

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>.

© Intel Corporation. Intel, o logotipo Intel e outras marcas Intel são marcas registradas da Intel Corporation ou de suas subsidiárias.

*Outros nomes e marcas podem ser propriedade de outras empresas.

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

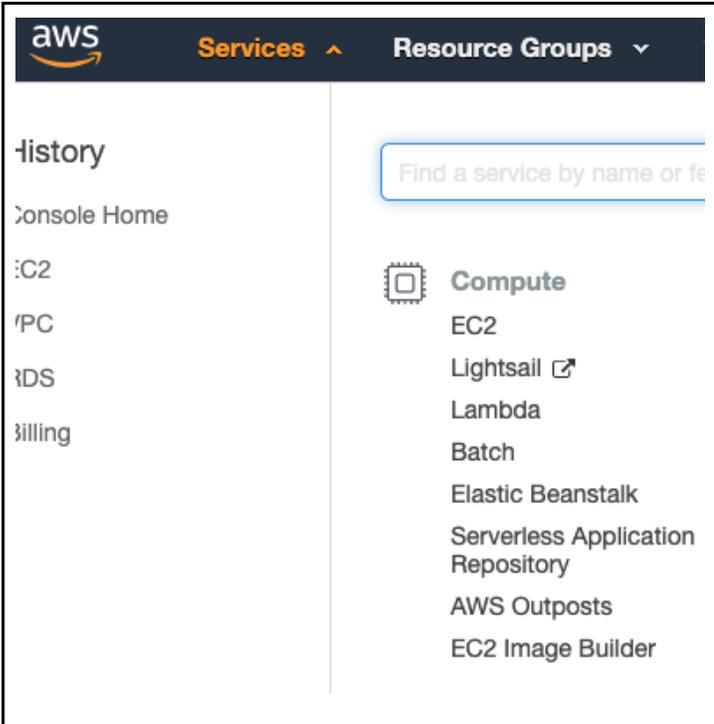
A computação em nuvem é o fornecimento sob demanda de recursos de TI na Internet com preços pré-pagos. Em vez de comprar e manter data centers e servidores físicos, você pode acessar serviços de tecnologia, como potência de computação, armazenamento e bancos de dados, de acordo com a necessidade a partir 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.

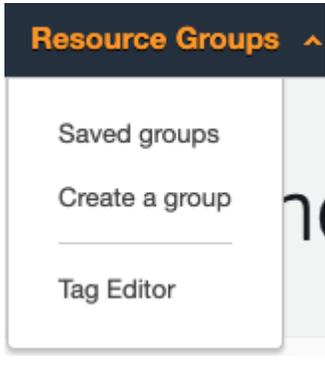
Com serviços totalmente gerenciados como o Amazon Relational Database Service, você pode apenas manter o foco em seus dados enquanto o provedor de nuvem gerencia todos os hardware e software subjacentes que fornecem o serviço. Com máquinas virtuais em execução na nuvem, você gerencia apenas o sistema 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

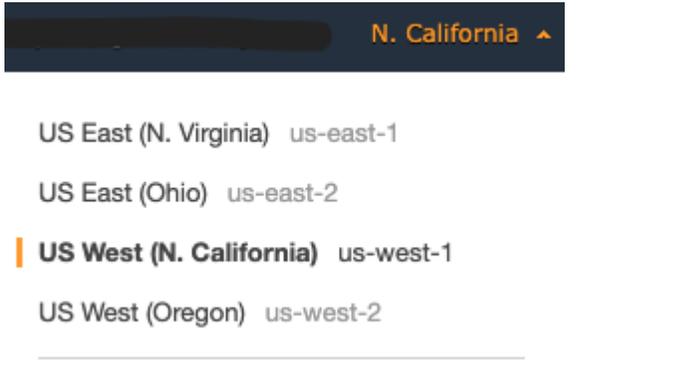
1.2.1 Serviços

| | |
|--|--|
|  | <p>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.</p> <p>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.</p> <p>Ao implantar serviços neste guia, forneceremos instruções que o direcionarão para esta tela para selecionar o serviço adequado.</p> |
|--|--|

1.2.2 Grupos de recursos

| | |
|---|---|
|  | <p>Ao lado de Services está o menu Resource Groups, no qual é possível criar ou visualizar os grupos de recursos que você criou.</p> <p>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.</p> |
|---|---|

1.2.3 Regiões

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

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

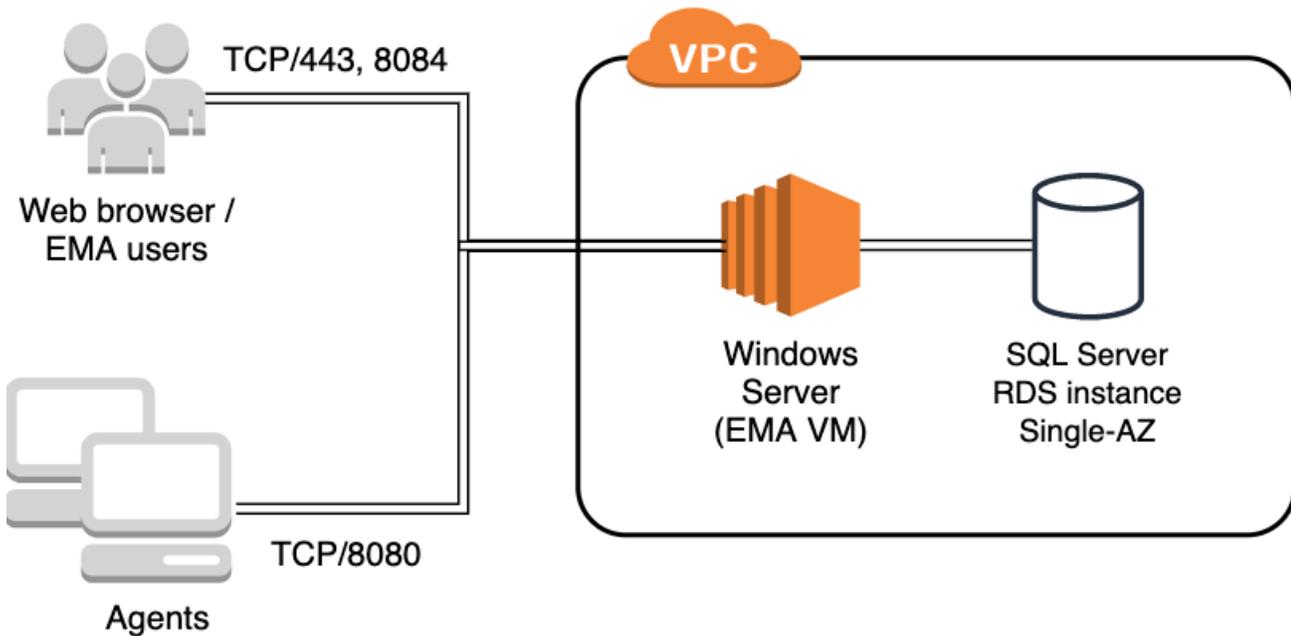
Se a sua organização já tem uma conta AWS, você deve pedir a um administrador de nuvem que lhe conceda acesso suficiente para poder criar todos os recursos listados neste guia.

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**.

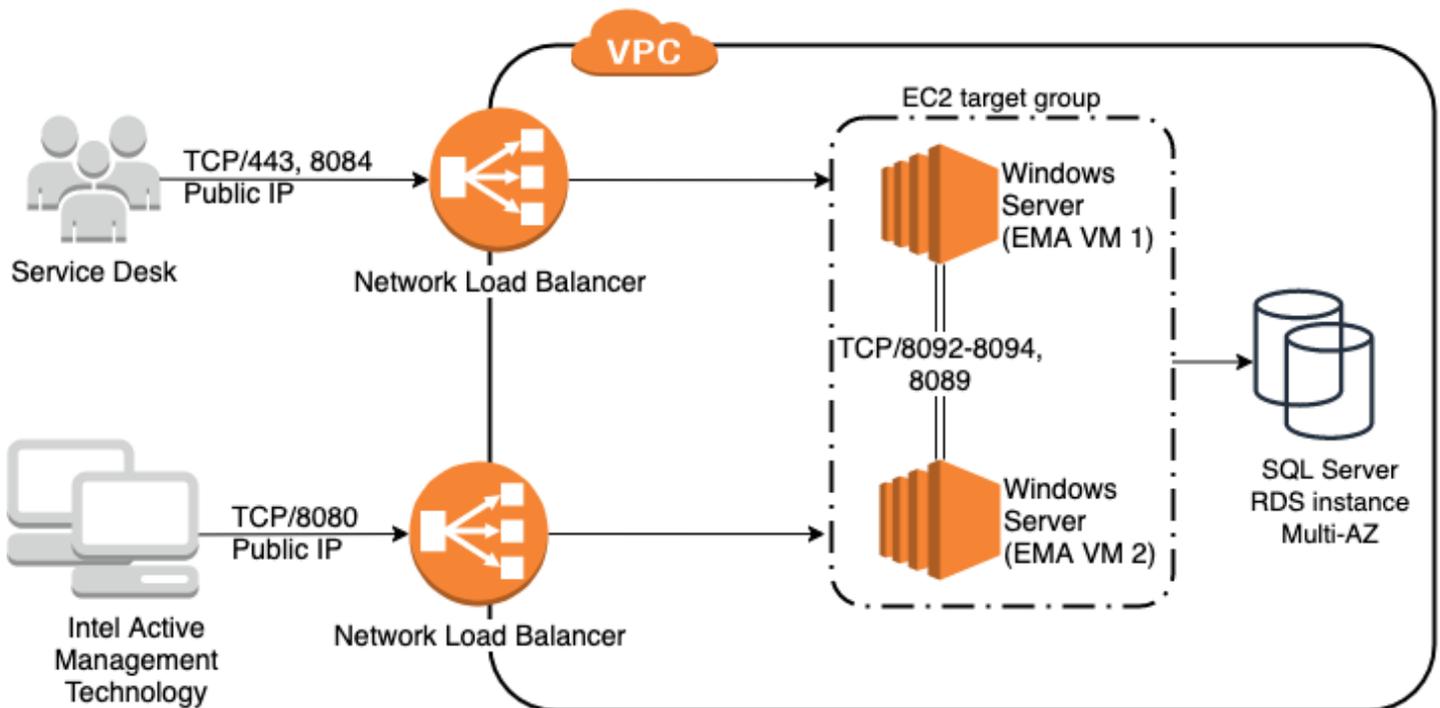
Consulte seu administrador de rede para saber se seria preferível usar um espaço de endereçamento específico. Se já tiver uma VPN estabelecida no provedor de nuvem, ou caso venha a ter futuramente, evite a sobreposição com sua rede corporativa para impedir problemas de roteamento. Você também precisa 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 Seleccione a região de implantação

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



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

US East (Ohio) us-east-2

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

US West (Oregon) us-west-2

4 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 Sessão 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>

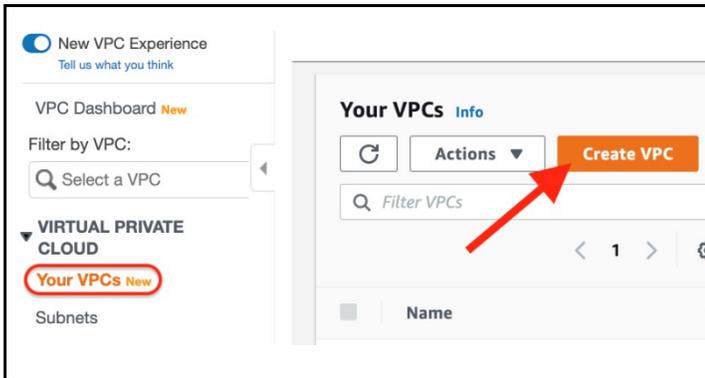
4.2 Crie uma VPC

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

| | |
|--|---|
|  <p>Networking & Content Delivery</p> <p>VPC</p> <p>CloudFront</p> | <p>No menu Services, em Network & Content Delivery, selecione VPC.</p> |
|--|---|

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

A screenshot of the 'Create VPC' configuration page. The page title is 'Create VPC' with an 'Info' link. Below the title is a description: 'A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.' The main section is 'VPC settings' and contains several fields: 'Name tag - optional' with a text input containing 'intel-ema-network'; 'IPv4 CIDR block' with a text input containing '10.250.0.0/24'; 'IPv6 CIDR block' with radio buttons for 'No IPv6 CIDR block' (selected) and 'Amazon-provided IPv6 CIDR block'; and 'Tenancy' with a dropdown menu set to 'Default'.

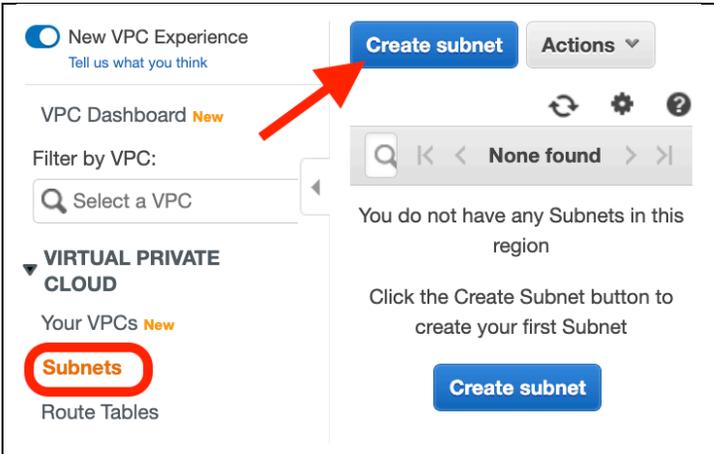
Insira os detalhes de rede conforme o seguinte

- **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



New VPC Experience
Tell us what you think

VP Dashboard **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs **New**

Subnets

Route Tables

Create subnet Actions

None found

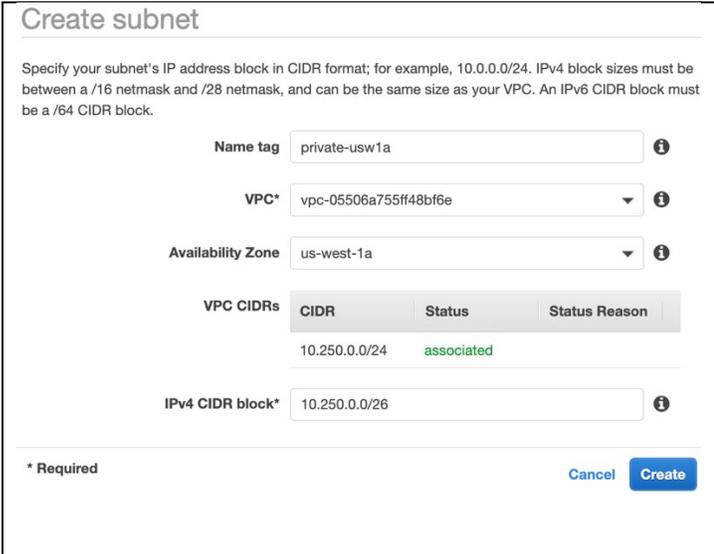
You do not have any Subnets in this region

Click the Create Subnet button to create your first Subnet

Create subnet

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

4.3.2 Crie a primeira sub-rede privada



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: private-usw1a

VPC*: vpc-05506a755ff48bf6e

Availability Zone: us-west-1a

| VPC CIDRs | CIDR | Status | Status Reason |
|-----------|---------------|------------|---------------|
| | 10.250.0.0/24 | associated | |

IPv4 CIDR block*: 10.250.0.0/26

* Required

Cancel Create

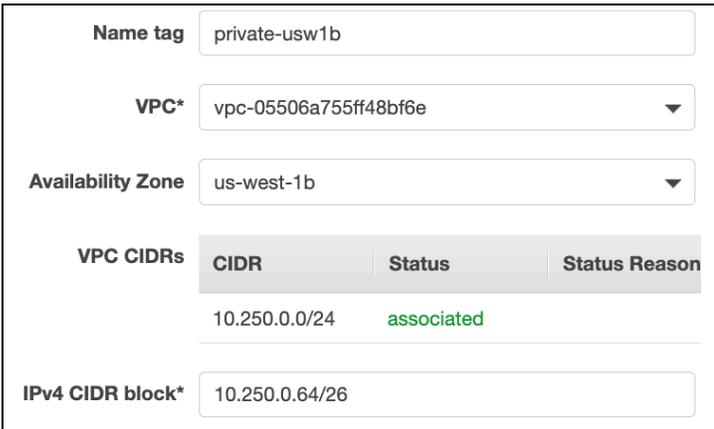
Clique no botão **Create subnet**.

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



Name tag: private-usw1b

VPC*: vpc-05506a755ff48bf6e

Availability Zone: us-west-1b

| VPC CIDRs | CIDR | Status | Status Reason |
|-----------|---------------|------------|---------------|
| | 10.250.0.0/24 | associated | |

IPv4 CIDR block*: 10.250.0.64/26

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

| <p>Name tag <input type="text" value="public-usw1a"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1a"/></p> <p>VPC CIDRs</p> <table border="1"> <thead> <tr> <th>CIDR</th> <th>Status</th> <th>Sta</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>associated</td> <td></td> </tr> </tbody> </table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.128/26"/></p> | CIDR | Status | Sta | 10.250.0.0/24 | associated | | <p>Clique no botão Create subnet.</p> <p>Configure a sub-rede como a seguir:</p> <ul style="list-style-type: none"> • Name tag: forneça um nome de sub-rede exclusivo. Exemplo: <i>public-usw1a</i> • 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: <i>us-west-1a</i> • IPv4 CIDR block: escolha um bloco IP não usado no espaço de endereço da sua VPC. Exemplo: <i>10.250.0.128/26</i> <p>Clique no botão Create.</p> |
|--|------------|--------|-----|---------------|------------|--|---|
| CIDR | Status | Sta | | | | | |
| 10.250.0.0/24 | associated | | | | | | |

4.3.5 Crie a segunda sub-rede pública

| <p>Name tag <input type="text" value="public-usw1b"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> <p>Availability Zone <input type="text" value="us-west-1b"/></p> <p>VPC CIDRs</p> <table border="1"> <thead> <tr> <th>CIDR</th> <th>Status</th> <th>Sta</th> </tr> </thead> <tbody> <tr> <td>10.250.0.0/24</td> <td>associated</td> <td></td> </tr> </tbody> </table> <p>IPv4 CIDR block* <input type="text" value="10.250.0.192/26"/></p> | CIDR | Status | Sta | 10.250.0.0/24 | associated | | <p>Clique no botão Create subnet.</p> <p>Configure a sub-rede como a seguir:</p> <ul style="list-style-type: none"> • Name tag: forneça um nome de sub-rede exclusivo. Exemplo: <i>public-usw1b</i> • 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: <i>us-west-1b</i> • IPv4 CIDR block: escolha um bloco IP não usado no espaço de endereço da sua VPC. Exemplo: <i>10.250.0.196/26</i> <p>Clique no botão Create.</p> |
|--|------------|--------|-----|---------------|------------|--|--|
| CIDR | Status | Sta | | | | | |
| 10.250.0.0/24 | associated | | | | | | |

4.3.6 Analise suas sub-redes

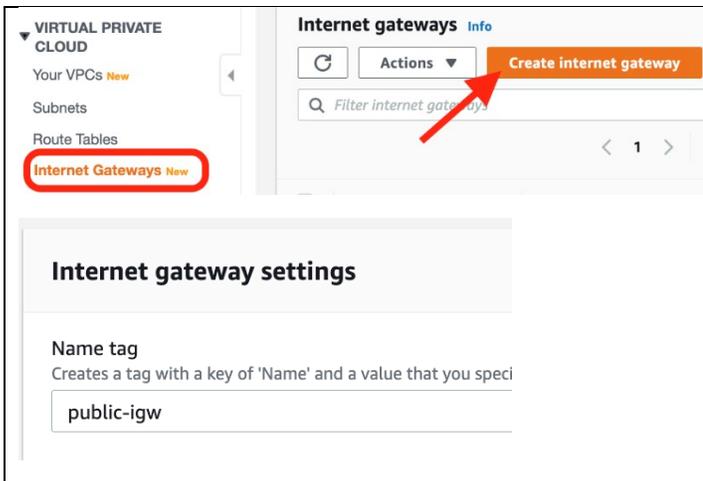
| <input type="checkbox"/> | Name | Subnet ID | State | VPC | IPv4 CIDR |
|--------------------------|---------------|------------------|-----------|-------------|------------------|
| <input type="checkbox"/> | private-usw1a | subnet-0850a... | available | vpc-0550... | 10.250.0.0/26 |
| <input type="checkbox"/>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

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



The screenshot shows the AWS Management Console interface for 'Internet gateways'. On the left sidebar, 'Internet Gateways' is selected and highlighted with a red circle. In the main content area, the 'Create internet gateway' button is highlighted with a red arrow. Below this, the 'Internet gateway settings' section is visible, with the 'Name tag' field containing the text 'public-igw'.

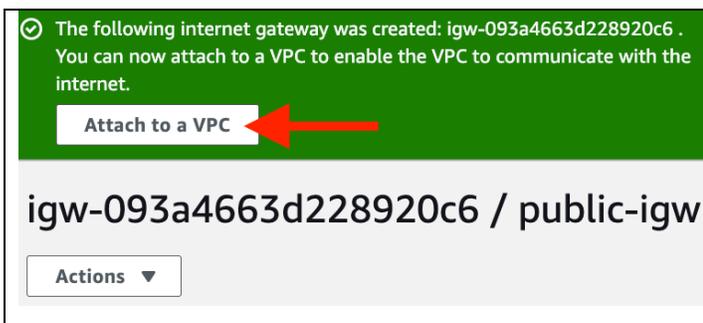
Na barra lateral da VPC, selecione Internet Gateways.

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



The screenshot shows a green confirmation banner with a checkmark icon. The text reads: 'The following internet gateway was created: igw-093a4663d228920c6. You can now attach to a VPC to enable the VPC to communicate with the internet.' Below the banner, the gateway ID 'igw-093a4663d228920c6 / public-igw' is displayed, and the 'Attach to a VPC' button is highlighted with a red arrow.

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

Attach to VPC (igw-05adc82a6f3c7c0e0) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

▶ **AWS Command Line Interface command**

Cancel **Attach internet gateway**

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

VIRTUAL PRIVATE CLOUD

- Your VPCs New
- Subnets
- Route Tables
- Internet Gateways New
- Egress Only Internet Gateways New
- DHCP Options Sets New
- Elastic IPs New
- Managed Prefix Lists New
- Endpoints
- Endpoint Services
- NAT Gateways New**
- Peering Connections

NAT gateways Info

Create NAT gateway

< 1 > ⚙

| Name | NAT gateway ID |
|------|----------------|
|------|----------------|

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

4.5.2 Crie o primeiro gateway NAT

Create NAT gateway [Info](#)

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

NAT gateway settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet

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

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

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

Create NAT gateway Info

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

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

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

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

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

New VPC Experience
Tell us what you think

VPC Dashboard New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs New

Subnets

Route Tables

Actions ▾

| | Name | Route Ta |
|--------------------------|------|-----------|
| <input type="checkbox"/> | | rtb-01705 |

4.6.2 Crie uma tabela de roteamento para sub-redes públicas

| | |
|--|---|
| <h3>Create route table</h3> <p>A route table specifies how packets are forwarded between the subnet your VPN connection.</p> <p>Name tag <input type="text" value="public-usw-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> | <p>Clique no botão Create route table.</p> <p>Configure a tabela de roteamento como a seguir:</p> <ul style="list-style-type: none">• Name tag: insira um nome exclusivo para a tabela de roteamento. Exemplo: <i>public-usw-routes</i>• VPC: selecione a rede virtual que você criou anteriormente. <p>Clique no botão Create.</p> <p>Clique no botão Close.</p> |
|--|---|

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

| | |
|--|--|
| <p>Name tag <input type="text" value="private-usw1a-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> | <p>Clique no botão Create route table.</p> <p>Configure a tabela de roteamento como a seguir:</p> <ul style="list-style-type: none">• Name tag: insira um nome exclusivo para a tabela de roteamento. Exemplo: <i>private-usw1a-routes</i>• VPC: selecione a rede virtual que você criou anteriormente. <p>Clique no botão Create.</p> <p>Clique no botão Close.</p> |
|--|--|

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

| | |
|--|--|
| <p>Name tag <input type="text" value="private-usw1b-routes"/></p> <p>VPC* <input type="text" value="vpc-05506a755ff48bf6e"/></p> | <p>Clique no botão Create route table.</p> <p>Configure a tabela de roteamento como a seguir:</p> <ul style="list-style-type: none">• Name tag: insira um nome exclusivo para a tabela de roteamento. Exemplo: <i>private-usw1b-routes</i>• VPC: selecione a rede virtual que você criou anteriormente. <p>Clique no botão Create.</p> <p>Clique no botão Close.</p> |
|--|--|

4.6.5 Analise a lista de tabelas de roteamento

| <input type="checkbox"/> | Name | Route Table ID |
|-------------------------------------|----------------------|-----------------------|
| <input type="checkbox"/> | | rtb-01705bd4b29e283ee |
| <input checked="" type="checkbox"/> | private-usw1a-routes | rtb-034336669e17ced15 |
| <input type="checkbox"/> | private-usw1b-routes | rtb-02a96e86856fc5cc0 |
| <input type="checkbox"/> | public-usw-routes | rtb-055fb6f346f460d0a |

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

| <input type="checkbox"/> | Name | Route Table ID |
|-------------------------------------|----------------------|-----------------------|
| <input type="checkbox"/> | | rtb-01705bd4b29e283ee |
| <input checked="" type="checkbox"/> | private-usw1a-routes | rtb-034336669e17ced15 |
| <input type="checkbox"/> | private-usw1b-routes | rtb-02a96e86856fc5cc0 |
| <input type="checkbox"/> | public-usw-routes | rtb-055fb6f346f460d0a |

Route Table: rtb-034336669e17ced15

Summary **Routes** Subnet Associations

Edit routes

View All routes

| Destination | Target |
|---------------|--------|
| 10.250.0.0/24 | local |

Edit routes

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

Add route

nat-002ed77f6a9ef0841 usw1a-nat-gw

* Required Cancel Save routes

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

Route Table: rtb-034336669e17ced15

Summary Routes **Subnet Associations**

Edit subnet associations

None found

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

Edit subnet associations

Route table rtb-034336669e17ced15 (private-usw1a-routes)

Associated subnets subnet-0850a0c96d7a404da

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

* Required Cancel Save

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

Summary **Routes** Subnet Associations

Edit routes

View All routes

| Destination | Target |
|---------------|--------|
| 10.250.0.0/24 | local |

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**.

Edit routes

| Destination | Target | Status |
|---------------|-----------------------|--------|
| 10.250.0.0/24 | local | active |
| 0.0.0.0/0 | nat-06c46b8e4e4ed5c32 | |

Add route

*** Required** Cancel Save routes

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

Summary **Routes** Subnet Associations

Edit routes

View All routes

| Destination | Target |
|---------------|--------|
| 10.250.0.0/24 | local |

Edit routes

| Destination | Target | Status |
|---------------|--------|--------|
| 10.250.0.0/24 | local | active |

Add route

Destination: 0.0.0.0/0 Target: igw-093a4663d228920c6

igw-093a4663d228920c6 public-igw

* Required Cancel Save routes

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

Summary Routes **Subnet Associations**

Edit subnet associations

Subnet ID IPv4 CIDR

You do not have any subnet associations.

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

Associated subnets subnet-07aff7a001005ed34 subnet-0110cd4da4ec72e62

Filter by attributes or search by keyword

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

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.

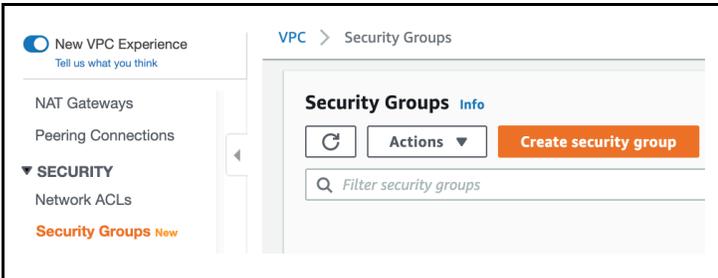
Para obter mais informações sobre grupos de segurança da VPC, acesse link a seguir:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

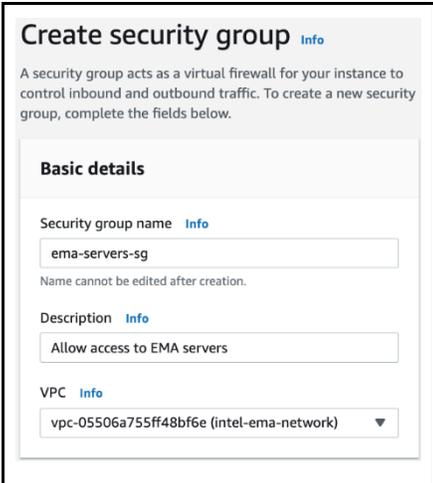
4.7.1 Crie um grupo de segurança para a(s) VM(s)

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

| | |
|---|---|
|  | <p>Na barra lateral de seção VPC, selecione Security Groups.</p> <p>Clique no botão Create security group.</p> |
|---|---|

4.7.1.2 Configurar informações básicas do grupo de segurança

| | |
|--|---|
|  | <p>Insira as informações básicas para o grupo de segurança que permitirá acesso ao servidor EMA.</p> <ul style="list-style-type: none">• Security group name: insira um nome exclusivo. Exemplo: <i>ema-server-sg</i>• Description (opcional): insira uma descrição para o grupo de segurança. Exemplo: <i>Allow access to EMA servers</i>• VPC: selecione a VPC que você criou anteriormente. |
|--|---|

4.7.1.3 Adicione uma regra de entrada para tráfego da Web

Inbound rules Info

Inbound rule 1 Delete

Type Info Protocol Info Port range Info

HTTPS TCP 443

Source type Info Source Info Description - optional Info

Custom Q trusted networks for web

10.250.0.0/24 X

[Redacted] /32 X

Add rule

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

Inbound rule 2 Delete

Type Info Protocol Info Port range Info

Custom TCP 8084

Source type Info Source Info Description - optional Info

Custom Q trusted networks for websocket

10.250.0.0/24 X

[Redacted] /32 X

Add rule

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

Type Info Protocol Info Port range Info

Custom TCP 8080

Source type Info Source Info Description - optional Info

Custom Q EMA agent traffic

0.0.0.0/0 X

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

Details

Security group name: ema-servers-sg
Security group ID: sg-06acbdce6cea22f15

Description: Allow access to EMA servers
VPC ID: vpc-001161d1e7e50afb2

Owner: 312506926764
Inbound rules count: 4
Permission entries: 4

Outbound rules count: 1
Permission entry: 1

Inbound rules | Outbound rules | Tags

| Type | Protocol | Port range | Source | Description - optional |
|------------|----------|------------|-------------|----------------------------------|
| Custom TCP | TCP | 8084 | ████████/32 | Trusted network(s) for websocket |
| Custom TCP | TCP | 8080 | 0.0.0.0/0 | EMA agent traffic |
| RDP | TCP | 3389 | ████████/32 | Trusted network(s) for RDP |
| HTTPS | TCP | 443 | ████████/32 | Trusted network(s) for web |

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

Type: Custom TCP
Protocol: TCP
Port range: 8092 - 8094
Source type: Custom
Source: sg-06acbdce6cea22f15
Description - optional: EMA internal

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

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

Custom TCP TCP 8089

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

Custom Q EMA admin port

sg-06acbdce6cea22f15

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 | ██████████/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 | ██████████/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

New VPC Experience
Tell us what you think

NAT Gateways
Peering Connections

▼ SECURITY
Network ACLs
Security Groups **New**

VPC > Security Groups

Security Groups [Info](#)

Actions **Create security group**

Filter security groups

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

Create security group Info

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

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

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

Inbound rules Info

Inbound rule 1

Type Info

Source type Info

Security Groups

- sg-03661abff0a38ee50
- ema-server-sg | sg-03661abff0a38ee50

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.

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

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>

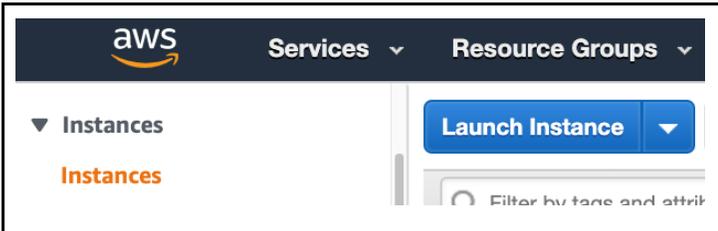
5.2 Criar máquina(s) virtual(is)

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

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

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

Q Windows Server | Search by Systems Manager parameter

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

Quick Start (19) 1 to 19 of 19 AMIs

- My AMIs (0)
- AWS Marketplace (393)
- Community AMIs (2144)

Windows
Free tier eligible

Microsoft Windows Server 2019 Base - ami-0d1b8b740ddc3b78d **Select**

Microsoft Windows 2019 Datacenter edition. [English] 64-bit (x86)

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

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

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

Step 2: Choose an Instance Type

Filter by: **General purpose** **Current generation** [Show/Hide](#)

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

| | Family | Type | vCPUs | Memory (GiB) |
|--------------------------|-----------------|--------------------------------|-------|--------------|
| <input type="checkbox"/> | General purpose | t2.nano | 1 | 0.5 |
| <input type="checkbox"/> | General purpose | t2.micro Free tier eligible | 1 | 1 |
| <input type="checkbox"/> | General purpose | t2.small | 1 | 2 |
| <input type="checkbox"/> | General purpose | t2.medium | 2 | 4 |
| <input type="checkbox"/> | General purpose | t2.large | 2 | 8 |

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

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

Step 3: Configure Instance Details

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

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

Number of instances [Launch into Auto Scal](#)

Purchasing option Request Spot instances

Network No default VPC found. [Create a new default VPC](#).

Subnet 59 IP Addresses available

Auto-assign Public IP

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

Step 4: Add Storage

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

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

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

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

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

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below.

Assign a security group: Create a new security group
 Select an existing security group

| Security Group ID | Name | Description |
|--|----------------|--|
| <input type="checkbox"/> sg-04c1e0cf58c3b592e | default | default VPC security group |
| <input type="checkbox"/> sg-017cfe786b8c9004a | ema-db-sg | Allow traffic from EMA server(s) to the database |
| <input checked="" type="checkbox"/> sg-06acbdce6cea22f15 | ema-servers-sg | Allow access to EMA servers |

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

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair ▼

Key pair name

ema-demo

Download Key Pair

... You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel **Launch Instances**

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)

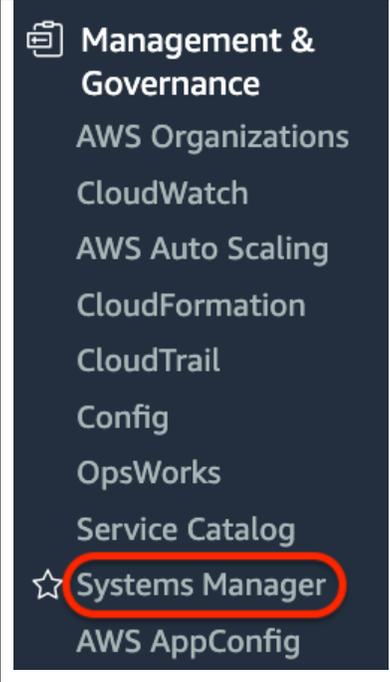
Para implantações de servidor distribuído, repita o procedimento anterior para criar o segundo servidor Intel EMA, selecionando uma sub-rede diferente e atribuindo uma tag de nome diferente, como *ema-server-2*.

6 Configure o AWS Systems Manager (apenas servidor distribuído)

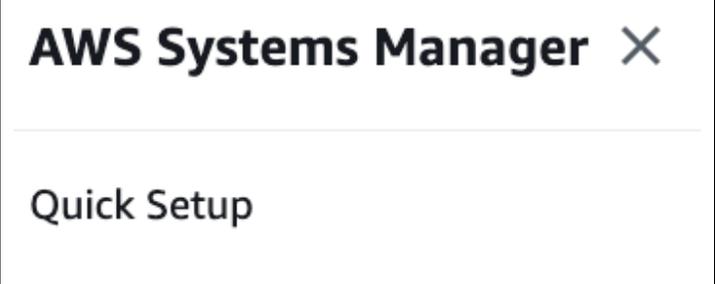
O AWS Systems Manager é um serviço que oferece maior visibilidade e controle de sua infraestrutura na AWS. Precisamos usar o componente do Session Manager que nos permitirá ter acesso remoto às VMs que não possuem um endereço de IP público.

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

6.1 Acesse o serviço do Systems Manager

| | |
|---|--|
|  <p>Management & Governance</p> <ul style="list-style-type: none">AWS OrganizationsCloudWatchAWS Auto ScalingCloudFormationCloudTrailConfigOpsWorksService Catalog★ Systems ManagerAWS AppConfig | <p>No menu Services na seção Management & Governance, selecione Systems Manager.</p> |
|---|--|

6.2 Inicie a configuração rápida

| | |
|---|--|
|  <p>AWS Systems Manager ✕</p> <hr/> <p>Quick Setup</p> | |
|---|--|

6.3 Escolha as opções de permissões

Quick Setup Info

Configure required security roles and commonly used Systems Manager capabilities.

Permissions (Required)

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

Instance profile role

Use the default role

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

Choose an existing role

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

Assume role for Systems Manager

Use the default role

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

Choose an existing role

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

6.4 Escolha as opções de configurações

Configuration options

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

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

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

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

6.5 Escolha os objetivos

Targets

Targets are the Amazon EC2 instances to manage with Systems Manager.

Target selection method

- Choose all instances in the current AWS account and Region
- Specify instance tags
- Choose instances manually

Cancel Enable

6.6 Verifique a lista de instâncias gerenciadas

AWS Systems Manager > Managed Instances

Managed Instances | Settings

Managed instances

View details Agent auto update Configure Inventory Actions

| Instance ID | Name | Ping status | Platform type | Platform name | Platform version | Agent version | IP address | Computer name | Association status |
|---|--------------|-------------|---------------|--|------------------|---------------|-------------|---------------------------|--------------------|
| <input type="radio"/> i-0a6a82fc33afa0cf7 | ema-server-2 | Online | Windows | Microsoft Windows Server 2019 Datacenter | 10.0.17763 | 3.0.222.0 | 10.250.0.82 | EC2AMAZ-PM4CVE0.WORKGROUP | Pending |
| <input type="radio"/> i-06364ced48ee5bb96 | ema-server-1 | Online | Windows | Microsoft Windows Server 2019 Datacenter | 10.0.17763 | 3.0.222.0 | 10.250.0.16 | EC2AMAZ-8BHE25G.WORKGROUP | Success |

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:

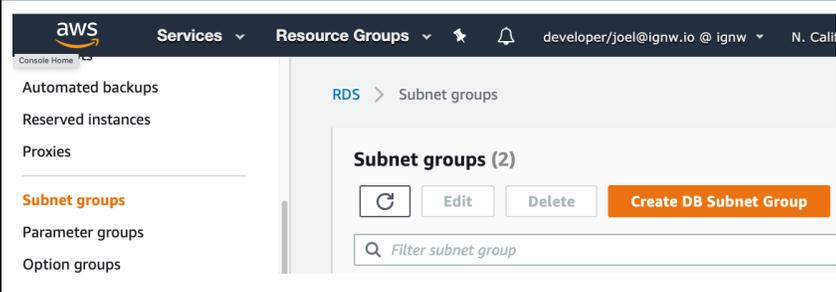
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

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

Create DB Subnet Group

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

Subnet group details

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

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

Description

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

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

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

Subnets selected (2)

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

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

Amazon RDS

Dashboard
Databases
Query Editor
Performance Insights

RDS > Databases

Databases

Group resources

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

| | |
|--|--|
| <p>Create database</p> <p>Choose a database creation method Info</p> <p><input checked="" type="radio"/> Standard Create You set all of the configuration options, including ones for availability, security, backups, and maintenance.</p> <p><input type="radio"/> Easy Create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.</p> | <p>Selecione o método de criação Standard Create.</p> |
|--|--|

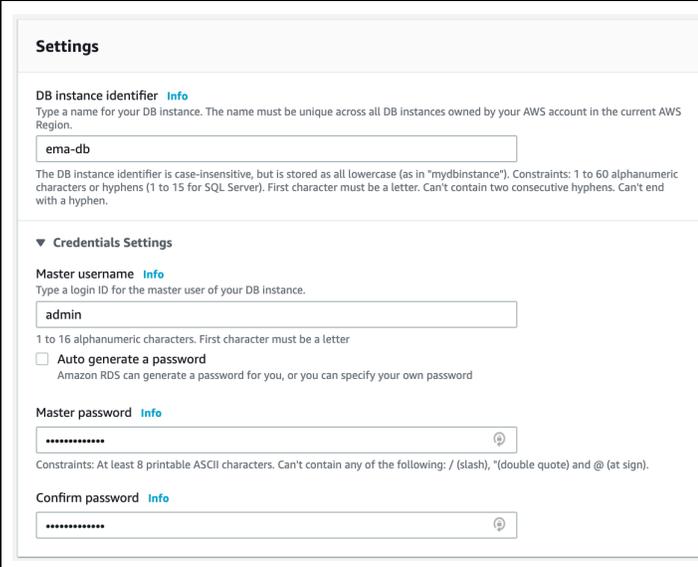
7.3.2 Escolha o tipo de mecanismo e edição

| | |
|---|--|
| <p>Engine options</p> <p>Engine type Info</p> <p><input type="radio"/> Amazon Aurora </p> <p><input type="radio"/> MySQL </p> <p><input type="radio"/> MariaDB </p> <p><input type="radio"/> PostgreSQL </p> <p><input type="radio"/> Oracle </p> <p><input checked="" type="radio"/> Microsoft SQL Server </p> <p>Edition</p> <p><input type="radio"/> SQL Server Express Edition Affordable database management system that supports database sizes up to 10 GB.</p> <p><input type="radio"/> SQL Server Web Edition In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.</p> <p><input checked="" type="radio"/> SQL Server Standard Edition Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.</p> <p><input type="radio"/> SQL Server Enterprise Edition Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.</p> <p>Version Info</p> <p>SQL Server 2017 14.00.3281.6.v1</p> <p>License license-included</p> | <p>Selecione o mecanismo do Microsoft SQL Server.</p> <p>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.</p> |
|---|--|

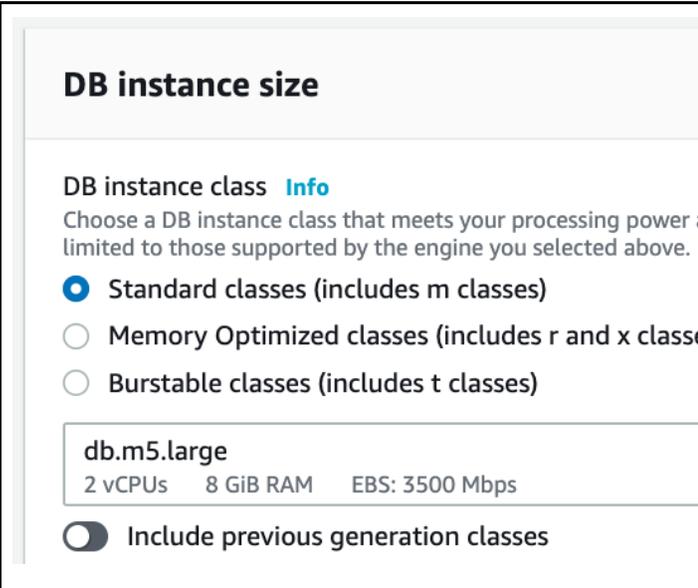
7.3.3 Escolha o modelo de implantação

| | |
|---|---|
| <p>Templates</p> <p>Choose a sample template to meet your use case.</p> <p><input checked="" type="radio"/> Production Use defaults for high availability and fast, consistent performance.</p> <p><input type="radio"/> Dev/Test This instance is intended for development use outside of a production environment.</p> | <p>Em Templates, selecione Production.</p> |
|---|---|

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

| | |
|--|--|
|  <p>The screenshot shows the 'Settings' section of the AWS RDS console. It includes the 'DB instance identifier' field with the value 'ema-db'. Below it, the 'Credentials Settings' section is expanded, showing the 'Master username' field with the value 'admin' and the 'Auto generate a password' checkbox checked. The 'Master password' and 'Confirm password' fields are also visible, both containing masked characters.</p> | <p>Atribua um nome exclusivo ao banco de dados. Exemplo: <i>ema-db</i></p> <p>Crie um nome de usuário e uma senha.</p> |
|--|--|

7.3.5 Configure o tamanho da instância de banco de dados

| | |
|--|--|
|  <p>The screenshot shows the 'DB instance size' configuration page. It features a section for 'DB instance class' with three radio button options: 'Standard classes (includes m classes)', 'Memory Optimized classes (includes r and x classes)', and 'Burstable classes (includes t classes)'. The 'Standard classes' option is selected. Below the options, the instance class 'db.m5.large' is displayed, along with its specifications: '2 vCPUs', '8 GiB RAM', and 'EBS: 3500 Mbps'. At the bottom, there is a checkbox for 'Include previous generation classes' which is currently unchecked.</p> | <p>Configure a classe da instância de banco de dados para oferecer os recursos adequados. Sugerido: <i>db.m5.large</i></p> |
|--|--|

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

| | |
|--|---|
| <p>Connectivity</p> <p>Virtual private cloud (VPC) Info VPC that defines the virtual networking environment for this DB instance.</p> <p>intel-ema (vpc-001161d1e7e50afb2) ▼</p> <p>Only VPCs with a corresponding DB subnet group are listed.</p> <p>ⓘ After a database is created, you can't change the VPC selection.</p> <p>► Additional connectivity configuration</p> | <p>Em Connectivity, selecione a VPC que você criou anteriormente e expanda a seção Additional connectivity configuration.</p> |
|--|---|

7.3.8 Configure a conectividade — Configuração adicional da conectividade

| | |
|---|---|
| <p>▼ Additional connectivity configuration</p> <p>Subnet group Info DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.</p> <p>ema-db-subnet-group ▼</p> <p>Publicly accessible Info</p> <p><input type="radio"/> Yes Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.</p> <p><input checked="" type="radio"/> No RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.</p> <p>VPC security group Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)</p> <p><input checked="" type="radio"/> Choose existing Choose existing VPC security groups</p> <p><input type="radio"/> Create new Create new VPC security group</p> <p>Existing VPC security groups</p> <p>Choose VPC security groups ▼</p> <p>ema-db-sg ✕</p> <p>Availability Zone Info</p> <p>No preference ▼</p> <p>Database port Info TCP/IP port that the database will use for application connections.</p> <p>1433</p> | <p>Escolha o grupo de sub-redes de dados que você criou anteriormente.</p> <p>Desmarque o grupo de segurança padrão da VPC e escolha o grupo de segurança existente criado anteriormente para o banco de dados.</p> |
|---|---|

7.3.9 Analise e crie

| | | | | | | | | | |
|---|-------------------|------------|---------|----------|------------------|------------|--------------|-------------------|---|
| <p>Estimated monthly costs</p> <table><tr><td>DB instance</td><td>735.11 USD</td></tr><tr><td>Storage</td><td>2.76 USD</td></tr><tr><td>Provisioned IOPS</td><td>110.00 USD</td></tr><tr><td>Total</td><td>847.87 USD</td></tr></table> <p>This billing estimate is based on on-demand usage as described in Amazon RDS Pricing. Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.</p> <p>Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.</p> <p><small>You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.</small></p> <p>Cancel Create database</p> | DB instance | 735.11 USD | Storage | 2.76 USD | Provisioned IOPS | 110.00 USD | Total | 847.87 USD | <p>Analise o custo estimado e clique no botão Create database.</p> |
| DB instance | 735.11 USD | | | | | | | | |
| Storage | 2.76 USD | | | | | | | | |
| Provisioned IOPS | 110.00 USD | | | | | | | | |
| Total | 847.87 USD | | | | | | | | |

7.4 Obtenha o nome de host do banco de dados

| | |
|---|---|
| <p>Connectivity & security Monitoring</p> <hr/> <p>Connectivity & security</p> <p>Endpoint & port</p> <p>Endpoint</p> <p>ema-db.creq7zxsavq4.us-west-1.rds.amazonaws.com</p> <p>Port</p> <p>1433</p> | <p>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.</p> |
|---|---|

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 instâncias 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.

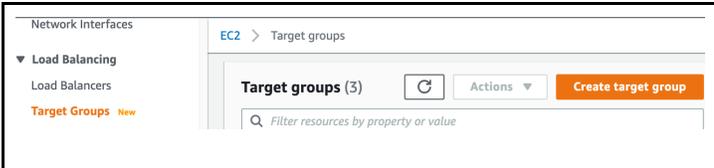
Há outras possibilidades de configuração do balanceamento de carga que não foram abordadas neste documento. Consulte seu departamento de TI referente a quaisquer requisitos ou práticas que possa querer implementar. Para obter mais informações sobre o balanceamento de carga na AWS, acesse o seguinte link:

<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

| | |
|--|---|
|  | <p>Na barra lateral da EC2, em Load Balancing, selecione Target Groups.</p> <p>Clique no botão Create target group.</p> |
|--|---|

8.2.2 Configure um grupo de destino para TCP/443

| | |
|--|--|
| <p>Target group name</p> <input type="text" value="ema-web"/> <p>Up to 32 alphanumeric characters, including</p> <p>Protocol : Port</p> <p>TCP ▼ : 443</p> <p>VPC</p> <p>Select the VPC containing the instances you</p> <input type="text" value="intel-ema-network"/> <p>vpc-05506a755ff48bf6e IPv4: 10.250.0.0/24</p> <p>Health checks</p> <p>The associated load balanc</p> <p>Health check protocol</p> <p>TCP ▼</p> | <p>Configure o grupo de destino como segue:</p> <ul style="list-style-type: none">• Target type: <i>Instances</i>• Target group name: insira um nome exclusivo. Exemplo: <i>ema-web</i>• Protocol: <i>TCP</i>• Port: <i>443</i>• VPC: selecione a VPC que você criou anteriormente.• Health check protocol: <i>TCP</i> <p>Clique em Next para avançar para a tela Register targets.</p> |
|--|--|

8.2.2.1 Registre ambas as instancias EC2 como destinos

Register targets

Step 2 of 2

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

Available instances (2)

Filter resources by property or value

| <input type="checkbox"/> | Instance ID | Name | State | Security groups | Zone | Subnet ID |
|--------------------------|---------------------|--------------|---------|-----------------|------------|----------------|
| <input type="checkbox"/> | i-00f8db1dd6650c6c8 | ema-server-1 | running | ema-servers-sg | us-west-1a | subnet-080e857 |
| <input type="checkbox"/> | i-0f180ebc233227eda | ema-server-2 | running | ema-servers-sg | us-west-1c | subnet-0a16634 |

0 selected

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

443

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Targets (2)

Remove all pending

All

Filter resources by property or value

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

2 pending

Cancel Previous **Create target group**

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.

Target groups (3)



Ac

Q Filter resources by property or value

| <input type="checkbox"/> | Name ▲ | ARN | Port ▼ | Protocol |
|--------------------------|---------------|------------------------|--------|----------|
| <input type="checkbox"/> | ema-swarm | arn:aws:elasticload... | 8080 | TCP |
| <input type="checkbox"/> | ema-web | arn:aws:elasticload... | 443 | TCP |
| <input type="checkbox"/> | ema-websocket | arn:aws:elasticload... | 8084 | TCP |

8.2.6 Habilite Stickiness para o grupo de destino TCP/443

8.2.6.1 Detalhes do grupo de destino

Attributes

Stickiness
Disabled

Deregistration delay
300 seconds

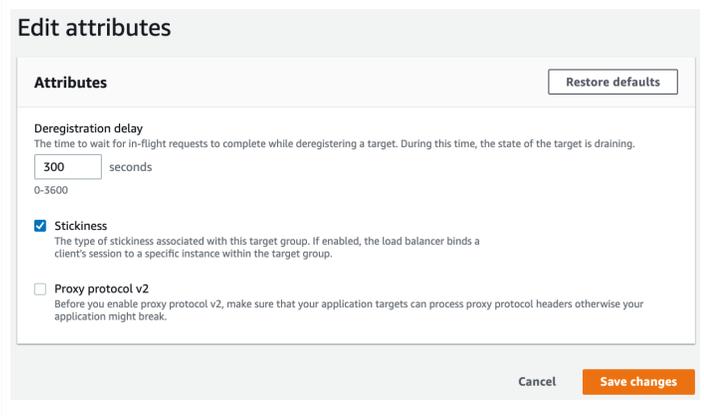
Slow start duration
0 seconds

Load balancing algorithm
Round robin

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

| | |
|--|---|
|  | <p>Habilite a bandeira Stickiness.</p> <p>Clique no botão Save changes.</p> |
|--|---|

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).

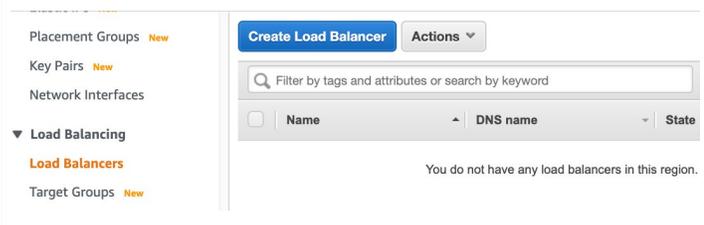
8.2.8 Nota sobre o monitoramento da integridade do grupo de destino

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.

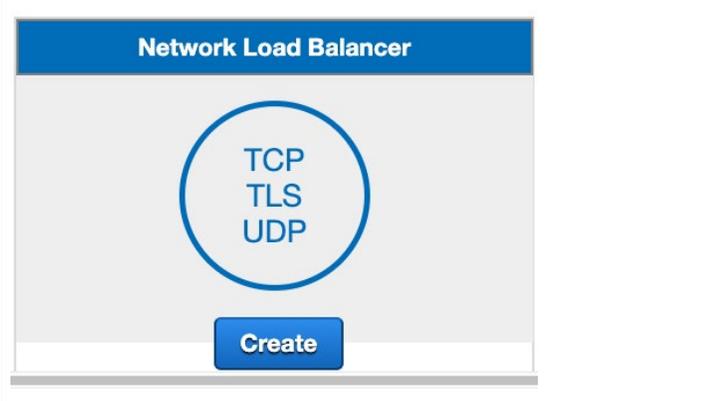
8.3 Criar um balanceador de carga de rede para receber tráfego da Internet

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

| | |
|--|---|
|  | <p>Na barra lateral da EC2, em Load Balancing, selecione Load Balancers e clique em Create Load Balancer.</p> |
|--|---|

8.3.2 Escolha o tipo de balanceador de carga

| | |
|--|---|
|  | <p>Clique no botão Create e no título Select Network Load Balancer.</p> |
|--|---|

8.3.3 Configure o balanceador de carga

8.3.3.1 Configuração básica

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

Step 1: Configure Load Balancer

Basic Configuration

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

Name ⓘ

Scheme ⓘ internet-facing internal

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

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

| Load Balancer Protocol | Load Balancer Port | |
|------------------------|--------------------|---|
| TCP | 443 | ✕ |
| TCP | 8084 | ✕ |

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

- TCP 443
- TCP 8084

8.3.3.3 Zonas de disponibilidade

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.

[Create and manage Elastic IPs in the VPC console](#)

VPC ⓘ vpc-05506a755ff48bf6e (10.250.0.0/24) | intel-ema-network

Availability Zones

us-west-1a subnet-07aff7a001005ed34 (public-usw1a)

us-west-1b subnet-0110cd4da4ec72e62 (public-usw1b)

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

Step 3: Configure Routing

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

Target group

Target group ⓘ Existing target group

Name ⓘ ema-web

Target type Instance IP

Protocol ⓘ TCP

Port ⓘ 443

Health checks

Protocol ⓘ TCP

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

Step 4: Register Targets

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

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

Registered targets

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

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

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

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**.

Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer [Edit](#)

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

▼ Routing [Edit](#)

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

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

8.3.4 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

ema-web-balancer

ema-web-balancer-9faa96fc... provisioning vpc-05506a755ff4E

Load balancer: ema-web-balancer

Description **Listeners** Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

Add listener Edit Delete

| Listener ID | Security policy | SSL Certificate | ALPN policies | Default action |
|--|-----------------|-----------------|---------------|--------------------|
| TCP : 443 arn...d7449b4094cd34d1 | N/A | N/A | N/A | Forward to ema-web |
| <input checked="" type="checkbox"/> TCP : 8084 arn...40417262f99b8abc | N/A | N/A | N/A | Forward to ema-web |

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

Listeners ema-web-balancer | TCP:8084

View/edit listener. Each listener must include one action of type forward. Update

ema-web-balancer | **TCP : 8084**

Listeners belonging to Network Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. [Learn more](#)

ARN
arn:aws:elasticloadbalancing:us-west-1:802420695018:listener/net/ema-web-balancer/9faa96fc630182c2/40417262f99b8abc

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen to for traffic.
TCP : 8084

Default action(s)
Indicate how this listener will route traffic

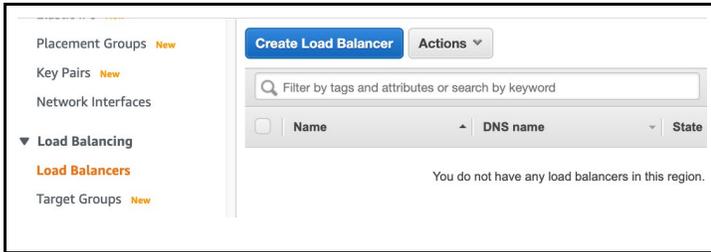
1. Forward to...
ema-websocket

Mude a ação padrão para encaminhar para o ouvinte websocket.

Clique no botão **Update**.

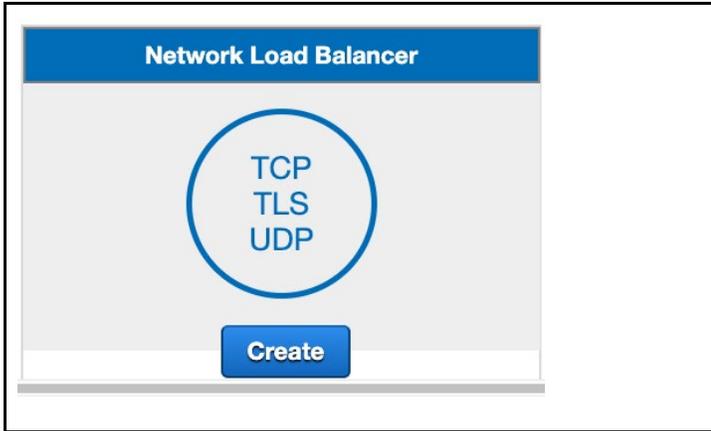
8.4 Criar um balanceador de carga de rede para tráfego swarm

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**.

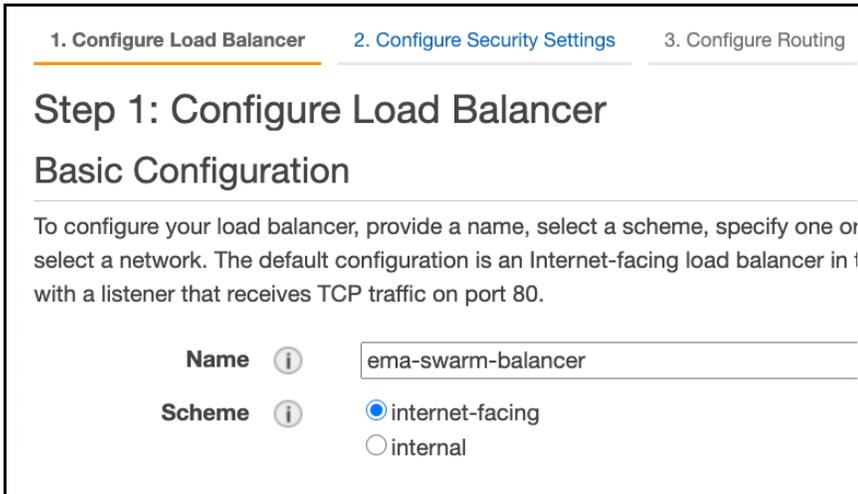
8.4.2 Escolha o tipo de balanceador de carga



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

| <h4>Listeners</h4> <p>A listener is a process that checks for connection requests, using the protocol and port configured.</p> <table border="1"><thead><tr><th>Load Balancer Protocol</th><th>Load Balancer Port</th></tr></thead><tbody><tr><td>TCP</td><td>8080</td></tr></tbody></table> | Load Balancer Protocol | Load Balancer Port | TCP | 8080 | <p>Na seção Listeners, adicione ouvintes para esses protocolos e portas.</p> <ul style="list-style-type: none">• <i>TCP 8080</i> |
|--|------------------------|--------------------|-----|------|---|
| Load Balancer Protocol | Load Balancer Port | | | | |
| TCP | 8080 | | | | |

8.4.3.3 Zonas de disponibilidade

| | |
|---|--|
| <h4>Availability Zones</h4> <p>Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.</p> <p>Create and manage Elastic IPs in the VPC console</p> <p>VPC: vpc-05506a755ff48bf6e (10.250.0.0/24) intel-ema-network</p> <p>Availability Zones</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> us-west-1a subnet-07aff7a001005ed34 (public-usw1a) IPv4 address: Assigned by AWS<input checked="" type="checkbox"/> us-west-1b subnet-0110cd4da4ec72e62 (public-usw1b) IPv4 address: Assigned by AWS | <p>Configure a seção Availability Zones da seguinte forma:</p> <ul style="list-style-type: none">• 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 <i>Assigned by AWS</i>. <p>Clique no botão Next: Configure Security Settings.</p> |
|---|--|

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

| | |
|---|--|
| <p>1. Configure Load Balancer 2. Configure Security Settings 3. Configure Routing</p> <h4>Step 3: Configure Routing</h4> <p>Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.</p> <h4>Target group</h4> <p>Target group: Existing target group</p> <p>Name: ema-swarm</p> <p>Target type: Instance (selected), IP</p> <p>Protocol: TCP</p> <p>Port: 8080</p> <h4>Health checks</h4> <p>Protocol: TCP</p> <p>Cancel Previous Next: Register Targets</p> | <p>Na Step 3: Configure Routing, configure o grupo de destino da seguinte forma.</p> <ul style="list-style-type: none">• Target group: <i>Existing target group</i>• Name: selecione o nome do grupo de destino TCP/8080 que você criou anteriormente. Exemplo: <i>ema-swarm</i> <p>Clique no botão Next: Register Targets.</p> |
|---|--|

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**.

[1. Configure Load Balancer](#) [2. Configure Security Settings](#) [3. Configure Routing](#)

Step 5: Review

Please review the load balancer details before continuing

▼ Load balancer

[Edit](#)

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

▼ Routing

[Edit](#)

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

[Cancel](#)

[Previous](#)

[Create](#)

8.4.4 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.

| <input type="checkbox"/> | Name | DNS name | State |
|-------------------------------------|--------------------|------------------------------|--------|
| <input type="checkbox"/> | ema-swarm-balancer | ema-swarm-balancer-2dd41f... | active |
| <input checked="" type="checkbox"/> | 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/err 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/>

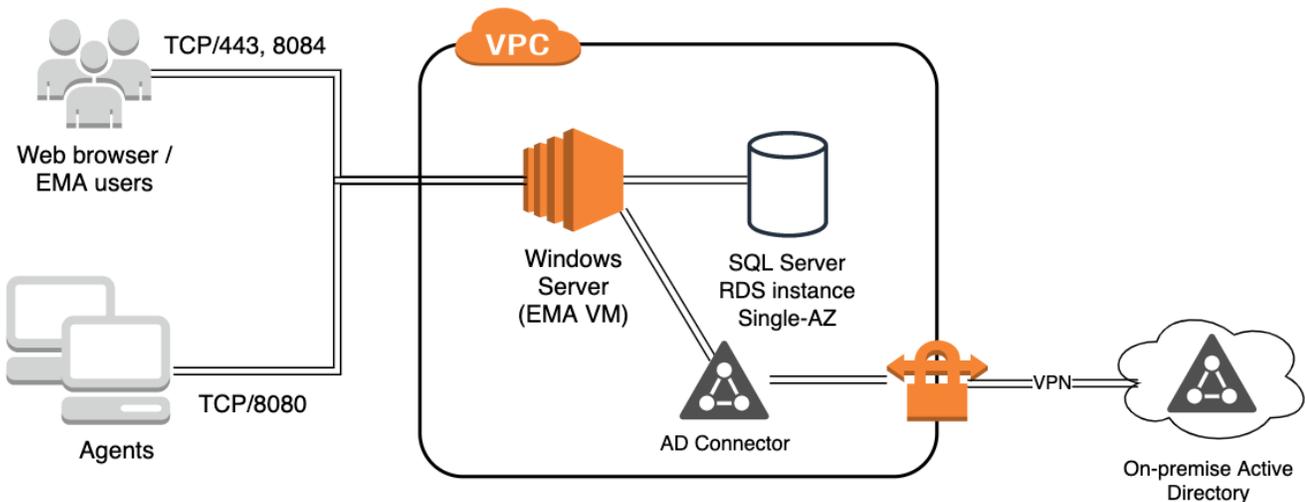
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.html

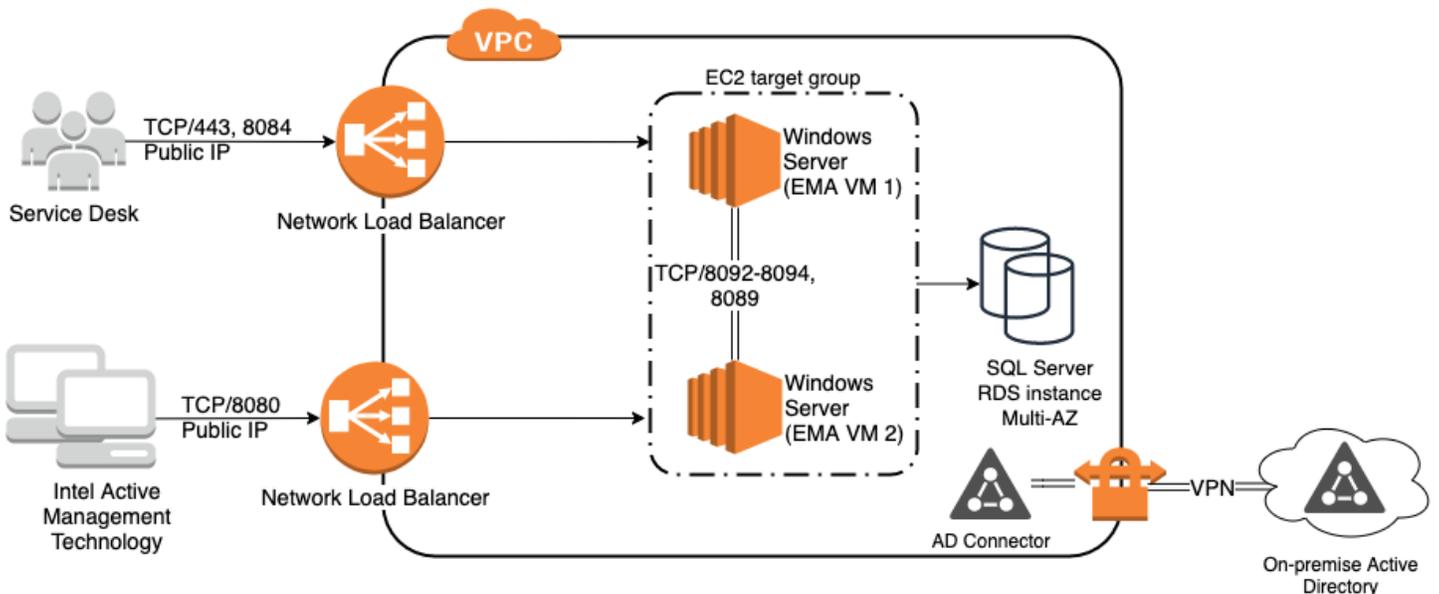
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html

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.