

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>.

© 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	Como navegar pelo console do Azure	1
1.2.1	Menu de serviços	1
1.2.2	Expansão do menu de serviços	1
1.2.3	Busca de um serviço por nome	2
1.3	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	Implantação de grupos de recursos	3
3.1	Visão geral dos grupos de recursos	3
3.2	Criar um Grupo de recursos	4
3.2.1	Selecione o serviço de grupos de recursos	4
3.2.2	Adicione um grupo de recursos	4
3.2.3	Configure o grupo de recursos	5
3.2.4	Analise e crie	5
4	Implantação de rede	5
4.1	Visão geral	5
4.2	Crie uma rede virtual	6
4.2.1	Navegue até o serviço de redes virtuais	6
4.2.2	Adicione uma rede virtual	6
4.2.3	Configure os detalhes básicos da Rede virtual	7
4.2.4	Configure o espaço de endereço IPv4	7
4.2.5	Adicione sub-rede para servidores do Intel EMA	8
4.2.6	Habilite o Azure Bastion	8
4.2.7	Analise	9
4.3	Grupo de segurança da aplicação (ASG)	9
4.3.1	Navegue até o serviço de grupos de segurança da aplicação	9
4.3.2	Adicione um grupo de segurança da aplicação	9
4.3.3	Configure o Grupo de segurança da aplicação (ASG)	10
4.4	Grupos de segurança de rede	10
4.4.1	Crie o grupo de segurança de rede para a sub-rede de servidores do Intel EMA	10
4.4.2	Configure o grupo de segurança de rede	12
4.4.3	Analise	17
4.4.4	Associe o grupo de segurança de rede à sua sub-rede	17
4.4.5	Crie o grupo de segurança de rede para a sub-rede Azure Bastion	18
4.4.6	Configure o grupo de segurança de rede	19
4.4.7	Configure as regras de segurança de saída	21
4.4.8	Associe o grupo de segurança de rede com a sua sub-rede do Azure Bastion	24
5	Implantação do servidor SQL	25
5.1	Visão geral	25
5.2	Crie o servidor SQL	25
5.2.1	Adicione um novo servidor SQL	25
5.2.2	Configure os detalhes básicos para o servidor SQL	26
5.2.3	Configure o firewall do servidor SQL	27

6	Conjunto de disponibilidade (apenas servidor distribuído)	28
6.1	Crie o conjunto de disponibilidade	28
7	Implantação do balanceador de carga (apenas servidor distribuído)	29
7.1	Crie o balanceador de carga	29
7.1.1	Navegue até o serviço de balanceadores de carga	29
7.1.2	Informações básicas do balanceador de carga	30
7.2	Atualize a configuração do balanceador de carga	31
7.2.1	Adicione a segunda configuração do front-end	31
7.2.2	Configure o segundo front-end	31
7.2.3	Adicione um pool de back-end	32
8	Implantação da máquina virtual	32
8.1	Visão geral	32
8.2	Criar máquina(s) virtual(is)	33
8.2.1	Adicione uma VM e configure o básico	33
8.2.2	Adicione um disco de dados para o armazenamento de arquivos de log	34
8.2.3	Configure a interface de rede da VM	35
8.2.4	Configure a opção de balanceamento de carga da VM (apenas servidor distribuído)	36
8.2.5	Crie máquinas virtuais adicionais (apenas servidor distribuído)	36
8.2.6	Associe a(s) máquina(s) virtual(is) com o grupo de segurança da aplicação	36
9	Continue a configuração do balanceador de carga (apenas servidor distribuído)	37
9.1	Configure as investigações de integridade	37
9.1.1	Acesse a tela de investigações de integridade	37
9.1.2	Adicione investigações de integridade para tráfego Web	37
9.1.3	Adicione investigações de integridade para tráfego Swarm	38
9.1.4	Adicione investigações de integridade para tráfego Websocket	38
9.2	Configure as regras de balanceamento de carga	39
9.2.1	Acesse a tela de regras de balanceamento de carga	39
9.2.2	Crie uma regra para tráfego Web	40
9.2.3	Crie uma regra para tráfego Websocket	40
9.2.4	Crie uma regra para tráfego Swarm	42
9.3	Crie a regra de saída para o tráfego de back-end do NAT	42
9.3.1	Adicione uma regra de saída	43
9.3.2	Configure a regra de saída	44
10	Conecte as máquinas virtuais usando o Azure Bastion	44
11	Apêndice A — Notas sobre a integração do Active Directory*	45
11.1	Diagrama de arquitetura de alto nível com a integração do Active Directory	46
11.1.1	Implantação de servidor único	46
11.1.2	Implantação de servidor distribuído	46
11.2	Usando o Azure AD Connect para ampliar o Active Directory para a nuvem	46

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.

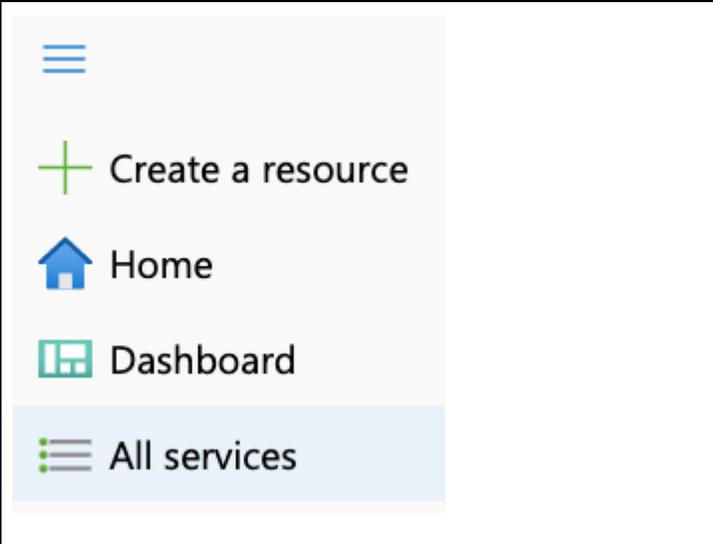
Com serviços totalmente gerenciados, como o servidor Azure SQL, você pode se concentrar em seus dados, enquanto o provedor de nuvem gerencia todo o hardware e software subjacentes que oferecem o serviço. Com máquinas virtuais em execução na nuvem, você gerencia apenas o sistema operacional convidado 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

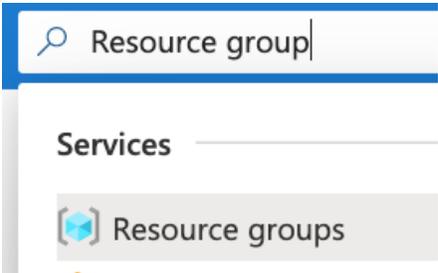
 A screenshot of the Microsoft Azure logo, which consists of a blue rectangle with a white hamburger menu icon on the left and the text "Microsoft Azure" in white on the right.	Depois de ter feito o login no portal do Microsoft Azure, em http://portal.azure.com/ , você verá um ícone de menu no canto superior esquerdo.
--	---

1.2.2 Expansão do menu de serviços

 A screenshot of the expanded Azure services menu. It shows a vertical list of items: a hamburger menu icon, a green plus sign followed by "Create a resource", a blue house icon followed by "Home", a blue dashboard icon followed by "Dashboard", and a blue hamburger menu icon followed by "All services". The "All services" item is highlighted with a light blue background.	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.
--	--

GENERAL (17) ▾	
COMPUTE (35) ▾	
NETWORKING (29) ▴	
Virtual networks	
Load balancers	
CDN profiles	

1.2.3 Busca de um serviço por nome

	<p>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.</p> <p>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.</p>
---	--

1.3 Antes de começar

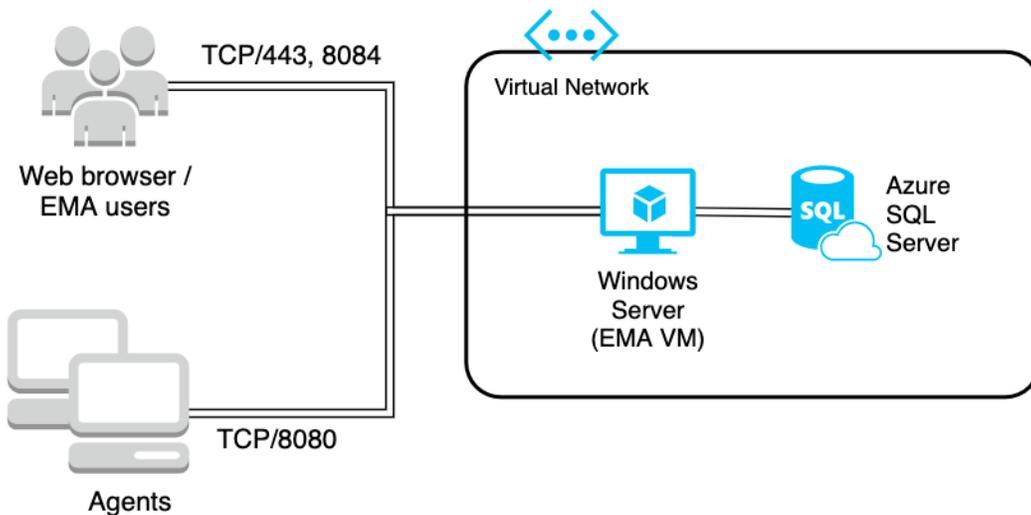
Se a sua organização já tem uma conta Azure, você deve pedir a um administrador de nuvem que lhe conceda acesso suficiente para poder criar todos os recursos listados neste guia.

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.

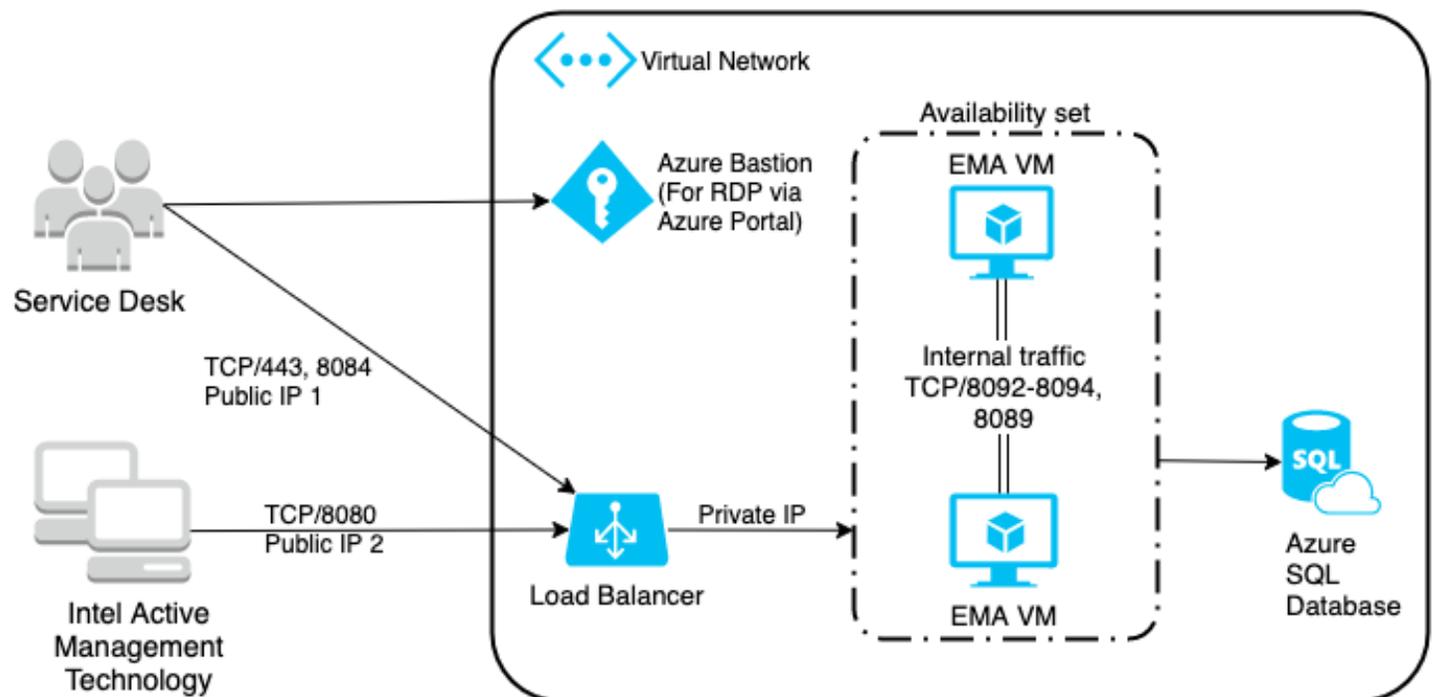
Consulte seu administrador de rede para saber se seria preferível usar um espaço de endereçamento específico. Se já tiver uma VPN estabelecida no provedor de nuvem, ou caso venha a ter futuramente, evite a sobreposição com sua rede corporativa para impedir problemas de roteamento. Você também precisa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

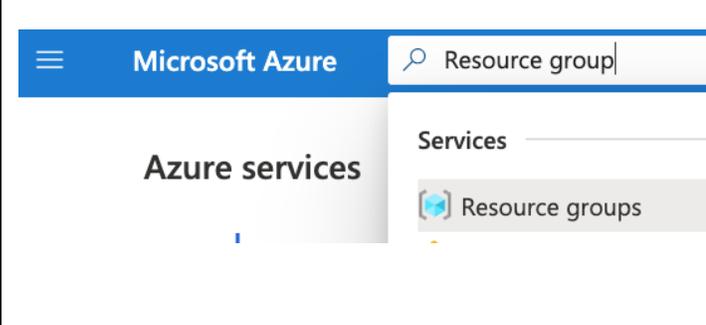
Um grupo de recursos é caracterizado como um contêiner que reúne os recursos relacionados para uma solução Azure para que você possa implantar, atualizar e excluí-los como um grupo. Você também pode ver facilmente as cobranças de todos os recursos

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

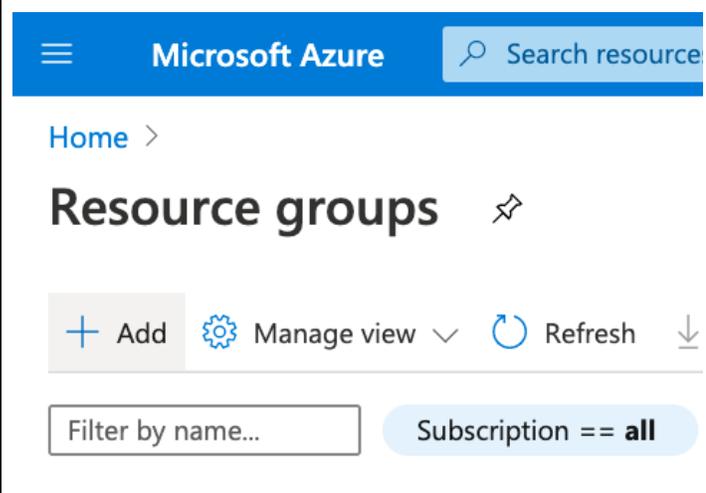
Para mais informações sobre Grupos de recursos, acesse o seguinte link: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>.

3.2 Criar um Grupo de recursos

3.2.1 Seleccione o serviço de grupos de recursos

	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre Resource groups e, em seguida, clique no item de lista exibido.</p>
--	--

3.2.2 Adicione um grupo de recursos

	<p>Clique no botão Add.</p>
---	------------------------------------

3.2.3 Configure o grupo de recursos

Home > Resource groups >

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution, or only those resources that you want to allocate resources to resource groups based on what makes the most sense for your solution.

Project details

Subscription * ⓘ

Resource group * ⓘ

Resource details

Region * ⓘ

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.

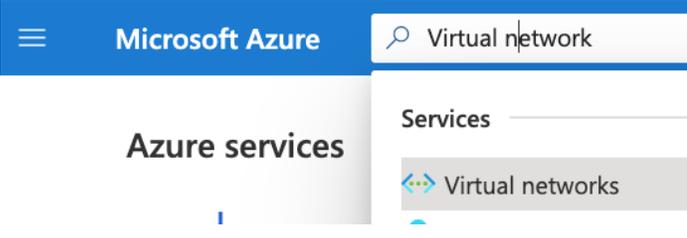
Para obter mais informações sobre recursos de rede implantados nesta seção, acesse os links a seguir ou procure links adicionais nas seções abaixo:

- 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/>

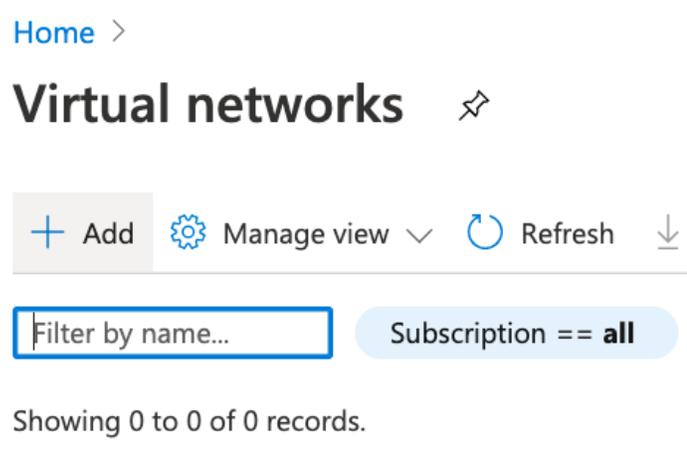
4.2 Crie uma rede virtual

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

4.2.1 Navegue até o serviço de redes virtuais

	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre Virtual networks e, em seguida, clique no item de lista exibido.</p>
---	---

4.2.2 Adicione uma rede virtual

	<p>Clique no botão Add.</p>
--	------------------------------------

4.2.3 Configure os detalhes básicos da Rede virtual

Home > Virtual networks >

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your Azure resources, such as Azure Virtual Machines (VM), to securely communicate over networks. VNet is similar to a traditional network that you'd operate in your data center. VNet provides the benefits of Azure's infrastructure such as scale, availability, and isolation.

Project details

Subscription * ⓘ

Resource group * ⓘ
[Create new](#)

Instance details

Name *

Region *

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

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses) 

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

<div data-bbox="120 163 682 214"><h3>Add subnet ✕</h3></div> <div data-bbox="120 319 678 411"><p>Subnet name * <input type="text" value="ema-servers"/></p></div> <div data-bbox="120 445 678 613"><p>Subnet address range * ⓘ <input type="text" value="10.250.0.0/26"/> 10.250.0.0 - 10.250.0.63 (59 + 5 Azure reserved addresses)</p></div> <div data-bbox="120 676 350 705"><h4>SERVICE ENDPOINTS</h4></div> <div data-bbox="120 756 678 856"><p>Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more</p></div> <div data-bbox="120 898 678 999"><p>Services ⓘ <input type="text" value="Microsoft.Sql"/></p></div> <div data-bbox="120 1050 467 1100"><p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p></div>	<p>Clique no botão Add Subnet e configure a sub-rede conforme abaixo.</p> <p>Subnet name: insira um nome de sub-rede exclusivo. Exemplo: <i>ema-servers</i></p> <p>Subnet address range: insira um intervalo de endereços de sub-rede não usados, contido no espaço de endereço IPv4 que você inseriu anteriormente. Exemplo: <i>10.250.0.0/26</i></p> <p>No menu suspenso Services, selecione Microsoft.Sql.</p> <p>Clique no botão Add para finalizar a sub-rede.</p> <p>Clique no botão Next: Security.</p>
---	---

4.2.6 Habilite o Azure Bastion

<div data-bbox="110 1251 678 1276"><p>Basics IP Addresses <u>Security</u> Tags Review + create</p></div> <div data-bbox="110 1306 500 1369"><p>BastionHost ⓘ <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p></div> <div data-bbox="110 1402 867 1436"><p>Bastion name * <input type="text" value="EmaBastion"/></p></div> <div data-bbox="110 1461 867 1516"><p>AzureBastionSubnet address space * <input type="text" value="10.250.0.64/26"/> 10.250.0.64 - 10.250.0.127 (64 addresses)</p></div> <div data-bbox="110 1541 867 1596"><p>Public IP address * <input type="text" value="(New) EmaBastion"/> Create new</p></div> <div data-bbox="110 1621 500 1684"><p>DDoS Protection Standard ⓘ <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p></div> <div data-bbox="110 1709 500 1772"><p>Firewall ⓘ <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p></div>	<p>Defina as configurações de segurança conforme abaixo.</p> <p>BastionHost: <i>Enable</i></p> <p>Bastion name: insira um nome de Bastion exclusivo. Exemplo: <i>EmaBastion</i></p> <p>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: <i>10.250.0.64/26</i></p> <p>Public IP address: clique no link Create new, defina um nome exclusivo e, em seguida, clique no botão OK Exemplo: <i>EmaBastion</i></p>
---	---

4.2.7 Analise

Clique no botão **Review + create**.

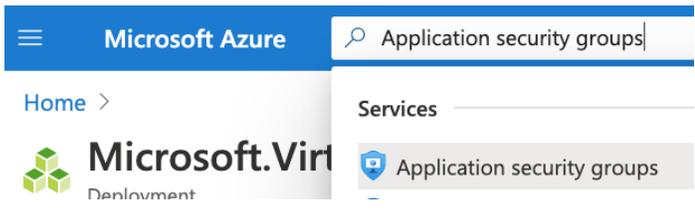
Analise as informações de rede na tela e clique no botão **Create**.

4.3 Grupo de segurança da aplicação (ASG)

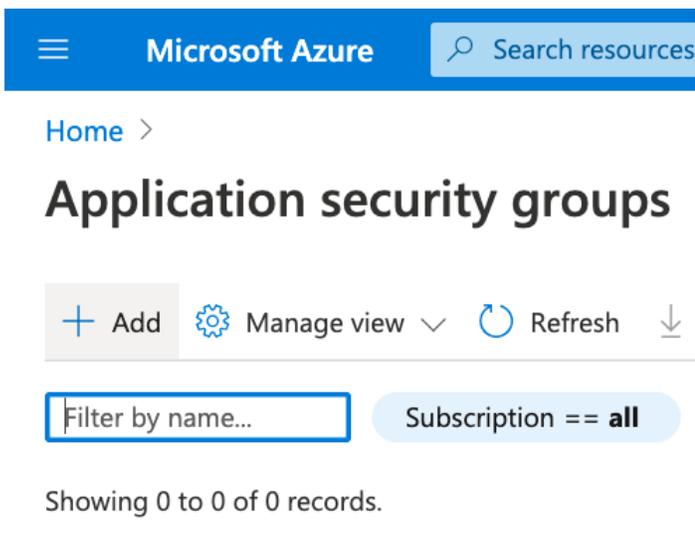
Você pode pensar em um ASG como um identificador especial que pode ser aplicado a uma máquina virtual de forma a lhe permitir direcionar mais facilmente a máquina virtual à regra de firewall, o que faremos na seção Grupo de segurança de rede. A fim de nos prepararmos para isso, vamos criar um ASG através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

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

4.3.2 Adicione um grupo de segurança da aplicação

	<p>Clique no botão Add.</p>
--	------------------------------------

4.3.3 Configure o Grupo de segurança da aplicação (ASG)

<p>Home > Application security groups ></p> <h2>Create an application security group</h2> <p>Basics Tags Review + create</p> <p>Project details</p> <p>Subscription * <input type="text"/></p> <p>Resource group * <input type="text" value="intel-ema-resources"/> Create new</p> <p>Instance details</p> <p>Name * <input type="text" value="ema-servers"/></p> <p>Region * <input type="text" value="(US) West US"/></p>	<p>Insira os detalhes básicos conforme abaixo.</p> <ul style="list-style-type: none">• Resource group: selecione o grupo de recursos que você criou anteriormente.• Name: insira um nome exclusivo para o ASG. Exemplo: <i>ema-servers</i>• Region: confirme se essa é a região onde você deseja implantar seus recursos. <p>Clique no botão Review + create.</p> <p>Analise as informações na tela e clique no botão Create.</p>
---	--

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.

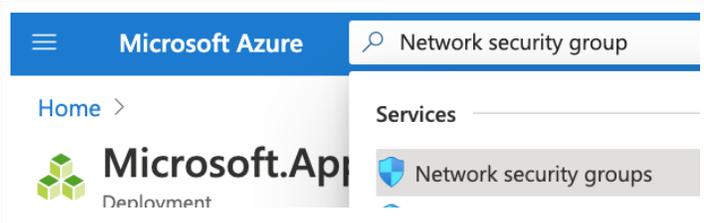
DenyAllInbound: nega todo o tráfego de entrada de qualquer fonte para qualquer fonte.

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.

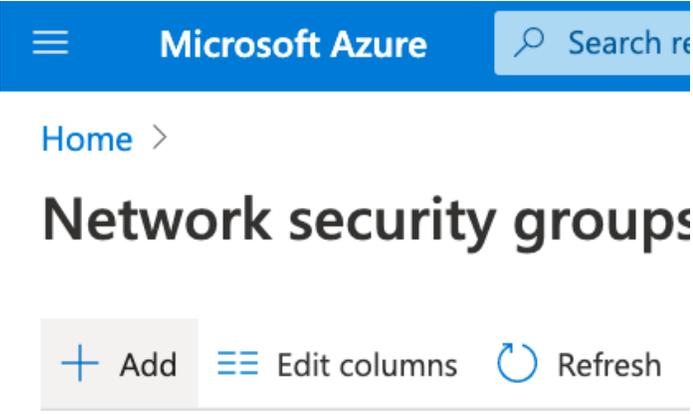
Para obter mais informações sobre os grupos de segurança de rede, acesse o seguinte link: <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

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

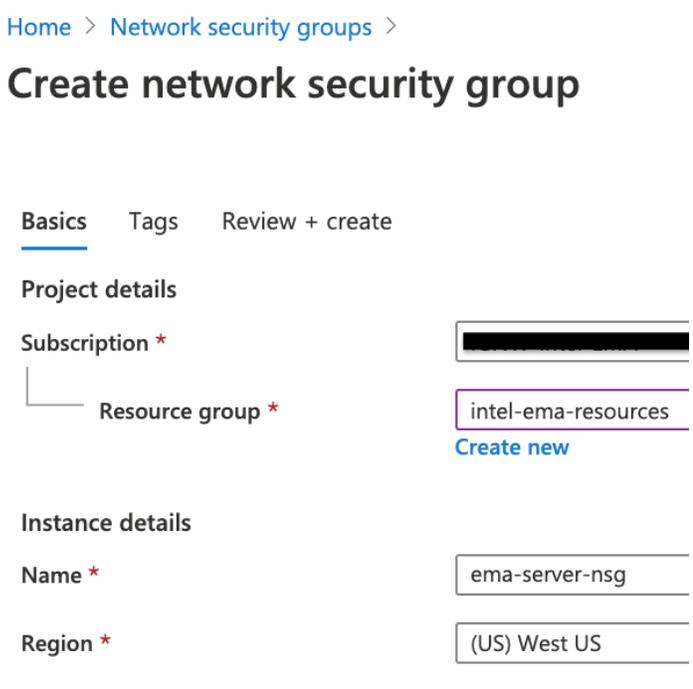
	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre Network security groups e, em seguida, clique no item de lista exibido.</p>
--	--

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

Home > Network security groups > **ema-server-nsg** | Inbound security rules

Network security group

Search (Cmd+/) << + Add Default rules Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules

Priority	Name	Port
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBala...	Any
65500	DenyAllInBound	Any

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

Add inbound security rule

ema-server-nsg

Basic

Source * ⓘ

IP Addresses

Source IP addresses/CIDR ranges * ⓘ

10.0.0.0/24 or 2001:1234::/64

Add your own trusted network in the field above

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

ema-servers

Destination port ranges * ⓘ

3389

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

RDP

Description

Allow RDP from trusted sources to EMA servers

Add

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

Add inbound security rule

ema-server-nsg

Basic

Source * ⓘ

IP Addresses

Source IP addresses/CIDR ranges * ⓘ

10.0.0.0/24 or 2001:1234::/64

Add your own trusted network here

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

ema-servers

Destination port ranges * ⓘ

443,8084

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

110

Name *

web

Description

Allow web traffic from trusted sources to EMA servers

Add

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

Add inbound security rule

ema-server-nsg

Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

ema-servers

Destination port ranges * ⓘ

8080

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

120

Name *

swarm

Description

Allow swarm traffic from any source to EMA servers

Add

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)

Add inbound security rule

ema-server-nsg

Basic

Source * ⓘ

Application security group

Source application security group * ⓘ

ema-servers

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

ema-servers

Destination port ranges * ⓘ

8092-8094,8089

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

130

Name *

ema_internal

Description

Allow internal communication between EMA servers

Add

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		 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**.

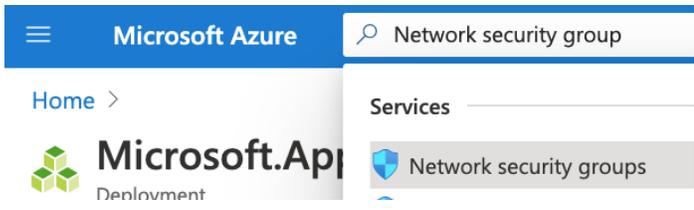
4.4.4.2 Associe o grupo de segurança de rede à sub-rede

<h3>Associate subnet</h3> <p>ema-server-nsg</p> <p>Virtual network ⓘ</p> <input type="text" value="intel-ema-network"/> <p>Subnet ⓘ</p> <input type="text" value="ema-servers"/>	<p>Selecione a sub-rede que você criou anteriormente para os servidores EMA e clique em OK.</p>
--	--

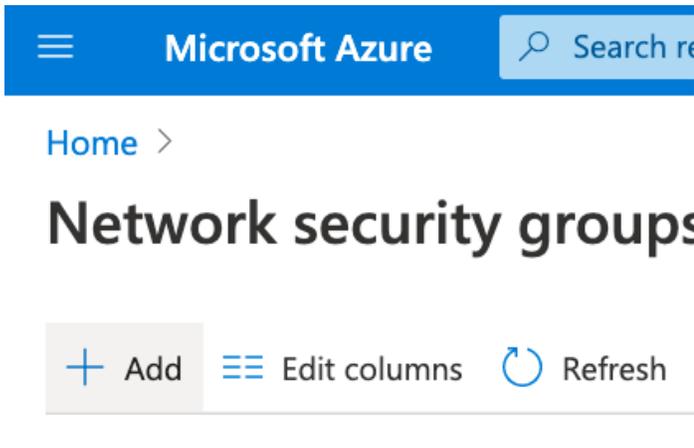
4.4.5 Crie o grupo de segurança de rede para a sub-rede Azure Bastion

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

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

4.4.5.2 Adicione um grupo de segurança de rede

	<p>Clique no botão Add.</p>
---	------------------------------------

4.4.5.3 Configure os detalhes básicos do grupo de segurança de rede

Create network security group

Basics Tags Review + create

Project details

Subscription *

Resource group *
[Create new](#)

Instance details

Name *

Region *

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

ema-bastion-nsg | Inbound security rules

Network security group

Search (Cmd+ /) << + Add Default rules Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules

Priority	Name
65000	AllowVnetIn
65001	AllowAzureL
65500	DenyAllInBo

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

Add inbound security rule

ema-bastion-nsg

Basic

Source * ⓘ

Service Tag

Source service tag * ⓘ

Internet icon-networking-67

Source port ranges * ⓘ

*

Destination * ⓘ

Any

Destination port ranges * ⓘ

443

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

AllowHttpsInbound

Description

Allow HTTPS to Azure Bastion

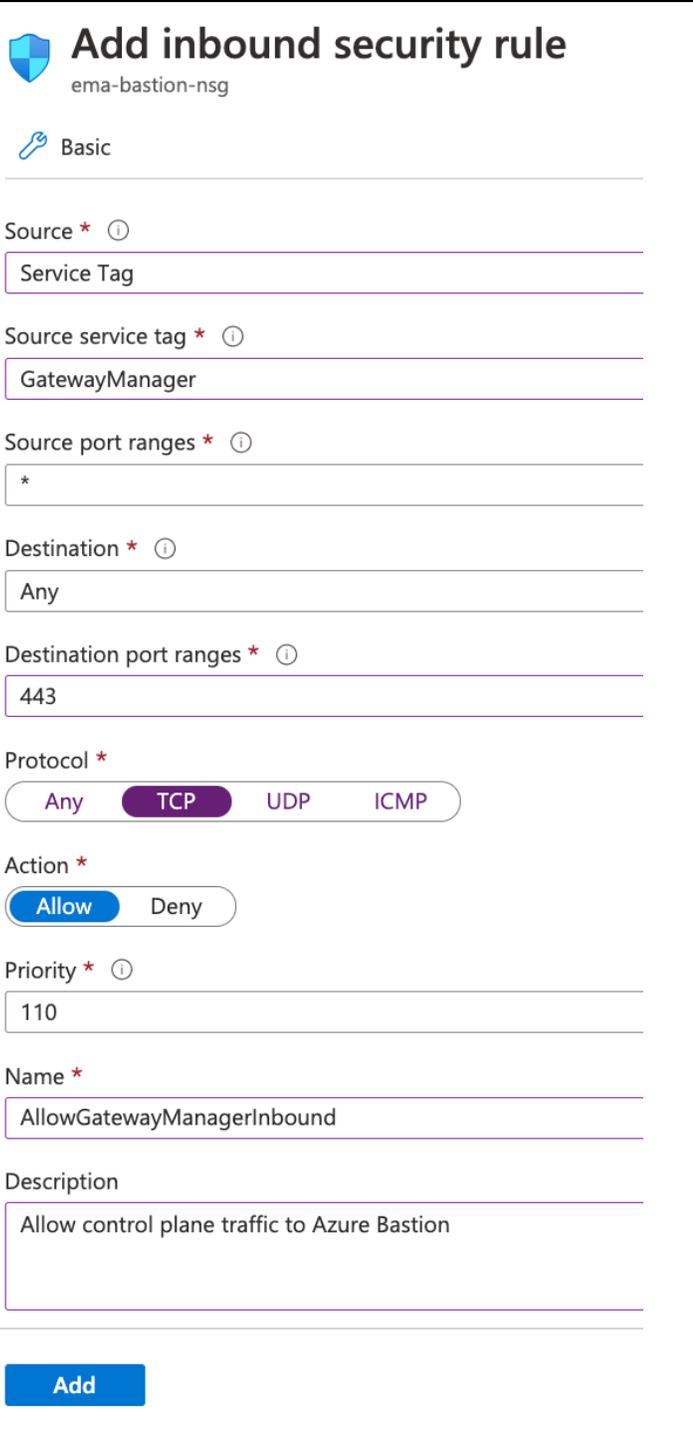
Add

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

	<p>Clique no botão Add perto do topo da tela e configure a regra conforme abaixo.</p> <ul style="list-style-type: none">• Source: <i>Service Tag</i>• Source service tag: <i>GatewayManager</i>• Source port ranges: *• Destination: <i>Any</i>• Destination port ranges: <i>443</i>• Protocol: <i>TCP</i>• Action: <i>Allow</i>• Priority: use o valor atribuído automaticamente.• Name: insira um nome exclusivo. Exemplo: <i>AllowGatewayManagerInbound</i>• Description: <i>Permitir tráfego do plano de controle para o Azure Bastion</i> <p>Clique no botão Add na parte inferior da tela.</p>
--	---

4.4.7 Configure as regras de segurança de saída

	<p>Na barra lateral, abaixo de "Inbound security rules", clique em "Outbound security rules".</p>
---	---

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

Add outbound security rule

ema-bastion-nsg

Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Service Tag

Destination service tag ⓘ

VirtualNetwork

Destination port ranges * ⓘ

22,3389

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

AllowRdpOutbound

Description

Allow SSH and RDP connections from Azure Bastion to our vi

Add

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

Add outbound security rule

ema-bastion-nsg

Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Service Tag

Destination service tag ⓘ

AzureCloud

Destination port ranges * ⓘ

443

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

110

Name *

AllowAzureCloudOutbound

Description

Add

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

ema-bastion-nsg | Subnets

Network security group

Search (Cmd+/) << + Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Search subnets

Name

No results.

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

Associate subnet

ema-bastion-nsg

Virtual network ⓘ

intel-ema-network

Subnet ⓘ

AzureBastionSubnet

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% de 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/>

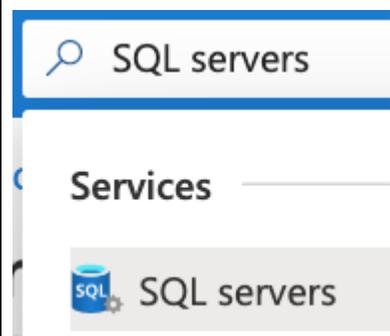
<https://docs.microsoft.com/en-us/azure/azure-sql/database/>

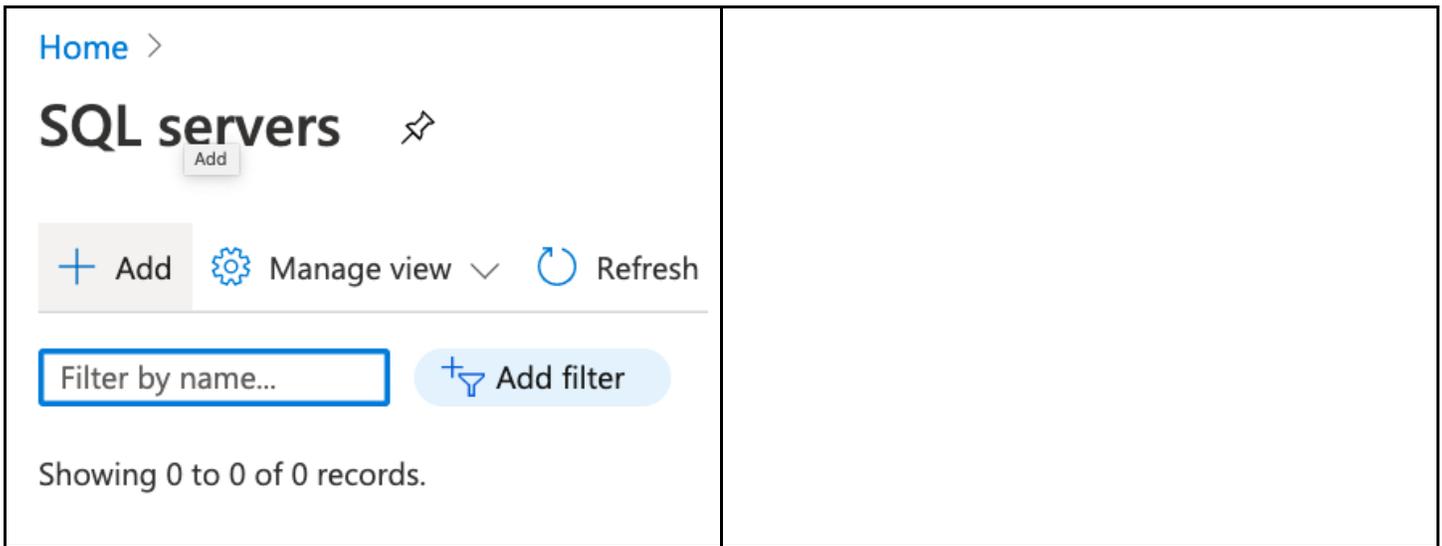
<https://docs.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla>

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

 A screenshot of the Azure portal search interface. At the top, there is a search bar with a magnifying glass icon and the text 'SQL servers'. Below the search bar, there is a 'Services' section. Under 'Services', there is a search result for 'SQL servers' with a small SQL logo icon to its left.	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre SQL servers e, em seguida, clique no item de lista exibido.</p> <p>Clique no botão Add.</p>
--	---



5.2.2 Configure os detalhes básicos para o servidor SQL

Home > SQL servers >

Create SQL Database Server

Microsoft

Basics Networking Additional settings Tags Review + create

SQL database server is a logical container for managing databases and elastic pools. Complete the Basic tab, then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Server details

Enter required settings for this server, including providing a name and location.

Server name *
 .database.windows.net

Location *

Administrator account

Server admin login *

Password *

Confirm password *

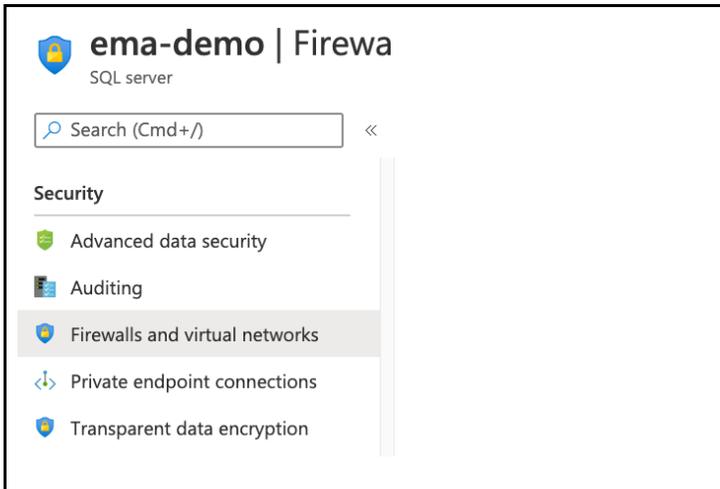
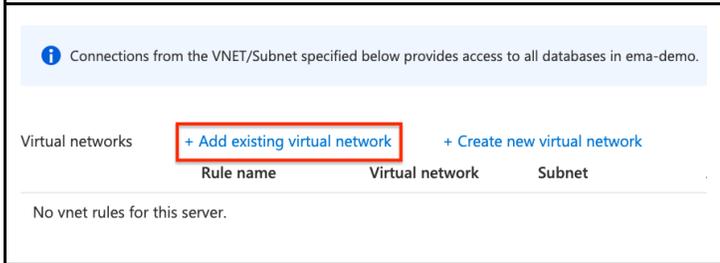
Insira os detalhes básicos conforme abaixo.

- **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

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

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

Create/Update

virtual network rule

Name * ⓘ

allow-ema-servers ✓

provide vnet rule name

Subscription * ⓘ

Virtual network * ⓘ

intel-ema-network

Subnet name / Address prefix * ⓘ

ema-servers / 10.250.0.0/26

Virtual network	Service endpoint stat...
intel-ema-network/e...	Enabled

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.

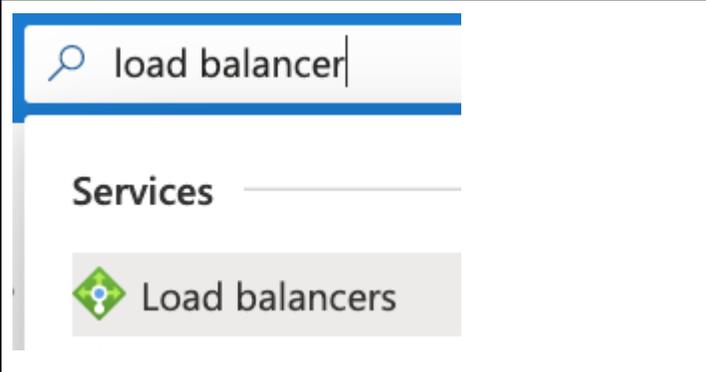
Se estiver implantando apenas um servidor único, você pode ignorar esta seção.

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

 A screenshot of the Azure portal search interface. At the top, a search bar contains the text 'load balancer'. Below the search bar, the word 'Services' is displayed. Underneath, a search result is shown with a green diamond icon containing a white gear and the text 'Load balancers'.	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre Load balancers e, em seguida, clique no item de lista exibido.</p>
---	---

7.1.2 Informações básicas do balanceador de carga

Create load balancer

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription * [dropdown]

Resource group * intel-ema-resources [dropdown]
[Create new](#)

Instance details

Name * ema-load-balancer [input]

Region * (US) West US [dropdown]

Type * Internal Public

SKU * Basic Standard

i Standard Load Balancer is secure by default. This means Network Security Groups (NSGs) are used to explicitly permit and whitelist allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource. Please configure an NSG to ensure communication if needed. For outbound communication, an explicit outbound rule is needed. [Learn more about outbound connectivity](#)

Public IP address

Public IP address * Create new Use existing

Public IP address name * ema-load-balancer-ip [input]

Public IP address SKU Standard

Assignment Dynamic Static

Add a public IPv6 address No Yes

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*

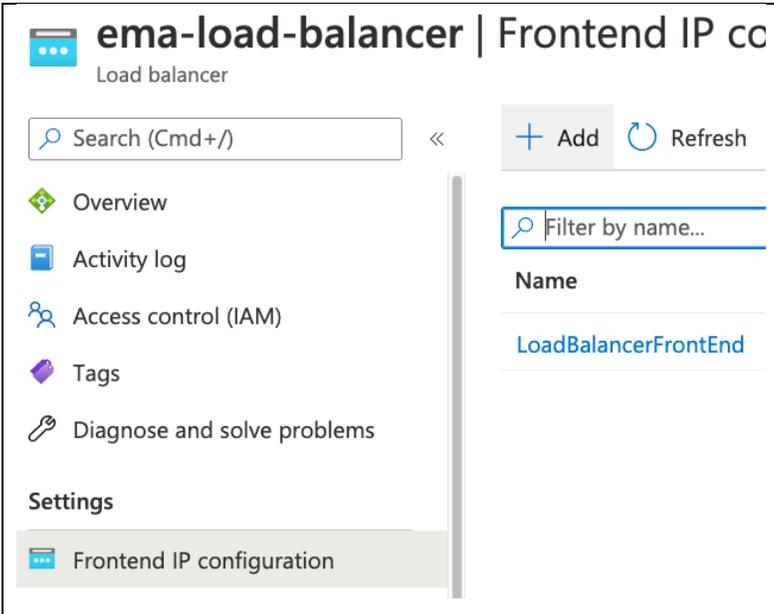
Clique no botão **Review + create**.

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



ema-load-balancer | Frontend IP configuration
Load balancer

Search (Cmd+/) << + Add Refresh

Filter by name...

Name
LoadBalancerFrontEnd

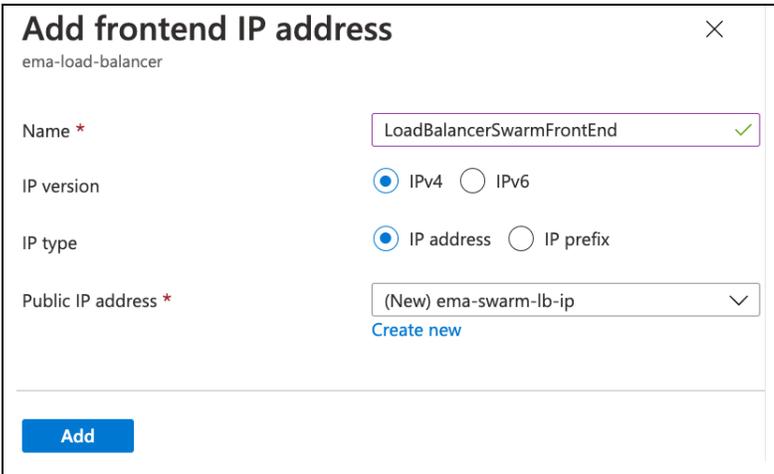
Settings

Frontend IP configuration

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

Clique no botão **Add**.

7.2.2 Configure o segundo front-end



Add frontend IP address

ema-load-balancer

Name * LoadBalancerSwarmFrontEnd ✓

IP version IPv4 IPv6

IP type IP address IP prefix

Public IP address * (New) ema-swarm-lb-ip
[Create new](#)

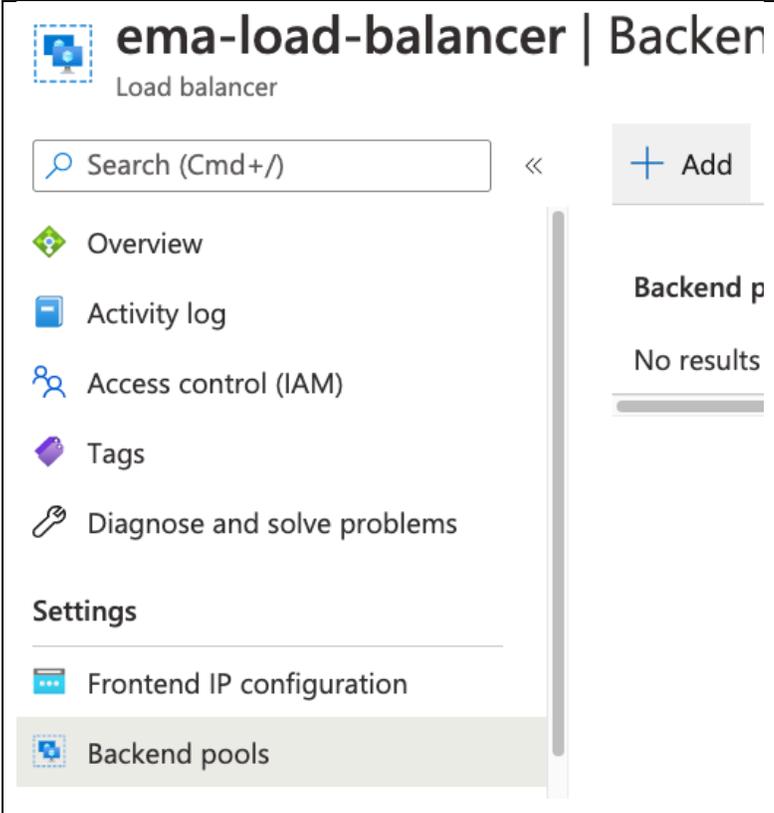
Add

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

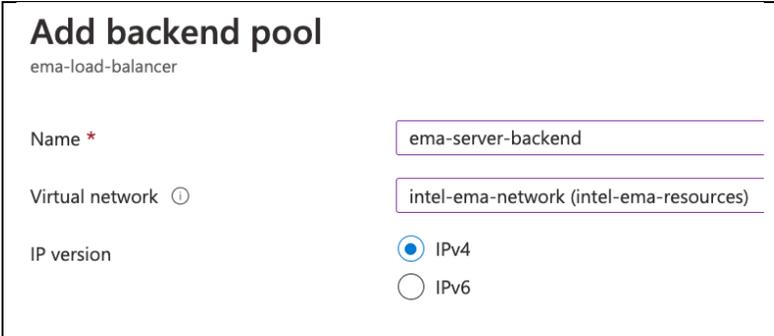
Para "Public IP address", clique no link **Create new** e dê um nome para o endereço IP.
Exemplo: *ema-swarm-lb-ip*

Clique no botão **Add**.

7.2.3 Adicione um pool de back-end

	<p>Na barra lateral, em Settings, clique em Backend pools.</p> <p>Clique no botão Add.</p>
--	---

Configure o pool de back-end

	<p>Insira um nome exclusivo para o pool de back-end. Exemplo: <i>ema-server-backend</i></p> <p>Selecione sua rede virtual existente.</p> <p>Clique no botão Add.</p> <p>Este pool de back-end estará disponível para seleção mais tarde, quando criarmos nossas máquinas virtuais.</p>
--	---

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

Create a virtual machine

Basics Disks Networking Management Advanced Tags

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options **For multi-server deployment only**

Availability set * [Create new](#)

Image * [Browse all public and private images](#)

Azure Spot instance Yes No

Size * [Select size](#)

Administrator account

Username *

Password *

Confirm password *

Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

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

Basics **Disks** Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *

Encryption type *

Enable Ultra Disk compatibility Yes No

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk	Attach an existing disk			

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

8.2.2.2 Configure os detalhes do novo disco

Home > Virtual machines > Create a virtual machine >

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name *

Source type *

Size * **256 GiB**
Standard HDD
[Change size](#)

Encryption type *

Enable shared disk Yes No
Shared disk not available for the selected size.

OK

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

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
0	ema-server-1_logs	256	Standard HDD	Read-only

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

[Review + create](#) [< Previous](#) [Next : Networking >](#)

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

Basics Disks **Networking** Management Advanced ...

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ intel-ema-network [Create new](#)

Subnet * ⓘ ema-servers (10.250.0.0/26) [Manage subnet configuration](#)

Public IP ⓘ None [Create new](#)

NIC network security group ⓘ None Basic Advanced

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)

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? Yes No

Load balancing settings

- **Application Gateway** is an HTTP/HTTPS web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. [Learn more about Application Gateway](#)
- **Azure Load Balancer** supports all TCP/UDP network traffic, port-forwarding, and outbound flows. [Learn more about Azure Load Balancer](#)

Load balancing options * ⓘ

Select a load balancer * ⓘ

Select a backend pool * ⓘ [Create new](#)

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**.

The screenshot shows the 'Settings' sidebar on the left with 'Networking' selected. The main content area has three tabs: 'Inbound port rules', 'Outbound port rules', and 'Application security groups'. The 'Application security groups' tab is active, and a button labeled 'Configure the application security groups' is visible.

Selecione o grupo de segurança da aplicação criado anteriormente.

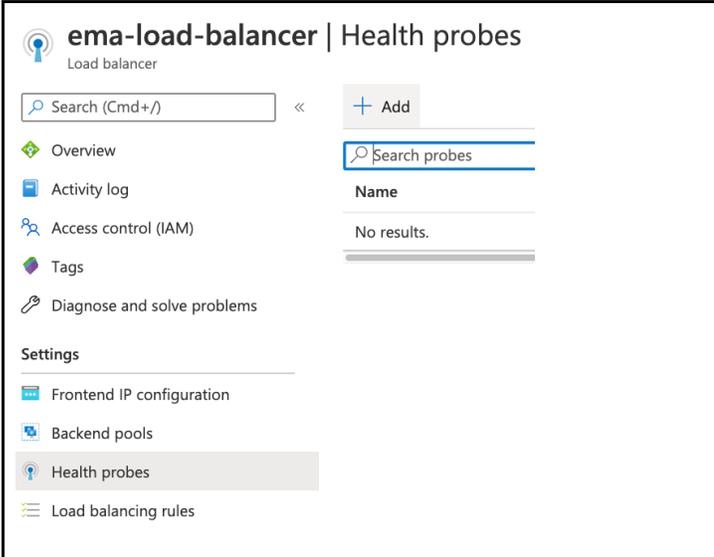
The screenshot shows the 'Application security groups' list. The 'ema-servers' group is highlighted with a purple border. Below it is a search filter box containing 'Filter the application secur'. At the bottom, the 'ema-servers' group is listed with a blue checkmark icon next to it.

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

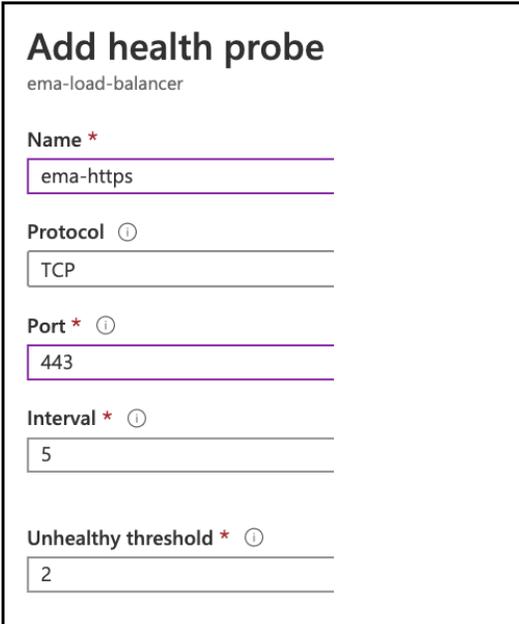
Agora que as máquinas virtuais foram criadas, podemos voltar à configuração do balanceador de carga para configurar as verificações de integridade e as regras de encaminhamento, a fim de direcionar o tráfego de entrada para as portas de VM de back-end apropriadas.

9.1 Configure as investigações de integridade

9.1.1 Acesse a tela de investigações de integridade

	<p>Use a barra de pesquisa no topo da tela para pesquisar sobre Load balancers e, em seguida, clique no item de lista exibido.</p> <p>Clique no balanceador de carga criado anteriormente.</p> <p>Em Settings na barra lateral, clique em Health probes.</p>
---	---

9.1.2 Adicione investigações de integridade para tráfego Web

	<p>Clique no botão Add e configure a investigação de integridade conforme abaixo.</p> <ul style="list-style-type: none">• Name: insira um nome exclusivo. Exemplo: <i>ema-https</i>• Protocol: <i>TCP</i>• Port: <i>443</i> <p>Clique no botão OK.</p>
--	---

9.1.3 Adicione investigações de integridade para tráfego Swarm

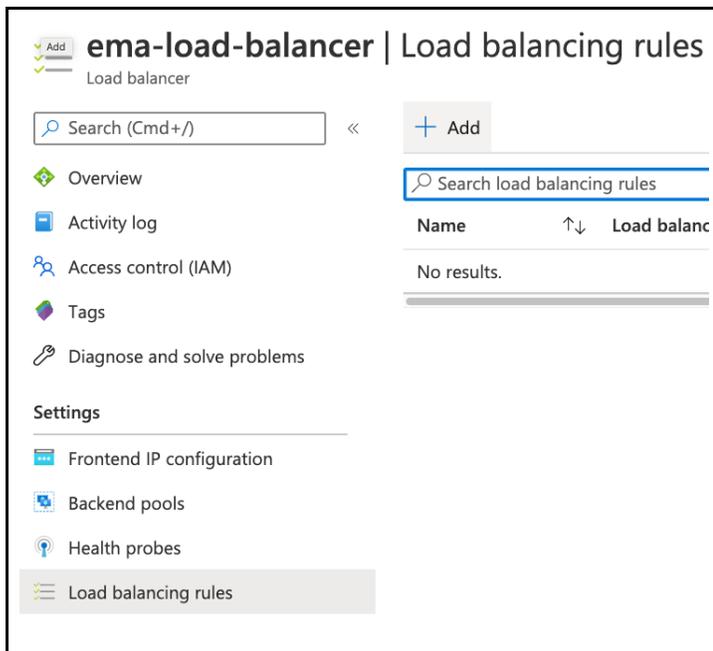
<h4>Add health probe</h4> <p>ema-load-balancer</p> <p>Name *</p> <input type="text" value="ema-swarm"/> <p>Protocol ⓘ</p> <input type="text" value="TCP"/> <p>Port * ⓘ</p> <input type="text" value="8080"/> <p>Interval * ⓘ</p> <input type="text" value="5"/> <p>Unhealthy threshold * ⓘ</p> <input type="text" value="2"/>	<p>Clique no botão Add e configure a investigação de integridade conforme abaixo.</p> <ul style="list-style-type: none">• Name: insira um nome exclusivo. Exemplo: <i>ema-swarm</i>• Protocol: <i>TCP</i>• Port: <i>8080</i> <p>Clique no botão OK.</p>
--	--

9.1.4 Adicione investigações de integridade para tráfego WebSocket

<h4>Add health probe</h4> <p>ema-load-balancer</p> <p>Name *</p> <input type="text" value="ema-websocket"/> <p>Protocol ⓘ</p> <input type="text" value="TCP"/> <p>Port * ⓘ</p> <input type="text" value="8084"/> <p>Interval * ⓘ</p> <input type="text" value="5"/> <p>Unhealthy threshold * ⓘ</p> <input type="text" value="2"/>	<p>Clique no botão Add e configure a investigação de integridade conforme abaixo.</p> <ul style="list-style-type: none">• Name: insira um nome exclusivo. Exemplo: <i>ema-websocket</i>• Protocol: <i>TCP</i>• Port: <i>8084</i> <p>Clique no botão OK.</p>
--	--

9.2 Configure as regras de balanceamento de carga

9.2.1 Acesse a tela de regras de balanceamento de carga



ema-load-balancer | Load balancing rules
Load balancer

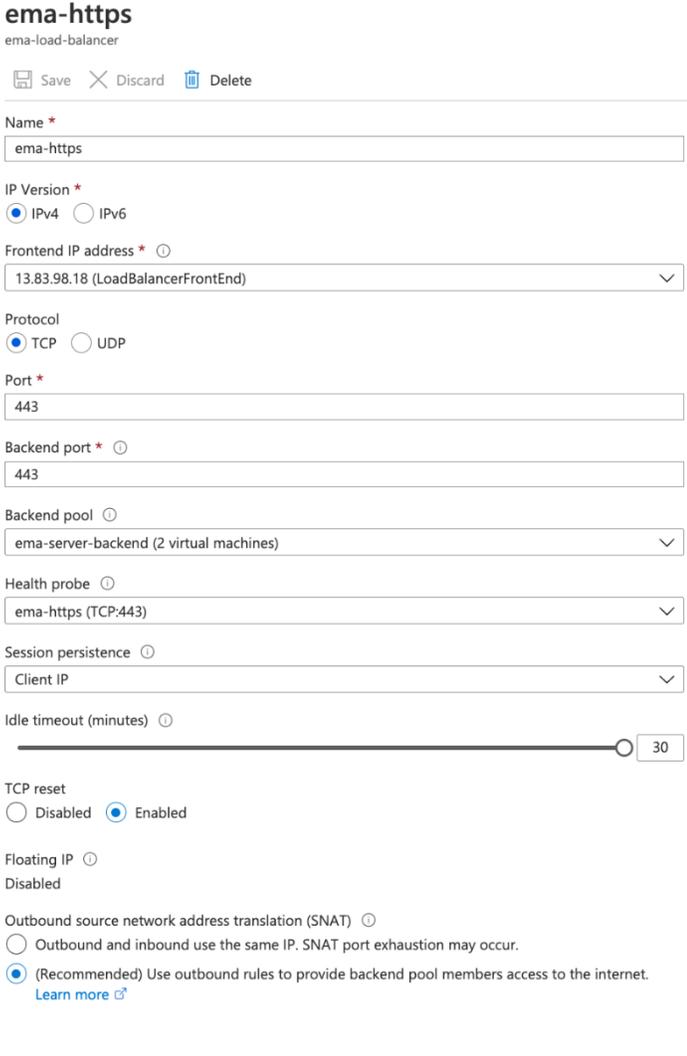
Search (Cmd+/) << + Add

Search load balancing rules

Name	Load balance
No results.	

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

9.2.2 Crie uma regra para tráfego Web

 <p>ema-https ema-load-balancer</p> <p>Save Discard Delete</p> <p>Name * ema-https</p> <p>IP Version * <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6</p> <p>Frontend IP address * ⓘ 13.83.98.18 (LoadBalancerFrontEnd)</p> <p>Protocol <input checked="" type="radio"/> TCP <input type="radio"/> UDP</p> <p>Port * 443</p> <p>Backend port * ⓘ 443</p> <p>Backend pool ⓘ ema-server-backend (2 virtual machines)</p> <p>Health probe ⓘ ema-https (TCP:443)</p> <p>Session persistence ⓘ Client IP</p> <p>Idle timeout (minutes) ⓘ 30</p> <p>TCP reset <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled</p> <p>Floating IP ⓘ Disabled</p> <p>Outbound source network address translation (SNAT) ⓘ <input type="radio"/> Outbound and inbound use the same IP. SNAT port exhaustion may occur. <input checked="" type="radio"/> (Recommended) Use outbound rules to provide backend pool members access to the internet. Learn more</p>	<p>Clique no botão Add e configure a regra conforme abaixo.</p> <ul style="list-style-type: none">• Name: <i>ema-https</i>• Frontend IP address: selecione o front-end do balanceador de carga usado para tráfego web. Exemplo: <i>LoadBalancerFrontEnd</i>• Protocol: <i>TCP</i>• Port: <i>443</i>• Backend Port: <i>443</i>• Backend pool: selecione o pool de back-end que você criou anteriormente. Exemplo: <i>ema-server-backend</i>• Health probe: selecione a investigação de integridade da porta 443 que você criou anteriormente. Exemplo: <i>ema-https</i>• Session persistence: <i>Client IP</i>• Idle timeout (minutes): defina para o valor máximo (30)• TCP reset: <i>Enabled</i>• Outbound source network address translation: <i>Use outbound rules to provide backend pool members access to the internet.</i> <p>Clique no botão OK.</p>
---	---

9.2.3 Crie uma regra para tráfego WebSocket

 <p>ema-websocket ema-load-balancer</p> <p>Save Discard Delete</p> <p>Name * ema-websocket</p> <p>IP Version * <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6</p> <p>Frontend IP address * ⓘ 13.83.98.18 (LoadBalancerFrontEnd)</p> <p>Protocol <input checked="" type="radio"/> TCP <input type="radio"/> UDP</p> <p>Port * 8084</p> <p>Backend port * ⓘ 8084</p> <p>Backend pool ⓘ ema-server-backend (2 virtual machines)</p> <p>Health probe ⓘ ema-websocket (TCP:8084)</p> <p>Session persistence ⓘ Client IP</p> <p>Idle timeout (minutes) ⓘ 30</p> <p>TCP reset <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled</p> <p>Floating IP ⓘ Disabled</p> <p>Outbound source network address translation (SNAT) ⓘ <input type="radio"/> Outbound and inbound use the same IP. SNAT port exhaustion may occur. <input checked="" type="radio"/> (Recommended) Use outbound rules to provide backend pool members access to the internet. Learn more</p>	<p>Clique no botão Add e configure a regra conforme abaixo.</p> <ul style="list-style-type: none">• Name: <i>ema-websocket</i>• Frontend IP address: selecione o front-end do balanceador de carga usado para tráfego web. Exemplo: <i>LoadBalancerFrontEnd</i>• Protocol: <i>TCP</i>• Port: <i>8084</i>• Backend Port: <i>8084</i>• Backend pool: selecione o pool de back-end que você criou anteriormente. Exemplo: <i>ema-server-backend</i>
---	--

ema-websocket
ema-load-balancer

Save Discard Delete

Name *
ema-websocket

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ
13.83.98.18 (LoadBalancerFrontEnd)

Protocol
 TCP UDP

Port *
8084

Backend port * ⓘ
8084

Backend pool ⓘ
ema-server-backend (2 virtual machines)

Health probe ⓘ
ema-websocket (TCP:8084)

Session persistence ⓘ
Client IP

Idle timeout (minutes) ⓘ
30

TCP reset
 Disabled Enabled

Floating IP ⓘ
Disabled

Outbound source network address translation (SNAT) ⓘ
 Outbound and inbound use the same IP. SNAT port exhaustion may occur.
 (Recommended) Use outbound rules to provide backend pool members access to the internet.
[Learn more](#)

- **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

ema-swarm

ema-load-balancer

Save Discard Delete

Name *
ema-swarm

IP Version *
 IPv4 IPv6

Frontend IP address *

Protocol
 TCP UDP

Port *

Backend port *

Backend pool

Health probe

Session persistence

Idle timeout (minutes)

TCP reset
 Disabled Enabled

Floating IP

Outbound source network address translation (SNAT) (Recommended) Use outbound rules to provide backend pool members access to the internet. [Learn more](#)

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.*

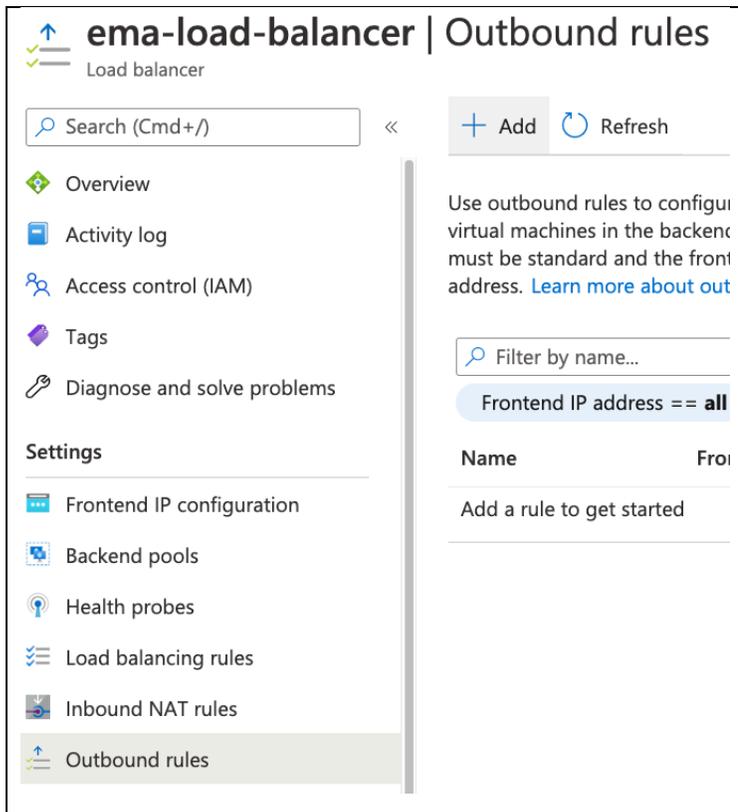
Clique no botão **OK**.

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



The screenshot shows the Azure portal interface for configuring an outbound rule on a load balancer. The page title is 'ema-load-balancer | Outbound rules'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a 'Settings' section with options for Frontend IP configuration, Backend pools, Health probes, Load balancing rules, Inbound NAT rules, and Outbound rules (which is selected). The main content area includes an 'Add' button, a 'Refresh' button, a search bar, and a filter 'Frontend IP address == all'. Below this is a table with columns 'Name' and 'Frontend IP address', and a message 'Add a rule to get started'.

ema-load-balancer | Outbound rules
Load balancer

Search (Cmd+/) << + Add Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

- Frontend IP configuration
- Backend pools
- Health probes
- Load balancing rules
- Inbound NAT rules
- Outbound rules

Use outbound rules to configure virtual machines in the backend must be standard and the front address. [Learn more about out](#)

Filter by name...
Frontend IP address == all

Name	Frontend IP address
Add a rule to get started	

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

Add outbound rule

ema-load-balancer

Name *

Frontend IP address *
[Create new](#)

Protocol All TCP UDP

Idle timeout (minutes) Max: 30

TCP Reset Enabled Disabled

Backend pool *
[Create new](#)

Port allocation

Azure automatically assigns the number of outbound ports to use for source network address translation (SNAT) based on the number of frontend IP addresses and backend pool instances.
[Learn more about outbound connectivity](#)

Port allocation

Outbound ports Choose by *

Ports per instance 42664

Frontend IPs 2

Maximum number of backend instances

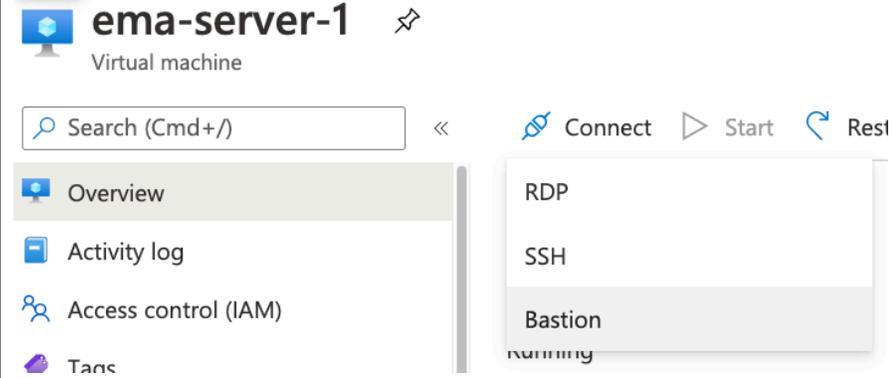
[Add](#)

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



ema-server-1
Virtual machine

Search (Cmd+/) << [Connect](#) [Start](#) [Reset](#)

- Overview
- Activity log
- Access control (IAM)
- Tags

RDP

SSH

Bastion

Running

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

<p>RDP SSH BASTION</p> <p> Bastion is an Azure service</p> <p>Use Bastion</p>	<p>Clique no botão Use Bastion.</p>
<p> Connect using Azure Bastion Azure Bastion Service enables you to securely connect to your Azure virtual network, without exposing a public IP address without the need of any additional client/agent on the virtual machine. Bastion.</p> <p>Using Bastion: EmaBastion, Provisioning State: Succeeded</p> <p>Please enter username and password to your virtual machine</p> <p><input checked="" type="checkbox"/> Open in new window</p> <p>Username * ⓘ <input type="text" value="ema"/></p> <p>Password * ⓘ <input type="password" value="....."/></p> <p>Connect</p>	<p>Insira as credenciais da VM e clique no botão Connect.</p> <p>Uma janela do navegador será aberta, com sua sessão de RDP para essa VM.</p>

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](#)

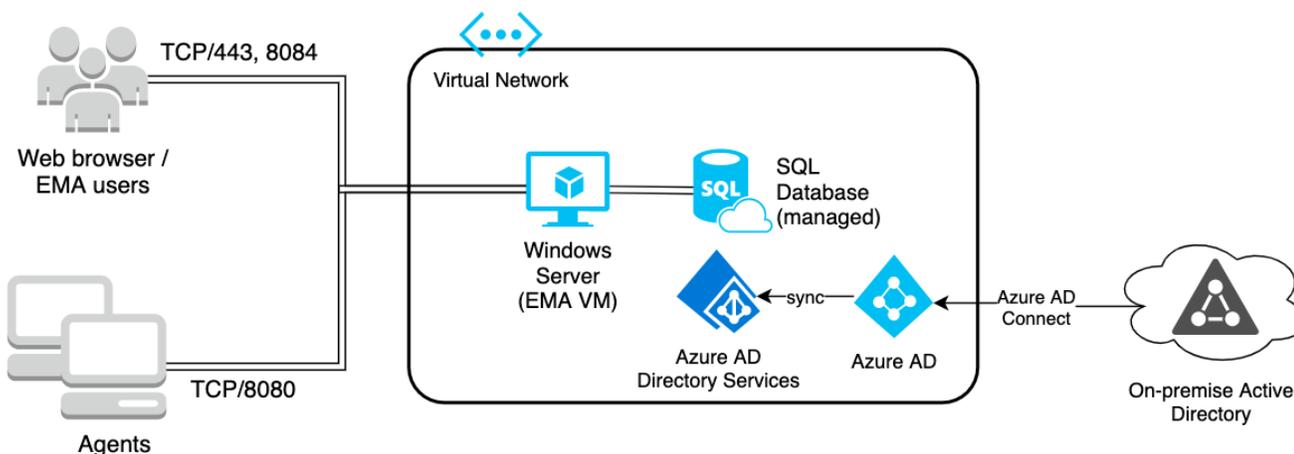
[Documentação do Azure AD Domain Services](#)

[Compare os serviços baseados no Active Directory no Azure](#)

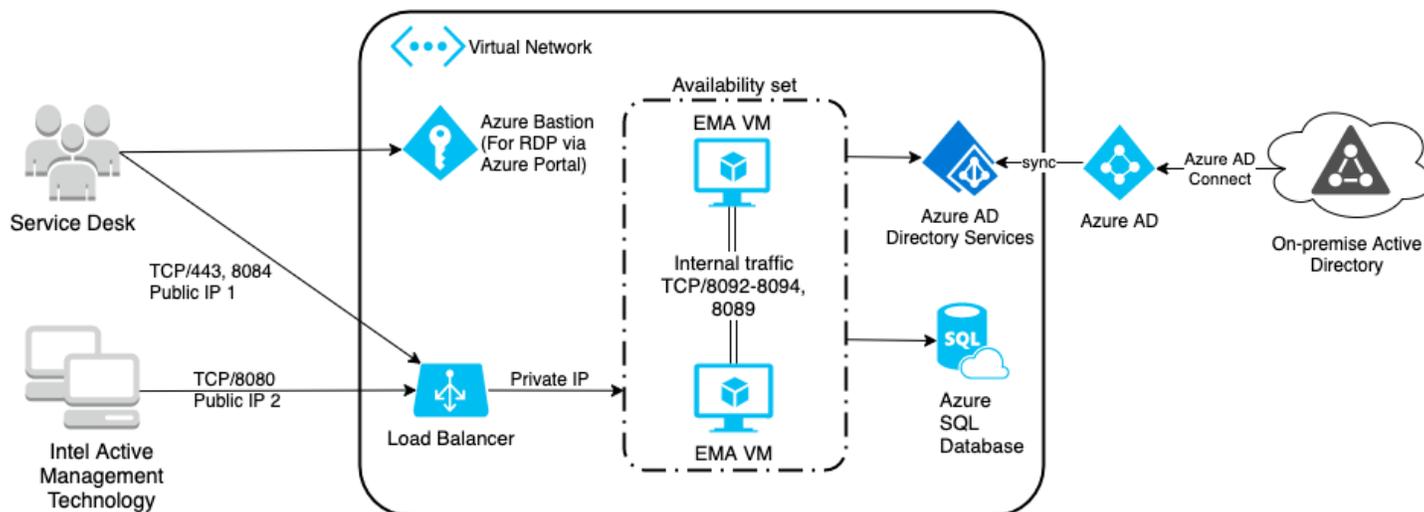
[Sincronização do Azure AD Connect: compreenda e personalize a sincronização](#)

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-requisitos 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.](#)