

Intel® Endpoint Management Assistant (Intel® EMA)

Microsoft Azure* 部署指南

英特尔® 版本 1.3.3

2020 年 10 月

法律免责声明

英特尔技术可能需要支持的硬件、软件或服务激活。

没有任何产品或组件能保证绝对安全。

您的成本和结果可能会有所不同。

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

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

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

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

© 英特尔公司。英特尔、英特尔标志和其他英特尔标识是英特尔公司或其子公司的商标。

*文中涉及的其它名称及商标属于各自所有者资产。

目录

| | | |
|----------|----------------------------|-----------|
| 1 | 简介 | 1 |
| 1.1 | 云计算简介 | 1 |
| 1.2 | 操作 Azure 控制台 | 1 |
| 1.2.1 | 服务菜单 | 1 |
| 1.2.2 | 展开服务菜单 | 1 |
| 1.2.3 | 按名称搜索服务 | 2 |
| 1.3 | 开始之前 | 2 |
| 2 | 高层级架构图 | 3 |
| 2.1 | 单服务器部署 | 3 |
| 2.2 | 分布式服务器部署 | 3 |
| 3 | 资源组部署 | 4 |
| 3.1 | 资源组概述 | 4 |
| 3.2 | 创建资源组 | 4 |
| 3.2.1 | 选择资源组服务 | 4 |
| 3.2.2 | 添加资源组 | 4 |
| 3.2.3 | 配置资源组 | 5 |
| 3.2.4 | 查看和创建 | 5 |
| 4 | 网络部署 | 5 |
| 4.1 | 概述 | 5 |
| 4.2 | 创建虚拟网络 | 6 |
| 4.2.1 | 导航到虚拟网络服务 | 6 |
| 4.2.2 | 添加虚拟网络 | 6 |
| 4.2.3 | 配置虚拟网络基本详细信息 | 7 |
| 4.2.4 | 配置 IPv4 地址空间 | 7 |
| 4.2.5 | 为 Intel EMA 服务器添加子网 | 8 |
| 4.2.6 | 启用 Azure Bastion | 8 |
| 4.2.7 | 审阅 | 9 |
| 4.3 | 应用程序安全组 (ASG) | 9 |
| 4.3.1 | 导航到应用程序安全组服务 | 9 |
| 4.3.2 | 添加应用程序安全组 | 9 |
| 4.3.3 | 配置应用程序安全组 (ASG) | 10 |
| 4.4 | 网络安全组 | 10 |
| 4.4.1 | 为 Intel EMA 服务器子网创建网络安全组 | 10 |
| 4.4.2 | 配置网络安全组 | 12 |
| 4.4.3 | 审阅 | 17 |
| 4.4.4 | 将网络安全组与子网关联 | 17 |
| 4.4.5 | 为 Azure Bastion 子网创建网络安全组 | 18 |
| 4.4.6 | 配置网络安全组 | 19 |
| 4.4.7 | 配置出站安全规则 | 21 |
| 4.4.8 | 将网络安全组与 Azure Bastion 子网关联 | 24 |
| 5 | SQL 服务器部署 | 24 |
| 5.1 | 概述 | 24 |
| 5.2 | 创建 SQL 服务器 | 25 |
| 5.2.1 | 添加新的 SQL 服务器 | 25 |
| 5.2.2 | 配置 SQL 服务器的基本详细信息 | 26 |
| 5.2.3 | 配置 SQL 服务器防火墙 | 26 |
| 6 | 可用性集合 (仅限于分布式服务器) | 27 |

| | | |
|-----------|---|-----------|
| 6.1 | 创建“可用性集合” | 28 |
| 7 | 负载均衡器部署 (仅限于分布式服务器) | 28 |
| 7.1 | 创建负载均衡器 | 28 |
| 7.1.1 | 导航到负载均衡器服务 | 28 |
| 7.1.2 | 负载均衡器基本信息 | 29 |
| 7.2 | 更新负载均衡器配置 | 30 |
| 7.2.1 | 添加第二个前端配置 | 30 |
| 7.2.2 | 配置第二个前端 | 30 |
| 7.2.3 | 添加后端池 | 31 |
| 8 | 虚拟机部署 | 31 |
| 8.1 | 概述 | 31 |
| 8.2 | 创建虚拟机 | 32 |
| 8.2.1 | 添加虚拟机并配置基本信息 | 32 |
| 8.2.2 | 添加数据磁盘以存储日志文件 | 33 |
| 8.2.3 | 配置虚拟机网络接口 | 34 |
| 8.2.4 | 配置虚拟机负载均衡选项 (仅限于分布式服务器) | 34 |
| 8.2.5 | 创建额外的虚拟机 (仅限于分布式服务器) | 35 |
| 8.2.6 | 将虚拟机与应用程序安全组关联 | 35 |
| 9 | 继续负载均衡器配置 (仅限于分布式服务器) | 36 |
| 9.1 | 配置运行状况探测器 | 36 |
| 9.1.1 | 转到 Health Probes 屏幕 | 36 |
| 9.1.2 | 为 Web 流量添加运行状况探测器 | 36 |
| 9.1.3 | 为 Swarm 流量添加运行状况探测器 | 37 |
| 9.1.4 | 为 Websocket 流量添加运行状况探测器 | 37 |
| 9.2 | 配置负载均衡规则 | 38 |
| 9.2.1 | 转到 Load Balancing Rules 屏幕 | 38 |
| 9.2.2 | 创建 Web 流量规则 | 39 |
| 9.2.3 | 创建 Websocket 流量规则 | 39 |
| 9.2.4 | 创建 Swarm 流量规则 | 41 |
| 9.3 | 创建到 NAT 后端流量的出站规则 | 41 |
| 9.3.1 | 添加出站规则 | 42 |
| 9.3.2 | 配置出站规则 | 43 |
| 10 | 使用 Azure Bastion 连接到虚拟机 | 43 |
| 11 | 附录 A - 有关 Active Directory* 集成的说明 | 44 |
| 11.1 | 使用 Active Directory 集成的高层级架构图 | 45 |
| 11.1.1 | 单服务器部署 | 45 |
| 11.1.2 | 分布式服务器部署 | 45 |
| 11.2 | 使用 Azure AD Connect 将 Active Directory 扩展到云 | 45 |

1 简介

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

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

1.1 云计算简介

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

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

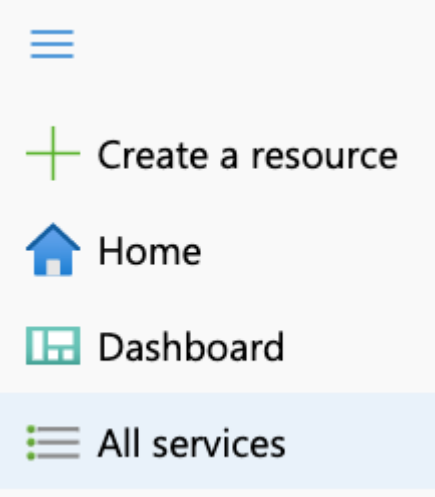
借助像 Azure SQL Server 之类的完全托管服务, 您可以将精力仅放在数据上, 而让云提供商管理提供相关服务的底层硬件和软件。借助在云中运行的虚拟机, 您只需要管理操作系统及其上安装的软件, 而云提供商则管理底层硬件并尽量为您提供最佳的可靠性和可用性。




1.2 操作 Azure 控制台

1.2.1 服务菜单

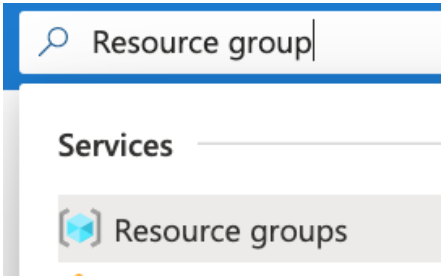
| | |
|---|--|
|  | 通过 http://portal.azure.com/ 登录 Microsoft Azure 门户后, 您会在左上角看到一个菜单图标。 |
|---|--|

1.2.2 展开服务菜单

| | |
|---|--|
|  | 如果单击该图标, 然后选择 All Services, 您将看到一个服务列表, 其中将服务分为“GENERAL”、“COMPUTE”、“NETWORKING”和“SECURITY”等类别。 这可以帮助您探索在各种类别下可能对您组织有用的服务。 |
|---|--|

| | |
|--|--|
| GENERAL (17) ————— ∨ | |
| COMPUTE (35) ————— ∨ | |
| NETWORKING (29) ————— ^ | |
|  Virtual networks | |
|  Load balancers | |
|  CDN profiles | |

1.2.3 按名称搜索服务

| | |
|---|---|
|  | <p>在本指南中，由于我们已经知道所需的服务名称，因此我们将使用屏幕顶部的搜索栏找到该服务，然后从出现的列表中选择它。</p> <p>例如，要创建资源组，我可以在搜索栏中输入“Resource group”，然后单击 Services 类别下方出现的项目。</p> |
|---|---|

1.3 开始之前

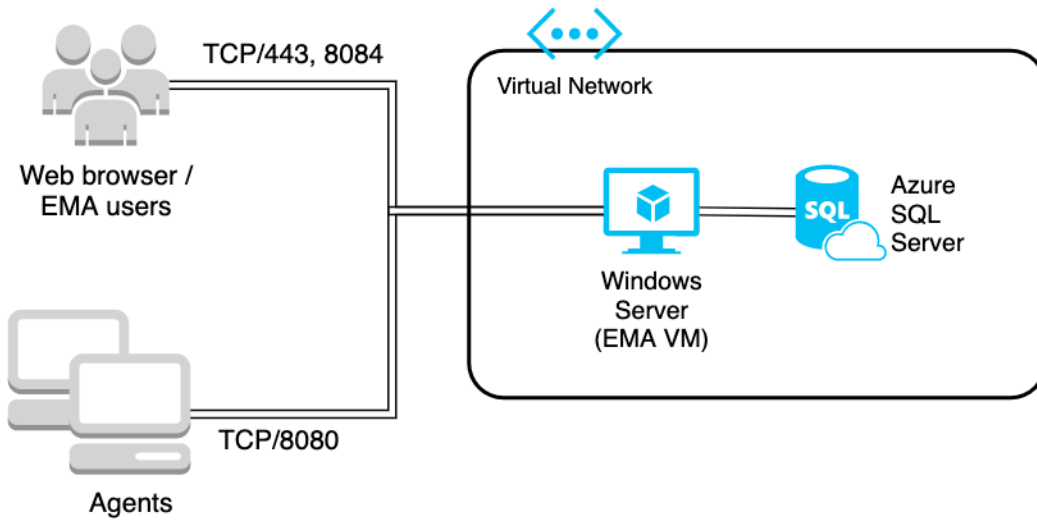
如果您的组织已经有 Azure 帐户，则应要求云管理员授予您足够的访问权限，以便创建本指南中列出的所有资源。

如果您的组织没有 Azure 帐户，或者您希望以个人身份对其进行评估，则可以转到 <https://azure.microsoft.com/en-us/free/> 创建一个免费帐户。

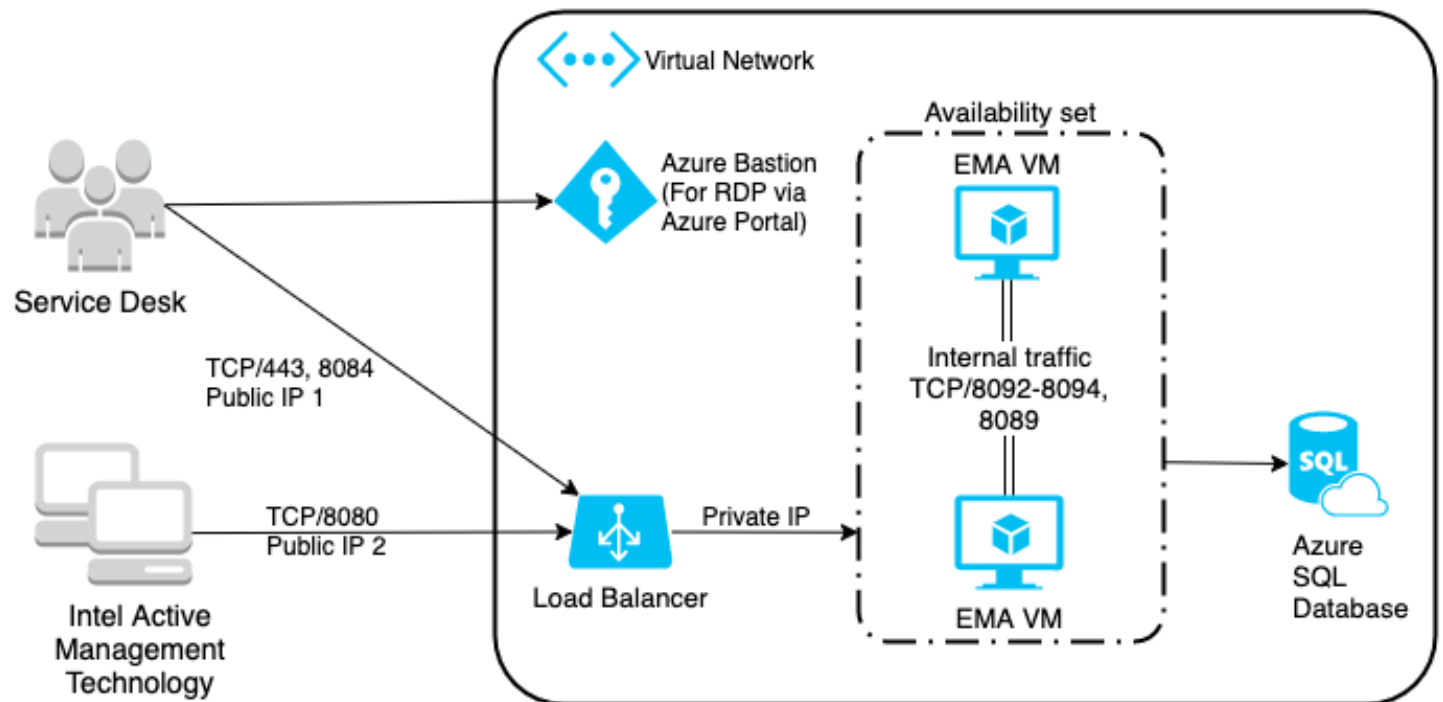
请与您的网络管理员联系，询问是否存在可供使用的首选的地址空间。如果您已经建立了连接到云提供商的 VPN，或者将来要建立此类连接，则您应避免与企业网络重叠，以免出现路由问题。您还需要找出数据是通过哪个源 IP 地址离开组织并到达云端的，以便仅允许受信任的网络通过互联网访问 Intel EMA 虚拟机。

2 高层级架构图

2.1 单服务器部署



2.2 分布式服务器部署



3 资源组部署

3.1 资源组概述

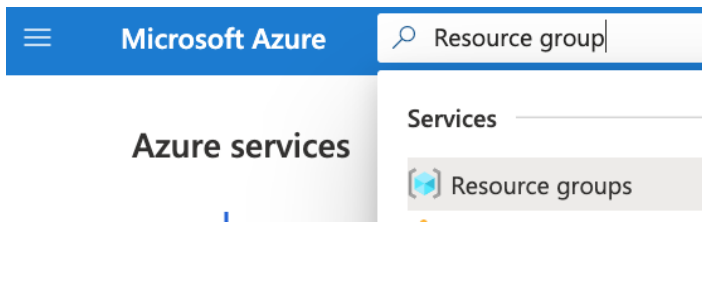
资源组是一个容器，其中包含用于 Azure 解决方案的相关资源，以便您轻松地将它们作为一个组进行部署、更新和删除。您还可以轻松查看该组中所有资源的计费费用。您需要为在 Azure 中部署的所有内容选择一个现有的资源组，所以我们现在先创建一个。

有关资源组的更多信息，请访问以下链接：

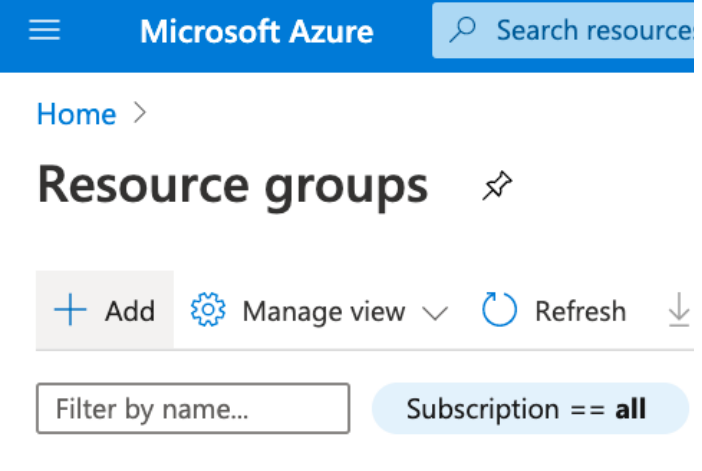
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>。

3.2 创建资源组

3.2.1 选择资源组服务

| | |
|---|--|
|  | 使用屏幕顶部的搜索栏搜索 Resource groups ，然后单击出现的列表项。 |
|---|--|

3.2.2 添加资源组

| | |
|---|-------------------|
|  | 单击 Add 按钮。 |
|---|-------------------|

3.2.3 配置资源组

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 * ⓘ

请输入以下基本详细信息。

- Resource group:** 为资源组输入唯一的名称。
示例: *intel-ema-resources*
- Region:** 选择您要部署资源的区域。
示例: *(US) West US*

注意: 创建其他资源时, 系统可能会提示您输入区域。它应该默认认为您在此处选择的区域, 但是如果没有, 则本指南将提醒您设置适当的区域。

3.2.4 查看和创建

- 单击 **Review + create** 按钮。
- 查看屏幕上的信息, 然后单击 **Create** 按钮。

4 网络部署

4.1 概述

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

创建虚拟网络时, 您将需要提供自定义的私有 IP 地址空间。Azure 将在需要时从该地址空间为资源分配私有 IP 地址。建议避免使用与组织的其他网络范围重叠的地址空间, 以免在网络通过 VPN 连接后产生路由冲突。

创建虚拟网络时, 我们还需要创建至少一个子网。子网让您可以对 VPC 网络分段, 将其一部分的地址空间分配给各个子网。然后, 您可以将 Azure 资源部署到特定的子网中。

我们将创建网络安全组并将其附加到子网, 以允许和控制入站流量。通过在子网上启用服务端点, 可允许流量从虚拟机传输到 SQL Server。

我们将部署 Azure Bastion 服务, 让您可以通过 Azure 门户将 RDP 或 SSH 导入虚拟机, 而不必将虚拟机上的 RDP 端口暴露到互联网上。

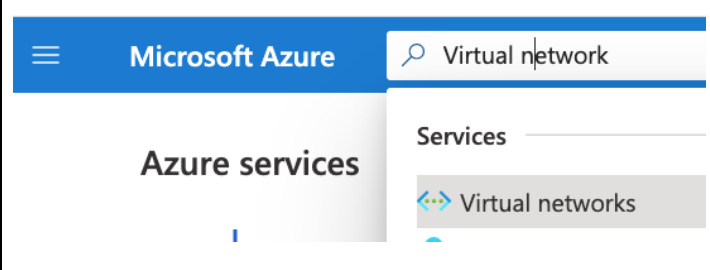
有关本节中部署的网络资源的更多信息, 请访问以下链接或在随后的章节中查找其他链接:

- 虚拟网络: <https://docs.microsoft.com/en-us/azure/virtual-network/>
- VNet 服务端点: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>
- Azure Bastion: <https://docs.microsoft.com/en-us/azure/bastion/>

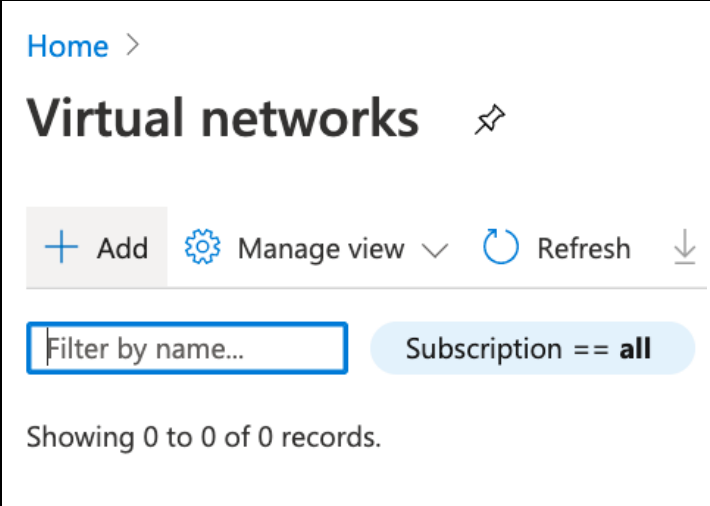
4.2 创建虚拟网络

请按照以下过程创建具有单个子网的虚拟网络。

4.2.1 导航到虚拟网络服务

| | |
|--|---|
|  | <p>使用屏幕顶部的搜索栏搜索 Virtual networks，然后单击出现的列表项。</p> |
|--|---|

4.2.2 添加虚拟网络

| | |
|---|--------------------------|
|  | <p>单击 Add 按钮。</p> |
|---|--------------------------|

4.2.3 配置虚拟网络基本详细信息

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 private networks. VNet is similar to a traditional network that you'd operate in your data center, but it has all the benefits of Azure's infrastructure such as scale, availability, and isolation.

Project details

Subscription * ⓘ

Resource group * ⓘ
[Create new](#)

Instance details

Name *

Region *

请输入以下基本详细信息。

- **Resource group:** 选择先前创建的资源组。
示例: *intel-ema-resources*
- **Name:** 为资源组输入唯一名称。
示例: *intel-ema-network*
- **Region:** 确认要在其中部署资源的区域。
示例: *(US) West US*


单击 **Next: IP Addresses** 按钮并继续下一步。

4.2.4 配置 IPv4 地址空间

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) 

单击垃圾箱图标以删除默认地址空间，然后键入新的 IPv4 地址空间。

示例: 10.250.0.0/24

如果您的公司已建立或将建立与云的私有 IP 连接，您应该咨询您的网络工程团队选择可用的 IP 地址块，避免路由冲突。

4.2.5 为 Intel EMA 服务器添加子网

| | |
|--|--|
| <div><h3>Add subnet ✕</h3><p>Subnet name * <input type="text" value="ema-servers"/></p><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><p>SERVICE ENDPOINTS</p><p>Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more</p><p>Services ⓘ <input type="text" value="Microsoft.Sql"/></p><p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p></div> | <p>单击 Add Subnet 按钮，然后按如下所示配置子网。</p> <p>Subnet name: 输入唯一的子网名称。 示例: <i>ema-servers</i></p> <p>Subnet address range: 输入 IPv4 地址空间 (您之前已提供) 中包含的未使用子网地址范围。 示例: <i>10.250.0.0/26</i></p> <p>从 Services 下拉菜单中，选择 Microsoft.Sql。</p> <p>单击 Add 按钮以确认子网。</p> <p>单击 Next: Security 按钮。</p> |
|--|--|

4.2.6 启用 Azure Bastion

| | |
|---|--|
| <div><p>Basics IP Addresses Security Tags Review + create</p><p>BastionHost ⓘ <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p><p>Bastion name * <input type="text" value="EmaBastion"/></p><p>AzureBastionSubnet address space * <input type="text" value="10.250.0.64/26"/> 10.250.0.64 - 10.250.0.127 (64 addresses)</p><p>Public IP address * <input type="text" value="(New) EmaBastion"/> Create new</p><p>DDoS Protection Standard ⓘ <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p><p>Firewall ⓘ <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p></div> | <p>按如下所示配置 Security 设置。</p> <p>BastionHost: 选择 <i>Enable</i></p> <p>Bastion name: 输入唯一的 Bastion 名称。 示例: <i>EmaBastion</i></p> <p>AzureBastionSubnet address space: 输入虚拟网络的地址空间中包含的未使用的地址空间。必须为 /26 或更大。 示例: <i>10.250.0.64/26</i></p> <p>Public IP address: 单击 Create new 链接，提供唯一的名称，然后单击 OK 按钮。 示例: <i>EmaBastion</i></p> |
|---|--|

4.2.7 审阅

单击 **Review + create** 按钮。

查看屏幕上的网络详细信息，然后单击 **Create** 按钮。

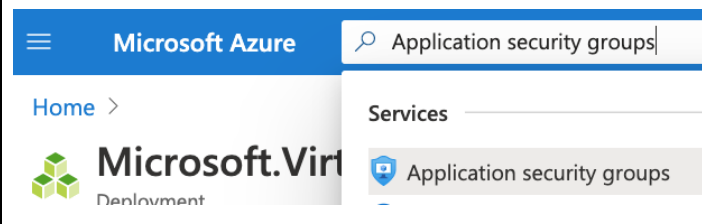
4.3 应用程序安全组 (ASG)

您可以将 ASG 视为可以应用于虚拟机的特殊标记，以便通过防火墙规则更轻松地将虚拟机定位为目标，相关设置将在“网络安全组”部分中完成。为了做好准备，我们将通过以下步骤创建一个 ASG。

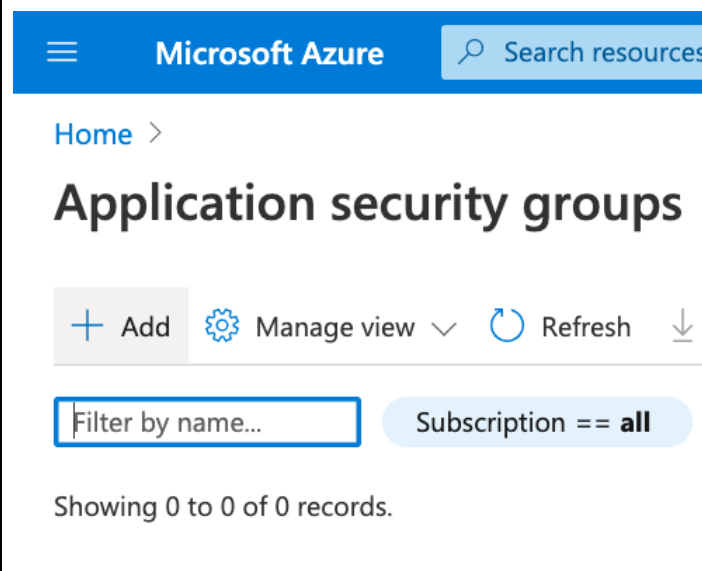
有关应用程序安全组的更多信息，请访问以下链接：

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups>。

4.3.1 导航到应用程序安全组服务

| | |
|--|--|
|  | <p>使用屏幕顶部的搜索栏搜索 Application security groups，然后单击出现的列表项。</p> |
|--|--|

4.3.2 添加应用程序安全组

| | |
|---|--------------------------|
|  | <p>单击 Add 按钮。</p> |
|---|--------------------------|

4.3.3 配置应用程序安全组 (ASG)

Home > Application security groups >

Create an application security group

Basics Tags Review + create

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

请输入以下基本详细信息。

- Resource group:** 选择先前创建的资源组。
- Name:** 为 ASG 输入唯一名称。
示例: *ema-servers*
- Region:** 确认要在其中部署资源的区域。

单击 **Review + create** 按钮。

查看屏幕上的信息, 然后单击 **Create** 按钮。

4.4 网络安全组

网络安全组 (NSG) 包含安全规则, 可允许或拒绝发送到或接收自多类 Azure 资源的入站和出站网络通信。对于每个规则, 您可以指定来源和目标、端口和协议。

创建 NSG 时, Azure 包含一组无法删除的默认规则, 但是它们的优先级非常低, 如果有需要, 您一般可以使用优先级更高的规则覆盖它们。默认规则如下所示:

AllowVNetInBound: 允许虚拟网络中资源之间的所有流量。

AllowAzureLoadBalancerInBound: 允许流量从 Azure 负载均衡器传输到您的虚拟网络。

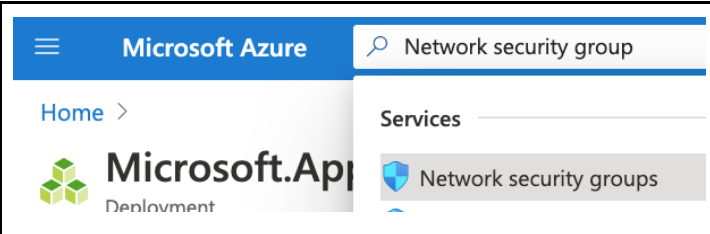
DenyAllInbound: 拒绝从任何来源到任何来源的所有入站流量。

在本节中, 我们将创建一个 NSG 并添加需要的所有规则, 以允许与我们的 Intel EMA 虚拟机通信。我们将创建第二个 NSG, 以允许 Azure Bastion 子网所需的流量。

有关网络安全组的更多信息, 请访问以下链接: <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>。

4.4.1 为 Intel EMA 服务器子网创建网络安全组

4.4.1.1 导航到网络安全组服务



Microsoft Azure

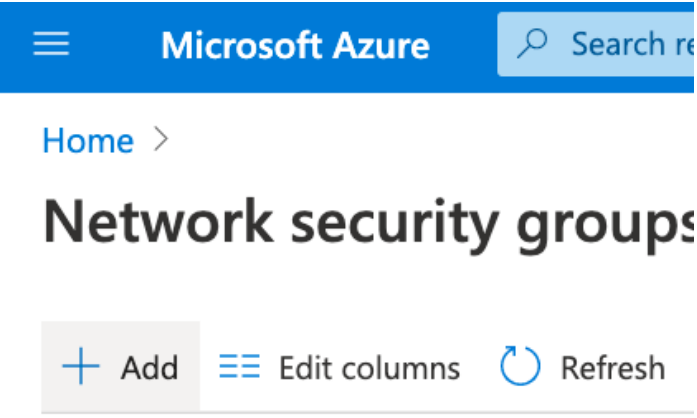
Search: Network security group

Services

- Network security groups

使用屏幕顶部的搜索栏搜索 **Network security groups**, 然后单击出现的列表项。

4.4.1.2 添加网络安全组



单击 **Add** 按钮。

4.4.1.3 配置网络安全组 (NSG) 的基本详细信息



请输入以下基本详细信息。

- **Resource group**: 选择先前创建的资源组。
- **Name**: 为 NSG 输入唯一名称。
示例: *ema-server-nsg*
- **Region**: 确认要在其中部署资源的区域。

单击 **Review + create** 按钮。

查看屏幕上的网络详细信息，然后单击 **Create** 按钮。

当看到部署成功的弹出消息时，单击 **Go To Resource** 按钮。

4.4.2 配置网络安全组

4.4.2.1 导航到入站安全规则



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 |

从安全组侧栏的 **Settings** 下，选择 **Inbound security rules**。

注意：按照下面的步骤创建各个规则后，请等待规则创建完成并显示在列表中，以便 Azure 可以正确地自动增加优先级。

4.4.2.2 创建 RDP 规则

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

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *IP Addresses*
- **Source IP addresses/CIDR ranges:** 输入创建虚拟网络时，我们定义的 Azure Bastion 子网的 CIDR 范围。
示例: 10.250.0.64/26
- **Source port ranges:** *
- **Destination:** *Application security group*
- **Destination application security group:** *ema-servers* (或您命名的其他名称)
- **Destination port ranges:** *3389*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 为规则输入唯一的名称。
示例: *RDP*
- **Description:** *Allow RDP from trusted sources to Intel EMA servers*

完成后，单击屏幕底部的 **Add** 按钮。

4.4.2.3 创建 Web 流量规则

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

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *IP Addresses*
- **Source IP addresses/CIDR ranges:** 输入您信任的网络，该网络应获得从互联网访问 EMA Web 界面的许可。或者，如果您不希望设限，可以将“Source”设置为“Any”。
- **Source port ranges:** *
- **Destination:** *Application security group*
- **Destination application security group:** *ema-servers* (或您命名的其他名称)
- **Destination port ranges:** *443,8084*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 为规则输入唯一的名称。
示例: *Web*
- **Description:** *Allow web traffic from trusted sources to Intel EMA servers*

完成后，单击屏幕底部的 **Add** 按钮。

4.4.2.4 创建 Swarm 流量规则

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

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *Any*
- **Source port ranges:** *
- **Destination:** *Application security group*
- **Destination application security group:** *ema-servers* (或您命名的其他名称)
- **Destination port ranges:** *8080*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 为规则输入唯一的名称。
示例: *swarm*
- **Description:** *Allow swarm traffic from any source to Intel EMA servers*

完成后，单击屏幕底部的 **Add** 按钮。

4.4.2.5 添加内部流量规则（仅限于分布式服务器）

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

如果要部署分布式服务器架构，请遵循此过程，否则可以跳过。
单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *Application security group*
- **Source application security group:** *ema-servers* (或您命名的其他名称)
- **Source port ranges:** *
- **Destination:** *Application security group*
- **Destination application security group:** *ema-servers* (或您命名的其他名称)
- **Destination port ranges:** *8092-8094,8089*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 请输入唯一的名称。
示例: *ema_internal*
- **Description:** *Allow internal communication between Intel EMA servers*

完成后，单击屏幕底部的 **Add** 按钮。

4.4.3 审阅

完成后，您应该会看到如下图所示的表格。

注意：如果您要部署分布式服务器架构，则应只包含 *ema_internal* 规则。

[+](#) Add [🔄](#) Default rules [🔄](#) Refresh

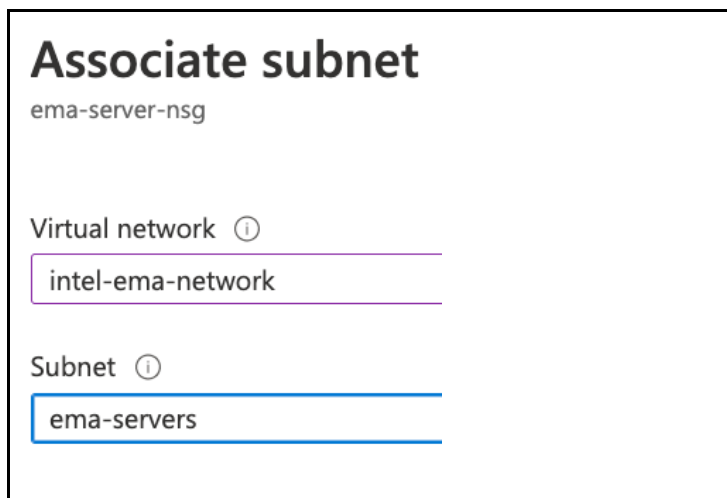
| Priority | Name | Port | Protocol | Source | Destination |
|----------|-------------------------------|----------------|----------|-----------------------|-----------------------|
| 100 | i RDP | 3389 | TCP | 10.250.0.64/26 | 🛡️ ema-servers |
| 110 | i web | 443,8084 | TCP | ██████████ | 🛡️ ema-servers |
| 120 | i swarm | 8080 | TCP | Any | 🛡️ ema-servers |
| 130 | i 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 将网络安全组与子网关联

4.4.4.1 导航到网络安全组的子网关联

从安全组侧边栏的 **Settings** 下，选择 **Subnets**，然后单击 **Associate** 按钮。

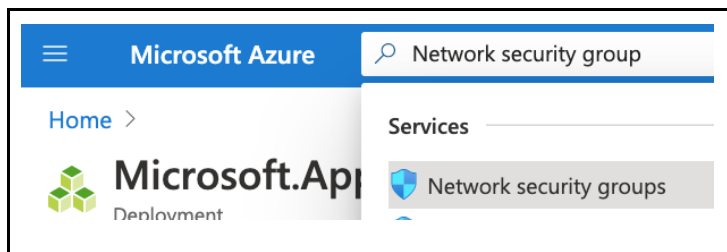
4.4.4.2 将网络安全组与子网关联

| | |
|--|--|
|  | <p>选择您先前为 EMA 服务器创建的子网，然后单击 OK。</p> |
|--|--|

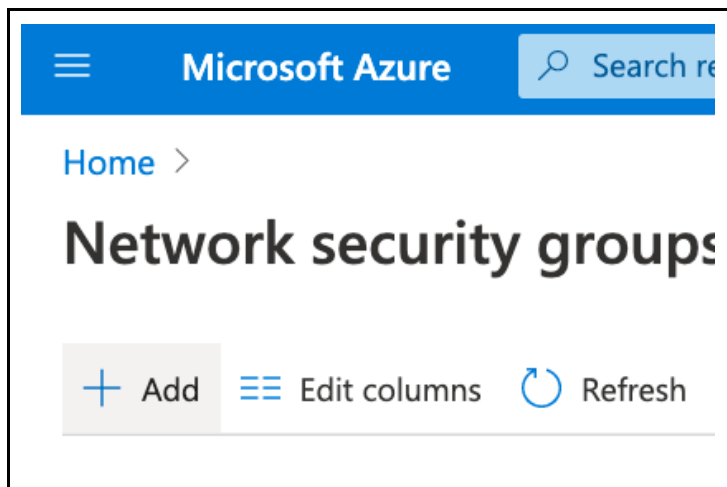
4.4.5 为 Azure Bastion 子网创建网络安全组

请参考: <https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg>

4.4.5.1 导航到网络安全组服务

| | |
|---|--|
|  | <p>使用屏幕顶部的搜索栏搜索 Network security groups，然后单击出现的列表项。</p> |
|---|--|

4.4.5.2 添加网络安全组

| | |
|--|--------------------------|
|  | <p>单击 Add 按钮。</p> |
|--|--------------------------|

4.4.5.3 配置网络安全组的基本详细信息

Create network security group

Basics Tags Review + create

Project details

Subscription * IGNW-Intel-EMA

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

Instance details

Name * ema-bastion-nsg

Region * (US) West US

请输入以下基本详细信息。

- **Resource group**: 选择先前创建的资源组。
- **Name**: 请输入唯一的名称。
示例: *ema-bastion-nsg*
- **Region**: 确认要在其中部署资源的区域。

单击 **Review + create** 按钮。

查看屏幕上的网络详细信息, 然后单击 **Create** 按钮。

当看到部署成功的弹出消息时, 单击 **Go To Resource** 按钮。

4.4.6 配置网络安全组

4.4.6.1 导航到入站安全规则

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 |

从安全组侧栏的 **Settings** 下, 选择 **Inbound security rules**。

注意: 按照下面的步骤创建各个规则后, 请等待规则创建完成并显示在列表中, 以便 Azure 可以正确地自动增加优先级。

4.4.6.2 创建允许 HTTPS 到 Azure Bastion 的规则

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

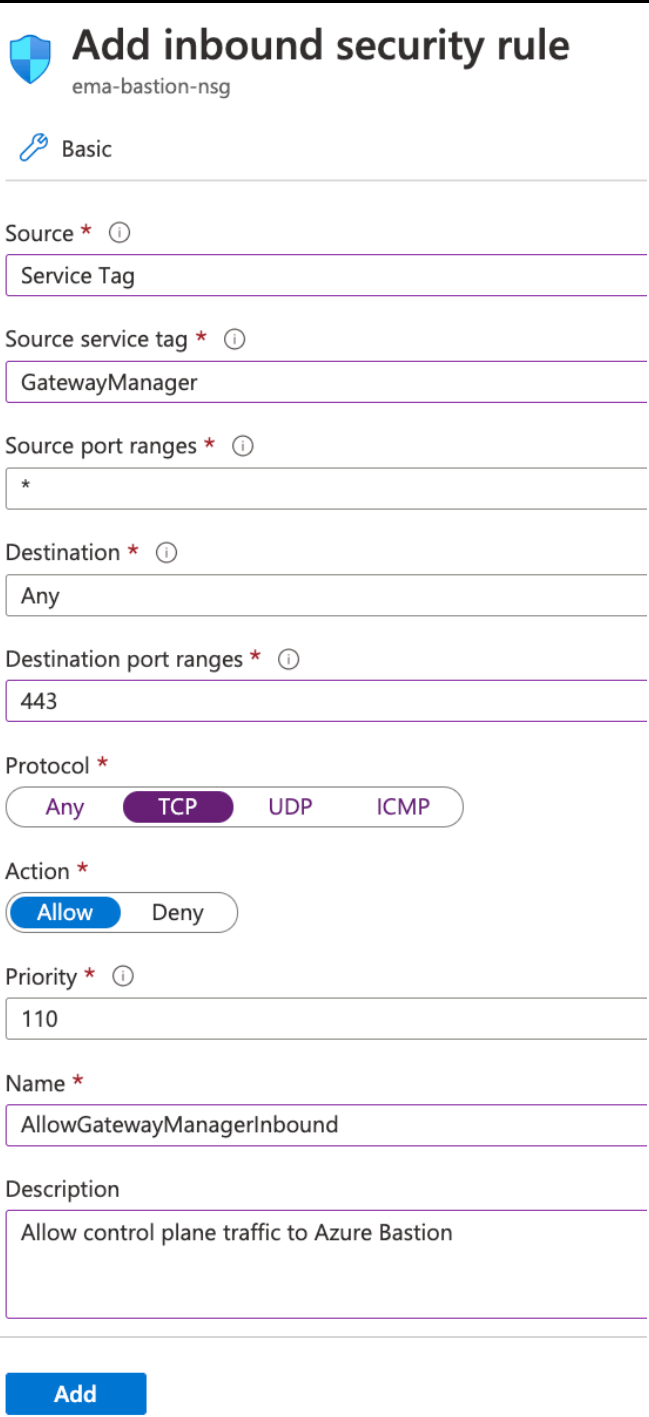
Add

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

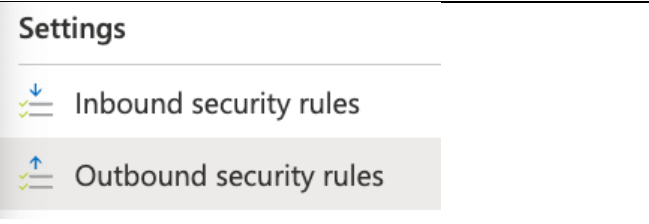
- **Source:** *Service Tag*
- **Source service tag:** *Internet*
- **Source port ranges:** *
- **Destination:** *Any*
- **Destination port ranges:** *443*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 请输入唯一的名称。
示例: *AllowHttpsInbound*
- **Description:** *Allow HTTPS to Azure Bastion*

单击屏幕底部的 **Add** 按钮。

4.4.6.3 创建允许 Gateway Manager 到 Azure Bastion 的规则

| | |
|--|--|
|  <p>Add inbound security rule ema-bastion-nsg</p> <p>Basic</p> <p>Source * ⓘ Service Tag</p> <p>Source service tag * ⓘ GatewayManager</p> <p>Source port ranges * ⓘ *</p> <p>Destination * ⓘ Any</p> <p>Destination port ranges * ⓘ 443</p> <p>Protocol * Any TCP UDP ICMP</p> <p>Action * Allow Deny</p> <p>Priority * ⓘ 110</p> <p>Name * AllowGatewayManagerInbound</p> <p>Description Allow control plane traffic to Azure Bastion</p> <p>Add</p> | <p>单击屏幕顶部附近的 Add 按钮，并按如下所示配置规则。</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: 使用自动分配的值。• Name: 请输入唯一的名称。 示例: <i>AllowGatewayManagerInbound</i>• Description: <i>Allow control plane traffic to Azure Bastion</i> <p>单击屏幕底部的 Add 按钮。</p> |
|--|--|

4.4.7 配置出站安全规则

| | |
|--|---|
|  <p>Settings</p> <p>Inbound security rules</p> <p>Outbound security rules</p> | <p>在侧边栏的 Inbound security rules 下方，单击“Outbound security rules”。</p> |
|--|---|

4.4.7.1 启用到虚拟网络的 SSH/RDP 出口流量

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

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *Any*
- **Source port ranges:** *
- **Destination:** *Service Tag*
- **Destination service tag:** *VirtualNetwork*
- **Destination port ranges:** *22,3389*
注意：Azure Bastion 需要同时允许两个端口，即使您不需要使用其中一个。
- **Protocol:** *Any*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 请输入唯一的名称。
示例： *AllowGatewayManagerInbound*
- **Description:** *Allow RDP connections from Azure Bastion to our virtual network*

单击屏幕底部的 **Add** 按钮。

4.4.7.2 启用到 Azure 服务的出口

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

单击屏幕顶部附近的 **Add** 按钮，并按如下所示配置规则。

- **Source:** *Any*
- **Source port ranges:** *
- **Destination:** *Service Tag*
- **Destination service tag:** *AzureCloud*
- **Destination port ranges:** *443*
- **Protocol:** *TCP*
- **Action:** *Allow*
- **Priority:** 使用自动分配的值。
- **Name:** 请输入唯一的名称。
示例: *AllowAzureCloudOutbound*
- **Description:** *Allow Azure Bastion to connect to public Azure service endpoints.*

单击屏幕底部的 **Add** 按钮。

4.4.8 将网络安全组与 Azure Bastion 子网关联

4.4.8.1 导航到网络安全组的子网关联

| | |
|--|---|
| | <p>从安全组侧边栏的 Settings 下，选择 Subnets，然后单击 Associate 按钮。</p> |
|--|---|

4.4.8.2 将网络安全组与子网关联

| | |
|--|--|
| | <p>选择您先前为 EMA 服务器创建的子网，然后单击 OK。</p> |
|--|--|

5 SQL 服务器部署

5.1 概述

Azure 具有完全托管的平台即服务 (PaaS) 数据库引擎，该引擎包括两个组件：

面向 Azure 的 Intel® EMA Web 部署指南 - 2020 年 10 月

- 逻辑 SQL 服务器，它具有与其关联的 DNS 主机名。
- 一个或多个 SQL 数据库，可以分别对其进行配置以实现规模和性能调节。

作为一项托管服务，Azure 无需用户参与即可处理大部分的数据库管理功能，例如升级、补丁、备份和监视，以便让数据库在 SQL 服务器数据库引擎的最新稳定版上以 99.99% 的可用性保持运行。它还提供了标准的高可用性以及高级 HA 模型。

SQL 数据库让您轻松地利用两种不同的购买模型定义和扩展性能：[vCore-based purchasing model](#) 和 [DTU-based purchasing model](#)。

- [vCore-based purchasing model](#) 让您可以选择 vCore 的数量、内存容量、存储容量和速度。
- [DTU-based purchasing model](#) 按照三个服务等级提供了计算、内存和 I/O 资源的混合配置，以支持从轻到重的数据库工作负载。

要将其与我们的 Intel EMA 服务器一起使用，我们只需要提前创建逻辑 SQL 服务器。Intel EMA 安装过程中会动态创建 SQL 数据库。完成该安装过程后，可以返回到 Azure 管理控制台以查看数据库设置并根据需要进行调整。

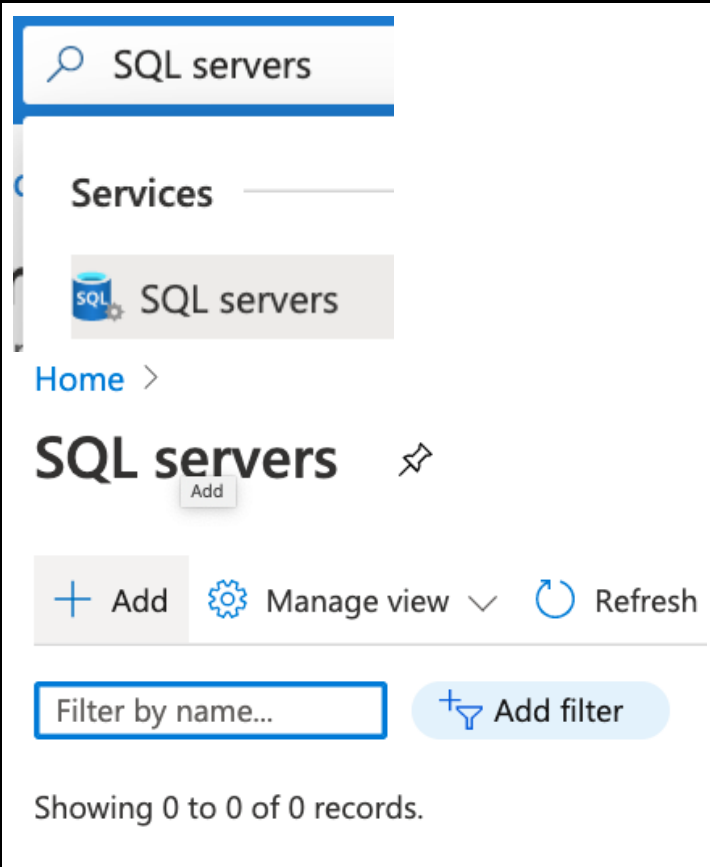
有关 Azure SQL 服务器、SQL 数据库和高可用性模型的更多信息，请访问以下链接：

<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 创建 SQL 服务器

请按照以下过程创建一个 Azure SQL 服务器，并启用从我们的虚拟机子网对它的访问权限。

5.2.1 添加新的 SQL 服务器

| | |
|---|---|
|  | <p>使用屏幕顶部的搜索栏搜索 SQL servers，然后单击出现的列表项。</p> <p>单击 Add 按钮。</p> |
|---|---|

5.2.2 配置 SQL 服务器的基本详细信息

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 * ✓

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

请输入以下基本详细信息。

- **Resource group:** 选择先前创建的资源组。
- **Server name:** 输入一个全球唯一的名称。
示例: *ema-demo*
注意: 您在此处选择的名称将与后缀 ".database.windows.net" 一起构成 DNS 名称, 您可以在 Intel EMA 安装过程中使用该名称访问数据库。
- **Location:** 确认要在其中部署资源的区域。
- 提供管理员账户的用户名和密码。

单击 **Review + create** 按钮。

查看屏幕上的信息, 然后单击 **Create** 按钮, 再转到创建时所在的资源。

5.2.3 配置 SQL 服务器防火墙

ema-demo | Firewa

SQL server

Search (Cmd+/) <<

Security

- Advanced data security
- Auditing
- Firewalls and virtual networks**
- Private endpoint connections
- Transparent data encryption

从 SQL 服务器侧栏中的 **Security** 部分中, 选择 **Firewalls and virtual networks**。

i Connections from the VNET/Subnet specified below provides access to all databases in ema-demo.

Virtual networks

+ Add existing virtual network

+ Create new virtual network

| Rule name | Virtual network | Subnet |
|--------------------------------|-----------------|--------|
| No vnet rules for this server. | | |

在右侧窗口中，向下滚动并单击 **Add existing virtual network**。

5.2.3.1 命名规则并选择现有的网络和子网

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 |

输入虚拟网络规则详细信息，如下所示：

- Name:** 请输入唯一的名称。
示例: *allow-ema-servers*
- Virtual network:** 确保已选择先前创建的虚拟网络。
- Subnet name / Address prefix:** 确保已选择先前创建的子网。

单击 **OK** 按钮。

6 可用性集合 (仅限于分布式服务器)

“可用性集合”是虚拟机的逻辑分组，它可以指示 Azure 确保虚拟机能够在多个物理服务器、计算机架、存储单元和网络交换机上运行。这样做的目的是，如果发生硬件或软件故障，则仅影响您的一部分虚拟机，而您的整体解决方案可以保持正常运行。

请按照以下过程创建“可用性集合”，以便稍后创建虚拟机时分配给虚拟机。

如果仅部署单个服务器，则可以跳过本部分。

有关“可用性集合”的更多信息，请访问以下链接：

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

6.1 创建“可用性集合”

1. 使用屏幕顶部的搜索栏搜索 **Availability sets**，然后单击出现的列表项。
2. 单击 **Add** 按钮。
3. 请输入以下基本信息。
 - a. **Resource group**: 选择先前创建的资源组。
 - b. **Name**: 请输入唯一的名称。
示例: *ema-servers*
 - c. **Region**: 确认要在其中部署资源的区域。
4. 单击 Review + create 按钮。
5. 查看屏幕上的信息，然后单击 Create 按钮。

7 负载均衡器部署 (仅限于分布式服务器)

Azure 负载均衡器是第 4 级 (TCP) 负载均衡器，可在应用程序的多个实例之间分配用户流量。通过分散负载，负载平衡可降低应用程序负担过重、运行缓慢或无法工作的风险。负载均衡器运行状况探测器可监视每个虚拟机上的特定端口，并且仅将流量分配给正在工作的虚拟机。

我们将仅使用最初定义的前端配置来创建负载均衡器。稍后创建虚拟机时，我们会将其附加到负载均衡器的后端。负载均衡器将具有单独的前端 IP 地址，以用于 Web 流量和 Swarm 流量。

将虚拟机附加到负载均衡器后，我们会返回到负载均衡器配置，设置运行状况检查和转发规则，以将传入流量定向到适当的后端虚拟机端口。

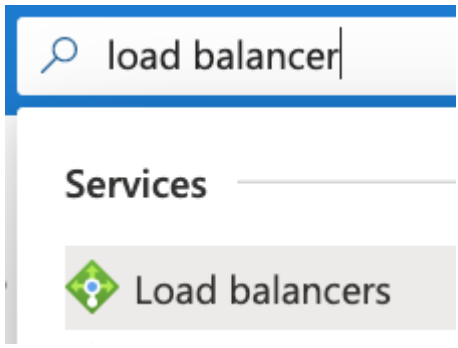
如果仅部署单个服务器，则可以跳过本部分。

有关跨 Windows* 虚拟机进行负载均衡的更多信息，请访问以下链接：

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-load-balancer>

7.1 创建负载均衡器

7.1.1 导航到负载均衡器服务

| | |
|--|---|
|  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 and the text 'Load balancers'. | <p>使用屏幕顶部的搜索栏搜索 Load balancers，然后单击出现的列表项。</p> |
|--|---|

7.1.2 负载均衡器基本信息

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 *

Resource group * [Create new](#)

Instance details

Name * ✓

Region * ✓

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 * ✓

Public IP address SKU

Assignment Dynamic Static

Add a public IPv6 address No Yes

单击 **Add** 按钮。

请输入以下基本信息。

- **Resource group:** 选择先前创建的资源组。
- **Name:** 请输入唯一的名称。
示例: *ema-load-balancer*
- **Region:** 确认要在其中部署资源的区域。
- **Type:** 请选择 *Public*
- **SKU:** *Standard*
- **Public IP address:** *Create new*
- **Public IP address name:** *ema-web-lb-ip*

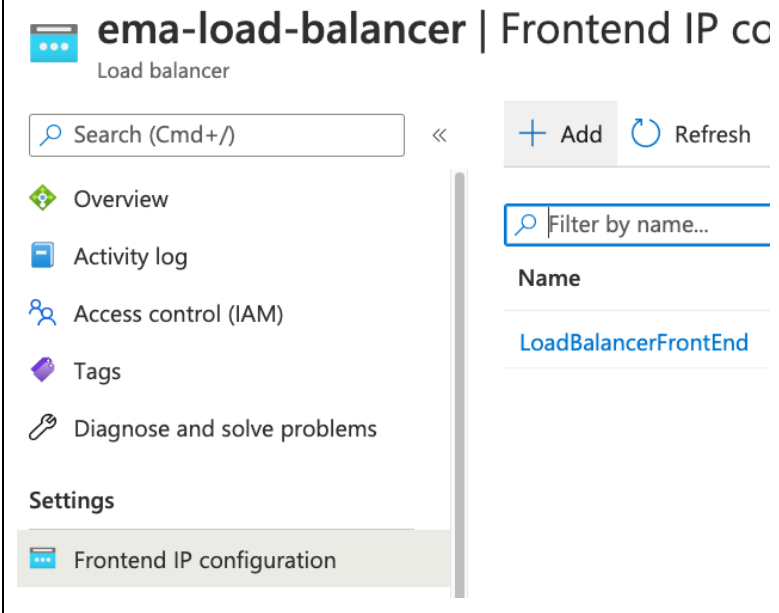
单击 **Review + create** 按钮。

查看屏幕上的信息，然后单击 **Create** 按钮。

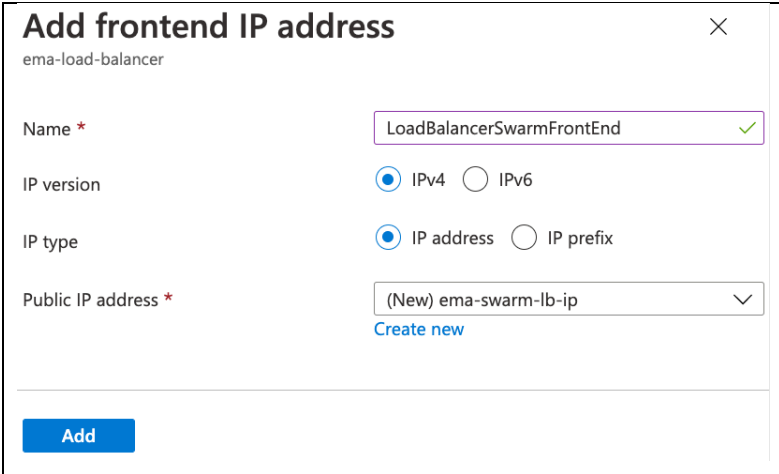
部署成功后，单击 **Go to Resource** 按钮。

7.2 更新负载均衡器配置

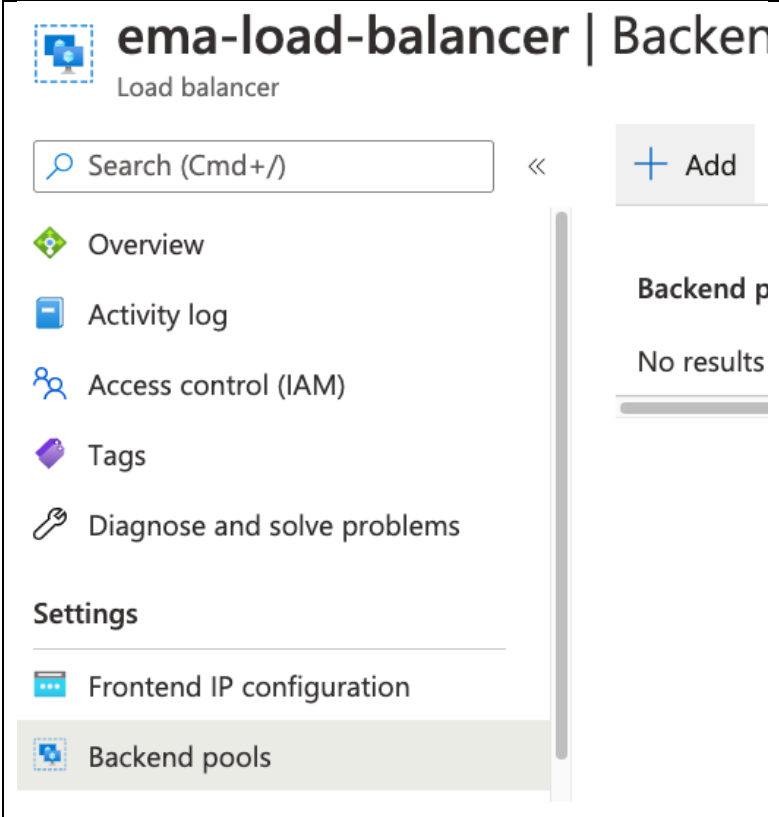
7.2.1 添加第二个前端配置

| | |
|--|---|
|  | <p>在侧边栏中的 Settings 下，单击 Frontend IP Configuration。</p> <p>单击 Add 按钮。</p> |
|--|---|

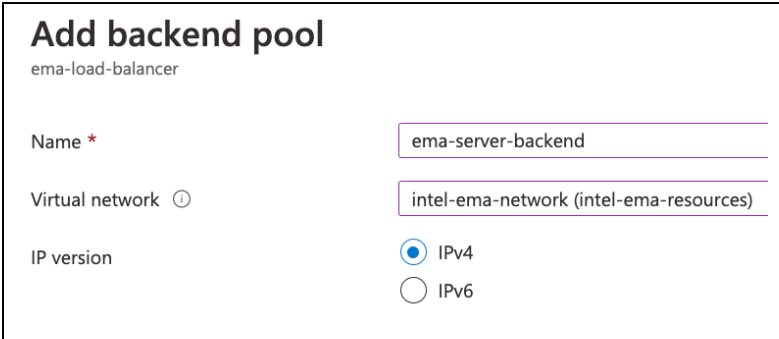
7.2.2 配置第二个前端

| | |
|---|--|
|  | <p>为前端输入唯一的名称。 示例: <i>LoadBalancerSwarmFrontEnd</i></p> <p>对于公共 IP 地址，单击 Create new 链接，然后为 IP 地址命名。 示例: <i>ema-swarm-lb-ip</i></p> <p>单击 Add 按钮。</p> |
|---|--|

7.2.3 添加后端池

| | |
|--|--|
|  | <p>在侧边栏中的 Settings 下，单击 Backend pools。 单击 Add 按钮。</p> |
|--|--|

配置后端池

| | |
|--|---|
|  | <p>输入唯一的后端池名称。 示例: <i>ema-server-backend</i></p> <p>选择您的现有虚拟网络。</p> <p>单击 Add 按钮。</p> <p>后面当我们创建虚拟机时，该后端池可供我们选择。</p> |
|--|---|

8 虚拟机部署

8.1 概述

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

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

对于分布式服务器部署，这些额外的步骤已包括在下面的过程中，但如果您是单服务器部署，即可跳过这些步骤。这些步骤包括创建第二个虚拟机、将虚拟机与可用性集合关联，以及将虚拟机附加到负载均衡器。

有关基于 Windows 的虚拟机的更多信息，请访问以下链接：

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/overview>

8.2 创建虚拟机

8.2.1 添加虚拟机并配置基本信息

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 ✓

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

使用屏幕顶部的搜索栏搜索 **Virtual machines**，然后单击出现的列表项。

单击 **Add** 按钮。

如下配置虚拟机基本信息：

- **Resource group**：选择先前创建的资源组。
- **Name**：请输入唯一的名称。
示例：*ema-server-1*
- **Region**：确认要在其中部署资源的区域。
- **Availability options**：
 - (仅限于单服务器) *No infrastructure redundancy required*
 - (仅限于分布式服务器) *Availability set*
- **Availability set** (仅限于分布式服务器)：选择先前创建的“可用性集合”。
- **Image**：选择最新支持的 Windows Server 映像
- **Size**：选择机器的规格。
推荐：*Standard_E2sv3 - 2 vcpus, 16 GiB memory*
- **Azure Spot instance**: *No*
- 提供管理员账户信息
- **Public inbound ports**: *None*

单击 **Next: Disks** 按钮。

8.2.2 添加数据磁盘以存储日志文件

8.2.2.1 创建并附加新磁盘

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 | | | |

单击链接 **Create and attach a new disk**。

8.2.2.2 配置新磁盘的详细信息

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 *
Standard HDD
[Change size](#)

Encryption type *

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

OK

按照如下所示配置磁盘详细信息。

- Name:** 接受默认名称或输入唯一的磁盘名称。
- Source type:** *None (empty disk)*
- Size:** 单击“Change size”链接以设置磁盘类型和磁盘大小。我们建议采用 256 GB 标准硬盘驱动器。
- Encryption type:** Default

单击 **OK** 按钮。

8.2.2.3 审查数据磁盘列表

| <p>Data disks</p> <p>You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.</p> <table border="1"><thead><tr><th>LUN</th><th>Name</th><th>Size (GiB)</th><th>Disk type</th><th>Host caching</th></tr></thead><tbody><tr><td>0</td><td>ema-server-1_logs</td><td>256</td><td>Standard HDD</td><td>Read-only</td></tr></tbody></table> <p>Create and attach a new disk Attach an existing disk</p> <p>Advanced</p> <p>Review + create < Previous Next : Networking ></p> | LUN | Name | Size (GiB) | Disk type | Host caching | 0 | ema-server-1_logs | 256 | Standard HDD | Read-only | <p>审查数据磁盘的信息，然后单击 Next: Networking 按钮。</p> <p>注意：启动虚拟机后，您将需要使用 Windows 磁盘管理实用工具来初始化、格式化和挂载存储磁盘。</p> |
|---|-------------------|------------|--------------|--------------|--------------|---|-------------------|-----|--------------|-----------|--|
| LUN | Name | Size (GiB) | Disk type | Host caching | | | | | | | |
| 0 | ema-server-1_logs | 256 | Standard HDD | Read-only | | | | | | | |

8.2.3 配置虚拟机网络接口

| | |
|---|---|
| <p>Basics Disks Networking Management Advanced ...</p> <p>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</p> <p>Network interface</p> <p>When creating a virtual machine, a network interface will be created for you.</p> <p>Virtual network * ⓘ <input type="text" value="intel-ema-network"/> Create new</p> <p>Subnet * ⓘ <input type="text" value="ema-servers (10.250.0.0/26)"/> Manage subnet configuration</p> <p>Public IP ⓘ <input type="text" value="None"/> Create new</p> <p>NIC network security group ⓘ <input checked="" type="radio"/> None <input type="radio"/> Basic <input type="radio"/> Advanced</p> | <p>选择 Networking 选项卡并配置网络接口，如下所示：</p> <ul style="list-style-type: none">• Virtual network: 选择之前创建的 VPC。• Subnet: 确保选择了先前创建的子网。• Public IP: <i>None</i>• NIC network security group: <i>None</i> <p>如果是单服务器部署，请单击 Review + create 按钮，检查屏幕上的信息，然后单击 Create 按钮。</p> <p>如果这是分布式服务器部署，则在下一步中继续网络配置。</p> |
|---|---|

8.2.4 配置虚拟机负载均衡选项（仅限于分布式服务器）

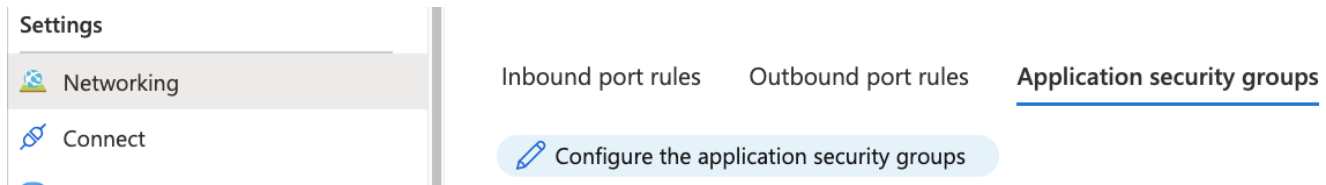
| | |
|---|---|
| <p>Load balancing</p> <p>You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more</p> <p>Place this virtual machine behind an existing load balancing solution? <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Load balancing settings</p> <ul style="list-style-type: none">• 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 <p>Load balancing options * ⓘ <input type="text" value="Azure load balancer"/> Create new</p> <p>Select a load balancer * ⓘ <input type="text" value="ema-load-balancer"/> Create new</p> <p>Select a backend pool * ⓘ <input type="text" value="ema-server-backend"/> Create new</p> | <p>在 Networking 屏幕的下半部分配置 Load balancing。</p> <ul style="list-style-type: none">• Place this virtual machine behind an existing load balancing solution: <i>Yes</i>• Load balancing options: <i>Azure load balancer</i>• Select a load balancer: 选择您先前创建的负载均衡器。• Select a backend pool: 选择您先前创建的后端池。 <p>单击 Review + create 按钮，查看屏幕上的信息，然后单击 Create 按钮以完成虚拟机的创建。</p> |
|---|---|

8.2.5 创建额外的虚拟机（仅限于分布式服务器）

对于分布式服务器部署，请按照上述步骤创建至少一个额外的虚拟机。

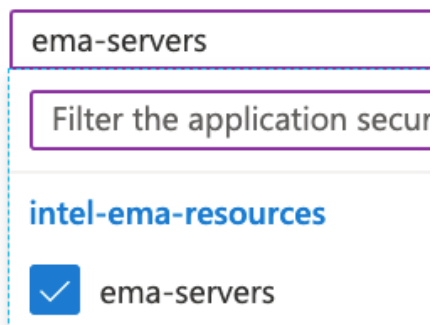
8.2.6 将虚拟机与应用程序安全组关联

对于您创建的每个虚拟机，请在侧边栏中的 **Settings** 类别下，依次选择 **Networking** 和 **Application security groups** 选项卡，然后单击 **Configure the application security groups**。



选择先前创建的应用程序安全组。

Application security groups

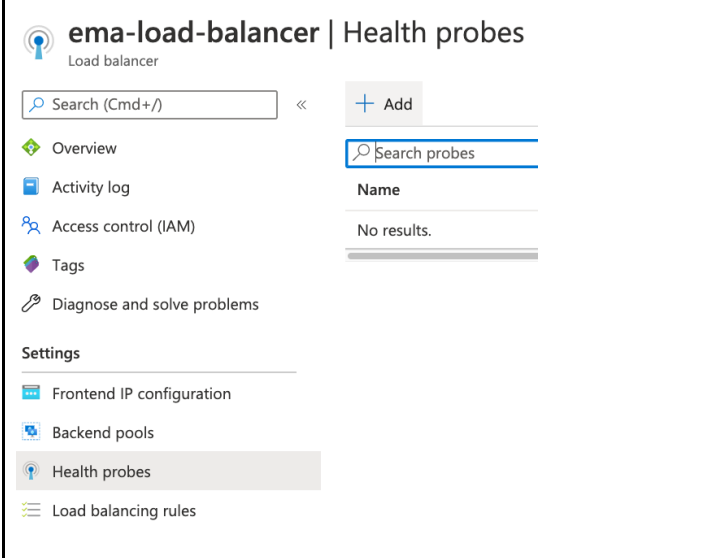


9 继续负载均衡器配置（仅限于分布式服务器）

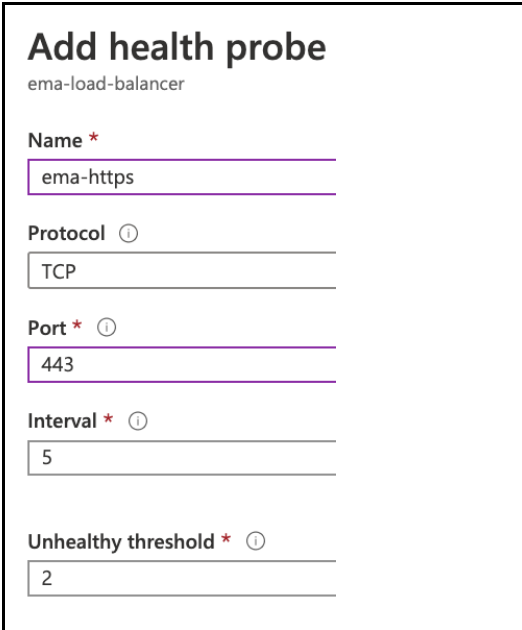
创建虚拟机后，我们现在可以返回到负载均衡器配置，设置运行状况检查和转发规则，以将传入流量走向到适当的后端虚拟机端口。

9.1 配置运行状况探测器

9.1.1 转到 Health Probes 屏幕

| | |
|--|--|
|  | <p>使用屏幕顶部的搜索栏搜索 Load balancers，然后单击出现的列表项。</p> <p>单击先前创建的负载均衡器。</p> <p>在侧边栏的 Settings 下，单击 Health probes。</p> |
|--|--|

9.1.2 为 Web 流量添加运行状况探测器

| | |
|--|---|
|  | <p>单击 Add 按钮，然后按以下方式配置运行状况探测器。</p> <ul style="list-style-type: none">• Name: 请输入唯一的名称。 示例: <i>ema-https</i>• Protocol: <i>TCP</i>• Port: <i>443</i> <p>单击 OK 按钮。</p> |
|--|---|

9.1.3 为 Swarm 流量添加运行状况探测器

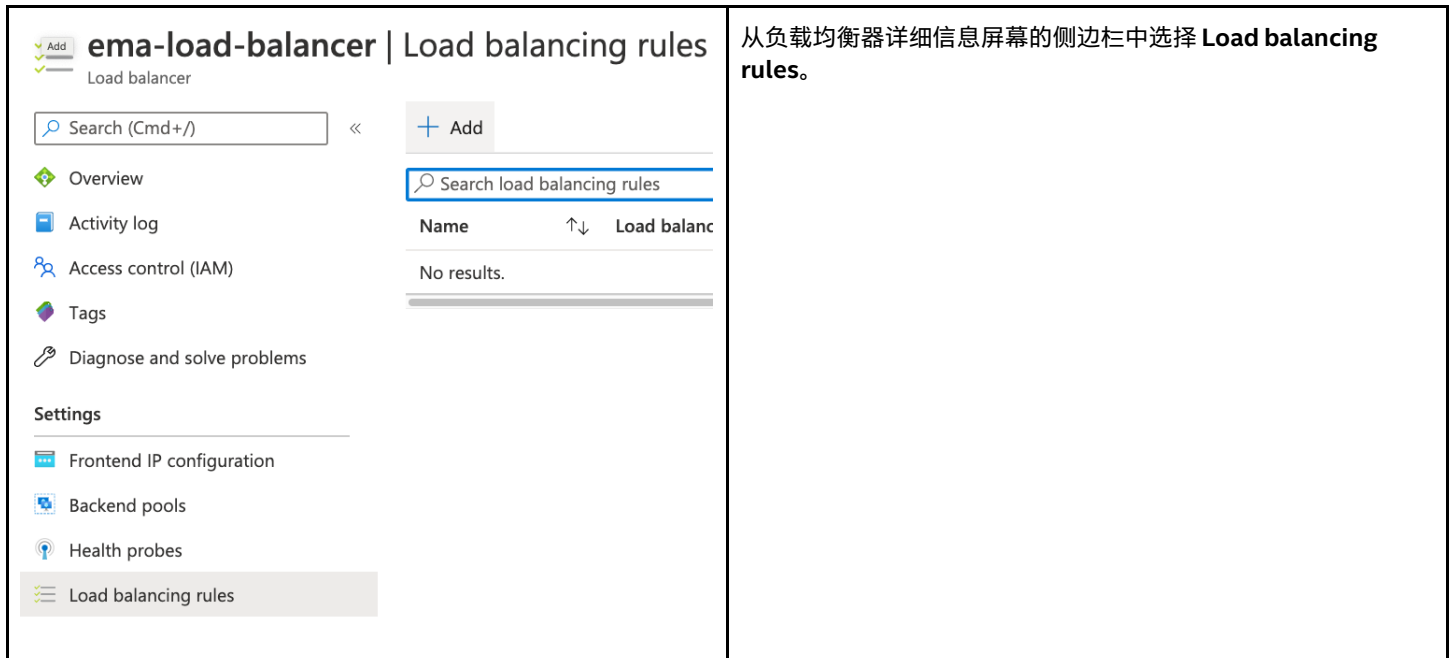
| | |
|--|--|
| <h4>Add health probe</h4> <p>ema-load-balancer</p> <p>Name *</p> <input type="text" value="ema-swarm"/> <p>Protocol ⓘ</p> <input type="text" value="TCP"/> <p>Port * ⓘ</p> <input type="text" value="8080"/> <p>Interval * ⓘ</p> <input type="text" value="5"/> <p>Unhealthy threshold * ⓘ</p> <input type="text" value="2"/> | <p>单击 Add 按钮，然后按以下方式配置运行状况探测器。</p> <ul style="list-style-type: none">• Name: 请输入唯一的名称。 示例: <i>ema-swarm</i>• Protocol: <i>TCP</i>• Port: <i>8080</i> <p>单击 OK 按钮。</p> |
|--|--|

9.1.4 为 Websocket 流量添加运行状况探测器

| | |
|--|--|
| <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>单击 Add 按钮，然后按以下方式配置运行状况探测器。</p> <ul style="list-style-type: none">• Name: 请输入唯一的名称。 示例: <i>ema-websocket</i>• Protocol: <i>TCP</i>• Port: <i>8084</i> <p>单击 OK 按钮。</p> |
|--|--|

9.2 配置负载均衡规则

9.2.1 转到 Load Balancing Rules 屏幕



The screenshot shows the Azure portal interface for the 'ema-load-balancer' resource. The page title is 'ema-load-balancer | Load balancing rules'. Below the title, there is a search bar with the text 'Search (Cmd+/)'. To the right of the search bar is an 'Add' button. Below the search bar is a search input field with the text 'Search load balancing rules'. Below the search input field is a table with the following structure:

| Name | Load balanc |
|-------------|-------------|
| No results. | |

The left sidebar contains the following navigation options:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Frontend IP configuration
 - Backend pools
 - Health probes
 - Load balancing rules (highlighted)

From the load balancer details information screen's sidebar, select **Load balancing rules**.

9.2.2 创建 Web 流量规则

| | |
|--|---|
| <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>单击 Add 按钮，然后按如下所示配置规则。</p> <ul style="list-style-type: none">• Name: <i>ema-https</i>• Frontend IP address: 选择用于 Web 流量的负载均衡器前端。 示例: <i>LoadBalancerFrontEnd</i>• Protocol: <i>TCP</i>• Port: <i>443</i>• Backend Port: <i>443</i>• Backend pool: 选择之前创建的后端池。 示例: <i>ema-server-backend</i>• Health probe: 选择先前创建的 443 端口的健康状况探测器。 示例: <i>ema-https</i>• Session persistence: <i>Client IP</i>• Idle timeout (minutes): 设置为最大值 (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>单击 OK 按钮。</p> |
|--|---|

9.2.3 创建 WebSocket 流量规则

| | |
|--|--|
| | <p>单击 Add 按钮，然后按如下所示配置规则。</p> <ul style="list-style-type: none">• Name: <i>ema-websocket</i>• Frontend IP address: 选择用于 Web 流量的负载均衡器前端。 示例: <i>LoadBalancerFrontEnd</i>• Protocol: <i>TCP</i>• Port: <i>8084</i>• Backend Port: <i>8084</i>• Backend pool: 选择之前创建的后端池。 示例: <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:** 选择先前创建的 8084 端口的运行状况探测器。
示例: *ema-websocket*
- **Session persistence:** *Client IP*
- **Idle timeout (minutes):** 设置为最大值 (30)
- **TCP reset:** *Enabled*
- **Outbound source network address translation:** *Use outbound rules to provide backend pool members access to the internet.*

单击 OK 按钮。

9.2.4 创建 Swarm 流量规则

ema-swarm
ema-load-balancer

Save Discard Delete

Name *
ema-swarm

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ
13.88.132.106 (LoadBalancerSwarmFrontEnd)

Protocol
 TCP UDP

Port *
8080

Backend port * ⓘ
8080

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

Health probe ⓘ
ema-swarm (TCP:8080)

Session persistence ⓘ
None

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](#)

单击 **Add** 按钮，然后按如下所示配置规则。

- **Name:** *ema-swarm*
- **Frontend IP address:** 选择在初始负载均衡器配置期间为 Swarm 流量创建的前端。
示例: *LoadBalancerSwarmFrontEnd*.
- **Protocol:** *TCP*
- **Port:** *8080*
- **Backend Port:** *8080*
- **Backend pool:** 选择之前创建的后端池。
示例: *ema-server-backend*
- **Health probe:** 选择先前创建的 8080 端口的运行状况探测器。
示例: *ema-swarm*
- **Session persistence:** *None*
- **Idle timeout (minutes):** 设置为最大值 (30)
- **TCP reset:** *Enabled*
- **Outbound source network address translation:**
Use outbound rules to provide backend pool members access to the internet.

单击 **OK** 按钮。

9.3 创建到 NAT 后端流量的出站规则

由于我们的虚拟机没有公共 IP 地址，因此我们需要对它们到互联网的出站流量使用源网络地址转换 (SNAT)。不必部署 Azure NAT 网关，我们现有的负载均衡器可以使用前端 IP 地址作为出站流量的源 IP 地址来实现此功能。

有关此主题的更多信息，请访问以下链接：

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections>.

9.3.1 添加出站规则

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 | |

在负载均衡器屏幕侧边栏的 Settings 部分中，单击 **Outbound rules**。
单击 **Add** 按钮。

9.3.2 配置出站规则

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

Frontend IPs

Maximum number of backend instances

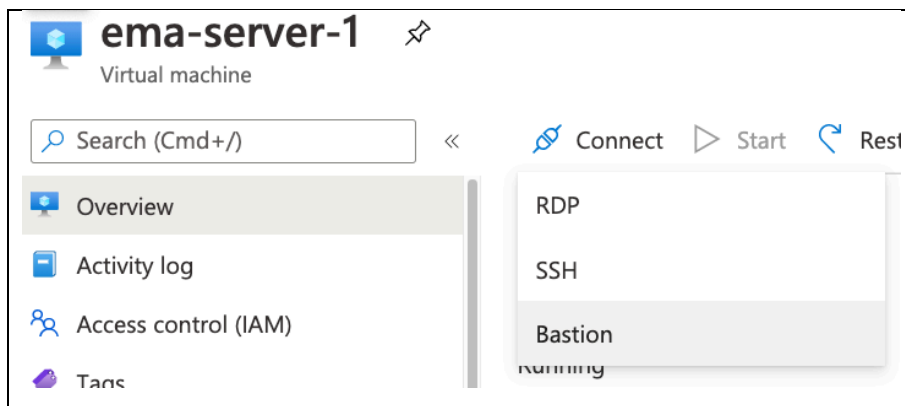
Add

按如下配置出站规则。



- **Name:** 请输入唯一的名称。
示例: *ema-server-outbound*
- **Frontend IP address:** 从下拉菜单中选择所有可用的 IP 地址。
- **Protocol:** *All*
- **TCP reset:** *Enabled*
- **Backend Pool:** 选择先前创建的后端池。
示例: *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:** 对于每个前端 IP 地址, 有 64,000 个端口可用于 SNAT。在此处选择一个数字后, 用端口总数除以该数字, 从而让每个后端实例拥有的可用端口数量相等。由于本部署指南假设我们要部署两个虚拟机, 因此我们在此处输入 **3**, 为以后有需要时再添加一个虚拟机留出空间。

单击 **Add** 按钮

10 使用 Azure Bastion 连接到虚拟机



要登录任何虚拟机, 请转到虚拟机的 Overview 屏幕, 单击 **Connect** 按钮, 然后选择 **Bastion**。

| | |
|--|--|
| <p>RDP SSH BASTION</p> <p> Bastion is an Azure service</p> <p>Use Bastion</p> | <p>单击 Use Bastion 按钮。</p> |
| <p> Connect using Azure Bastion Azure Bastion Service enables you to securely access 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>输入虚拟机的凭据，然后单击 Connect 按钮。</p> <p>此时将打开一个浏览器窗口，用以提供与该虚拟机相连的 RDP 会话。</p> |

11 附录 A - 有关 Active Directory* 集成的说明

您可以通过多种方式将 Active Directory* 与 Microsoft Azure 集成在一起，以便将您的虚拟机加入到域中，并使用 AD 身份验证。由于组织的需求可能千差万别，因此本附录仅简要说明如何将现有的本地目录扩展到云以达成上述目的。云提供商会不定期修改和扩展他们的服务产品，因此在部署生产解决方案之前，您应该自行研究，了解哪些服务最适合您的业务。如需阅读详情，请参考以下链接。

[Azure Active Directory 文档](#)

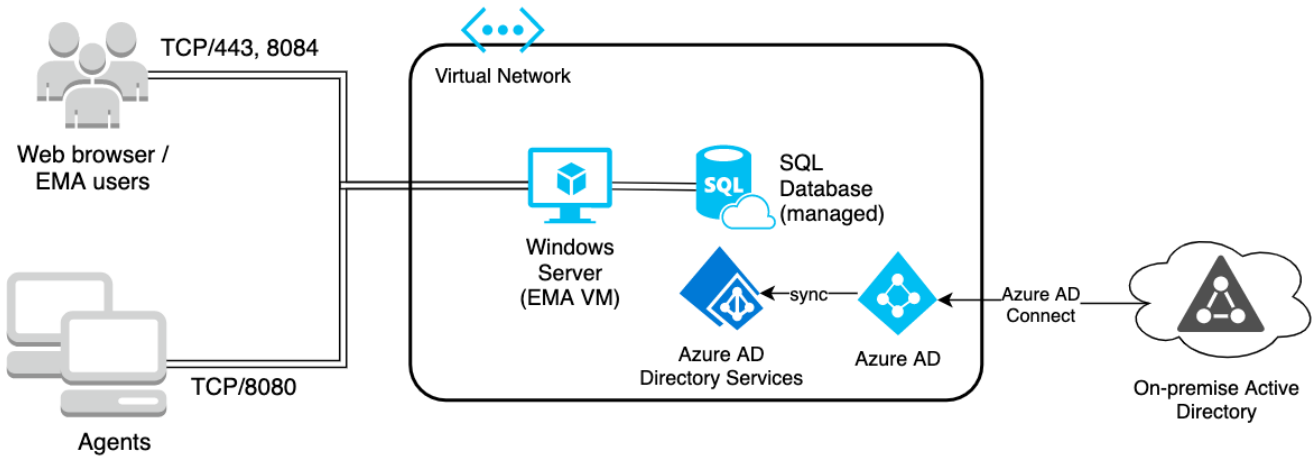
[Azure AD 域服务文档](#)

[比较 Azure 中基于 Active Directory 的服务](#)

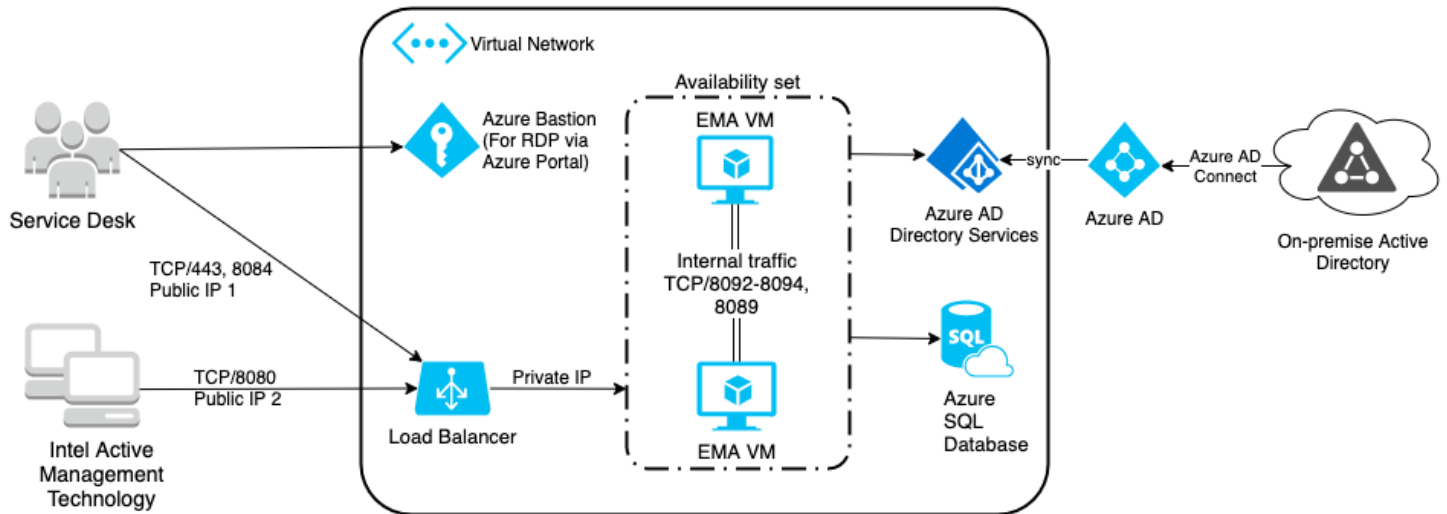
[Azure AD Connect 同步：了解和自定义同步](#)

11.1 使用 Active Directory 集成的高层级架构图

11.1.1 单服务器部署



11.1.2 分布式服务器部署



11.2 使用 Azure AD Connect 将 Active Directory 扩展到云

- ❑ 部署 Azure AD 目录服务 (AADDs) 资源，以便让虚拟机加入到 AD 域中。
 - ❑ 在此过程中，您需要为 AADDs 创建一个专用子网。
 - ❑ 从您的 Azure Active Directory 中添加一个有权限管理该托管域的用户。
 - ❑ 完成此设置可能需要一个小时或更长时间。完成此操作后，您需要更新虚拟网络的 DNS 服务器设置，以使用 AD DS 服务器 IP 地址。
- ❑ 将 AD Connect 部署到本地环境，以便将用户和密码哈希同步到 Azure Active Directory。
 - ❑ 将 AD Connect 软件下载并安装到网络上的联合域服务器。

- ❑ 使用快速设置。
- ❑ 输入 Azure AD 和 Azure AD DS 的凭据。
- ❑ 确保您的域名与您先前在 Azure AD 中添加并验证的自定义域相符。
- ❑ 配置完成后，每 30 分钟会进行一次后台同步。阅读 Microsoft 文档以获取有关其工作原理的更多信息。
- ❑ Azure AD Connect 下载位置：[从官方 Microsoft 下载中心下载 Microsoft Azure Active Directory Connect](#)。
- ❑ Azure AD Connect 的先决条件：[Azure AD Connect: 先决条件和硬件](#)。
- ❑ 一旦建立了该基础结构，即可按照以下链接所述，将虚拟机加入到域中：[将 Windows Server 虚拟机加入到 Azure AD 域服务托管域](#)。