**Tech Summit 2018**

**Hand­s-on lab**

Azure Network Best Practise Hands-on Lab

******Contents**

**Overview 3**

**EXERCISE 1: AZURE 虚拟网络实验 5**

**EXERCISE 2: AZURE NSG 网络安全组实验 11**

**EXERCISE 3: AZURE 负载均衡实验 17**

**EXERCISE 4: AZURE NAT实验 23**

**EXERCISE 5: AZURE VPN 网关实验 27**

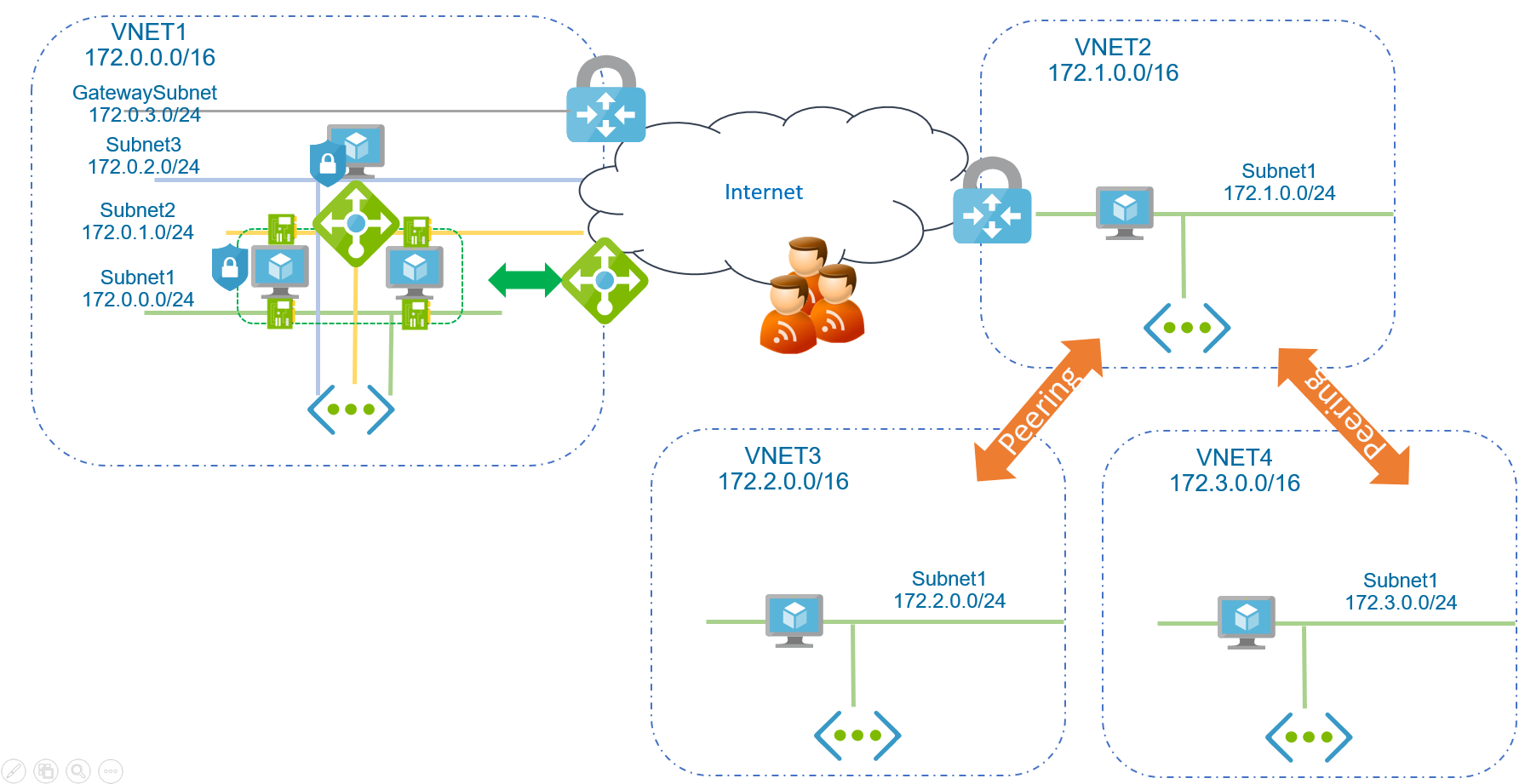
**EXERCISE 6: AZURE 对等互联实验 39**

**EXERCISE 7: AZURE NVA + UDR实验 53**

**EXERCISE 8: AZURE 专线演示实验 61**

Overview

本实验希望通过和大家一起在实际操作中深入了解AZURE网络概念，并掌握AZURE网络基本日常操作，熟悉AZURE云网络架构的最佳实践。



**Objectives**

1. 本实验手册分为八部分实验：
   * 实验一：AZURE虚拟网络实验
   * 实验二：AZURE NSG网络安全组实验
   * 实验三：AZURE 负载均衡实验
   * 实验四：AZURE NAT实验（选做）
   * 实验五：AZURE VPN网关实验
   * 实验六：AZURE 对等互联实验
   * 实验七：AZURE NVA+UDR实验（选做）
   * 实验八：AZURE 专线演示实验（只做演示学员无需操作）

**System requirements**

* 1. 实验前需准备如下内容:
  + Windows 10
  + Internet explorer

**Setup**

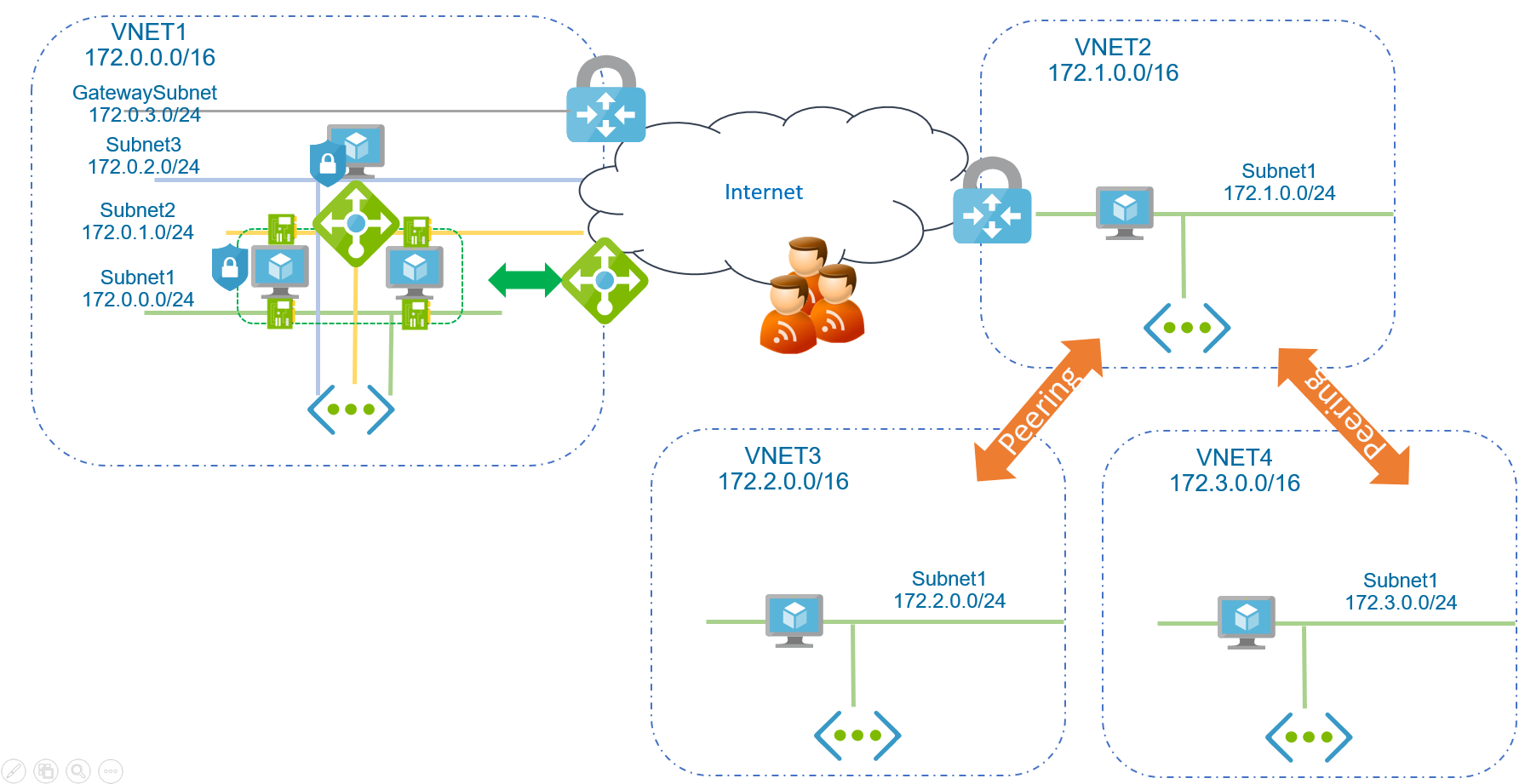
* 1. 实验前需要进行如下操作进行实验机器准备:
  2. Install Microsoft Windows 10.
  3. Check Azure Portal access using internet explorer （portal.azure.com）

**Exercises**

* 1. 本实验包含如下内容:
  2. AZURE虚拟网络实验
  3. AZURE NSG网络安全组实验
  4. AZURE 负载均衡实验
  5. AZURE NAT实验（选做）
  6. AZURE VPN网关实验
  7. AZURE 对等互联实验
  8. AZURE NVA+UDR实验（选做）
  9. 实验八：AZURE 专线演示实验（只做演示学员无需操作）
  10. 预计实验完成时间:  **45 minutes**.

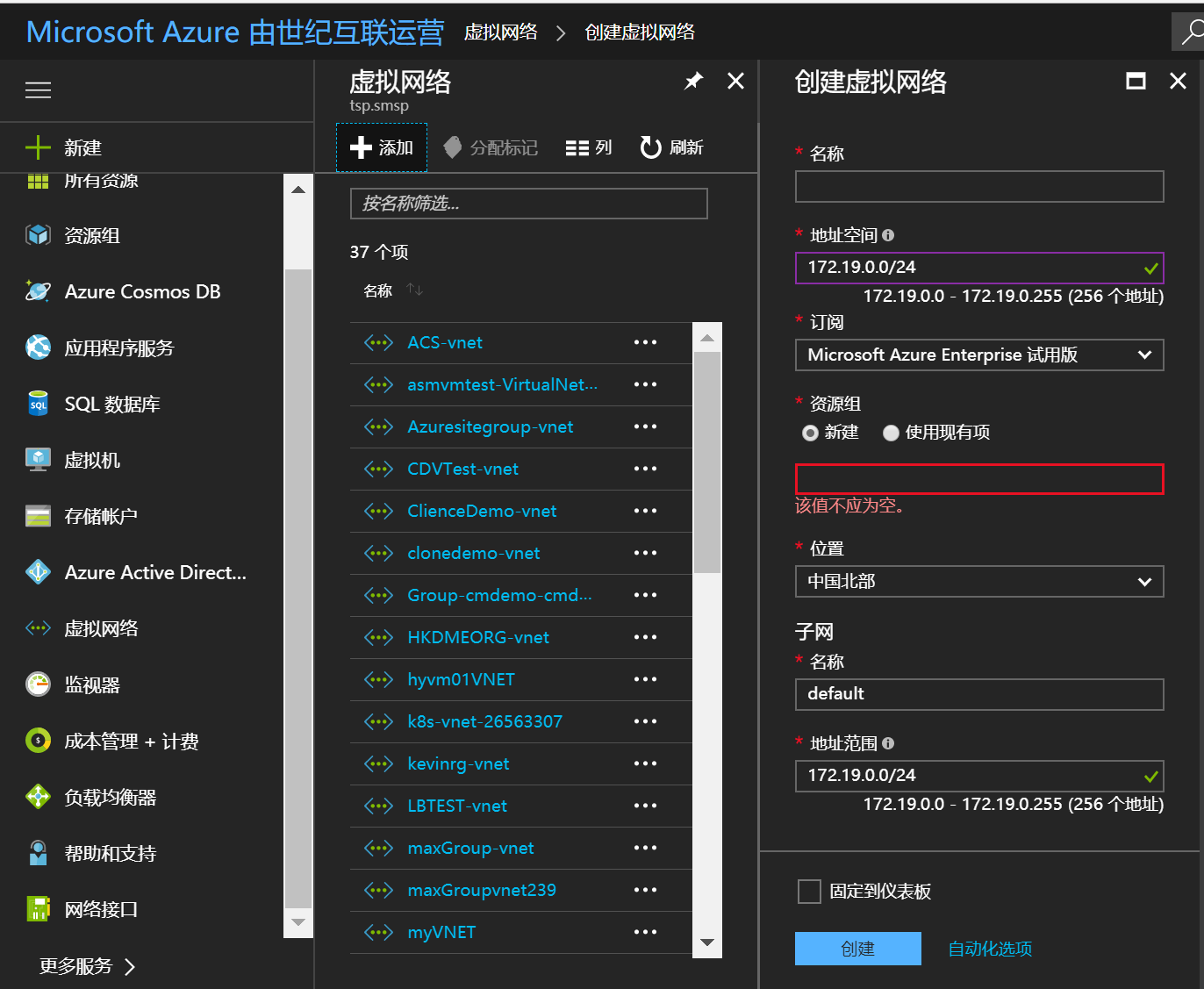
Exercise 1: AZURE虚拟网络实验

实验目标：建立VNET1，掌握虚拟网络内连通性



1. **创建虚拟网络VNET1**

进入AZURE Portal门户，选择虚拟网络并添加，输入名称VNET1，地址空间172.0.0.0/16，资源组名称tech014，位置East US2，子网名称Subnet1，地址空间172.0.0.0/24。注意区分大小写。



1. **添加子网**

选择虚拟网络，点击上一步创建的虚拟网络VNET1，选择子网并添加，添加子网Subnet2，名称Subnet2，地址空间172.0.1.0/24，网络安全组无，路由表无，服务终结点选中0个。注意区分大小写。



相同方法添加子网Subnet3，名称Subnet3，地址空间172.0.2.0/24，网络安全组无，路由表无，服务终结点选中0个。注意区分大小写。

1. **创建虚拟机**

访问<https://github.com/nonokangwei/TechSummit2018/blob/master/TwoNicVM.json> 拷贝双网卡虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称（建议使用VM1），选择资源组（选择之前VNET1所在资源组）。重复上述操作建立虚拟机VM2。

上述操作也可通过CLI完成：

az group deployment create --template-uri https://raw.githubusercontent.com/nonokangwei/TechSummit2018/master/TwoNicVM.json --parameters adminUsername=username adminPassword=password virtualMachineName=VMname -g resourcegroup

访问<https://github.com/nonokangwei/TechSummit2018/blob/master/OneNicVM.json>拷贝单网卡虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称（建议使用VM3），选择资源组（选择之前VNET1所在资源组）。

1. **测试虚拟机连通性**

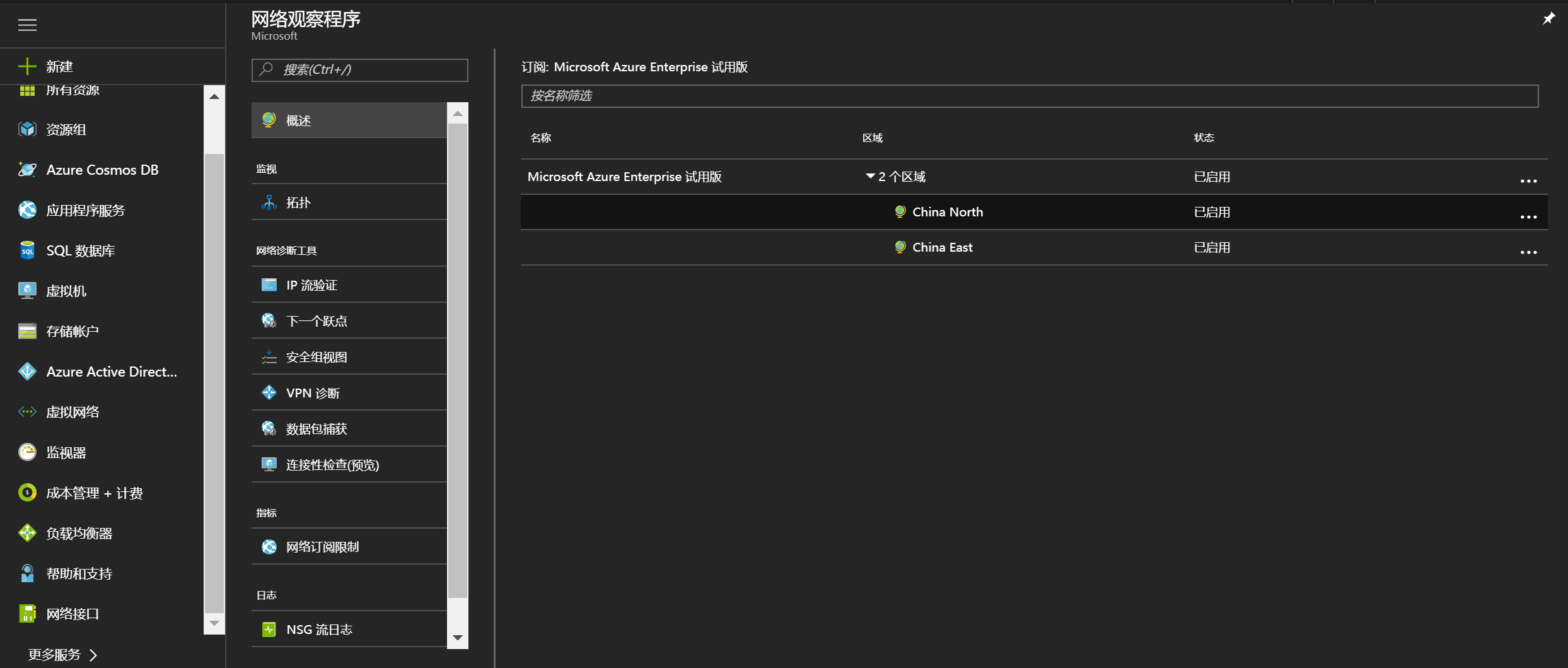
选择VM1，查看VM1公网ip，通过ssh访问（ssh username@vm1\_PublicIP）。远程登陆虚拟机后，ip addr list查看网卡地址。Ping 172.0.0.5 查看VNET1内网连通性。Curl [www.azure.com](http://www.azure.com) 查看VNET1的外网联通性。

1. **通过NetworkWatcher查看拓扑**

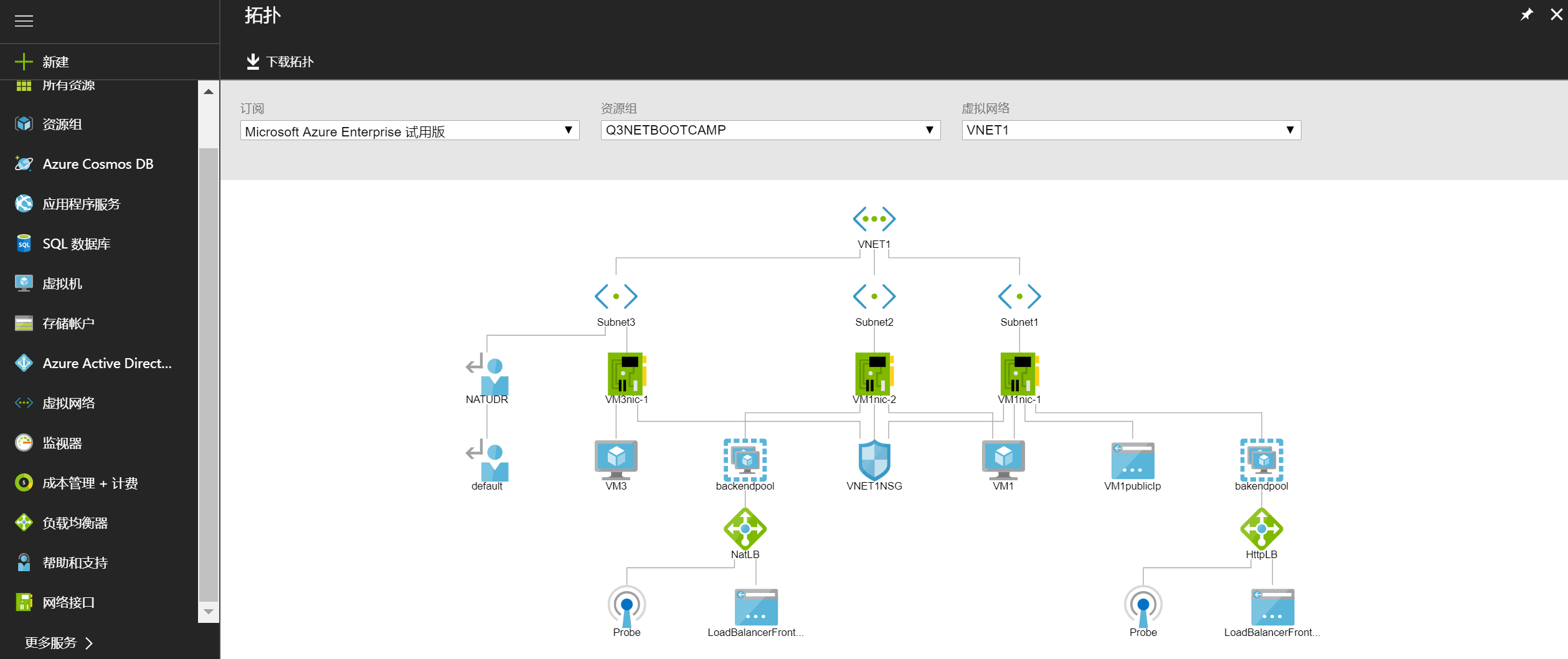
选择NetworkWatcher，



启用East US 2和West US 2的NetworkWatcher服务

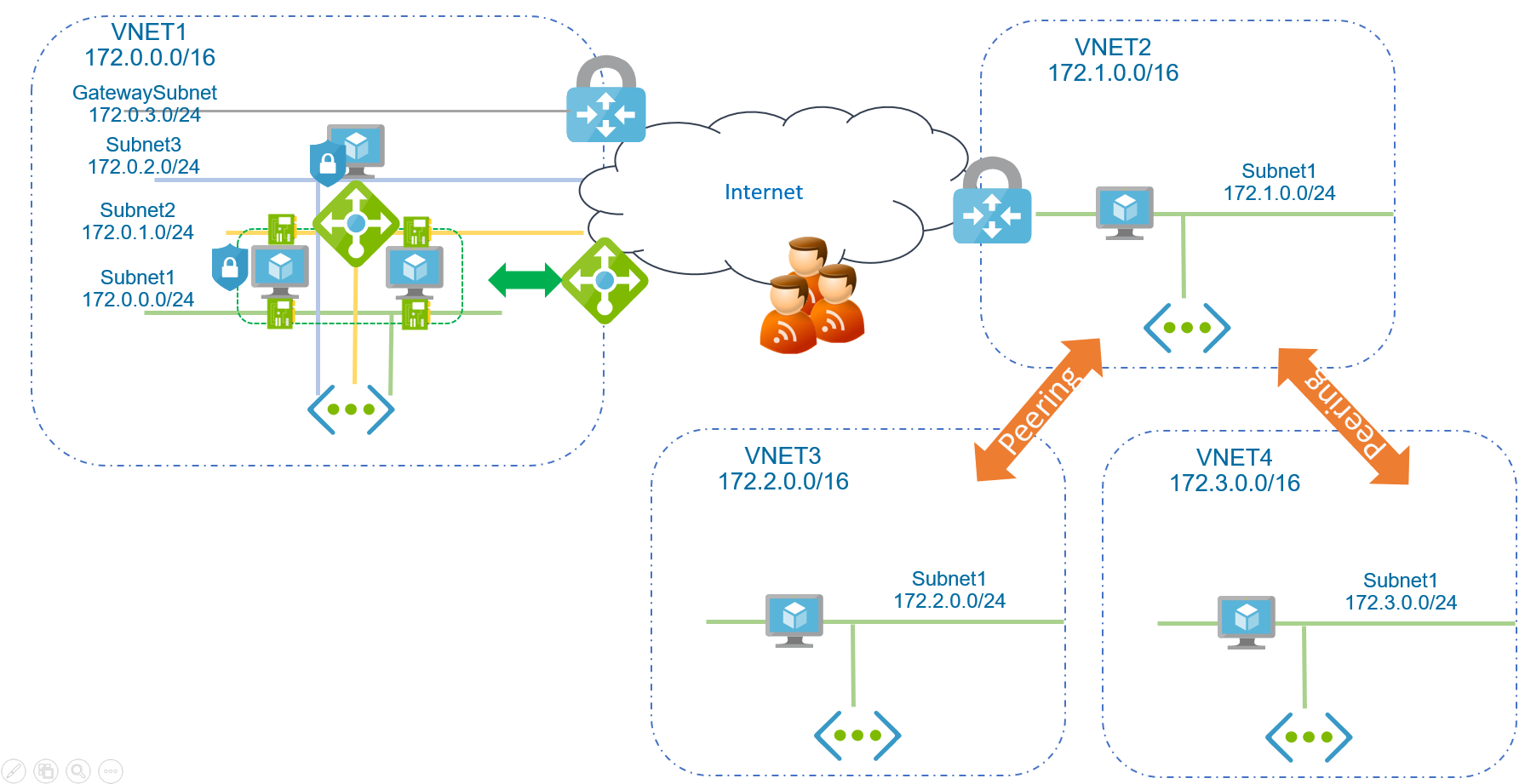


启用后选择拓扑，选择VNET1所在订阅，选择资源组，选择虚拟网络，获取网络拓扑结构

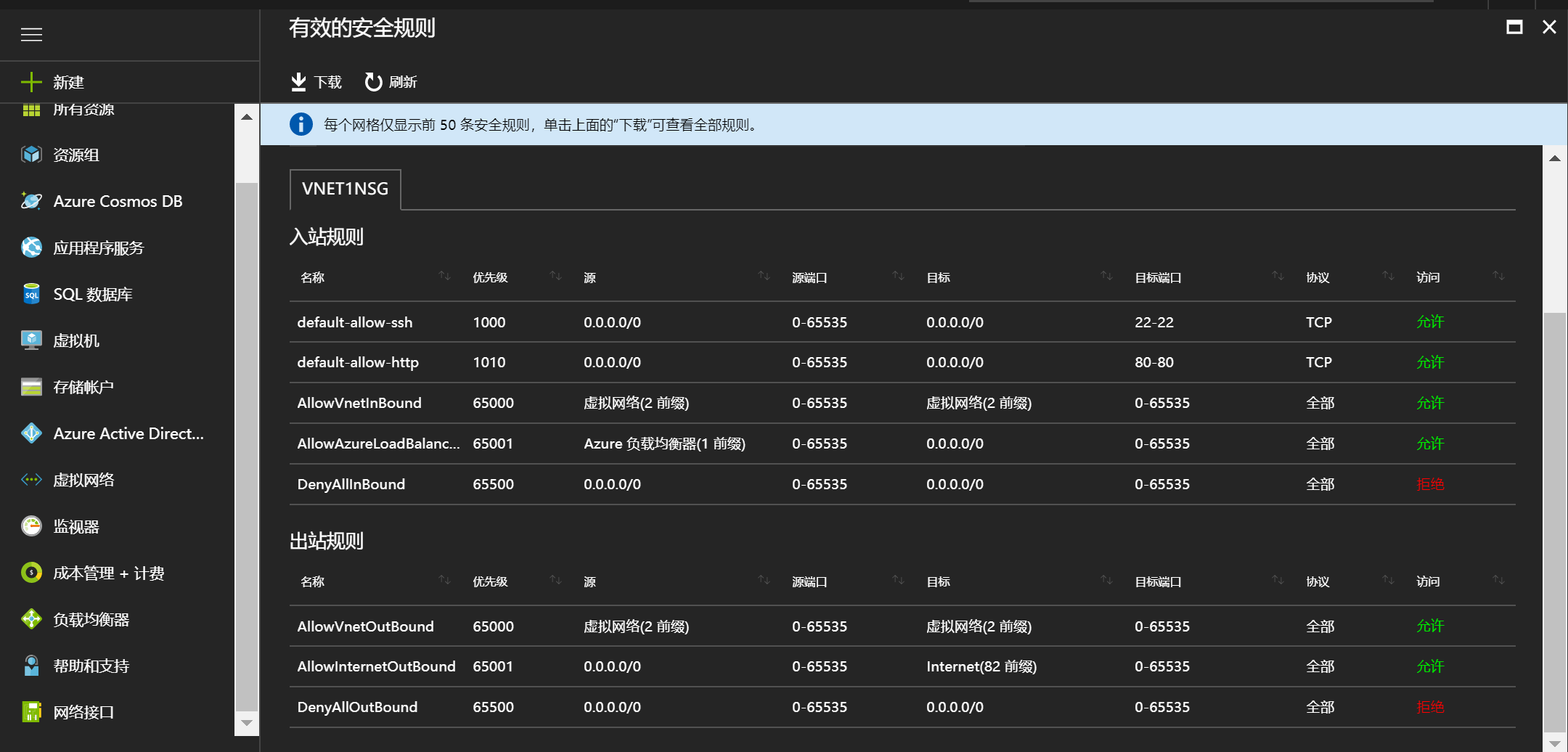
* 1. 

Exercise 2: AZURE NSG 网络安全组实验

实验目标：掌握NSG策略，如何通过主机NSG策略实现安全策略，如果通过子网NSG策略实现安全策略。



1. 选择虚拟机VM1，选择网络，选择VM1nic1的有效的安全规则



查看入站规则，理解入站优先级1000规则和入站优先级65000规则



1. 通过SSH VM1的公网IP远程登陆，登陆成功并退出
2. 选择虚拟机VM1，选择网络，点击优先级1000规则，将允许改为拒绝。再次模拟通过SSH VM1的公网IP远程登陆，登陆失败。验证完成后重新将拒绝改为允许恢复规则。
3. 重新登陆VM1，ping 172.0.0.5验证ping成功。通过本地ping VM2公网地址，验证ping失败，结合NSG策略思考失败原因。
4. 选择虚拟机VM2，选择网络，选择VM2nic-1，点击添加入站端口规则，选择高级，设置规则，源Any，源端口范围\*，目标Any，目标端口范围\*，协议Any，操作允许，优先级1020，名称default-allow-icmp，确定保存。再次尝试通过本地ping VM2的公网IP，验证连通性。思考NSG策略作用。
5. 重新登陆VM1，ping 172.0.0.5验证pingVM2成功。
6. 创建网络安全组

选择网络安全组，点击添加，



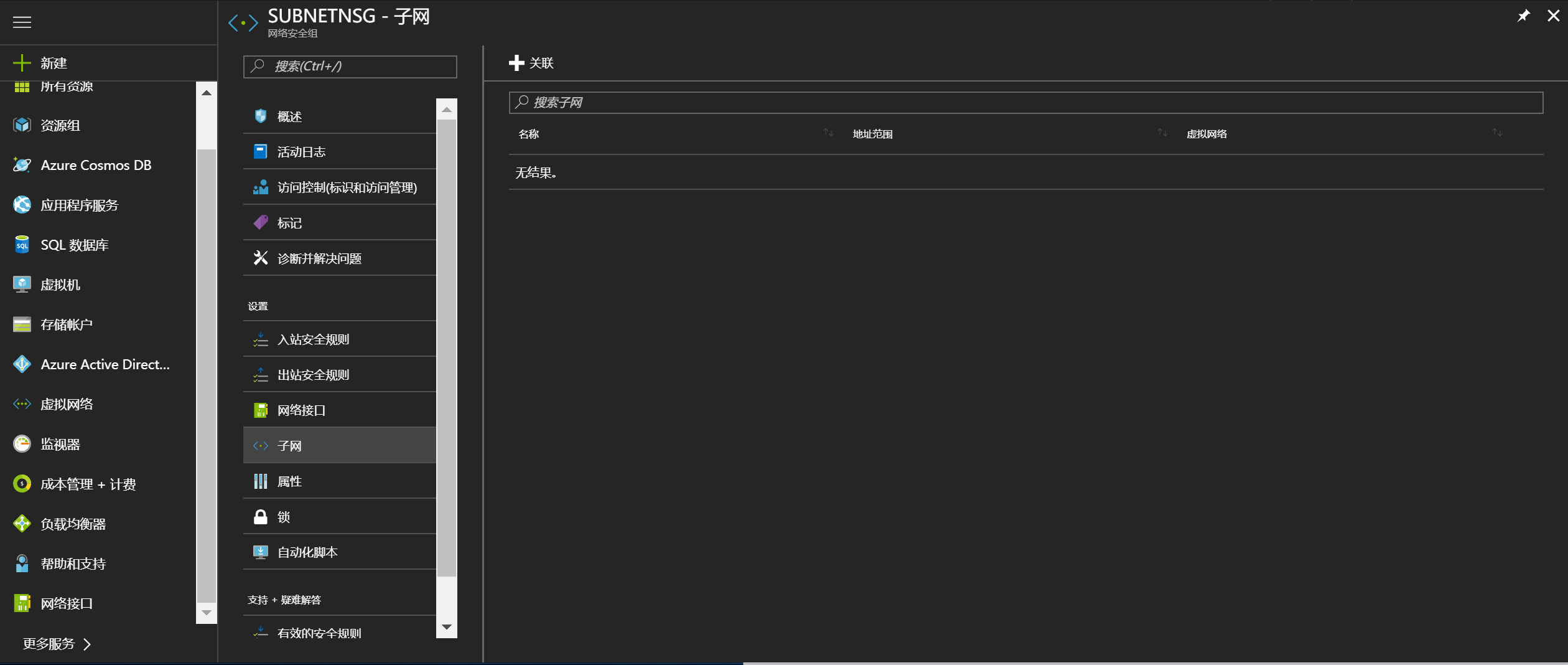
输入名称SUBNETNSG，资源组选择Tech014，位置East US 2

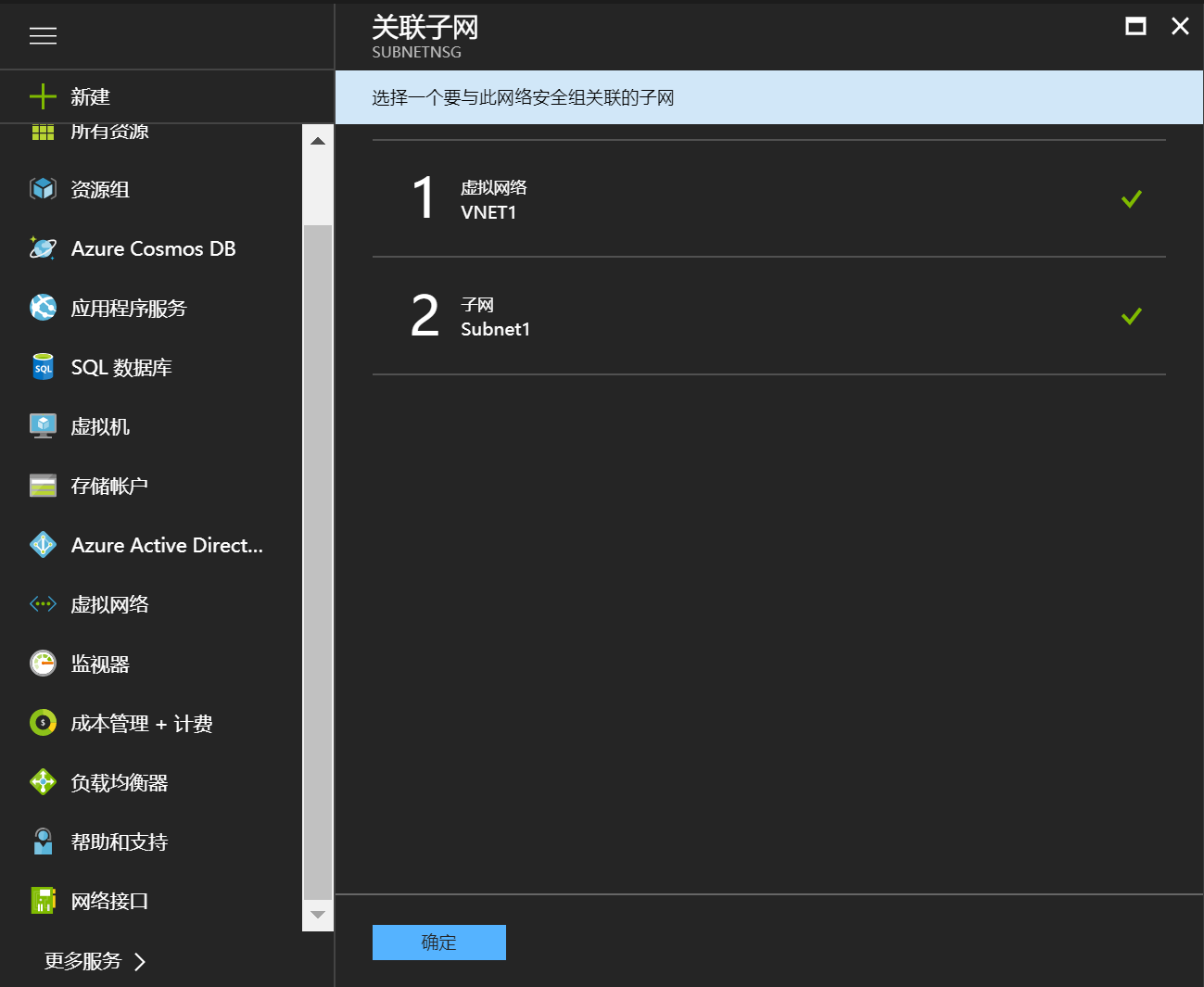
1. 创建网络安全组规则

选择创建的SUBNETNSG网络安全组，选择入站安全规则，点击添加，源IP Address，源IP地址范围172.0.0.4/32, 源端口范围\*，目标IP Address，目标IP地址范围172.0.0.5/32，目标端口范围\*，协议Any，操作拒绝，优先级1000，名称default-deny-vm1-vm2-icmp。

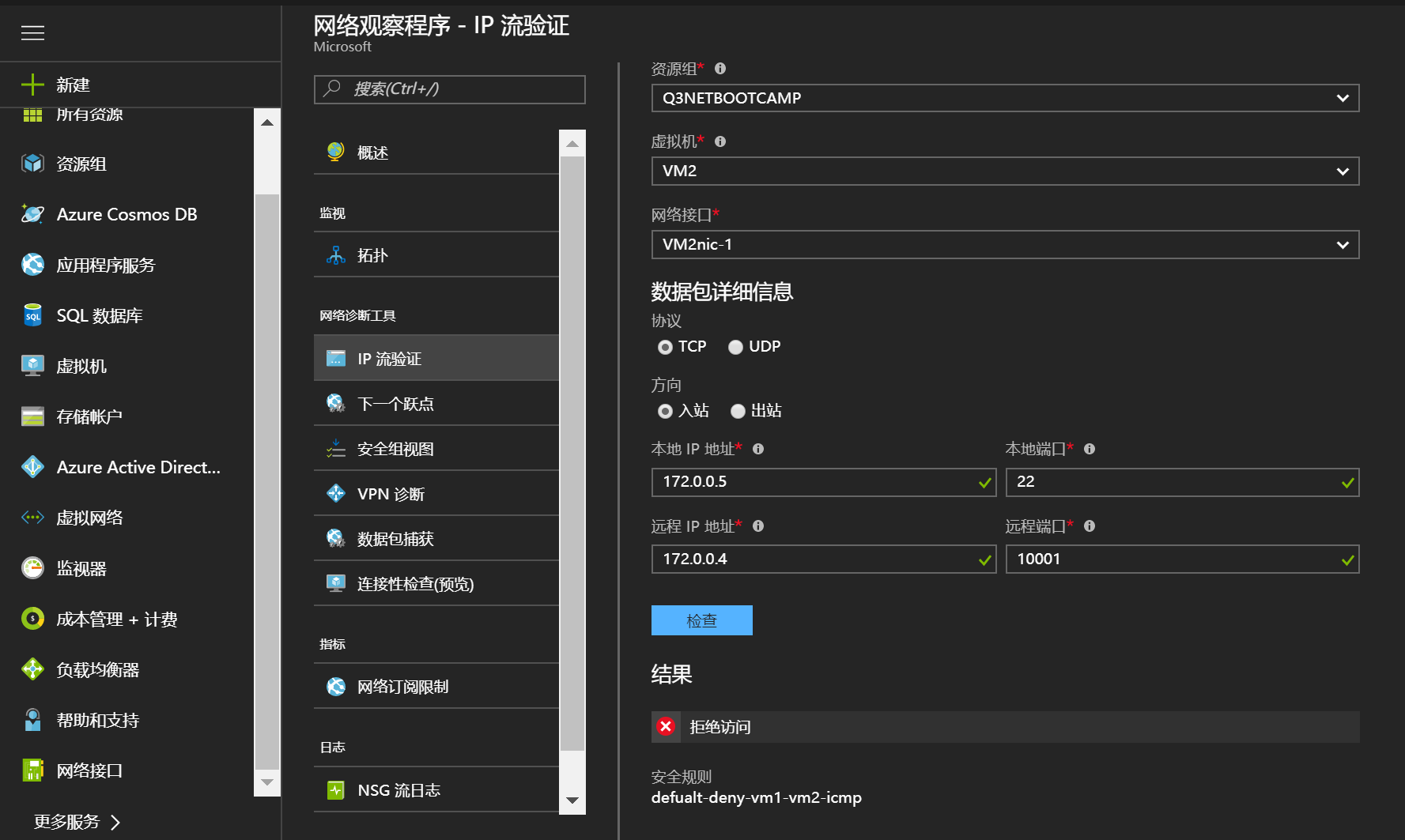
1. 关联子网网络安全组规则

选择创建的SUBNETNSG网络安全组，选择子网，点击关联，虚拟网络选择VNET1，子网选择Subnet1，保存。

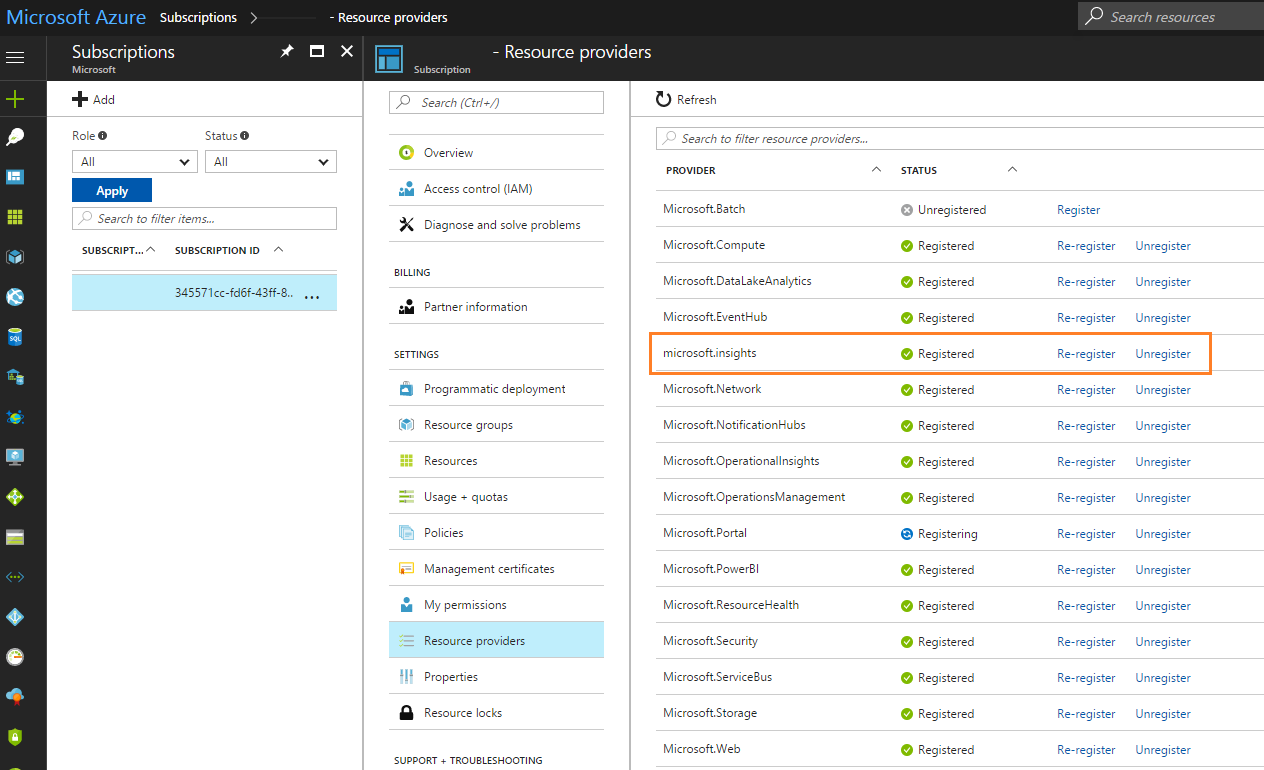




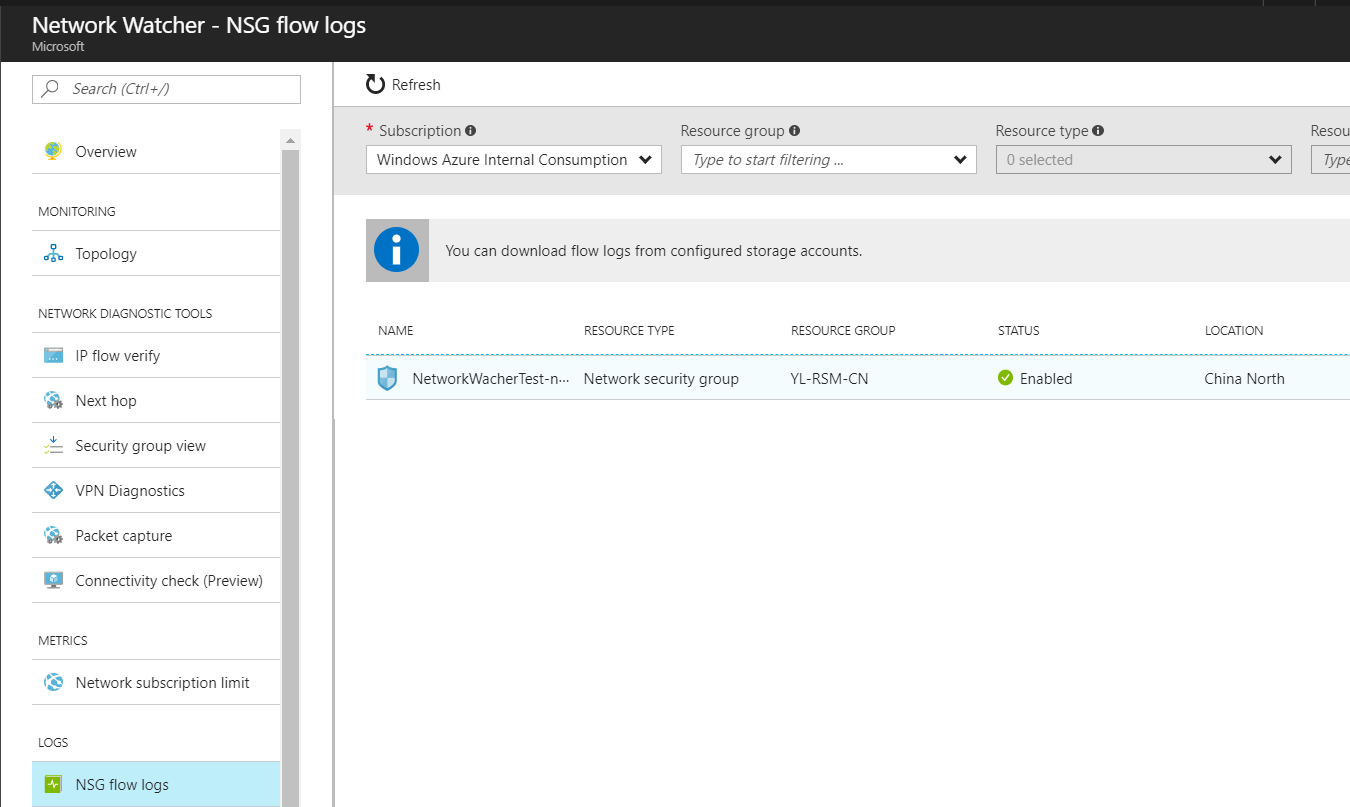
1. 登陆VM1，再次验证ping 172.0.0.5，此时ping失败。思考失败原因。
2. 选择网络观察程序（NetworkWatcher），点击IP流验证，资源组tech014，虚拟机VM2，网络接口VM2nic1，协议TCP，方向入站，本地IP地址172.0.0.5，本地端口22，源端IP地址172.0.0.4，源端端口10001，进行检查。查看检查结果。



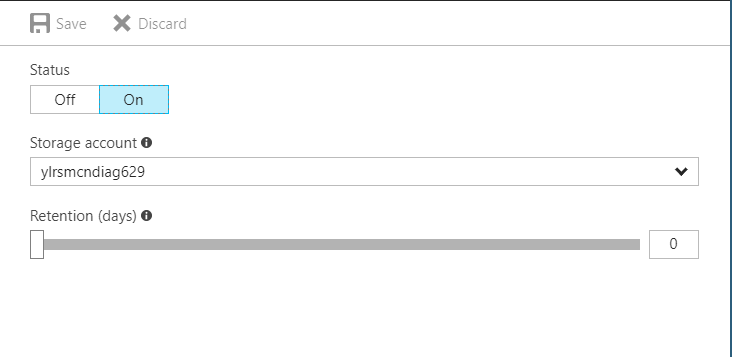
1. 以VM1为跳板机，ssh 172.0.1.5登陆VM2.，验证ping 172.0.0.4，ping成功，思考成功原因。
2. 取消子网网络安全组规则关联，恢复连通性。选择创建的SUBNETNSG网络安全组，选择子网，选择子网选择Subnet1取消关联。
3. 通过Network Watcher分析NSG日志（选作）。Network Watcher可以用于对网络安全组的日志进行分析，客户可以直观感受NSG当前运行情况。注册insight组件。



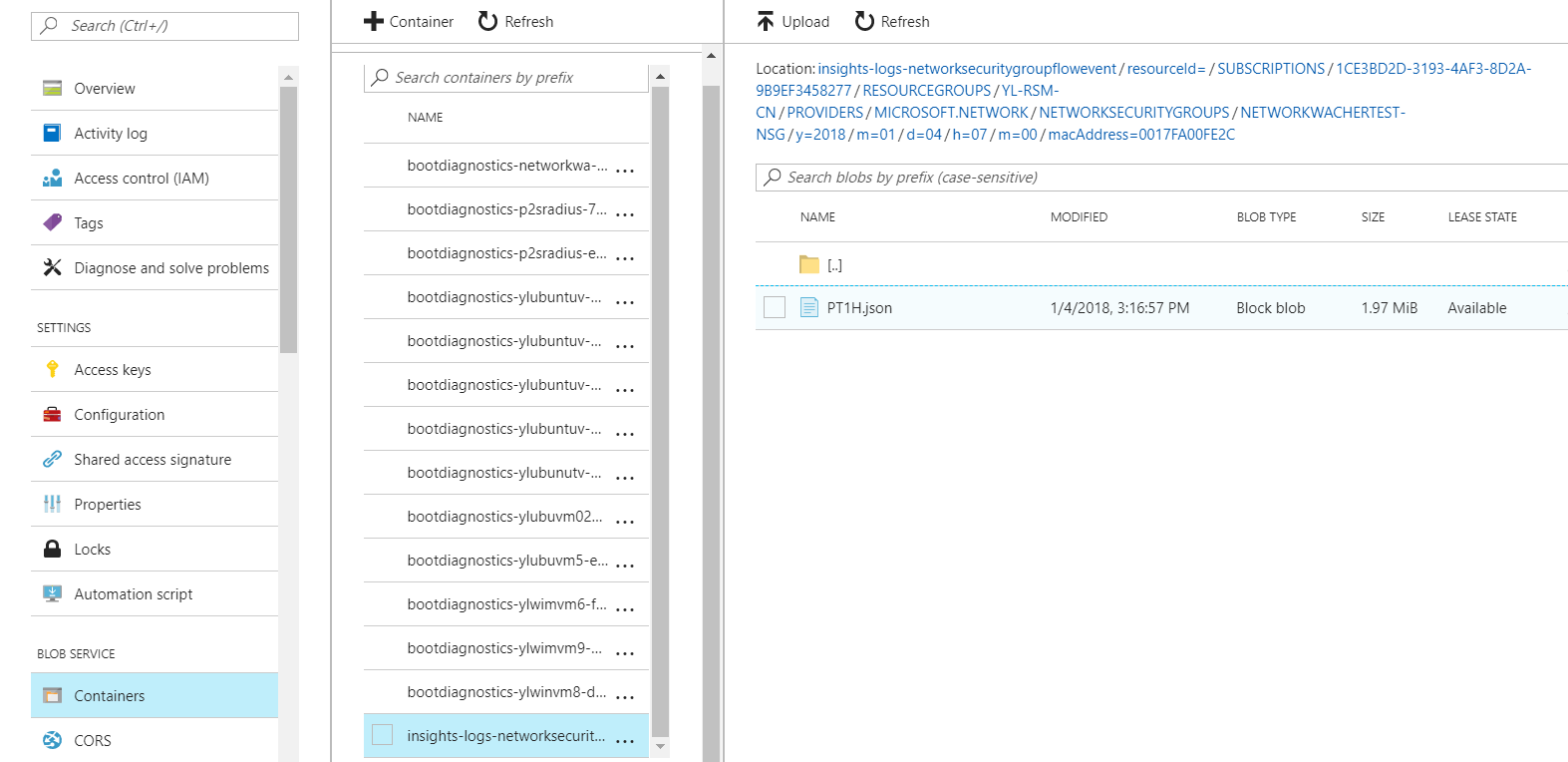
1. 选择需要监控日志的网络安全组（选作）



1. 选择存储账号并开启监控日志服务（选作）

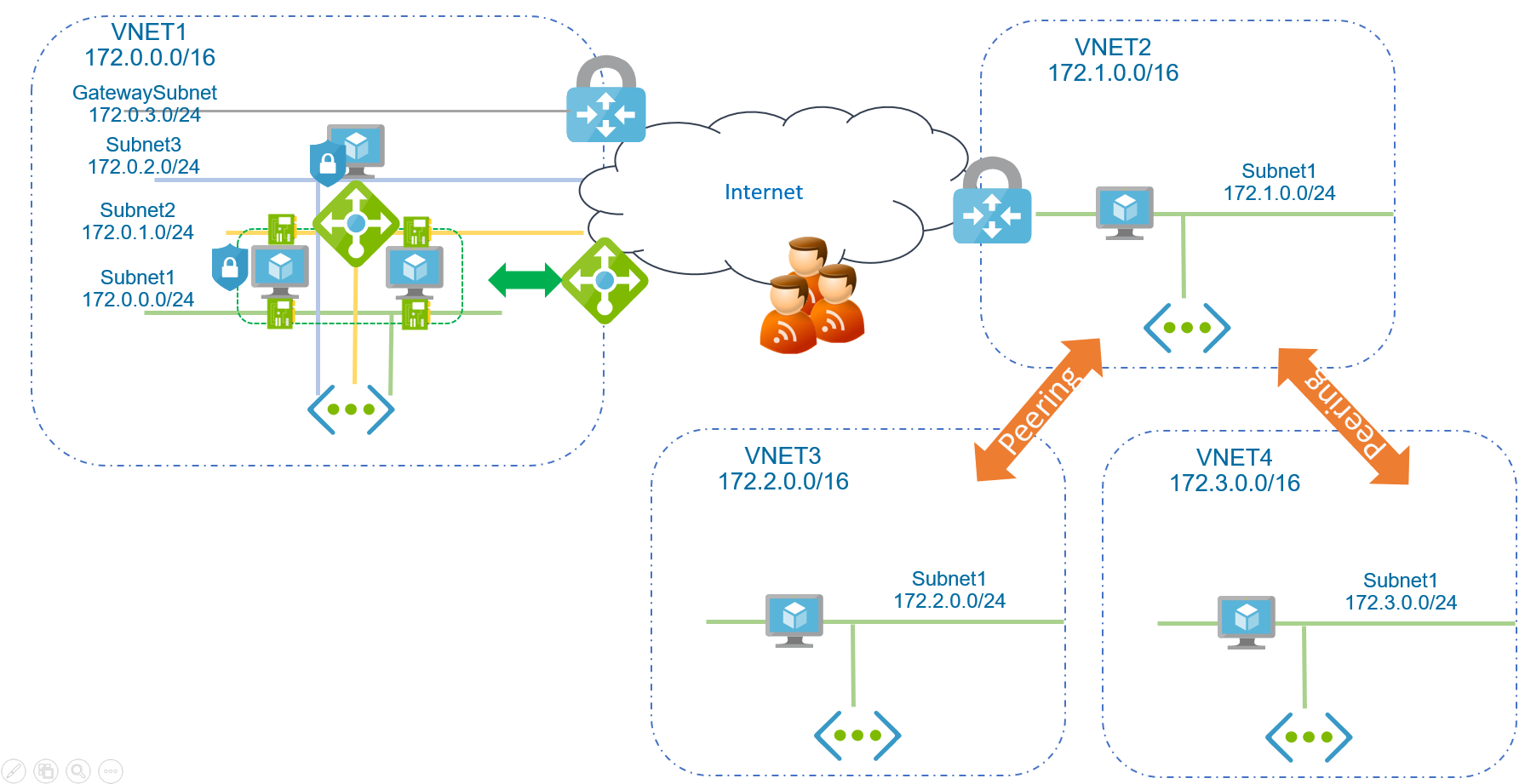


1. 下载日志并使用powerBI读取NSG日志（选作）



<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-visualize-nsg-flow-logs-power-bi>

Exercise 3: AZURE 负载均衡实验

* 1. 实验目标：掌握外网负载均衡
  2. 

1. **虚拟机准备工作**

登陆VM1，安装apache2，php服务

sudo apt-get update

sudo apt-get install apache2 -y

sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql -y

sudo systemctl restart apache2

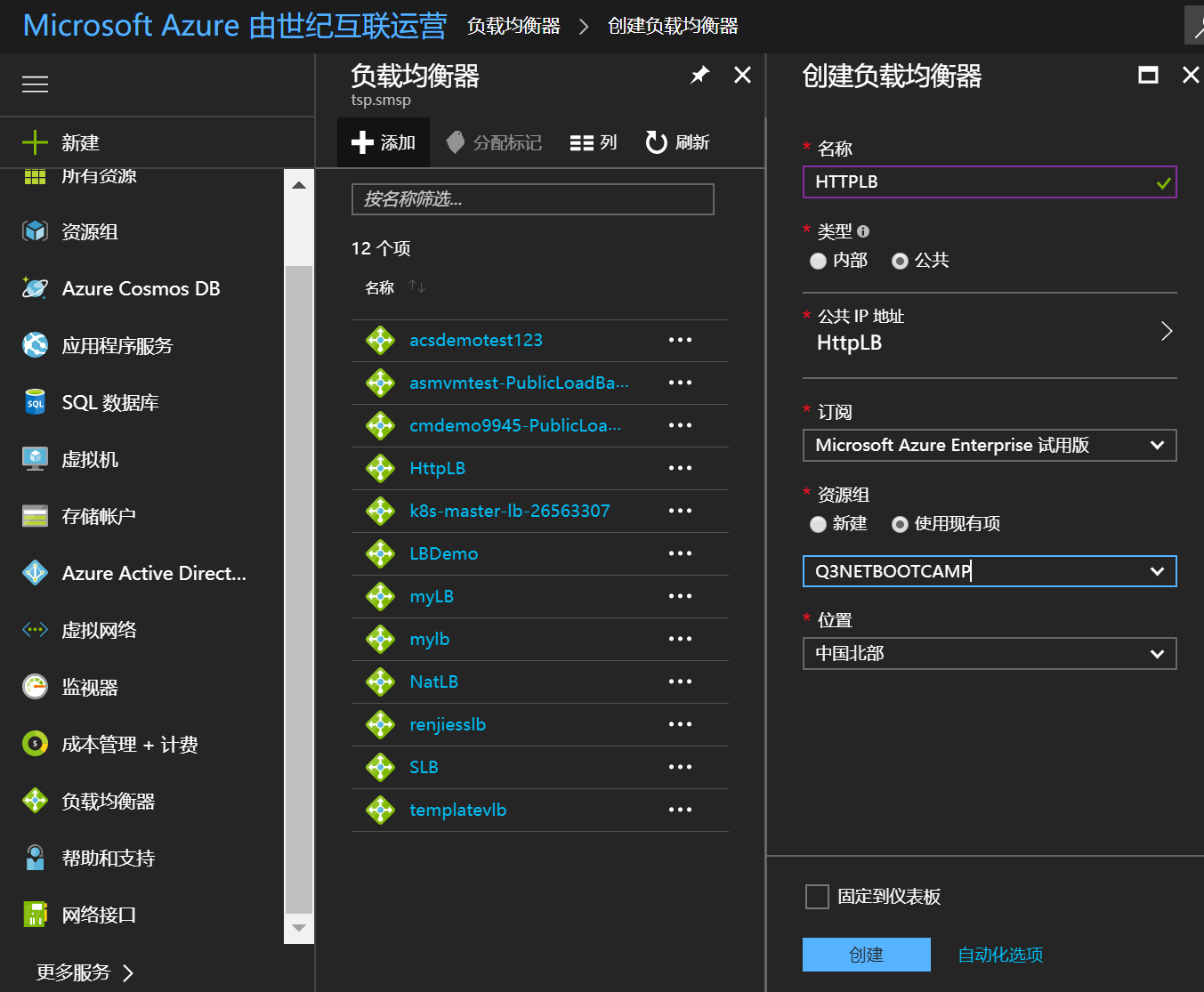
sudo rm /var/www/html/index.html

sudo wget [https://raw.githubusercontent.com/nonokangwei/ TechSummit2018/master/index.php -P /var/www/html/](https://raw.githubusercontent.com/nonokangwei/q3bootcamp/master/index.php%20-P%20/var/www/html/)

在VM2上重复上述操作

1. **创建公网负载均衡**

选择负载均衡，点击添加。名称HTTPLB，类型公共，公网IP地址新建名称HttpLB，资源组tech014，位置East US 2，选择基本类型负载均衡，选择创建。



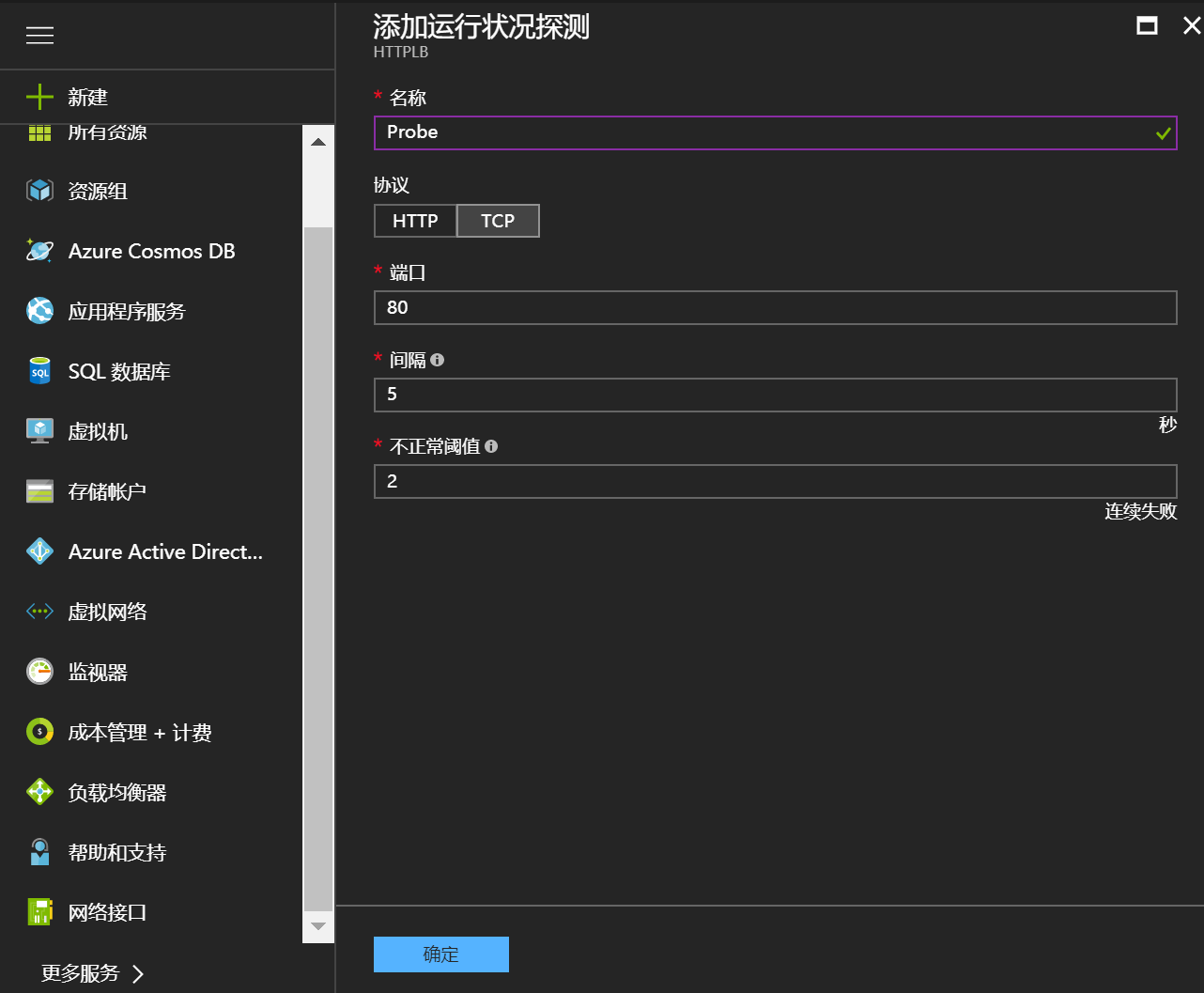
1. **创建负载均衡后端池**

选择前面创建的公网负载均衡HTTPLB，选择后端池，点击添加，名称BackendPool，关联到可用性集，可用性集NATAS，目标网络IP配置-目标虚拟机VM1，网络IP配置VM1nic1，目标虚拟机VM2，网络IP配置VM2nic1。确定创建。

1. **创建运行状况探测**

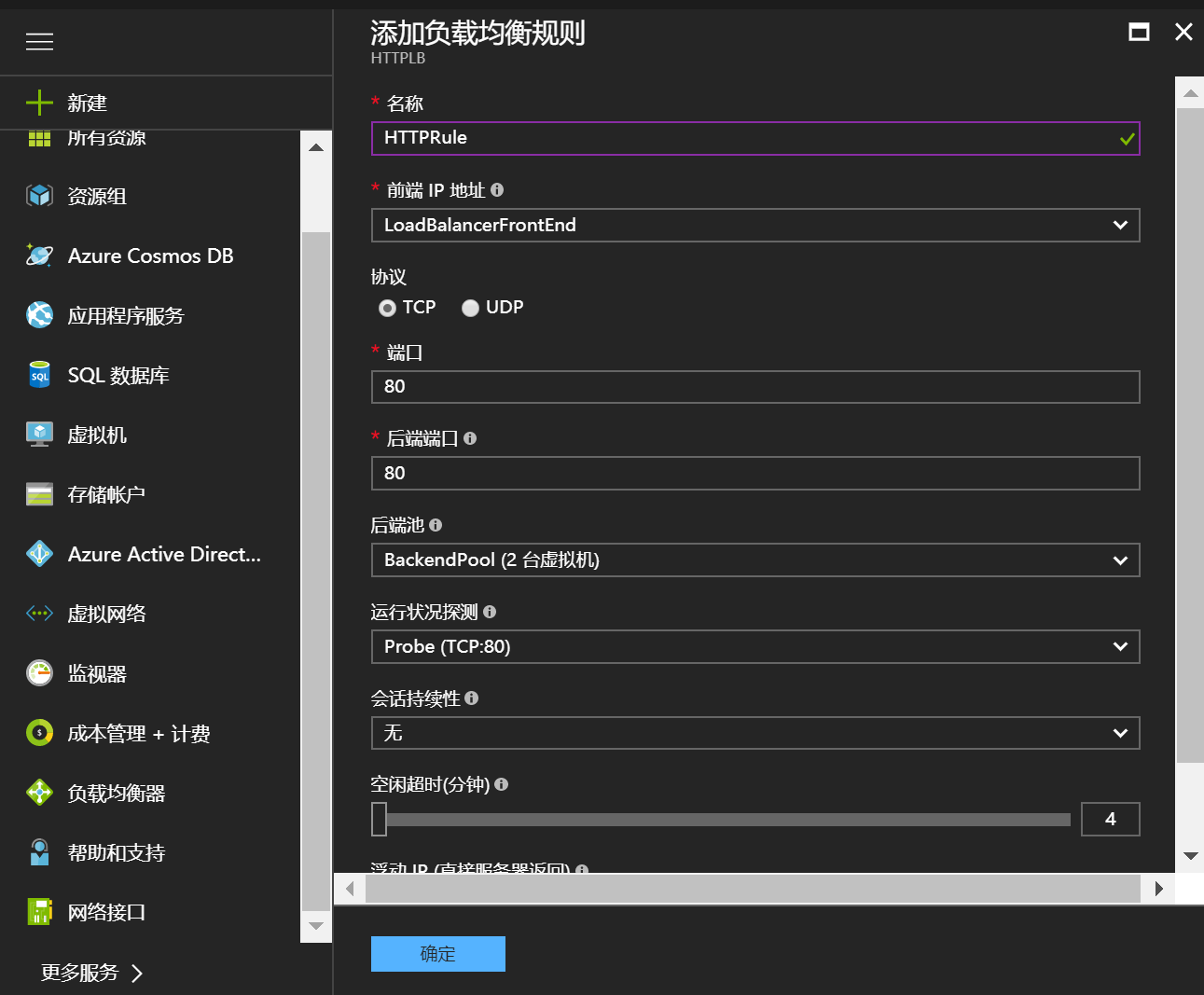
选择运行状况探测，点击添加，名称Probe，协议TCP，端口80，默认间隔和不正常阈值。确定创建。

可以尝试创建基于HTTP协议的Probe，并思考与TCP Probe的区别。



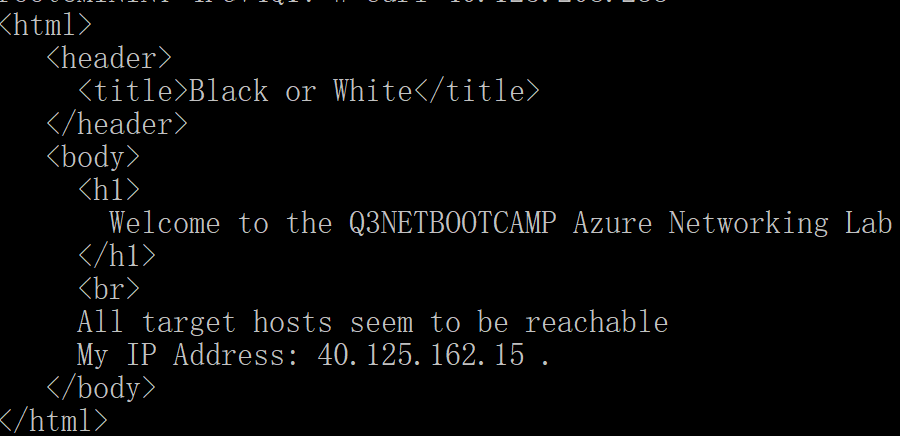
1. **创建负载均衡规则**

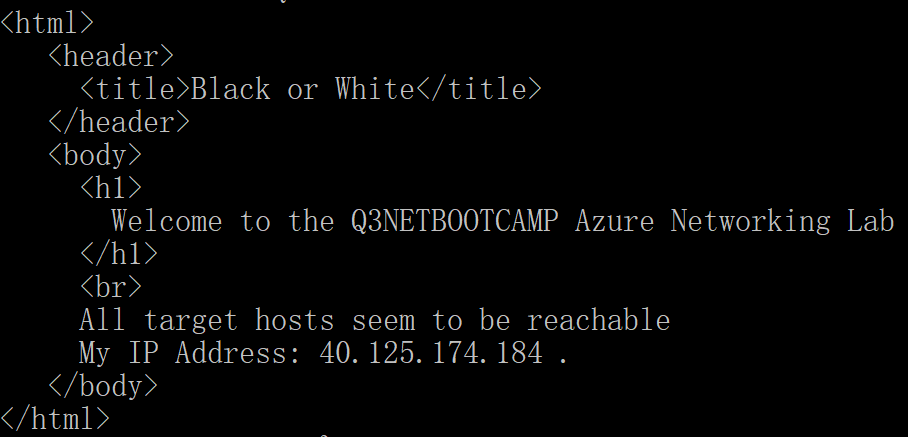
选择负载均衡规则，点击添加，名称HTTPRule，默认前端IP，协议TCP，端口80，后端端口80，其余均为默认。确认创建。



1. **确认负载均衡连通性**

查阅负载均衡公网IP，由本地发起curl 负载均衡公网IP 操作。确认输出中的My IP Address。反复发起curl操作，确认输出地址是否发生变化。





思考输出地址发生变化原因。

1. **会话一致性策略**

选择负载均衡HTTPLB，点击负载均衡规则，选择HTTPRule



更改会话持续性为客户端IP，并保存。



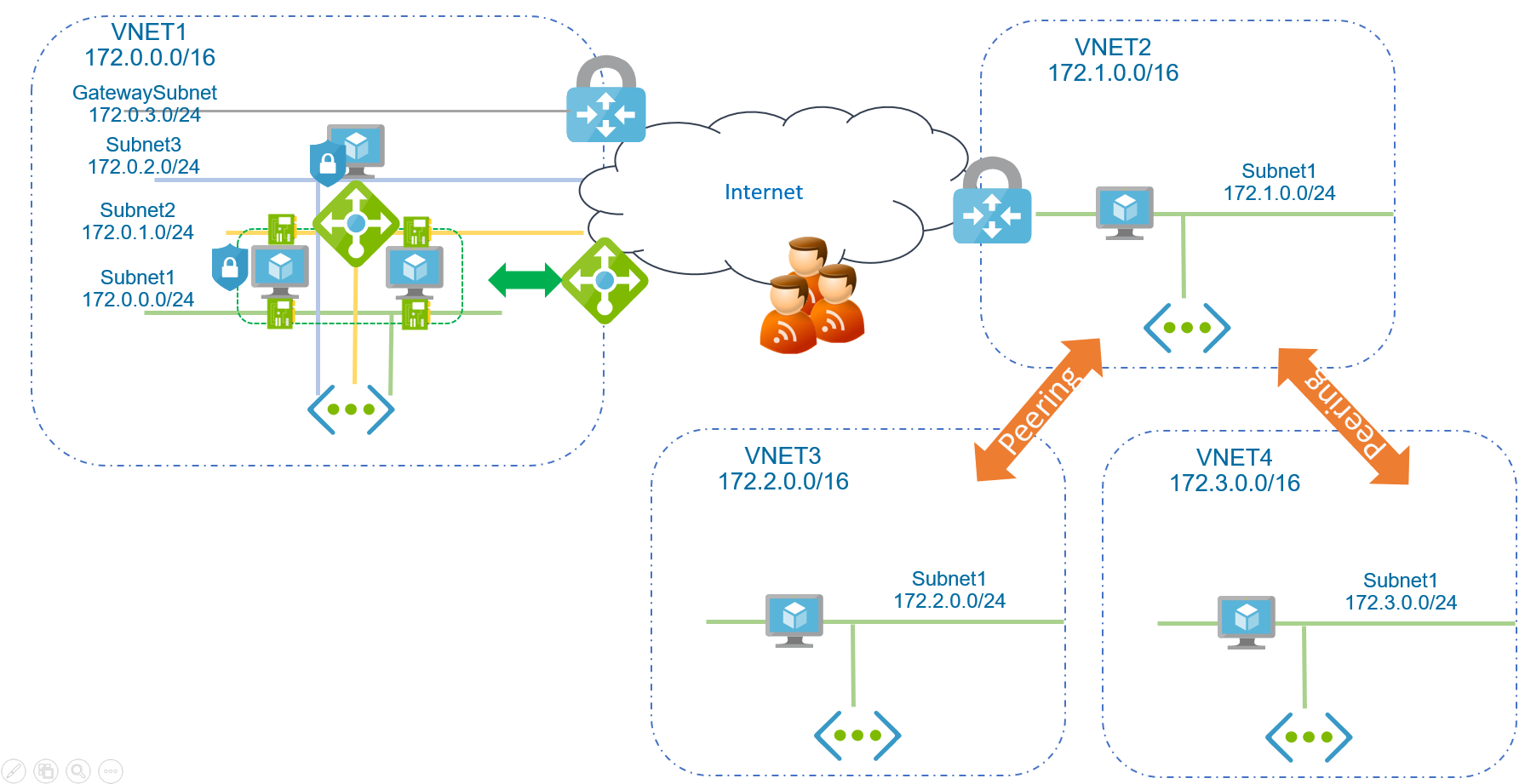
1. **确认会话持续性**

查阅负载均衡公网IP，由本地发起curl 负载均衡公网IP 操作。确认输出中的My IP Address。反复发起curl操作，确认输出地址是否发生变化。思考地址不变的原因。

思考不同应用对于负载均衡算法的要求。

Exercise 4: AZURE NAT实验（选做）

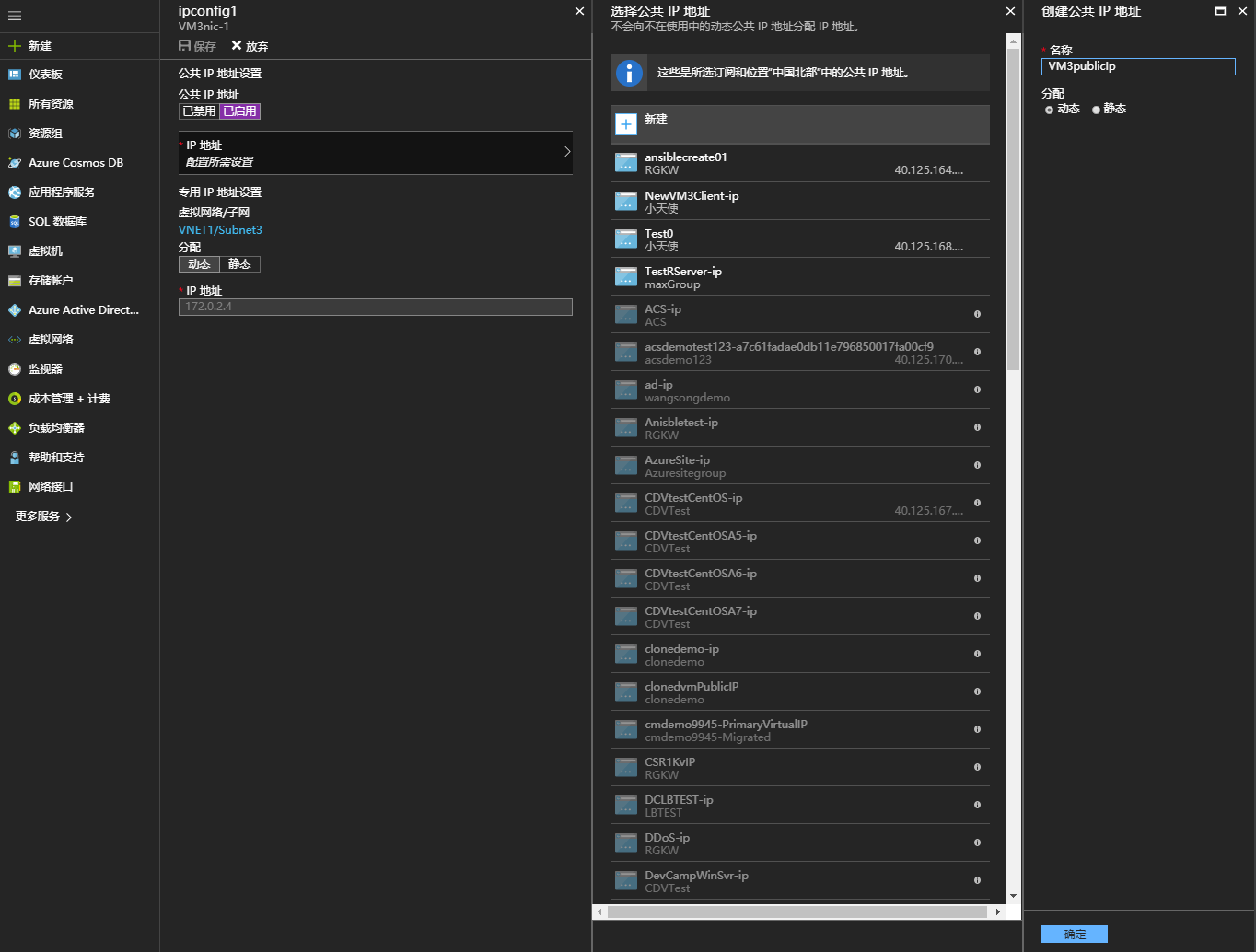
* 1. 实验目标：掌握VNET外网访问NAT策略，掌握端口转发策略。



1. **验证具有公网IP地址VM外网访问地址**

为VM3增加公网IP，远程登陆VM3，通过命令nslookup myip.opendns.com resolver1.opendns.com 确认外网访问所用公网IP地址。比对输出结果与该虚拟机AZURE所分配公网IP地址关系。

VM3增加公网IP方法：选择VM3，点击网络，选择网络接口VM3nic-1，选择IP配置，选择ipconfig1，将公网IP改为已启用，公共IP地址选择新建，名称VM3publicIp



1. **验证不具有公网IP地址VM外网访问地址**

依据上一步的反向操作删除VM3的公网地址。通过VM1或VM2作为跳板机，登陆VM3，通过命令nslookup myip.opendns.com resolver1.opendns.com 确认外网访问所用公网IP地址。比对输出结果与该虚拟机AZURE所分配公网IP地址关系。

1. **验证具有公网IP的负载均衡后端主机外网访问地址**

远程登陆VM1或VM2，通过命令nslookup myip.opendns.com resolver1.opendns.com 确认外网访问所用公网IP地址。比对输出结果与该虚拟机AZURE所分配公网IP地址关系以及与该虚拟机所关联负载均衡公网地址关系。

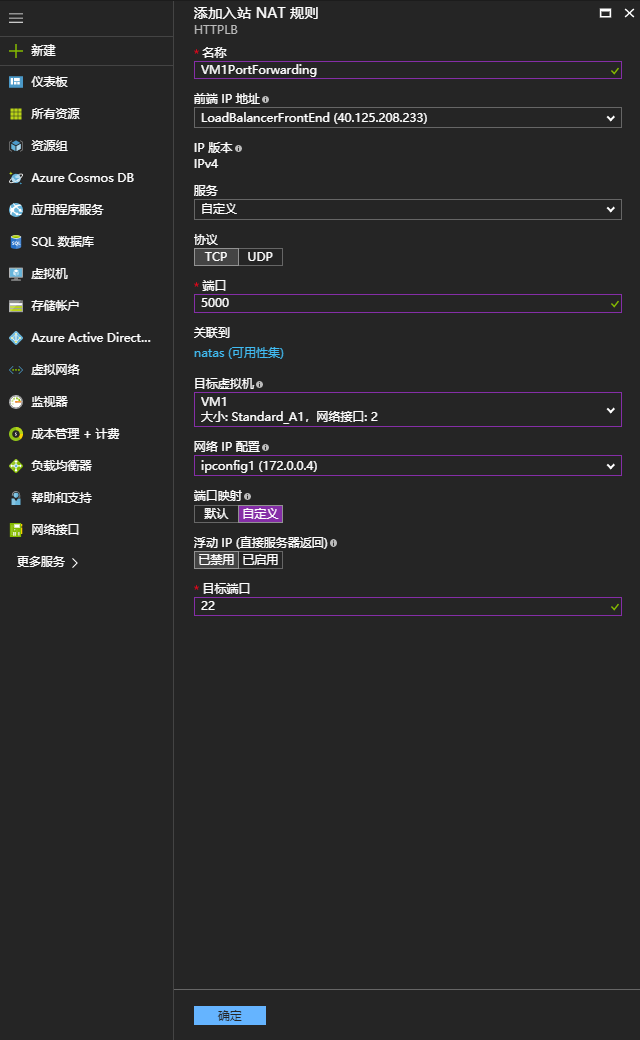
1. **验证不具有公网IP的负载均衡后端主机外网访问地址**

依据步骤一的反向操作关闭VM1的公网地址。通过VM2作为跳板机，登陆VM1，通过命令nslookup myip.opendns.com resolver1.opendns.com 确认外网访问所用公网IP地址。比对输出结果与该虚拟机所关联负载均衡公网地址关系。

1. **入向NAT端口转发规则**

依据步骤一的反向操作关闭VM2的公网地址，此时VM1和VM2均无公网地址。思考此时如何进行主机的远程登陆。

选择实验三创建的负载均衡HTTPLB，点击入站NAT规则，选择添加，名称VM1PortForwarding，前端IP地址默认，服务自定义，协议TCP，端口5000，目标主机VM1，网络IP配置VM1nic-1，端口映射自定义，目标端口22。同样操作添加名称VM2PortForwarding，前端IP地址默认，服务自定义，协议TCP，端口5001，目标主机VM2，网络IP配置VM2nic-1，端口映射自定义，目标端口22。

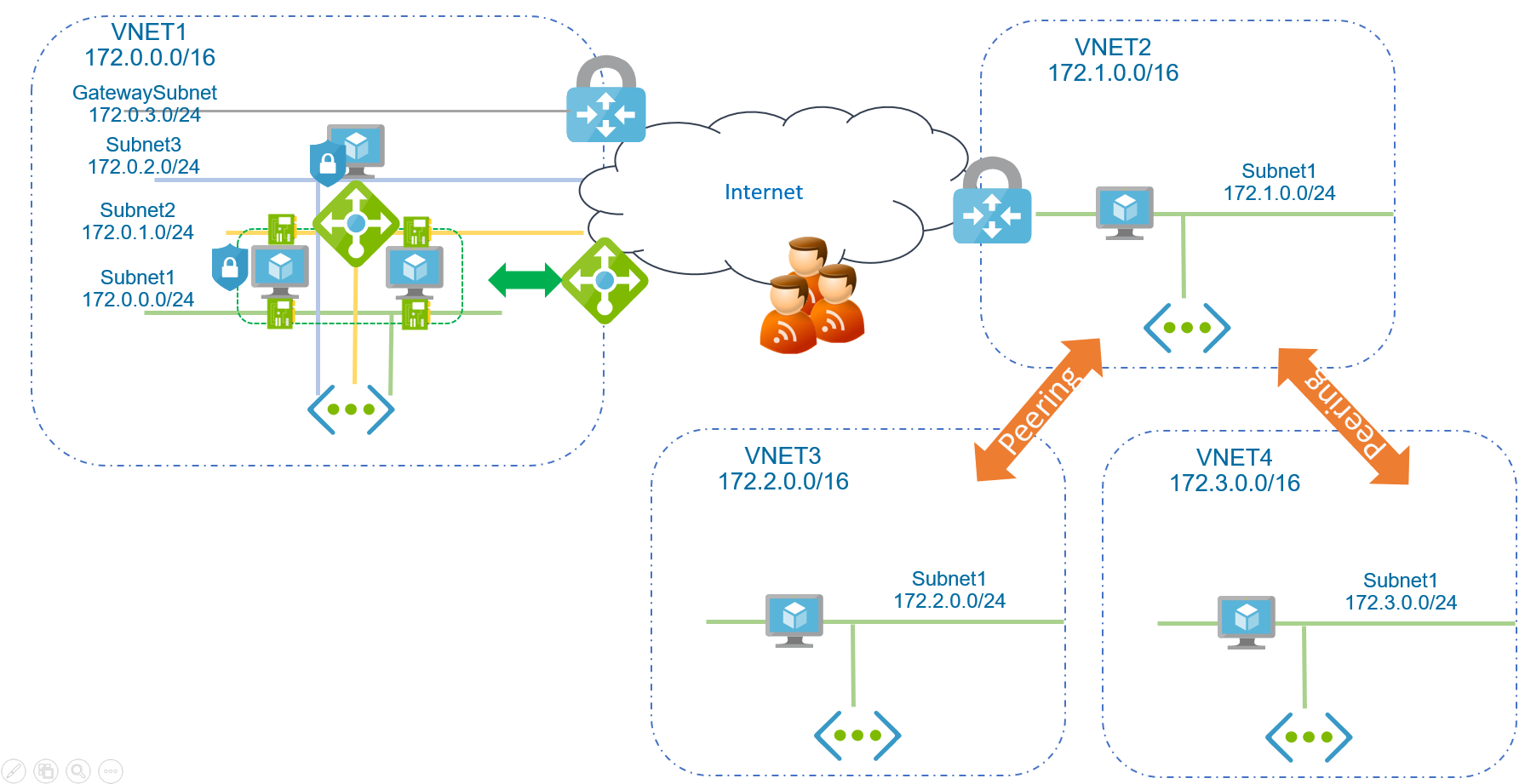


通过本地验证远程连接，获取HTTPLB负载均衡的公网IP地址，ssh 用户名@HTTPLB公网IP -p 入站NAT规则端口号。通过变换入站NAT规则端口号确认可以成功登陆VM1和VM2。

1. **思考如果VNET内有多个可用集主机需要通过统一公网IP端口转发方式进行远程登陆如何实现。**
2. **思考VNET所有主机希望通过固定公网IP访问外网及AZURE外部服务如何实现（可参阅实验七的架构）**

Exercise 5: AZURE VPN网关实验

实验目标：建立VNET1和VNET2之间的VPN互联连接，打通VNET1和VNET2虚拟子网



1. **创建网关子网**

选择VNET1虚拟网络，选择子网，选择添加网关子网



地址范围172.0.3.0/24，路由表无，服务终结点选中0个，确定创建。



1. **创建VNET2及相关子网**

选择虚拟网络，点击添加，名称VNET2，地址空间172.1.0.0/16，资源组tech014，位置选择West US 2，子网名称Subnet1，地址范围172.1.0.0/24，确定创建



选择VNET2，点击子网，选择添加网关子网，地址范围172.1.1.0/24，路由表无，服务终结点选中0个，确定创建。

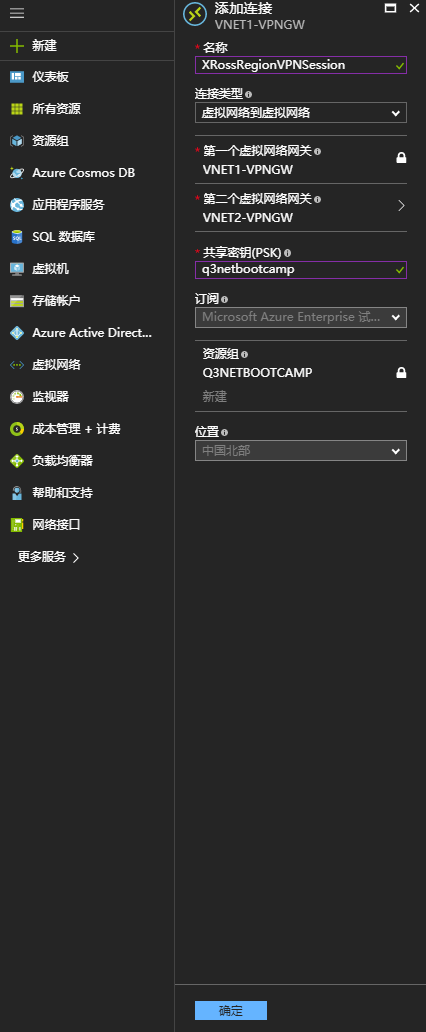


1. **配置VNET1下VPN配置**

选择虚拟网络网关，点击添加，名称VNET1-VPNGW，网关类型VPN，VPN类型基于路由的，SKU VpnGw1，虚拟网络VNET1，第一个IP配置新建名称VNET1-VPNGW，位置East US 2，确认创建。（此过程大概在30-45分钟，创建过程中可先跳至下一步进行操作）



选择虚拟网关VNET1-VPNGW，点击连接，选择添加。名称XRossRegionVPNSession，连接类型虚拟网络到虚拟网络，第一个虚拟网络网关VNET1-VPNGW，第二个虚拟网络网关VNET2-VPNGW，共享密钥techsummit2018，确认创建。



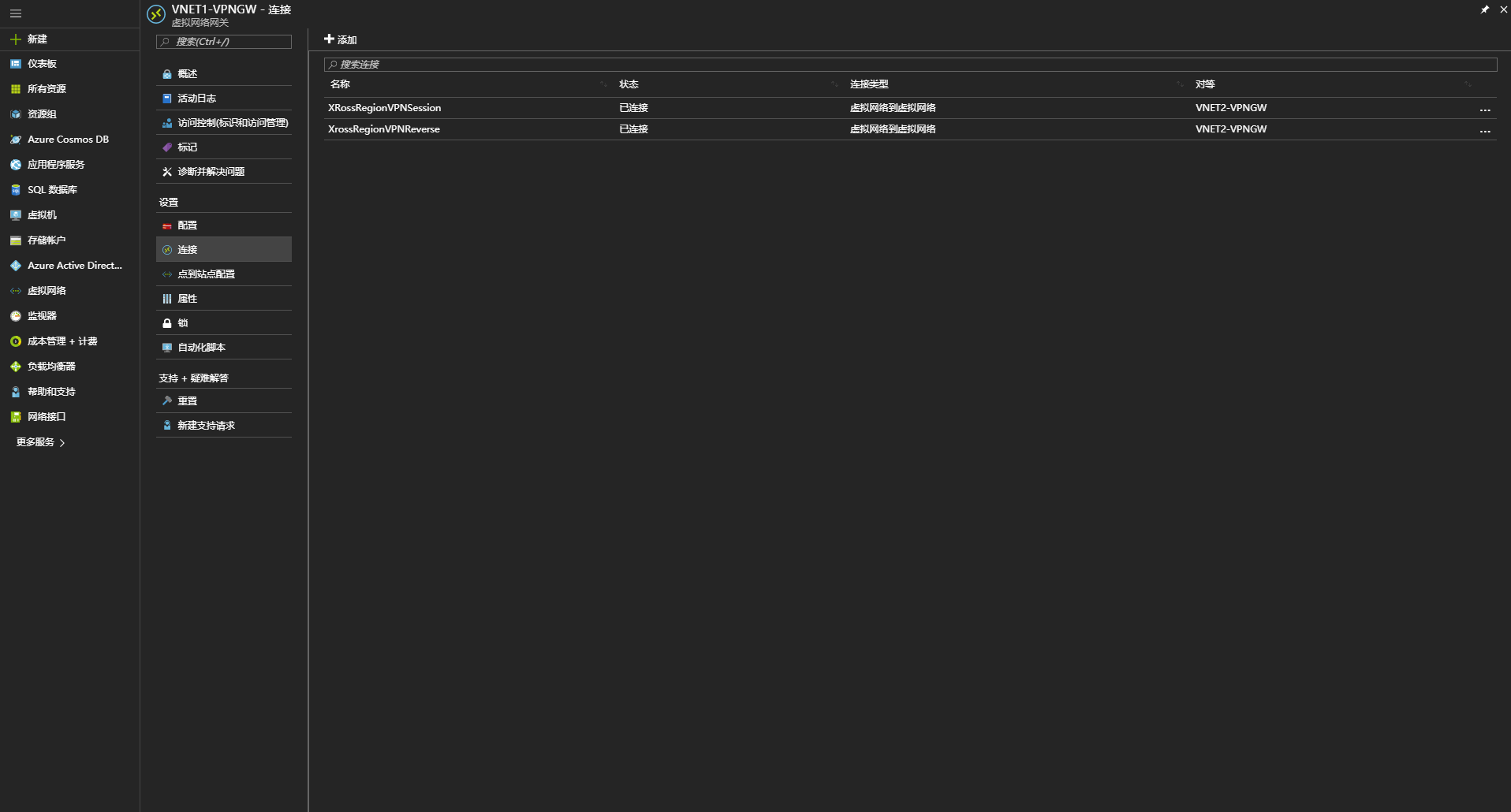
1. **配置VNET2下VPN配置**

选择虚拟网络网关，点击添加，名称VNET2-VPNGW，网关类型VPN，VPN类型基于路由的，SKU VpnGw1，虚拟网络VNET2，第一个IP配置新建名称VNET2-VPNGW，位置中国东部，确认创建。

选择虚拟网关VNET2-VPNGW，点击连接，选择添加。名称XRossRegionVPNReverse，连接类型虚拟网络到虚拟网络，第一个虚拟网络网关VNET2-VPNGW，第二个虚拟网络网关VNET1-VPNGW，共享密钥techsummit2018，确认创建。

1. **检查VPN连接状态**

选择虚拟网关VNET1-VPNGW，选择连接，查看XrossRegionVPNSession和XrossRegionVPNReverse状态为已连接状态。



1. **VNET2内创建VM4**

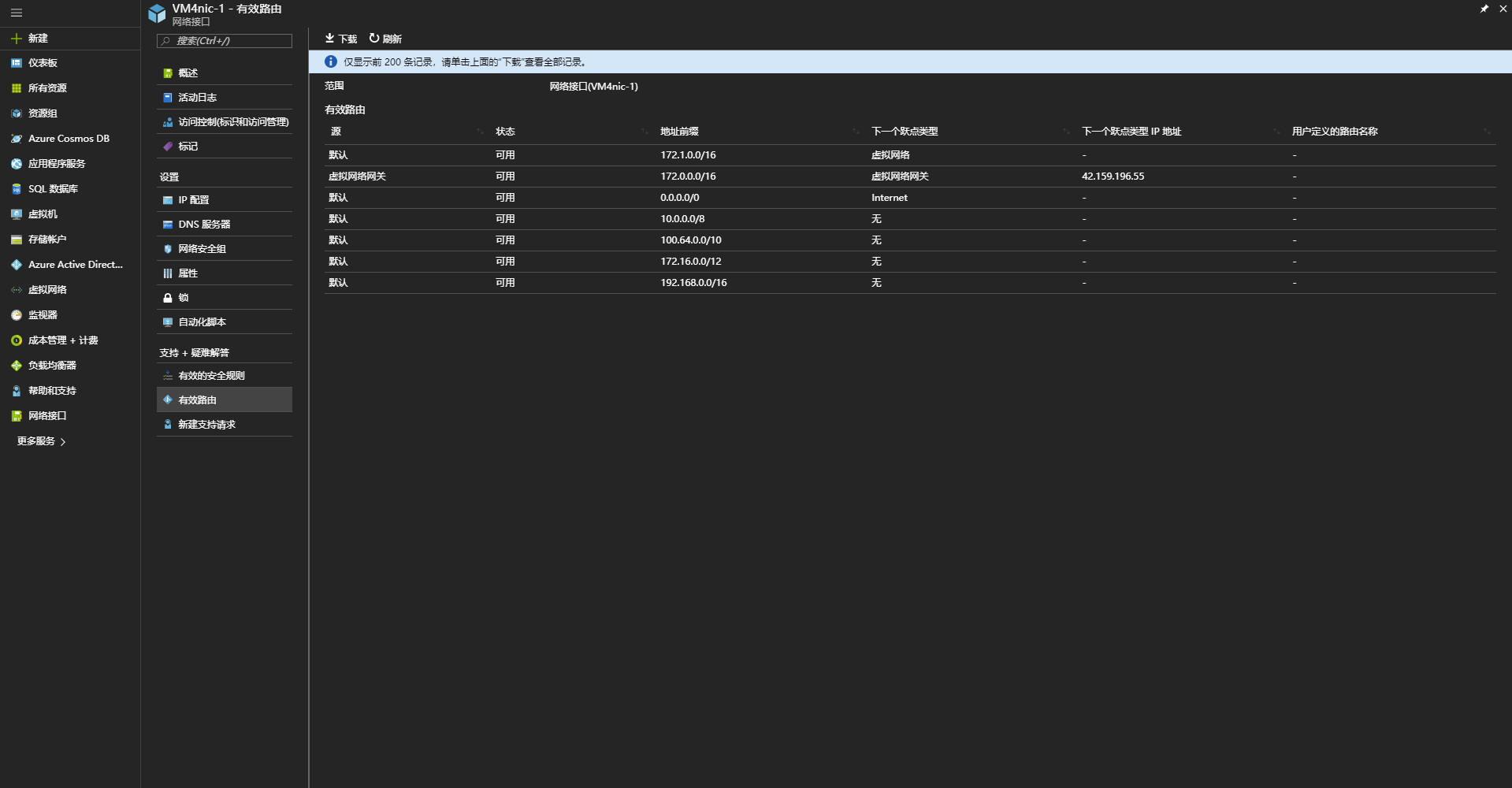
访问<https://github.com/nonokangwei/TechSummit2018/blob/master/VM4.json>拷贝VM4虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称VM4，选择资源组（选择之前VNET1所在资源组）。

上述操作也可通过CLI完成：

az group deployment create --template-uri https://raw.githubusercontent.com/nonokangwei/TechSummit2018/master/VM4.json --parameters adminUsername=username adminPassword=password virtualMachineName=VMname -g resourcegroup

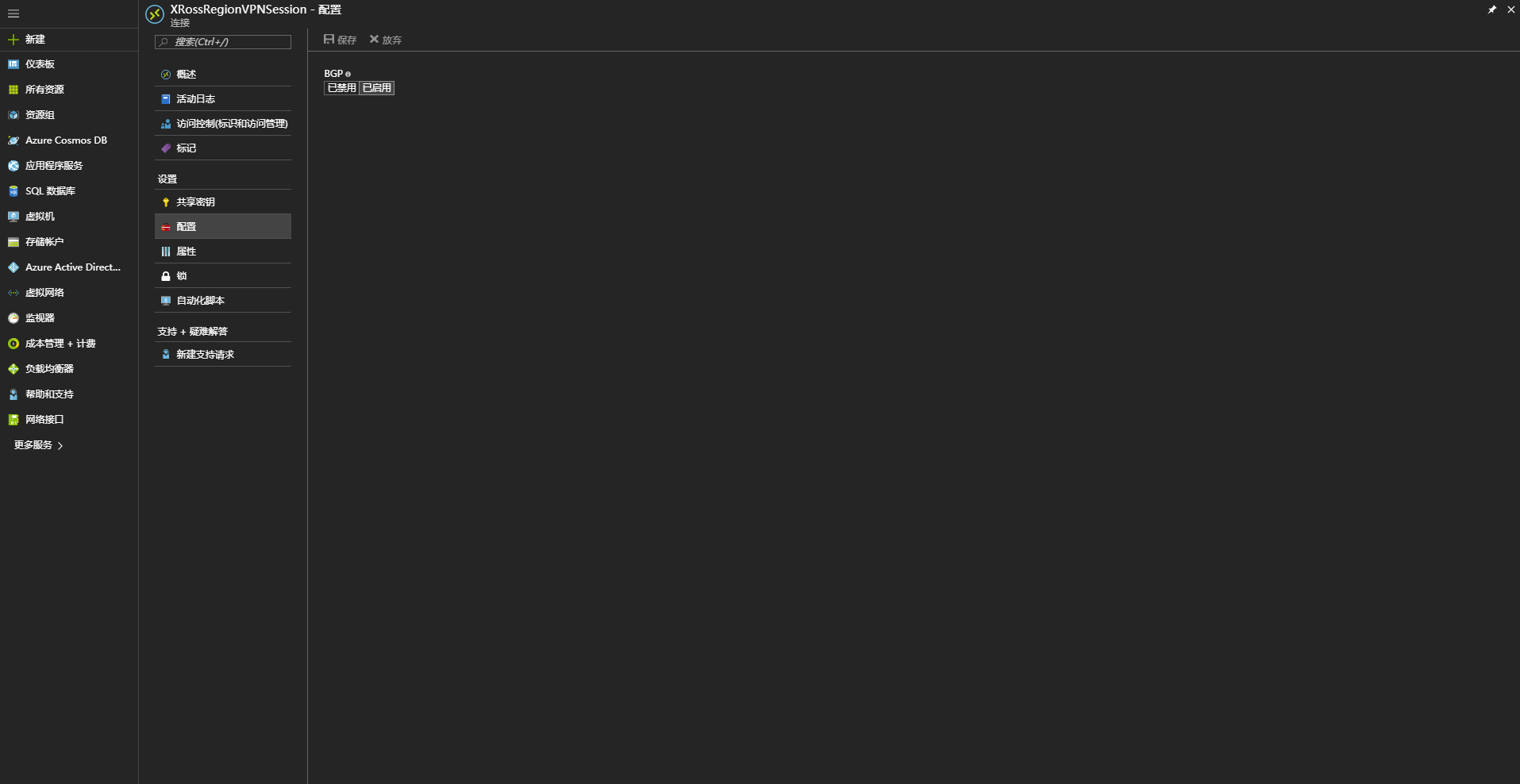
1. **验证VNET1和VNET2内虚拟机的连通性**

远程登陆VM4，ping 172.0.0.4（VM1的VNET1私网地址），验证互通性。Portal选择VM4，选择网络，选择网络接口VM4nic-1，选择有效路由，查看路由表，思考VPN连接对路由表的影响。

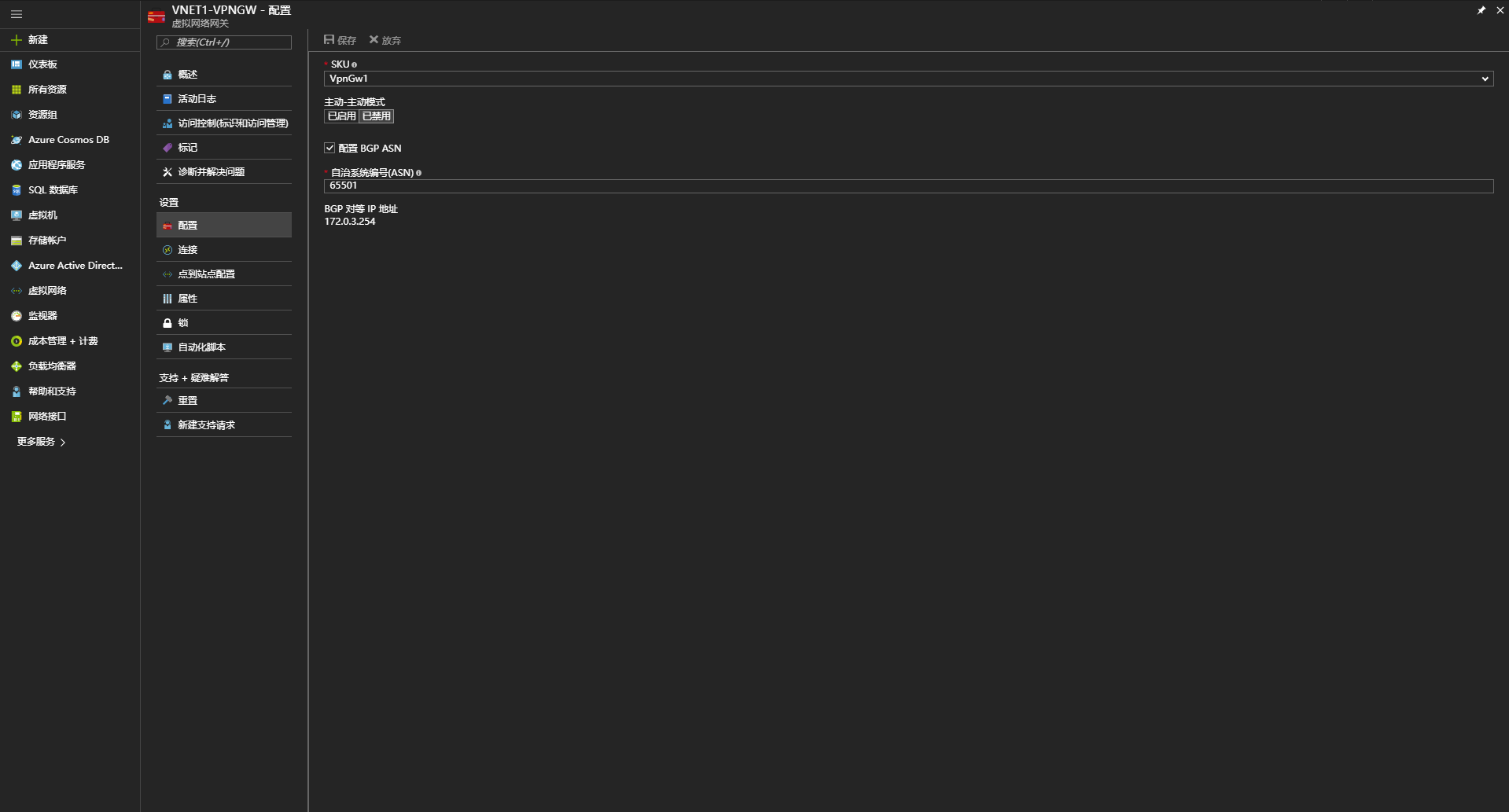


1. **配置BGP**

选择连接XrossRegionVPNSession，选择配置，设置BPG已启用，保存。

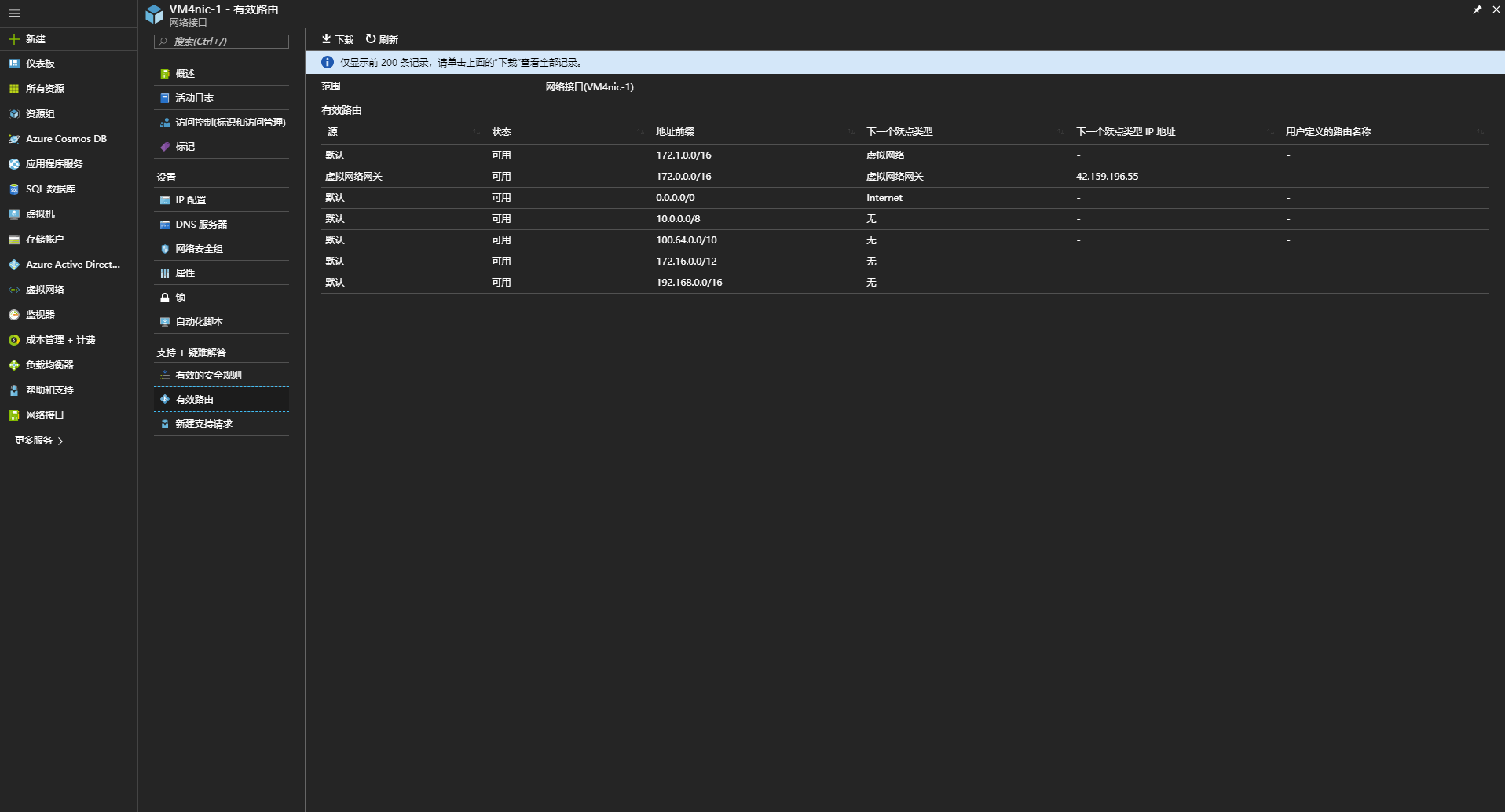


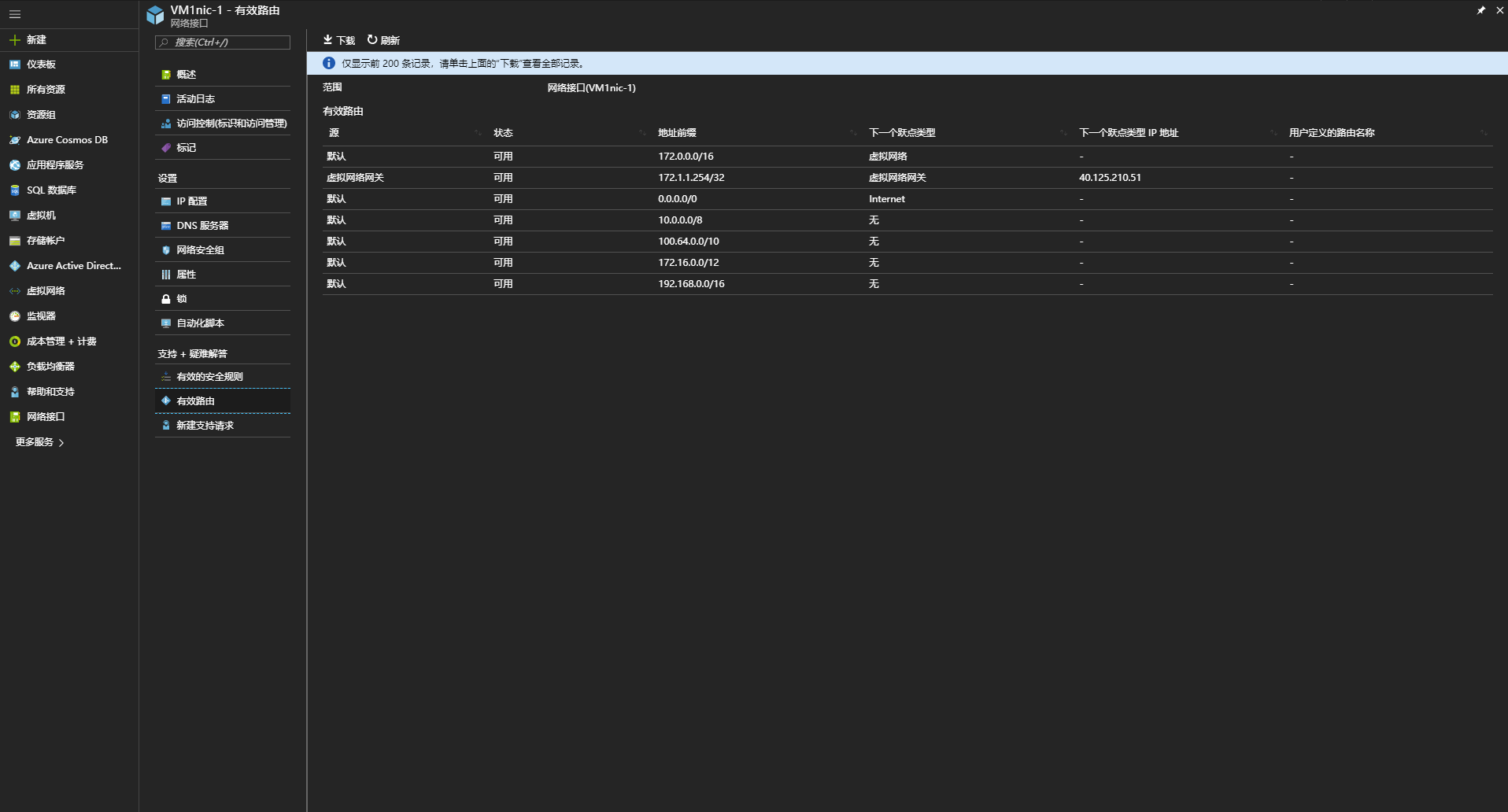
选择虚拟网关VNET1-VPNGW，选择配置，勾选配置BGP ASN，自治系统AS号65501，保存。并记录下BGP 对端IP地址。



1. **验证VNET1和VNET2内网联通性**

远程登陆VM4，ping 172.0.0.4（VM1的VNET1私网地址），验证互通性。Portal选择VM4，选择网络，选择网络接口VM4nic-1，选择有效路由，查看路由表。Portal选择VM1，选择网络，选择网络接口VM1nic-1，选择有效路由，查看路由表，思考单边打开BGP后VPN连接对路由表的影响。





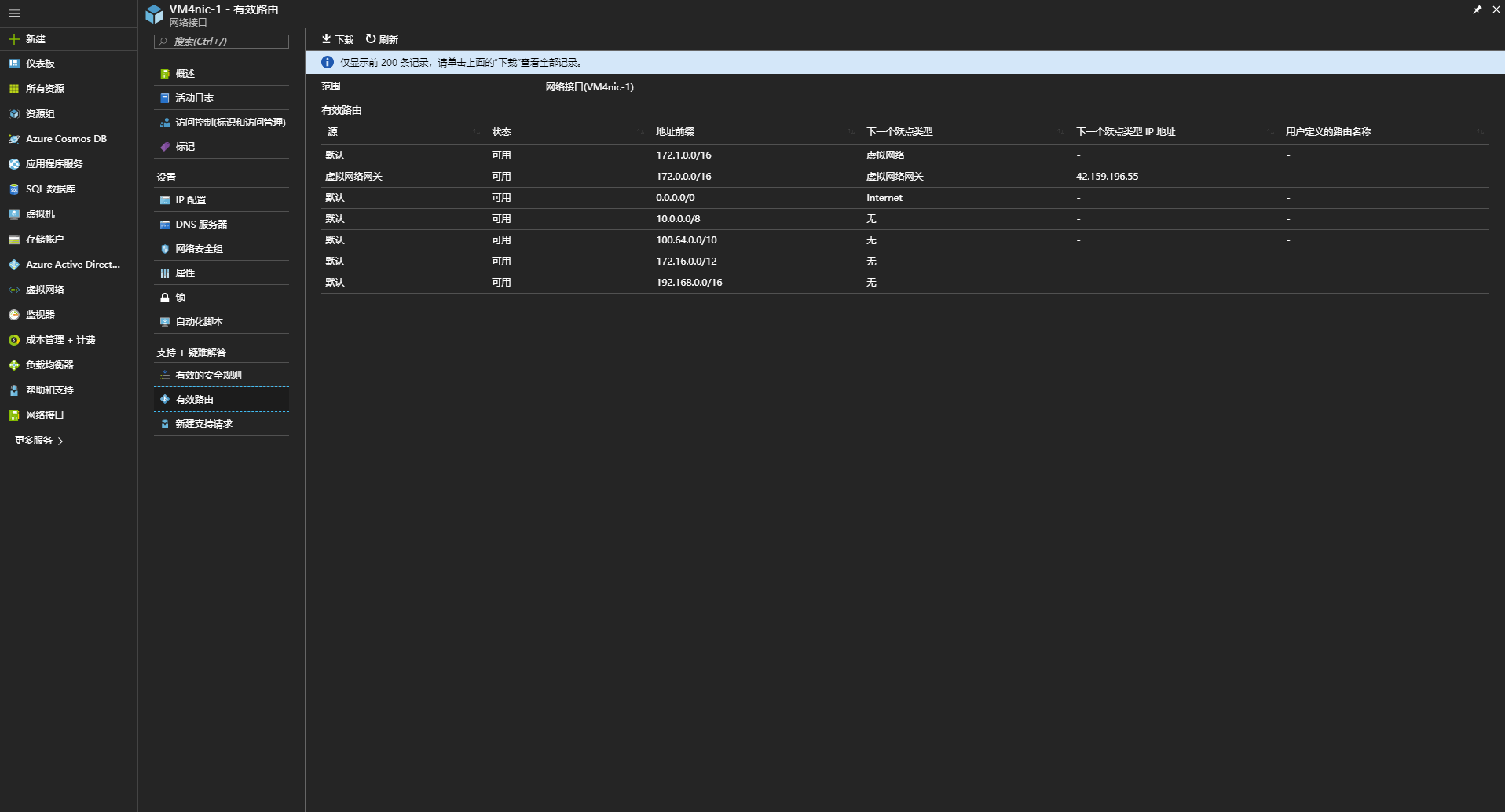
1. **配置BGP**

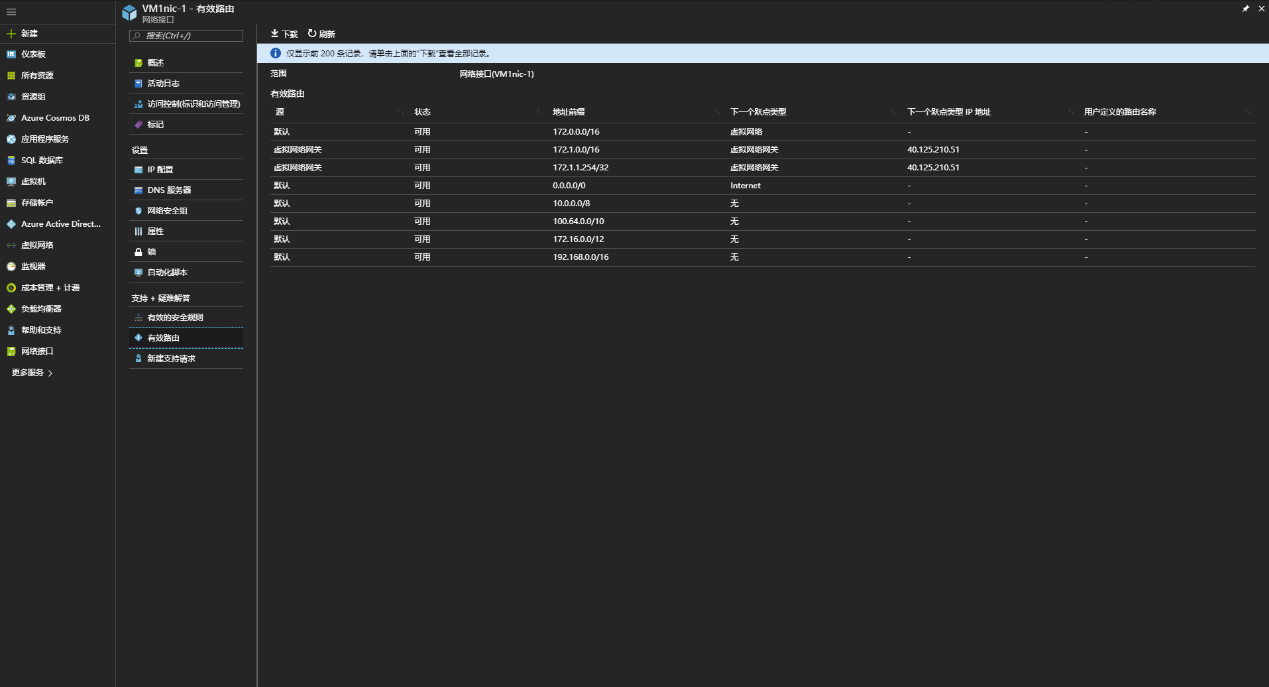
选择连接XrossRegionVPNReverse，选择配置，设置BPG已启用，保存。

选择虚拟网关VNET2-VPNGW，选择配置，勾选配置BGP ASN，自治系统AS号65502，保存。

1. **验证VNET1和VNET2内虚拟机的连通性**

远程登陆VM4，ping 172.0.0.4（VM1的VNET1私网地址），验证互通性。Portal选择VM4，选择网络，选择网络接口VM4nic-1，选择有效路由，查看路由表。Portal选择VM1，选择网络，选择网络接口VM1nic-1，选择有效路由，查看路由表。对比VM1nic-1有效路由表的变化。





1. **模拟与第三方设备建立VPN连接（选做）**

创建Local Network Gateway，在VNET1中创建LocalGW1用于模拟VNET2中网络信息，“IP address”为VNET2-VPNGW的公网IP地址，”Address Space“为VNET2的网络地址空间。如果需要配置BGP信息，ASN和peer address为VNET2-VPNGW的BGP信息。

在VNET2中按照同样方式创建LobalGW2用于模拟VNET1中的网络信息。

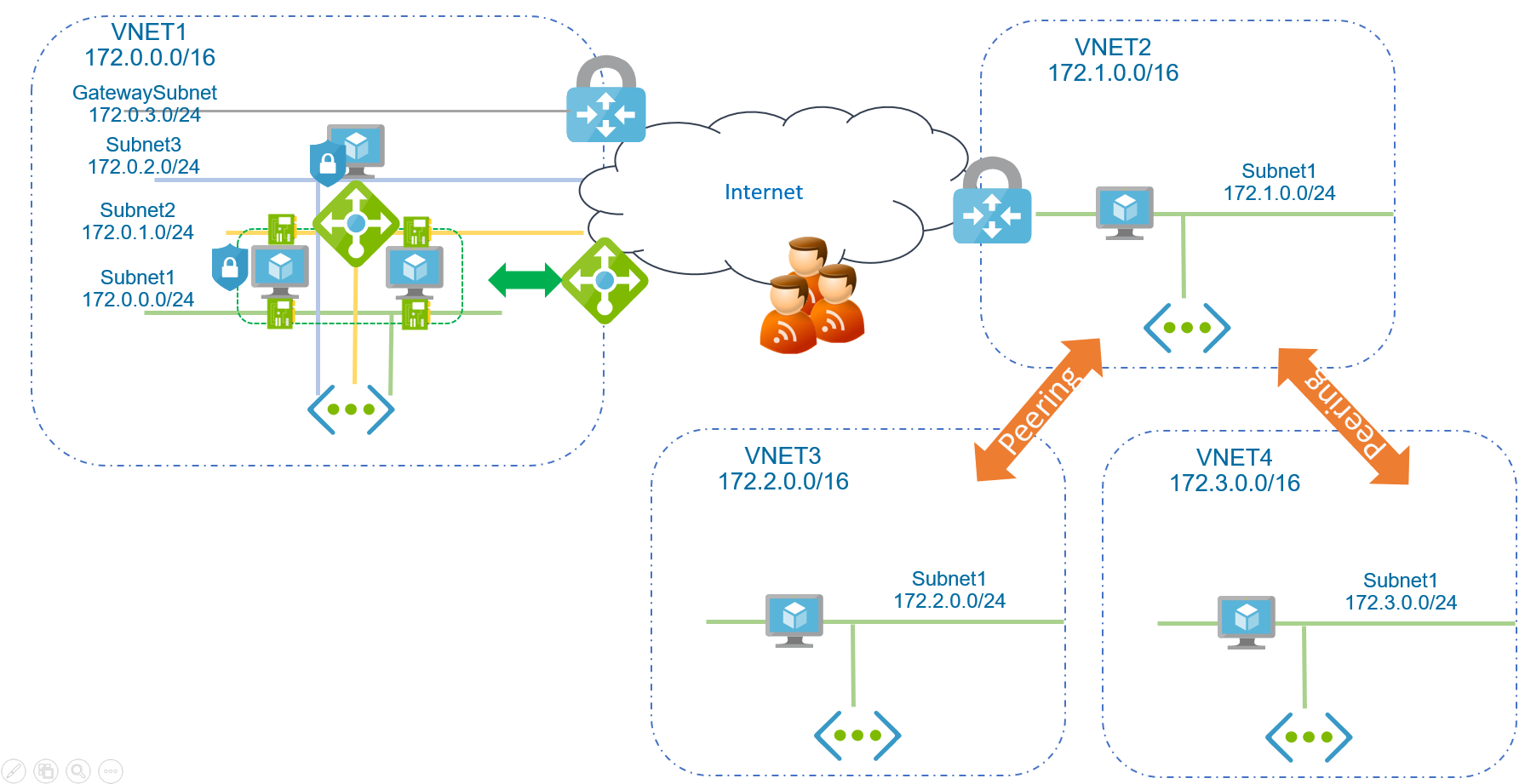
VNET1-VPNGW，删除VPN连接XrossRegionVPNReverse，创建Site-to-Site（IPSec）VPN，选择本地LocalGW1创建VPN连接，共享密钥techsummit2018。

VNET2-VPNGW按照同样方式创建。

Exercise 6: AZURE 对等互联实验

实验目标：

* 通过VNET Peering打通VNET2和VNET3
* 通过Transit GW打通VNET3和VNET1
* 通过NVA方式实现Transit Peering打通VNET3和VNET4



1. **创建VNET3**

选择虚拟网络，点击添加，名称VNET3，地址空间172.2.0.0/16，资源组tech014，位置选择West US 2，子网名称Subnet1，地址范围172.2.0.0/24，确定创建



1. **在VNET3中创建VM5**

访问<https://github.com/nonokangwei/TechSummit2018/blob/master/VM5.json>拷贝VM5虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称VM5，选择资源组（选择之前VNET1所在资源组）。

上述操作也可通过CLI完成：

az group deployment create --template-uri https://raw.githubusercontent.com/nonokangwei/TechSummit2018/master/VM5.json --parameters adminUsername=username adminPassword=password virtualMachineName=VMname -g resourcegroup

1. **配置VNET2和VNET3 Peering**

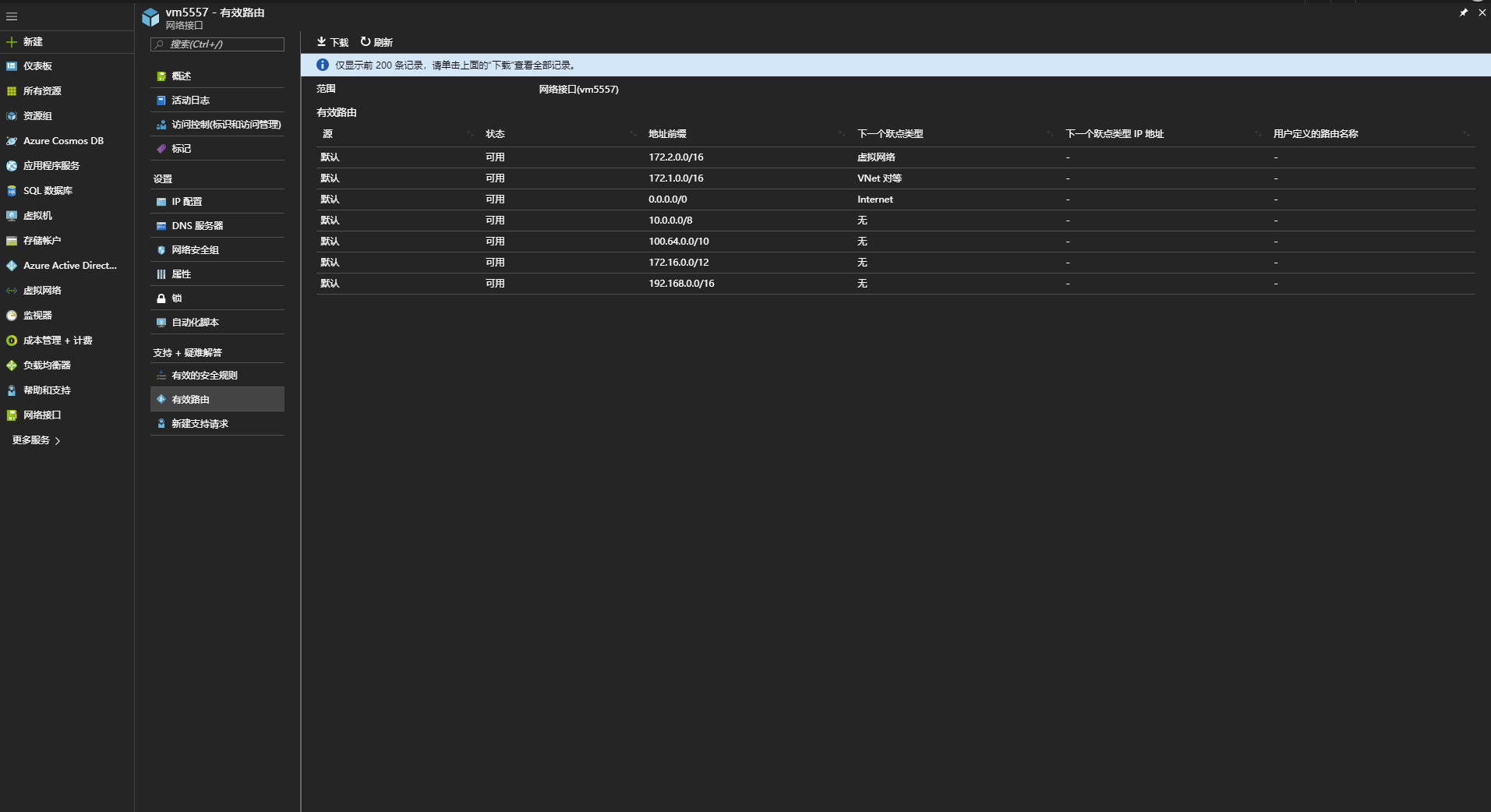
选择VNET2，选择对等，点击添加，名称VNET2VNET3，虚拟网络选择VNET3。



选择VNET3，选择对等，点击添加，名称VNET3VNET2，虚拟网络选择VNET2。

1. **验证VNET2和VNET3连通性。**

登陆VM5，ping 172.1.0.4 (VM4 VNET2内网地址)，检查连通性。查看VM5有效路由，选择VM5，选择网络，选择VM5nic-1，选择有效路由。思考Peering配置对路由表的影响



1. **验证VNET3和VNET1的连通性**

登陆VM5，ping 172.0.0.4 (VM1 VNET1内网地址)，检查连通性。思考为何无法实现互通。

1. **配置Transit Gateway**

选择VNET2，选择对等，选择VNET2VNET3，勾选允许网关传输，保存。

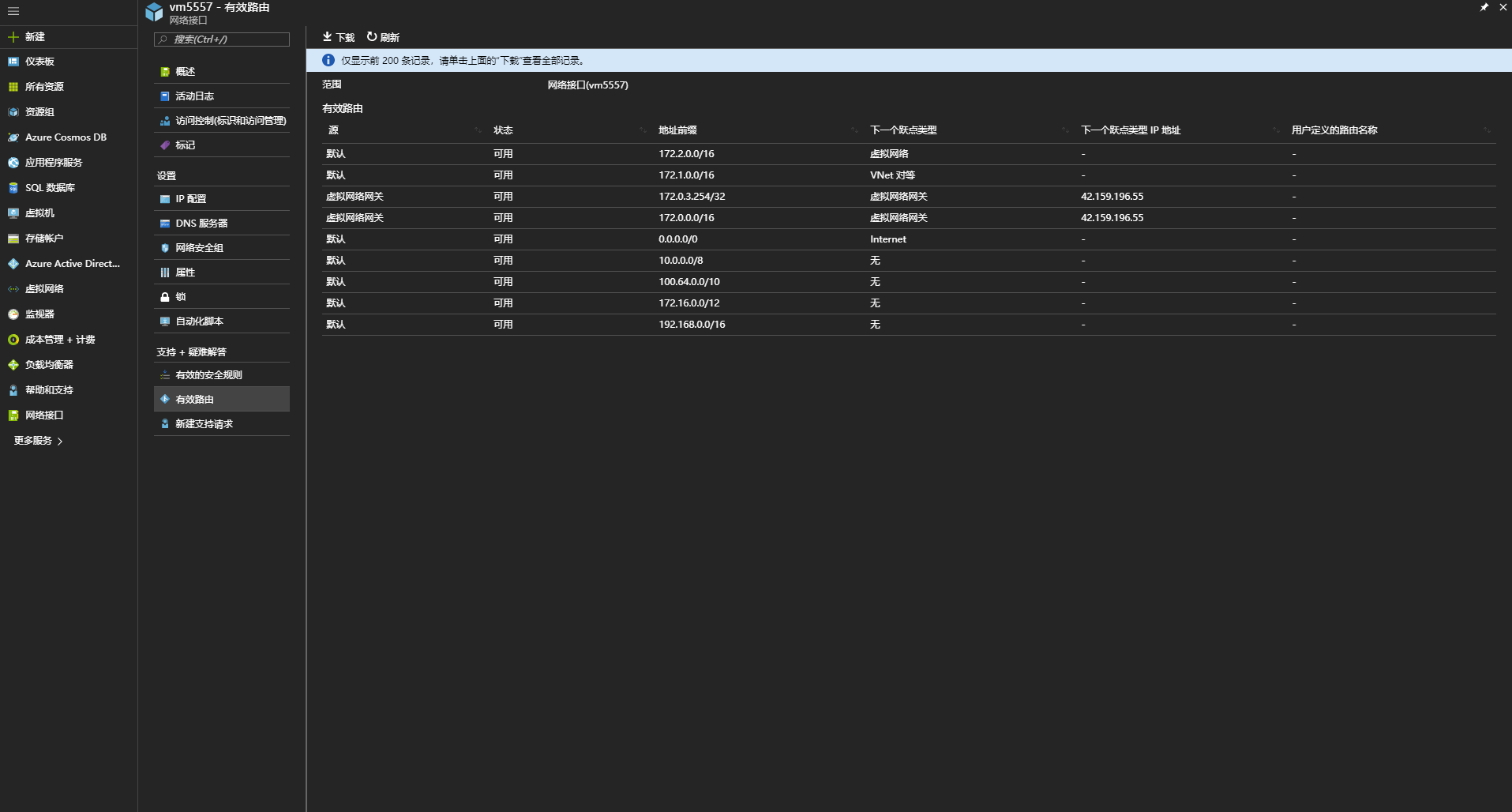


选择VNET3，选择对等，选择VNET3VNET2，勾选使用远程网关，保存。



1. **验证VNET3和VNET1的连通性**

登陆VM5，ping 172.0.0.4 (VM1 VNET1内网地址)，检查连通性。查看VM5有效路由，思考为何此时实现互通。

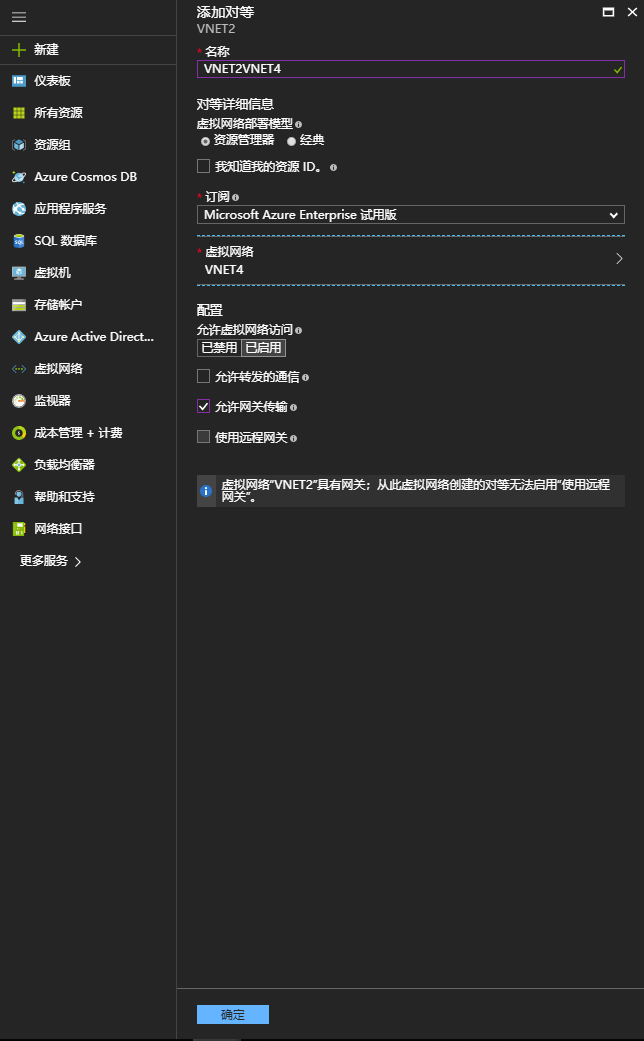


1. **创建VNET4并配置VNET4与VNET2 Peering对等互联**

请参照前面操作方法操作，VNET4（选择在区域West US 2中创建）参数请参阅下面截图







1. **VNET4中创建虚拟机VM6**

访问<https://github.com/nonokangwei/TechSummit2018/blob/master/VM6.json>拷贝VM6虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称VM6，选择资源组（选择之前VNET1所在资源组）。

上述操作也可通过CLI完成：

az group deployment create --template-uri https://raw.githubusercontent.com/nonokangwei/TechSummit2018/master/VM6.json --parameters adminUsername=username adminPassword=password virtualMachineName=VMname -g resourcegroup

1. **验证VNET3和VNET1的连通性**

登陆VM6，ping 172.1.0.4 (VM4 VNET2内网地址)，检查连通性。ping 172.0.0.4 (VM1 VNET1内网地址)，检查连通性。

1. **验证VNET3和VNET4的连通性**

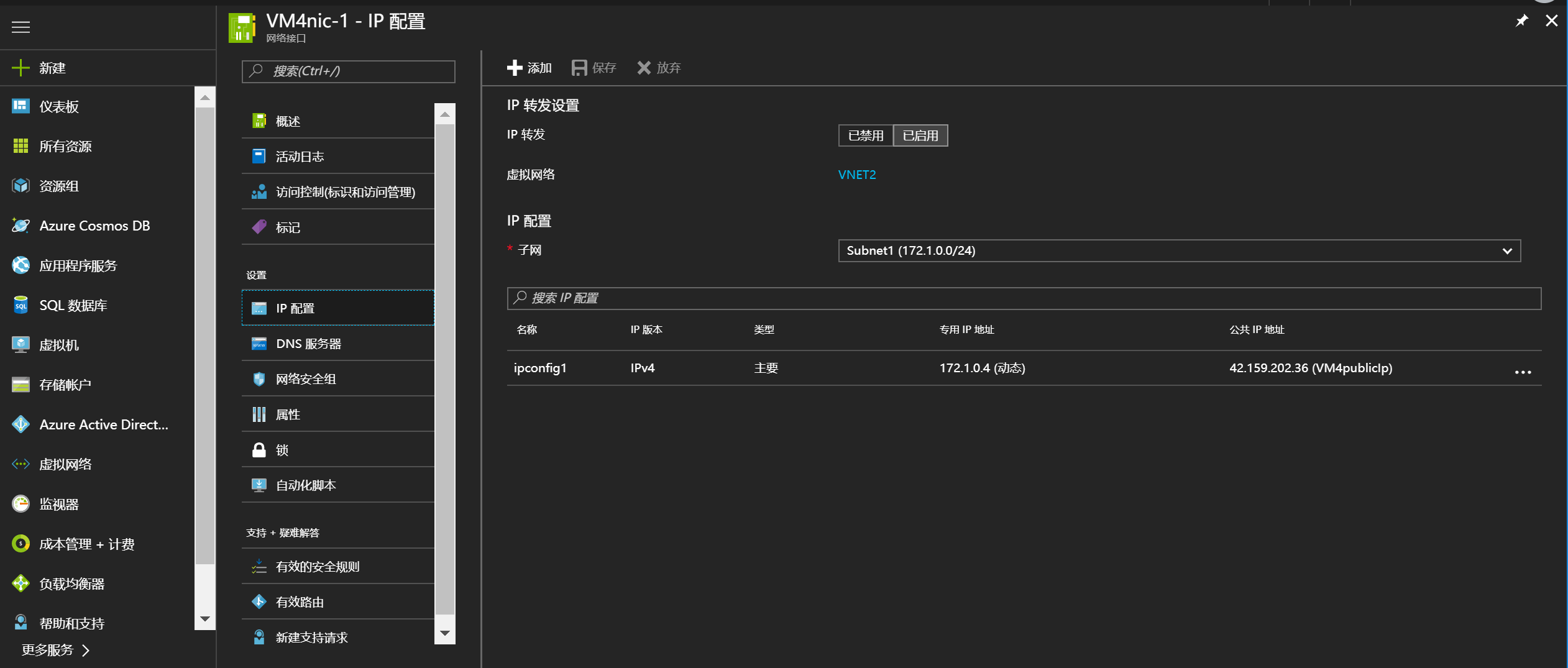
登陆VM6，ping 172.2.0.4 (VM5 VNET3内网地址)，检查连通性。思考为何无法ping通。

1. **配置VNET Peering Transit转发**

选择VNET2，选择对等，选择VNET2VNET3，配置勾选允许转发通信。选择VNET2VNET4，配置勾选允许转发通信。



选择VM4，选择网络，选择VM4nic-1，选择IP配置，配置IP转发配置已启用。

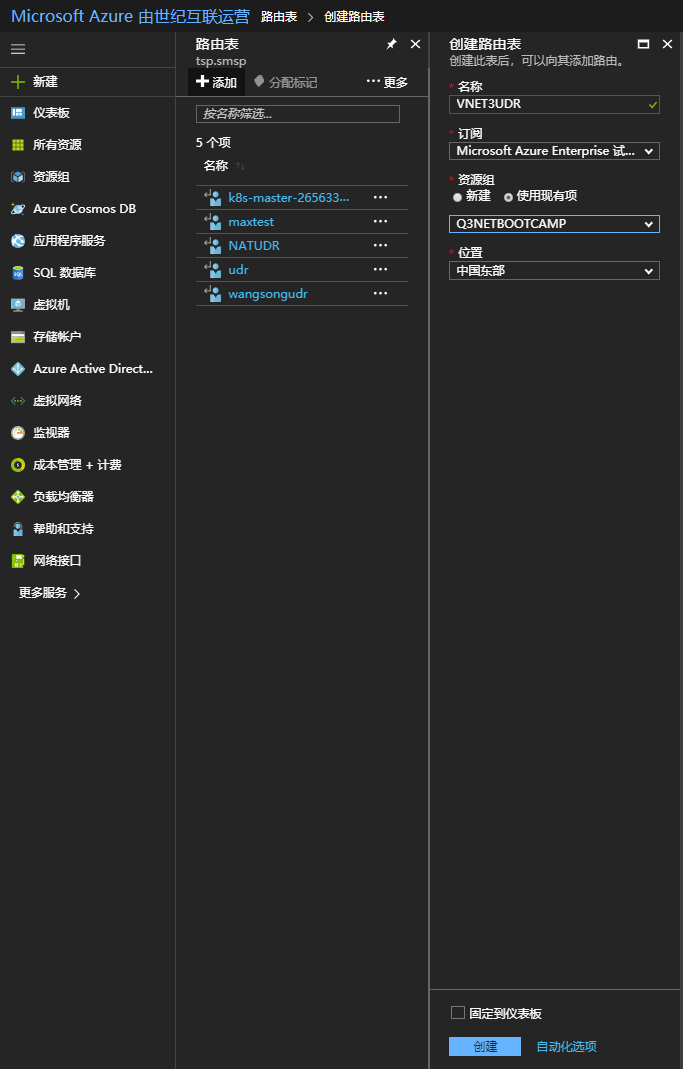


登陆VM4，开启Linux转发

sudo sysctl -w net.ipv4.ip\_forward=1

1. **配置UDR用户自定义路由**

选择路由表，选择添加，名称VNET3UDR，资源组tech014，位置选择West US 2，确认创建。

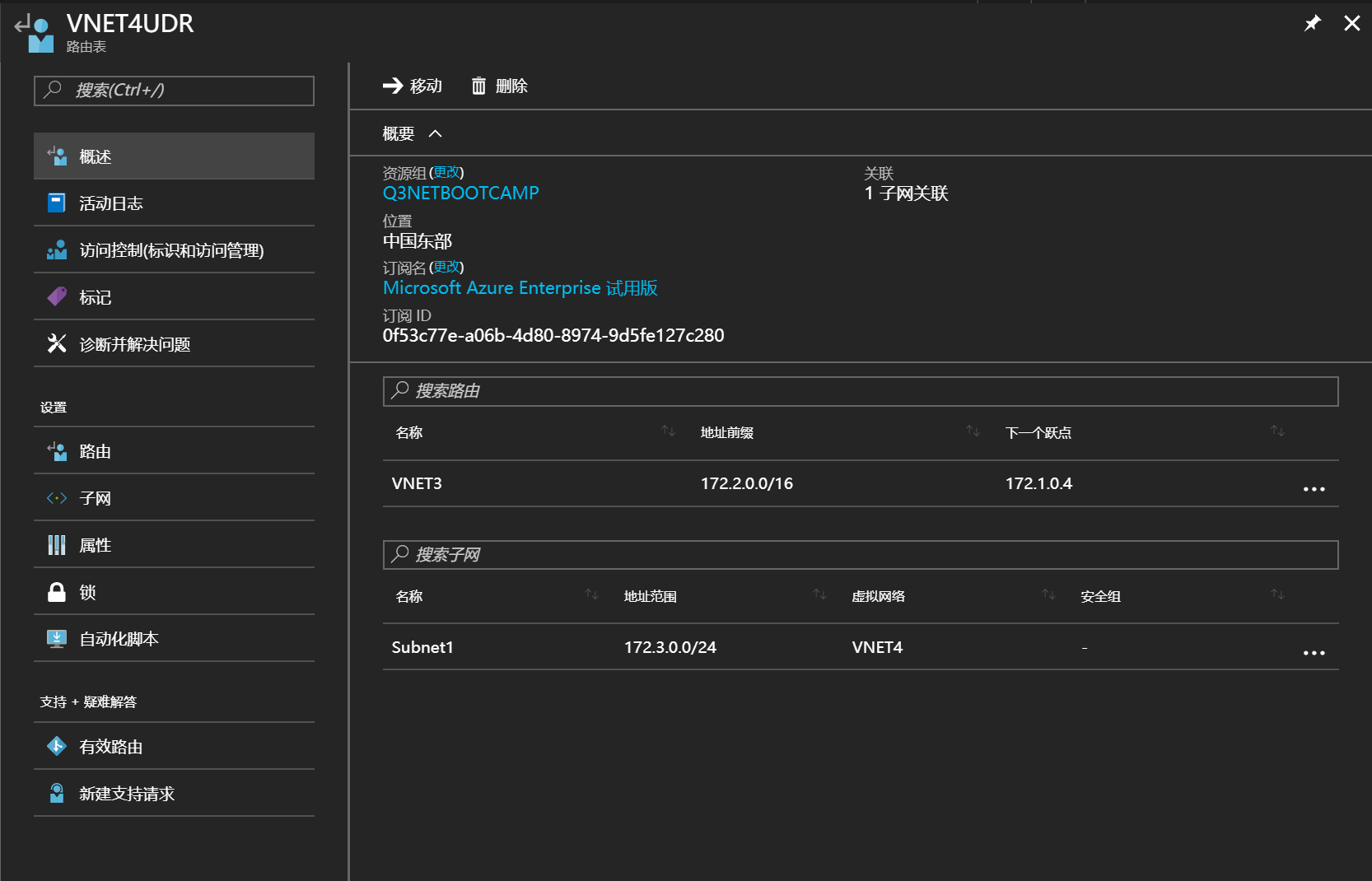


选择UDR路由表 VNET3UDR，选择路由，添加，路由名称VNET4，地址前缀172.3.0.0/24，下一跳类型虚拟设备，下一跳跃点地址172.1.0.4，确认创建。



选择UDR路由表 VNET3UDR，选择子网，选择关联，选择虚拟网络VNET3，选择子网Subnet1，确认关联。

相同操作创建VNET4UDR,，相关参数可参阅如下截图。

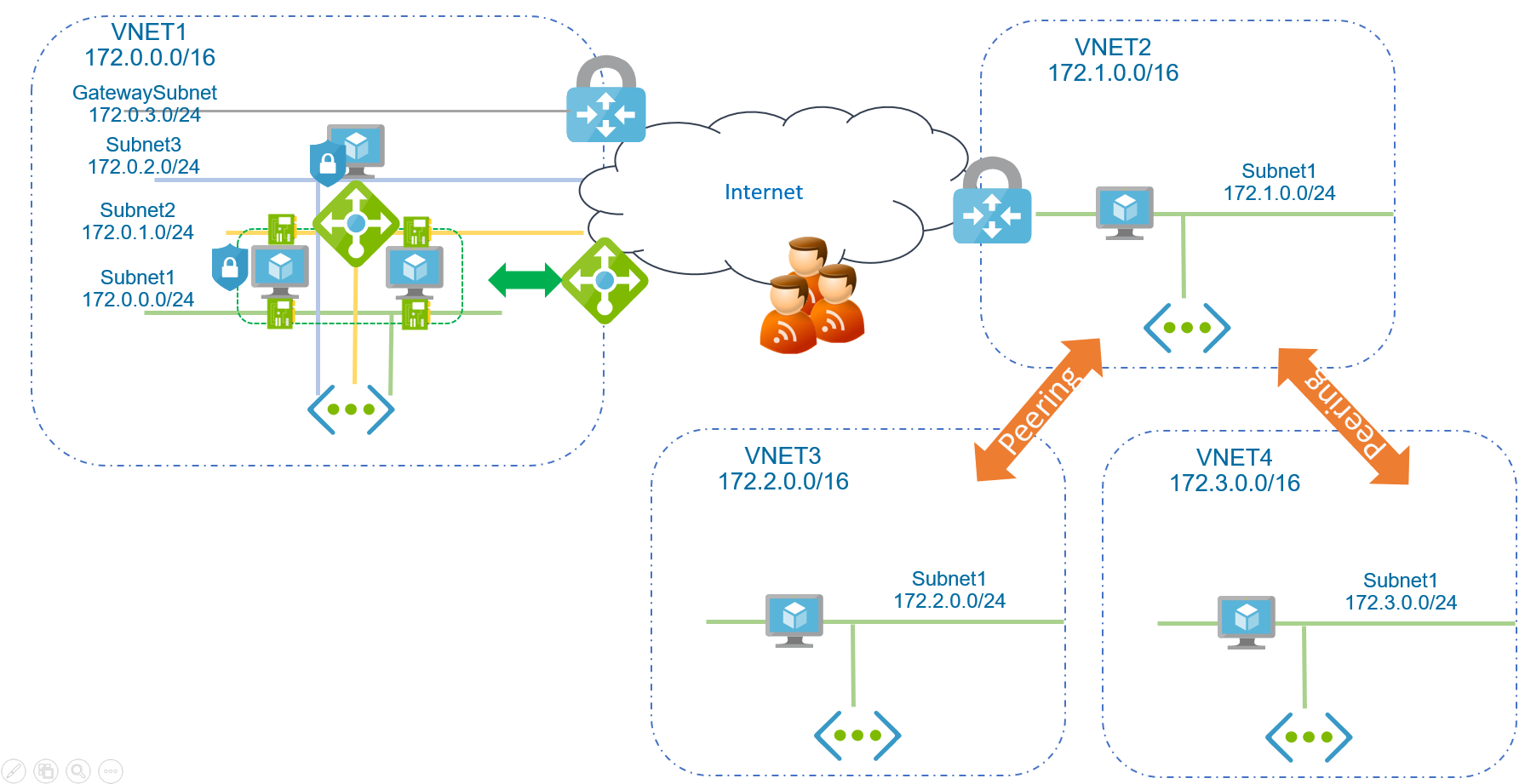


1. **验证VNET3和VNET4的连通性**

登陆VM6，ping 172.2.0.4 (VM5 VNET3内网地址)，检查连通性。

Exercise 7: NVA+UDR实验（选做）

实验目标：掌握NVA组网自定义部署网络架构



1. **创建虚拟机**

若实验一已经完成可以直接进入步骤二操作无需重复创建虚拟机。访问<https://github.com/nonokangwei/TechSummit2018/blob/master/TwoNicVM.json>拷贝双网卡虚拟机部署模板。登陆Portal选择新建，搜索模板或template，选择模板部署。编辑模板，将模板拷贝到编辑窗口中。编辑参数，输用户名，密码（建议使用Azuredemo!123），虚拟机名称（建议使用VM1），选择资源组（选择之前VNET1所在资源组）。重复上述操作建立虚拟机VM2.。

上述操作也可通过CLI完成：

az group deployment create --template-uri https://raw.githubusercontent.com/nonokangwei/TechSummit2018/master/TwoNicVM.json --parameters adminUsername=username adminPassword=password virtualMachineName=VMname -g resourcegroup

1. **开启路由转发**

登陆VM1

sudo sysctl -w net.ipv4.ip\_forward=1

重复操作在VM2

1. **准备iptables**

登陆VM1

sudo iptables -A FORWARD -i eth1 -j ACCEPT

sudo iptables -A FORWARD -i eth0 -j ACCEPT

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

重复操作在VM2

1. **准备策略路由表**

登陆VM1

sudo sed -i '$a201 slbroute' /etc/iproute2/rt\_tables

sudo ip rule add from 172.0.1.4 to 168.63.129.16 lookup slbroute

sudo ip route add 168.63.129.16 via 172.0.1.1 dev eth1 table slbroute

sudo ip route add 172.0.2.0/24 via 172.0.1.1

登陆VM2

sudo sed -i '$a201 slbroute' /etc/iproute2/rt\_tables

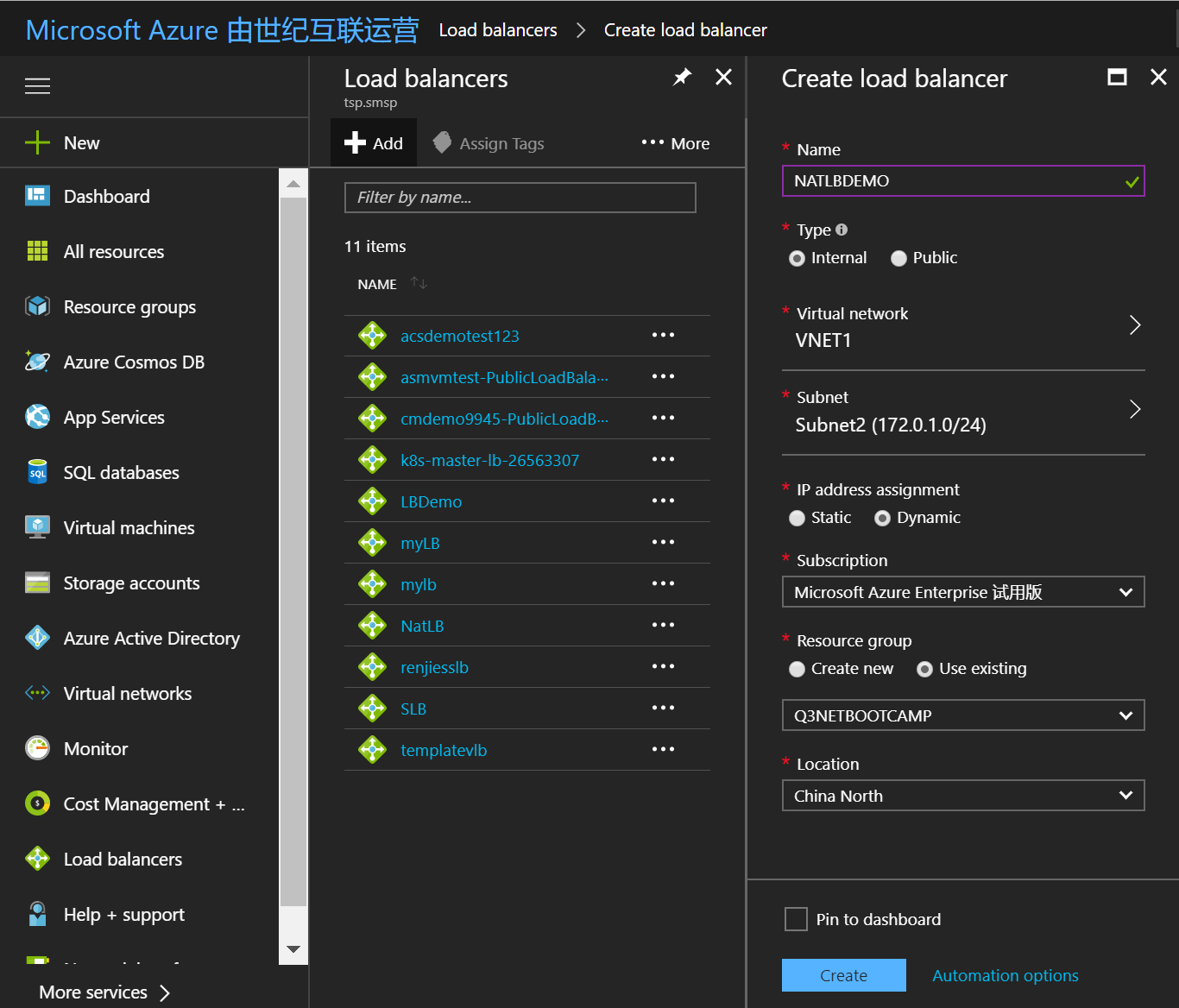
sudo ip rule add from 172.0.1.5 to 168.63.129.16 lookup slbroute

sudo ip route add 168.63.129.16 via 172.0.1.1 dev eth1 table slbroute

sudo ip route add 172.0.2.0/24 via 172.0.1.1

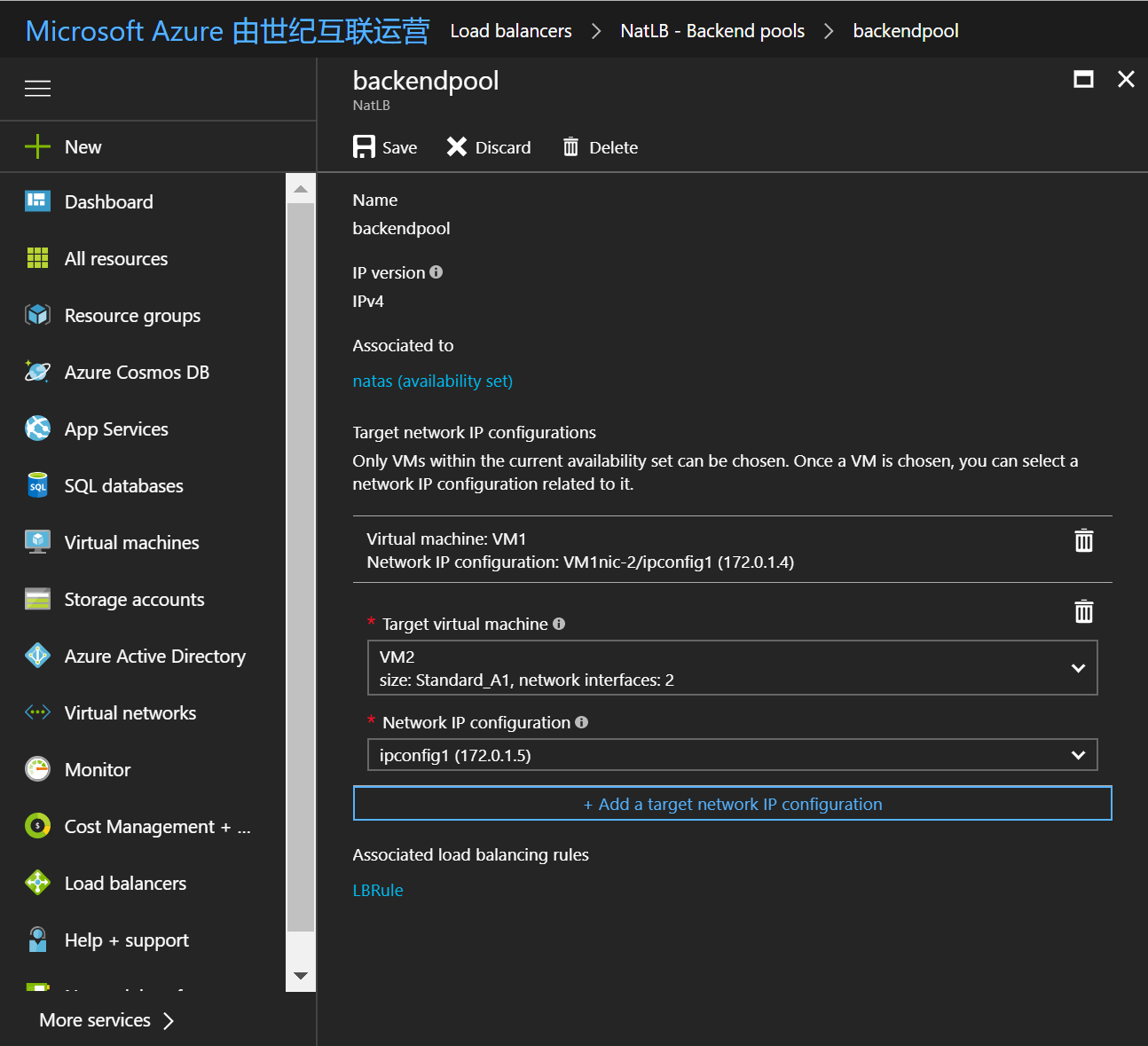
1. **创建内网负载均衡**

登陆Portal选择负载均衡，选择新建，给出负载均衡名称NATLBDEMO，指定类型为内网类型，选择虚拟网络VNET1，选择子网Subner2，指定现有资源组（设置为于VNET1所在资源组相同），点击创建。



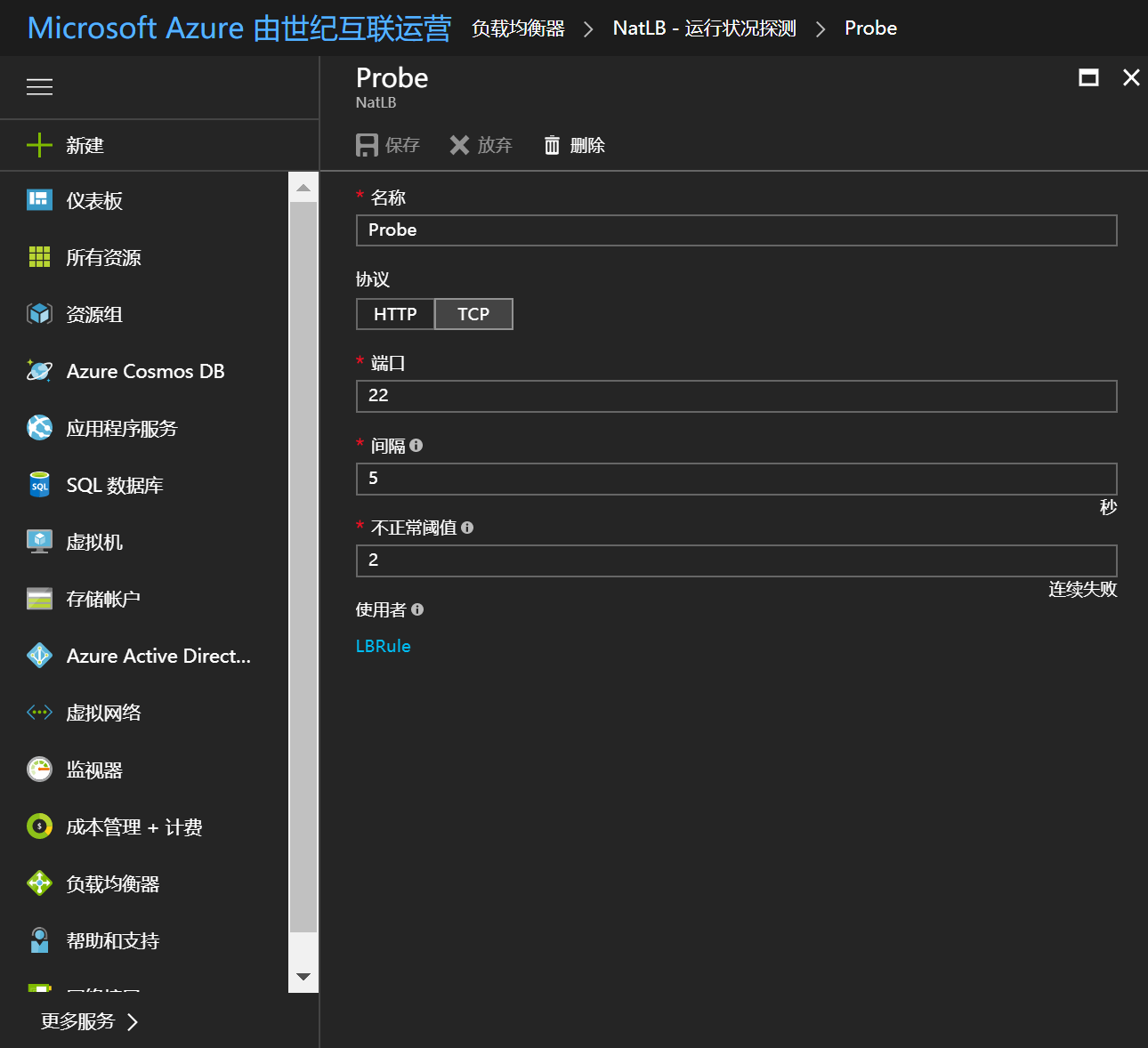
1. **创建内网负载均衡后端池**

选择上一步创建的内网负载拟机，点击后端池选择添加，按照下述截图输入相关参数，将VM1和VM2的NIC2加入到后端池中。

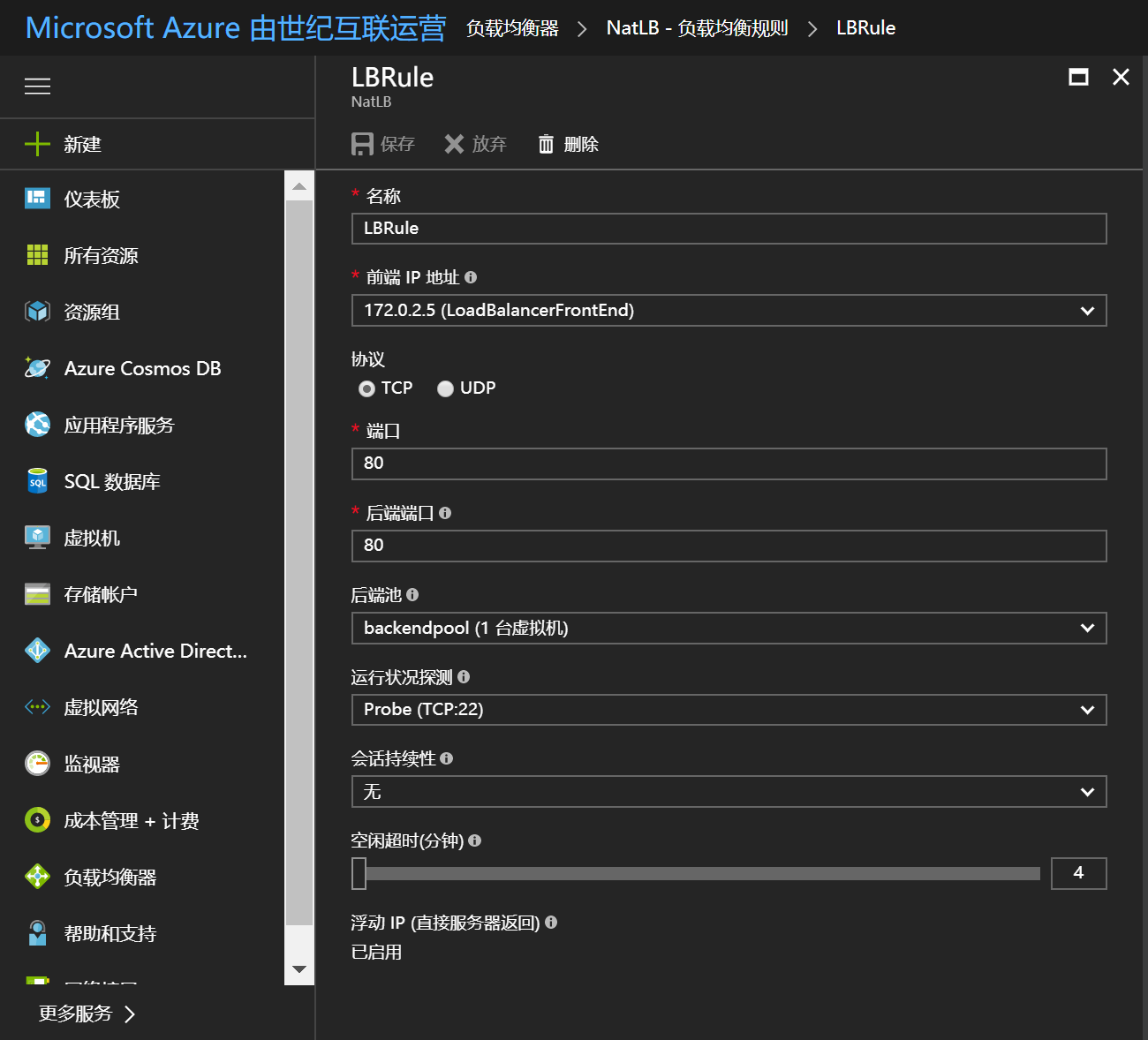


1. **添加内网负载均衡健康检查策略**

选择前面创建的内网负载拟机，点击运行状况探测选择添加，按照下述截图输入相关参数，



1. **添加内网负载均衡的策略规则**
2. **选择前面创建的内网负载拟机，点击负载均衡规则选择添加，按照下述截图输入相关参数，注意将浮动IP选项打开。**



1. **配置客户自定义路由UDR**

选择路由表并添加，输入UDR名称NATUDR，选择VNET1所在资源组，区域选择East US 2。选择刚刚创建的NATUDR，选择路由并添加，参数如下述截图：

下一跳172.0.1.6



选择子网并关联，虚拟网络选择VNET1，子网选择Subnet3。

1. **检查NAT策略**

登陆VM3，模拟curl [ifconfig.co](http://www.baidu.com) 无正常输出。

curl: (7) Failed to connect to ifconfig.co port 80: Connection timed out

原因默认虚拟机网卡不支持路由转发，选择VM1和VM2的NIC2，选择IP配置，开启转发功能。

重新模拟curl操作，此时应有正常输出。

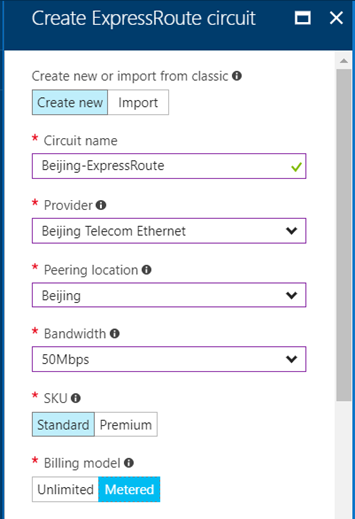
再次尝试curl ifconfig.co 查看输出结果是否为VM1或VM2的公网IP。多次尝试curl ifconfig.co 确认输出地址是否会变化。

Exercise 8: 专线演示实验（只做演示学员无需操作）

实验目标：掌握NVA组网自定义部署网络架构

1. **创建专线连接**

选择运营商（北京电信或上海电信）以及peering location（北京或上海），按照客户业务需求选择带宽。本地访问选择Standard，跨地域访问选择Premium。按流量计费选择Metering，包月计费选择Unlimited。



专线连接创建完成，将Service-Key交给电线运营商进行预铺设。

1. **创建不同类型的对等管理**

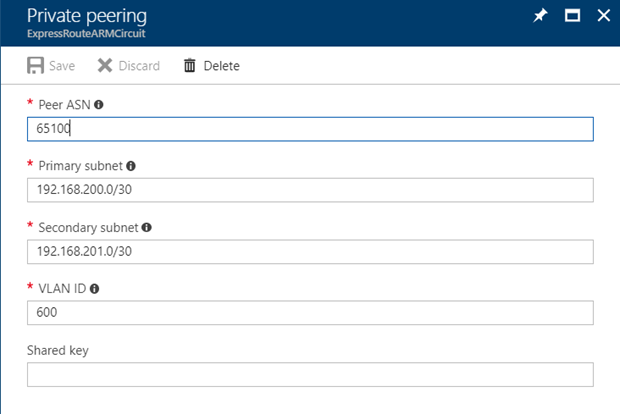
运营商预铺设完成后，链路状态变为“Provisioned”。用户可以在Portal上进行对等Peering的配置。

Peer ASN为用户一侧BGP AS号码，不能使用65515-65520，其他ASN均可以使用。

Primary subnet和Secondary subnet对应用户两条物理线路的IP地址设定。请指定两个/30子网用于用户设备与微软设备的互联。地址分配完成之后，用户使用第一个IP地址，微软使用第二个IP地址。

VLAN ID用于标识用户不同的对等Peering关系，用户自己指定即可。

Share key为用于BGP通讯过程MD5加密密钥，可选。



1. **创建专线网关**

用户需要在现有的VNET中创建专线网关用户和专线互联，从而与企业现有On premise互联。专线网关区别与VPN网关，需要单独创建。



1. **连接专线链路到专线网关**

最后需要将专线链路连接到专线网关。

一个专线链路最多可以支持100个专线网关共享使用（需要高级版本）

一个网关最多可以关联四个不同区域的专线链路

