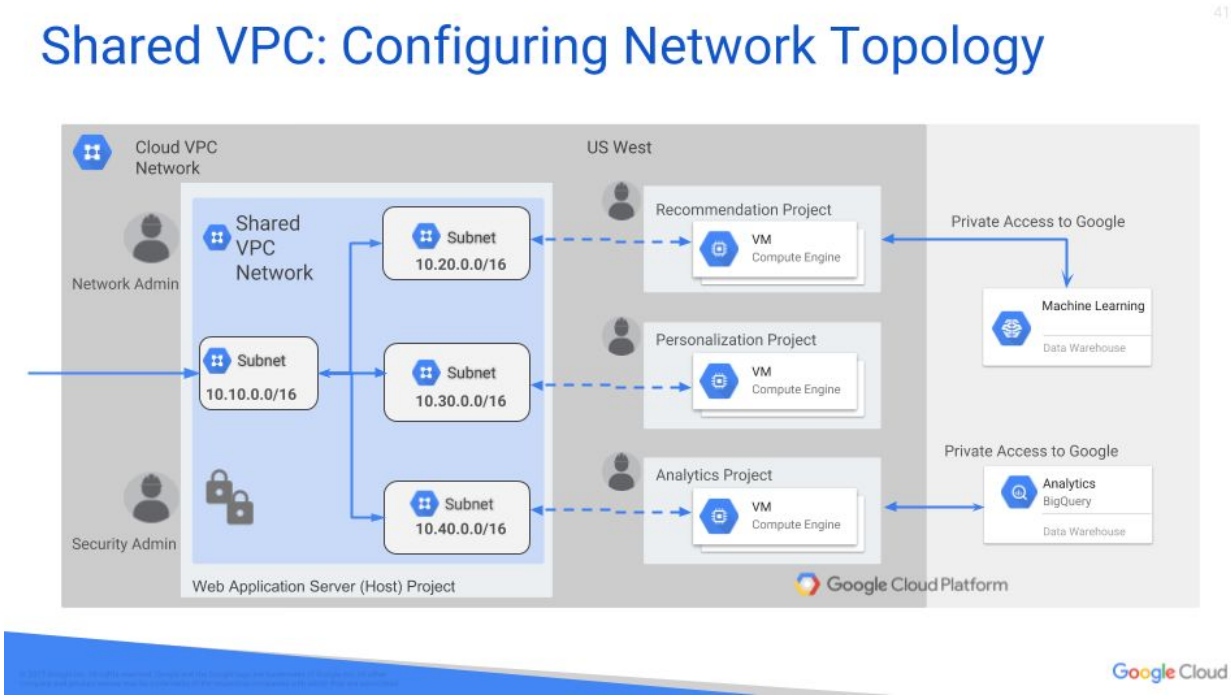
Google Cloud中配置Shared VPC

一 Shared VPC介绍

Google Cloud中有一种特殊的VPC，叫Shared VPC。这个VPC可以共享给其他Project使用。如下图：



在Shared VPC的使用中，有两种Project：Host Project和Service Project。上图中Shared VPC Network所在的蓝色的Project即是Host Project；而VM所在的Project为Service Project。在这种架构中，Network的组件，包括VPC、Subnet、IP Address、防火墙等都在Host Project中的Shared VPC中定义，Shared VPC把这些资源共享给Service Project，在Service Project中就可以使用这些资源了。

二 Shared VPC的配置

下面介绍Shared VPC的具体配置，包括Shared VPC权限、Host Project的配置和Service Project的使用。

1 Shared VPC的权限

由于Shared VPC要在多个Project中共享资源，所以开启Shared VPC要求有Project在Organization下。Organization的开启方法请参考“Google Cloud IAM中添加自定义域名”。

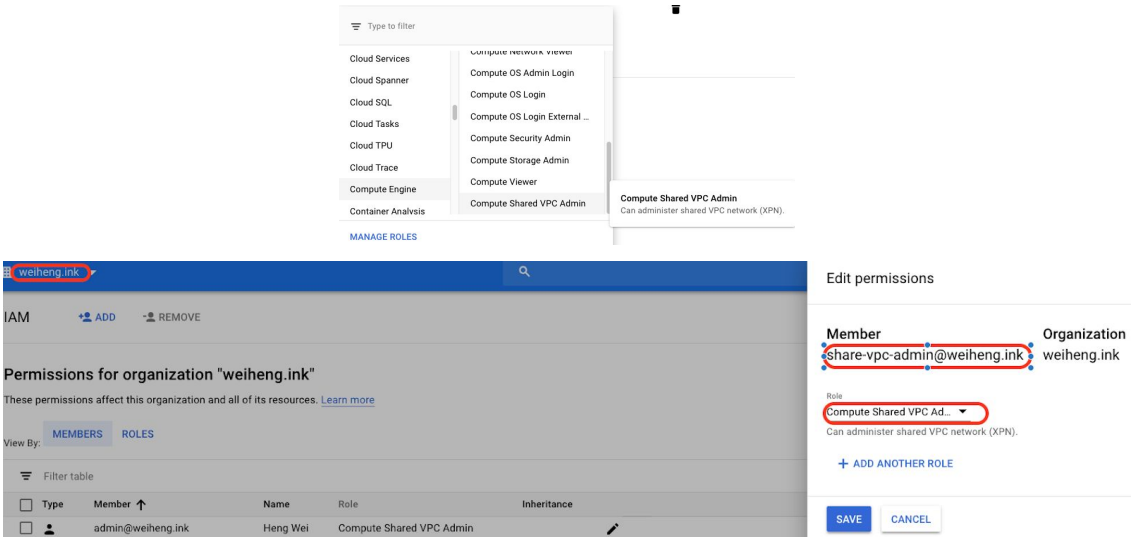
A. 资源准备：

- 3个用户：share-vpc-admin, p1-vm-admin, p2-vm-admin
- 3个Project：hw-host-project01, hw-svc-project01, hw-svc-project02

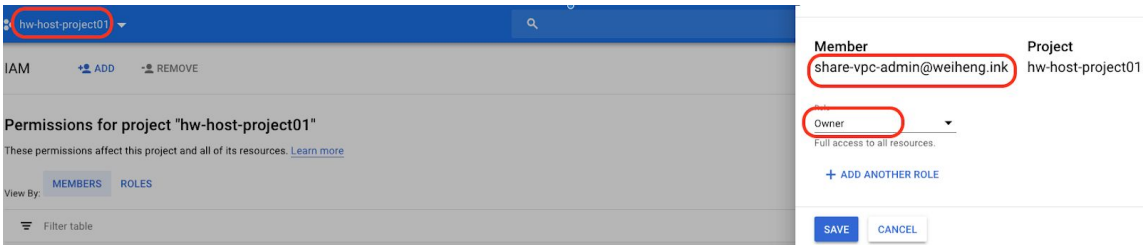
从名字可以看出各个用户和project的角色和功能。

B. 具体授权的操作如下：

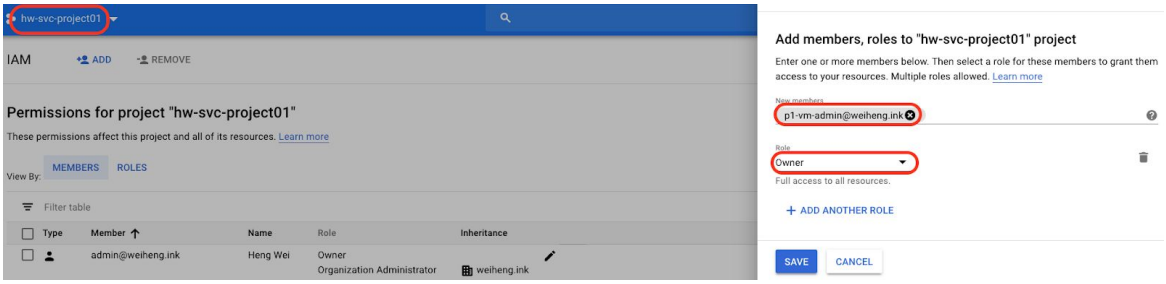
在weiheng.ink的组织下，给share-vpc-admin赋予Compute Shared VPC Admin（这个权限在Compute Engine下）的权限：



在hw-host-project的IAM中，给share-vpc-admin赋予：project owner权限：



在hw-svc-project01内，给p1-vm-admin赋予：project owner的权限：



类似的，在hw-svc-project02内给p2-vm-admin赋予project owner的权限。

2 Host Project中的配置

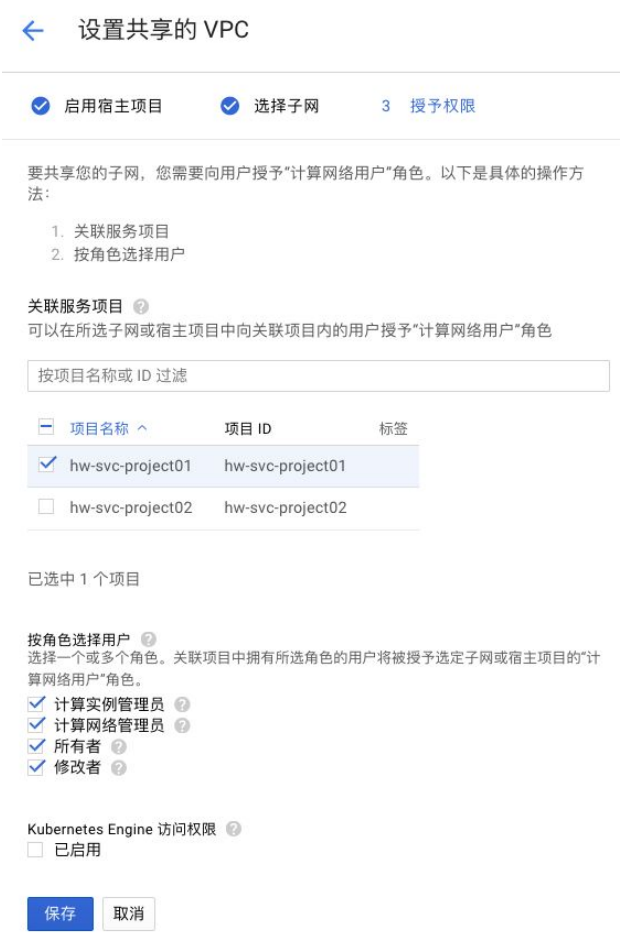
A. 创建VPC

B.创建两个子网sharevlan1和sharevlan2

C.开启shared VPC

D. 按照向导设置Shared VPC

出现设置共享VPC的界面，共分三步：启用宿主项目，选择子网和授予权限：



这样，sharevlan1就共享给了hw-svc-project01项目。

E. 手工设置Shared VPC共享

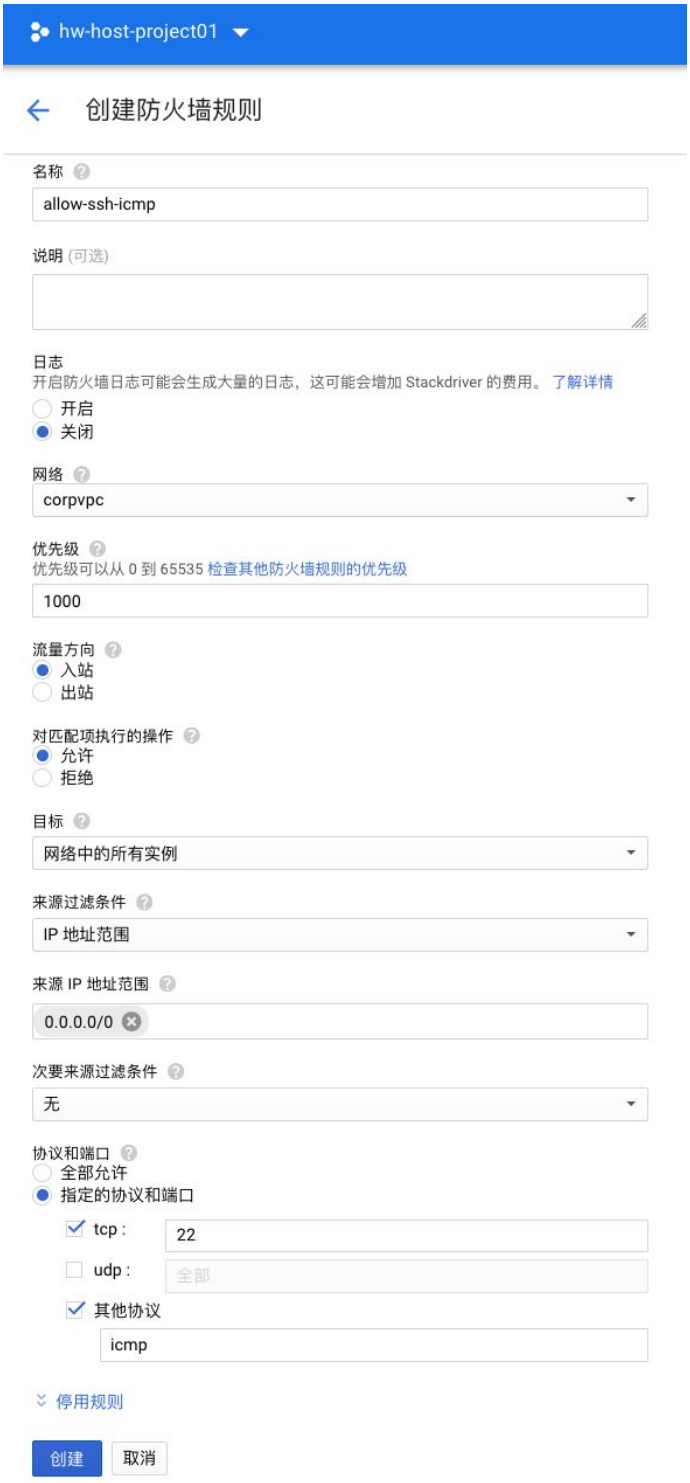
也可以通过配置关联项目实现共享：

选择子网和相应的项目：

这样配置以后，Sharevlan1共享给了hw-svc-project01，Sharevlan2共享给了hw-svc-project02。

F. 创建防火墙规则

Shared VPC的防火墙规则需要集中统一在host project中配置，在Service Project中不能自行配置防火墙规则。

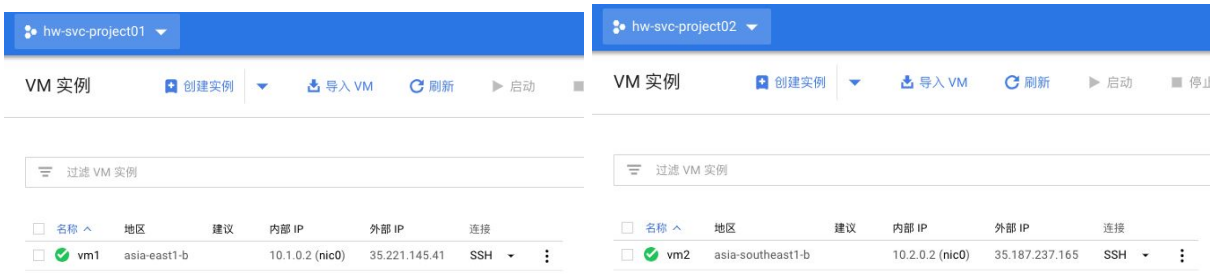


3 在Service Project中使用Shared VPC的资源

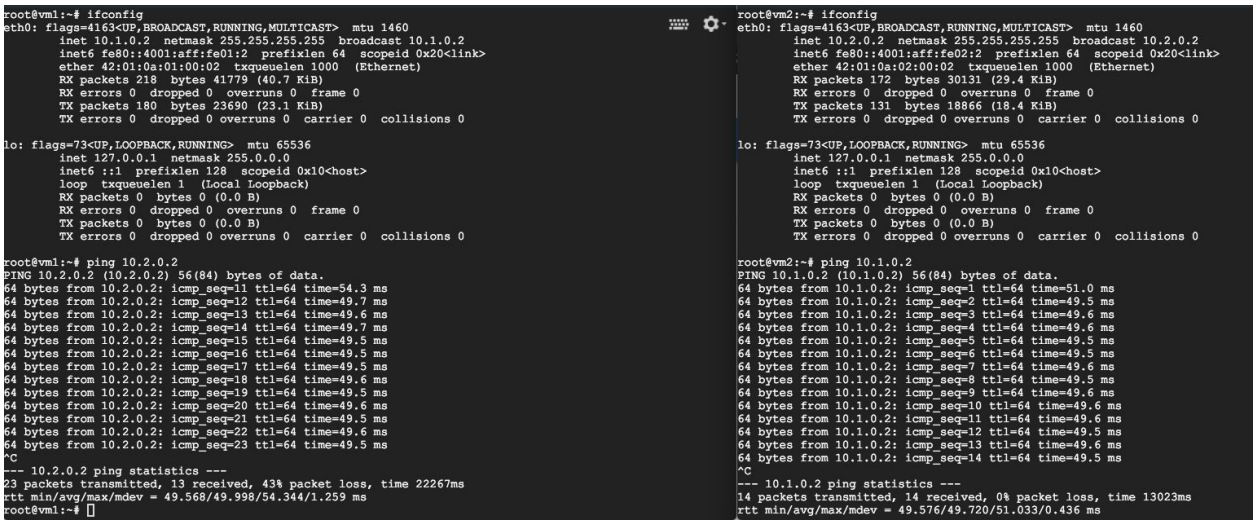
在Service Project中，用户可以像使用自己创建的VPC资源一样使用Shared VPC中的网络资源。

使用p1-vm-admin用户登录， 在hw-svc-project01中在sharevlan1的子网中，创建VM1：

同样，在hw-svc-project02中创建VM2。



创建成功后，VM间可以相互ping通：



三 总结

Google Cloud中的Shared VPC是一种集中管理网络资源的方法。在一个企业中，网络安全管理往往和系统管理、软件管理分开。为方便的对网络进行统一的管理和配置，便有了Shared VPC这样的功能。