4 Crie uma tabela de roteamento para a segunda sub-rede privada 13
4.6.5 Analise a lista de tabelas de roteamento 14
4.6.6 Edite rotas para a primeira tabela de roteamento de sub-rede privada 14
4.6.7 Edite associações de sub-rede para a primeira tabela de roteamento de sub-rede privada 15
4.6.8 Edite rotas para a segunda tabela de roteamento de sub-rede privada 15
4.6.9 Edite associações de sub-rede para a segunda tabela de roteamento de sub-rede privada 16
4.6.10 Edite rotas para a tabela de roteamento de sub-rede pública 17
4.6.11 Edite associações de sub-rede para a tabela de roteamento de sub-rede pública 17
4.7 Grupos de segurança 18
4.7.1 Crie um grupo de segurança para a(s) VM(s) 18
4.7.2 Atualize o grupo de segurança para permitir tráfego entre VMs Intel EMA (apenas servidor distribuído) 20
4.7.3 Crie um grupo de segurança para banco de dados 21

5 Implantação da máquina virtual 23

5.1 Visão geral ... 23
5.2 Criar máquina(s) virtual(is) ... 23
5.2.1 Acesse o serviço da EC2 ... 23
5.2.2 Inicie uma instância EC2 ... 23
5.2.3 Selecione uma Imagem de máquina da Amazon ... 24
5.2.4 Selecione o tipo de máquina ... 24
5.2.5 Configure os detalhes de instância ... 25
5.2.6 Adicione armazenamento ... 25
5.2.7 Adicione tags ... 25
5.2.8 Configure o grupo de segurança ... 26
5.2.9 Analise o lançamento da instância ... 26
5.2.10 Selecione um par de chave da EC2 ... 26
5.3 Criar uma segunda instância da EC2 (apenas servidor distribuído) ... 26

6 Configure o AWS Systems Manager (apenas servidor distribuído) ... 27

6.1 Acesse o serviço do Systems Manager ... 27
6.2 Inicie a configuração rápida ... 27
6.3 Escolha as opções de permissões ... 28
6.4 Escolha as opções de configurações ... 28
6.5 Escolha os objetivos ... 29
6.6 Verifique a lista de instâncias gerenciadas ... 29
6.7 Registrar em suas máquinas virtuais através do Session Manager ... 29

7 Implantação do Relational Database Service (RDS) ... 30

7.1 Acesse o serviço de RDS ... 30
7.2 Criar grupo de sub-redes de banco de dados ... 30
7.2.1 Detalhes do grupo de sub-redes ... 31
7.3 Criar um banco de dados ... 31
7.3.1 Escolha um método de criação de banco de dados ... 32
7.3.2 Escolha o tipo de mecanismo e edição ... 32
7.3.3 Escolha o modelo de implantação ... 32
7.3.4 Configure o nome da instância e as credenciais do usuário mestre ... 33
7.3.5 Configure o tamanho da instância de banco de dados ... 33
7.3.6 Configure o armazenamento (opcional) ... 33
7.3.7 Configure a conectividade ... 34
7.3.8 Configure a conectividade — Configuração adicional da conectividade ... 34
7.3.9 Analise e crie ... 35
7.4 Obtenha o nome de host do banco de dados ... 35

8 Implantação do balanceador de carga (apenas servidor distribuído) ... 36

8.1 Visão geral ... 36
8.2 Crie grupos de destino ... 36
8.2.1 Crie grupos de destino ... 36
8.2.2 Configure um grupo de destino para TCP/443 ... 37
8.2.3 Crie/configure um destino para TCP/8084 ... 38
8.2.4 Configure um destino para TCP/8080 ... 38
8.2.5 Analise os grupos de destino ... 39
8.2.6 Habilite Stickiness para o grupo de destino TCP/443 ... 39
8.2.7 Habilite Stickiness para o grupo de destino TCP/8084 ... 40
8.2.8 Nota sobre o monitoramento da integridade do grupo de destino ... 40
8.3 Criar um balanceador de carga de rede para receber tráfego da Internet ... 40
8.3.1 Crie o balanceador de carga ... 40
8.3.2 Escolha o tipo de balanceador de carga ... 40
8.3.3 Configure o balanceador de carga ... 41
8.3.4 Configure as regras de encaminhamento do balanceador de carga ... 43
8.4 Criar um balanceador de carga de rede para tráfego swarm ... 45
8.4.1 Crie o balanceador de carga ... 45

8.4.2 Escolha o tipo de balanceador de carga 45
8.4.3 Configure o balanceador de carga 45
8.4.4 Anote o nome do DNS do balanceador de carga 47

9 Apêndice A — Notas sobre a integração do Active Directory* 49

10 Diagrama de arquitetura com a integração do Active Directory 50

10.1 Implantação de servidor único 50
10.2 Implantação de servidor distribuído 50
10.3 Usando o conector AWS AD para estender o Active Directory para a nuvem 50

1 Introdução

Este documento descreve o procedimento para implantar infraestrutura no Amazon Web Services*, uma plataforma de computação em nuvem, necessária para oferecer suporte a uma ou mais instâncias do servidor Intel® Endpoint Management Assistant (Intel® EMA). É destinado a administradores de TI com conhecimento intermediário e avançado da infraestrutura de TI que podem ter conhecimento limitado sobre computação em nuvem.

Há vários componentes necessários para um ambiente de infraestrutura de nuvem completo. Recomendamos que você leia este guia com atenção para entender como eles estão configurados para trabalhar juntos. Uma descrição de cada componente é fornecida antes do procedimento de implantação, com um link para a documentação oficial do provedor de nuvem para obter mais informações, se necessário.

1.1 Sobre a computação em nuvem

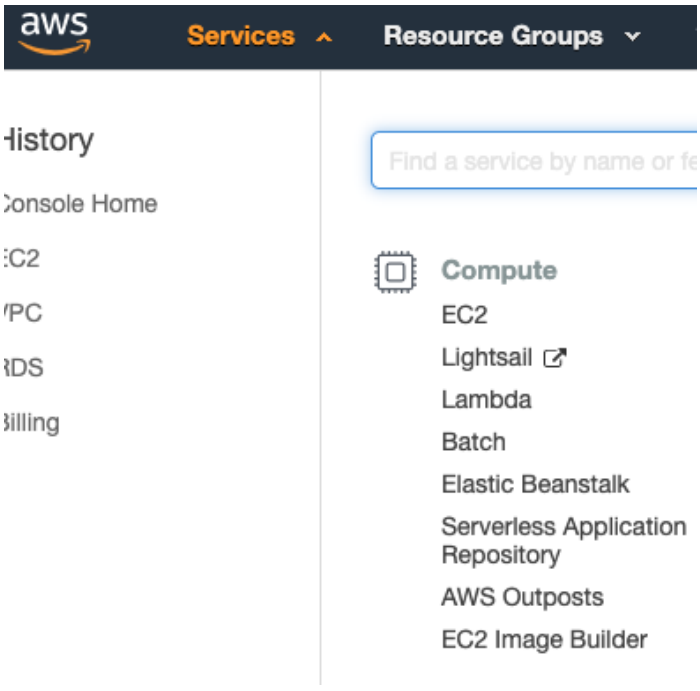
A computação em nuvem é o fornecimento sob demanda de recursos de TI na Internet com preços pré-pagos. Em vez de comprar e manter data centers e servidores físicos, você pode acessar serviços de tecnologia, como potência de computação, armazenamento e bancos de dados, de acordo com a necessidade a partir de um provedor na nuvem. Você pode provisionar apenas o que precisa no momento e dimensionar a capacidade para crescer e reduzir à medida que as necessidades dos negócios mudam.

Grandes provedores de nuvem têm data centers em todo o mundo, permitindo que você implante recursos geograficamente perto de onde seus clientes e usuários finais estão localizados.

Com serviços totalmente gerenciados como o Amazon Relational Database Service, você pode apenas manter o foco em seus dados enquanto o provedor de nuvem gerencia todos os hardware e software subjacentes que fornecem o serviço. Com máquinas virtuais em execução na nuvem, você gerencia apenas o sistema operacional convidado e o software instalado nele, enquanto o provedor de nuvem gerencia o hardware subjacente e se esforça para fornecer a melhor confiabilidade e disponibilidade.

1.2 Navegação no console de gerenciamento da AWS

1.2.1 Serviços

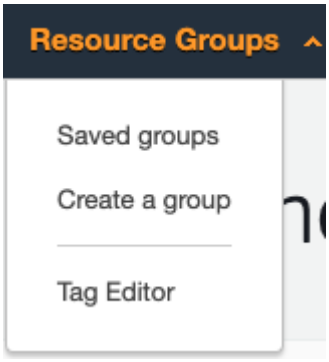


Depois de acessar o Console de Gerenciamento da AWS em https://aws.amazon.com/console/, você verá um menu Services no canto superior esquerdo da tela.

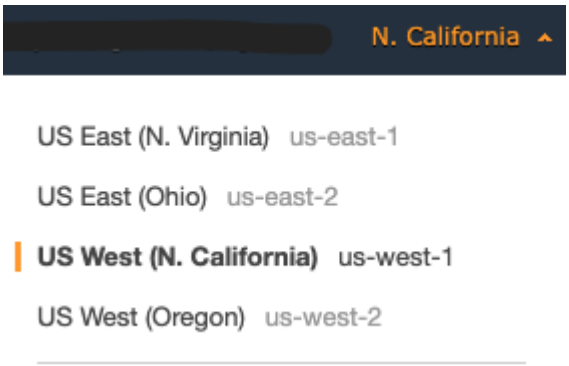
Se você clicar neste item, abrirá uma lista de todos os serviços que a AWS fornece, organizados por categoria como Computação, Armazenamento, Banco de Dados e outros.

Ao implantar serviços neste guia, forneceremos instruções que o direcionarão para esta tela para selecionar o serviço adequado.

1.2.2 Grupos de recursos

	Ao lado de Services está o menu Resource Groups, no qual é possível criar ou visualizar os grupos de recursos que você criou. Normalmente, você verá todos os recursos implantados na região atual, independentemente de quem implantou ou qual projeto ele pertence; portanto, ao usar grupos de recursos você pode obter uma lista filtrada de recursos com base em tags personalizadas que você atribuiu a cada recurso.

1.2.3 Regiões

	No canto superior direito do console de gerenciamento, você verá um menu no qual deve selecionar a região onde deseja implantar recursos. Você só poderá ver os recursos listados para a região selecionada.

Cada região da AWS contém vários locais distintos chamados Zonas de disponibilidade ou AZs. Cada Zona de disponibilidade é projetada para ser isolada de falhas em outras Zonas de disponibilidade.

1.3 Tags e Grupos de recursos

Tags são pares de chave-valor personalizados que podem ser atribuídos a vários tipos de recursos diferentes a serem implantados no AWS. Recomenda-se usar tags na medida em que os recursos são criados para que você possa monitorar mais facilmente o proprietário do recurso, a que projeto ele pertence, habilitar um grupo de recursos baseado em tag e habilitar relatórios de faturamento baseados em tag.

Não usaremos tagging nem criaremos um grupo de recursos neste guia, uma vez que existem muitas maneiras diferentes de fazer isso e acrescentariam uma série de etapas extras, mas você deve estar ciente de que eles existem no caso de querer implementar uma estratégia de agrupamento de recursos e tagging.

Para obter mais informações sobre o uso de tags, acesse o seguinte link:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

1.4 Antes de começar

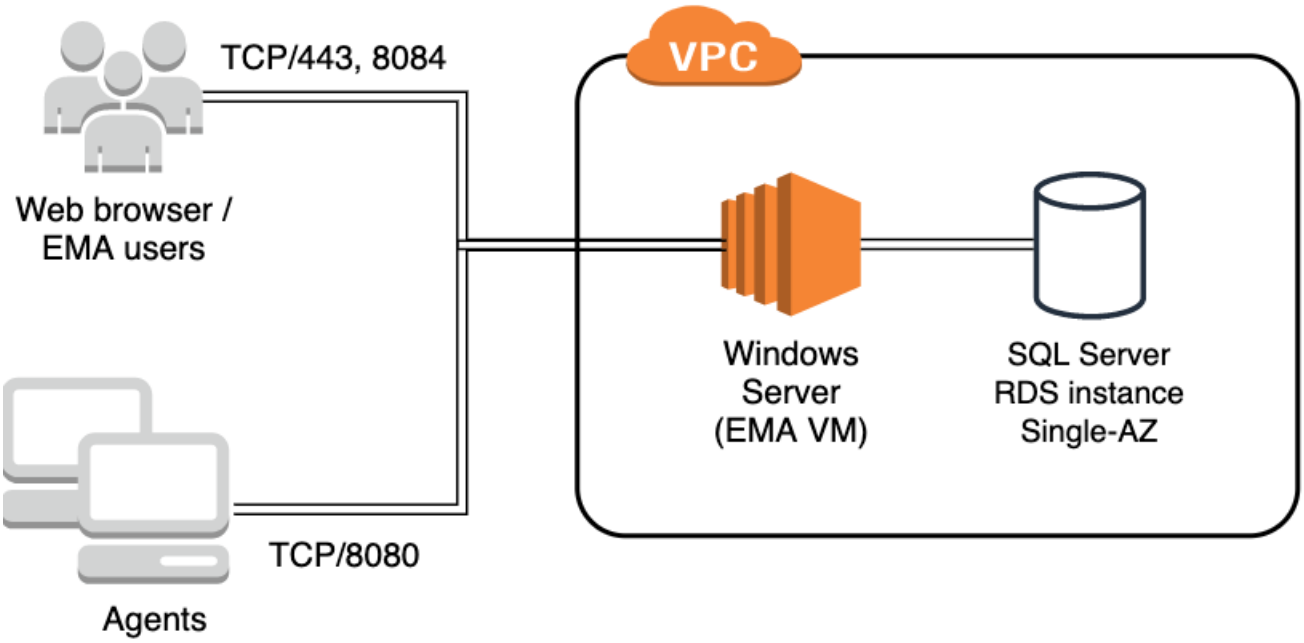
Se a sua organização já tem uma conta AWS, você deve pedir a um administrador de nuvem que lhe conceda acesso suficiente para poder criar todos os recursos listados neste guia.

Se a sua organização não tiver uma conta AWS, ou caso queira avaliar a plataforma como pessoa física, acesse https://aws.amazon.com/console/ e clique no botão **Create a Free Account**.

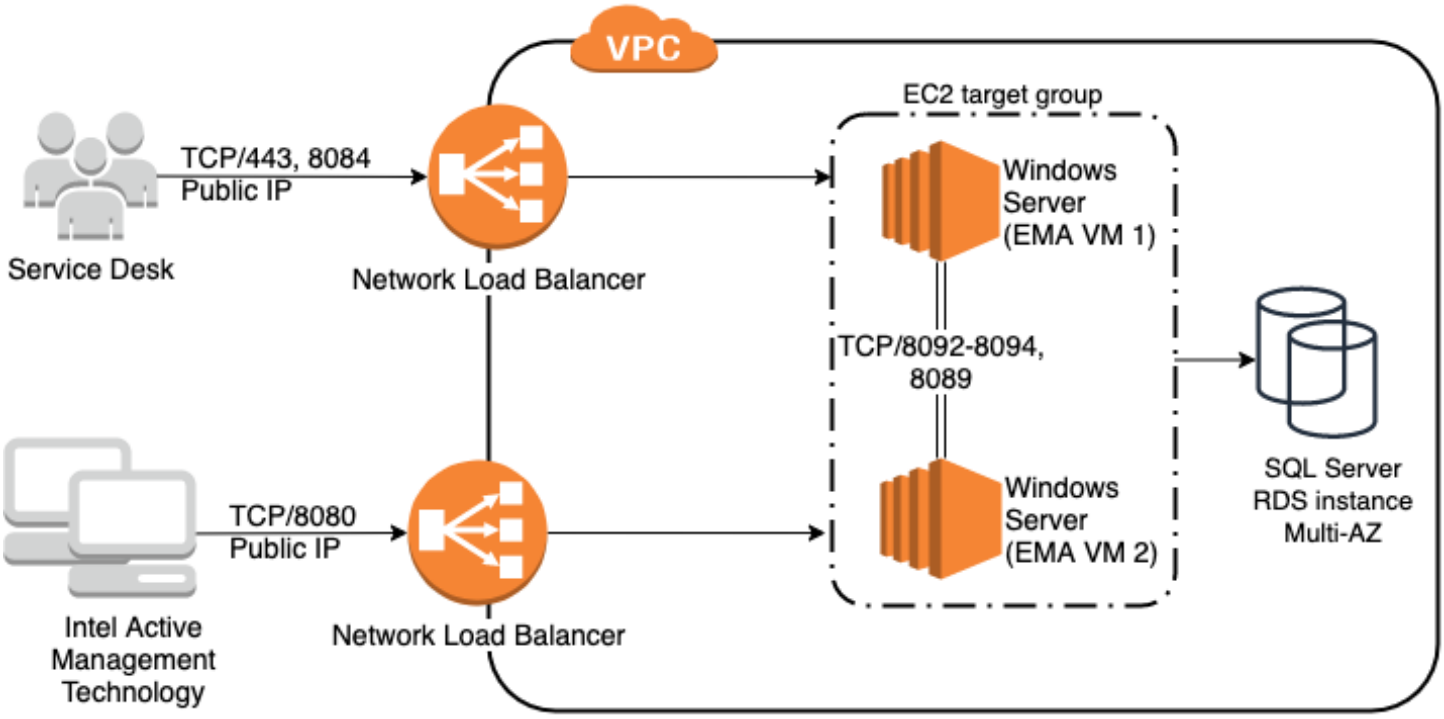
Consulte seu administrador de rede para saber se seria preferível usar um espaço de endereçamento específico. Se já tiver uma VPN estabelecida no provedor de nuvem, ou caso venha a ter futuramente, evite a sobreposição com sua rede corporativa para impedir problemas de roteamento. Você também precisa descobrir qual será o endereço IP fonte para o tráfego que sai da sua organização para chegar à nuvem, assim você permitirá que apenas as redes confiáveis atinjam a máquina virtual Intel EMA a partir da internet.

2 Diagramas de arquitetura de alto nível

2.1 Implantação de servidor único

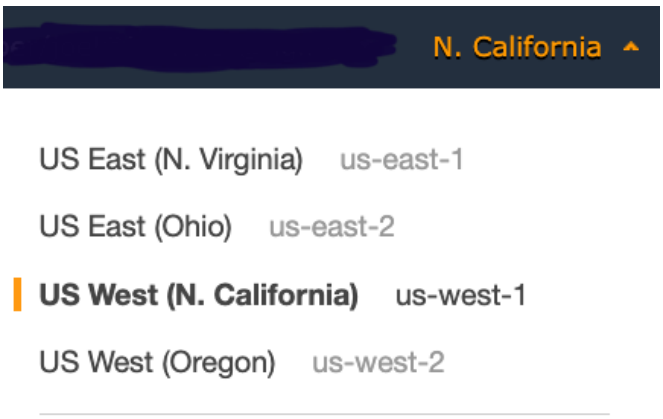


2.2 Implantação de servidor distribuído



3 Selecione a região de implantação

No menu da região no canto superior direito, escolha a região na qual deseja implantar recursos.



4 Implantação de rede

4.1 Visão geral

Para que máquinas virtuais se comuniquem umas com as outras, com o provedor de nuvem ou com a internet, precisamos primeiramente configurar um ambiente de rede. A Nuvem Privada Virtual (VPC) é o componente fundamental para sua rede privada na AWS e se assemelha a uma rede tradicional, exceto pelo fato de ser virtualizada na AWS. As VPCs são logicamente isoladas umas das outras.

Ao criar uma VPC, você precisará fornecer um espaço de endereço IP privado personalizado. A AWS atribuirá recursos a um endereço IP privado neste espaço de endereço quando necessário. Se as redes se conectarem por meio de uma VPN, recomenda-se evitar o uso de um espaço de endereço que se sobreponha às outras faixas de rede da sua organização para que não haja conflitos de roteamento. Consulte sua equipe de engenharia de rede para identificar um bloco de endereço IP disponível para evitar conflitos de roteamento caso sua empresa já tenha, ou venha a ter, conectividade de IP privada com a nuvem.

Depois de criar a VPC, também criaremos nossas sub-redes. As sub-redes permitem segmentar a rede VPC alocando uma parte do espaço de endereço da rede a cada sub-rede. Nossas sub-redes ficarão em duas Zonas de disponibilidade individuais (AZ) na Região escolhida para que possamos fornecer maior disponibilidade para nosso banco de dados e aplicação Intel EMA. Criaremos sub-redes públicas e privadas, dependendo se o recurso precisa de acesso direto à Internet com um endereço IP público.

Por padrão, o firewall da AWS não permite acesso de entrada a nossos recursos; portanto, parte da implantação da rede incluirá a criação de grupos de segurança para habilitar a comunicação de rede a esses recursos.

Para reduzir a superfície de ataque das nossas máquinas virtuais, o RDP não será permitido por meio do firewall da VPC. Em vez disso, usaremos o Sesssion Manager da AWS para habilitar o gerenciamento remoto das VMs. Além disso, nenhuma máquina virtual terá um endereço IP público para implementações de servidor distribuído.

Para obter mais informações sobre VPCs, acesse os seguintes links:
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html

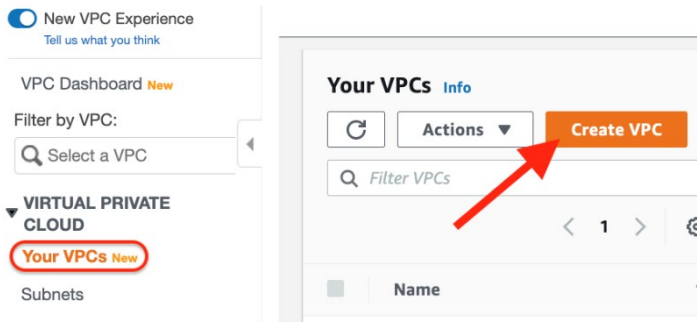
4.2 Crie uma VPC

O Assistente de VPC pode ser usado se você estiver implementando um servidor único com uma sub-rede pública, mas aqui criaremos todos os componentes de rede manualmente para dar melhor visibilidade ao que precisamos e porque o assistente em si não bastaria para uma implantação de servidor distribuído.

4.2.1 Acesse o serviço da VPC

	No menu **Services,** em **Network & Content Delivery**, selecione **VPC**.

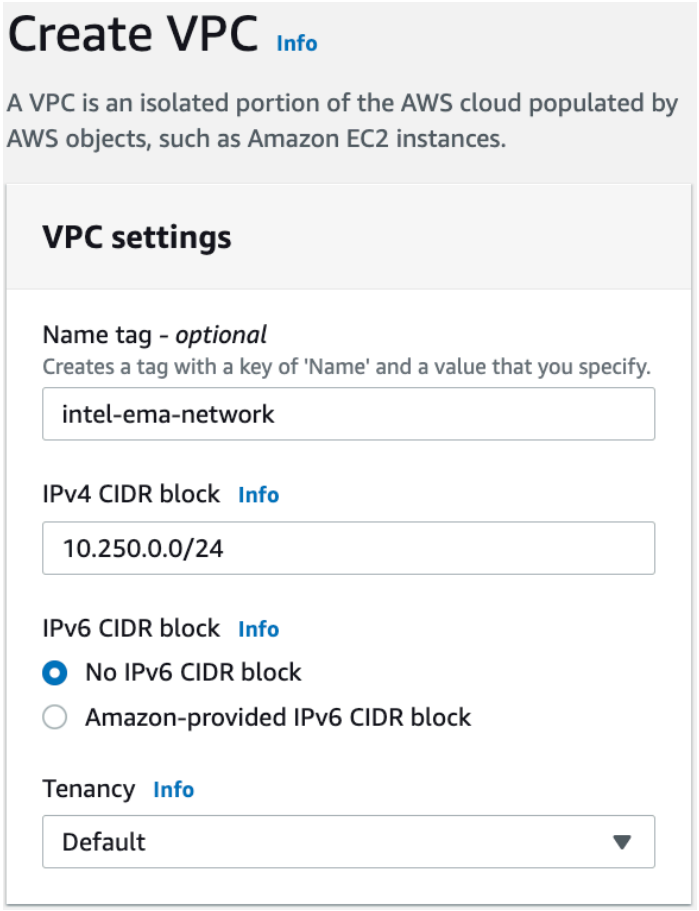
4.2.2 Crie uma VPC



Na barra lateral de VPC, selecione **Your VPCs**.

Clique no botão **Create VPC**.

4.2.3 Configure os detalhes da VPC



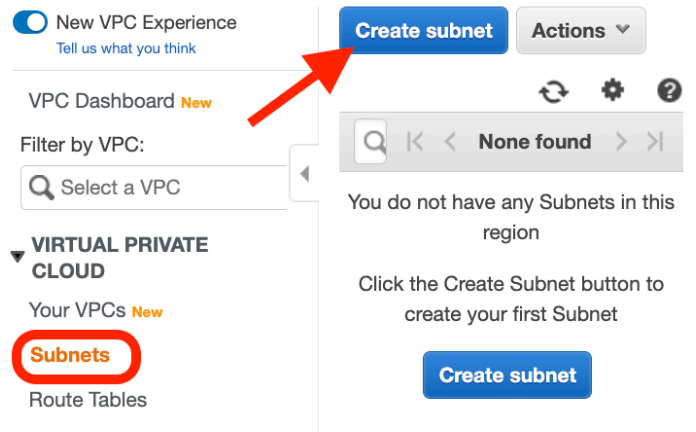
Insira os detalhes de rede conforme o seguinte

- **Name Tag**: Insira um nome exclusivo para a VPC. Exemplo: *intel-ema-network*
- **IPv4 CIDR block**: escolha uma rede não usada e grande o suficiente para conter suas sub-redes. Exemplo: *10.250.0.0/24*

Clique no botão **Create VPC**

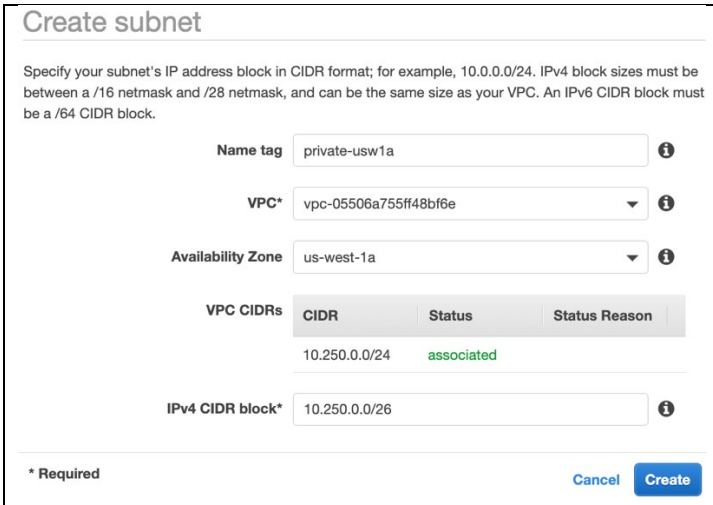
4.3 Criar sub-redes

4.3.1 Acesse a tela de sub-redes



Na barra lateral da VPC, selecione **Subnets**.

4.3.2 Crie a primeira sub-rede privada



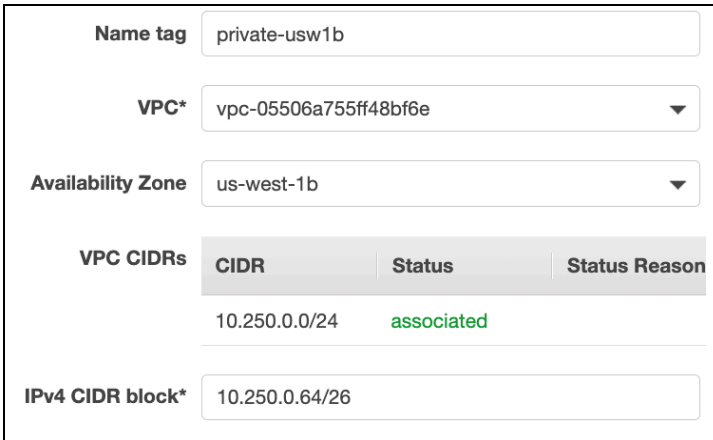
Clique no botão **Create subnet**.

Configure a sub-rede como a seguir:

- **Name tag**: forneça um nome de sub-rede exclusivo.
  Exemplo: *private-usw1a*
- **VPC**: selecione a rede virtual que você criou anteriormente.
- **Availability Zone**: usaremos duas zonas distintas em nosso projeto; portanto, use a primeira zona escolhida aqui.
  Exemplo: *us-west-1a*
- **IPv4 CIDR block**: escolha um bloco IP não usado no espaço de endereço da sua VPC.
  Exemplo: *10.250.0.0/26*

Clique no botão **Create**.

4.3.3 Crie a segunda sub-rede privada



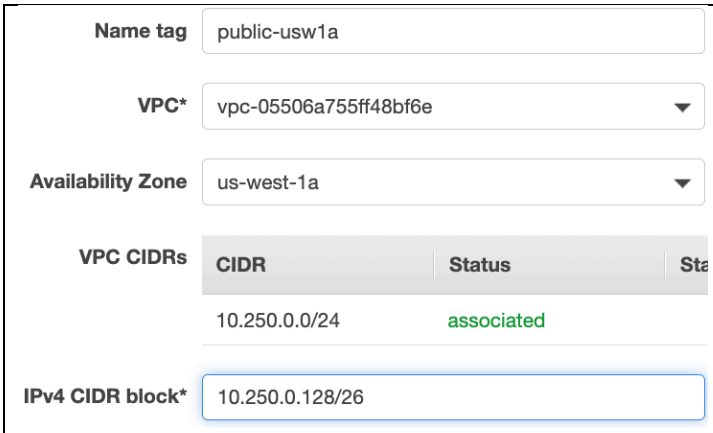
Clique no botão **Create subnet**.

Configure a sub-rede como a seguir:

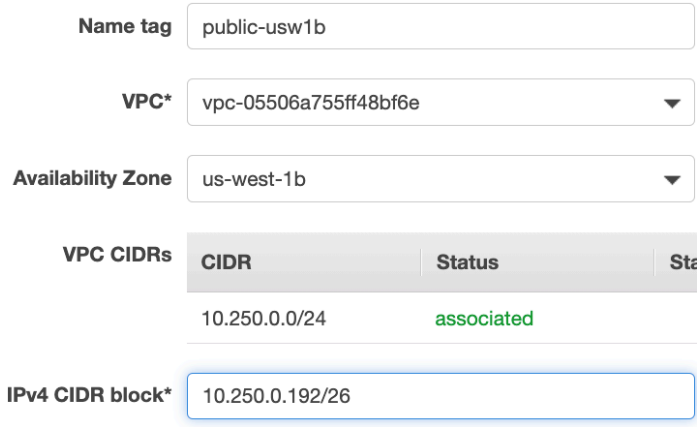
- **Name tag**: forneça um nome de sub-rede exclusivo.
  Exemplo: *private-usw1b*
- **VPC**: selecione a rede virtual que você criou anteriormente.
- **Availability Zone**: usaremos duas zonas distintas em nosso projeto; portanto, use a segunda zona escolhida aqui.
  Exemplo: *us-west-1b*

	• **IPv4 CIDR block**: escolha um bloco IP não usado no espaço de endereço da sua VPC. Exemplo: *10.250.0.64/26* Clique no botão **Create**.

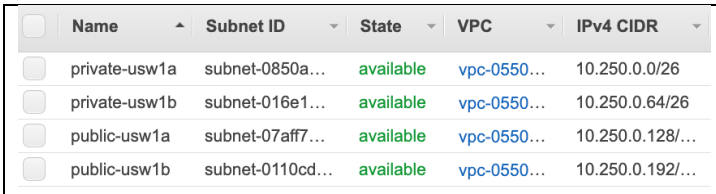
4.3.4 Crie a primeira sub-rede pública

	Clique no botão **Create subnet**. Configure a sub-rede como a seguir: • **Name tag**: forneça um nome de sub-rede exclusivo. Exemplo: *public-usw1a* • **VPC**: selecione a rede virtual que você criou anteriormente. • **Availability Zone**: usaremos duas zonas distintas em nosso projeto; portanto, use a primeira zona escolhida aqui. Exemplo: *us-west-1a* • **IPv4 CIDR block**: escolha um bloco IP não usado no espaço de endereço da sua VPC. Exemplo: *10.250.0.128/26* Clique no botão **Create**.

4.3.5 Crie a segunda sub-rede pública

	Clique no botão **Create subnet**. Configure a sub-rede como a seguir: • **Name tag**: forneça um nome de sub-rede exclusivo. Exemplo: *public-usw1b* • **VPC**: selecione a rede virtual que você criou anteriormente. • **Availability Zone**: usaremos duas zonas distintas em nosso projeto; portanto, use a segunda zona escolhida aqui. Exemplo: *us-west-1b* • **IPv4 CIDR block**: escolha um bloco IP não usado no espaço de endereço da sua VPC. Exemplo: *10.250.0.196/26* Clique no botão **Create**.

4.3.6 Analise suas sub-redes



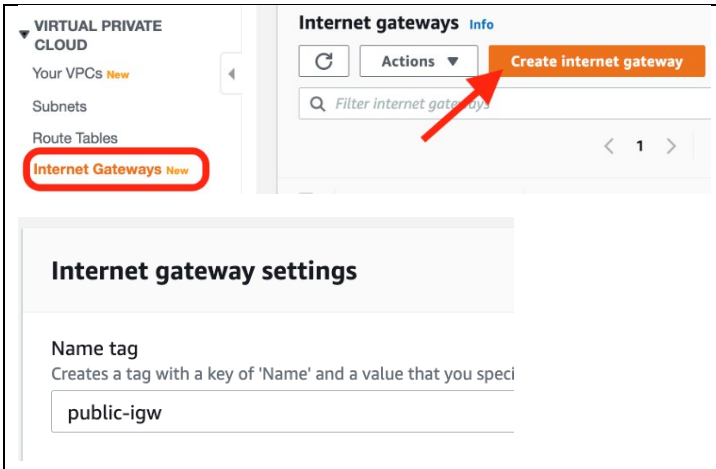
Name	Subnet ID	State	VPC	IPv4 CIDR
private-usw1a	subnet-0850a…	available	vpc-0550…	10.250.0.0/26
private-usw1b	subnet-016e1…	available	vpc-0550…	10.250.0.64/26
public-usw1a	subnet-07aff7…	available	vpc-0550…	10.250.0.128/…
public-usw1b	subnet-0110cd…	available	vpc-0550…	10.250.0.192/…

Analise sua lista de sub-redes. Você deve agora ter quatro sub-redes criadas.

4.4 Criar um gateway de internet para as sub-redes públicas

Para encaminhar o tráfego das sub-redes públicas para a Internet, precisamos implantar um gateway de internet e anexá-lo à VPC. Nós iremos configurar o encaminhamento em uma seção posterior.

4.4.1 Crie gateways de Internet



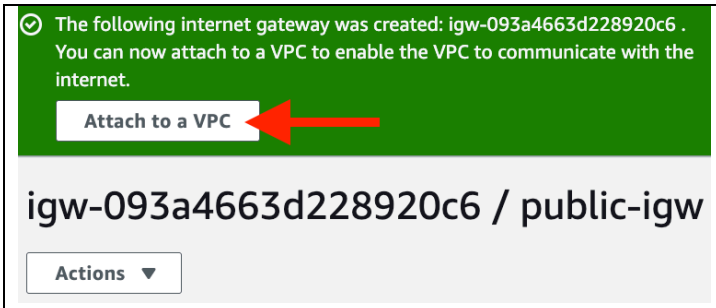
Na barra lateral da VPC, selecione Internet Gateways.

Clique em **Create Internet gateway**.

Insira uma tag de nome. Exemplo: *public-igw*

Clique no botão **Create Internet gateway** na parte inferior da tela para terminar.

4.4.2 Anexe o gateway de Internet à VPC



Quando o gateway de internet for criado, você terá que anexá-lo a uma VPC. Clique no botão conforme indicado. Você também pode fazer isso no menu Actions.

4.4.3 Insira os detalhes de anexo

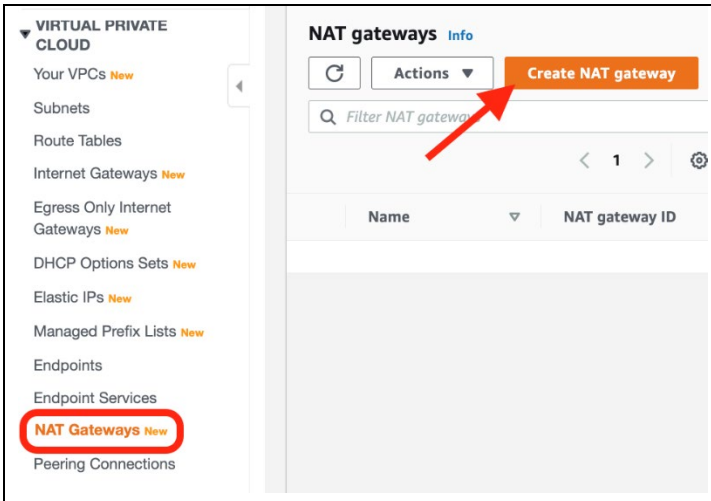
Selecione a VPC que você criou anteriormente.

Clique no botão **Attach internet gateway**.

4.5 Criar gateways NAT para as sub-redes privadas

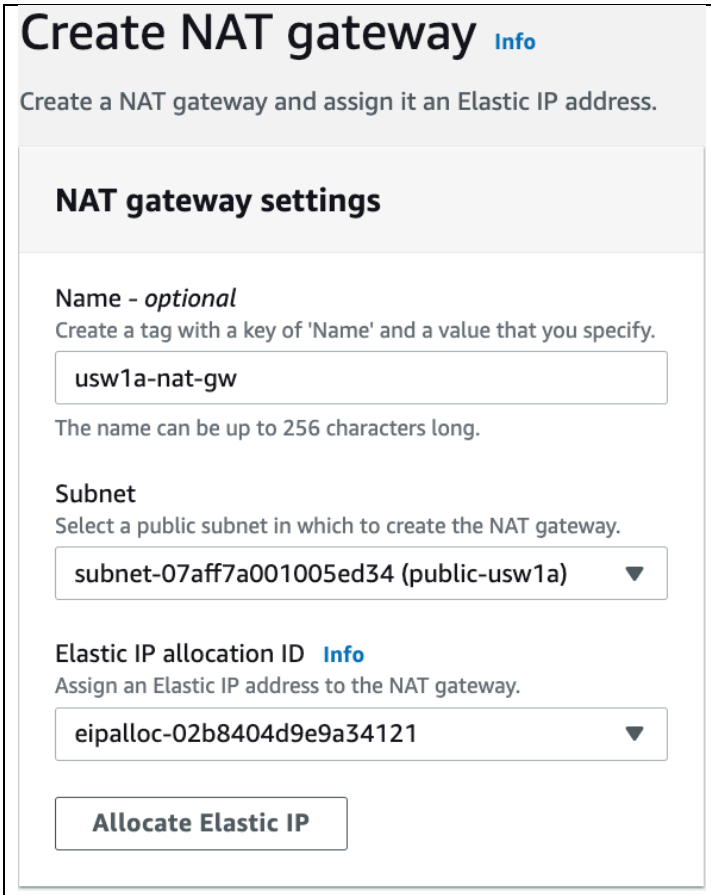
Um gateway NAT é um recurso zonal que pode ser usado por recursos nessa zona como um ponto de saída para tráfego de saída da internet. O gateway NAT executará a tradução de endereço e encaminhará o tráfego para o Gateway de Internet no sua VPC. Criaremos um para cada uma de nossas duas zonas de disponibilidade, assim não perdemos conectividade se uma das zonas cair.

4.5.1 Acesse os gateways NAT



Na barra lateral da VPC, selecione **NAT Gateways**.

4.5.2 Crie o primeiro gateway NAT



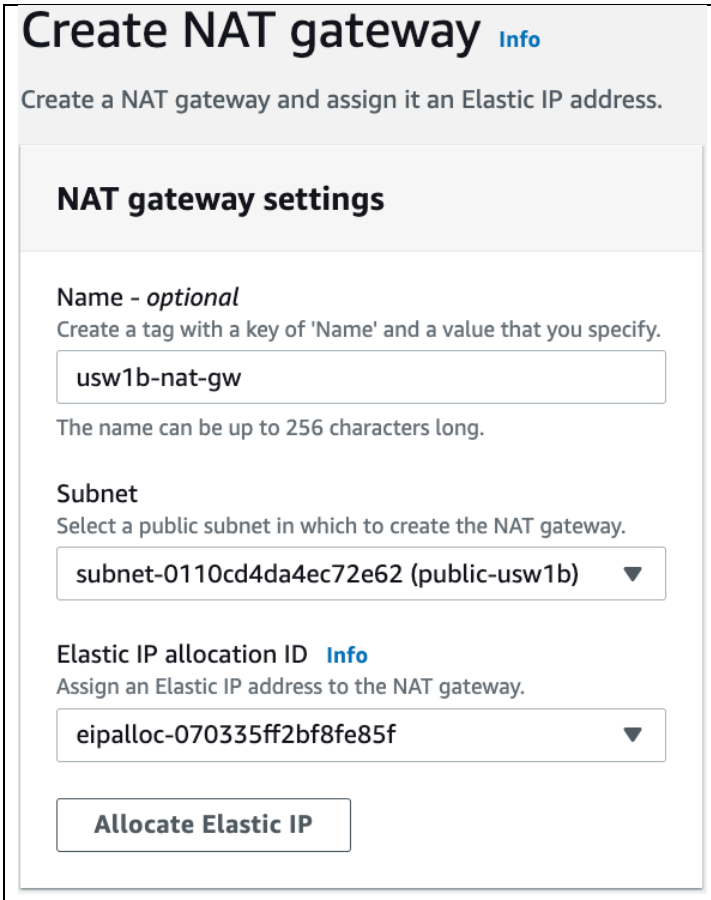
Clique no botão **Create NAT gateway**.

Defina as configurações do gateway NAT como a seguir:

- **Name** (opcional): insira um nome exclusivo para o gateway.
  Exemplo: *usw1a-nat-gw*
- **Subnet**: escolha a primeira sub-rede pública.
  Exemplo: *public-usw1a*
- **Elastic IP allocation ID**: clique no botão Allocate Elastic IP para preencher automaticamente este campo.

Clique no botão **Create NAT gateway** para terminar.

4.5.3 Crie o segundo gateway NAT



Clique no botão **Create NAT gateway**.

Defina as configurações do gateway NAT como a seguir:

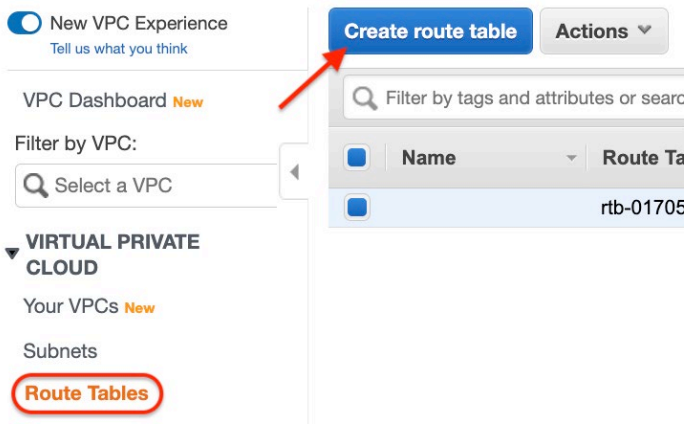
- **Name** (opcional): insira um nome exclusivo para o gateway.
  Exemplo: *usw1b-nat-gw*
- **Subnet**: escolha a segunda sub-rede pública.
  Exemplo: *public-usw1b*
- **Elastic IP allocation ID**: clique no botão Allocate Elastic IP para preencher automaticamente este campo.

Clique no botão **Create NAT gateway** para terminar.

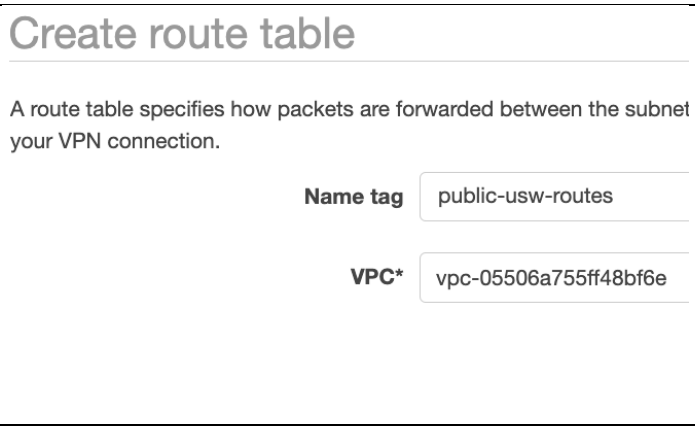
4.6 Criar e configurar tabelas de roteamento

Uma tabela de roteamento é um conjunto de regras, chamadas rotas, usado para determinar onde o tráfego de rede é direcionado. A VPC já inclui uma tabela de roteamento padrão que é usada para quaisquer sub-redes que não estão explicitamente associadas a uma tabela de roteamento. Nós vamos ignorar isso e criar três novas tabelas de roteamento, uma delas associada às nossas sub-redes públicas e duas delas para nossas sub-redes privadas. Nós adicionaremos rotas padrão aos Gateways NAT e ao Gateway de Internet.

4.6.1 Acesse as tabelas de roteamento



4.6.2 Crie uma tabela de roteamento para sub-redes públicas



Clique no botão **Create route table**.

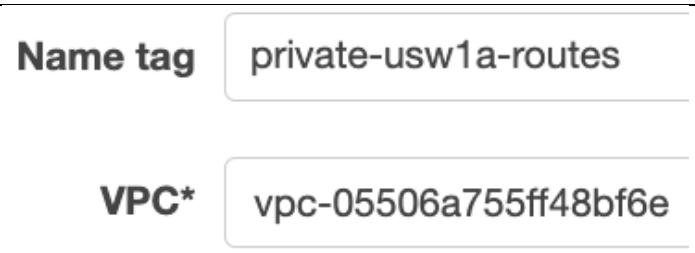
Configure a tabela de roteamento como a seguir:

- **Name tag**: insira um nome exclusivo para a tabela de roteamento.
  Exemplo: *public-usw-routes*
- **VPC**: selecione a rede virtual que você criou anteriormente.

Clique no botão **Create**.

Clique no botão **Close**.

4.6.3 Crie uma tabela de roteamento para a primeira sub-rede privada



Clique no botão **Create route table**.

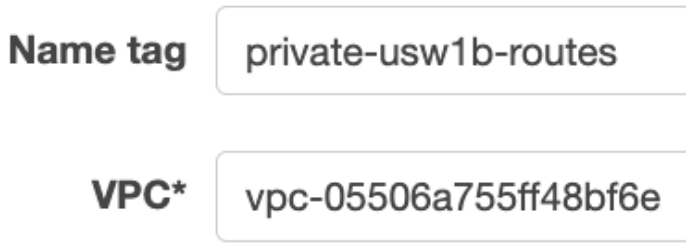
Configure a tabela de roteamento como a seguir:

- **Name tag**: insira um nome exclusivo para a tabela de roteamento.
  Exemplo: *private-usw1a-routes*
- **VPC**: selecione a rede virtual que você criou anteriormente.

Clique no botão **Create**.

Clique no botão **Close**.

4.6.4 Crie uma tabela de roteamento para a segunda sub-rede privada



Clique no botão **Create route table**.

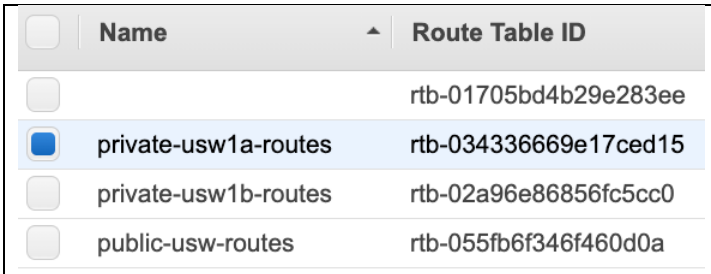
Configure a tabela de roteamento como a seguir:

- **Name tag**: insira um nome exclusivo para a tabela de roteamento.
  Exemplo: *private-usw1b-routes*
- **VPC**: selecione a rede virtual que você criou anteriormente.

Clique no botão **Create**.

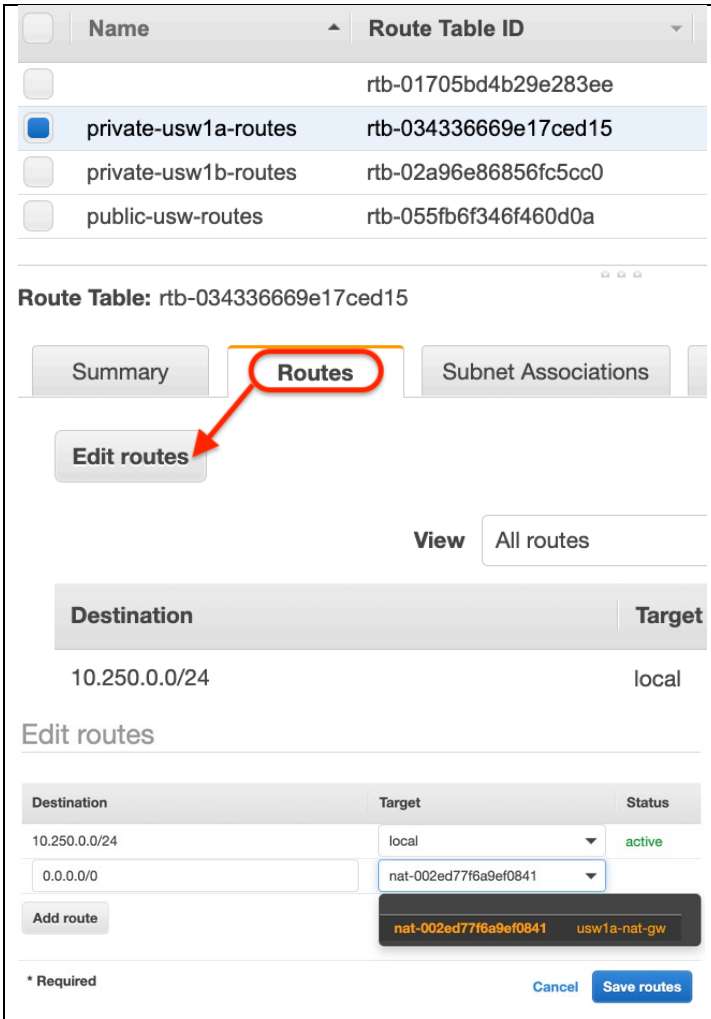
Clique no botão **Close**.

4.6.5 Analise a lista de tabelas de roteamento



Verifique se sua lista de tabelas de roteamento possui três novas entradas com as tags de nome que você escolheu.

4.6.6 Edite rotas para a primeira tabela de roteamento de sub-rede privada



Selecione a tabela de roteamento para a primeira sub-rede privada.
Exemplo: *private-usw1a-routes*

Selecione a guia **Routes** sob a lista.

Clique no botão **Edit routes**.

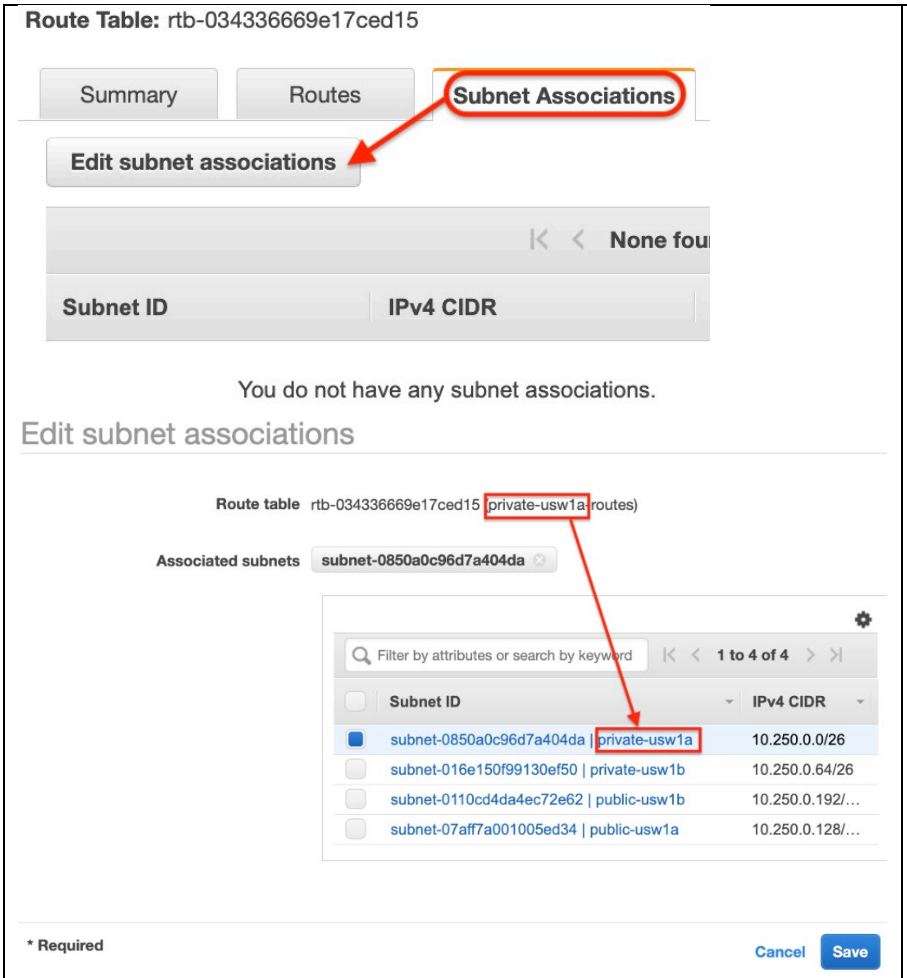
Clique no botão **Add route** e defina esses valores:

- **Destination**: *0.0.0.0/0*
- **Target**: selecione o Gateway NAT que você implantou na primeira zona de disponibilidade.
  Exemplo: *usw1a-nat-gw*

Clique no botão **Save routes**.

Clique no botão **Close**.

4.6.7 Edite associações de sub-rede para a primeira tabela de roteamento de sub-rede privada



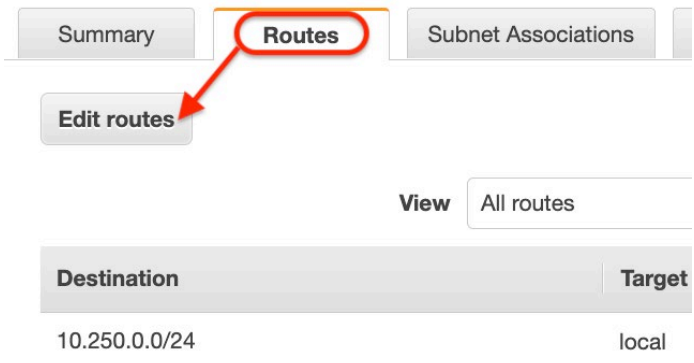
Selecione a guia **Subnet Associations**.

Clique no botão **Edit subnet associations**.

Selecione a primeira sub-rede privada para associar a esta tabela de roteamento. Se você seguiu os nomes de exemplo neste guia, será fácil combinar o nome da tabela de roteamento com a sub-rede.

Clique no botão **Save**.

4.6.8 Edite rotas para a segunda tabela de roteamento de sub-rede privada



Selecione a tabela de roteamento para a segunda sub-rede privada.
Exemplo: *private-usw1b-routes*

Selecione a guia **Routes** sob a lista.

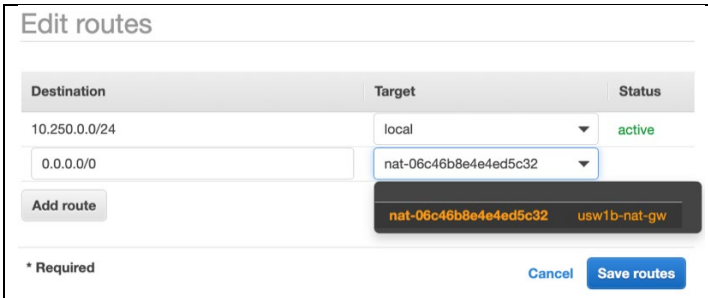
Clique no botão **Edit routes**.

Clique no botão **Add route** e defina esses valores:

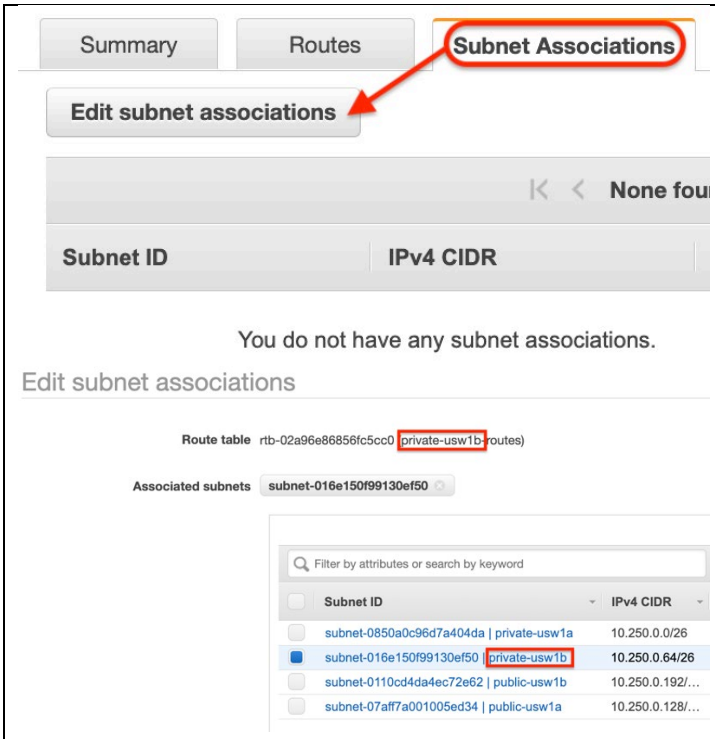
- **Destination**: *0.0.0.0/0*
- **Target**: selecione o Gateway NAT que você implantou na segunda zona de disponibilidade.
  Exemplo: *usw1b-nat-gw*

Clique no botão **Save routes**.

Clique no botão **Close**.



4.6.9 Edite associações de sub-rede para a segunda tabela de roteamento de sub-rede privada



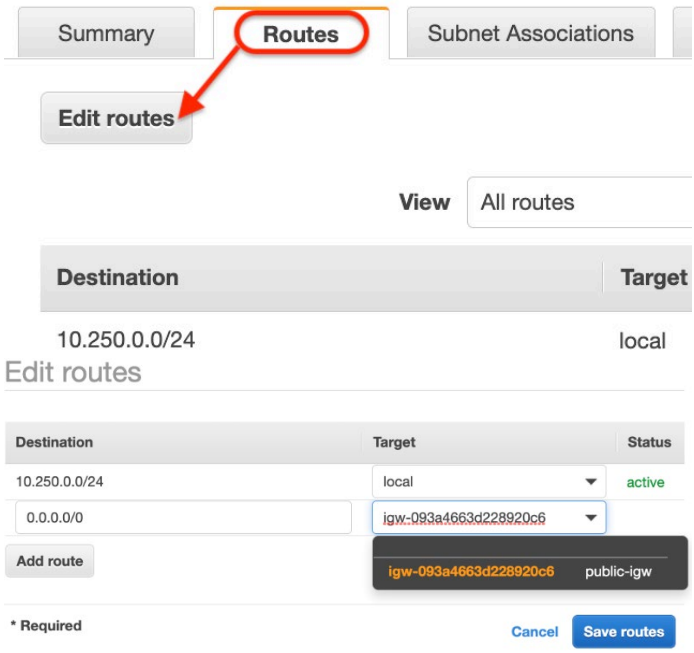
Selecione a guia **Subnet Associations**.

Clique no botão **Edit subnet associations**.

Selecione a primeira segunda sub-rede para associar a esta tabela de roteamento. Se você seguiu os nomes de exemplo neste guia, será fácil combinar o nome da tabela de roteamento com a sub-rede.

Clique no botão **Save**.

4.6.10 Edite rotas para a tabela de roteamento de sub-rede pública



Selecione a tabela de roteamento para as sub-redes públicas.
Exemplo: *public-usw-routes*

Selecione a guia **Routes** sob a lista.

Clique no botão **Edit routes**.

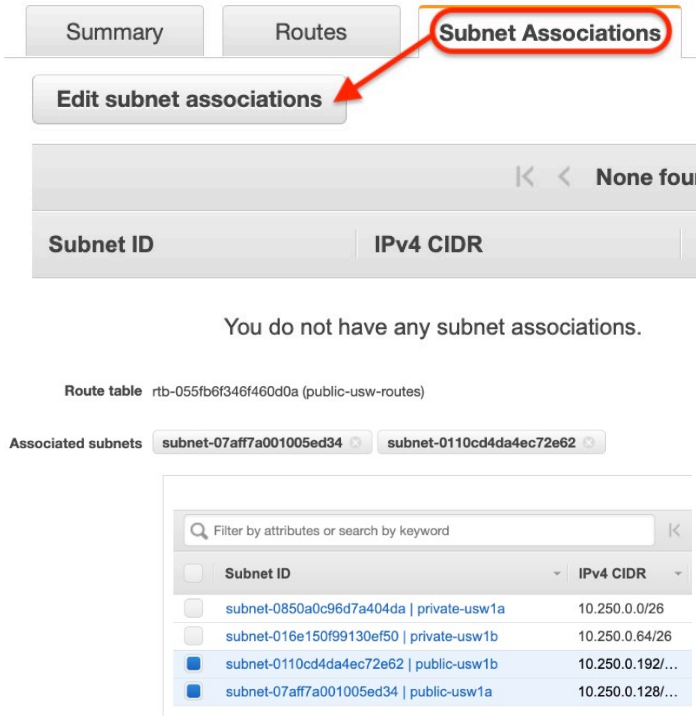
Clique no botão **Add route** e defina esses valores:

- **Destination**: *0.0.0.0/0*
- **Target**: selecione o Gateway de Internet que você implantou.
  Exemplo: *public-igw*

Clique no botão **Save routes**.

Clique no botão **Close**.

4.6.11 Edite associações de sub-rede para a tabela de roteamento de sub-rede pública



Selecione a guia **Subnet Associations**.

Clique no botão **Edit subnet associations**.

Selecione as duas sub-redes públicas para associar a esta tabela de roteamento.

Clique no botão **Save**.

4.7 Grupos de segurança

Um grupo de segurança atua como um firewall virtual para instâncias de máquina virtual para controlar o tráfego de entrada e saída. Quando criarmos uma VM mais tarde, poderemos anexar um ou mais grupos de segurança naquele momento. Você pode modificar as regras para um grupo de segurança a qualquer momento. Regras novas e modificadas são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

Ao criar as regras de grupo de segurança, você especificará a fonte e o destino. Essas podem ser expressadas como uma lista de redes IP ou como uma ID de grupo de segurança. Ao especificar um grupo de segurança como a fonte ou o destino para uma regra, a regra afetará todas as instâncias associadas ao grupo de segurança. Usaremos esse recurso para implantações de servidor distribuído para permitir o tráfego entre as VMs Intel EMA sem precisar ser excessivamente amplo e permitir todo o tráfego dentro da rede privada, que segue as melhores práticas de segurança de privilégios mínimos.

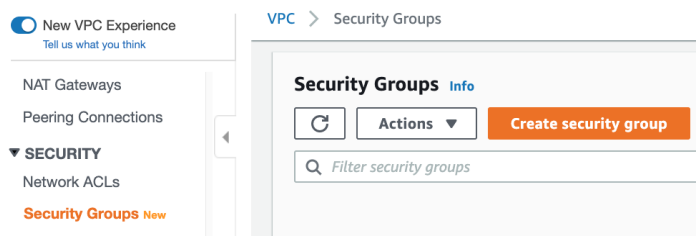
Nos procedimentos abaixo, criaremos um grupo de segurança para controlar o acesso às VMs Intel EMA e um grupo separado para controlar o acesso ao banco de dados.

Para obter mais informações sobre grupos de segurança da VPC, acesse link a seguir:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

4.7.1 Crie um grupo de segurança para a(s) VM(s)

Nota: alguns endereços de fonte no exemplo de imagens abaixo são editados porque seriam específicos para seu próprio ambiente de rede e não devem ser copiados literalmente. Em vez disso, use sua(s) própria(s) rede(s) de confiança.

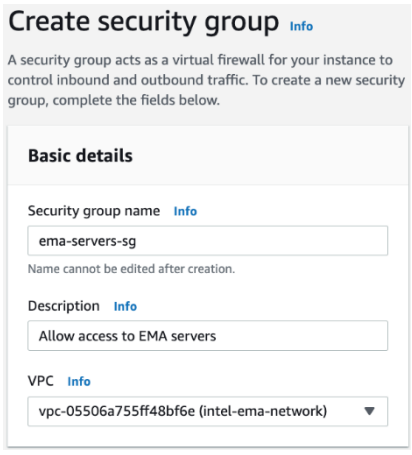
4.7.1.1 Crie um grupo de segurança



Na barra lateral de seção **VPC**, selecione **Security Groups.**

Clique no botão **Create security group**.

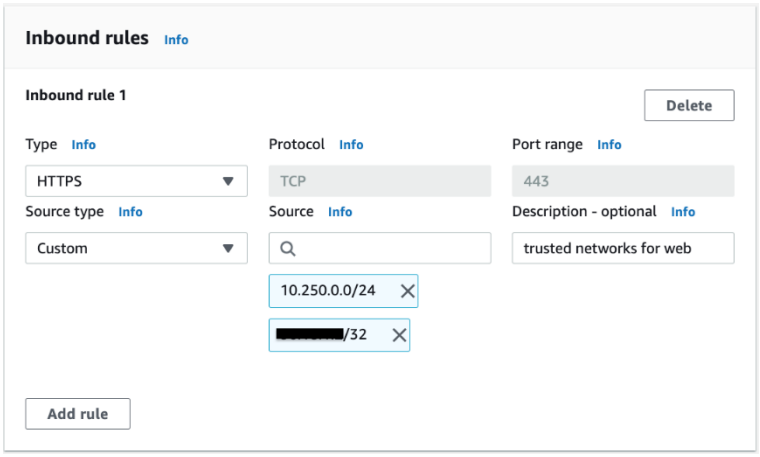
4.7.1.2 Configurar informações básicas do grupo de segurança



Insira as informações básicas para o grupo de segurança que permitirá acesso ao servidor EMA.

- **Security group name**: insira um nome exclusivo.
  Exemplo: *ema-server-sg*
- **Description** (opcional): insira uma descrição para o grupo de segurança.
  Exemplo: *Allow access to EMA servers*
- **VPC**: selecione a VPC que você criou anteriormente.

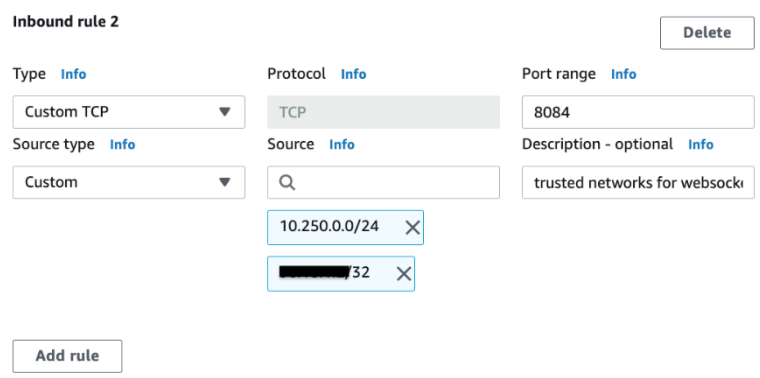
4.7.1.3 Adicione uma regra de entrada para tráfego da Web



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *HTTPS*
- **Description**: *Rede(s) confiável(is) para Web*
- **Source**: insira o bloco VPC CIDR para permitir verificações de integridade.
  Exemplo: *10.250.0.0/24*
  Você também pode inserir redes adicionais que devem ter permissão para acessar a interface de usuário Web do EMA, como a rede pública da qual o tráfego de sua central de serviço se originaria.

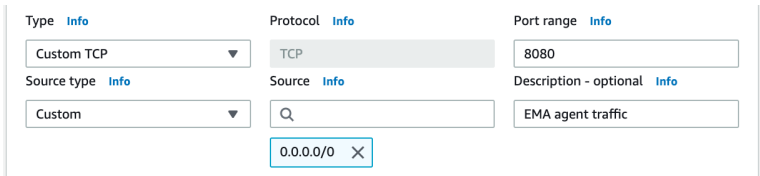
4.7.1.4 Adicione uma regra de entrada para tráfego WebSocket



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *Custom TCP*
- **Port range**: *8084*
- **Description**: *Rede(s) confiável(is) para WebSocket*
- **Source**: insira o bloco VPC CIDR para permitir verificações de integridade.
  Exemplo: *10.250.0.0/24*
  Você também pode inserir redes adicionais que devem ter permissão para acessar a interface de usuário Web do EMA, como a rede pública da qual o tráfego de sua central de serviço se originaria.

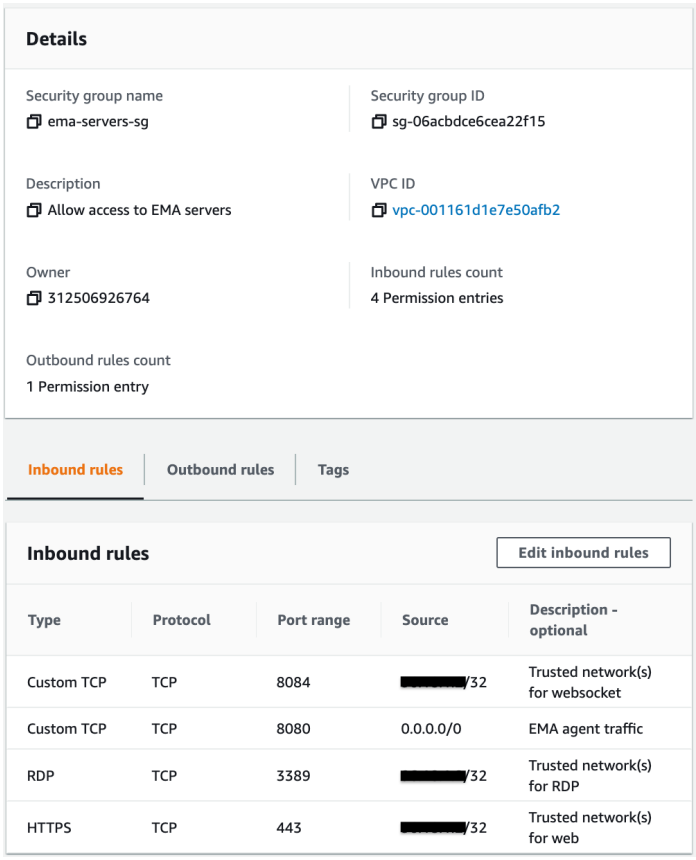
4.7.1.5 Adicione uma regra de entrada para tráfego Swarm



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *Custom TCP*
- **Port range**: *8080*
- **Description**: *Tráfego do EMA Agent*
- **Source**: *0.0.0.0/0*

4.7.1.6 Crie e analise



Clique no botão **Create security group** para salvar as regras.

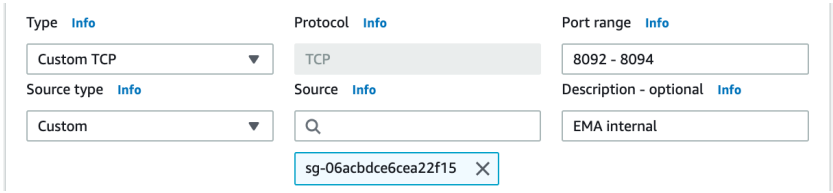
Analise a lista de regras para correção.

Nota: nós deixamos regras de saída com a regra padrão que permite todo o tráfego de saída.

4.7.2 Atualize o grupo de segurança para permitir tráfego entre VMs Intel EMA (apenas servidor distribuído)

Agora que criamos o grupo de segurança ema-server-sg, clique no botão **Edit inbound rules** e faça as alterações que se seguem abaixo.

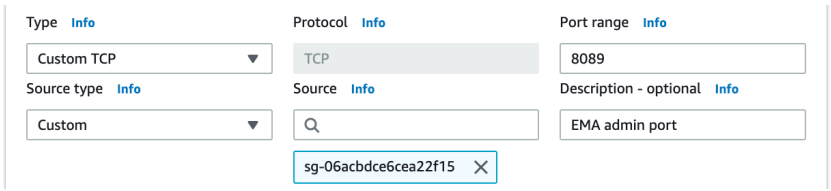
4.7.2.1 Adicione uma regra de entrada para tráfego interno para as portas 8092-8094



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *Custom TCP*
- **Port range**: *8092-8094*
- **Description**: *Interno EMA*
- **Source**: clique na caixa de texto vazia e selecione o nome do grupo de segurança que você criou na etapa anterior.

4.7.2.2 Adicione uma regra de entrada para tráfego interno para a porta 8089



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *Custom TCP*
- **Port range**: *8089*
- **Description**: *Porta de Admin do EMA*
- **Source**: clique na caixa de texto vazia e selecione o nome do grupo de segurança que você criou na etapa anterior.

4.7.2.3 Salve e analise a lista final para correção

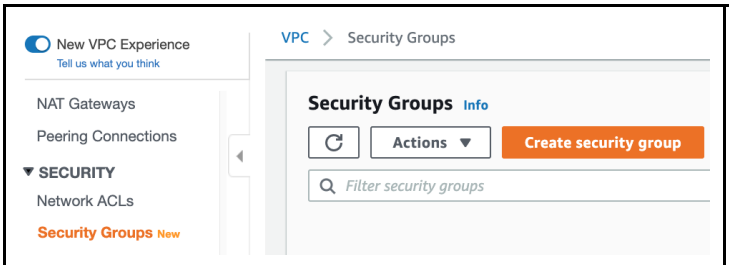
Clique no botão **Save rules**. Analise as regras para correção.

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 Crie um grupo de segurança para banco de dados

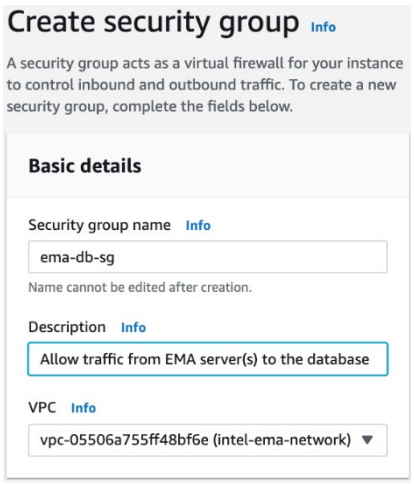
4.7.3.1 Crie um grupo de segurança



Na barra lateral da seção **VPC**, selecione **Security Groups.**

Clique no botão **Create security group**.

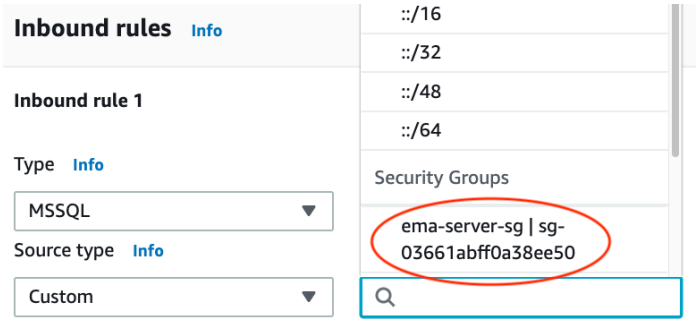
4.7.3.2 Configurar informações básicas do grupo de segurança



Insira as informações básicas para o grupo de segurança que permitirá acesso ao servidor EMA.

- **Security group name**: insira um nome exclusivo.
  Exemplo: *ema-db-sg*
- **Description** (opcional): insira uma descrição para o grupo de segurança.
  Exemplo: *Allow traffic from EMA server(s) to the database*
- **VPC**: selecione a VPC que você criou anteriormente.

4.7.3.3 Adicione regra de entrada para o MSSQL



Adicione uma regra de entrada com as seguintes configurações.

- **Type**: *MSSQL*
- **Source**: clique na caixa de texto vazia e selecione o grupo de segurança para os servidores EMA que você criou anteriormente.

4.7.3.4 Crie e analise

Clique no botão **Create security group**. Analise a lista de regras para correção.

5 Implantação da máquina virtual

5.1 Visão geral

A Amazon Elastic Compute Cloud* (Amazon EC2) oferece a flexibilidade da virtualização de computação sem precisar comprar e manter o hardware físico que a executa. No entanto, você ainda é responsável por manter o sistema operacional convidado e o software executado nele.

Você decidirá a quantidade de CPU, memória e armazenamento a ser alocada à instância EC2 no momento da criação, mas você pode aumentar todas as opções posteriormente ou reduzir a quantidade de CPU e memória para otimizar a VM para a carga de trabalho a fim de reduzir os custos.

A EC2 protege os logins para suas instâncias usando pares de chaves EC2 (AWS armazena a chave pública e você armazena a chave privada em um local seguro). Isso pode ser criado antecipadamente ou quando a instância EC2 for criada. Você precisará da chave privada para recuperar as credenciais de administrador geradas automaticamente para uma instância baseada em Windows. É possível ter vários pares de chave na EC2, mas você só pode associar uma instância a um par e isso não pode ser mudado após a instância ter sido criada.

O acesso da rede a suas instâncias EC2 pode ser protegido ao anexar um ou mais Grupos de segurança quando a instância for criada ou a qualquer momento posterior. Os Grupos de segurança de que precisamos já foram configurados na seção anterior.

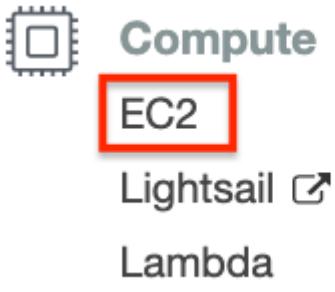
Para implantações de servidor distribuído, você pode pular algumas etapas adicionais incluídas no procedimento abaixo e em outras seções para implantações de servidor único. Essas etapas incluem a criação de uma segunda VM, a associação das VMs a um grupo de destino, anexar o grupo de destino ao balanceador de carga e configurar as regras de encaminhamento do balanceador de carga.

Para obter mais informações sobre instâncias EC2 ou pares de chaves, acesse os seguintes links:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-key-pairs.html

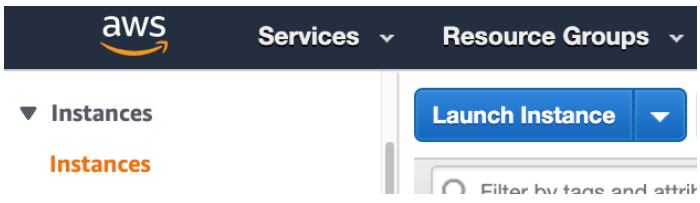
5.2 Criar máquina(s) virtual(is)

Siga o procedimento abaixo para criar uma instância EC2 para o servidor Intel EMA usando a imagem do Windows Server mais recente e anexar o grupo de segurança que nós criamos anteriormente.

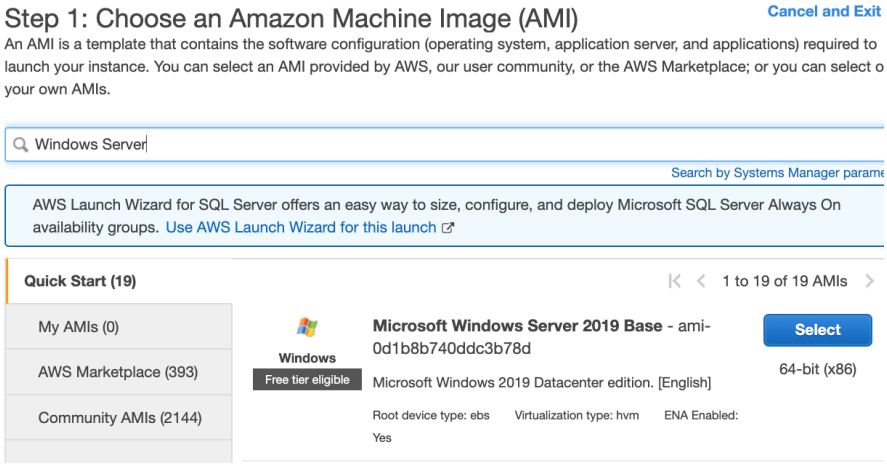
5.2.1 Acesse o serviço da EC2

	No menu **Services**, na seção **Compute**, selecione **EC2**.

5.2.2 Inicie uma instância EC2

	Selecione **Instances** na barra lateral e clique no botão **Launch Instance**.

5.2.3 Selecione uma Imagem de máquina da Amazon

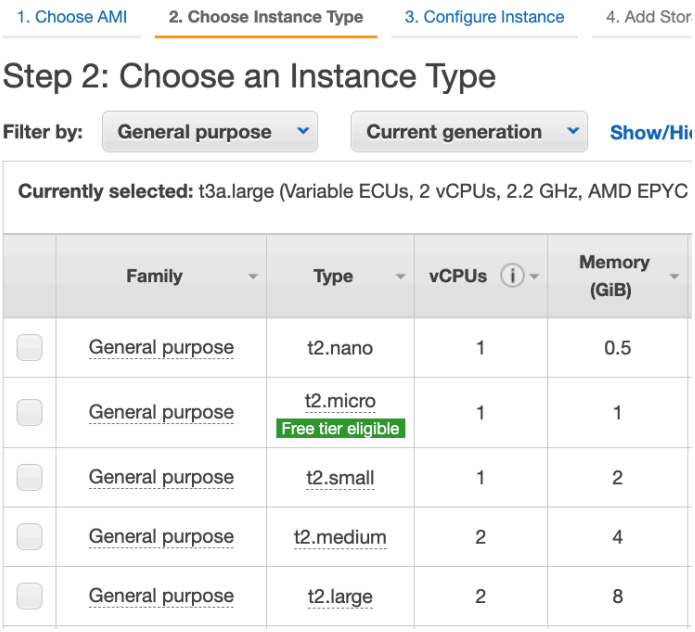


Procure a imagem da base de servidor Microsoft Windows* mais recente suportada pelo Intel EMA.

Consulte o Guia de instalação do servidor Intel® Endpoint Management Assistant para obter uma lista dos sistemas operacionais suportados.

Clique no botão **Select**.

5.2.4 Selecione o tipo de máquina

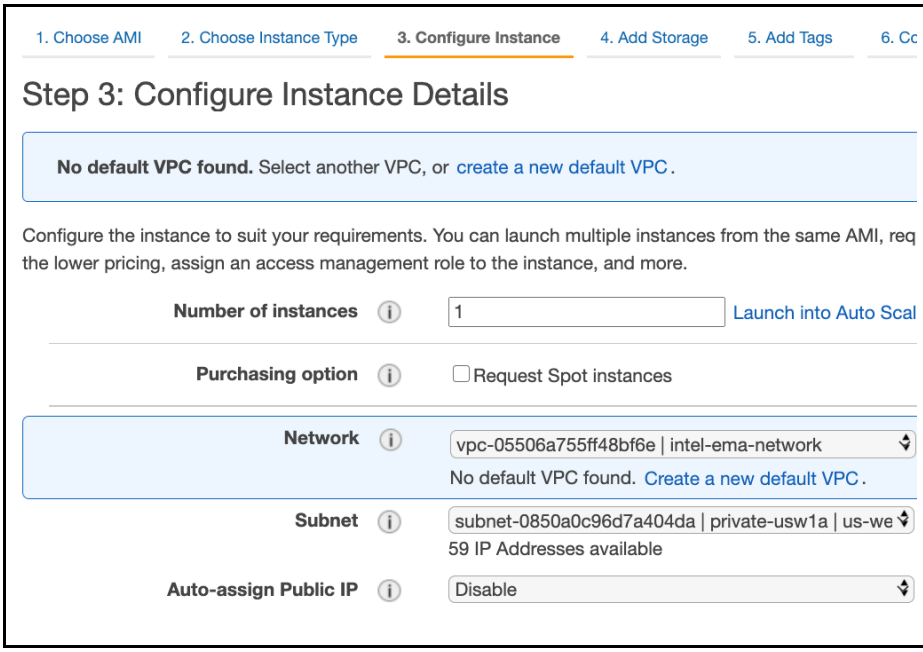


Escolha o tipo de máquina com a quantidade de recursos de CPU e memória de que você precisa. Você pode mudar isso mais tarde quando a instância estiver desligada, se necessário.

Consulte o Guia de instalação do servidor Intel® Endpoint Management Assistant para obter os requisitos do sistema.

Clique no botão **Next: Configure Instance Details**.

5.2.5 Configure os detalhes de instância



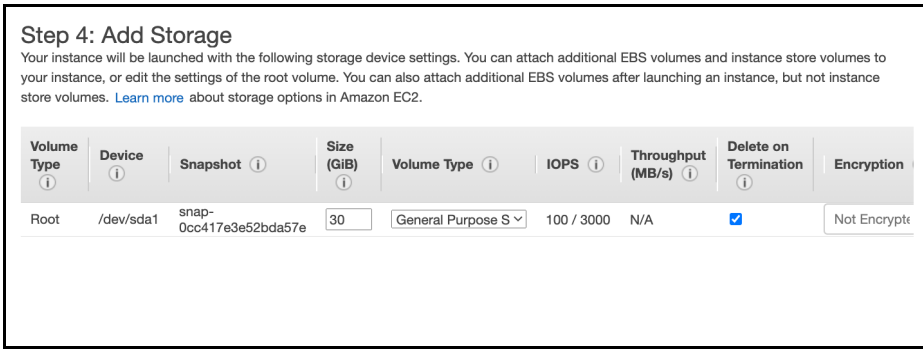
Configure os detalhes de instância como a seguir:

- **Network: configure** para a VPC que você criou anteriormente.
  Exemplo: *intel-ema-network*
- **Subnet**: escolha uma das sub-redes privadas.
  Exemplo: *private-usw1a*
- **Auto-assign Public IP**: *Disable*

As demais informações de instância nesta tela podem ser definidas como padrão.

Clique no botão **Next: Add Storage**.

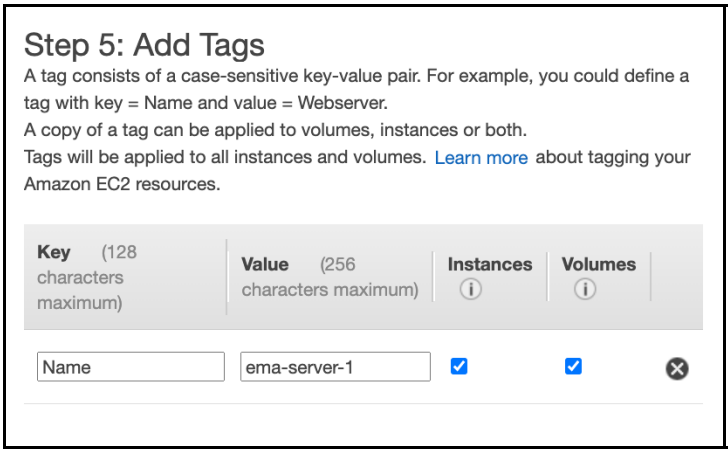
5.2.6 Adicione armazenamento



As configurações de armazenamento podem ser definidas como padrão, a menos que você precise de mais espaço. Consulte o Guia de instalação do servidor Intel® Endpoint Management Assistant para obter os requisitos do sistema.

Clique no botão **Next: Add Tags**.

5.2.7 Adicione tags

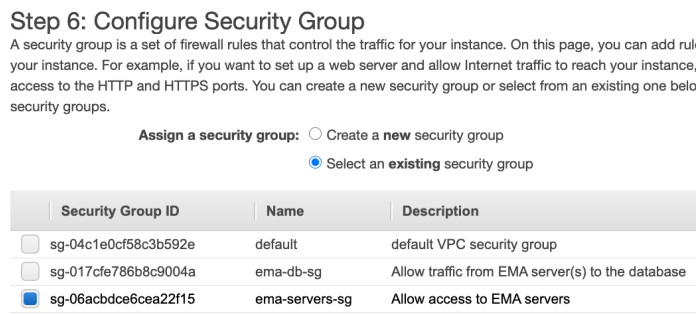


Adicione uma tag com a tecla “Name” e um valor do nome do servidor desejado.

Adicione quaisquer tags personalizadas que você queira para ajudar a organizar seus recursos, como discutido anteriormente na seção “Tags e Grupos de recursos” da introdução.

Clique no botão **Next: Configure Security Group**.

5.2.8 Configure o grupo de segurança



Configure o botão de seleção **Assign a security group** para *Select an existing security group*.

Selecione o grupo de segurança que você criou anteriormente para os servidores Intel EMA. Exemplo: *ema-servers-sg*

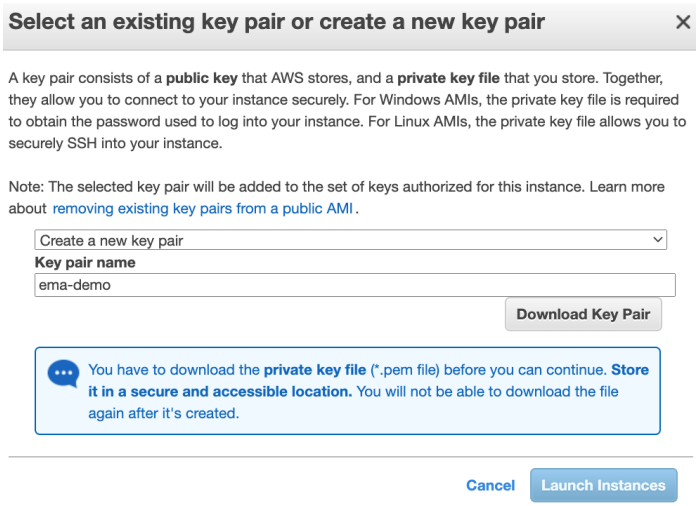
Clique no botão **Next: Review and Launch**.

Você pode receber um aviso de que não poderá se conectar à instância, uma vez que o grupo de segurança não tem a porta 3389 (RDP) aberta. Você pode ignorar essa mensagem e continuar, já que temos outra maneira de acessar a máquina virtual.

5.2.9 Analise o lançamento da instância

Analise os detalhes da instância e clique no botão **Launch**.

5.2.10 Selecione um par de chave da EC2



Você terá que selecionar um par de chave existente ou criar um novo par de chave.

Escolha o par de chave adequado na lista ou use a opção para criar um novo par de chave e clique no botão **Download Key Pair** para salvar o arquivo de chave privada em seu computador.

Se optar por usar um par de chave existente, você deve ter acesso ao arquivo de chave privada.

Clique no botão **Launch Instances**.

5.3 Criar uma segunda instância da EC2 (apenas servidor distribuído)

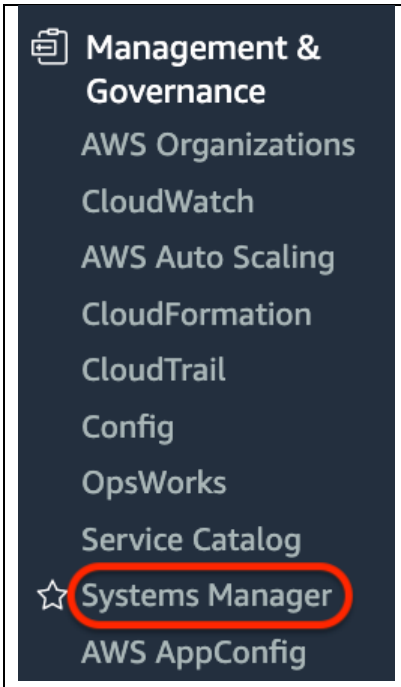
Para implantações de servidor distribuído, repita o procedimento anterior para criar o segundo servidor Intel EMA, selecionando uma sub-rede diferente e atribuindo uma tag de nome diferente, como *ema-server-2*.

6 Configure o AWS Systems Manager (apenas servidor distribuído)

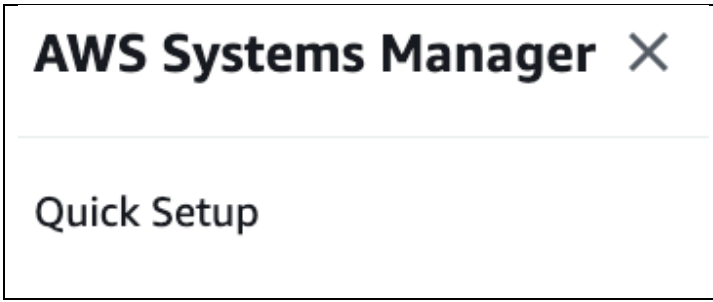
O AWS Systems Manager é um serviço que oferece maior visibilidade e controle de sua infraestrutura na AWS. Precisamos usar o componente do Session Manager que nos permitirá ter acesso remoto às VMs que não possuem um endereço de IP público.

Para saber mais sobre Systems Manager, acesse o seguinte link: https://aws.amazon.com/systems-manager/

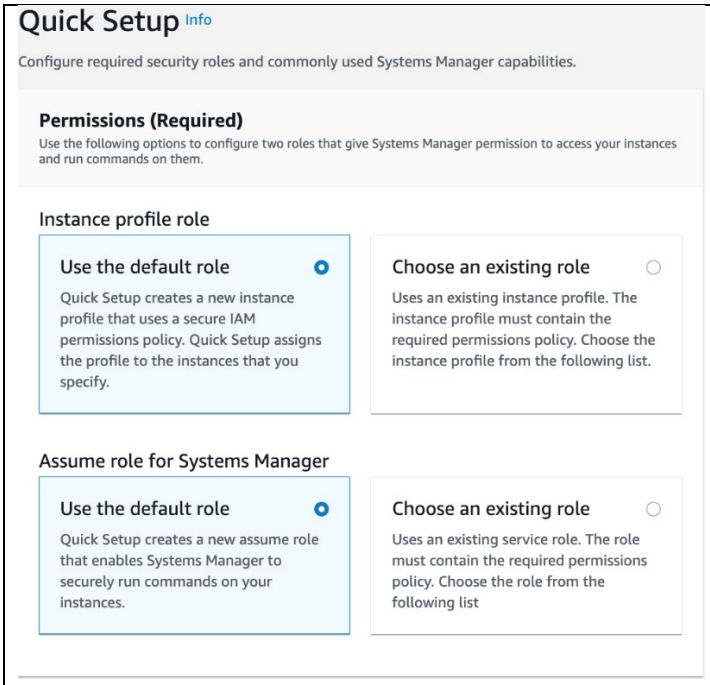
6.1 Acesse o serviço do Systems Manager

	No menu Services na seção Management & Governance, selecione Systems Manager.

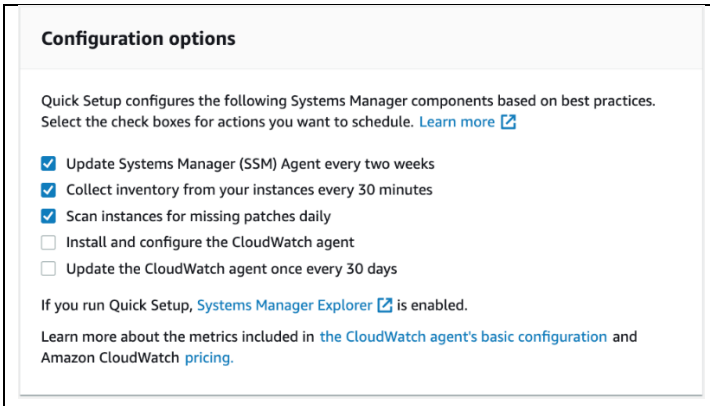
6.2 Inicie a configuração rápida

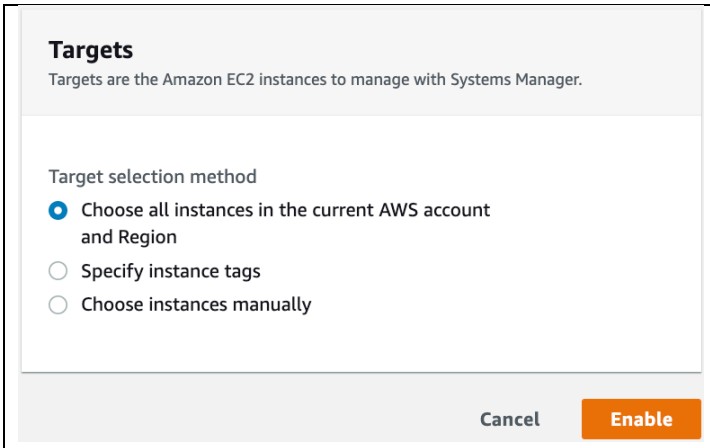
6.3 Escolha as opções de permissões



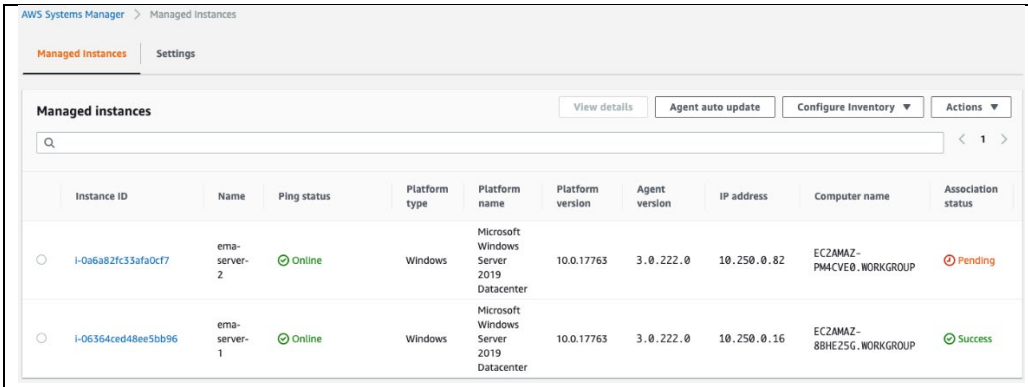
6.4 Escolha as opções de configurações



6.5 Escolha os objetivos



6.6 Verifique a lista de instâncias gerenciadas



Na barra lateral do Systems Manager, selecione Managed Instances.

Pode levar vários minutos para que suas máquinas virtuais apareçam nesta lista depois de executar a primeira configuração rápida.

Quando suas VMs tiverem sido registradas com sucesso no System Manager, você as verá listadas aqui.

6.7 Registrar em suas máquinas virtuais através do Session Manager

Usar o Session Manager através do console da AWS apenas permitirá que você se conecte a uma sessão Powershell* na VM. Para se conectar com o RDP, é necessário invocar o gerenciador de sessão de uma linha de comando local usando a AWS Command Line Interface (CLI) e transmitir uma opção para habilitar o encaminhamento de porta.

A instalação da AWS CLI está além do âmbito deste documento. Veja: https://aws.amazon.com/cli/ para obter mais informações.

Quando a CLI estiver instalada e configurada, e suas VMs estiverem aparecendo no AWS System Manager, você então poderá executar um comando CLI com esta sintaxe:

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

Substitua <instanceId> pela ID da instância EC2 na qual você quer se conectar. Exemplo: i-06364ced48ee5bb96

Se este comando for bem-sucedido, você poderá usar um cliente da Área de Trabalho Remota para se conectar ao localhost no localPortNumber que você especificou. Você pode fazer o login usando as credenciais para essa VM.

7 Implantação do Relational Database Service (RDS)

A AWS possui um mecanismo de banco de dados totalmente gerenciado para plataforma como um serviço chamado Amazon Relational Database Service (Amazon RDS), que facilita configurar, operar e escalar um banco de dados relacional na AWS Cloud. Ele oferece uma capacidade eficiente e redimensionável e gerencia tarefas de administração de banco de dados comuns, incluindo backup, patches de software, detecção automática de falhas e recuperação.

O bloco de construção básico do Amazon RDS é a instância de banco de dados. Uma instância de banco de dados é um ambiente isolado do banco de dados na AWS Cloud. Sua instância de banco de dados pode conter vários bancos de dados criados pelo usuário. Você pode acessar sua instância de banco de dados usando as mesmas ferramentas e aplicações utilizadas em uma instância de banco de dados autônoma. A capacidade de computação e memória de uma instância de banco de dados é determinada pela classe da instância de banco de dados. Você pode selecionar a instância de banco de dados que melhor atenda às suas necessidades. Se suas necessidades mudarem ao longo do tempo, você pode mudar as instâncias de banco de dados.

Como nossa VPC foi criada com várias sub-redes em diferentes Zonas de disponibilidade, será possível iniciar uma instância RDS com uma opção denominada implantação Multi-AZ. Ao escolher essa opção para nossa implantação da produção, sua instância de banco de dados principal é replicada automaticamente e sincronizada para uma instância de banco de dados secundária em uma Zona de disponibilidade diferente. Esta abordagem ajuda a oferecer suporte para redundância de dados e failover, eliminar congelamentos de E/S e minimizar os pontos das latências durante os backups do sistema. Criaremos um grupo de sub-redes de banco de dados que informará ao RDS quais zonas de disponibilidade devem ser usadas para essa finalidade.

Um grupo de segurança que criamos anteriormente neste guia será usado para controlar o acesso à instância do RDS e permitir que apenas a nossa instância do Intel EMA EC2 se conecte a ele.

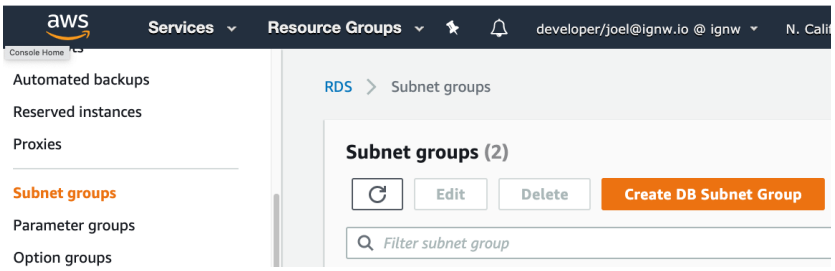
Para obter mais informações sobre RDS, acesse o seguinte link:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

Siga este procedimento para criar uma instância do Relational Database Service (RDS) e anexe o grupo de segurança criado anteriormente para permitir o tráfego da instância do Intel EMA EC2 para o banco de dados.

7.1 Acesse o serviço de RDS

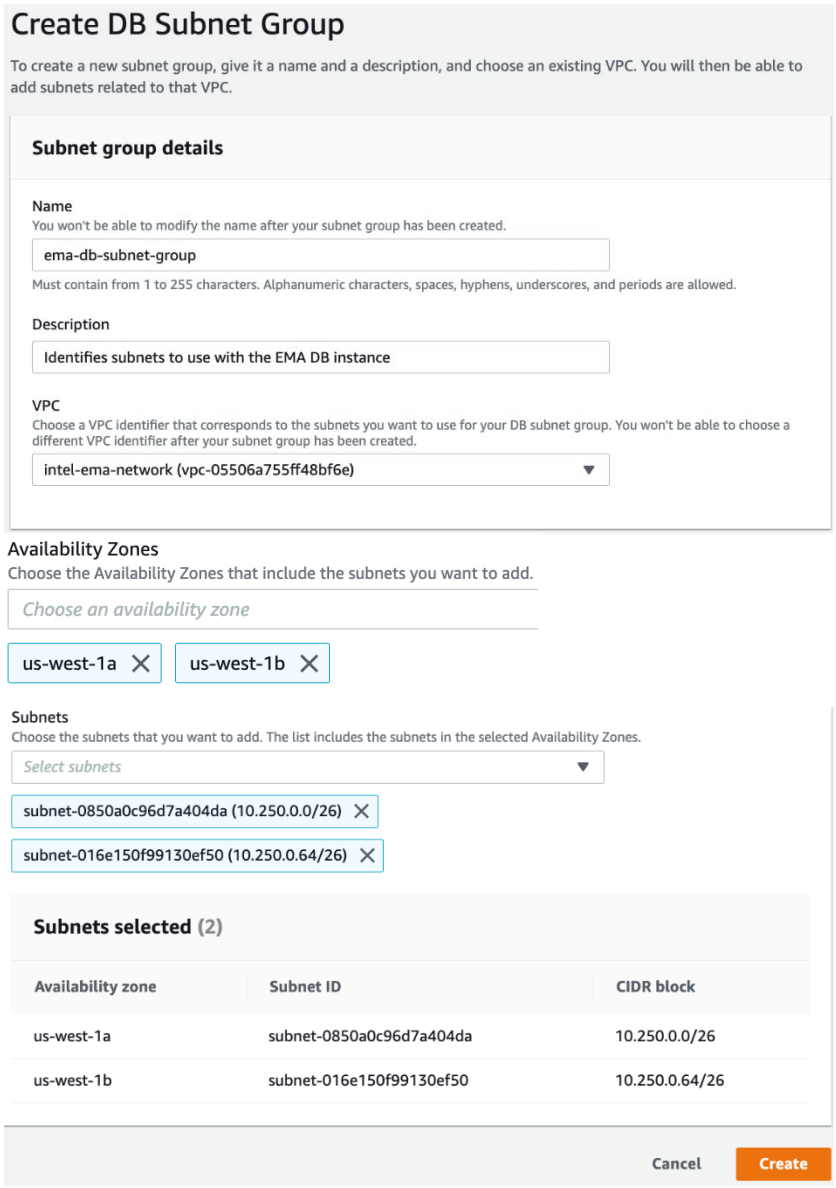
No menu **Services**, em **Database**, selecione **RDS**.

7.2 Criar grupo de sub-redes de banco de dados



Na barra lateral do **RDS**, selecione **Subnet groups** e clique no botão **Create DB Subnet Group**.

7.2.1 Detalhes do grupo de sub-redes

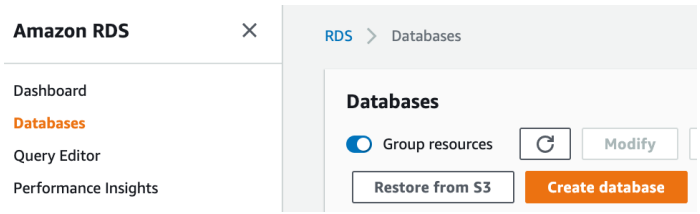


Insira os detalhes do grupo de sub-redes como segue.

- **Name**: insira um nome exclusivo.
  Exemplo: *ema-db-subnet-group*
- **Description** (opcional)
  Exemplo: *Identifies subnets to use with the EMA DB instance*
- **VPC**: selecione a VPC que você criou anteriormente.
- **Availability Zones**: selecione as duas zonas nas quais você criou as sub-redes.
- **Subnets**: escolha as duas sub-redes privadas que foram criadas anteriormente.

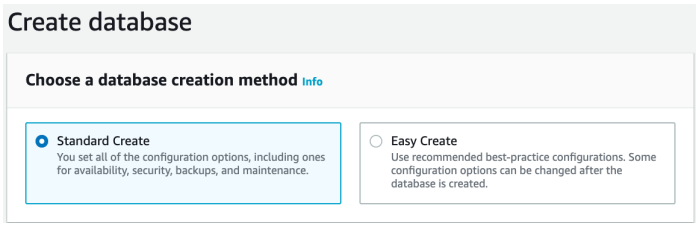
Clique no botão **Create**.

7.3 Criar um banco de dados



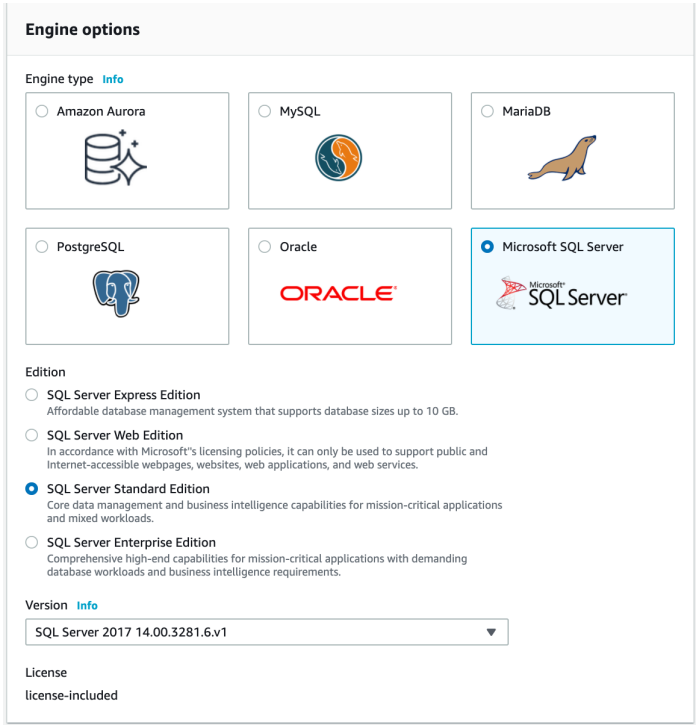
Na barra lateral do RDS, selecione Databases e clique no botão **Create database**.

7.3.1 Escolha um método de criação de banco de dados



Selecione o método de criação **Standard Create**.

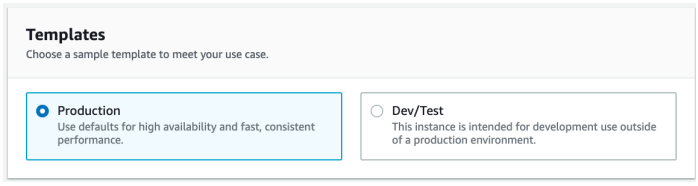
7.3.2 Escolha o tipo de mecanismo e edição



Selecione o mecanismo do **Microsoft SQL Server**.

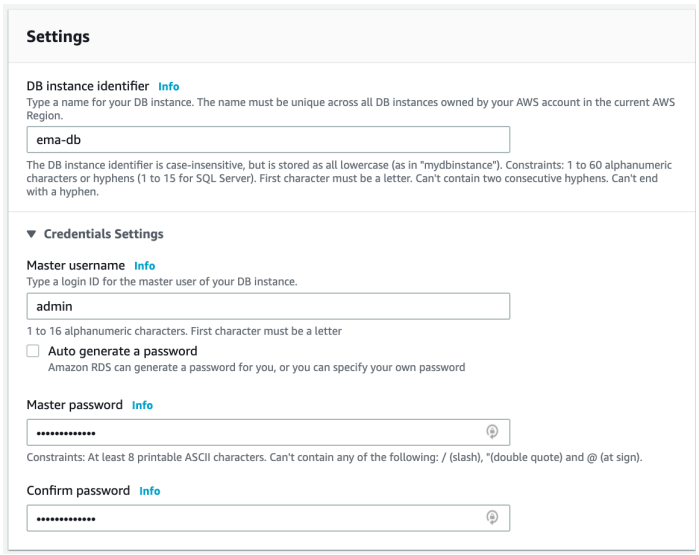
Selecione a edição do servidor SQL apropriada. Para fins desta documentação, estamos assumindo uma implantação de produção que utiliza o SQL Server Standard Edition. O SQL Server Express Edition pode ser usado para desenvolvimento e testes a fim de reduzir custos.

7.3.3 Escolha o modelo de implantação



Em Templates, selecione **Production**.

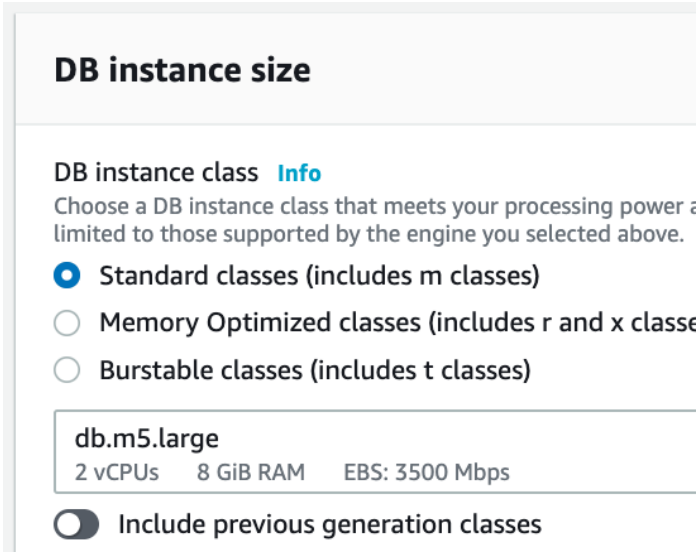
7.3.4 Configure o nome da instância e as credenciais do usuário mestre



Atribua um nome exclusivo ao banco de dados.
Exemplo: *ema-db*

Crie um nome de usuário e uma senha.

7.3.5 Configure o tamanho da instância de banco de dados

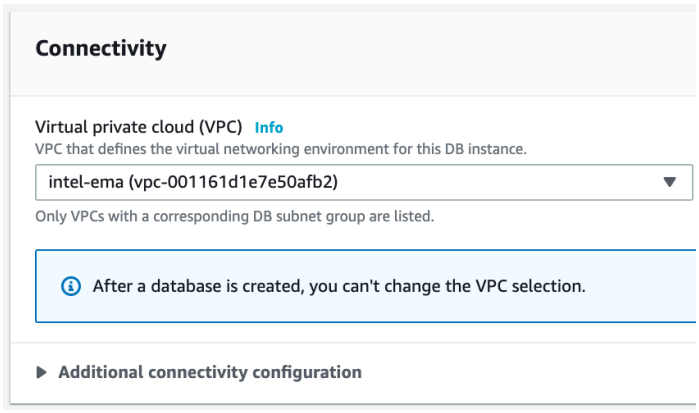


Configure a classe da instância de banco de dados para oferecer os recursos adequados.
Sugerido: *db.m5.large*

7.3.6 Configure o armazenamento (opcional)

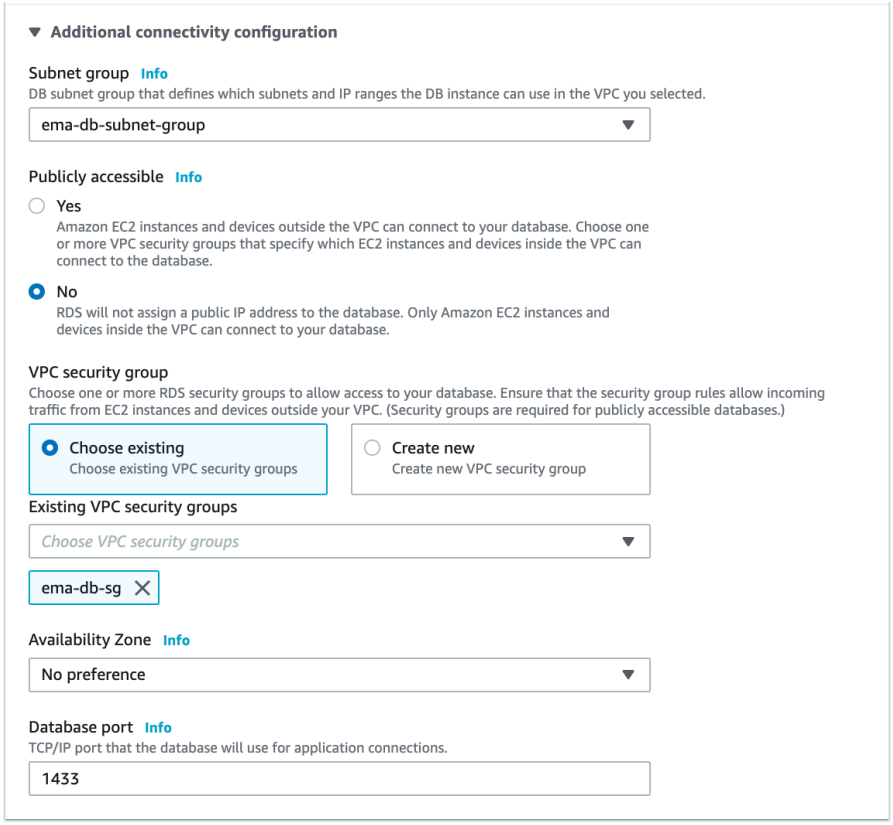
Você pode aumentar a quantidade padrão de armazenamento alocada, se desejar. Vamos deixar o padrão. Você ainda pode aumentar a capacidade de armazenamento posteriormente.

7.3.7 Configure a conectividade



Em **Connectivity**, selecione a VPC que você criou anteriormente e expanda a seção **Additional connectivity configuration**.

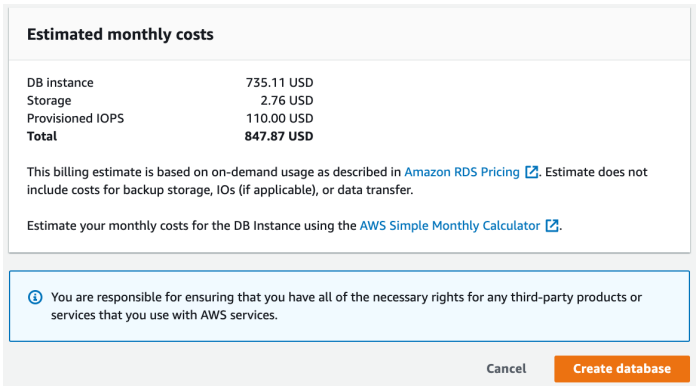
7.3.8 Configure a conectividade — Configuração adicional da conectividade



Escolha o grupo de sub-redes de dados que você criou anteriormente.

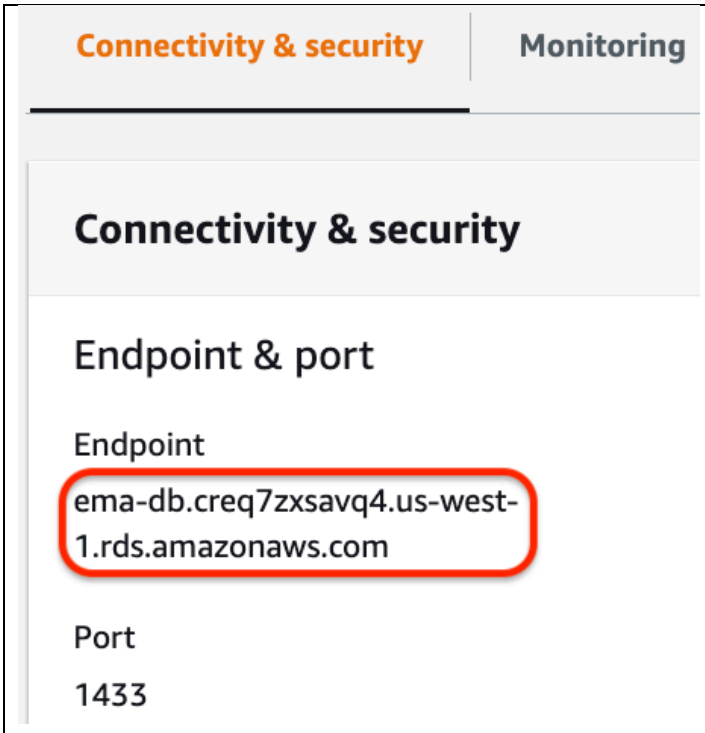
Desmarque o grupo de segurança padrão da VPC e escolha o grupo de segurança existente criado anteriormente para o banco de dados.

7.3.9 Analise e crie



Analise o custo estimado e clique no botão **Create database**.

7.4 Obtenha o nome de host do banco de dados



Depois que a implantação do banco de dados terminar, a página de detalhes exibirá o nome de host do banco de dados que você usará para configurar o software Intel EMA durante o processo de instalação.

8 Implantação do balanceador de carga (apenas servidor distribuído)

8.1 Visão geral

Um AWS Network Load Balancer é um balanceador de carga Layer-4 (TCP) que distribui o tráfego do usuário entre várias instâncias de suas aplicações. Ao espalhar a carga, o balanceamento de carga reduz o risco de que suas aplicações se tornem sobrecarregadas, lentas ou não funcionais. Após receber uma solicitação de conexão, o balanceador de carga seleciona um destino adequado a partir de um grupo de destino associado de acordo com as regras de encaminhamento e antecipa a conexão a esse destino.

Um *ouvinte* verifica as solicitações de conexão dos clientes usando o protocolo e a porta que você configurar, e encaminha as solicitações para o grupo de destino.

Cada *grupo de destino* encaminha as solicitações para um ou mais destinos registrados, como instancias de EC2, usando o protocolo e o número da porta que você especificar. Você pode configurar verificações de integridade por grupo de destino. As verificações de integridade são executadas em todos os destinos registrados para um grupo de destino especificado em uma regra para o ouvinte em seu balanceador de carga.

Permitiremos várias Zonas de disponibilidade para os balanceadores de carga que implantamos; assim, poderemos direcionar o tráfego para destinos em qualquer zona.

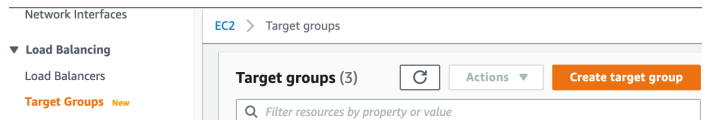
O balanceador de carga terá um nome de host gerado automaticamente, que apontará para os endereços voltados ao público dos balanceadores de carga relacionados em cada AZ. Será necessário criar um registro DNS do CNAME apelidando esse nome de host para usar seu domínio personalizado a fim de alcançar o(s) servidor(es) Intel EMA.

Há outras possibilidades de configuração do balanceamento de carga que não foram abordadas neste documento. Consulte seu departamento de TI referente a quaisquer requisitos ou práticas que possa querer implementar. Para obter mais informações sobre o balanceamento de carga na AWS, acesse o seguinte link:
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

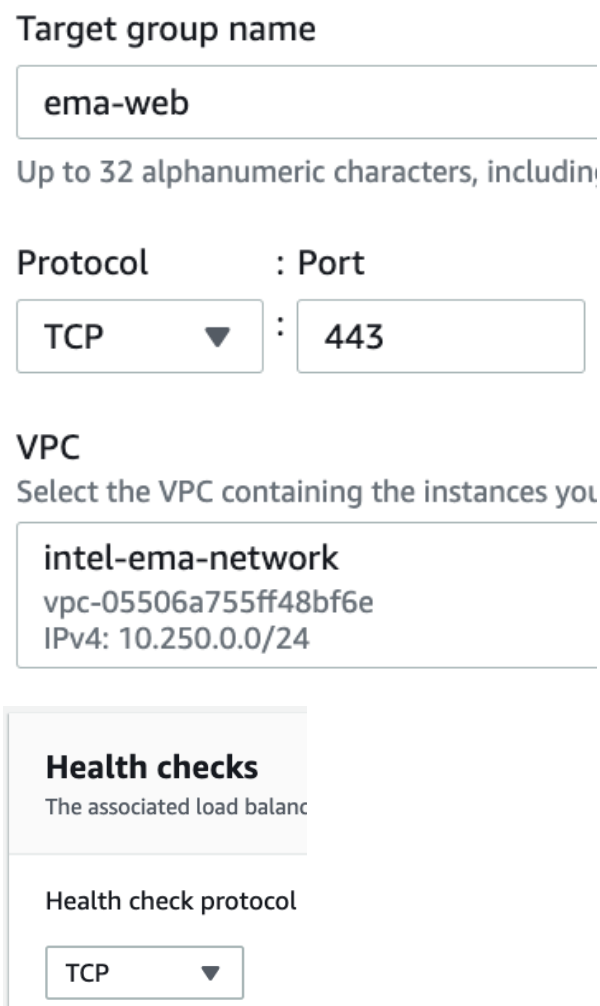
8.2 Crie grupos de destino

Siga este procedimento para criar um grupo de destino para cada porta TCP que será servida pelo nosso balanceador de carga, criar verificações de integridade, e registrar nossas máquinas virtuais para receber tráfego para cada grupo de destino.

8.2.1 Crie grupos de destino

	Na barra lateral da **EC2**, em **Load Balancing**, selecione **Target Groups**. Clique no botão **Create target group**.

8.2.2 Configure um grupo de destino para TCP/443

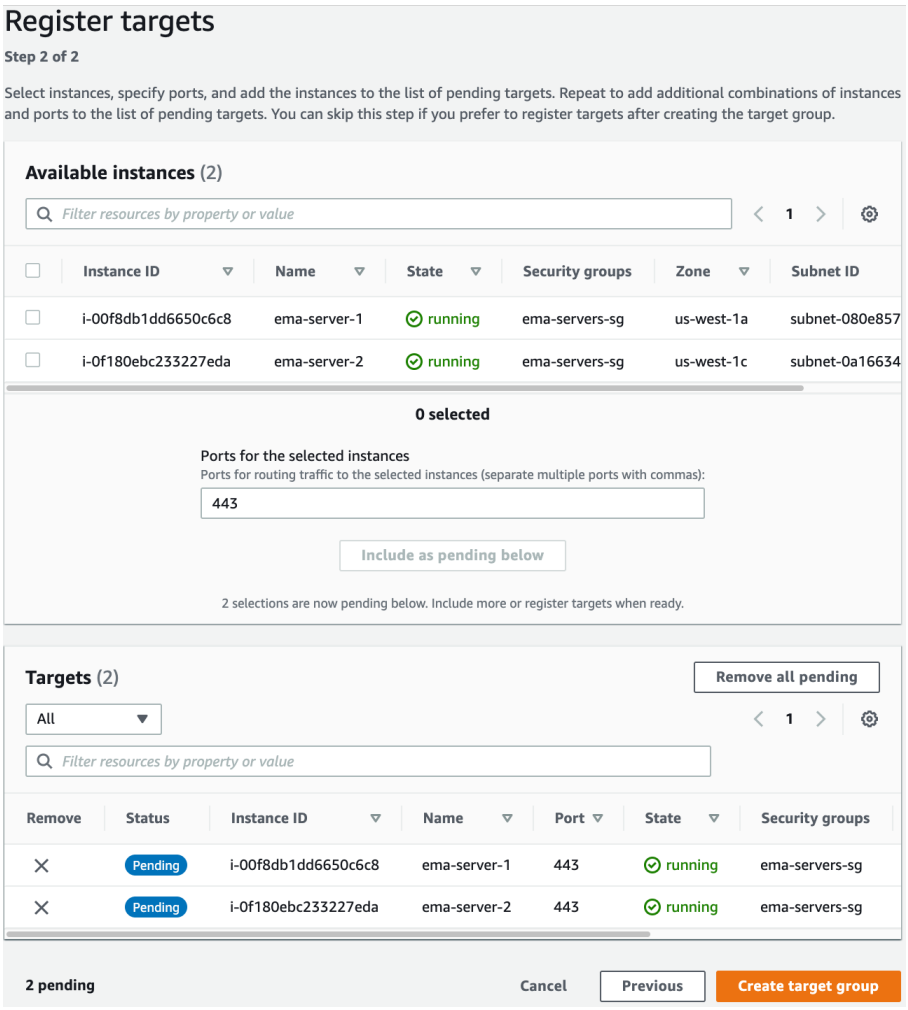


Configure o grupo de destino como segue:

- **Target type**: *Instances*
- **Target group name**: insira um nome exclusivo. Exemplo: *ema-web*
- **Protocol**: *TCP*
- **Port**: *443*
- **VPC**: selecione a VPC que você criou anteriormente.
- **Health check protocol**: *TCP*

Clique em **Next** para avançar para a tela **Register targets**.

8.2.2.1 Registre ambas as instancias EC2 como destinos



Selecione ambas as instâncias de VM EMA e clique no botão **Include as pending below**.

Clique no botão **Create target group**.

8.2.3 Crie/configure um destino para TCP/8084

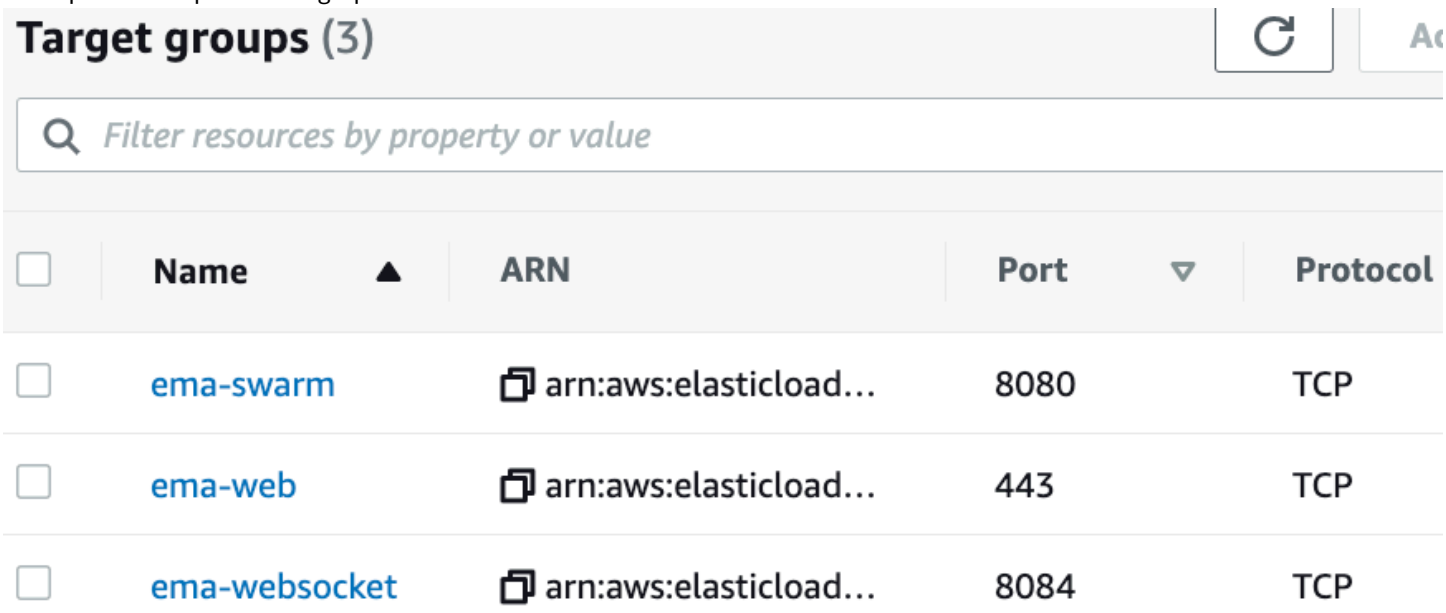
Repita as etapas acima para outro grupo de destino chamado “ema-websocket” para TCP/8084.

8.2.4 Configure um destino para TCP/8080

Repita as etapas acima para outro grupo de destino chamado “ema-swarm” para TCP/8080.

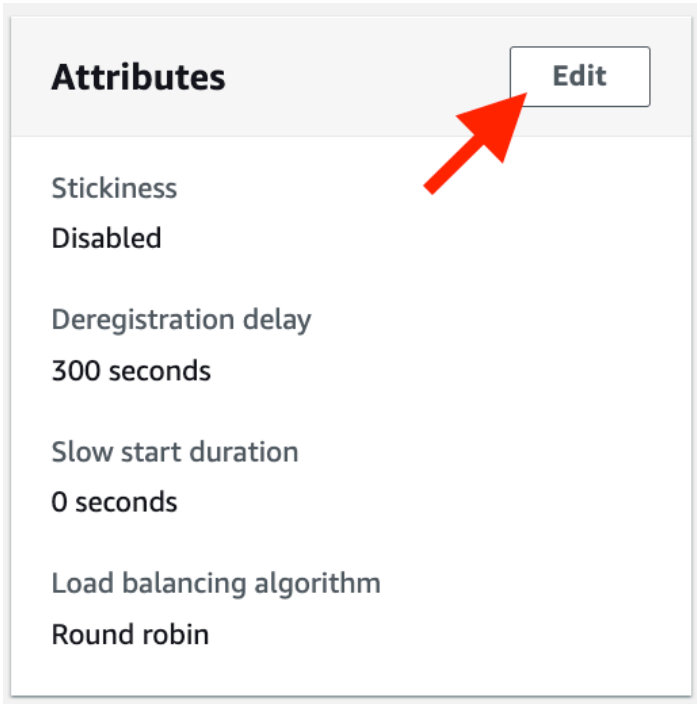
8.2.5 Analise os grupos de destino

Verifique se você possui três grupos de destino criados.

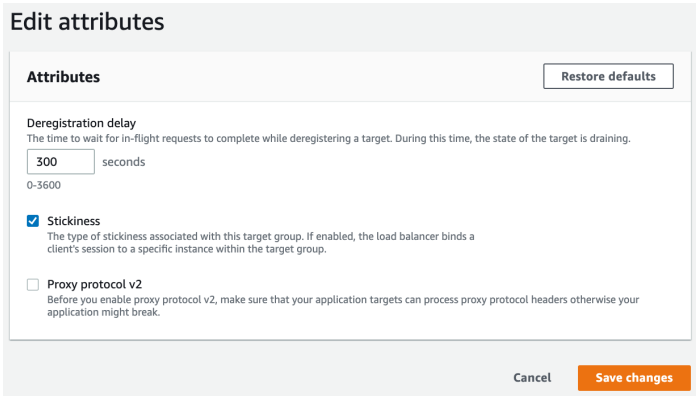


8.2.6 Habilite Stickiness para o grupo de destino TCP/443

8.2.6.1 Detalhes do grupo de destino

	Clique no nome do grupo de destino *ema-web* para acessar a tela de detalhes de grupo. Na seção **Attributes**, clique no botão **Edit**.

8.2.6.2 Edite os atributos

	Habilite a bandeira **Stickiness**. Clique no botão **Save changes**.

8.2.7 Habilite Stickiness para o grupo de destino TCP/8084

Repita as instruções anteriores para habilitar Stickiness para o grupo de destino ema-websocket (TCP/8084).

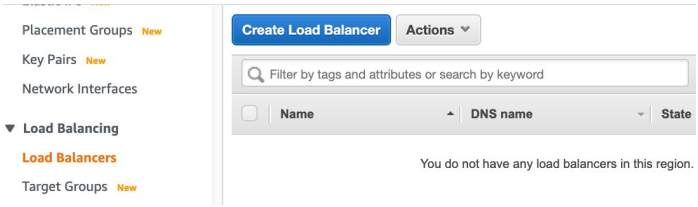
8.2.8 Nota sobre o monitoramento da integridade do grupo de destino

Em qualquer um dos grupos de destino, você pode verificar as abas **Targets** e **Monitoring** para ver o status da verificação de integridade das instâncias de destino. Essas verificações de integridade falharão inicialmente até que o software Intel EMA tenha sido instalado.

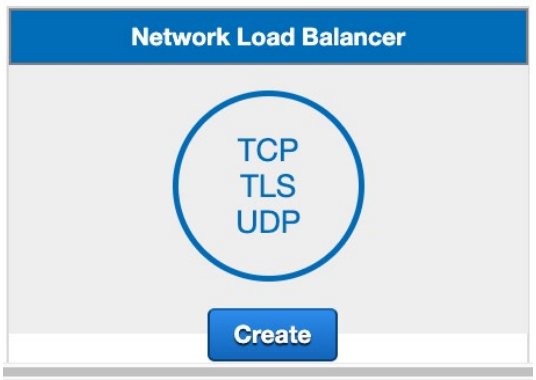
8.3 Criar um balanceador de carga de rede para receber tráfego da Internet

Siga este procedimento para criar um balanceador de carga de rede para distribuir o tráfego para grupos de destino adequados.

8.3.1 Crie o balanceador de carga

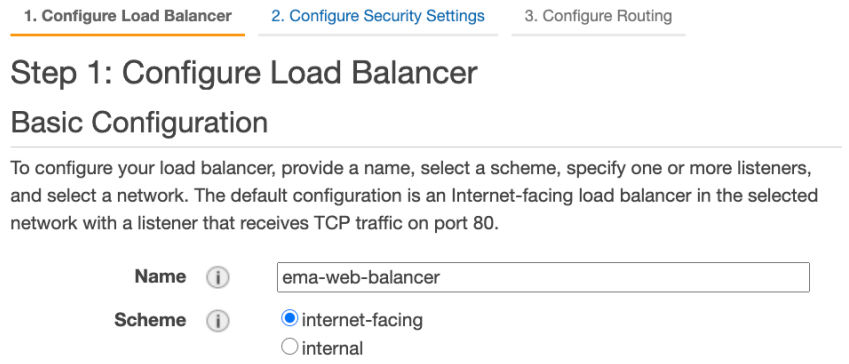
	Na barra lateral da **EC2**, em **Load Balancing**, selecione **Load Balancers** e clique em **Create Load Balancer**.

8.3.2 Escolha o tipo de balanceador de carga

	Clique no botão **Create** e no título Select **Network Load Balancer**.

8.3.3 Configure o balanceador de carga

8.3.3.1 Configuração básica



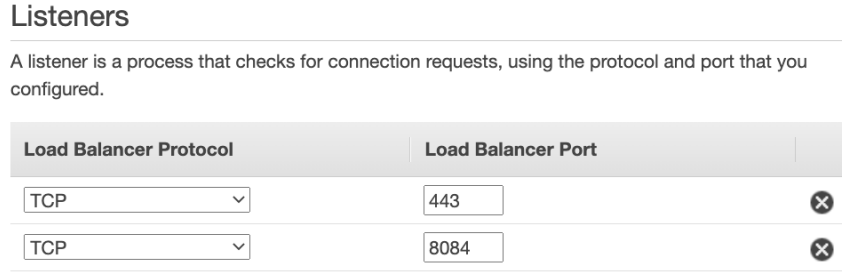
Insira a configuração básica.

Name: insira um nome exclusivo.
Exemplo: *ema-web-balancer*

Scheme: internet-facing.
Nota: se a sua organização tiver uma VPN site a site com acesso privado ao IP pela AWS, isso provavelmente se trata de um balanceador de carga interna vinculado às sub-redes privadas.

Para este guia, não presumimos esse acesso, portanto, será um balanceador de carga voltado para a Internet vinculado às sub-redes públicas.

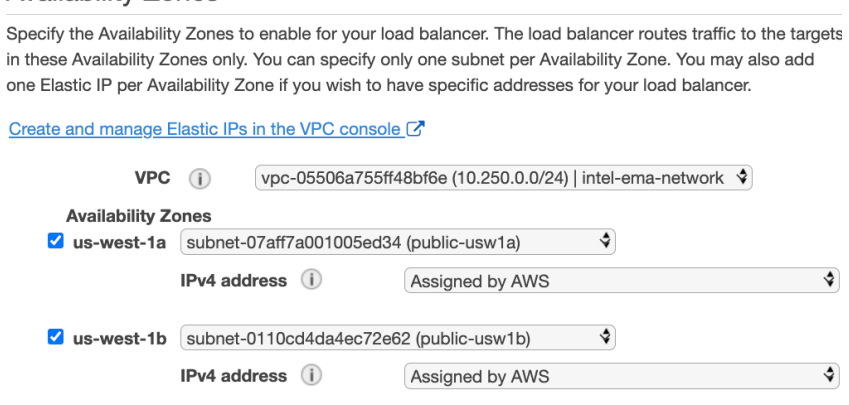
8.3.3.2 Ouvintes



Na seção **Listeners**, adicione ouvintes para esses protocolos e portas.

- *TCP 443*
- *TCP 8084*

8.3.3.3 Zonas de disponibilidade



Configure a seção **Availability Zones** da seguinte forma:

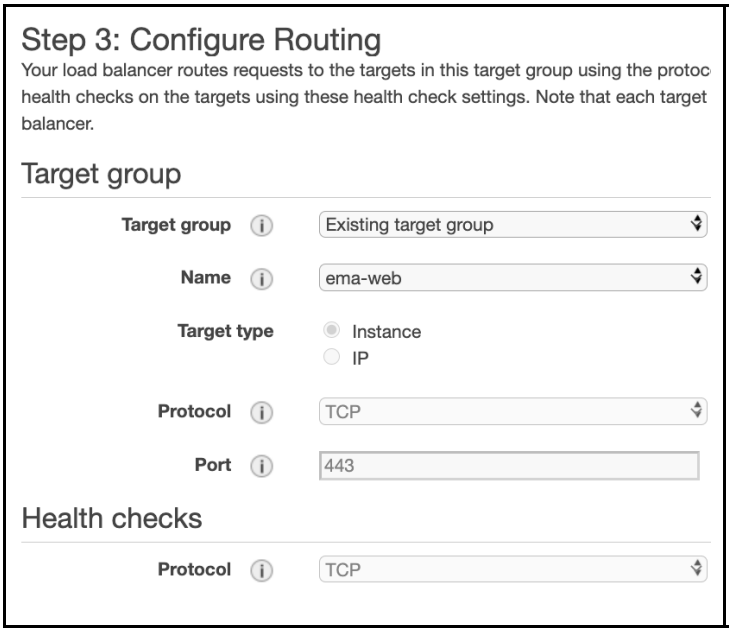
- **VPC**: selecione a VPC que você criou anteriormente.
- **Availability Zones**: habilite ambas as zonas de disponibilidade e selecione ambas as suas sub-redes públicas. O endereço IPv4 deve ser configurado para *Assigned by AWS*.

Clique no botão **Next: Configure Security Settings**.

8.3.3.4 Defina as configurações de segurança

Não há nada a ser configurado nesta etapa. Clique no botão **Next: Configure Routing**.

8.3.3.5 Configure o roteamento

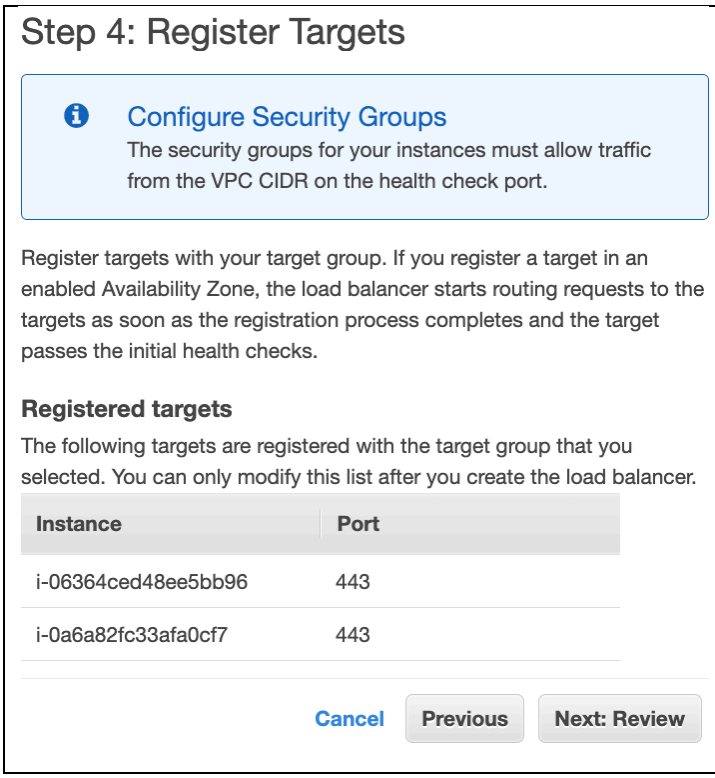


Na **Step 3: Configure Routing**, configure o grupo de destino da seguinte forma.

- **Target group**: *Existing target group*
- **Name**: selecione o nome do grupo de destino TCP/443 que você criou anteriormente.
  Exemplo: *ema-web*

Clique no botão **Next: Register Targets**.

8.3.3.6 Registre os destinos

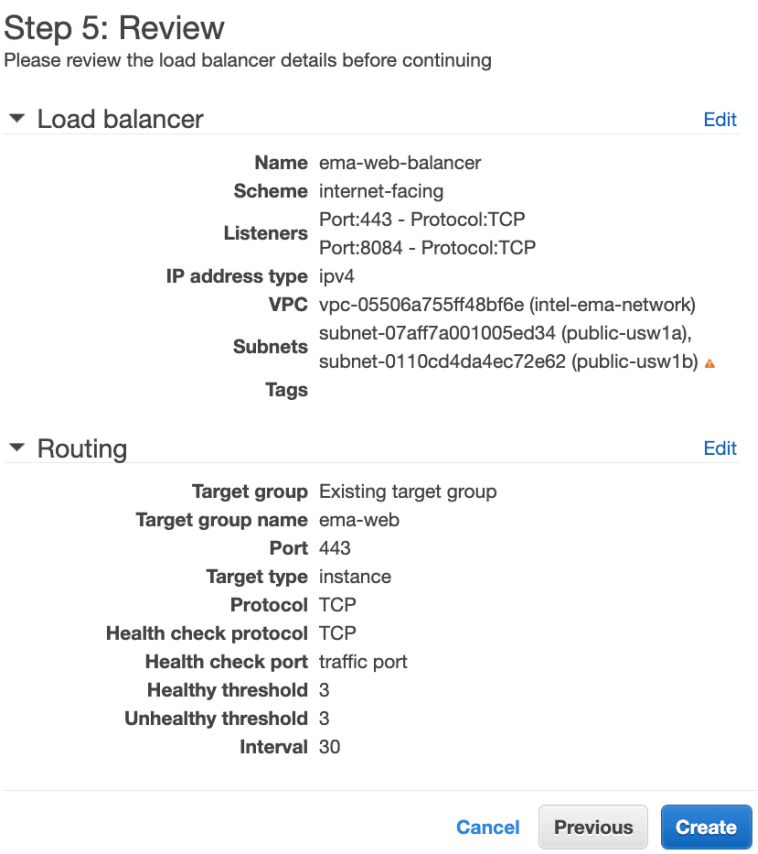


Confirme que esteja visualizando duas instâncias listadas como destinos registrados.

Clique no botão **Next: Review**.

8.3.3.7 Analise

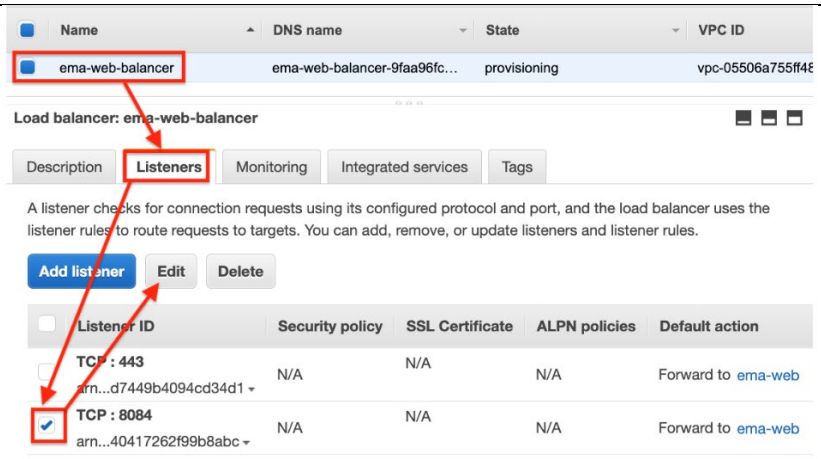
Na **Step 5: Review**, verifique se ele se parece com o exemplo fornecido aqui, depois clique no botão **Create**.



8.3.4 Configure as regras de encaminhamento do balanceador de carga

O destino de encaminhamento está correto para o ouvinte de porta 443, mas é preciso editar e mudar o ouvinte para a porta 8084 para encaminhar para o grupo de destino correto.

8.3.4.1 Edite os ouvintes do balanceador de carga



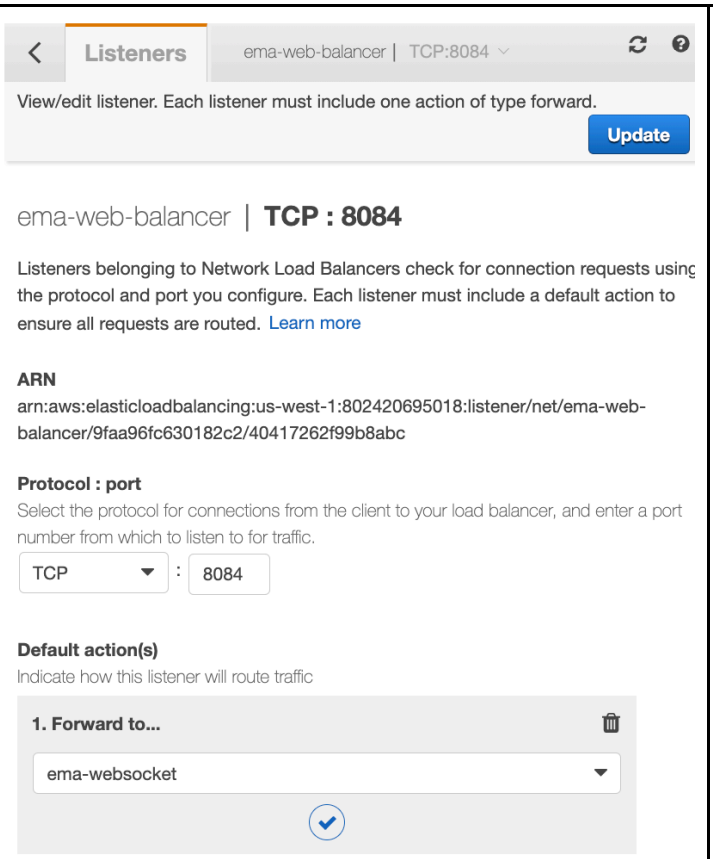
Selecione o balanceador de carga que você criou.

Selecione a aba **Listeners**.

Marque a caixa ao lado do ouvinte TCP/8084.

Clique no botão **Edit**.

8.3.4.2 Atualize a ação de encaminhamento do ouvinte TCP/8084

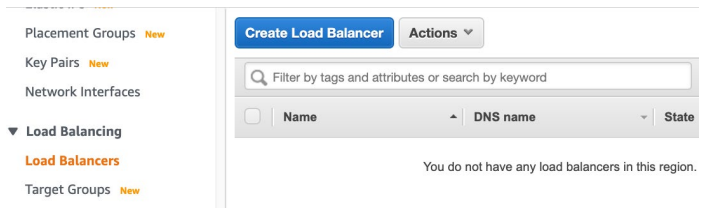


Mude a ação padrão para encaminhar para o ouvinte websocket.

Clique no botão **Update**.

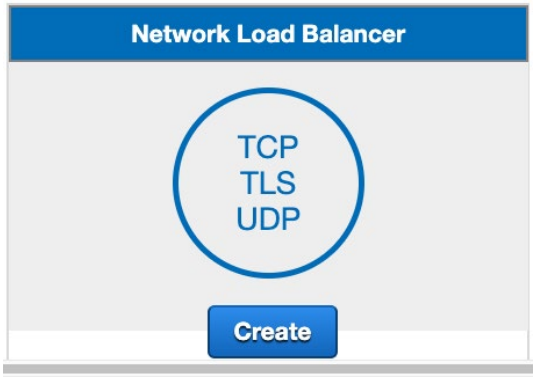
8.4 Criar um balanceador de carga de rede para tráfego swarm

8.4.1 Crie o balanceador de carga



Na barra lateral da **EC2**, em **Load Balancing**, selecione **Load Balancers** e clique em **Create Load Balancer**.

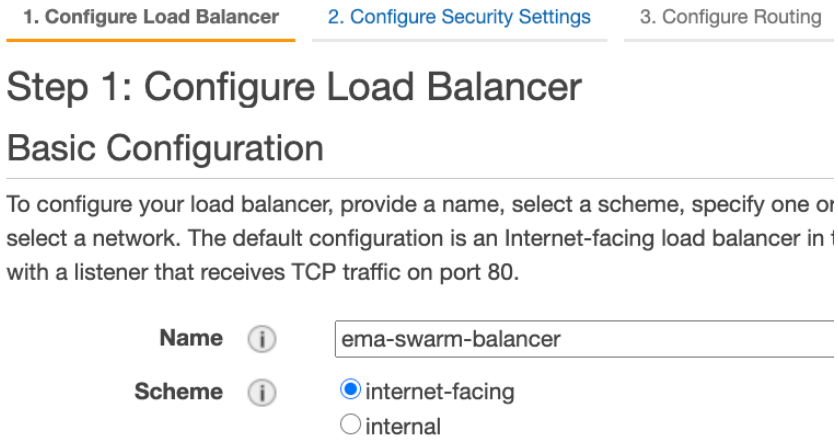
8.4.2 Escolha o tipo de balanceador de carga



Clique no botão **Create** e no título Select **Network Load Balancer**.

8.4.3 Configure o balanceador de carga

8.4.3.1 Configuração básica

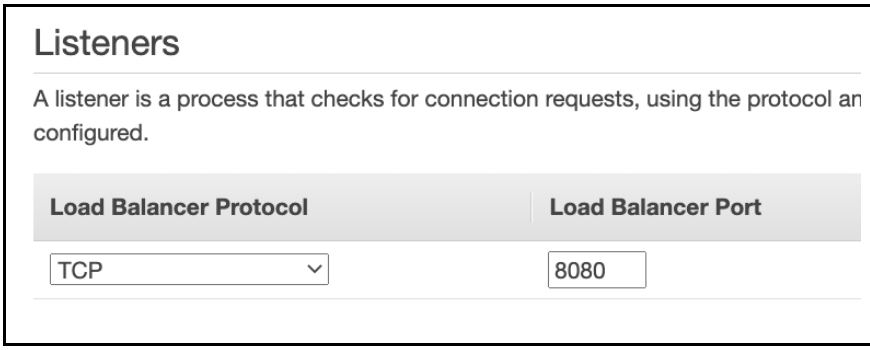


Insira a configuração básica.

Name: insira um nome exclusivo.
Exemplo: *ema-swarm-balancer*

Scheme: internet-facing.

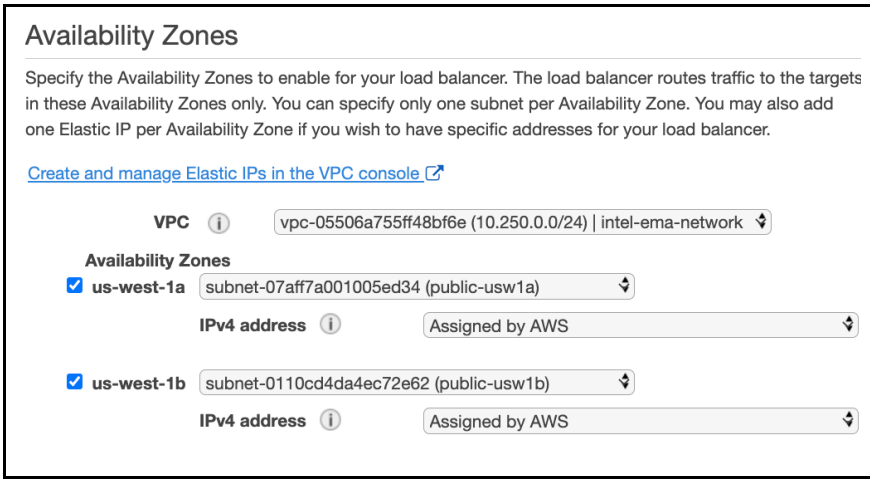
8.4.3.2 Ouvintes



Na seção **Listeners**, adicione ouvintes para esses protocolos e portas.

- *TCP 8080*

8.4.3.3 Zonas de disponibilidade



Configure a seção **Availability Zones** da seguinte forma:

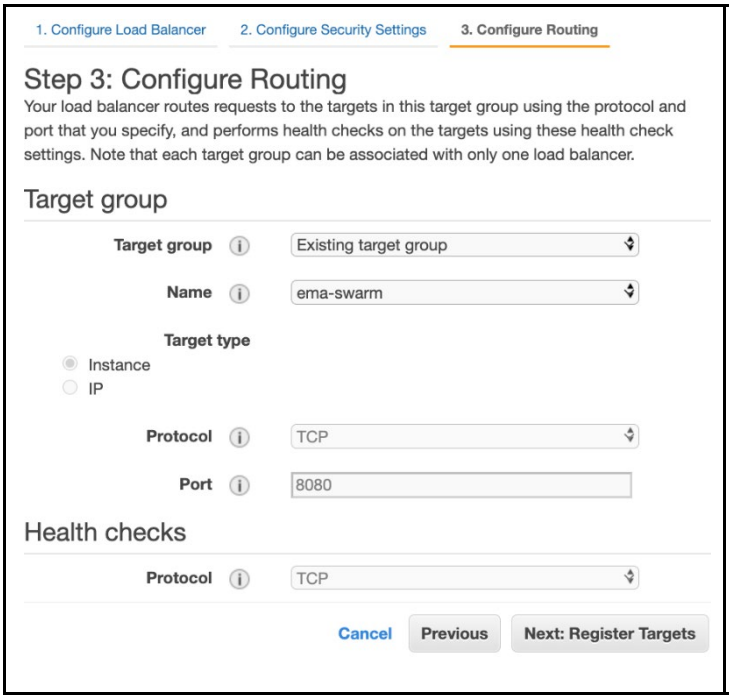
- **VPC**: selecione a VPC que você criou anteriormente.
- **Availability Zones**: habilite ambas as zonas de disponibilidade e selecione ambas as suas sub-redes públicas. O endereço IPv4 deve ser configurado para *Assigned by AWS*.

Clique no botão **Next: Configure Security Settings**.

8.4.3.4 Defina as configurações de segurança

Não há nada a ser configurado nesta etapa. Clique no botão **Next: Configure Routing**.

8.4.3.5 Configure o roteamento



Na **Step 3: Configure Routing**, configure o grupo de destino da seguinte forma.

- **Target group**: *Existing target group*
- **Name**: selecione o nome do grupo de destino TCP/8080 que você criou anteriormente. Exemplo: *ema-swarm*

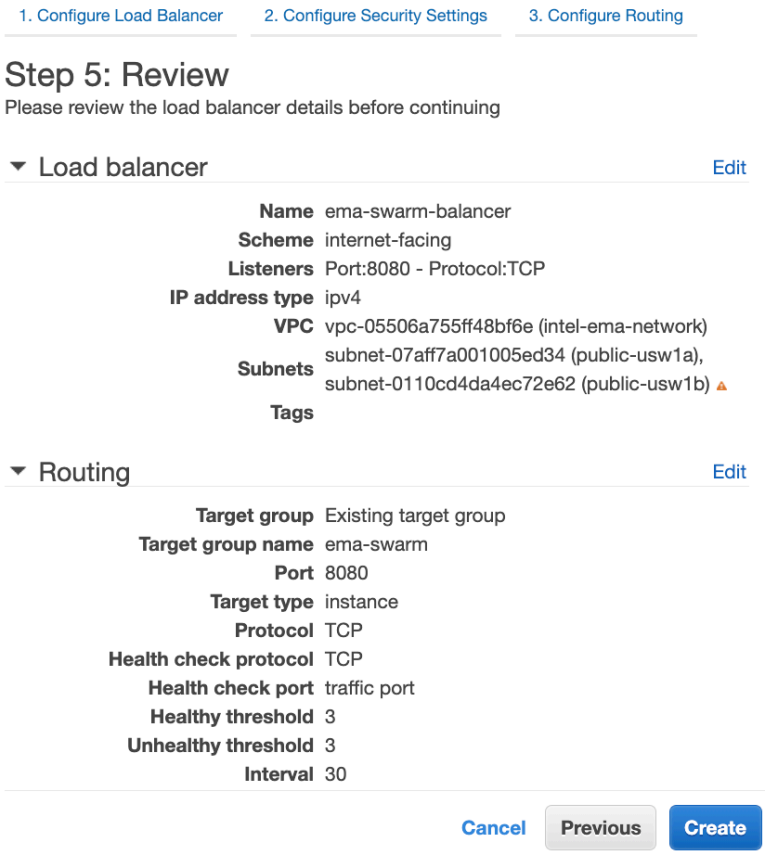
Clique no botão **Next: Register Targets**.

8.4.3.6 Registre os destinos

	Confirme que esteja visualizando duas instâncias listadas como destinos registrados. Clique no botão **Next: Review**.

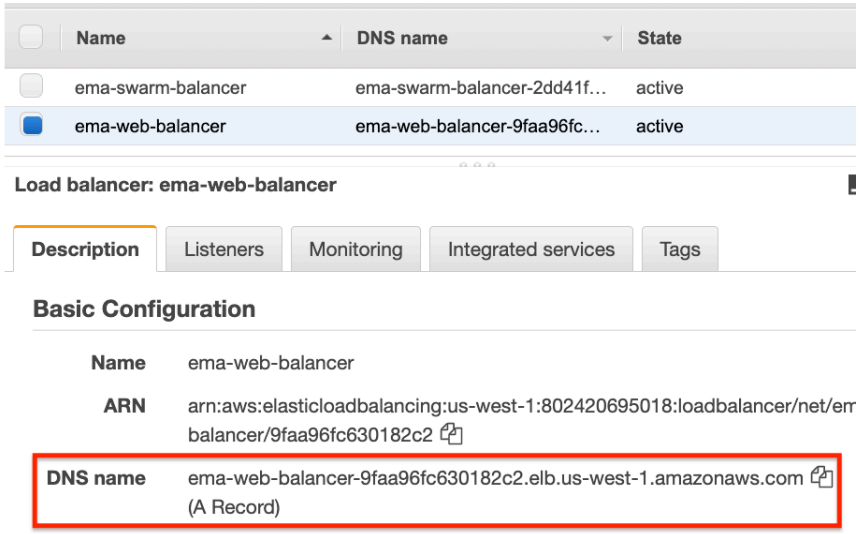
8.4.3.7 Analise

Na **Step 5: Review**, verifique se ele se parece com o exemplo fornecido aqui, depois clique no botão **Create**.



8.4.4 Anote o nome do DNS do balanceador de carga

Volte para a aba **Description** dos balanceadores de carga e anote os nomes do DNS. Será necessário criar registros CNAME com seu provedor de DNS para seu nome de domínio personalizado para que você possa direcionar seu tráfego de internet do Intel EMA e o tráfego de swarm para os balanceadores de carga.


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 Apêndice A — Notas sobre a integração do Active Directory*

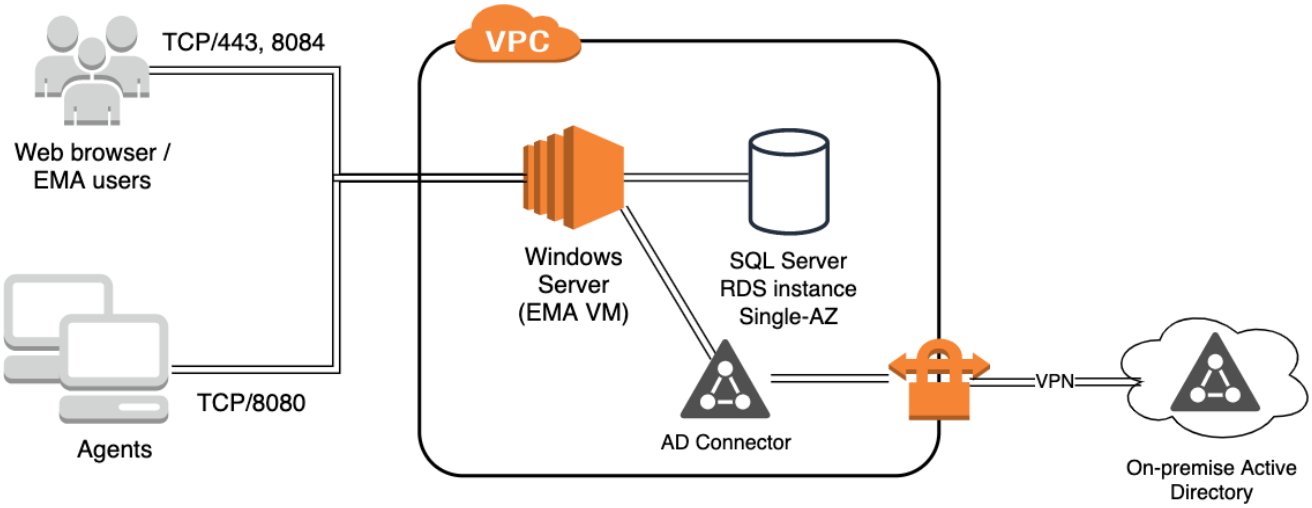
Há várias maneiras de integrar o Active Directory* à AWS para fazer a junção das suas máquinas virtuais a um domínio e usar a autenticação do AD. Como as necessidades da organização podem ser bastante variadas, este apêndice oferece apenas algumas dicas resumidas sobre como estender um diretório local existente para a nuvem para essa finalidade. Provedores de nuvem mudam e ampliam suas ofertas de serviço de tempos em tempos; portanto, você deve fazer sua própria pesquisa antes de implantar uma solução de produção e verificar o que faz mais sentido para a sua empresa.

Para obter mais informações sobre os serviços do Active Directory na AWS, acesse os seguintes links:

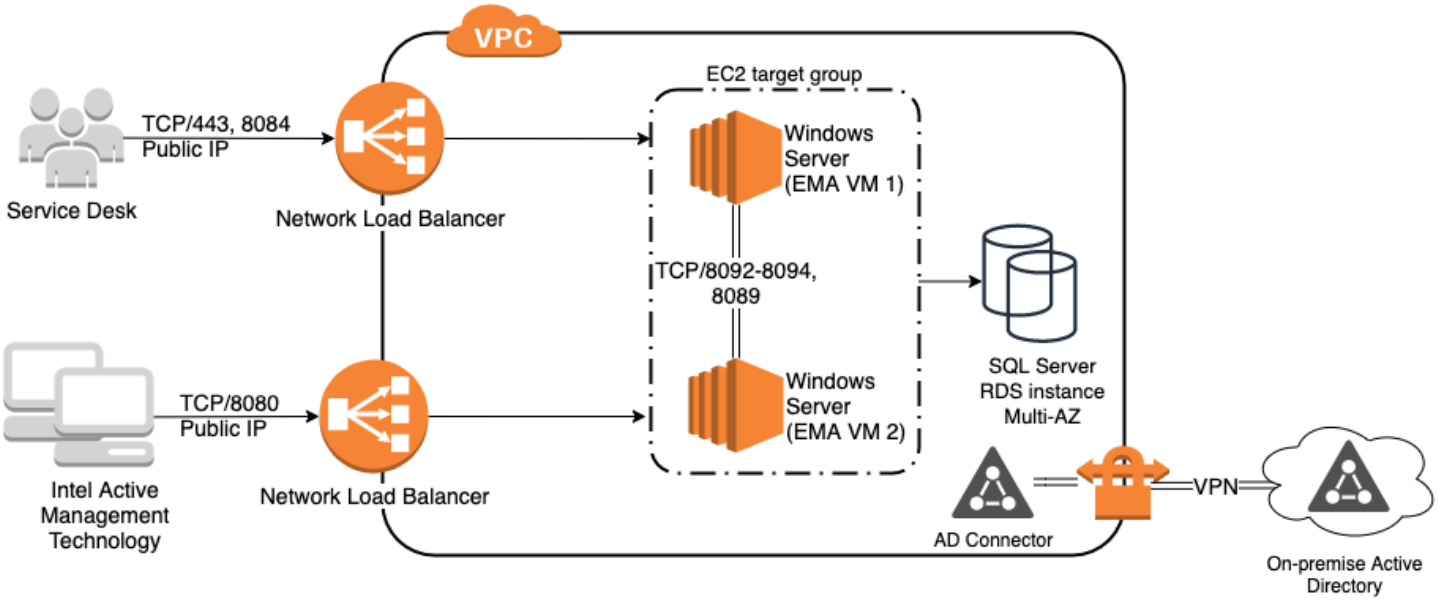
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.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

10 Diagrama de arquitetura com a integração do Active Directory

10.1 Implantação de servidor único



10.2 Implantação de servidor distribuído



10.3 Usando o conector AWS AD para estender o Active Directory para a nuvem

- ❑ Crie uma VPN para se conectar à sua rede local para fornecer conectividade aos seus controladores de domínio.
  - ❑ Crie um Gateway do cliente para representar a extremidade remota (local) da VPN.
  - ❑ Crie um Gateway virtual privado para fornecer roteamento entre a VPN e sua VPC.
  - ❑ Conecte o Gateway virtual privado à sua VPC.
  - ❑ Crie uma conexão VPN selecionando o novo Gateway do cliente e VPG.

        - ❏ Selecione a opção de roteamento estático e insira as redes disponíveis através da conexão VPN. Isso deve incluir seus controladores de domínio locais.
        - ❏ Você pode permitir que a Amazon gere seus endereços de túnel e chaves.
    - ❏ Baixe a configuração de conexão VPN para ajudar a configurar o outro lado.
    - ❏ Acesse sua tabela de roteamentos VPC e habilite a propagação de roteamento para que as rotas associadas à conexão VPN estejam disponíveis para sua rede VPC.
- ❏ Crie um recurso do Conector do AD para agir como proxy para seu AD local.
    - ❏ Selecione o Conector do AD como seu tipo de diretório.
    - ❏ Escolha o tamanho do diretório apropriado para o número de objetos que você precisa suportar.
    - ❏ Escolha sua VPC e duas sub-redes diferentes.
    - ❏ Insira as informações para o diretório local ao qual você se conectará.
        - ❏ Observe que é necessário ter uma conta de serviço. Os pré-requisitos são totalmente descritos nos links de documentação fornecidos abaixo.
- ❏ Crie um conjunto de Opções DHCP e associe à sua VPC para que as máquinas virtuais recebam os servidores DNS e o nome de domínio apropriados.
    - ❏ Forneça o nome de domínio do Active Directory e os servidores DNS. Outros parâmetros são opcionais.
    - ❏ Vá para sua VPC e associe às opções DHCP configuradas.
- ❏ Quando estiver configurando as instâncias EC2 da máquina virtual, use a opção de junção de Domínio para que a VM seja automaticamente conectada ao seu domínio do AD.