Intel® Endpoint Management Assistant (Intel® EMA)

Guia de implantação para Microsoft Azure*

Intel® Versão 1.3.3

Outubro de 2020

Isenção de responsabilidade legal

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

Nenhum produto ou componente pode ser totalmente seguro.

Os custos e resultados podem variar.

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

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

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

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

Sumário

1 Introdução

Este documento descreve o procedimento para implantar a infraestrutura no Microsoft Azure*, 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.

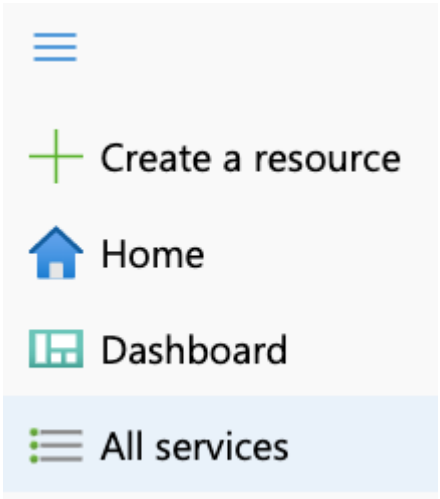
Com serviços totalmente gerenciados, como o servidor Azure SQL, você pode se concentrar em seus dados, enquanto o provedor de nuvem gerencia todo o hardware e software subjacentes que oferecem o serviço. Com máquinas virtuais em execução na nuvem, você gerencia apenas o sistema operacional convidado e o software instalado nele, enquanto o provedor de nuvem gerencia o hardware subjacente e se esforça para fornecer a melhor confiabilidade e disponibilidade.

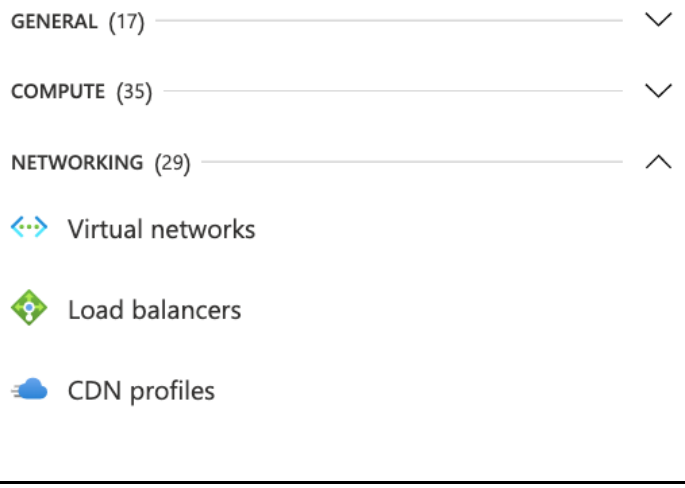
1.2 Como navegar pelo console do Azure

1.2.1 Menu de serviços

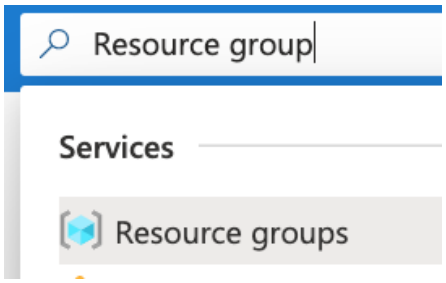
	Depois de ter feito o login no portal do Microsoft Azure, em http://portal.azure.com/, você verá um ícone de menu no canto superior esquerdo.

1.2.2 Expansão do menu de serviços

	Ao clicar nesse ícone e selecionar All services, você verá uma lista dos serviços agrupados em categorias como GENERAL, COMPUTE, NETWORKING, SECURITY, e outras. Isso serve para explorar os serviços disponíveis em várias categorias, que podem ser úteis para sua organização.



1.2.3 Busca de um serviço por nome



Neste guia, uma vez que já sabemos os nomes dos serviços de que precisamos, usaremos a barra de pesquisa no topo da tela para encontrar o serviço e depois selecioná-lo na lista apresentada.

Por exemplo, para criar um grupo de recursos, eu digitaria “Resource group” na barra de pesquisa e, em seguida, clicaria no item que aparece abaixo dele na categoria **Services**.

1.3 Antes de começar

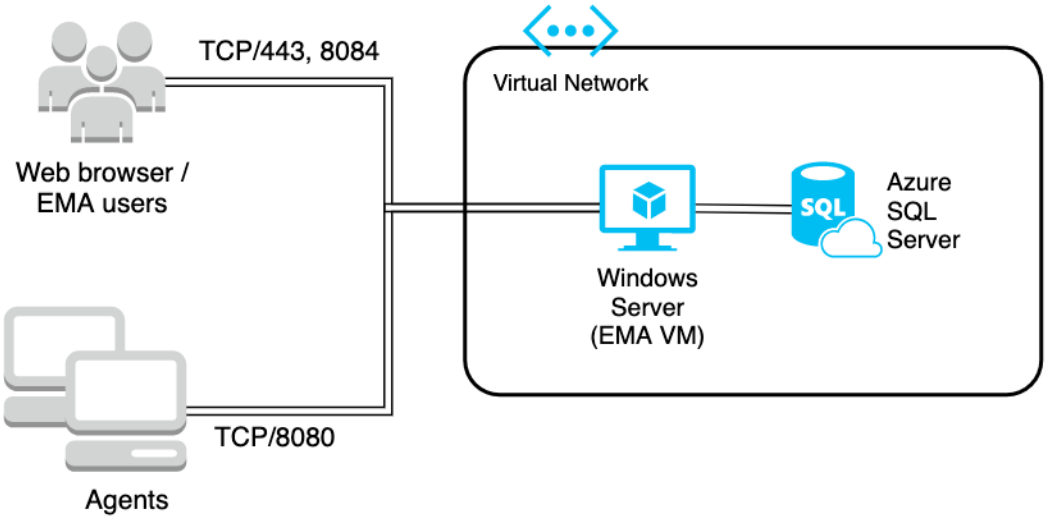
Se a sua organização já tem uma conta Azure, você deve pedir a um administrador de nuvem que lhe conceda acesso suficiente para poder criar todos os recursos listados neste guia.

Se a sua organização não tiver uma conta Azure, ou caso queira avaliar a plataforma como pessoa física, acesse https://azure.microsoft.com/en-us/free/ para criar uma conta gratuita.

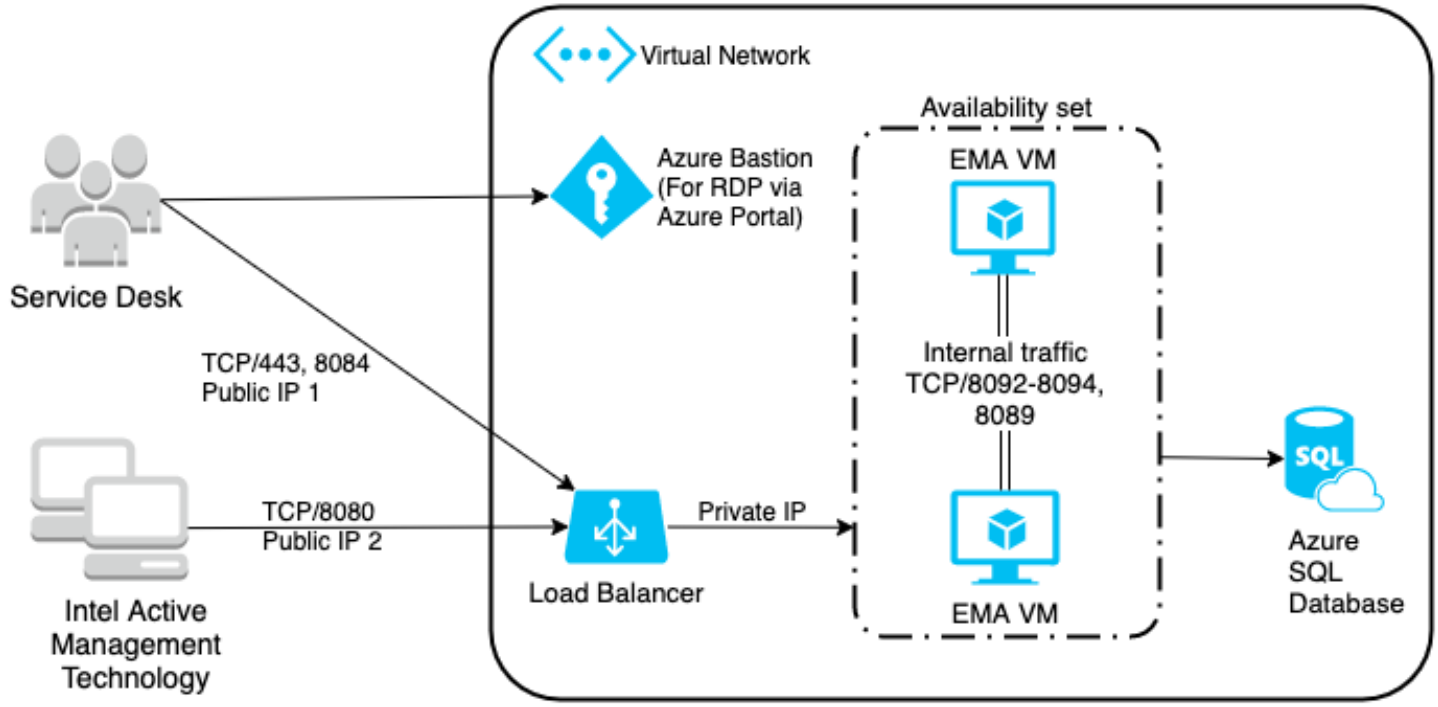
Consulte seu administrador de rede para saber se seria preferível usar um espaço de endereçamento específico. Se já tiver uma VPN estabelecida no provedor de nuvem, ou caso venha a ter futuramente, evite a sobreposição com sua rede corporativa para impedir problemas de roteamento. Você também precisa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

3.1 Visão geral dos grupos de recursos

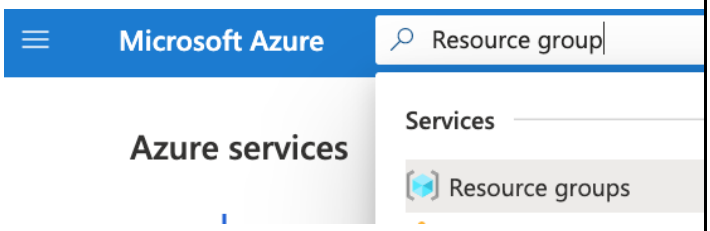
Um grupo de recursos é caracterizado como um contêiner que reúne os recursos relacionados para uma solução Azure para que você possa implantar, atualizar e excluí-los como um grupo. Você também pode ver facilmente as cobranças de todos os recursos

dentro do grupo. Você terá que selecionar um grupo de recursos existente para tudo o que for implantado no Azure; então, criaremos um primeiro.

Para mais informações sobre Grupos de recursos, acesse o seguinte link: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal.

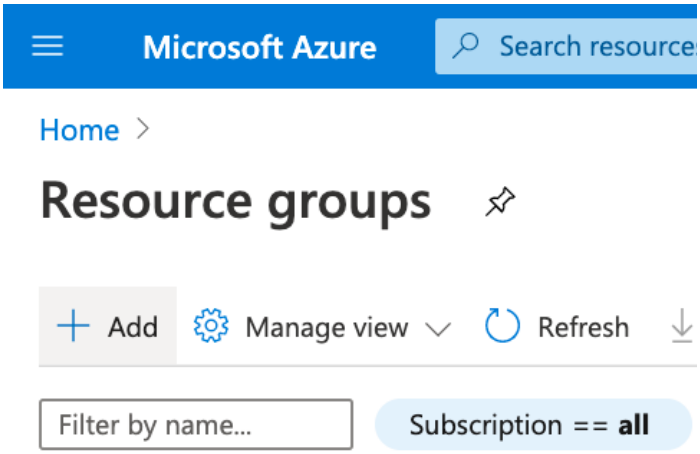
3.2 Criar um Grupo de recursos

3.2.1 Selecione o serviço de grupos de recursos



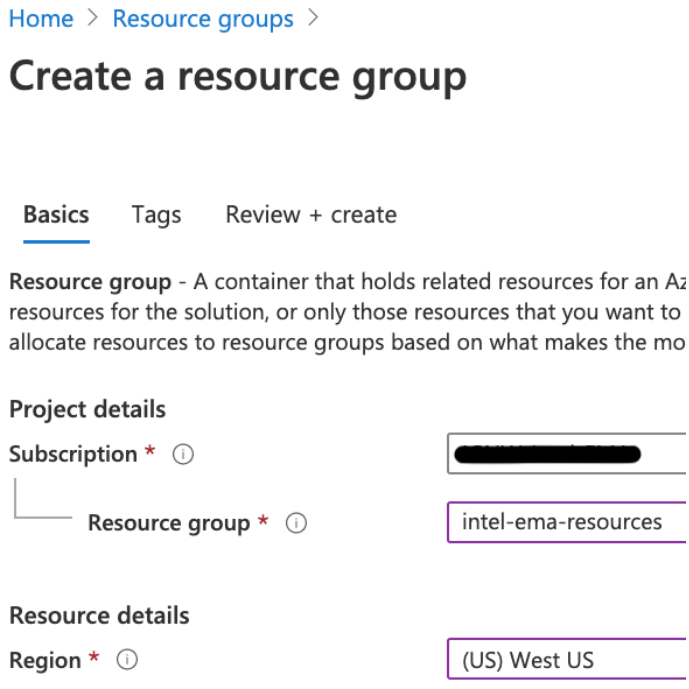
Use a barra de pesquisa no topo da tela para pesquisar sobre **Resource groups** e, em seguida, clique no item de lista exibido.

3.2.2 Adicione um grupo de recursos



Clique no botão **Add**.

3.2.3 Configure o grupo de recursos



Insira os detalhes básicos conforme abaixo.

- **Resource group**: insira um nome exclusivo para o grupo de recursos.
  Exemplo: *intel-ema-resources*
- **Region**: selecione uma região onde deseja implantar seus recursos.
  Exemplo: *(US) West US*

Nota: você precisa informar uma região ao criar outros recursos. O padrão deverá ser a região que você selecionar aqui; porém, caso não seja, este guia o lembrará de definir a região adequada.

3.2.4 Analise e crie

1. Clique no botão **Review + create**.
2. Analise as informações na tela e clique no botão **Create**.

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. Uma rede virtual é o alicerce fundamental para sua rede privada no Azure e assemelha-se a uma rede tradicional, exceto por ser virtualizada no Azure. As redes virtuais são logicamente isoladas umas das outras.

Ao criar uma rede virtual, você precisará fornecer um espaço de endereço IP privado personalizado. O Azure atribuirá recursos a um endereço IP privado a partir deste 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.

Quando criamos a rede virtual, também precisamos criar pelo menos uma sub-rede. As sub-redes permitem segmentar a rede virtual alocando uma parte do espaço de endereço da rede virtual a cada sub-rede. Então, você pode implantar recursos do Azure em uma sub-rede específica.

Vamos criar e anexar grupos de segurança de rede às sub-redes, para permitir e controlar o tráfego de entrada. O tráfego saindo das máquinas virtuais para o servidor SQL será permitido ao habilitar um ponto de extremidade de serviço na sub-rede.

Vamos implantar o serviço Azure Bastion, que permite os protocolos RDP ou SSH em suas máquinas virtuais, através do portal Azure, sem precisar expor a porta do RDP nas máquinas virtuais na internet.

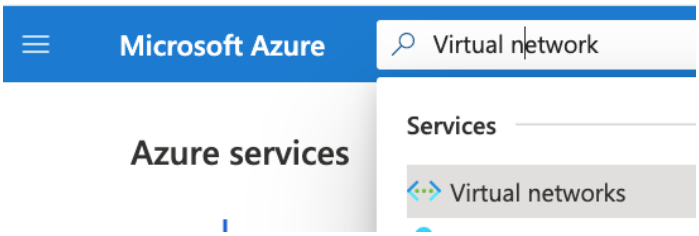
Para obter mais informações sobre recursos de rede implantados nesta seção, acesse os links a seguir ou procure links adicionais nas seções abaixo:

- Redes virtuais: https://docs.microsoft.com/en-us/azure/virtual-network/
- Terminais de serviço VNet: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview
- Azure Bastion: https://docs.microsoft.com/en-us/azure/bastion/

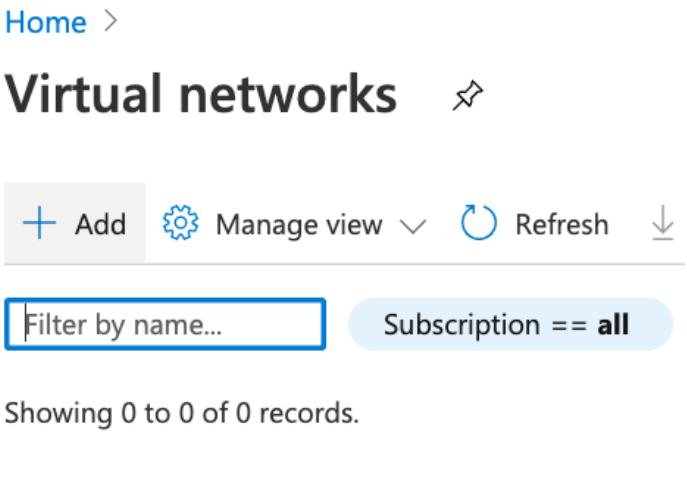
4.2 Crie uma rede virtual

Siga este procedimento para criar uma rede virtual com uma única sub-rede.

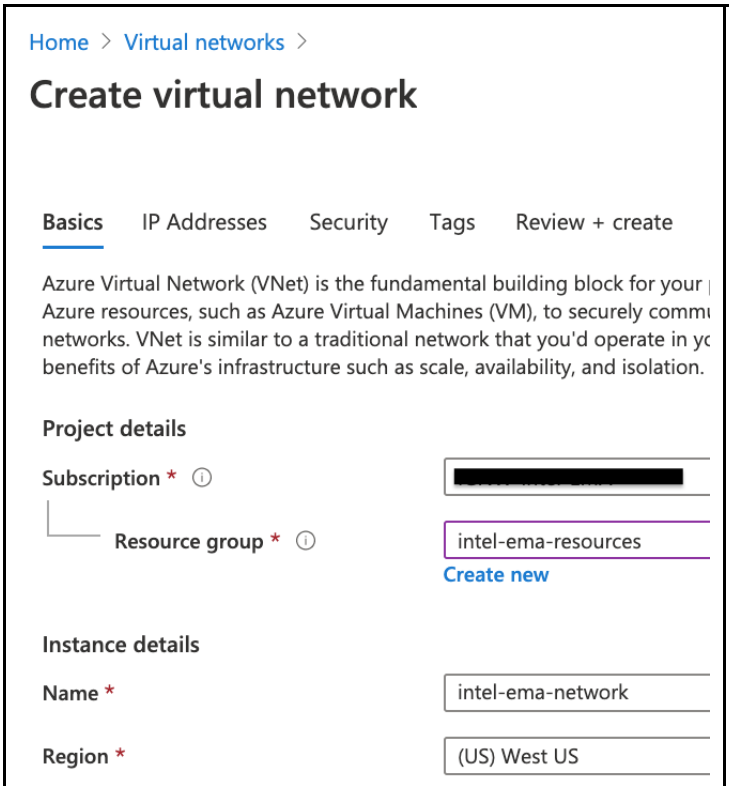
4.2.1 Navegue até o serviço de redes virtuais

	Use a barra de pesquisa no topo da tela para pesquisar sobre **Virtual networks** e, em seguida, clique no item de lista exibido.

4.2.2 Adicione uma rede virtual

	Clique no botão **Add**.

4.2.3 Configure os detalhes básicos da Rede virtual

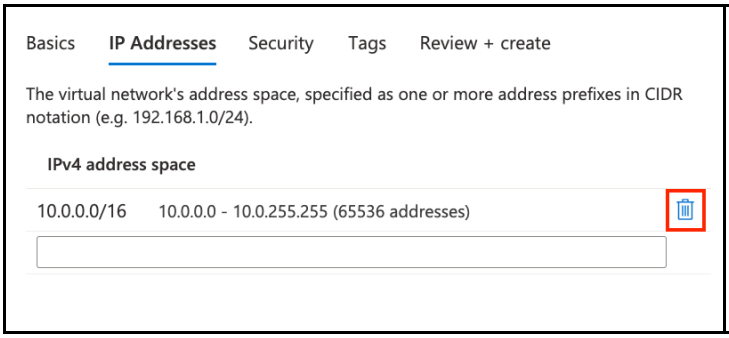


Insira os detalhes básicos conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
  Exemplo: *intel-ema-resources*
- **Name**: insira um nome exclusivo para o grupo de recursos.
  Exemplo: *intel-ema-network*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.
  Exemplo: *(US) West US*

Clique no botão **Next: IP Addresses** e siga para a próxima etapa.

4.2.4 Configure o espaço de endereço IPv4

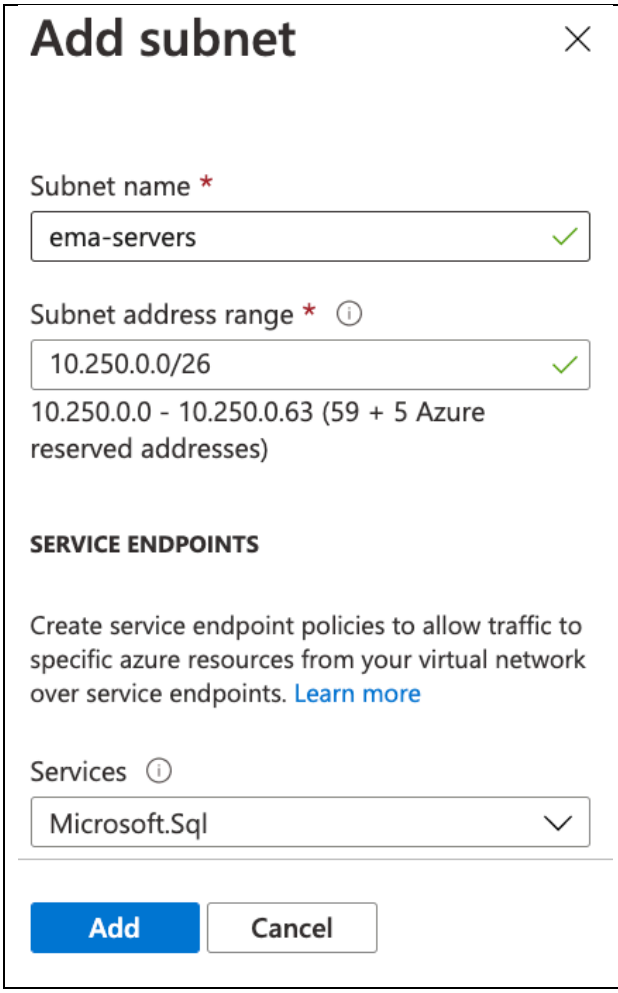


Clique no ícone da lixeira para excluir o espaço de endereço padrão e, em seguida, digite um novo espaço de endereço IPv4

Exemplo: 10.250.0.0/24

Consulte sua equipe de engenharia de rede para selecionar 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.

4.2.5 Adicione sub-rede para servidores do Intel EMA



Clique no botão **Add Subnet** e configure a sub-rede conforme abaixo.

Subnet name: insira um nome de sub-rede exclusivo.
Exemplo: *ema-servers*

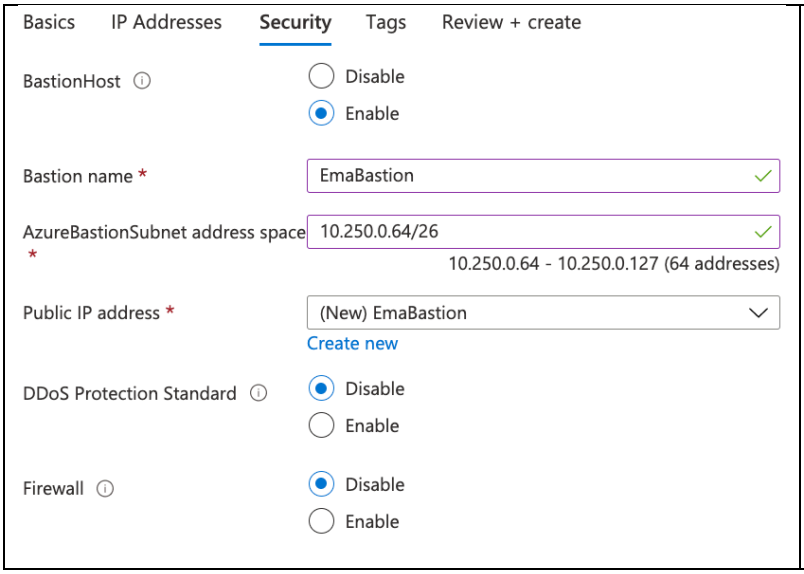
Subnet address range: insira um intervalo de endereços de sub-rede não usados, contido no espaço de endereço IPv4 que você inseriu anteriormente.
Exemplo: *10.250.0.0/26*

No menu suspenso **Services**, selecione **Microsoft.Sql**.

Clique no botão **Add** para finalizar a sub-rede.

Clique no botão **Next: Security**.

4.2.6 Habilite o Azure Bastion



Defina as configurações de segurança conforme abaixo.

BastionHost: *Enable*

Bastion name: insira um nome de Bastion exclusivo.
Exemplo: *EmaBastion*

AzureBastionSubnet address space: insira um espaço de endereço não usado contido no espaço de endereço da rede virtual. Ele deve ser /26 ou maior.
Exemplo: *10.250.0.64/26*

Public IP address: clique no link **Create new**, defina um nome exclusivo e, em seguida, clique no botão **OK**
Exemplo: *EmaBastion*

4.2.7 Analise

Clique no botão **Review + create**.

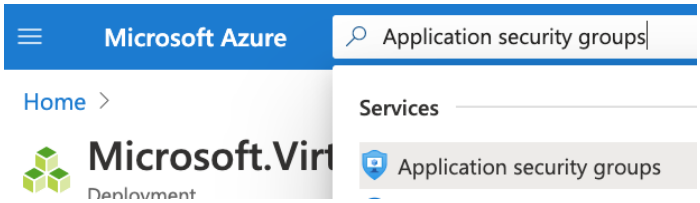
Analise as informações de rede na tela e clique no botão **Create**.

4.3 Grupo de segurança da aplicação (ASG)

Você pode pensar em um ASG como um identificador especial que pode ser aplicado a uma máquina virtual de forma a lhe permitir direcionar mais facilmente a máquina virtual à regra de firewall, o que faremos na seção Grupo de segurança de rede. A fim de nos prepararmos para isso, vamos criar um ASG através do procedimento abaixo.

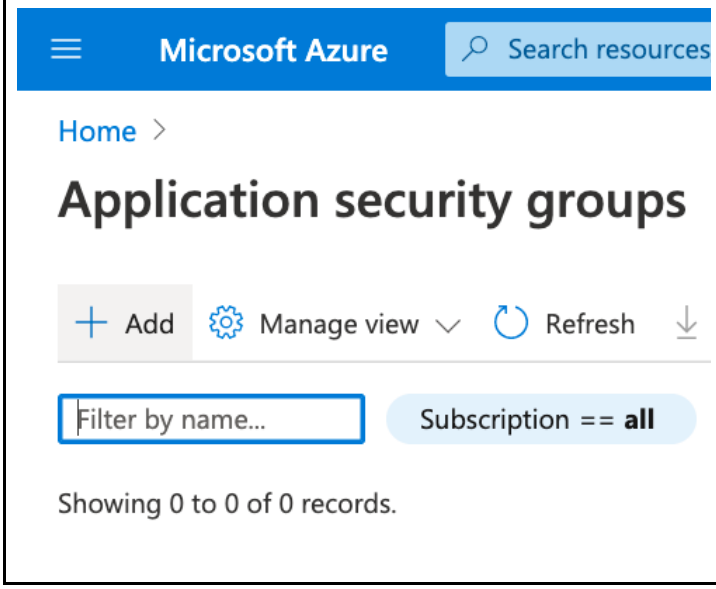
Para obter mais informações sobre os Grupos de segurança da aplicação, acesse o seguinte link: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups.

4.3.1 Navegue até o serviço de grupos de segurança da aplicação



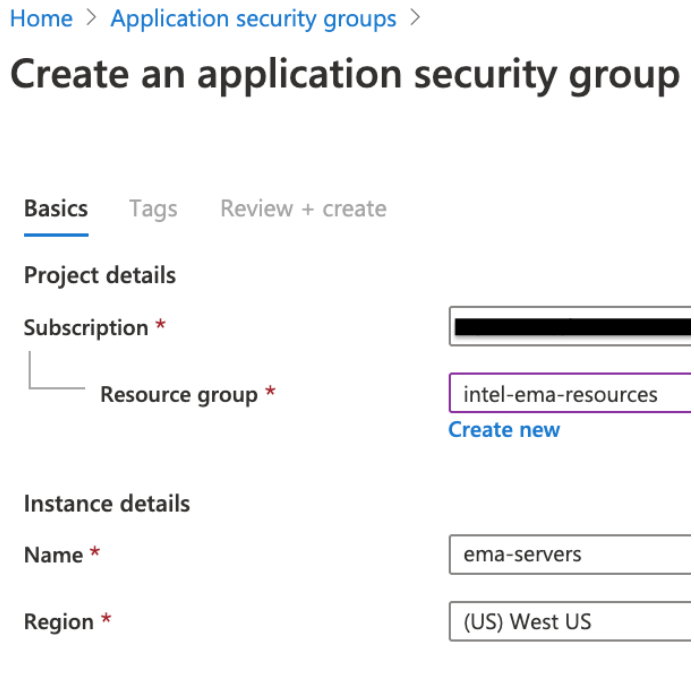
Use a barra de pesquisa no topo da tela para pesquisar sobre **Application security groups** e, em seguida, clique no item de lista exibido.

4.3.2 Adicione um grupo de segurança da aplicação



Clique no botão **Add**.

4.3.3 Configure o Grupo de segurança da aplicação (ASG)



Insira os detalhes básicos conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Name**: insira um nome exclusivo para o ASG. Exemplo: *ema-servers*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.

Clique no botão **Review + create**.

Analise as informações na tela e clique no botão **Create**.

4.4 Grupos de segurança de rede

Um Grupo de segurança de rede (NSG) contém regras de segurança que permitem ou negam o tráfego de rede de entrada, ou o tráfego de rede de saída de vários tipos de recursos do Azure. Para cada regra, você pode especificar a fonte e o destino, a porta e o protocolo.

Quando você cria um NSG, o Azure inclui um conjunto de regras padrão que não podem ser removidas, mas com prioridade muito baixa, e você as contornaria normalmente com regras de maior prioridade, se necessário. As regras padrão são as seguintes:

AllowVNetInBound: permite todo o tráfego entre recursos em sua rede virtual.

AllowAzureLoadBalancerInBound: permite todo o tráfego do Azure Load Balancer para sua rede virtual.

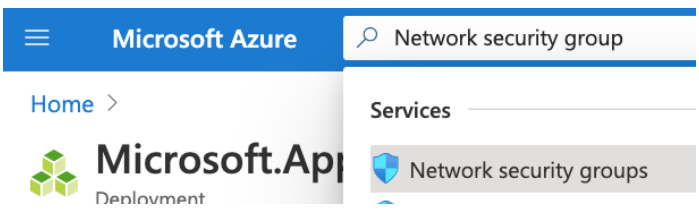
DenyAllInbound: nega todo o tráfego de entrada de qualquer fonte para qualquer fonte.

Nesta seção, criaremos um NSG e adicionaremos todas as regras necessárias para permitir o tráfego para nossa máquina virtual do Intel EMA. Vamos criar outro NSG para permitir o tráfego necessário para a sub-rede Azure Bastion.

Para obter mais informações sobre os grupos de segurança de rede, acesse o seguinte link: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

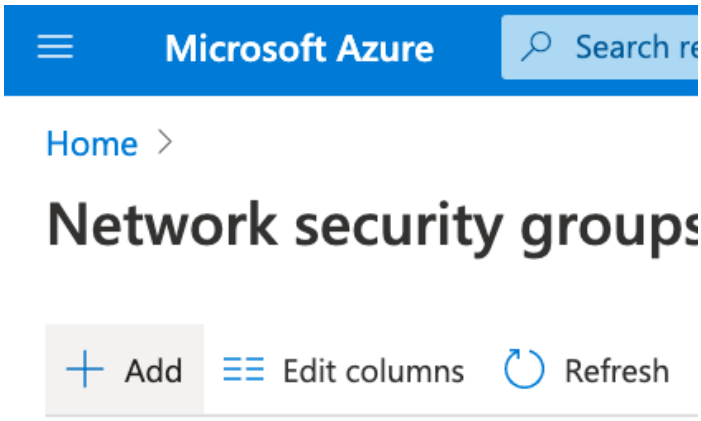
4.4.1 Crie o grupo de segurança de rede para a sub-rede de servidores do Intel EMA

4.4.1.1 Navegue até o serviço de grupos de segurança de rede



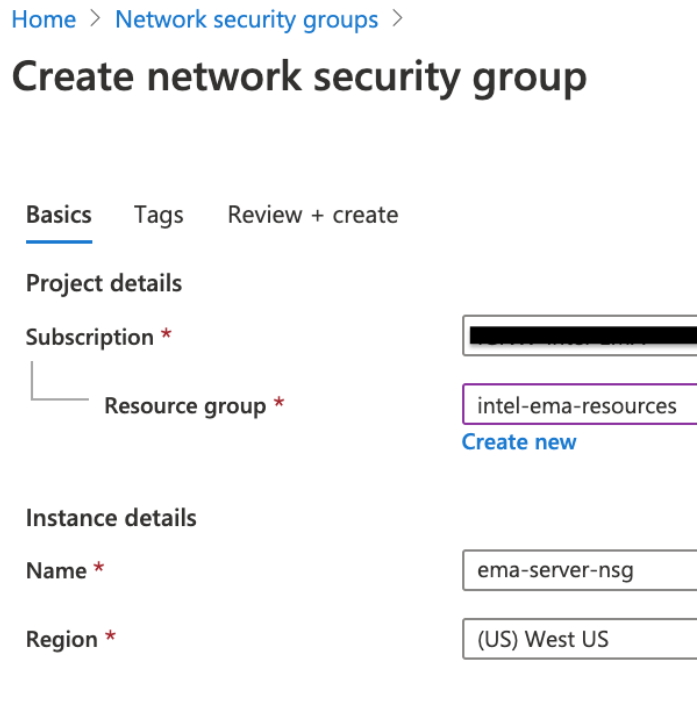
Use a barra de pesquisa no topo da tela para pesquisar sobre **Network security groups** e, em seguida, clique no item de lista exibido.

4.4.1.2 Adicione um grupo de segurança de rede



Clique no botão **Add**.

4.4.1.3 Configure os detalhes básicos do grupo de segurança de rede (NSG)



Insira os detalhes básicos conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Name**: insira um nome exclusivo para o NSG. Exemplo: *ema-server-nsg*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.

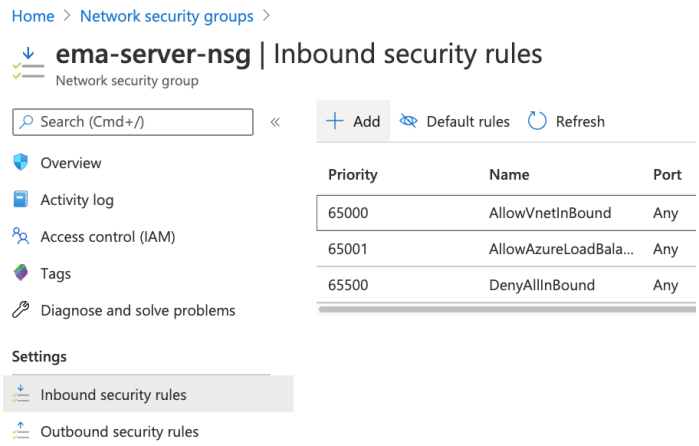
Clique no botão **Review + create**.

Analise as informações de rede na tela e clique no botão **Create**.

Ao ver a mensagem pop-up confirmando o sucesso da implantação, clique no botão **Go To Resource**.

4.4.2 Configure o grupo de segurança de rede

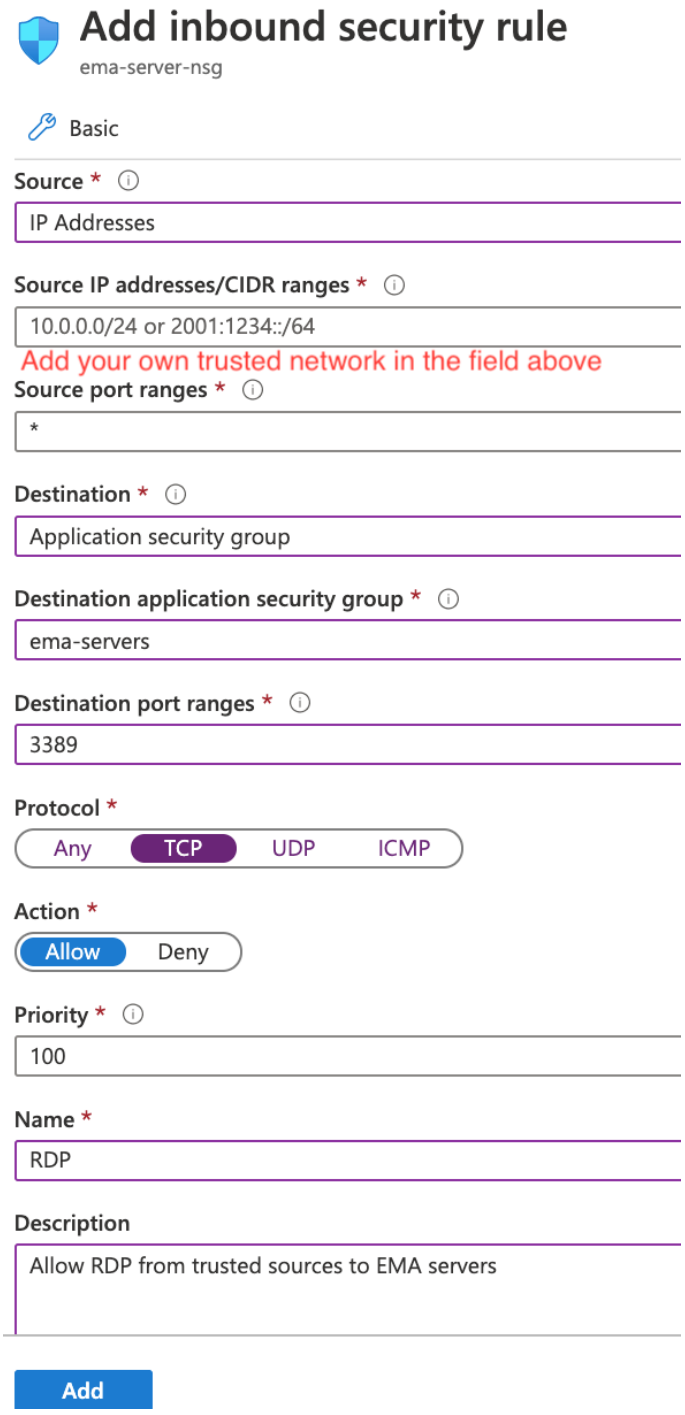
4.4.2.1 Navegue até as regras de segurança de entrada



Na barra lateral do grupo de segurança, em **Settings**, selecione **Inbound security rules**.

Nota: depois de criar cada regra com o procedimento abaixo, aguarde até que a criação seja concluída e a regra apareça na lista, para que o Azure possa incrementar Priority automaticamente e da forma correta.

4.4.2.2 Crie a regra de RDP

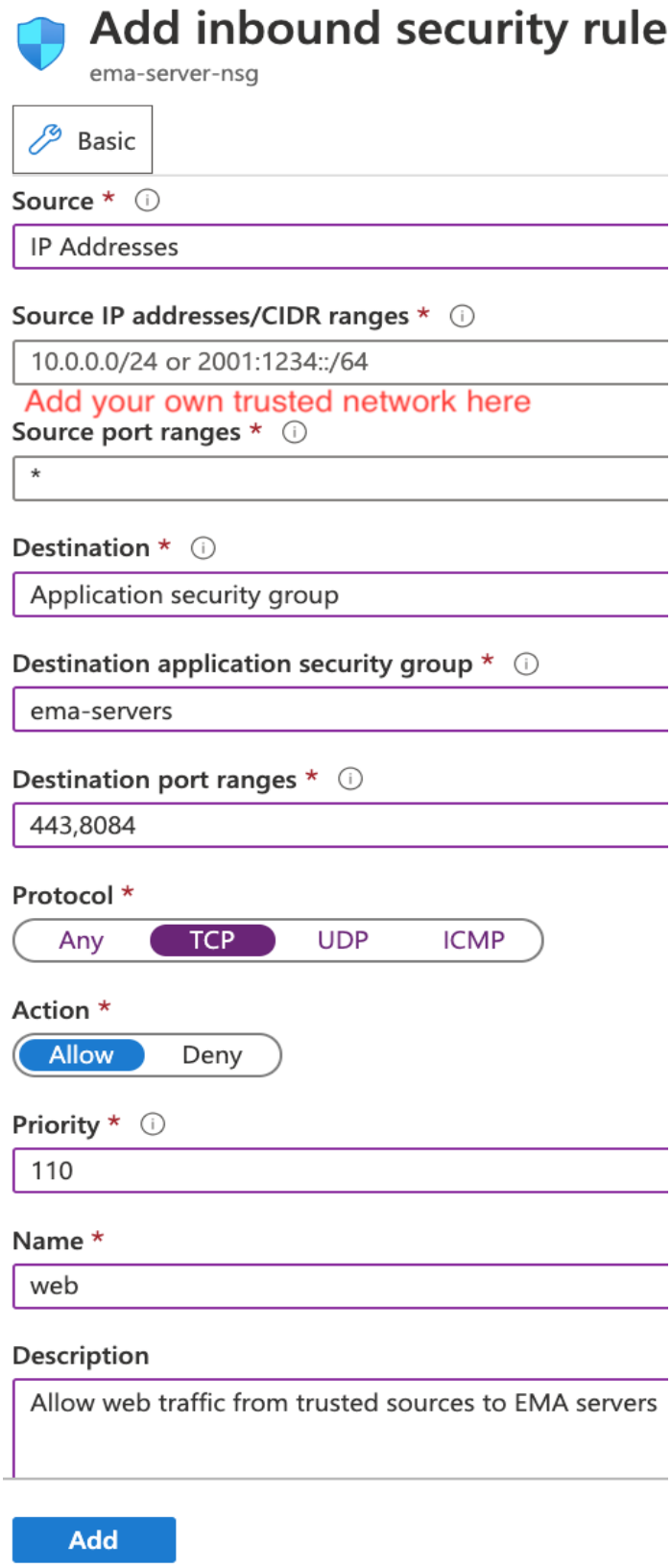


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *IP Addresses*
- **Source IP addresses/CIDR ranges**: insira o intervalo CIDR da sub-rede Azure Bastion que definimos quando a rede virtual foi criada.
  Exemplo: 10.250.0.64/26
- **Source port ranges**: *
- **Destination**: *Application security group*
- **Destination application security group**: *ema-servers* (ou o nome que você forneceu)
- **Destination port ranges**: *3389*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo para a regra.
  Exemplo: *RDP*
- **Description**: *Permitir RDP de fontes confiáveis para servidores Intel EMA*

Quando tiver terminado, clique no botão **Add** na parte inferior da tela.

4.4.2.3 Crie a regra de tráfego Web

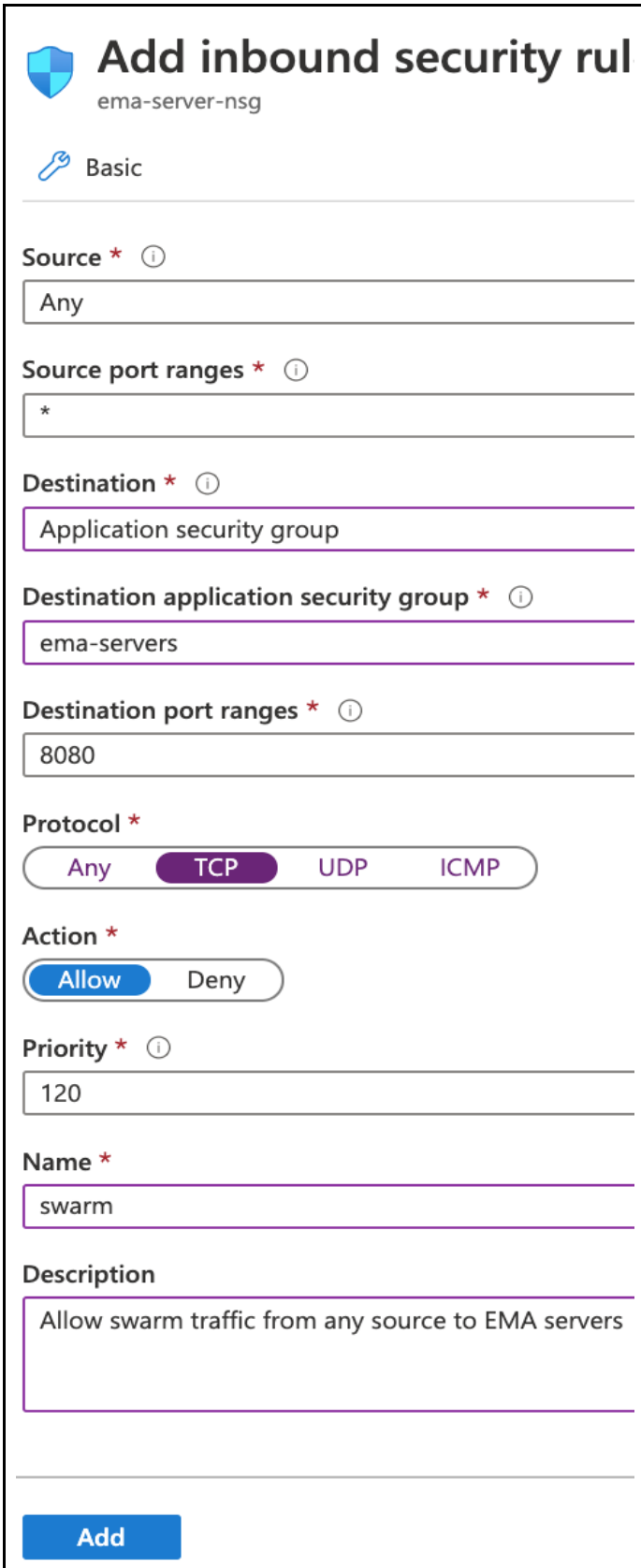


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *IP Addresses*
- **Source IP addresses/CIDR ranges**: insira sua(s) rede(s) confiável(is) que deve(m) ter permissão para acessar a interface web EMA pela internet. Como alternativa, você pode definir qualquer fonte (Source to Any) se não quiser restrições.
- **Source port ranges**: *
- **Destination**: *Application security group*
- **Destination application security group**: *ema-servers* (ou o nome que você forneceu)
- **Destination port ranges**: *443,8084*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo para a regra. Exemplo: *web*
- **Description**: *Permitir tráfego da web de fontes confiáveis para servidores Intel EMA*

Quando tiver terminado, clique no botão **Add** na parte inferior da tela.

4.4.2.4 Crie a regra de tráfego Swarm

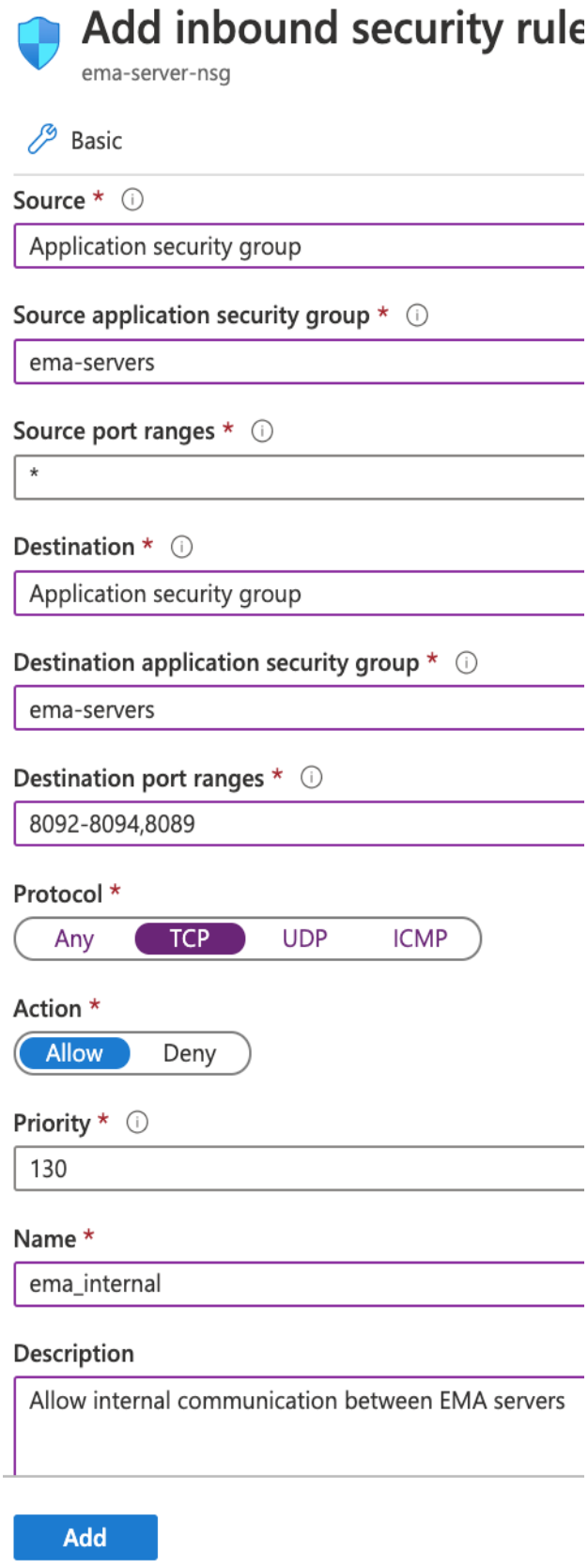


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Any*
- **Source port ranges**: *
- **Destination**: *Application security group*
- **Destination application security group**: *ema-servers* (ou o nome que você forneceu)
- **Destination port ranges**: *8080*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo para a regra. Exemplo: *swarm*
- **Description**: *Permitir tráfego swarm de qualquer fonte para servidores Intel EMA*

Quando tiver terminado, clique no botão **Add** na parte inferior da tela.

4.4.2.5 Adicione a regra de tráfego interno (apenas servidor distribuído)



Siga este procedimento se estiver implantando uma arquitetura de servidor distribuído; do contrário, você pode ignorá-lo.

Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Application security group*
- **Source application security group**: *ema-servers* (ou o nome que você forneceu)
- **Source port ranges**: *
- **Destination**: *Application security group*
- **Destination application security group**: *ema-servers* (ou o nome que você forneceu)
- **Destination port ranges**: *8092-8094,8089*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo.
  Exemplo: *ema_internal*
- **Description**: *Permitir tráfego swarm de qualquer fonte para servidores Intel EMA*

Quando tiver terminado, clique no botão **Add** na parte inferior da tela.

4.4.3 Analise

Quando tiver terminado, você deve ter uma tabela semelhante à imagem abaixo.

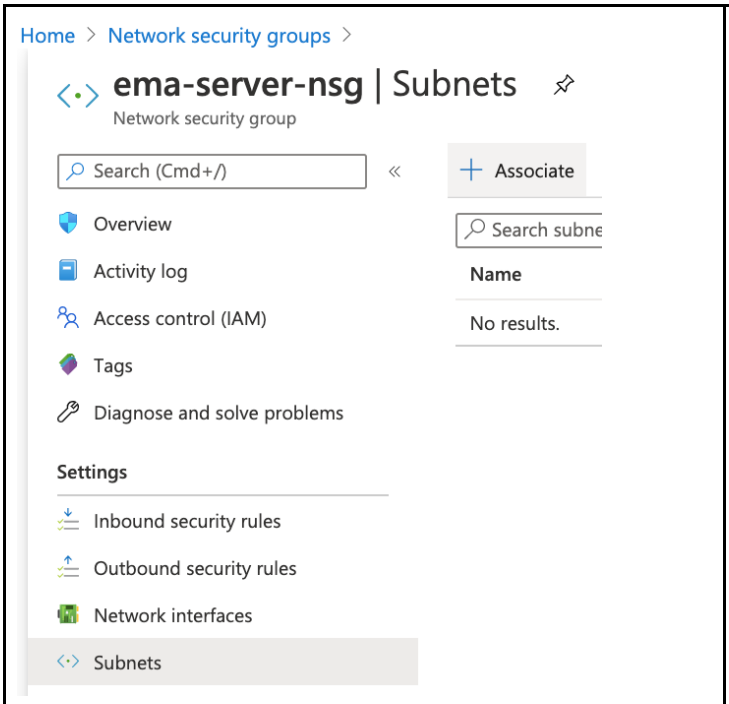
Nota: você deve ter apenas a regra *ema_internal* se estiver implantando uma arquitetura de servidor distribuído.

+ Add Default rules Refresh

Priority	Name	Port	Protocol	Source	Destination
100	RDP	3389	TCP	10.250.0.64/26	ema-servers
110	web	443,8084	TCP	[redacted]	ema-servers
120	swarm	8080	TCP	Any	ema-servers
130	ema_internal	8092-8094,8089	TCP	ema-servers	ema-servers
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

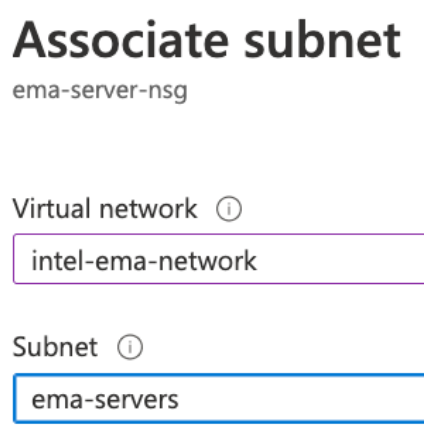
4.4.4 Associe o grupo de segurança de rede à sua sub-rede

4.4.4.1 Navegue até associações de sub-rede do grupo de segurança de rede



Na barra lateral do grupo de segurança, em **Settings**, selecione **Subnets** e clique no botão **Associate**.

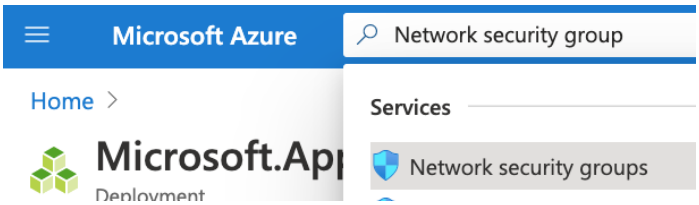
4.4.4.2 Associe o grupo de segurança de rede à sub-rede

	Selecione a sub-rede que você criou anteriormente para os servidores EMA e clique em **OK**.

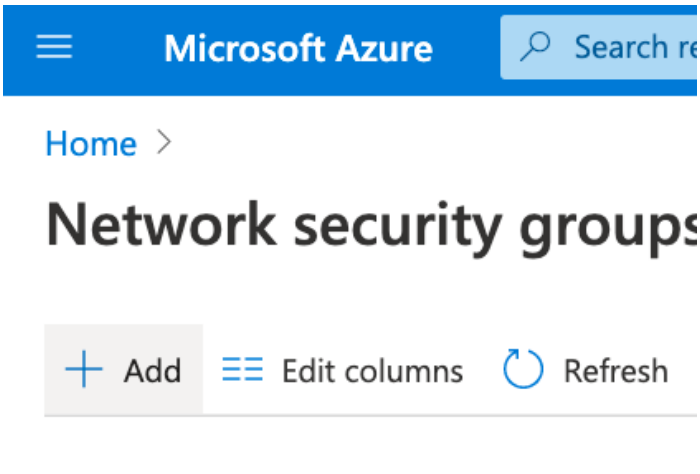
4.4.5 Crie o grupo de segurança de rede para a sub-rede Azure Bastion

Referência: https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg

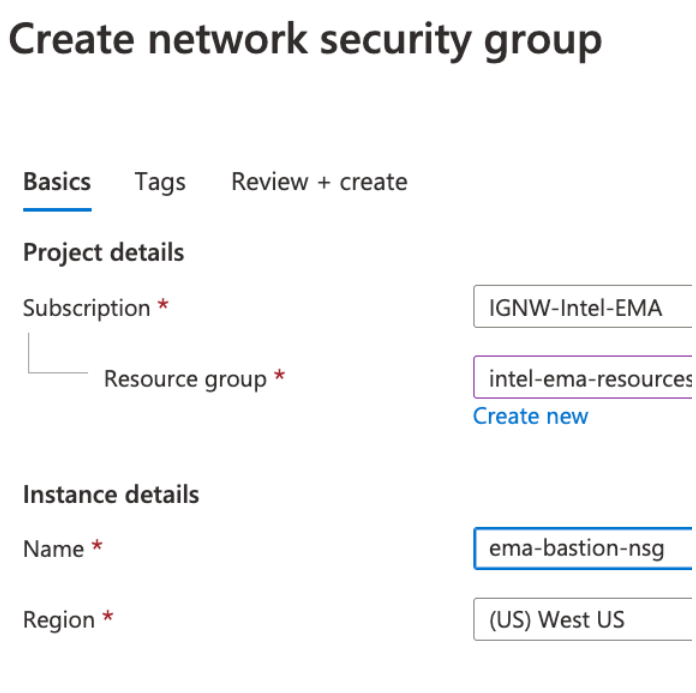
4.4.5.1 Navegue até o serviço de grupos de segurança de rede

	Use a barra de pesquisa no topo da tela para pesquisar sobre **Network security groups** e, em seguida, clique no item de lista exibido.

4.4.5.2 Adicione um grupo de segurança de rede

	Clique no botão **Add**.

4.4.5.3 Configure os detalhes básicos do grupo de segurança de rede



Insira os detalhes básicos conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Name**: insira um nome exclusivo.
  Exemplo: *ema-bastion-nsg*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.

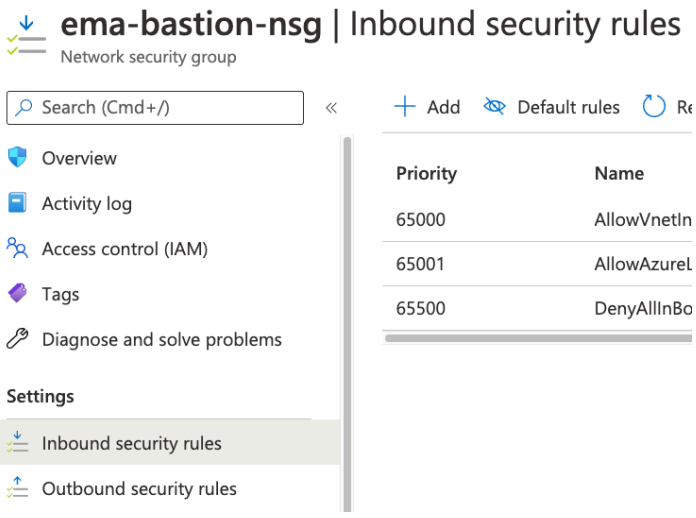
Clique no botão **Review + create**.

Analise as informações de rede na tela e clique no botão **Create**.

Ao ver a mensagem pop-up confirmando o sucesso da implantação, clique no botão **Go To Resource**.

4.4.6 Configure o grupo de segurança de rede

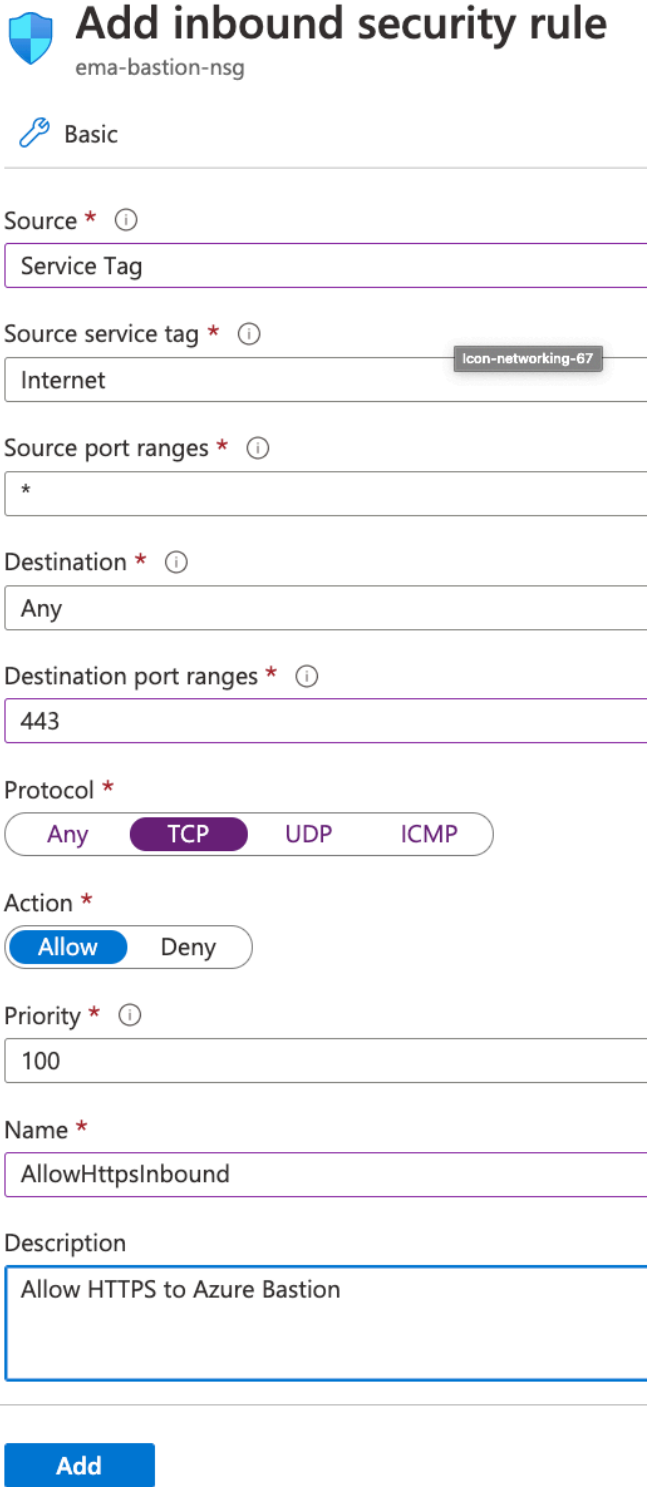
4.4.6.1 Navegue até as regras de segurança de entrada



Na barra lateral do grupo de segurança, em **Settings**, selecione **Inbound security rules**.

Nota: depois de criar cada regra com o procedimento abaixo, aguarde até que a criação seja concluída e a regra apareça na lista, para que o Azure possa incrementar Priority automaticamente e da forma correta.

4.4.6.2 Crie uma regra permitindo o HTTPS para o Azure Bastion

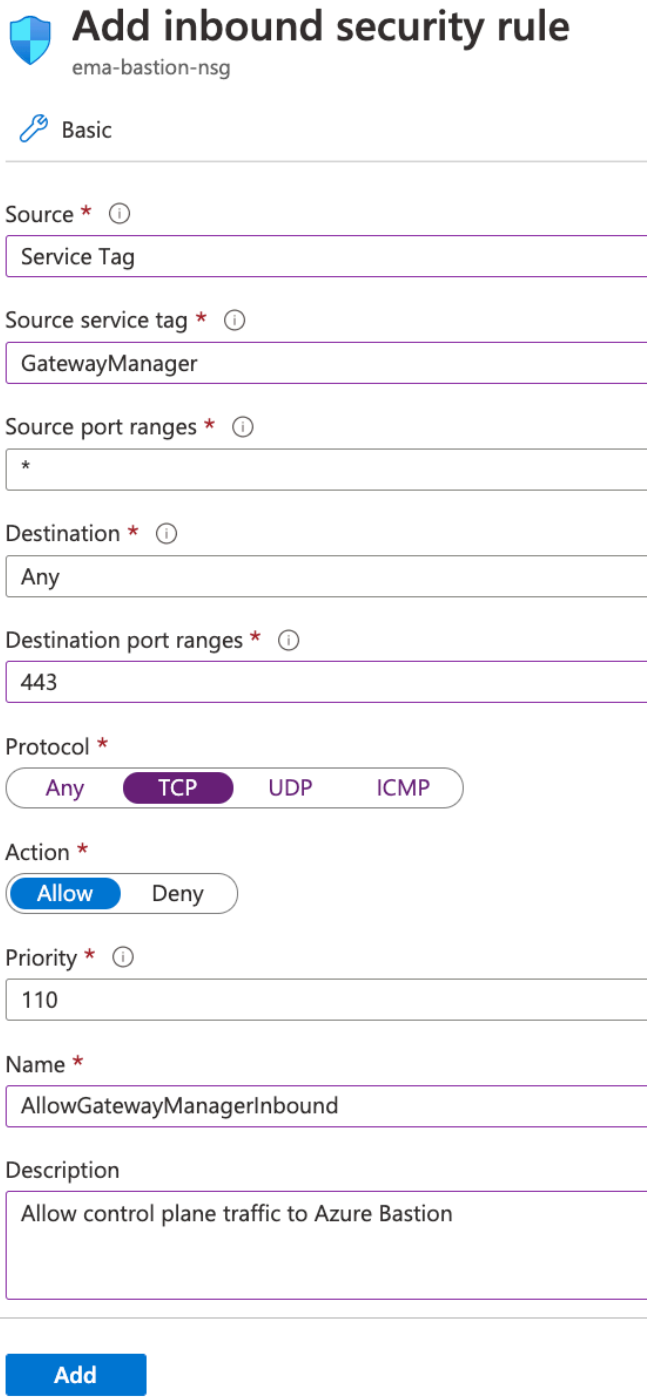


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Service Tag*
- **Source service tag**: *Internet*
- **Source port ranges**: *
- **Destination**: *Any*
- **Destination port ranges**: *443*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo.
  Exemplo: *AllowHttpsInbound*
- **Description**: *Permitir HTTPS para o Azure Bastion*

Clique no botão **Add** na parte inferior da tela.

4.4.6.3 Crie uma regra permitindo o gerenciador de gateway para o Azure Bastion

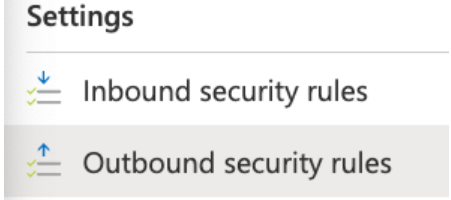


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Service Tag*
- **Source service tag**: *GatewayManager*
- **Source port ranges**: *
- **Destination**: *Any*
- **Destination port ranges**: *443*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo.
  Exemplo: *AllowGatewayManagerInbound*
- **Description**: *Permitir tráfego do plano de controle para o Azure Bastion*

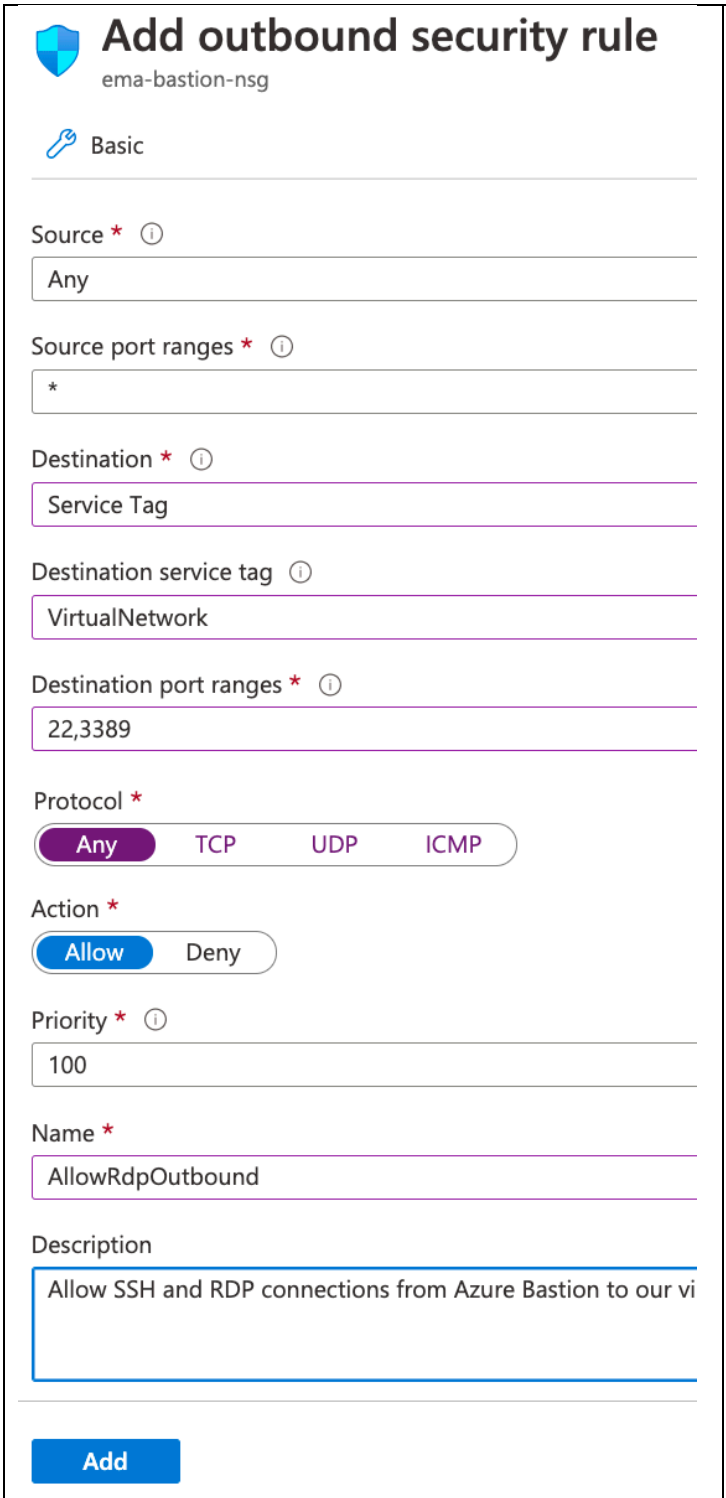
Clique no botão **Add** na parte inferior da tela.

4.4.7 Configure as regras de segurança de saída



Na barra lateral, abaixo de “Inbound securty rules”, clique em “Outbound security rules”.

4.4.7.1 Habilite o tráfego de saída SSH/RDP para a nossa rede virtual

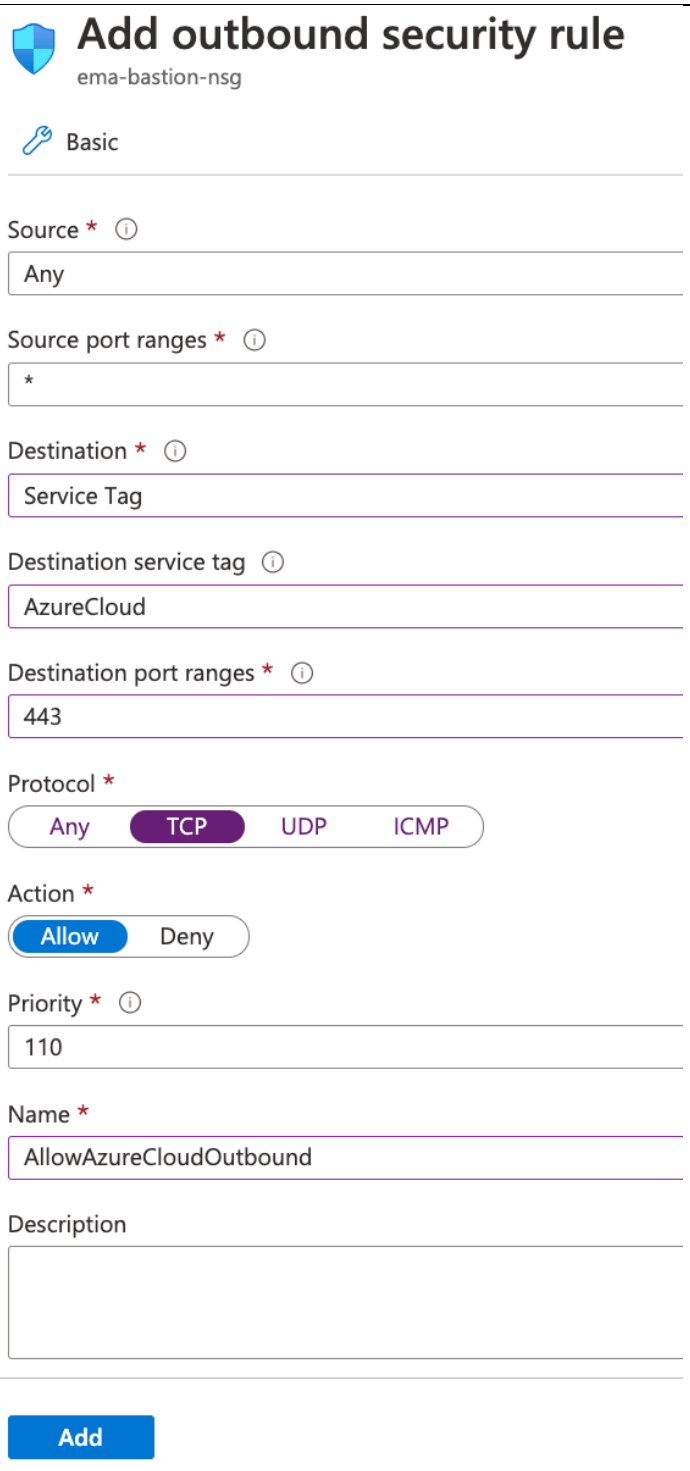


Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Any*
- **Source port ranges**: *
- **Destination**: *Service Tag*
- **Destination service tag**: *VirtualNetwork*
- **Destination port ranges**: *22,3389*
  Nota: o Azure Bastion requer que as duas portas tenham permissão, mesmo se você não precisar de uma ou da outra.
- **Protocol**: *Any*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo.
  Exemplo: *AllowGatewayManagerInbound*
- **Description**: *Permitir conexões de RDP do Azure Bastion para nossa rede virtual*

Clique no botão **Add** na parte inferior da tela.

4.4.7.2 Habilite a saída para os serviços do Azure



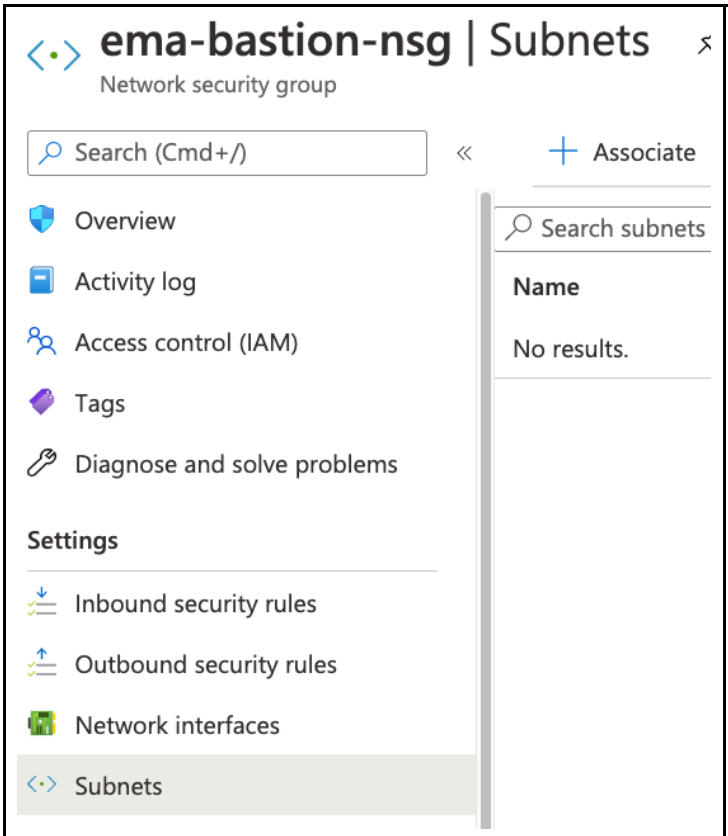
Clique no botão **Add** perto do topo da tela e configure a regra conforme abaixo.

- **Source**: *Any*
- **Source port ranges**: *
- **Destination**: *Service Tag*
- **Destination service tag**: *AzureCloud*
- **Destination port ranges**: *443*
- **Protocol**: *TCP*
- **Action**: *Allow*
- **Priority**: use o valor atribuído automaticamente.
- **Name**: insira um nome exclusivo.
  Exemplo: *AllowAzureCloudOutbound*
- **Description**: *Permitir que o Azure Bastion se conecte a endpoints de serviço do Azure*

Clique no botão **Add** na parte inferior da tela.

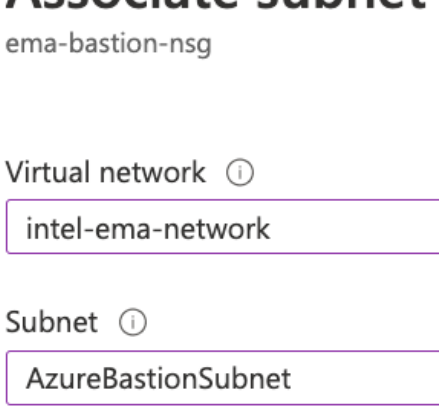
4.4.8 Associe o grupo de segurança de rede com a sua sub-rede do Azure Bastion

4.4.8.1 Navegue até associações de sub-rede do grupo de segurança de rede



Na barra lateral do grupo de segurança, em **Settings**, selecione **Subnets** e clique no botão **Associate**.

4.4.8.2 Associe o grupo de segurança de rede à sub-rede



Selecione a sub-rede que você criou anteriormente para os servidores EMA e clique em **OK**.

5 Implantação do servidor SQL

5.1 Visão geral

O Azure possui um mecanismo de banco de dados de plataforma como um serviço (PaaS) totalmente gerenciado, que possui dois componentes:

- Um servidor SQL lógico, que terá um nome de host do DNS associado a ele.
- Um ou mais bancos de dados SQL, que podem ser configurados individualmente para escala e desempenho.

Ser um serviço gerenciado significa que o Azure administra a maioria das funções de gerenciamento de dados, como atualização, reparação, backups e monitoramento, sem envolvimento do usuário para manter o banco de dados em execução na versão estável mais recente do mecanismo de banco de dados do servidor SQL, com 99,99% da disponibilidade. Também fornece alta disponibilidade padrão, com um modelo HA premium disponível.

O banco de dados SQL permite definir e escalar o desempenho facilmente em dois modelos de aquisição diferentes: um modelo de aquisição baseado em vCore e um modelo de aquisição baseado em DTU.

- O modelo de aquisição baseado em vCore permite escolher o número de vCores, a quantidade de memória e a quantidade e velocidade de armazenamento.
- O modelo de aquisição baseado em DTU oferece um conjunto de recursos de computação, memória e E/S em três níveis de serviços, para oferecer suporte leve a cargas de trabalho pesadas do banco de dados.

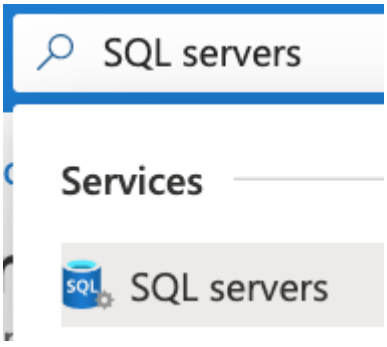
Para usar isso com nosso servidor Intel EMA, precisamos apenas criar o servidor lógico SQL previamente. O banco de dados SQL será criado dinamicamente durante o processo de instalação do Intel EMA. Depois de concluir o processo de instalação, você pode voltar ao console de gerenciamento do Azure para analisar as configurações do banco de dados e ajustá-las, se desejado.

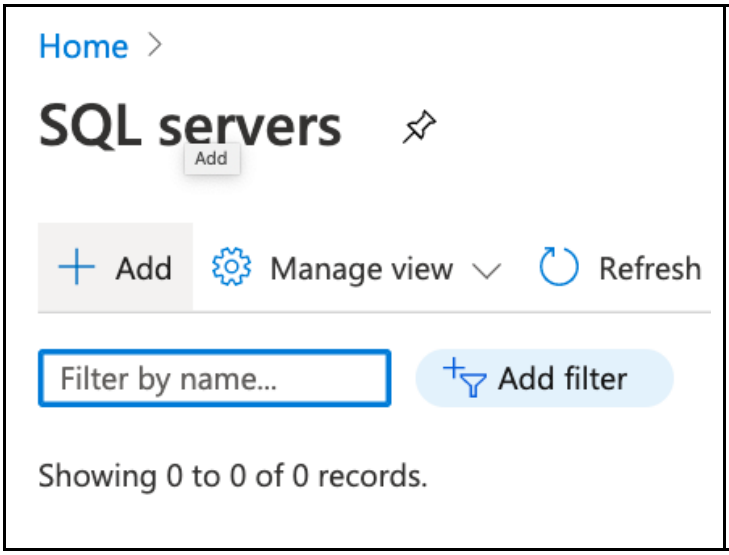
Para obter mais informações sobre o servidor Azure SQL, o banco de dados SQL e o modelo de alta disponibilidade, acesse os seguintes links:
https://docs.microsoft.com/en-us/azure/azure-sql/
https://docs.microsoft.com/en-us/azure/azure-sql/database/
https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla

5.2 Crie o servidor SQL

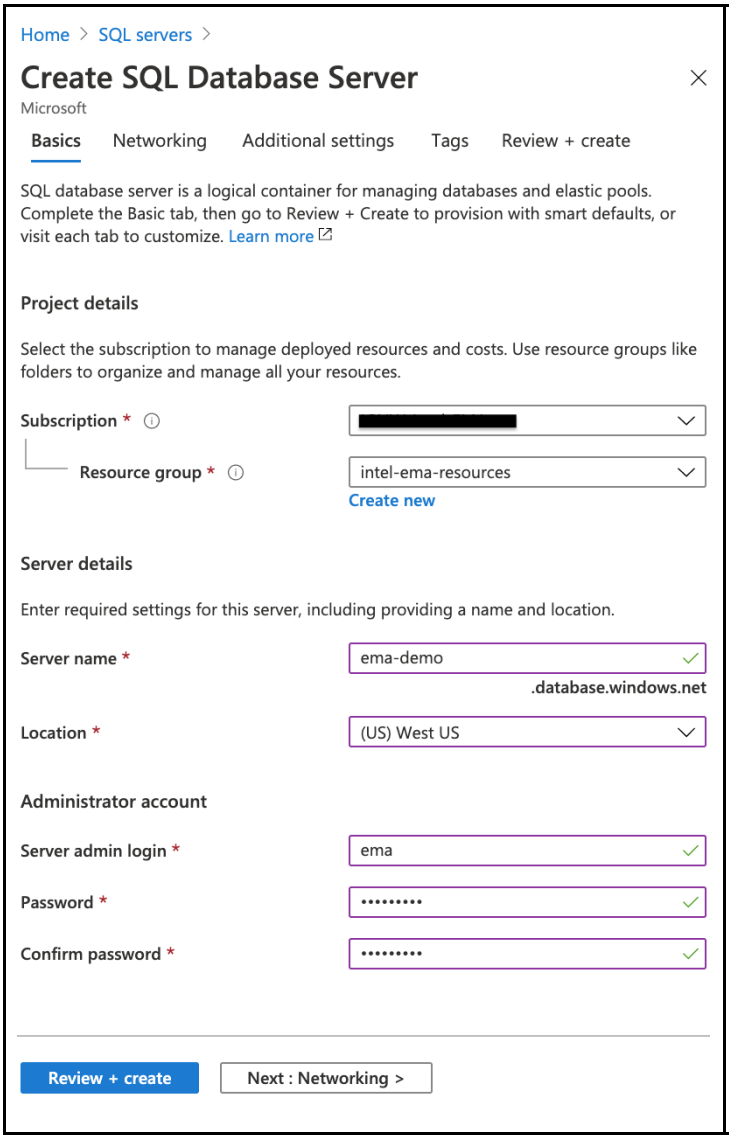
Siga o procedimento abaixo para criar um servidor Azure SQL e habilitar o acesso a ele a partir de nossa sub-rede da máquina virtual.

5.2.1 Adicione um novo servidor SQL

	Use a barra de pesquisa no topo da tela para pesquisar sobre **SQL servers** e, em seguida, clique no item de lista exibido. Clique no botão **Add**.



5.2.2 Configure os detalhes básicos para o servidor SQL



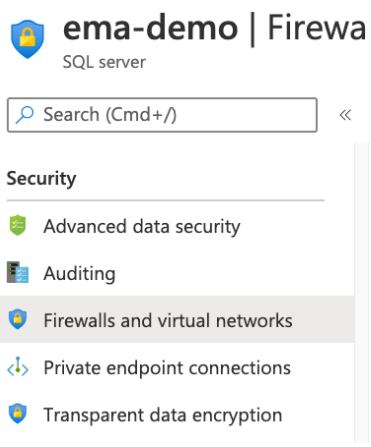
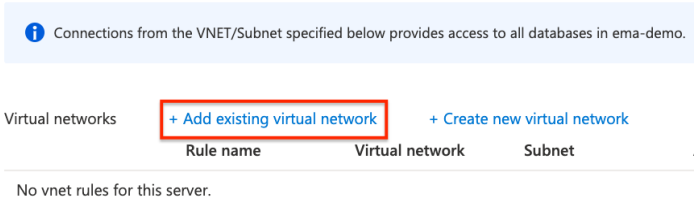
Insira os detalhes básicos conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Server name**: insira um nome globalmente exclusivo. Exemplo: *ema-demo*
  Nota: o nome que você escolher aqui será associado ao sufixo “.database.window.net” para formar um nome de DNS que pode ser usado para acessar o banco de dados durante o processo de instalação do Intel EMA.
- **Location**: confirme se essa é a região onde você deseja implantar seus recursos.
- Forneça um nome de usuário e senha para a conta de administrador.

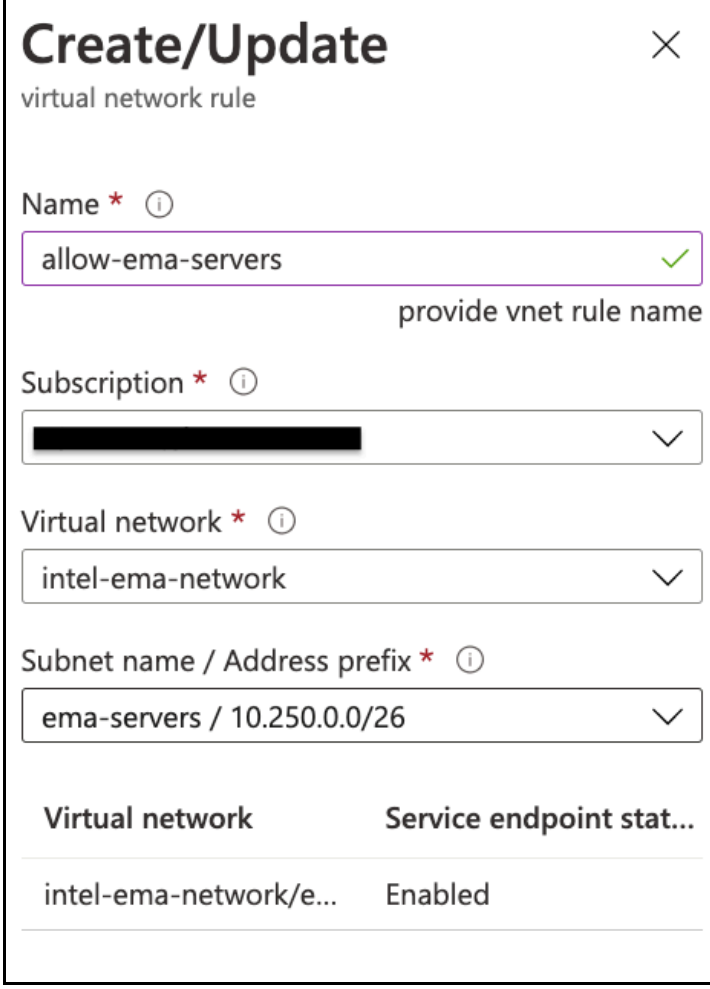
Clique no botão **Review + create**.

Analise as informações na tela, clique no botão **Create** e, em seguida, vá para o recurso quando ele for criado.

5.2.3 Configure o firewall do servidor SQL

	Na barra lateral do servidor SQL, na seção **Security**, selecione **Firewalls and virtual networks**.
	Na janela à direita, role para baixo e clique em **Add existing virtual network**.

5.2.3.1 Forneça um nome para a regra e selecione a sub-rede e rede existentes



Insira os detalhes da regra da rede virtual conforme abaixo:

- **Name**: insira um nome exclusivo.
  Exemplo: *allow-ema-servers*
- **Virtual network**: certifique-se de que a rede virtual que você criou anteriormente está selecionada.
- **Subnet name / Address prefix**: certifique-se de que a sub-rede criada anteriormente está selecionada.

Clique no botão **OK**.

6 Conjunto de disponibilidade (apenas servidor distribuído)

Um conjunto de disponibilidade é um agrupamento lógico de máquinas virtuais que informa ao Azure para garantir que elas sejam executadas em vários servidores físicos, racks de computação, unidades de armazenamento e comutadores de rede. O propósito é que, caso ocorra uma falha de hardware ou software, apenas um subconjunto de suas VMs (máquinas virtuais) seja afetado e sua solução geral permaneça operacional.

Siga o procedimento abaixo para criar um conjunto de disponibilidade, para que possamos atribuí-lo às nossas VMs quando forem criadas mais tarde.

Se estiver implantando apenas um servidor único, você pode ignorar esta seção.

Para obter mais informações sobre conjuntos de disponibilidade, acesse os seguintes links:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets

6.1 Crie o conjunto de disponibilidade

1. Use a barra de pesquisa no topo da tela para pesquisar sobre **Availability sets** e, em seguida, clique no item de lista exibido.
2. Clique no botão **Add**.
3. Insira as informações básicas conforme abaixo.
    a. **Resource group**: selecione o grupo de recursos que você criou anteriormente.

b. **Name**: insira um nome exclusivo.
Exemplo: *ema-servers*

c. **Region**: confirme se essa é a região onde você deseja implantar seus recursos.

4. Clique no botão Review + create.

5. Analise as informações na tela e clique no botão Create.

7 Implantação do balanceador de carga (apenas servidor distribuído)

Um Azure 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. A investigação de integridade do balanceador de carga monitora uma dada porta em cada VM e distribui apenas o tráfego para uma VM operacional.

Criaremos o balanceador de carga com apenas a configuração de front-end definida inicialmente. Quando criarmos nossas máquinas virtuais posteriormente, anexaremos essas VMs ao back-end do balanceador de carga. O balanceador de carga terá os endereços IP de front-end separados para tráfego web e para o tráfego swarm.

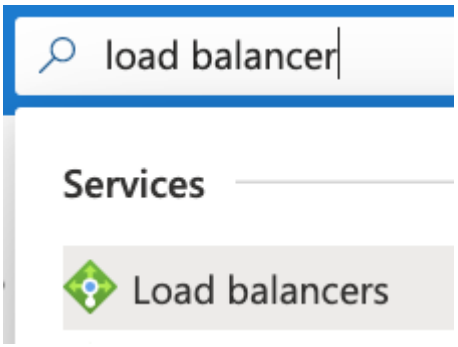
Após as VMs terem sido anexadas ao balanceador de carga, retornaremos à configuração do balanceador de carga para configurar as verificações de integridade e as regras de encaminhamento, a fim de direcionar o tráfego de entrada para as portas de VM de back-end apropriadas.

Se estiver implantando apenas um servidor único, você pode ignorar esta seção.

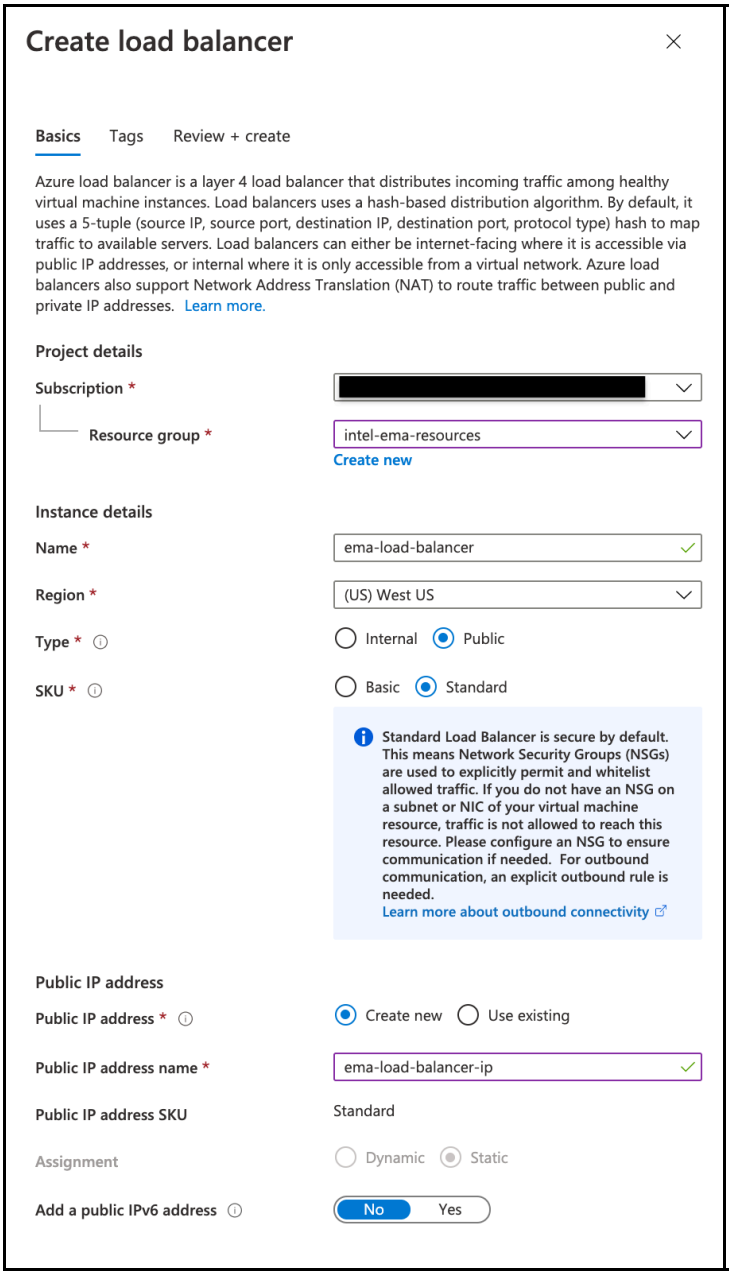
Para obter mais informações sobre o balanceamento de carga nas VMs do Windows*, acesse o seguinte link:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-load-balancer

7.1 Crie o balanceador de carga

7.1.1 Navegue até o serviço de balanceadores de carga

	Use a barra de pesquisa no topo da tela para pesquisar sobre **Load balancers** e, em seguida, clique no item de lista exibido.

7.1.2 Informações básicas do balanceador de carga



Clique no botão **Add**.

Insira as informações básicas conforme abaixo.

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Name**: insira um nome exclusivo.
  Exemplo: *ema-load-balancer*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.
- **Type**: *Public*
- **SKU**: *Standard*
- **Public IP address**: *Create new*
- **Public IP address name**: *ema-web-lb-ip*

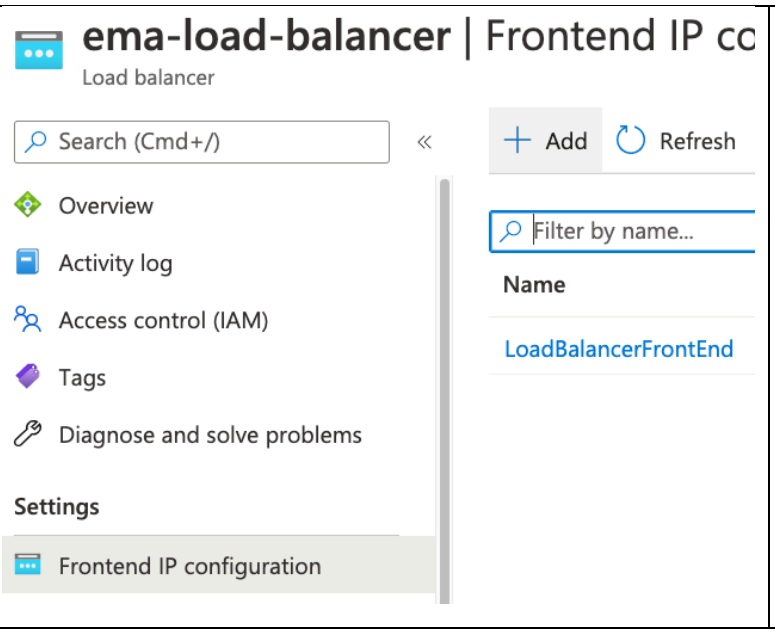
Clique no botão **Review + create**.

Analise as informações na tela e clique no botão **Create**.

Uma vez que a implantação foi bem-sucedida, clique no botão **Go to Resource**.

7.2 Atualize a configuração do balanceador de carga

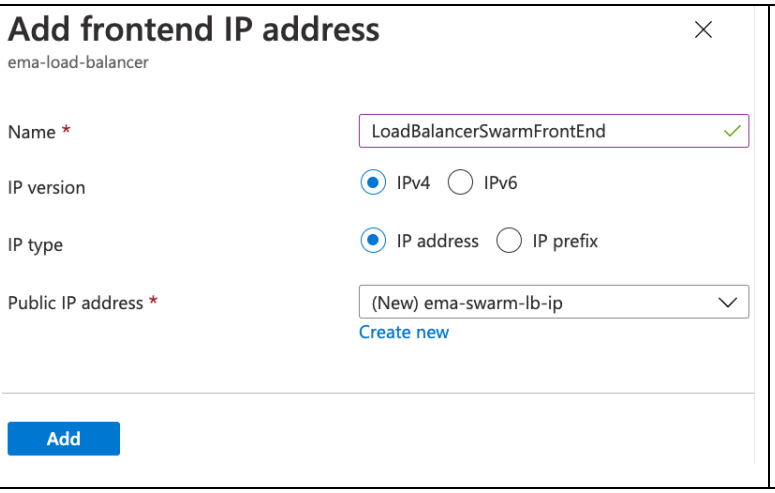
7.2.1 Adicione a segunda configuração do front-end



Na barra lateral, em **Settings**, clique em **Frontend IP Configuration**

Clique no botão **Add**.

7.2.2 Configure o segundo front-end

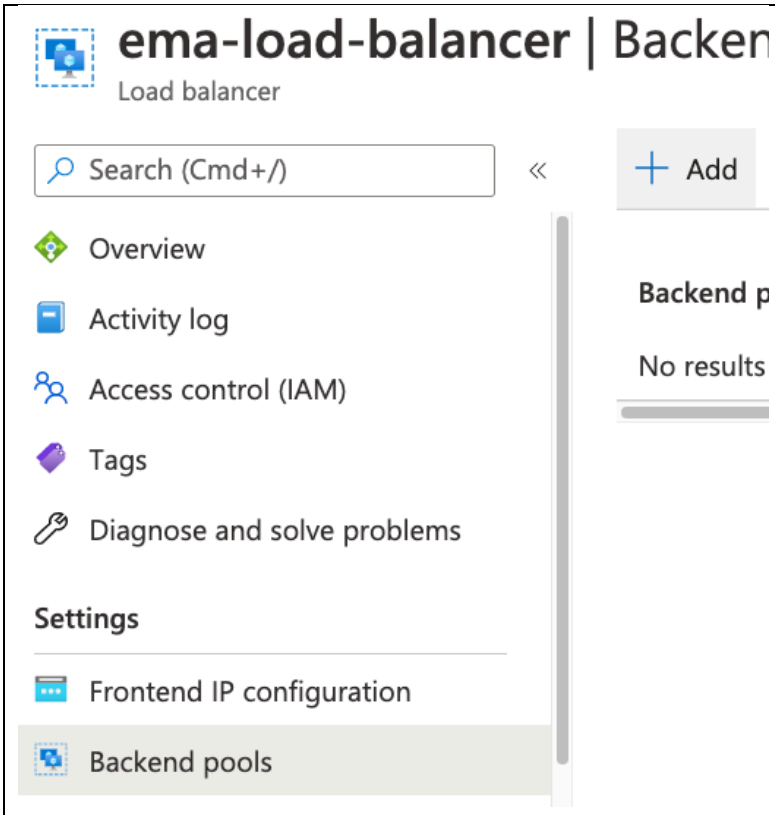


Insira um nome exclusivo para o front-end.
Exemplo:

Para “Public IP address”, clique no link **Create new** e dê um nome para o endereço IP.
Exemplo: *ema-swarm-lb-ip*

Clique no botão **Add**.

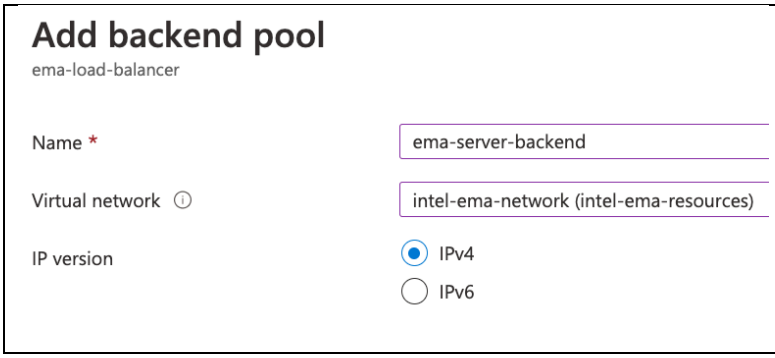
7.2.3 Adicione um pool de back-end



Na barra lateral, em **Settings**, clique em **Backend pools**.

Clique no botão **Add**.

Configure o pool de back-end



Insira um nome exclusivo para o pool de back-end. Exemplo: *ema-server-backend*

Selecione sua rede virtual existente.

Clique no botão **Add**.

Este pool de back-end estará disponível para seleção mais tarde, quando criarmos nossas máquinas virtuais.

8 Implantação da máquina virtual

8.1 Visão geral

As máquinas virtuais (VM) do Azure oferecem a flexibilidade de 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.

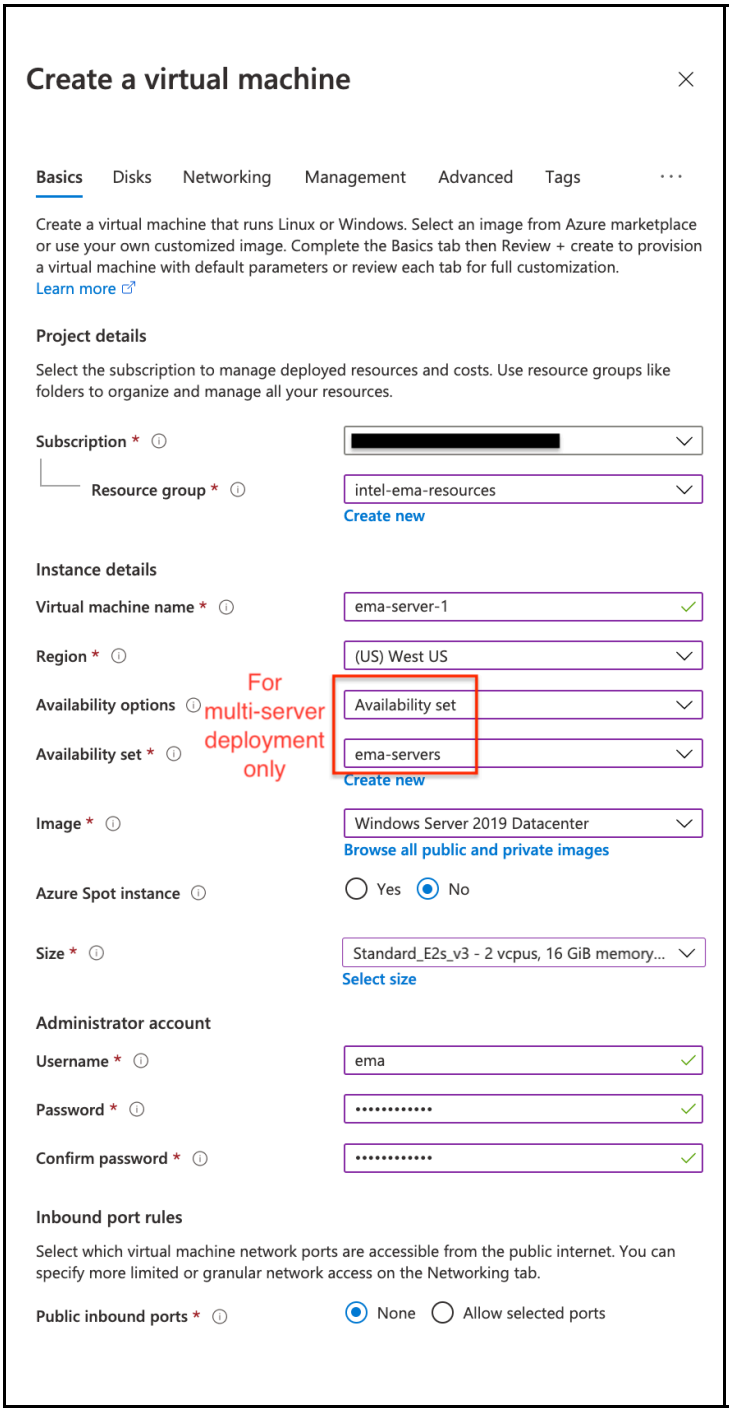
Você decidirá a quantidade de CPU, memória e armazenamento a ser alocada à VM no momento da criação, mas você pode aumentar todas as opções posteriormente ou reduzir a quantidade de CPU e memória para otimizar a VM para a carga de trabalho a fim de reduzir os custos.

Para implantações de servidor distribuído, você pode pular algumas etapas adicionais incluídas no procedimento abaixo para implantações de servidor único. Estas incluem a criação de uma segunda VM, associação das VMs a um conjunto de disponibilidade, e anexar as VMs ao balanceador de carga.

Para obter mais informações sobre as máquinas virtuais baseadas no Windows, acesse os seguintes links:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/overview

8.2 Criar máquina(s) virtual(is)

8.2.1 Adicione uma VM e configure o básico



Use a barra de pesquisa no topo da tela para pesquisar sobre **Virtual machines** e, em seguida, clique no item de lista exibido.

Clique no botão **Add**.

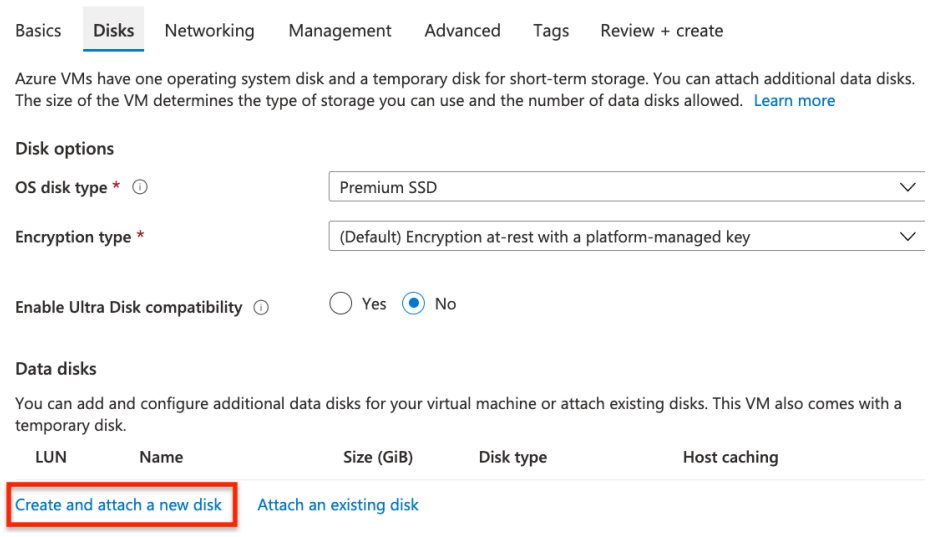
Configure os elementos básicos da VM conforme abaixo:

- **Resource group**: selecione o grupo de recursos que você criou anteriormente.
- **Name**: insira um nome exclusivo.
  Exemplo: *ema-server-1*
- **Region**: confirme se essa é a região onde você deseja implantar seus recursos.
- **Availability options**:
  (para servidor único apenas) *No infrastructure redundancy required*
  (para servidor distribuído apenas) *Availability set*
- **Availability set** (para servidor distribuído apenas): escolha o conjunto de disponibilidade que você criou anteriormente.
- **Image**: escolha a imagem mais recente suportada pelo Windows Server
- **Size**: escolha o tamanho da máquina.
  Recomendado: *Standard_E2sv3 - 2 vcpus, 16 GiB memory*
- **Azure Spot instance**: *No*
- Forneça informações da conta de administrador
- **Public inbound ports**: *None*

Clique no botão **Next: Disks**.

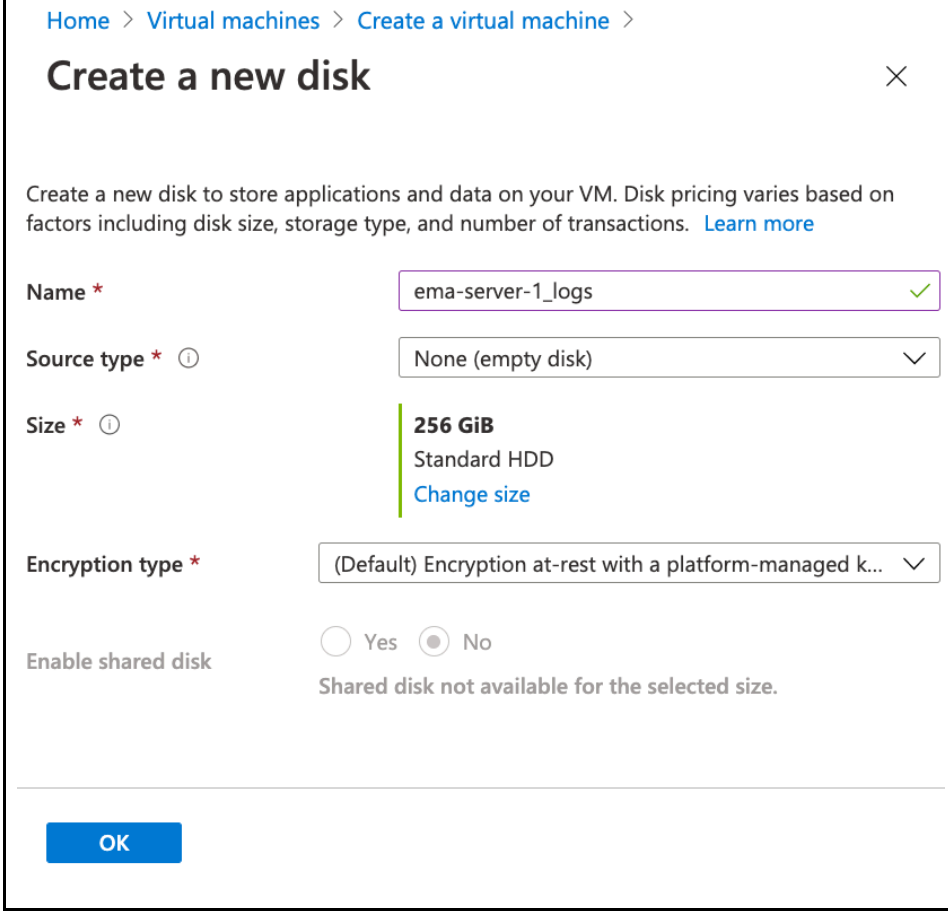
8.2.2 Adicione um disco de dados para o armazenamento de arquivos de log

8.2.2.1 Crie e anexe o novo disco



Clique no link **Create and attach a new disk**.

8.2.2.2 Configure os detalhes do novo disco

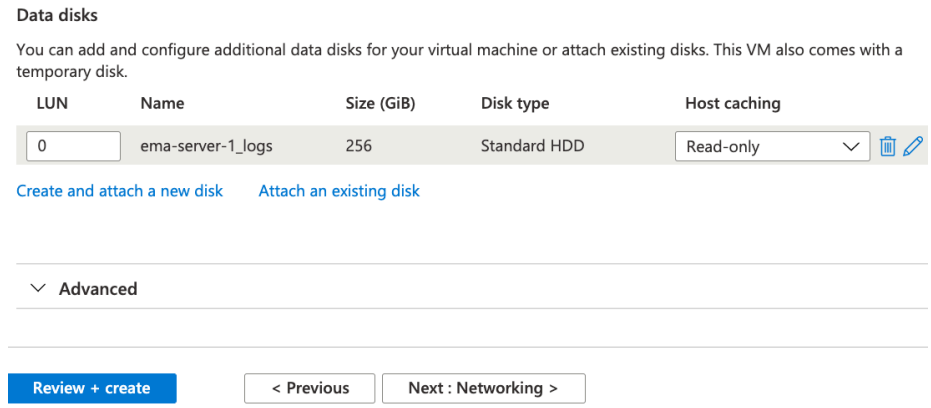


Configure os detalhes do disco conforme abaixo.

- **Name**: aceite o nome padrão ou insira um nome exclusivo de disco.
- **Source type**: *None (empty disk)*
- **Size**: clique no link Change size para definir o tipo e o tamanho de disco. Sugerimos uma unidade de disco rígido padrão de 256 GiB.
- **Encryption type**: Default

Clique no botão **OK**.

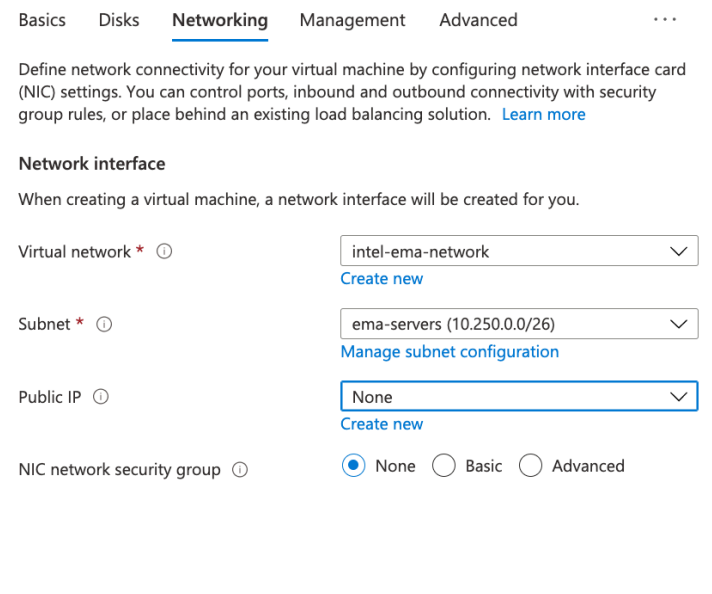
8.2.2.3 Analise a lista dos discos de dados



Analise as informações para o disco de dados e, em seguida, clique no botão **Next: Networking**.

Nota: depois que a VM for inicializada, você precisará usar o utilitário Gerenciamento de Disco do Windows para inicializar, formatar e instalar o disco de armazenamento.

8.2.3 Configure a interface de rede da VM



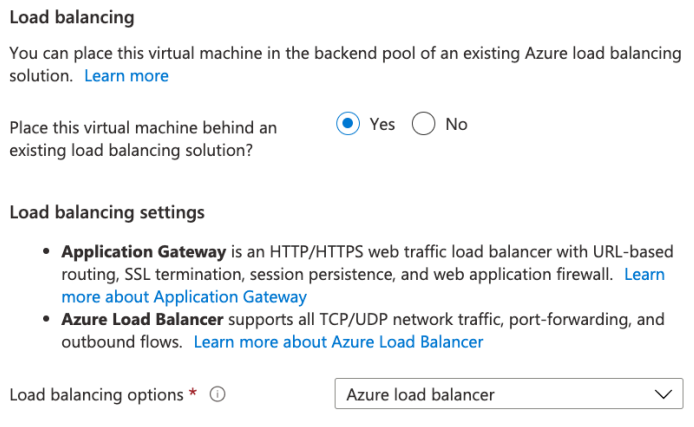
Selecione a guia de rede e configure a interface de rede conforme abaixo:

- **Virtual network**: selecione a VPC que você criou anteriormente.
- **Subnet**: certifique-se de que a sub-rede criada anteriormente está selecionada.
- **Public IP**: *None*
- **NIC network security group**: *None*

Se esta for uma implantação de servidor único, clique no botão **Review + create**, analise as informações na tela e, em seguida, clique no botão **Create**.

Se esta for uma implantação de servidor distribuído, continue a configuração de rede na próxima etapa.

8.2.4 Configure a opção de balanceamento de carga da VM (apenas servidor distribuído)



Configure o **Load balancing** na metade inferior da tela de rede.

- **Place this virtual machine behind an existing load balancing solution**: *Yes*
- **Load balancing options**: *Azure load balancer*
- **Select a load balancer**: selecione o balanceador de carga que você criou anteriormente.
- **Select a backend pool:** selecione o pool de back-end que você criou anteriormente.

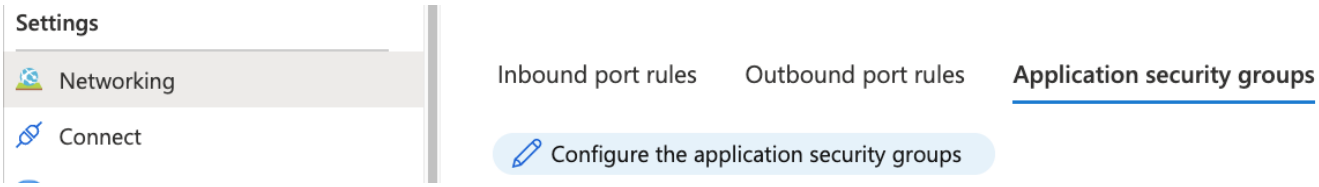
Clique no botão **Review + create**, analise as informações na tela e, em seguida, clique no botão **Create** para terminar de criar a VM.

8.2.5 Crie máquinas virtuais adicionais (apenas servidor distribuído)

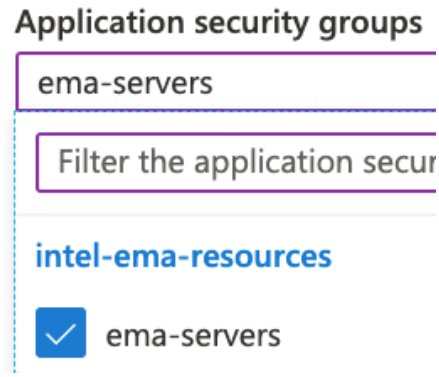
Para uma implantação de servidor distribuído, crie pelo menos uma VM adicional após o procedimento anterior.

8.2.6 Associe a(s) máquina(s) virtual(is) com o grupo de segurança da aplicação

Para cada VM que você criou, sob a categoria **Settings** na barra lateral, selecione **Networking** e a guia **Application security groups**. Em seguida, clique em **Configure the application security groups**.



Selecione o grupo de segurança da aplicação criado anteriormente.

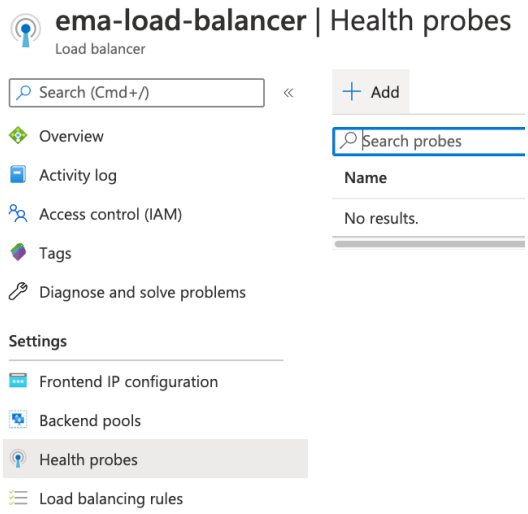


9 Continue a configuração do balanceador de carga (apenas servidor distribuído)

Agora que as máquinas virtuais foram criadas, podemos voltar à configuração do balanceador de carga para configurar as verificações de integridade e as regras de encaminhamento, a fim de direcionar o tráfego de entrada para as portas de VM de back-end apropriadas.

9.1 Configure as investigações de integridade

9.1.1 Acesse a tela de investigações de integridade

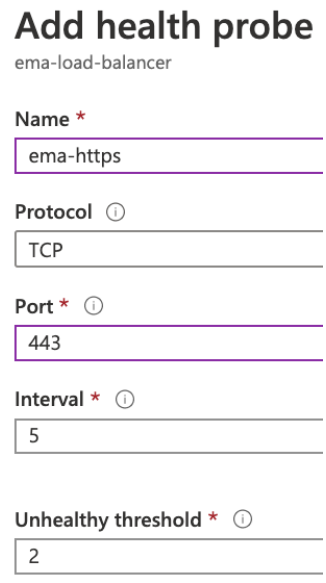


Use a barra de pesquisa no topo da tela para pesquisar sobre **Load balancers** e, em seguida, clique no item de lista exibido.

Clique no balanceador de carga criado anteriormente.

Em **Settings** na barra lateral, clique em **Health probes**.

9.1.2 Adicione investigações de integridade para tráfego Web

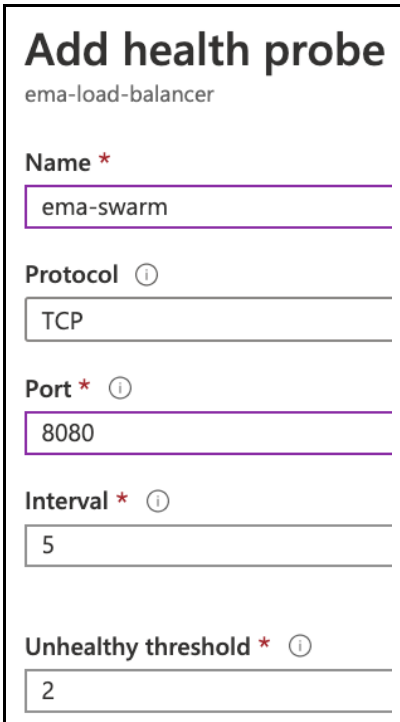


Clique no botão **Add** e configure a investigação de integridade conforme abaixo.

- **Name**: insira um nome exclusivo.
  Exemplo: *ema-https*
- **Protocol**: *TCP*
- **Port**: *443*

Clique no botão **OK**.

9.1.3 Adicione investigações de integridade para tráfego Swarm

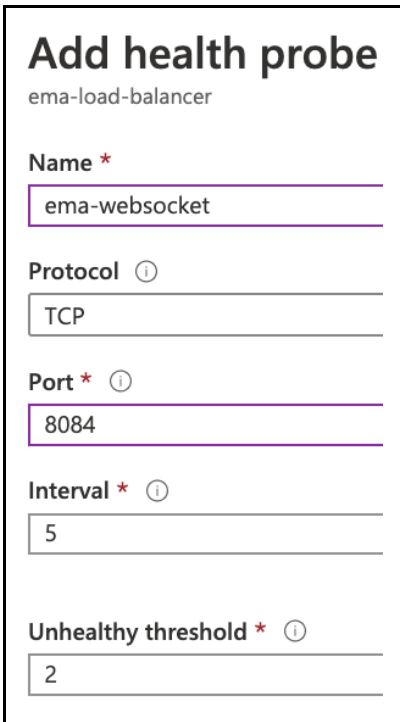


Clique no botão **Add** e configure a investigação de integridade conforme abaixo.

- **Name**: insira um nome exclusivo.
  Exemplo: *ema-swarm*
- **Protocol**: *TCP*
- **Port**: *8080*

Clique no botão **OK**.

9.1.4 Adicione investigações de integridade para tráfego Websocket



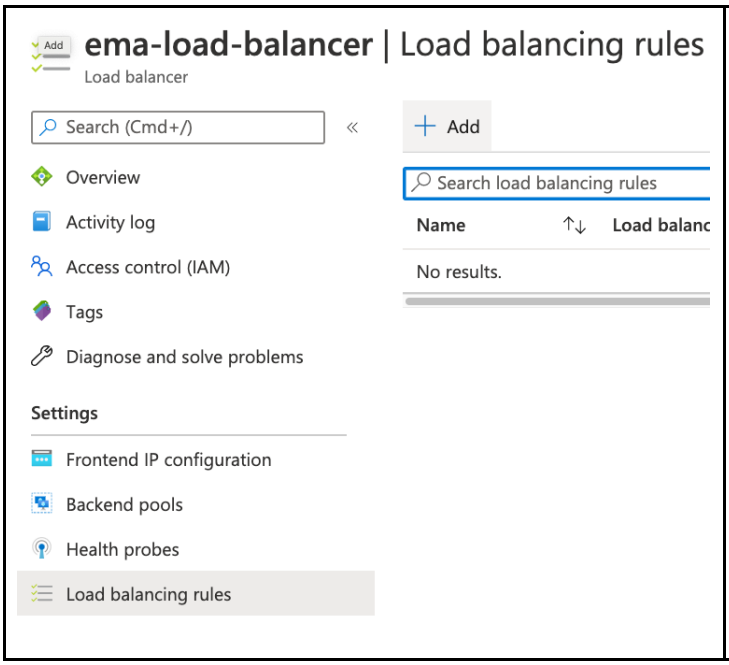
Clique no botão **Add** e configure a investigação de integridade conforme abaixo.

- **Name**: insira um nome exclusivo.
  Exemplo: *ema-websocket*
- **Protocol**: *TCP*
- **Port**: *8084*

Clique no botão **OK**.

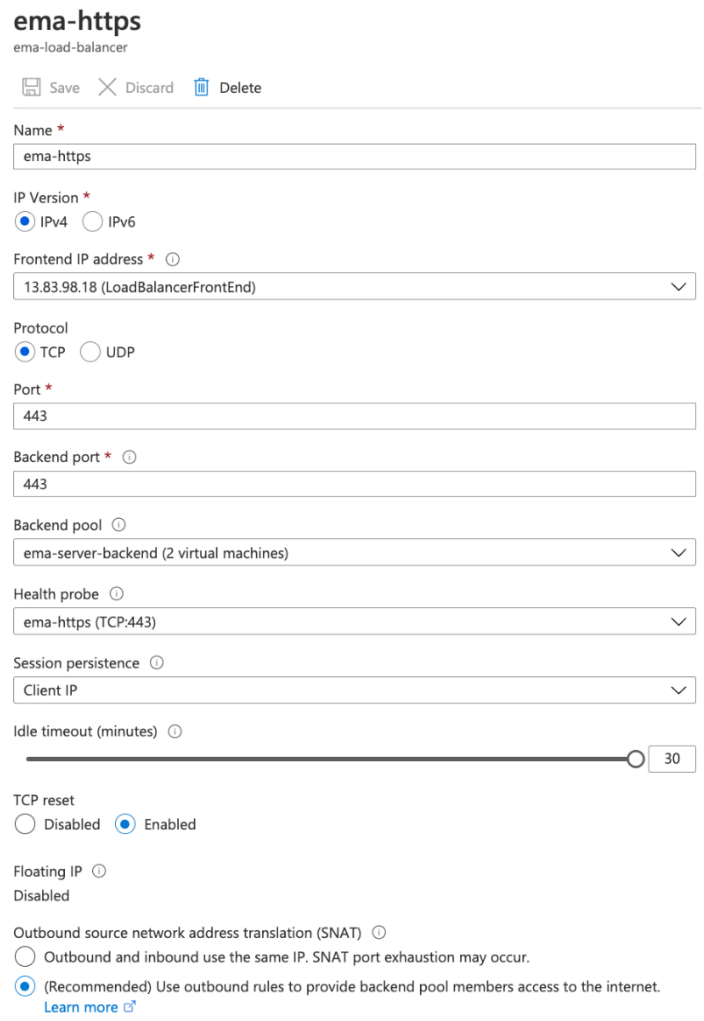
9.2 Configure as regras de balanceamento de carga

9.2.1 Acesse a tela de regras de balanceamento de carga



Selecione Load balancing rules na barra lateral da tela de detalhes do balanceador de carga.

9.2.2 Crie uma regra para tráfego Web



Clique no botão **Add** e configure a regra conforme abaixo.

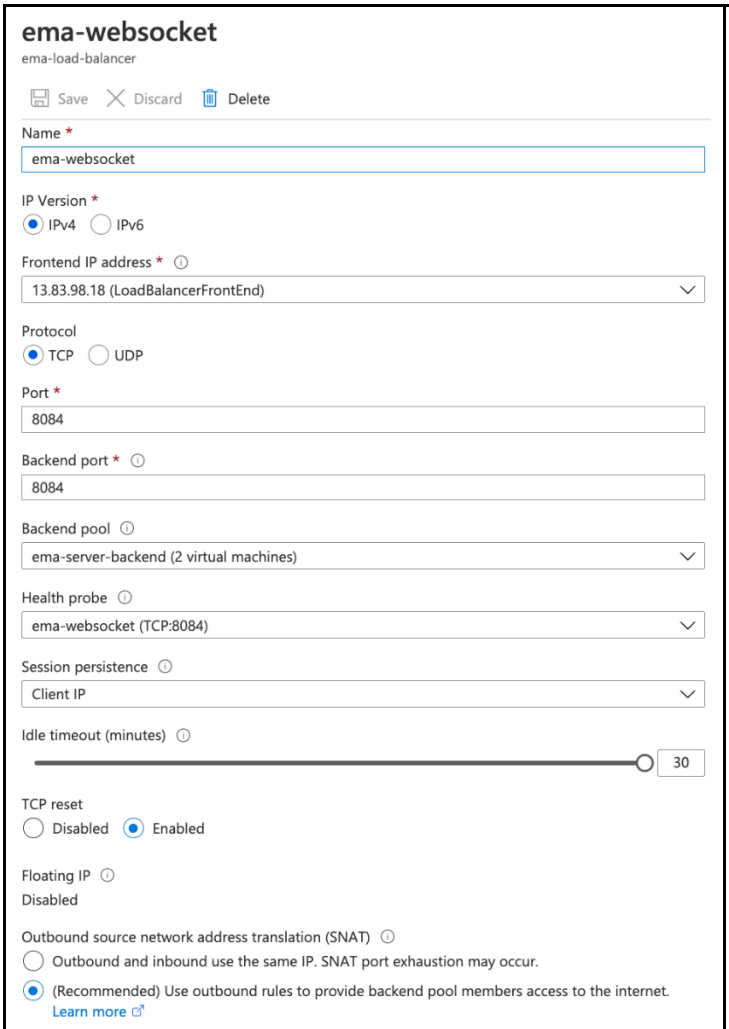
- **Name**: *ema-https*
- **Frontend IP address**: selecione o front-end do balanceador de carga usado para tráfego web.
  Exemplo: *LoadBalancerFrontEnd*
- **Protocol**: *TCP*
- **Port**: *443*
- **Backend Port**: *443*
- **Backend pool**: selecione o pool de back-end que você criou anteriormente.
  Exemplo: *ema-server-backend*
- **Health probe**: selecione a investigação de integridade da porta 443 que você criou anteriormente.
  Exemplo: *ema-https*
- **Session persistence**: *Client IP*
- **Idle timeout (minutes)**: defina para o valor máximo (30)
- **TCP reset**: *Enabled*
- **Outbound source network address translation**: *Use outbound rules to provide backend pool members access to the internet.*

Clique no botão **OK**.

9.2.3 Crie uma regra para tráfego Websocket

Clique no botão **Add** e configure a regra conforme abaixo.

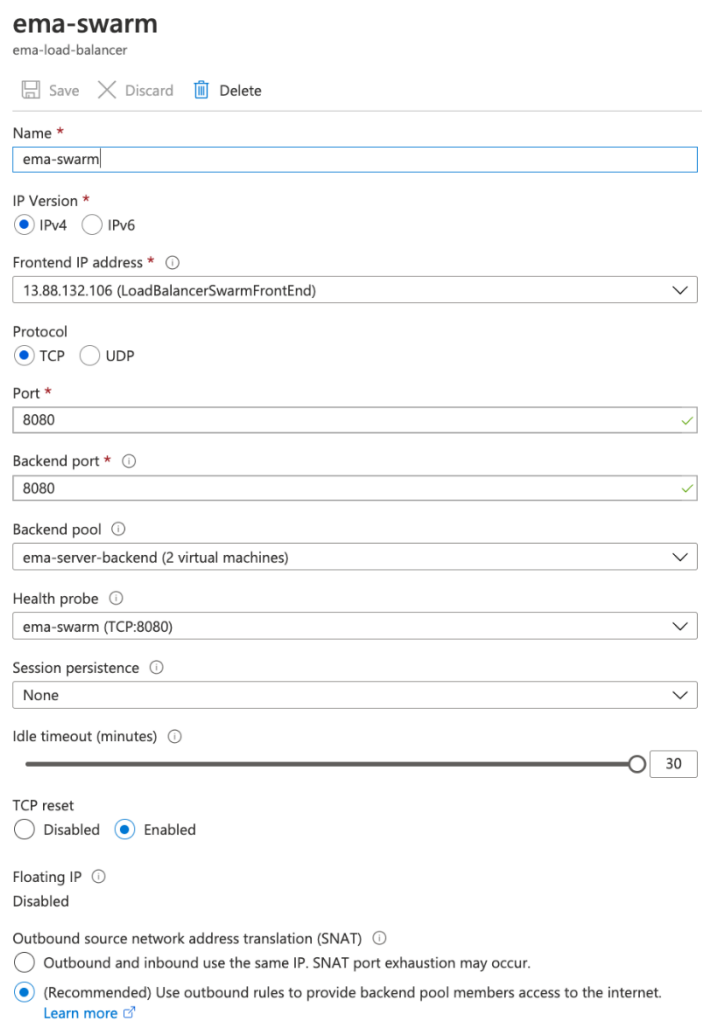
- **Name**: *ema-websocket*
- **Frontend IP address**: selecione o front-end do balanceador de carga usado para tráfego web.
  Exemplo: *LoadBalancerFrontEnd*
- **Protocol**: *TCP*
- **Port**: *8084*
- **Backend Port**: *8084*
- **Backend pool**: selecione o pool de back-end que você criou anteriormente.
  Exemplo: *ema-server-backend*



- **Health probe**: selecione a investigação de integridade da porta 8084 que você criou anteriormente. Exemplo: *ema-websocket*
- **Session persistence**: *Client IP*
- **Idle timeout (minutes)**: defina para o valor máximo (30)
- **TCP reset**: *Enabled*
- **Outbound source network address translation**: *Use outbound rules to provide backend pool members access to the internet.*

Clique no botão **OK**.

9.2.4 Crie uma regra para tráfego Swarm



Clique no botão **Add** e configure a regra conforme abaixo.

- **Name**: *ema-swarm*
- **Frontend IP address**: escolha o front-end criado para o tráfego swarm durante a configuração inicial do balanceador de carga.
  Exemplo: *LoadBalancerSwarmFrontEnd.*
- **Protocol**: *TCP*
- **Port**: *8080*
- **Backend Port**: *8080*
- **Backend pool**: selecione o pool de back-end que você criou anteriormente.
  Exemplo: *ema-server-backend*
- **Health probe**: selecione a investigação de integridade da porta 8080 que você criou anteriormente.
  Exemplo: *ema-swarm*
- **Session persistence**: *None*
- **Idle timeout (minutes)**: defina para o valor máximo (30)
- **TCP reset**: *Enabled*
- **Outbound source network address translation**: *Use outbound rules to provide backend pool members access to the internet.*

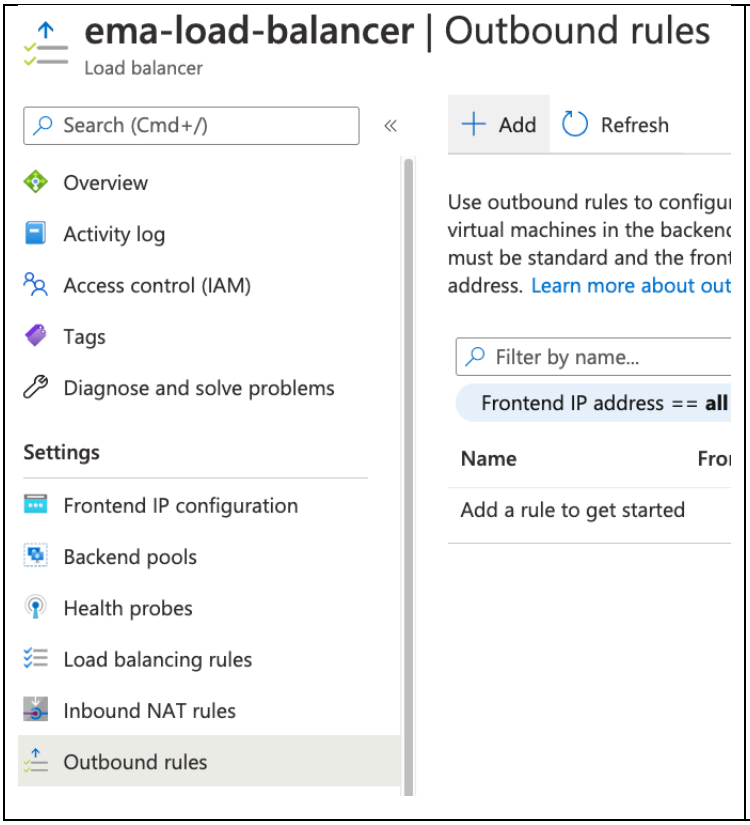
Clique no botão **OK**.

9.3 Crie a regra de saída para o tráfego de back-end do NAT

Como nossas máquinas virtuais não têm endereços de IP públicos, precisamos usar a conversão de endereços de rede de origem (SNAT) para seu tráfego de saída para a internet. Em vez de implantar um gateway de NAT do Azure, nosso balanceador de carga existente pode fornecer este recurso usando seus endereços IP de front-end como endereços IP de fonte para o tráfego de saída.

Para obter mais informações sobre este tópico, acesse o seguinte link: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections.

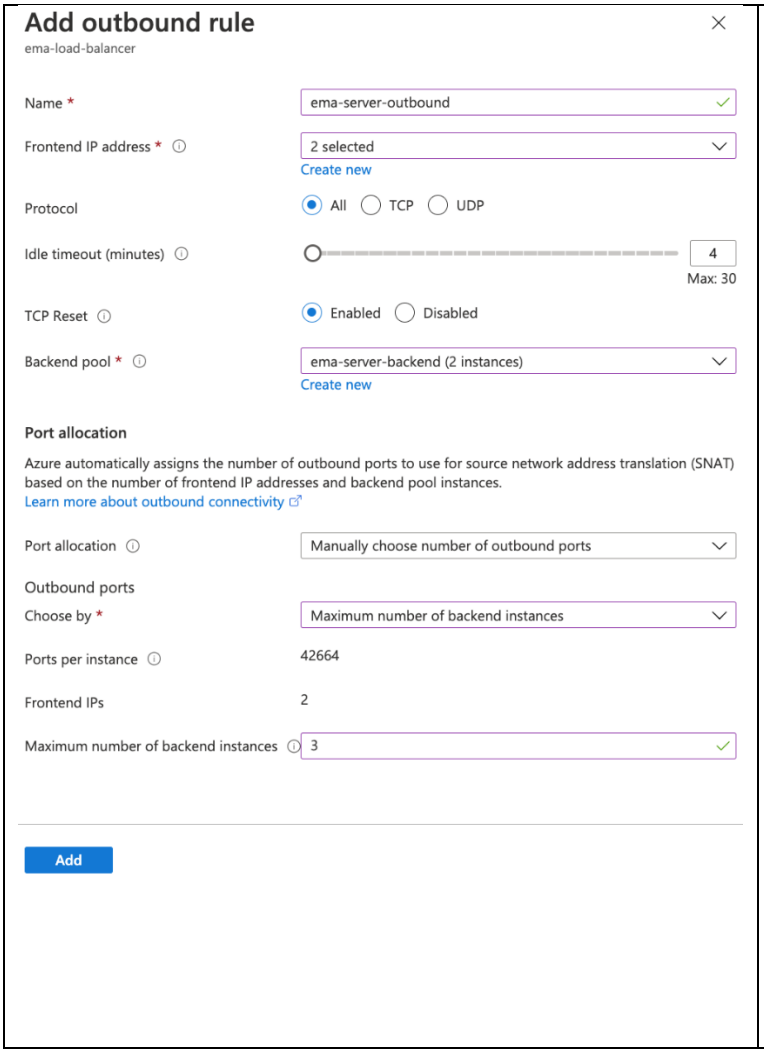
9.3.1 Adicione uma regra de saída



Na tela do balanceador de carga, na seção “Settings” da barra lateral, clique em **Outbound rules**.

Clique no botão **Add**.

9.3.2 Configure a regra de saída

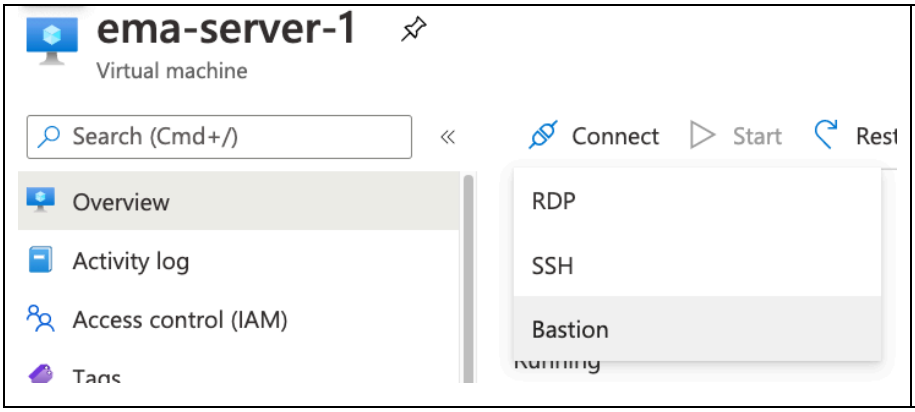


Configure a regra de saída conforme abaixo.

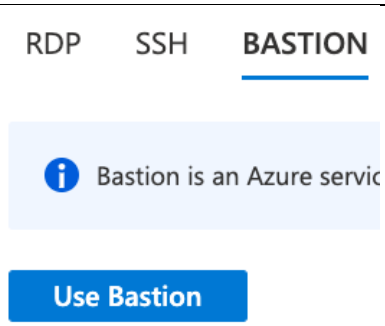
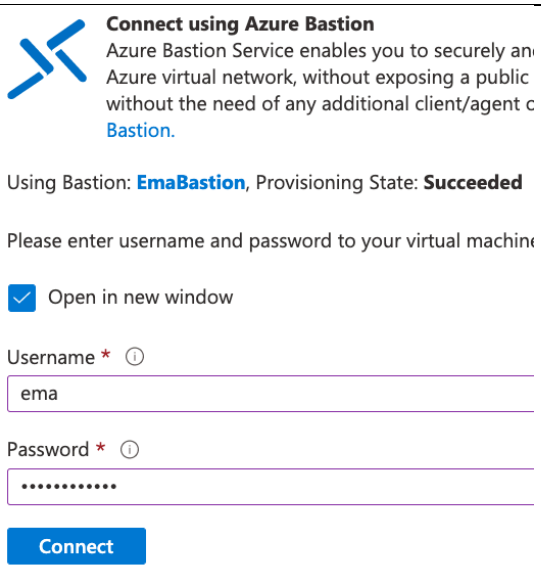
- **Name**: insira um nome exclusivo.
  Exemplo: *ema-server-outbound*
- **Frontend IP address**: selecione todos os endereços IP disponíveis no menu suspenso.
- **Protocol**: *All*
- **TCP Reset**: *Enabled*
- **Backend Pool**: selecione o pool de back-end que foi criado anteriormente.
  Exemplo: *ema-server-backend*
- **Port allocation**: *Manually choose number of outbound ports*
- **Outbound ports Choose by**: *Maximum number of backend instances*
- **Maximum number of backend instances**: para cada endereço IP de front-end, existem 64.000 portas disponíveis para uso no SNAT. Ao escolher um número aqui, o pool total de portas será dividido por esse número, de modo que cada instância de back-end terá um número igual de portas disponível.
  Como este guia de implantação assume que estamos implantando duas VMs, vamos inserir **3** aqui para dar espaço para adicionar outra VM, se necessário.

Clique no botão **Add**.

10 Conecte as máquinas virtuais usando o Azure Bastion



Para fazer login em qualquer uma das máquinas virtuais, acesse a tela “Overview” da VM, clique no botão **Connect** e então selecione **Bastion**.

	Clique no botão **Use Bastion**.
	Insira as credenciais da VM e clique no botão **Connect**. Uma janela do navegador será aberta, com sua sessão de RDP para essa VM.

11 Apêndice A — Notas sobre a integração do Active Directory*

Há várias maneiras de integrar o Active Directory* ao Microsoft Azure 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. Os links para leitura adicional são fornecidos aqui.

Documentação do Azure Active Directory

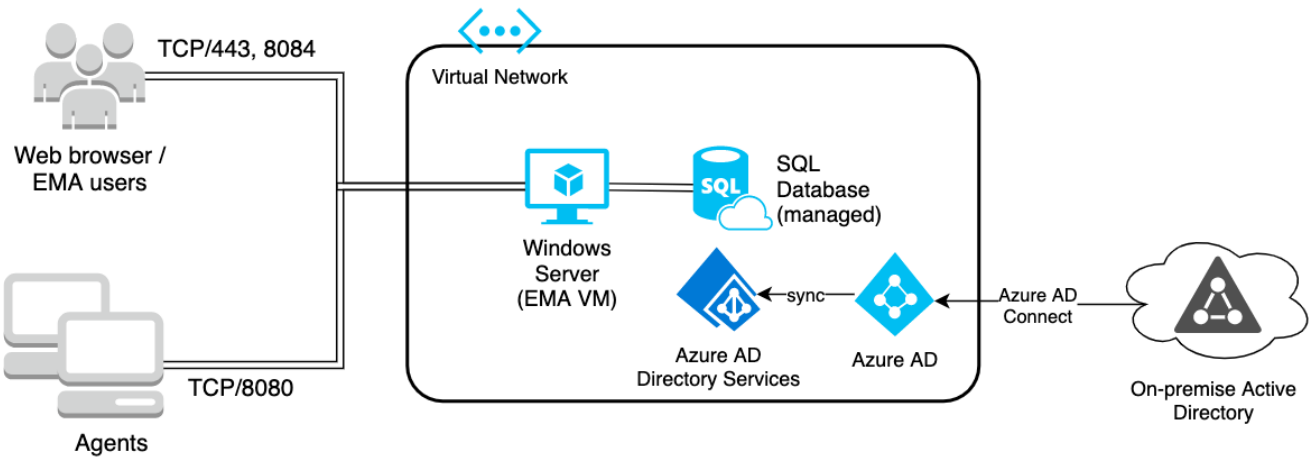
Documentação do Azure AD Domain Services

Compare os serviços baseados no Active Directory no Azure

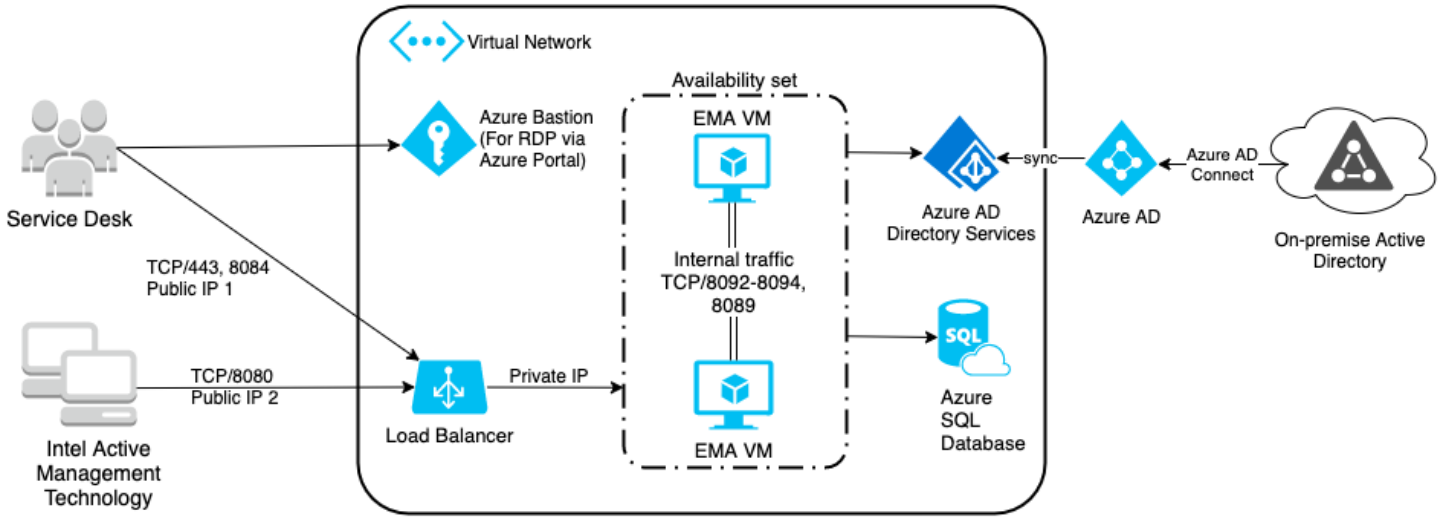
Sincronização do Azure AD Connect: compreenda e personalize a sincronização

11.1 Diagrama de arquitetura de alto nível com a integração do Active Directory

11.1.1 Implantação de servidor único



11.1.2 Implantação de servidor distribuído



11.2 Usando o Azure AD Connect para ampliar o Active Directory para a nuvem

- ❑ Implemente um recurso do Azure AD Directory Services (AADDS) para que você possa associar sua(s) máquina(s) virtual(is) ao domínio do AD.
  - ❑ Durante este processo, você precisará criar uma sub-rede dedicada para os AADDS.
  - ❑ Adicione um usuário do seu Azure Active Directory que terá privilégios para administrar este domínio gerenciado.
  - ❑ Pode demorar uma hora ou mais para concluir a instalação. Após a instalação ter sido concluída, você precisará atualizar as configurações do servidor DNS para que a sua rede virtual use os endereços IP do servidor AD DS.

- ❑ Implemente o AD Connect em seu ambiente local para sincronizar os seus usuários e hashes de senha com seu Azure Active Directory.
    - ❑ Baixe e instale o software do AD Connect para um servidor associado a domínios em sua rede.
    - ❑ Use as configurações expressas.
    - ❑ Insira suas credenciais para o Azure AD e o Azure AD DS.
    - ❑ Certifique-se de que seu nome de domínio corresponda a um domínio personalizado que você adicionou e verificou anteriormente no Azure AD.
    - ❑ Depois que a configuração estiver concluída, uma sincronização de 30 minutos será realizada em segundo plano. Leia a documentação da Microsoft para obter mais informações sobre como isso funciona.
    - ❑ Local para download do Azure AD Connect: Baixe o Microsoft Azure Active Directory Connect no Centro de download oficial da Microsoft.
    - ❑ Pré-requistos do Azure AD Connect: Azure AD Connect: pré-requisitos e hardware.
- ❑ Quando esta infraestrutura estiver em funcionamento, você pode seguir as instruções no link seguinte para associar uma VM ao domínio: Associe uma VM do servidor do Windows a um domínio gerenciado do Azure AD Domain Services.