

Intel® Endpoint Management Assistant (Intel® EMA)

Google Cloud Platform 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 GCP 控制台	1
1.2.1	服务菜单	1
1.2.2	展开服务菜单	1
1.3	资源在 GCP 中是如何组织的	2
1.4	开始之前	3
2	高层级架构图	4
2.1	单服务器部署	4
2.2	分布式服务器部署	4
3	网络部署	5
3.1	概述	5
3.2	虚拟私有云网络	5
3.2.1	导航到 VPC 网络	5
3.2.2	创建 VPC 网络	6
3.2.3	配置 VPC 网络	6
3.2.4	添加子网	7
3.2.5	确认 VPC	7
3.2.6	转到 VPC 网络详细信息	8
3.2.7	分配私有服务连接 IP 范围	8
3.2.8	输入私有服务 IP 范围详细信息	8
3.3	防火墙规则	8
3.3.1	导航至防火墙规则	9
3.3.2	为 RDP 流量创建防火墙规则	10
3.3.3	为 Web 流量创建防火墙规则 (仅限于单服务器部署)	11
3.3.4	为 Web 流量创建防火墙规则 (仅限于分布式服务器部署)	13
3.3.5	为 Swarm 流量创建防火墙规则	14
3.3.6	为服务器间的流量传输创建防火墙规则 (仅限于分布式服务器部署)	15
3.4	部署 Cloud NAT 和 Cloud Router	16
3.4.1	导航到 Cloud NAT	16
3.4.2	配置 Cloud NAT 详细信息和创建 Cloud Router	17
4	Cloud SQL 部署	18
4.1	创建 Cloud SQL Server	18
4.1.1	导航至 SQL 服务	18
4.1.2	创建 SQL Server 实例	19
4.1.3	选择数据库引擎	19
4.1.4	配置基本的实例信息	20
4.1.5	配置机器类型和存储	20
4.1.6	配置连接性	21
4.1.7	配置备份、恢复和高可用性	21
4.1.8	获取数据库 IP 地址	22
5	虚拟机部署	23
5.1	概述	23
5.2	创建 GCE 虚拟机实例	23
5.2.1	配置虚拟机基本详细信息	23
5.2.2	配置虚拟机类型	24
5.2.3	配置虚拟机启动映像	24
5.2.4	配置虚拟机访问和防火墙	24

5.2.5	配置虚拟机网络	25
5.2.6	配置虚拟机网络接口 (单服务器部署)	25
5.2.7	配置虚拟机网络接口 (分布式服务器部署)	26
5.2.8	确认创建虚拟机	26
5.2.9	设置 Windows 密码	26
5.3	创建第二个 GCE 虚拟机实例 (仅限于分布式服务器部署)	26
5.4	使用 RDP 登录虚拟机	26
6	负载均衡器部署 (仅限于分布式服务器部署)	28
6.1	创建非托管实例组	28
6.1.1	导航至实例组	28
6.1.2	创建非托管实例组	29
6.1.3	创建更多实例组	29
6.2	创建运行状况检查	29
6.2.1	为 Web 后端创建运行状况检查	29
6.2.2	为 Swarm 后端创建运行状况检查	30
6.3	导航至负载均衡	30
6.4	创建 HTTPS 负载均衡器	31
6.4.1	选择 HTTP(S) 负载均衡	31
6.4.2	为负载均衡器设置名称	31
6.4.3	后端服务配置	31
6.4.4	前端配置	33
6.4.5	检查并最终确定	34
6.5	创建 TCP 负载均衡器	34
6.5.1	选择 TCP 负载均衡	34
6.5.2	为负载均衡器设置名称	34
6.5.3	后端服务配置	35
6.5.4	前端配置	36
6.5.5	检查并最终确定	36
6.6	Intel EMA Server 的 DNS	36
7	附录 B — 有关与 Active Directory* 集成的说明	38

1 简介

本文档介绍了将基础架构部署到 Google Cloud Platform* (GCP, 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

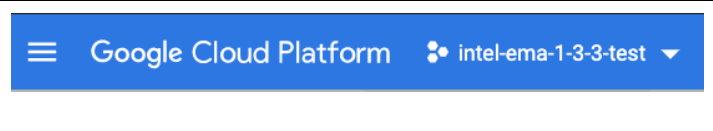
云计算采用即用即付的定价方式, 通过互联网按需交付 IT 资源。您无需购买、拥有和维护物理数据中心和服务, 便可以从云提供商处按需访问技术服务, 例如计算能力、存储和数据库。您可以只配置现在需要的资源, 并随着业务需求的变化进行调整, 以增加和减少资源。

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。

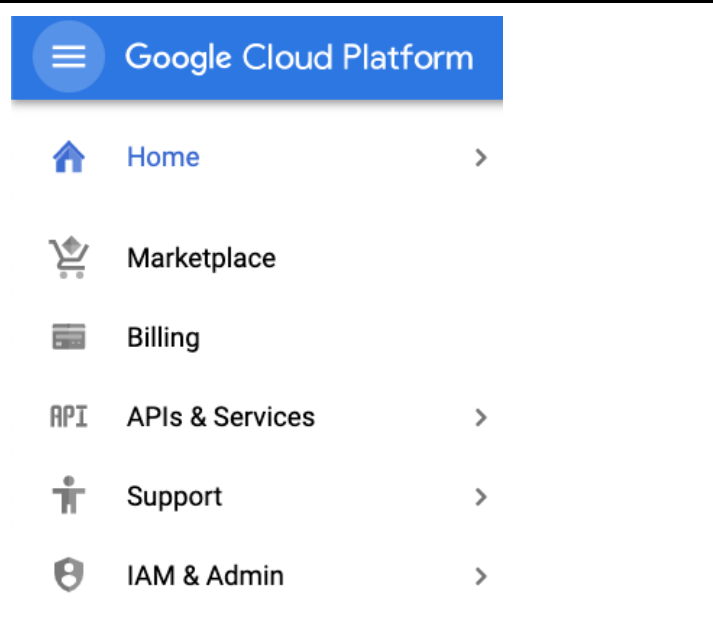
借助 Cloud SQL 等完全托管的服务, 您可以专注于自己的数据, 而云提供商则可以管理提供该服务的所有底层硬件和软件。借助在云中运行的虚拟机, 您只需要管理访客操作系统及其上安装的软件, 而云提供商则管理底层硬件并尽量为您提供最佳的可靠性和可用性。

1.2 操作 GCP 控制台

1.2.1 服务菜单

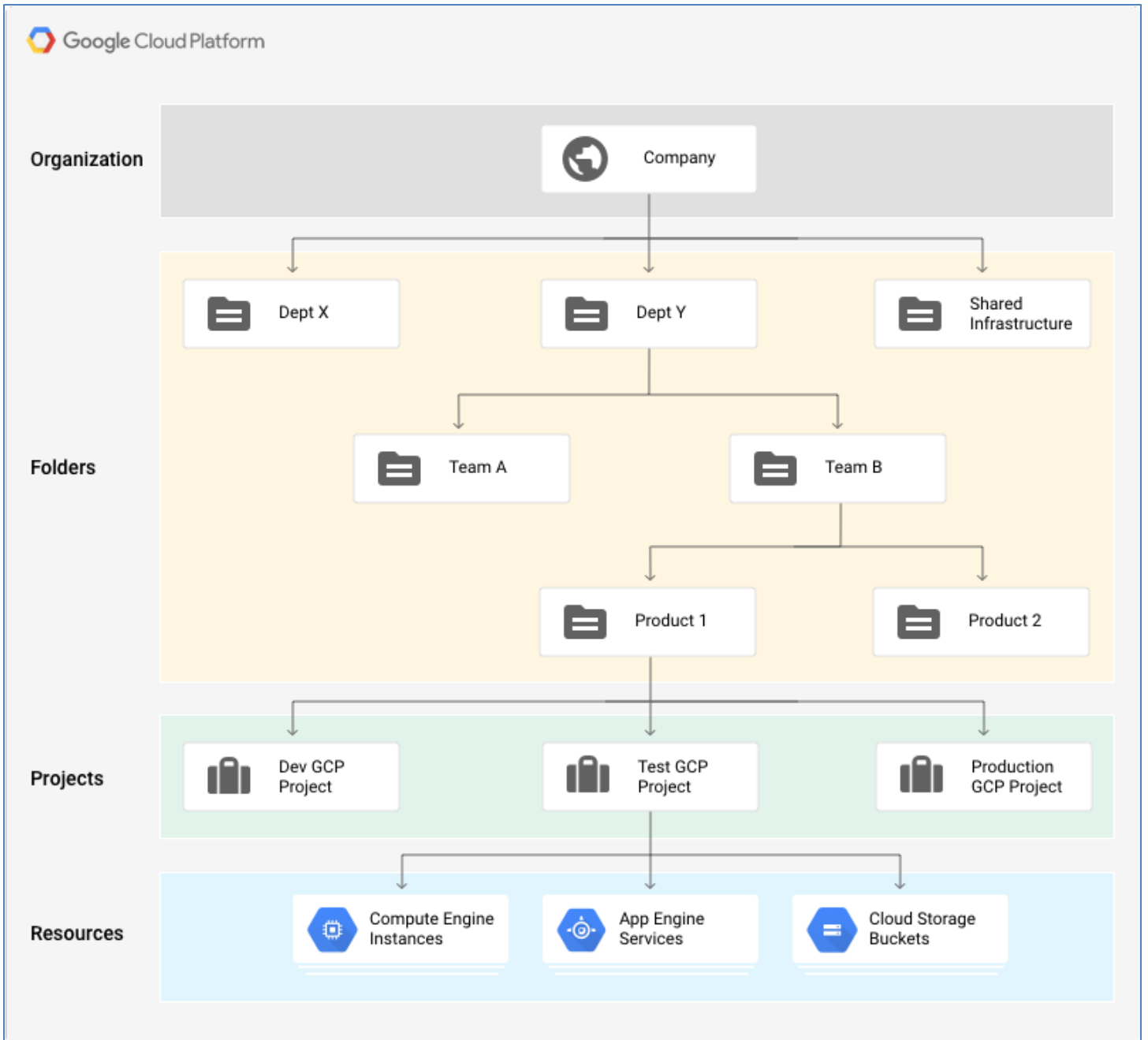
	通过 https://console.cloud.google.com/ 登录 GCP 控制台后, 您会在左上角看到服务菜单图标。您将在右侧看到一个 Project 菜单, 在创建项目后, 您可以在其中选择要部署资源的项目。
--	--

1.2.2 展开服务菜单

	当您单击服务菜单图标时, 您将看到以下服务列表, 它由“COMPUTE”、“STORAGE”和其它几部分组成。 在本指南中, 我们将提供相关说明, 以便我们部署需要的各个组件时, 指导您从此菜单中选择对应的服务。
--	---

1.3 资源在 GCP 中是如何组织的

GCP 中的所有资源都是部署到项目中的。如果您创建了个人账户，那么这就是您拥有的唯一结构。如果您创建的是“Organization”账户，则项目可以直接位于“Organization”节点下，或者选择将它们分组为“Folders”再安排在“Organization”节点下。



1.4 开始之前

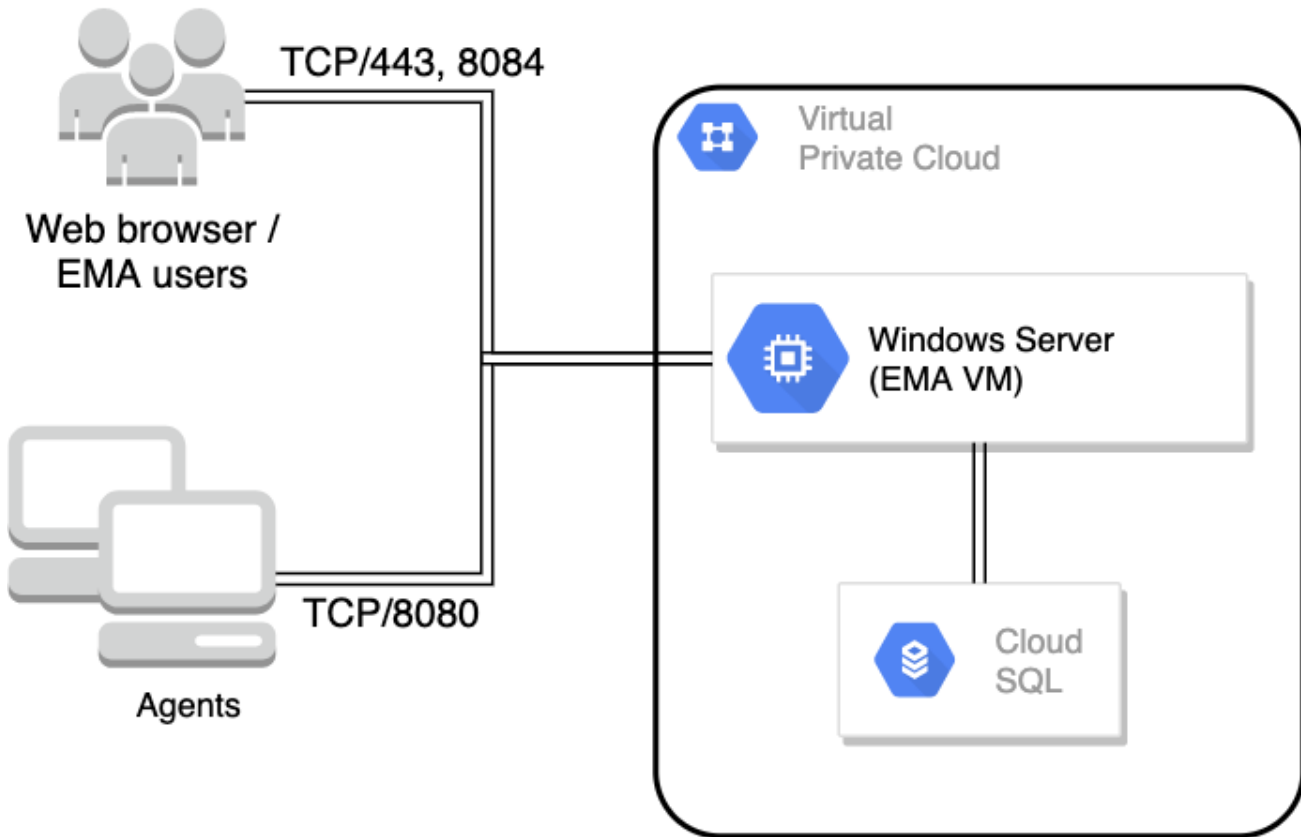
如果您的组织已有 GCP 帐户，那么您应该要求云管理员为您创建一个项目，并授予您“项目所有人”的访问权限。如果您是云管理员，则可以转到 GCP 中的 **IAM & Admin > Manage Resource** 菜单自行创建项目。

如果您的组织没有 GCP 帐户，或者您想以个人身份进行评估，则可以转到 <https://console.cloud.google.com/> 并使用 Google* 账户登录，然后您便能使用促销信用额度开始免费试用。

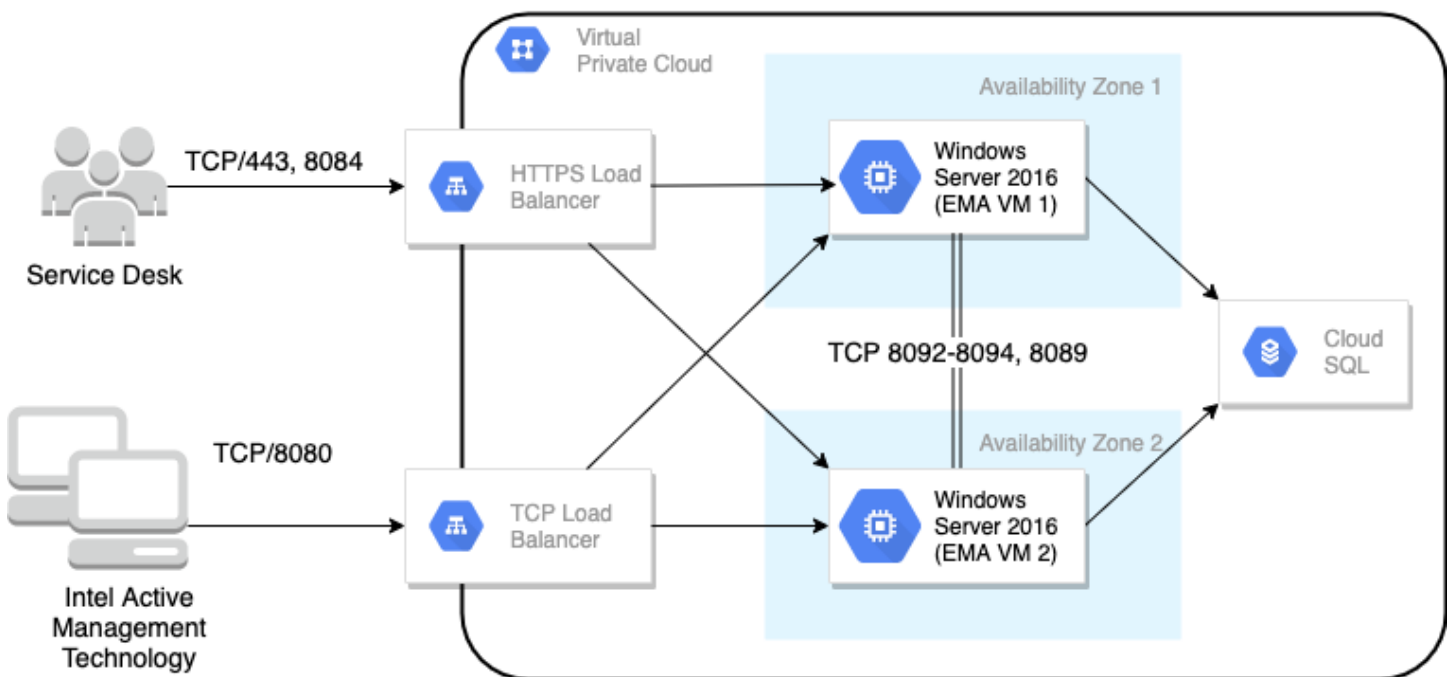
请与您的网络管理员联系，询问是否存在可供使用的首选的地址空间。如果您已经建立了连接到云提供商的 VPN，或者将来要建立此类连接，则您应避免与企业网络重叠，以免出现路由问题。您还需要找出数据是通过哪个源 IP 地址离开组织并到达云端的，以便仅允许受信任的网络通过互联网访问 Intel EMA 虚拟机。

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 网络部署

3.1 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。虚拟私有云网络（VPC 网络）是 GCP 中私有网络的主要构建基块，它与传统网络非常相似，但在 GCP 中它是虚拟化的。VPC 网络是一种全球资源，由数据中心的一系列区域虚拟子网络（子网）组成，所有区域均通过全球广域网互相连接。VPC 网络在逻辑上是相互隔离的。

创建 VPC 网络时，您需要提供自定义的私有 IP 地址空间。GCP 将在需要时从该地址空间分配资源私有 IP 地址。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确定可用的 IP 地址块，避免路由冲突。

我们还需要为私有服务访问分配 IP 块，以允许虚拟机通过私有连接而不是通过公共端点来访问 Google 服务。

创建 VPC 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，您可以将资源部署到特定的子网中。

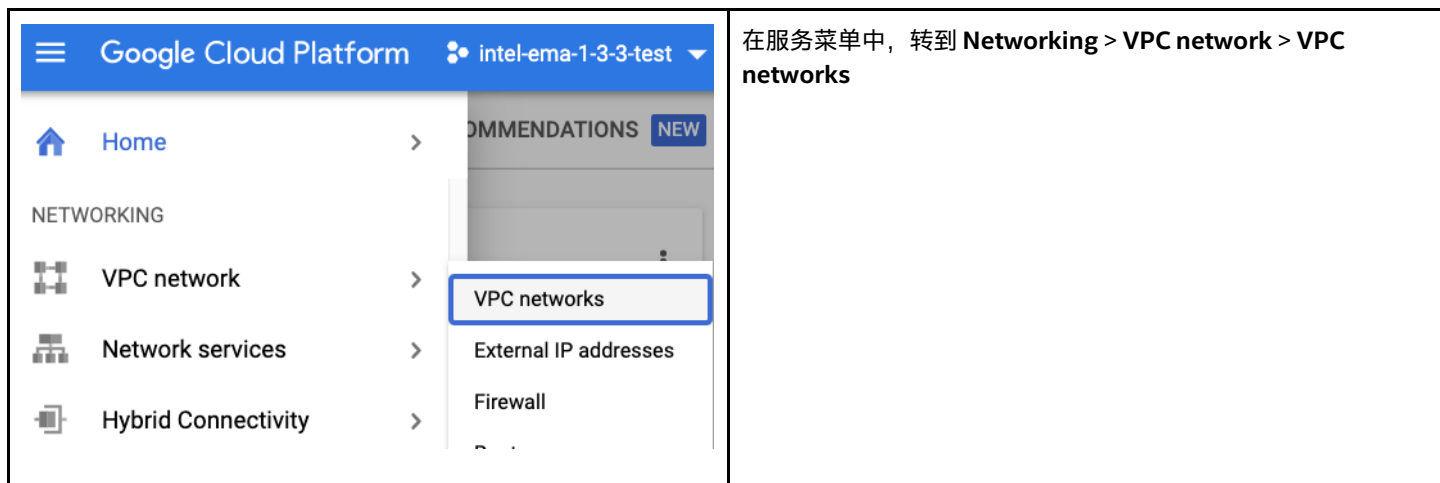
有关本节中所部署的服务的更多信息，请参见以下链接：

- VPC: <https://cloud.google.com/vpc/docs>
- 私有 Google 访问通道: <https://cloud.google.com/vpc/docs/configure-private-google-access>
- Cloud NAT: <https://cloud.google.com/nat/docs/overview>
- Cloud Router: <https://cloud.google.com/network-connectivity/docs/router>

3.2 虚拟私有云网络

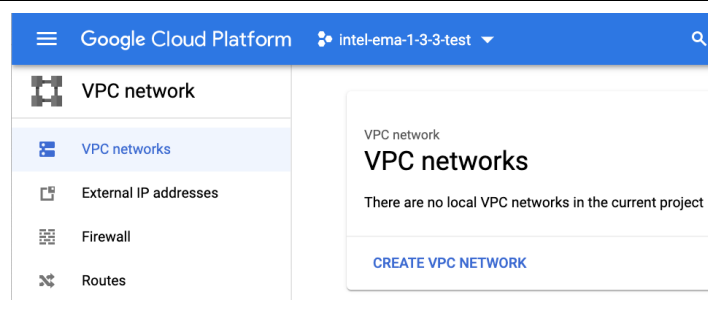
请按照以下过程创建具有单个子网的 VPC 网络

3.2.1 导航到 VPC 网络

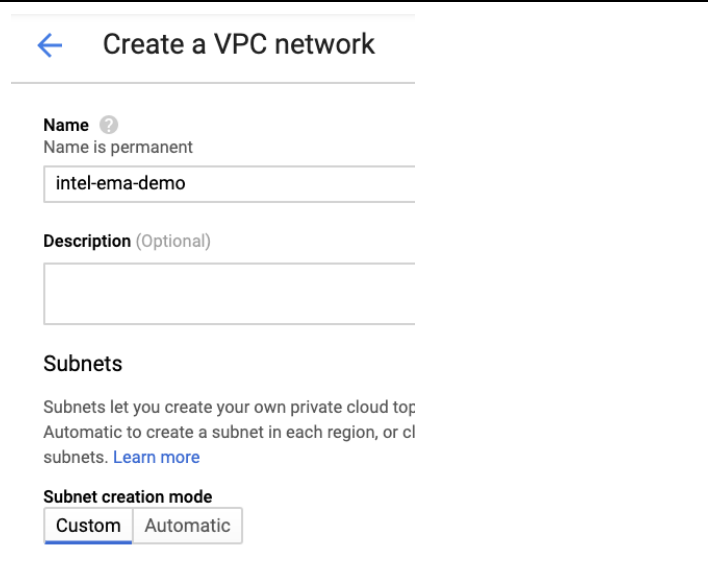


The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the user's account name 'intel-ema-1-3-3-test', and a dropdown arrow. Below the navigation bar, the 'NETWORKING' section is expanded, showing a list of services: 'VPC network', 'Network services', and 'Hybrid Connectivity'. The 'VPC network' service is selected, and a sub-menu is displayed with the following options: 'VPC networks', 'External IP addresses', and 'Firewall'. The 'VPC networks' option is highlighted with a blue border. To the right of the screenshot, the text reads: '在服务菜单中，转到 **Networking > VPC network > VPC networks**'.

3.2.2 创建 VPC 网络

	单击 CREATE VPC NETWORK
--	------------------------------

3.2.3 配置 VPC 网络

	按如下配置 VPC 网络： <ul style="list-style-type: none">• Name: 输入唯一的名称 示例: <i>intel-ema-demo</i>• Subnet creation mode: <i>Custom</i>
---	---

3.2.4 添加子网

New subnet

Name *
ema-servers ?
Lowercase letters, numbers, hyphens allowed

[Add a description](#)

Region *
us-central1 ?

IP address range *
10.250.0.0/24 ?

[CREATE SECONDARY IP RANGE](#)

Private Google access ?
 On
 Off

Flow logs
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

[CANCEL](#) [DONE](#)

按如下所示配置 **New subnet** 部分：

- **Name:** 输入唯一的子网名称
示例: *ema-servers*
- **Region:** 选择您要部署资源的区域
示例: *us-central1*
- **IP address range:** 输入要使用的 IP 地址范围
示例: *10.250.0.0/24*
- **Private Google access:** *On*

单击 **Done** 按钮。

3.2.5 确认 VPC

Dynamic routing mode ?

Regional
Cloud Routers will learn routes only in the region in which they were created

Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

DNS server policy
No server policy ?

Maximum Transmission Unit (MTU)
1460

[CREATE](#) [CANCEL](#)

您可以将其余设置保留为默认值。

单击 **Create** 按钮以确定 VPC 网络。

3.2.6 转到 VPC 网络详细信息

VPC networks + CREATE VPC NETWORK ↻ REFRESH

Name ↑	Region	Subnets	MTU ?	Mode
intel-ema-demo		0	1460	Custom

单击新建的 VPC 的名称以进入详细信息屏幕。

3.2.7 分配私有服务连接 IP 范围

← VPC network details ✎ EDIT 🗑️ DELETE VPC NETWORK

intel-ema-demo

Subnet creation mode
Custom subnets

Dynamic routing mode
Regional

DNS server policy
None

Maximum transmission unit
1460

Subnets Static internal IP addresses Firewall rules Routes VPC Network Peering **Private service connection**

Allocated IP ranges for services ⓘ Private connections to services ⓘ

Allocate IP range ↶ Release

No IP range allocated in this network. If you want to privately connect to a service, allocate a range and then create a private connection.

单击 **Private service connection**。

单击 **Allocate IP range** 按钮。

3.2.8 输入私有服务 IP 范围详细信息

Allocate an internal IP range

Name ⓘ
Name is permanent

google-private-access

Description (Optional)

IP range

Custom
Specify an IP address range

10.251.0.0/16

Each service producer requires a minimum prefix size. For Google, it is /24.

Automatic
Specify a prefix length, and then Google automatically selects an available range

CANCEL ALLOCATE

按如下所示配置 IP 分配：

- Name: 为 IP 范围输入唯一的名称。
示例: *google-private-access*
- IP range: *Custom* 输入未使用的 IP 地址范围。
Google 要求前缀大小至少为 /24, 但建议使用 /16。
示例: *10.251.0.0/16*

单击 **Allocate** 按钮。

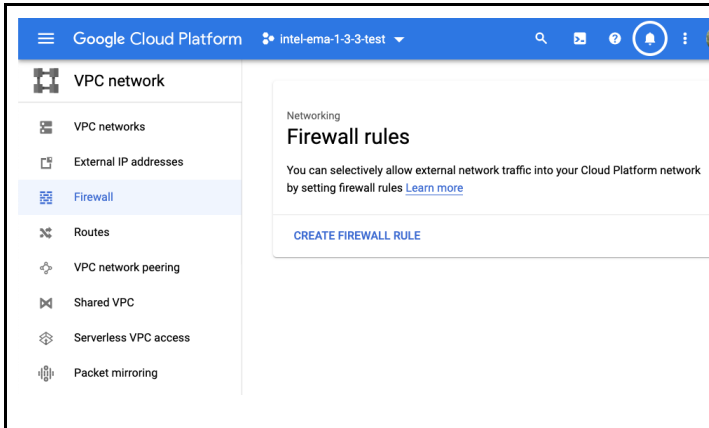
3.3 防火墙规则

每个 VPC 网络都能实施可配置的分布式虚拟防火墙。您可以通过防火墙规则控制允许哪些数据包到达哪些目的地。每个 VPC 网络都有两个隐含的防火墙规则，它们会阻止所有传入连接并允许所有传出连接。

我们指定目标或目的地的方法之一是使用标记，我们在后面会将标记应用于虚拟机，以使相关的防火墙规则对这些虚拟机生效。

有关使用 VPC 防火墙的更多信息，请访问以下链接：<https://cloud.google.com/vpc/docs/firewalls>

3.3.1 导航至防火墙规则



在服务菜单中，转到 **Networking > VPC network > Firewall**。

单击 **CREATE FIREWALL RULE**。

3.3.2 为 RDP 流量创建防火墙规则

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
allow-rdp-from-google-iap 🗑️ ?
Lowercase letters, numbers, hyphens allowed

Description
Allow Remote Desktop access through Google's Identity-Aware Proxy service

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

Network *
intel-ema-demo ▼ ?

Priority *
1000 ?
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ?
 Ingress
 Egress

Action on match ?
 Allow
 Deny

Targets
All instances in the network ▼ ?

Source filter
IP ranges ▼ ?

Source IP ranges *
35.235.240.0/20 ✕ for example, 0.0.0.0/0, 192.168.2.0/24 ?

Second source filter
None ▼ ?

Protocols and ports ?
 Allow all
 Specified protocols and ports

tcp : 3389

udp : all

Other protocols
protocols, comma separated, e.g. ah, sctp

∨ **DISABLE RULE**

CREATE **CANCEL**

我们需要允许来自 Identity-Aware Proxy (IAP) 服务使用的 Google IP 范围的入口流量，以便通过该服务登录虚拟机。

按如下方法配置防火墙规则。

- **Name:** 输入唯一的名称
示例: *allow-rdp-from-google-iap*
- **Description:** *Allow Remote Desktop access through Google's Identity-Aware Proxy service*
- **Network:** 选择您先前创建的 VPC
- **Targets:** *All instances in the network*
- **Source filter:** *IP ranges*
- **Source IP ranges:** *35.235.240.0/20*
- **Specified protocols and ports:**
tcp: 3389

单击 **Create** 按钮。

Second source filter
None

Protocols and ports ?

Allow all

Specified protocols and ports

tcp : 3389

udp : all

Other protocols

protocols, comma separated, e.g. ah, sctp

DISABLE RULE

CREATE CANCEL

3.3.3 为 Web 流量创建防火墙规则 (仅限于单服务器部署)

intel-ema-1-3-3-test Search pr

Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
allow-web-from-trusted-to-ema
Lowercase letters, numbers, hyphens allowed

Description
Allow HTTPS (TCP/443) and [websocket](#) (TCP/8084) traffic from trusted sources to the EMA server

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

On

Off

Network *
intel-ema-demo

Priority *
1000
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

创建新的防火墙规则并进行如下配置。

- **Name:** 输入唯一的名称
示例: *allow-web-from-trusted-to-ema*
- **Description:** *Allow web traffic from trusted sources to the server*
- **Network:** 选择您先前创建的 VPC
- **Targets:** *Specified target tags*
- **Target tags:** *ema-server*
- **Source filter:** *IP ranges*
- **Source IP ranges:** 输入应该具有访问权限的受信任网络
- **Specified protocols and ports:**
tcp: 443,8084

单击 **Create** 按钮。

Direction of traffic ?

- Ingress
- Egress

Action on match ?

- Allow
- Deny

Targets

Specified target tags ▼ ?

Target tags *

ema-server ✕

Source filter

IP ranges ▼ ?

Source IP ranges *

for example, 0.0.0.0/0, 192.168.2.0/24 ?

Second source filter

None ▼ ?

Protocols and ports ?

- Allow all
- Specified protocols and ports

tcp : 443,8084

udp : all

Other protocols

protocols, comma separated, e.g. ah, sctp

3.3.4 为 Web 流量创建防火墙规则 (仅限于分布式服务器部署)

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
allow-web-from-load-balancer ⓘ ?
Lowercase letters, numbers, hyphens allowed

Description
Allow web traffic from the Google load balancer

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

Network *
intel-ema-demo ⓘ ?

Priority *
1000 ⓘ ?
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ?
 Ingress
 Egress

Action on match ?
 Allow
 Deny

Targets
Specified target tags ⓘ ?

Target tags *
ema-server ✕

Source filter
IP ranges ⓘ ?

Source IP ranges *
35.191.0.0/16 ✕ 130.211.0.0/22 ✕ for example, 0.0.0.0/0, 192.168.2.0 ⓘ ?

Second source filter
None ⓘ ?

Protocols and ports ?
 Allow all
 Specified protocols and ports

tcp : 443,8084
 udp : all
 Other protocols
protocols, comma separated, e.g. ah, sctp

◇ **DISABLE RULE**

CREATE **CANCEL**

创建新的防火墙规则并进行如下配置。

- **Name:** 输入唯一的名称
示例: *allow-web-from-load-balancer*
- **Description:** *Allow web traffic from the Google load balancer*
- **Network:** 选择您先前创建的 VPC
- **Targets:** *Specified target tags*
- **Target tags:** *ema-server*
- **Source filter:** IP ranges
- **Source IP ranges:**
 - *35.191.0.0/16*
 - *130.211.0.0/22*
- **Specified protocols and ports:**
 - *tcp: 443,8084*

单击 **Create** 按钮。

3.3.5 为 Swarm 流量创建防火墙规则

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
allow-swarm-from-any-to-ema

Lowercase letters, numbers, hyphens allowed

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

On

Off

Network *
intel-ema-demo

Priority *
1000

Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ?

Ingress

Egress

Action on match ?

Allow

Deny

Targets
Specified target tags

Target tags *
ema-server

Source filter
IP ranges

Source IP ranges *
0.0.0.0/0 for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter
None

Protocols and ports ?

Allow all

Specified protocols and ports

tcp : 8080

udp : all

Other protocols

protocols, comma separated, e.g. ah, sctp

DISABLE RULE

CREATE

CANCEL

创建新的防火墙规则并进行如下配置。

- **Name:** 输入唯一的名称
示例: *allow-swarm-from-any-to-ema*
- **Description:** *Allow EMA agent traffic from anywhere to the server*
- **Network:** 选择您先前创建的 VPC
- **Targets:** *Specified target tags*
- **Target tags:** *ema-server*
- **Source filter:** *IP ranges*
- **Source IP ranges:** *0.0.0.0/0*
- **Specified protocols and ports:**
tcp: 8080

单击 **Create** 按钮。

3.3.6 为服务器间的流量传输创建防火墙规则（仅限于分布式服务器部署）

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
allow-ema-internal ⓘ ?
Lowercase letters, numbers, hyphens allowed

Description
Allow internal communication between EMA servers

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)
 On
 Off

Network *
intel-ema-demo ?

Priority *
1000 ?
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic ?
 Ingress
 Egress

Action on match ?
 Allow
 Deny

Targets
Specified target tags ?

Target tags *
ema-server ✕

Source filter
Source tags ?

Source tags *
ema-server ?

Second source filter
None ?

Protocols and ports ?
 Allow all
 Specified protocols and ports

tcp : 8092-8094,8089

udp : all

Other protocols
protocols, comma separated, e.g. ah, sctp

◇ DISABLE RULE

CREATE CANCEL

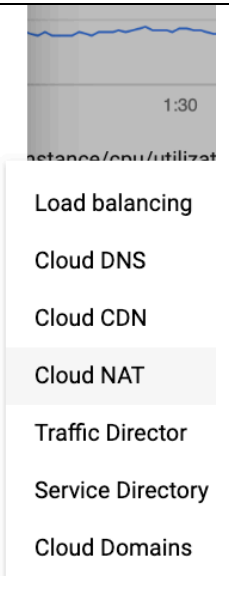
创建新的防火墙规则并进行如下配置。

- **Name:** 输入唯一的名称
示例: *allow-ema-internal*
- **Description:** *Allow internal communication between EMA servers*
- **Network:** 选择您先前创建的 VPC
- **Targets:** *Specified target tags*
- **Target tags:** *ema-server*
- **Source filter:** *Source tags*
- **Source tags:** *ema-server*
- **Specified protocols and ports:**
tcp: 8092-8094,8089

单击 **Create** 按钮。

3.4 部署 Cloud NAT 和 Cloud Router

3.4.1 导航到 Cloud NAT

<p>NETWORKING</p> <ul style="list-style-type: none">VPC network >Network services >Hybrid Connectivity >Network Service TiersNetwork Security >Network Intelligence > 	<p>从服务菜单，转到 Networking > Network services > Cloud NAT</p> <p>单击“Get started”</p>
---	--

3.4.2 配置 Cloud NAT 详细信息和创建 Cloud Router

← Create a NAT gateway

Cloud NAT lets your VM instances and container pods communicate with the internet using a shared, public IP address.

Cloud NAT uses NAT gateway to manage those connections. A NAT gateway is region and VPC network specific. If you have VM instances in multiple regions, you'll need to create a NAT gateway for each region. [Learn more](#)

Gateway name ⓘ
Name is permanent

Select Cloud Router ⓘ

VPC network ⓘ

Region ⓘ

Subnet(s): 1

Cloud Router ⓘ

Create new router

No Suggestions

NAT IP addresses ⓘ

Destination (external)
Internet

⌵ **Advanced configurations**

Create a router

Google Cloud Router dynamically exchanges routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP)

Name ⓘ
Name is permanent

Description (Optional)

Network ⓘ

Region ⓘ
Region is permanent

按如下所示配置 NAT 网关：

- **Gateway name:** 输入唯一的名称
示例: *ema-usc1-nat-gw*
- **VPC network:** 选择之前创建的 VPC
- **Region:** 选择要部署虚拟机的区域。
- **Cloud Router:** 从下拉菜单中选择 *Create new router*.
 - 为 Cloud Router 输入唯一的名称
示例: *ema-usc1-router*
 - 单击 **Create** 按钮以确定 Cloud Router。

单击 **Create** 按钮以确定 Cloud NAT 网关。

4 Cloud SQL 部署

Google Cloud SQL for SQL Server 是一个完全托管的平台即服务 (PaaS) 数据库引擎，其功能包括：

- 自定义计算机类型，具有多达 624 GB RAM 和 96 个 CPU。
- 高达 30 TB 的可用存储空间，并能够根据需要自动增加存储大小。
- 在 [Google Cloud Console](#) 中创建和管理实例。
- 美国、欧盟、亚洲或澳大利亚可用实例。
- 客户数据在 Google 的内部网络以及数据库表、临时文件和备份中进行了加密。
- 支持使用 Cloud SQL 代理或 SSL/TLS 协议进行安全的外部连接。
- 使用 BAK 和 SQL 文件导入数据库。
- 使用 BAK 文件导出数据库。
- 自动化和按需备份。
- 集成 Stackdriver 日志记录和监控。
- 已启用 SQL Server 代理以加快复制和其他工作。

注意：Cloud SQL 不支持 AD 身份验证。

有关 Cloud SQL 的更多信息，包括不支持的功能的完整列表，请访问以下链接：<https://cloud.google.com/sql/docs/sqlserver>

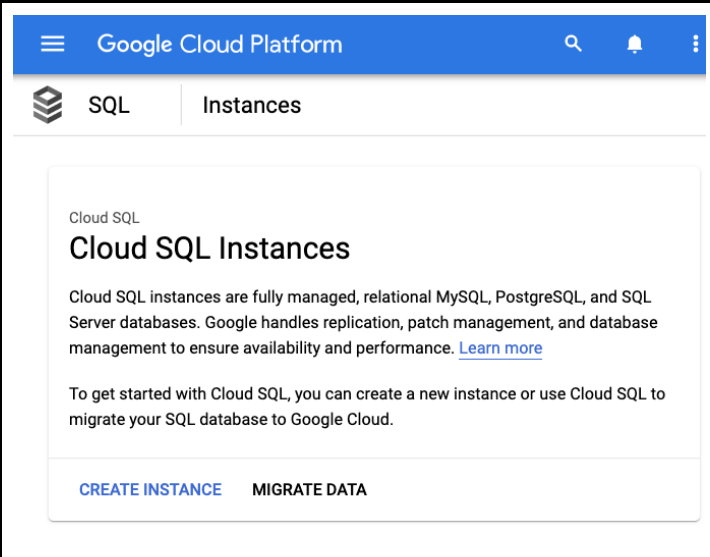
4.1 创建 Cloud SQL Server

请按照以下过程创建 SQL Server 数据库，并授予对您的虚拟机的访问权限。

4.1.1 导航至 SQL 服务

	<p>在服务菜单中，转到 Storage > SQL</p>
--	--

4.1.2 创建 SQL Server 实例



The screenshot shows the Google Cloud Platform interface for SQL instances. The top navigation bar includes the Google Cloud Platform logo, a search icon, and a notification bell. Below the navigation bar, the 'SQL' and 'Instances' tabs are visible. The main content area features a 'Cloud SQL Instances' section with a brief description of Cloud SQL instances and a 'CREATE INSTANCE' button.

Google Cloud Platform

SQL Instances

Cloud SQL

Cloud SQL Instances

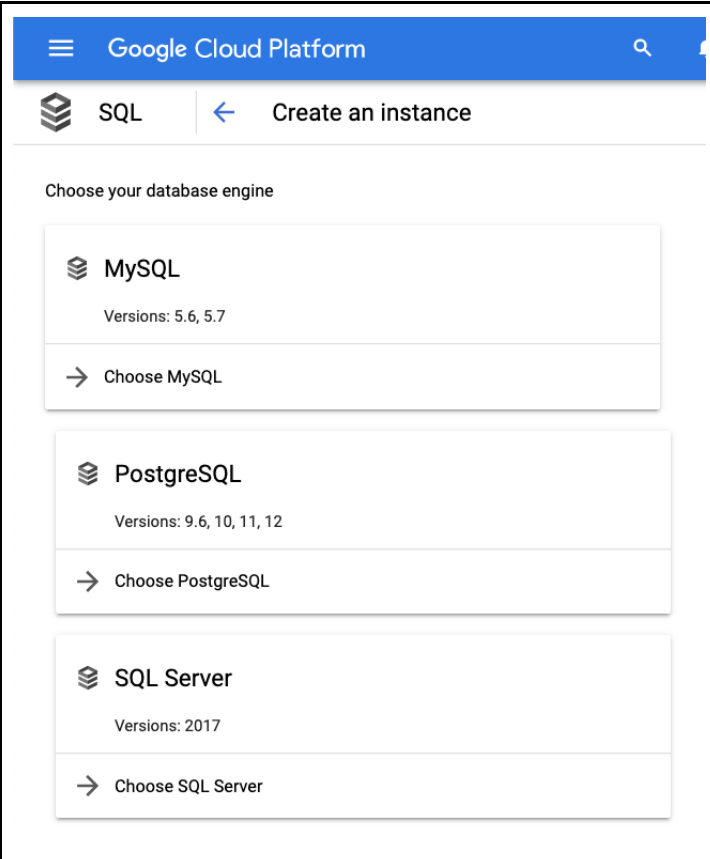
Cloud SQL instances are fully managed, relational MySQL, PostgreSQL, and SQL Server databases. Google handles replication, patch management, and database management to ensure availability and performance. [Learn more](#)

To get started with Cloud SQL, you can create a new instance or use Cloud SQL to migrate your SQL database to Google Cloud.

[CREATE INSTANCE](#) [MIGRATE DATA](#)

单击 **CREATE INSTANCE**

4.1.3 选择数据库引擎



The screenshot shows the 'Create an instance' page in Google Cloud Platform. The top navigation bar includes the Google Cloud Platform logo, a search icon, and a notification bell. Below the navigation bar, the 'SQL' and 'Create an instance' tabs are visible. The main content area features a 'Choose your database engine' section with three options: MySQL, PostgreSQL, and SQL Server. Each option includes a 'Choose' button.

Google Cloud Platform

SQL Create an instance

Choose your database engine

MySQL
Versions: 5.6, 5.7
→ Choose MySQL

PostgreSQL
Versions: 9.6, 10, 11, 12
→ Choose PostgreSQL

SQL Server
Versions: 2017
→ Choose SQL Server

选择 *SQL Server* 作为数据库引擎。

4.1.4 配置基本的实例信息

Google Cloud Platform intel-ema-1-3-3-test

SQL Create a SQL Server instance

Instance info

Instance ID
Choice is permanent. Use lowercase letters, numbers, and hyphens. Start with a letter.
ema-db

Password
Your default service admin username is 'sqlserver'.
..... Generate

Location ?
For better performance, keep your data close to the services that need it.

Region Choice is permanent
us-central1 (Iowa)

Zone Can be changed at any time
Any

按如下所示配置基本详细信息。

- **Instance ID:** 输入唯一的名称
示例: *ema-db*
- **Password:** 创建一个密码。
请注意, 默认服务管理员用户名是 'sqlserver'。
- **Region:** 使用与子网相同的区域。
- **Zone:** *Any*

4.1.5 配置机器类型和存储

1 Machine type and storage

Database version and edition
Each edition has limits for cores, memory, and storage. If you customize beyond these limits, you'll be pointed to an edition that better suits your needs. [Learn more](#)
SQL Server 2017 Standard (most common)

Machine type ?
Choose a preset or customize your own. For better performance, choose a machine type with enough memory to hold your largest table. [Learn more](#)
Standard (most common) Satisfies most use cases

1vCPU, 4 GB 2vCPU, 8 GB 4vCPU, 16 GB Custom

Storage capacity
Higher capacity improves performance, up to the limits set by the machine type. Capacity can't be decreased later.
20 GB 100 GB 200 GB 1 TB Custom

Enable automatic storage increases
If enabled, whenever you're nearing capacity, storage will be incrementally (and permanently) increased. [Learn more](#)

Storage type
SSD

在 **Configuration options** 下, 按如下所示配置 **Machine type and storage**。

- **Database version and edition:** *SQL Server 2017 Standard*
- **Machine type:** *Standard*

除非您有特殊需要, 否则可以将存储设置保留为默认值。

有关系统要求的建议, 请参阅《Intel® Endpoint Management Assistant Server 安装指南》。



4.1.6 配置连接性

<p>2 Connectivity ^</p> <p>Choose how you would like to connect to your database instance. For extra security, consider using the Cloud SQL proxy to connect to your instances after creation.</p> <p><input checked="" type="checkbox"/> Private IP</p> <p>Private IP connectivity requires additional APIs and permissions. You may need to contact your organization's administrator for help enabling or using this feature. Currently, Private IP cannot be disabled once it has been enabled.</p> <p>Associated networking Select a network to create a private connection</p> <p>intel-ema-demo ▾</p> <p>Managed services network connection ? Create a service connection by providing an allocated IP range.</p> <p><input checked="" type="radio"/> Select the IP range</p> <p>google-private-access ▾</p> <p><input type="radio"/> Use an automatically allocated IP range</p> <p>Connect Cancel</p> <p><input type="checkbox"/> Public IP</p> <p>Close</p>	<p>在 Configuration options 下，按如下所示配置 Connectivity。</p> <ul style="list-style-type: none">• Private IP: 勾选<ul style="list-style-type: none">○ 确认弹出窗口以启用 Google 的 Service Networking API (如果有显示)。○ Associated networking: 选择您先前创建的 VPC○ 选择您先前附加到 VPC 以用于 Google 私有访问的 IP 范围。○ 单击 Connect 按钮。当 "Managed service network connection" 子部分消失时，您便可以继续操作。• Public IP: 不勾选 <p>单击 Close 按钮以折叠 Connectivity 部分。</p>
---	--

4.1.7 配置备份、恢复和高可用性

<p>3 Backups, recovery, and high availability ^</p> <p>Backups Automated backups and point in time recovery help protect your data from loss at a minimal cost.</p> <p><input checked="" type="checkbox"/> Automate backups</p> <p>12:00 AM – 4:00 AM ▾</p> <p>Choose the best window of time for your data to be automatically backed up. May continue outside window until complete. Hours shown in your local time zone (UTC-6).</p> <p>∨ Location options</p> <p>Availability Choice affects cost. You can change this option at any time by editing your instance.</p> <p><input type="radio"/> Single zone In case of outage, no failover. Not recommended for production instances.</p> <p><input checked="" type="radio"/> High availability (regional) Automatic failover to another zone within your selected region. Recommended for production instances. Increases cost. Learn more</p> <p>Close</p>	<p>在 Configuration options 下，按如下所示配置 Backups, recovery, and high availability。</p> <p>备份设置由您自行决定。</p> <p>建议为生产部署启用 High availability 选项。</p> <p>单击 Create 按钮以完成数据库创建。</p>
---	---

4.1.8 获取数据库 IP 地址

<p> Connect to this instance</p> <p>Private IP address</p> <p>10.251.0.5 </p>	<p>创建数据库后，“Overview”页面将在“Connect to this instance”部分中显示其私有 IP 地址。</p>
--	---

5 虚拟机部署

5.1 概述

Google Compute Engine (GCE) 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。

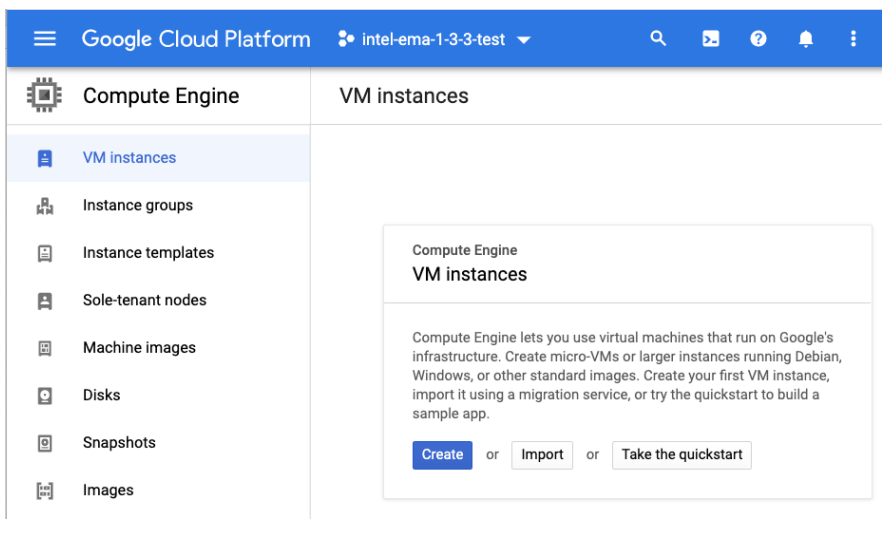
在项目中创建实例时，请指定该实例的区、操作系统和机器类型。删除实例后，该实例将从项目中删除。机器类型决定了创建时分配给 GCE 虚拟机 (VM) 的 CPU 和内存（“存储”是一个单独的选项），但是您也可以更改已停止实例的机器类型，或在以后增加存储量。

每个计算引擎实例都属于一个 VPC 网络。同一网络中的实例通过局域网协议相互通信。实例使用互联网与自己网络之外的任何虚拟或物理计算机进行通信。

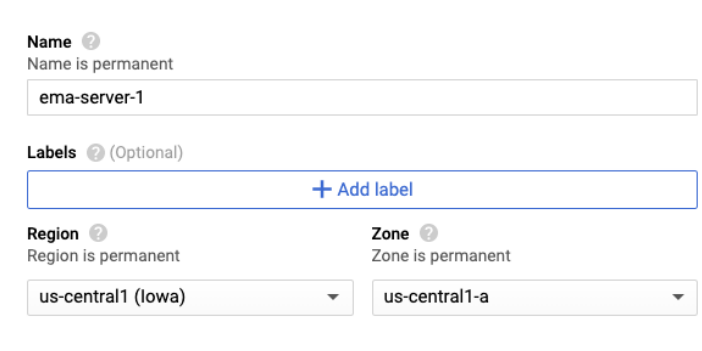
有关 Google Compute Engine 的更多信息，请访问以下链接：

<https://cloud.google.com/compute><https://cloud.google.com/compute/docs/concepts>

5.2 创建 GCE 虚拟机实例

	<p>在服务菜单中，转到 Compute > Compute Engine > VM instances。</p> <p>单击 Create 按钮。</p>
--	--

5.2.1 配置虚拟机基本详细信息

	<p>按如下方法配置虚拟机基本详细信息。</p> <ul style="list-style-type: none">• Name: 输入唯一的名称 示例: <i>ema-server-1</i>• Region: 选择我们之前使用的相同区域。• Zone: 选择一个与其他 EMA 虚拟机不同的区
---	--

5.2.2 配置虚拟机类型

Machine configuration

Machine family

General-purpose | Memory-optimized | Compute-optimized

Machine types for common workloads, optimized for cost and flexibility


Series

E2

CPU platform selection based on availability

Machine type

e2-standard-2 (2 vCPU, 8 GB memory)

	vCPU	Memory
	2	8 GB

选择适当的机器类型。有关系统要求，请参阅《Intel® Endpoint Management Assistant Server 安装指南》。

您可以稍后在虚拟机关机时进行更改。

5.2.3 配置虚拟机启动映像

Boot disk

New 50 GB standard persistent disk

Image

Windows Server 2019 Datacenter

Change

将 **Boot disk** 设置为 Intel EMA 支持的最新 Windows* Server Datacenter 版本。

有关支持的操作系统，请参阅《Intel® Endpoint Management Assistant Server 安装指南》。

5.2.4 配置虚拟机访问和防火墙

Identity and API access

Service account

Compute Engine default service account

Access scopes

Allow default access

Allow full access to all Cloud APIs

Set access for each API

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

Allow HTTP traffic

Allow HTTPS traffic

Management, security, disks, networking, sole tenancy

You will be billed for this instance. [Compute Engine pricing](#)

Create Cancel

在 **Identity and API access** 部分，您可以保留默认值，以授予虚拟机将日志写入 Google Cloud Logging 的权限，也可执行其他操作。

在 Firewall 部分，应清除两个复选框，因为我们将通过网络标记允许网络访问，相关选项将在下一步中进行配置。

单击 **Management, security, disks, networking** 链接以展开此部分，然后继续下一步。

5.2.5 配置虚拟机网络

Management Security Disks **Networking** Sole Tenancy

Network tags ? (Optional)

ema-server allow-rdp

Hostname ?
Set a custom hostname for this instance or leave it default. Choice is permanent

ema-server-1.us-central1-a.c.intel-ema-1-3-3-test.internal

Network interfaces ?
Network interface is permanent

intel-ema-demo ema-server (10.250.0.0/24)

选择 **Networking** 选项卡。

设置以下 **Network tags**:

- ema-server

单击网络界面上的铅笔图标，然后继续下一步。

5.2.6 配置虚拟机网络接口 (单服务器部署)

Network interface

Network ?
intel-ema-demo

Subnetwork ?
ema-servers (10.250.0.0/24)

Primary internal IP ?
ema-server-1-private-ip (10.250.0.3)

Show alias IP ranges

External IP ?
ema-server-1-public-ip (34.122.76.61)

Network Service Tier ?
Premium

IP forwarding ?
Off

Public DNS PTR Record ?
 Enable
PTR domain name

Done Cancel

将 **Primary internal IP** 设置为 *Reserve static internal IP address*

为 IP 保留输入唯一的名称

示例: *ema-server-1-private-ip*

单击 Reserve 按钮。

将 **External IP** 设置为 Create IP address。

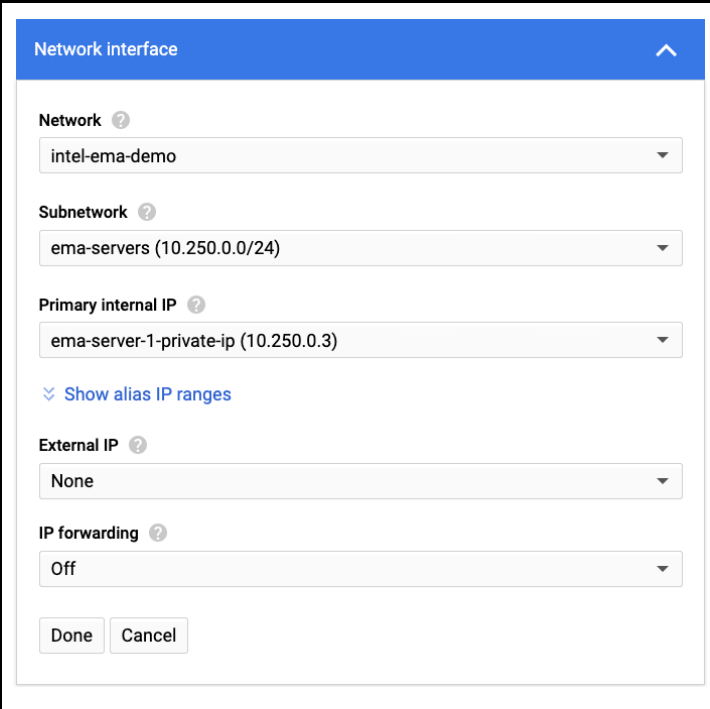
为 IP 保留输入唯一的名称

示例: *ema-server-1-public-ip*

单击 Reserve 按钮。

单击 **Done** 按钮。

5.2.7 配置虚拟机网络接口 (分布式服务器部署)



将 **Primary internal IP** 设置为 *Reserve static internal IP address*

为 IP 保留输入唯一的名称
示例: *ema-server-1-private-ip*

单击 Reserve 按钮。

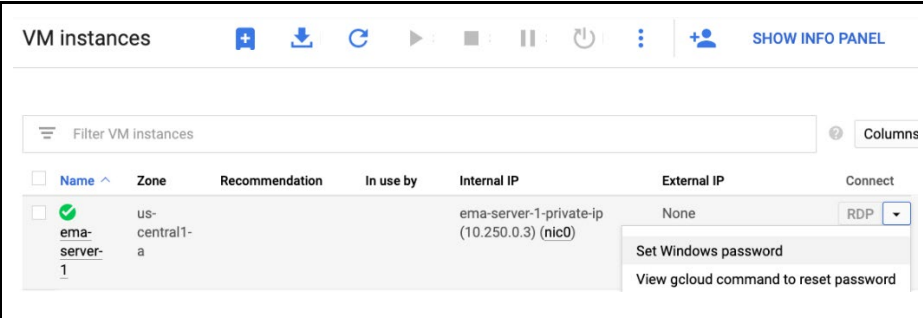
将 **External IP** 设为 None。

单击 **Done** 按钮。

5.2.8 确认创建虚拟机

单击屏幕底部的 **Create** 按钮以完成虚拟机的创建。

5.2.9 设置 Windows 密码



创建虚拟机之后，您可以从虚拟机实例列表中单击 Connect 箭头按钮，以为其设置 Windows 密码。

5.3 创建第二个 GCE 虚拟机实例 (仅限于分布式服务器部署)

对于分布式服务器部署，请重复前面的步骤以创建另一个虚拟机。建议您部署到其他区，以减轻某个区停机所产生的影响。

5.4 使用 RDP 登录虚拟机

对于没有公共 IP 地址的虚拟机，本节介绍了一种使用 Google 的 Identity-Aware Proxy (IAP) 将 RDP 通过隧道连接到虚拟机的方法。

这部分要求您已安装 Cloud SDK，以便访问 gcloud 命令行实用程序。有关安装说明，请参阅：

<https://cloud.google.com/sdk/docs/install>

一旦安装并配置了 gcloud 实用程序，便可以启动连接虚拟机的 IAP 隧道，从而将您选择的本地端口转发到虚拟机的 RDP 端口。
命令示例：

```
gcloud compute start-iap-tunnel ema-server-1 3389 --local-host-  
port=localhost:33389 --zone=us-central1-a
```

您将需要调整命令，使其具有正确的服务器名称和区域才能正常工作。

有关使用 IAP 进行 TCP 转发的更多信息，请访问以下链接：<https://cloud.google.com/iap/docs/using-tcp-forwarding>

6 负载均衡器部署 (仅限于分布式服务器部署)

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，负载均衡可降低应用程序负担过重、运行缓慢或无法工作的风险。

我们将使用 HTTPS 负载均衡器处理 Web 流量，并使用 TCP 代理负载均衡器处理 Swarm 流量。在 HTTPS LB 创建期间，您需要有 SSL/TLS 证书。

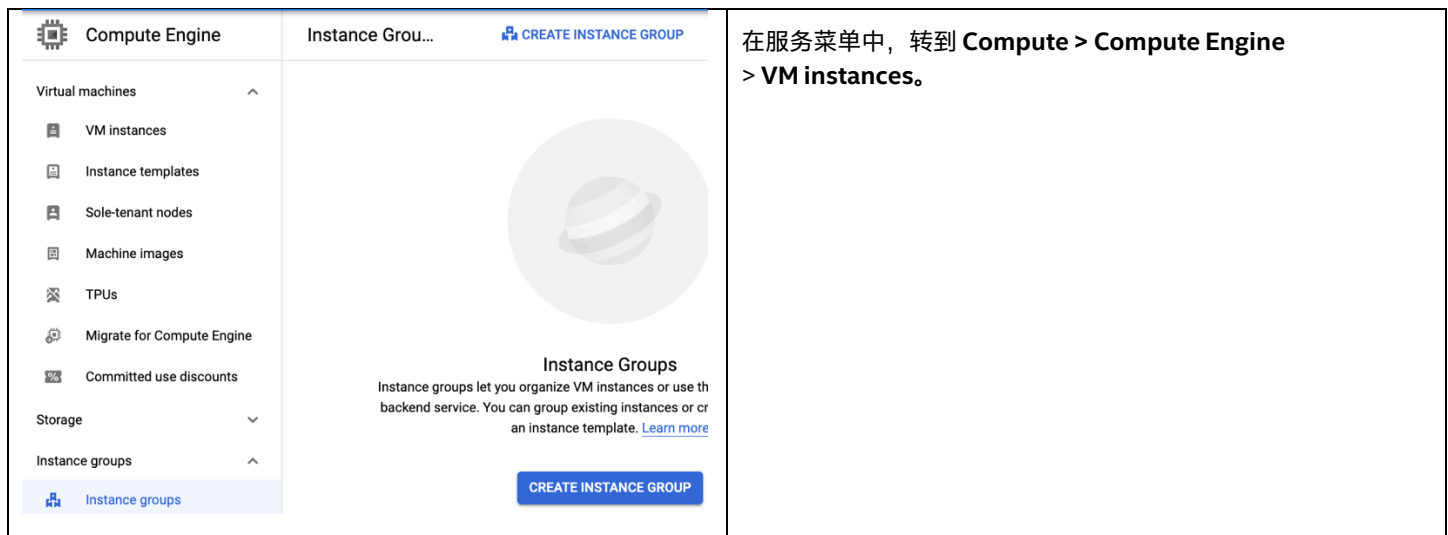
负载均衡器的后端是一个实例组。我们的虚拟机需要手动配置，不支持自动扩展，因此我们将使用非托管实例组。这些是分区资源，因此我们需要为部署了 Intel EMA 虚拟机的各个区创建单独的实例组。

另一个重要的注意事项是，我们使用的 TCP 负载均衡器仅接受前端某些已知端口上的流量，因此在服务器上安装 Intel EMA 之后，需要您更新某些设置。《Intel EMA Server 安装指南》中提供了有关如何执行此操作的说明。

有关 Google 负载均衡的更多信息，请访问以下链接：<https://cloud.google.com/load-balancing/docs>

6.1 创建非托管实例组

6.1.1 导航至实例组



Compute Engine Instance Grou... CREATE INSTANCE GROUP

Virtual machines ^

- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Migrate for Compute Engine
- Committed use discounts

Storage v

Instance groups ^

Instance groups

Instance Groups

Instance groups let you organize VM instances or use the backend service. You can group existing instances or create an instance template. [Learn more](#)

CREATE INSTANCE GROUP

在服务菜单中，转到 **Compute > Compute Engine > VM instances**。

6.1.2 创建非托管实例组

To create an instance group, select one of the options:

- New managed instance group (stateless)**
Use for stateless serving and batch workloads.
Supports:
 - autoscaling
 - autohealing, updating, regional deployments
 - load balancing
- New managed instance group (stateful)**
Use for workloads that require persistent data or configuration such as databases or legacy monolithic applications.
Supports:
 - preserving the state of disks and metadata
 - autohealing, updating, regional deployments
 - load balancing
- New unmanaged instance group**
Use for load balancing across a group of VMs that you manage yourself.
Supports:
 - load balancing

Organize VM instances in a group to manage them together. [Instance groups](#)

Name Name is permanent
ema-usc1a

Description (Optional)
Intel EMA instances in the us-central1-a zone

Location
Region Region is permanent: us-central1 (Iowa) | **Zone** Zone is permanent: us-central1-a

Port name mapping (Optional)
A load balancer sends traffic to an instance group through a named port. Create a named port to map the incoming traffic to a specific port number, then go to "HTTP load balancing" to create a load balancer using this instance group.

Port name	Port numbers
web	443
redirection	8084
swarm	8080

[+ Add item](#)

Network
intel-ema-demo

Subnetwork
ema-servers (10.250.0.0/24)

VM instances
ema-server-1

No available instances

You will be billed for VM instances in this group. [Compute Engine pricing](#)

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

单击 **Create Instance Group** 按钮。

按如下所示配置实例组：

- Name:** 为实例组输入唯一的名称
示例: *ema-usc1a*
- Description (optional):** *Intel EMA instances in the us-central1-a zone*
- Location:** 选择您的首选区域和分区
示例: *us-central1-a*
- Port name mapping:** 添加以下项目
 - web: 443*
 - redirection: 8084*
 - swarm: 8080*
- Network:** 选择您的 VPC 网络
- Subnetwork:** 选择您的子网
- VM instances:** 选择此区内的所有虚拟机。
至少应选择一个。

单击 **Create** 按钮

6.1.3 创建更多实例组

请按照前面的步骤为已部署 Intel EMA 虚拟机的各个其他区创建一个非托管实例组。

6.2 创建运行状况检查

我们需要创建运行状况检查，以便负载均衡器能够确定哪些实例运行状况良好并且可以接收流量。

6.2.1 为 Web 后端创建运行状况检查

← Create a health check

Health checking mechanisms determine whether VM instances respond properly to traffic. You cannot create a legacy health check using this page. For more information, refer to the [Health Checks Concepts](#) documentation.

Name
ema-web

Description

Scope
 Global
 Regional

Protocol
HTTPS

Port
443

从 Compute Engine 侧边栏中，选择 **Health checks**。

单击 **Create Health Check**。

按如下所示配置运行状况检查：

- Name:** 为运行状况检查输入唯一的名称
示例: *ema-web*
- Scope:** Global
- Protocol:** HTTPS
- Port:** 443

您可以接受其他默认值。

单击 **Create** 以确认创建运行状况检查。

6.2.2 为 Swarm 后端创建运行状况检查

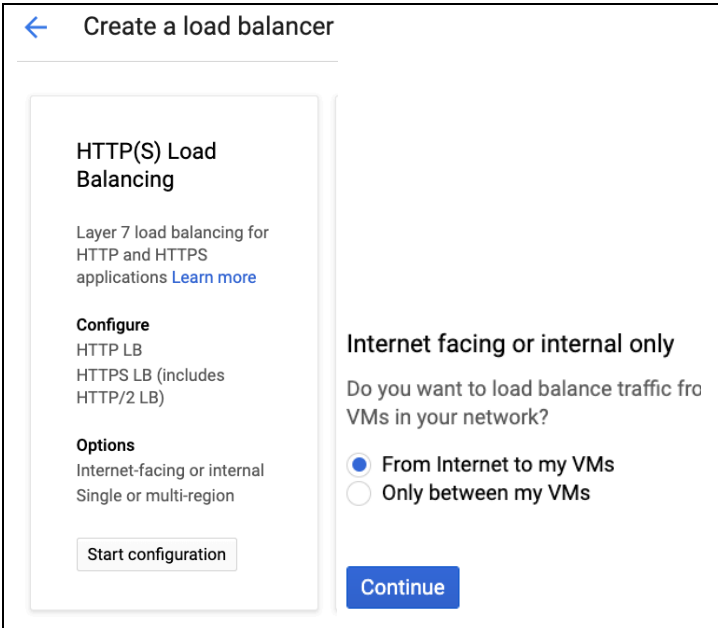
<p>← Create a health check</p> <p>Health checking mechanisms determine whether VM instances respond properly to traffic. You cannot create a legacy health check using this page. For more information, refer to the Health Checks Concepts documentation.</p> <p>Name ema-swarm</p> <p>Description</p> <p>Scope <input checked="" type="radio"/> Global <input type="radio"/> Regional</p> <p>Protocol TCP</p> <p>Port 8080</p>	<p>从 Compute Engine 侧边栏中，选择 Health checks。</p> <p>单击 Create Health Check。</p> <p>按如下所示配置运行状况检查：</p> <ul style="list-style-type: none">• Name: 为运行状况检查输入唯一的名称 示例: <i>ema-swarm</i>• Scope: Global• Protocol: TCP• Port: 8080 <p>您可以接受其他默认值。</p> <p>单击 Create 以确认创建运行状况检查。</p>
--	---

6.3 导航至负载均衡

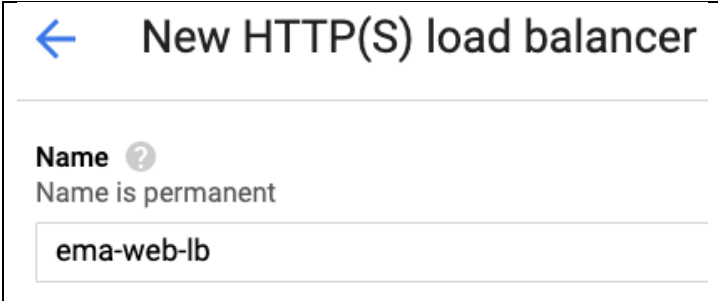
<p>Network services</p> <ul style="list-style-type: none">Load balancingCloud DNSCloud CDNCloud NATTraffic DirectorService DirectoryCloud Domains	<p>Load balancing</p> <p>Load balancers Backends Frontends</p> <p>Network Services Load balancing</p> <p>Load balancers distribute inc VM instances to help your ap</p> <p>Create load balancer</p>	<p>从服务菜单，转到 Networking > Network services > Load Balancing</p>
---	--	---

6.4 创建 HTTPS 负载均衡器

6.4.1 选择 HTTP(S) 负载均衡

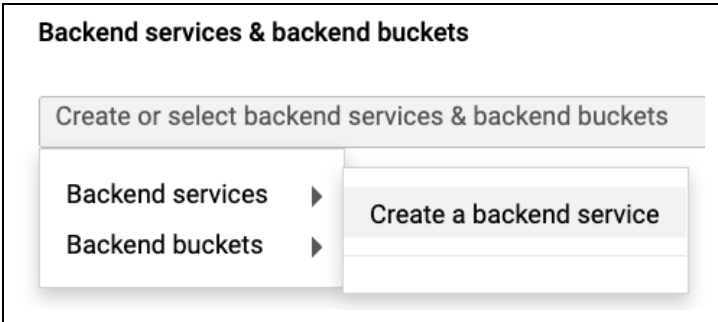
	<p>单击 Create load balancer。</p> <p>在 HTTP(S) Load Balancing 下，单击 Start configuration 按钮。</p> <p>选择“From Internet to my VMs”。</p> <p>单击 Continue 按钮。</p>
--	---

6.4.2 为负载均衡器设置名称

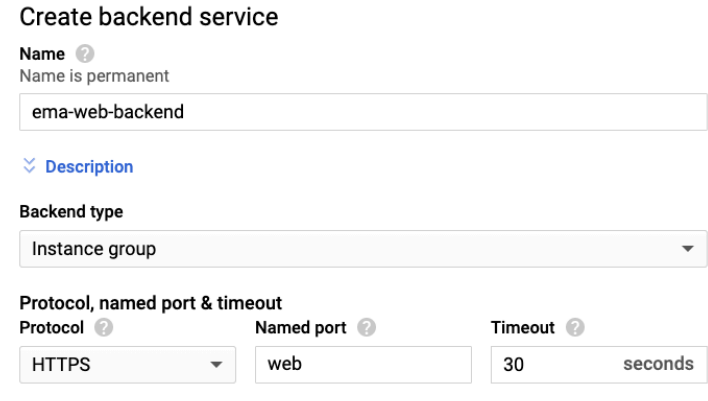
	<p>为负载均衡器输入唯一的名称 示例: <i>ema-web-lb</i></p>
---	--

6.4.3 后端服务配置

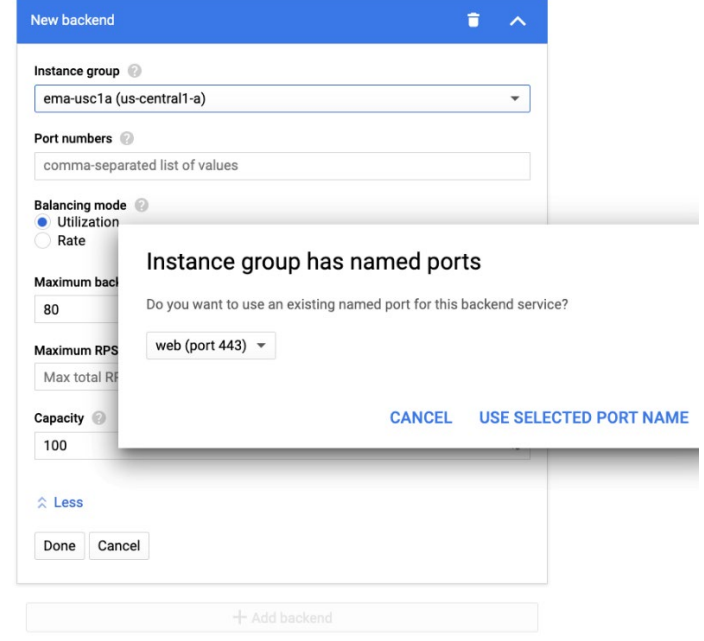
6.4.3.1 创建后端服务

	<p>单击 Backend configuration</p> <p>在下拉菜单中，导航至 Backend services > Create a backend service。</p>
--	---

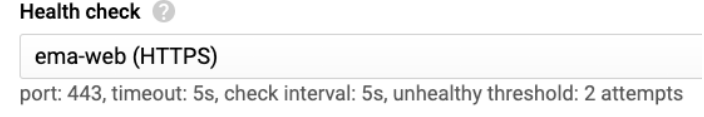
6.4.3.2 配置后端服务基本详细信息

	<p>按如下所示配置后端服务：</p> <ul style="list-style-type: none">• Name: 为后端服务输入唯一的名称 示例: <i>ema-web-backend</i>• Backend type: <i>Instance group</i>• Protocol: <i>HTTPS</i>• Named port: <i>web</i>
--	---

6.4.3.3 添加后端

	<p>在 New backend 部分中，选择您先前创建的第一个实例组。</p> <p>您将看到一个弹出窗口，询问您是否要使用现有的命名端口。选择 web (port 443) 并单击 Use Selected Port Name。</p> <p>单击 Done。</p> <p>对于您先前创建的其他非托管实例组，请单击 Add Backend 按钮，然后按说明重复这些操作。</p>
---	---

6.4.3.4 设置运行状况检查

	<p>从 Health check 下拉菜单中，选择您先前创建的 ema-web (HTTPS) 运行状况检查。</p>
--	--

6.4.3.5 启用会话保持

	<p>单击 Advanced configurations 以显示其他选项。</p> <p>将 Sessional affinity 设置为 <i>Generated cookie</i>。</p> <p>单击 Create 按钮。</p>
--	---

Security

Cloud Armor security policy [?] (Optional)

None

Session affinity [?] Affinity cookie TTL [?]

Generated cookie 0 seconds

Connection draining timeout [?]

300 seconds

Custom request headers [?] (Optional)

+ Add header

Press Ctrl+Space to get suggestions in the header value field

⤴ Hide advanced configurations

Create Cancel

6.4.4 前端配置

New Frontend IP and port

Name [?] (Optional) [?]
Name is permanent

ema-web-frontend

Add a description

Protocol [?]

HTTPS (includes HTTP/2)

Network Service Tier [?]

Premium (Current project-level tier, [change](#)) [?]

Standard [?]

IP version IP address

IPv4 ema-web-lb-ip (34.107.156.222)

Port

443

Certificate [?]

ema-web

⌵ Additional certificates

SSL policy [?]

GCP default

QUIC negotiation [?]

Automatic (default)

Done Cancel

单击 **Frontend configuration**。

按如下所示配置前端：

- **Name:** 为前端输入唯一的名称
示例: *ema-web-frontend*
- **Protocol:** *HTTPS*
- **IP address:** 从菜单中选择 Create IP address
 - 为 IP 地址输入唯一的名称
示例: *ema-web-lb-ip*
 - 单击 **Reserve**
- **Port:** *443*
- **Certificate:** 选择创建一个新证书并输入您的 SSL 证书信息

单击 **Done** 按钮。

6.4.5 检查并最终确定

New HTTP(S) load balancer

Name [?]
Name is permanent

- Backend configuration**
You have configured 1 backend(s)
- Host and path rules**
You have created host and path rules
- Frontend configuration**
Your frontend is configured
- Review and finalize**
Optional →

Review and finalize

Backend

Backend services

1. **ema-web-backend**
Endpoint protocol: **HTTPS** Named port: **web** Timeout: **30 seconds** Cloud CDN: **disabled** Health check: **ema-web**

Advanced configurations

Instance group	Zone	Autoscaling	Balancing mode	Capacity	Selected ports
ema-us-c1a	us-central1-a	No configuration	Max backend utilization: 80%	100%	443
ema-us-c1c	us-central1-c	No configuration	Max backend utilization: 80%	100%	443

Host and path rules

Hosts	Paths	Backend
All unmatched (default)	All unmatched (default)	ema-web-backend

Frontend

Protocol	IP:Port	Certificate	SSL policy	Network Tier
HTTPS	34.107.156.222:443	ema-web	GCP default	Premium

单击 **Review and finalize**。

检查屏幕上的信息，然后单击 **Create** 按钮。

6.5 创建 TCP 负载均衡器

6.5.1 选择 TCP 负载均衡

TCP Load Balancing

Layer 4 load balancing or proxy for applications that rely on TCP/SSL protocol [Learn more](#)

Configure
TCP LB
SSL Proxy
TCP Proxy

Options
Internet-facing or internal
Single or multi-region

Internet facing or internal only

Do you want to load balance traffic from VMs in your network?

- From Internet to my VMs
- Only between my VMs

Multiple regions or single region

Do you want to place the backends for across multiple regions?

- Multiple regions (or not sure yet)
- Single region only

单击 **Create load balancer**。

在 **TCP Load Balancing** 下，单击 **Start configuration** 按钮。

选择 "From Internet to my VMs"。

选择 "Multiple regions"

单击 **Continue** 按钮。

6.5.2 为负载均衡器设置名称

New TCP/SSL load balancer

Name

为此负载均衡器输入唯一的名称。
示例: *ema-swarm-lb*

6.5.3 后端服务配置

6.5.3.1 配置后端服务基本详细信息

<h3>Backend configuration</h3> <p>Name ema-swarm-lb Add a description</p> <p>Backend type</p> <p><input checked="" type="radio"/> Instance group <input type="radio"/> Zonal network endpoint group</p> <p>Protocol <input type="text" value="TCP"/> <input <="" p="" type="button" value="?"/><p>Named port * <input type="text" value="swarm"/></p><p>Timeout * <input type="text" value="30"/></p></p>	<p>按如下所示配置后端服务：</p> <ul style="list-style-type: none">• Backend type: <i>Instance group</i>• Protocol: <i>TCP</i>• Named port: <i>swarm</i>
---	--

6.5.3.2 添加后端

<h3>New backend</h3> <p>Instance group * <input type="text" value="ema-usc1a"/></p> <p>Port numbers * <input type="text" value="8080"/></p> <p>Balancing mode <input checked="" type="radio"/> Utilization <input type="radio"/> Connection</p> <p>Maximum backend utilization * <input type="text" value="80"/> % <input <="" p="" type="button" value="?"/><p>Maximum connecti... Connections <input <="" p="" type="button" value="?"/><p>Scope <input type="text" value="per instance"/></p><p>Capacity <input type="text" value="100"/> % <input <="" p="" type="button" value="?"/><p>SHOW LESS</p><p>CANCEL DONE</p></p></p></p>	<p>在 New backend 部分中，选择您先前创建的第一个实例组。</p> <p>您将看到一个弹出窗口，询问您是否要使用现有的命名端口。选择 swarm (port 8080) 并单击 Use Selected Port Name。</p> <p>其余设置可以保留为默认值。</p> <p>单击 Done。</p> <p>对于您先前创建的其他非托管实例组，请单击 Add Backend 按钮，然后按说明重复这些操作。</p>
---	---

6.5.3.3 设置运行状况检查

<p>Health check * <input type="text" value="ema-swarm"/></p> <p>port: 8080, timeout: 5s, check interval: 5s, unhealthy threshold: 2 attempts</p>	<p>从 Health check 下拉菜单中，选择您先前创建的 ema-swarm 运行状况检查。</p>
--	--

6.5.4 前端配置

Frontend configuration

Specify an IP address, port and protocol. This IP address is the frontend IP for your clients requests. For SSL, a certificate must also be assigned.

New Frontend IP and port

Name
ema-swarm-frontend

▼ DESCRIPTION

Protocol
TCP

Network Service Tier ?
 Premium (Current project-level tier, [change](#)) ?
 Standard (us-central1) ?

IP version
IPv4

IP address
ema-swarm-lb-ip

Port
9092

Proxy protocol
Off

[CANCEL](#) [DONE](#)

单击 **Frontend configuration**。

按如下所示配置前端：

- **Name:** 为前端输入唯一的名称
示例: *ema-swarm-frontend*
- **Protocol:** *TCP*
- **IP address:** 从菜单中选择 Create IP address
 - 为 IP 地址输入唯一的名称
示例: *ema-swarm-lb-ip*
 - 单击 **Reserve**
- **Port:** *9092*
您可以从列表中选择备用端口。需要注意的是，您稍后可以按照《Intel EMA Server 安装指南》中的说明进行操作，以通知服务器转发匹配的端口。

单击 **Done** 按钮。

6.5.5 检查并最终确定

← New TCP/SSL load balancer

Name
ema-swarm-lb

Backend configuration
 Frontend configuration
 Review and finalize (optional)

[CREATE](#) [CANCEL](#)

Frontend

Protocol	IP:Port	Certificate	SSL Policy	Proxy Protocol
TCP	:9092	-		Off

Backend

Endpoint protocol	Named port	Timeout	Health check
TCP	swarm	30 seconds	ema-swarm

▼ ADVANCED CONFIGURATIONS

Name	Type	Zone	Autoscaling	Balancing mode	Selected p
ema-usc1a	Instance group	us-central1-a	No configuration	Max backend utilization: 80%	8080
ema-usc1c	Instance group	us-central1-c	No configuration	Max backend utilization: 80%	8080

单击 **Review and finalize**。

检查屏幕上的信息，然后单击 **Create** 按钮。

6.6 Intel EMA Server 的 DNS

对于单服务器部署，如果您拥有自己的域，则需要创建一个 DNS 记录，它指向为 Intel EMA 虚拟机保留的公共 IP 地址。

对于分布式服务器部署，您需要创建一个 DNS 记录，指向负载均衡器的公共 IP 地址。

有关此任务，请咨询您的 DNS 管理员。

7 附录 B — 有关与 Active Directory* 集成的说明

从 2020 年 2 月起，Microsoft AD* 托管服务已全面提供。我们尚未使用此新服务测试过 Intel EMA 部署，但以下链接提供了进一步的详情。

<https://cloud.google.com/blog/products/identity-security/managed-service-for-microsoft-active-directory-is-ga>

https://cloud.google.com/managed-microsoft-ad/?hl=en_US