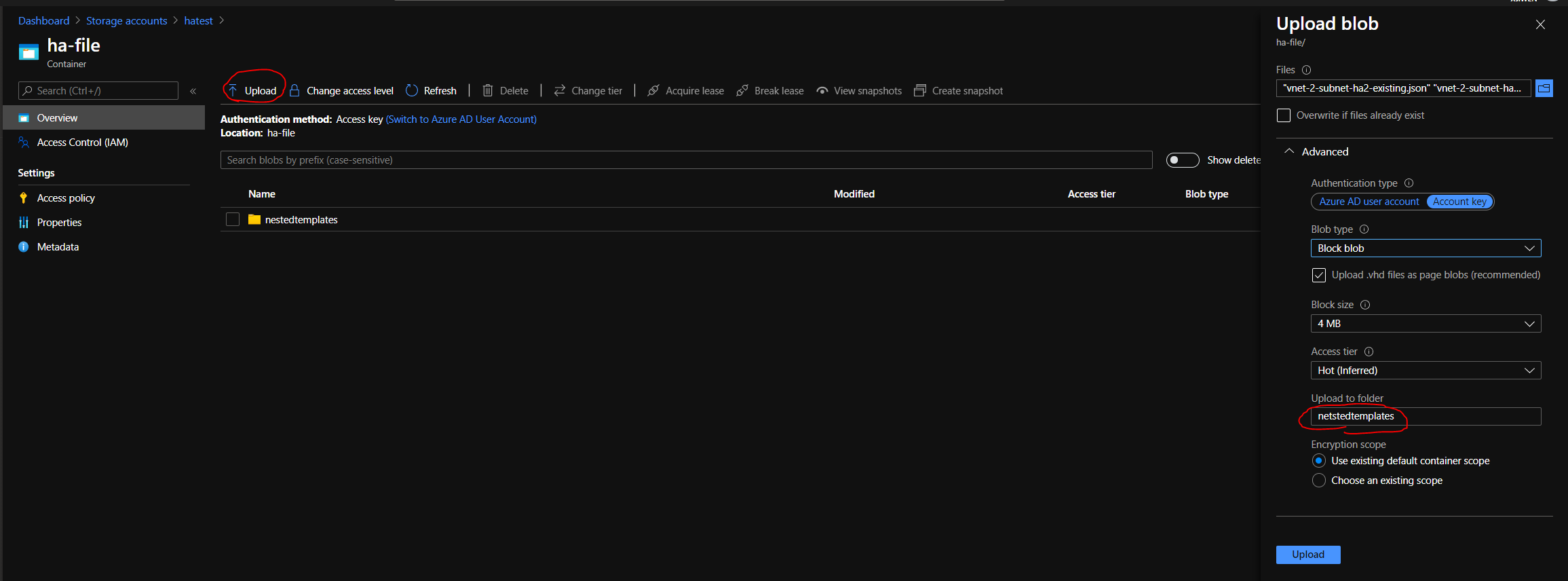
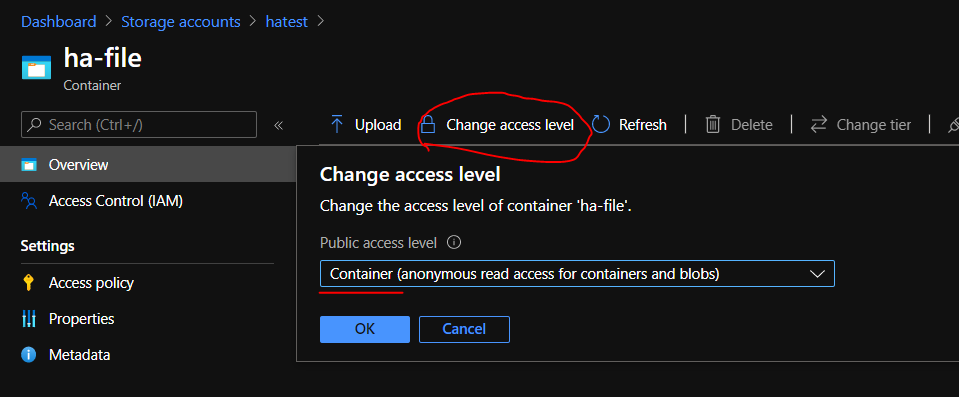
R80.40 HA Cluster deploy guide for Azure

1. 上传文件到Azure存储中，目录为ha-test/nestedtemplates。 文件名：load-balancer.json, vnet-2-subnet-ha-new.json，vnet-2-subnet-ha-existing.json。可参考

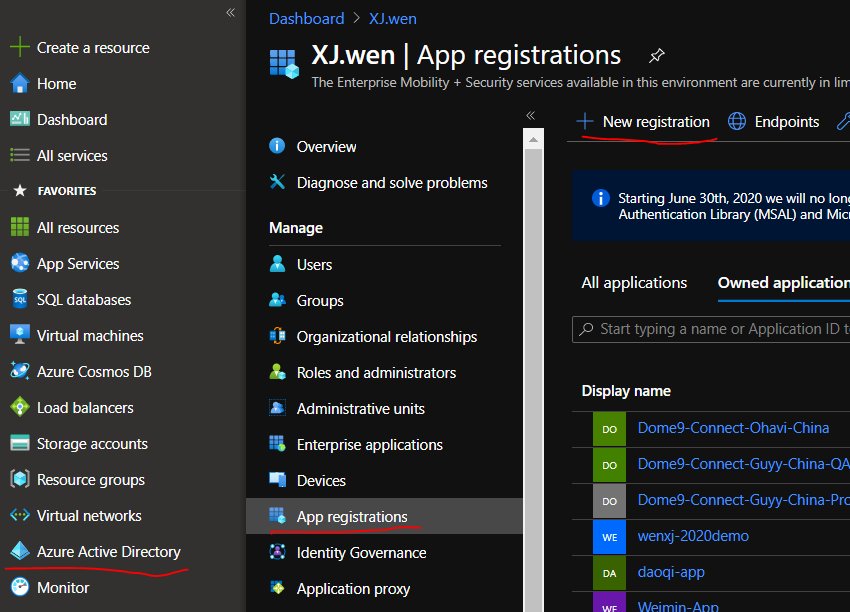
《R80.30 VMSS and MGMT deployment instructions-1.docx》。即在存储账号的“Containers”中创建目录“ha-test”（自己定义），进入该目录，点击上方的“upload”上传文件，在右侧的advanced菜单里，“upload to folder”里输入“nestedtemplates”，注意不要输错，整个名字和部署脚本里的要一致。完成后，确认该目录的“change access level”是“Container”。



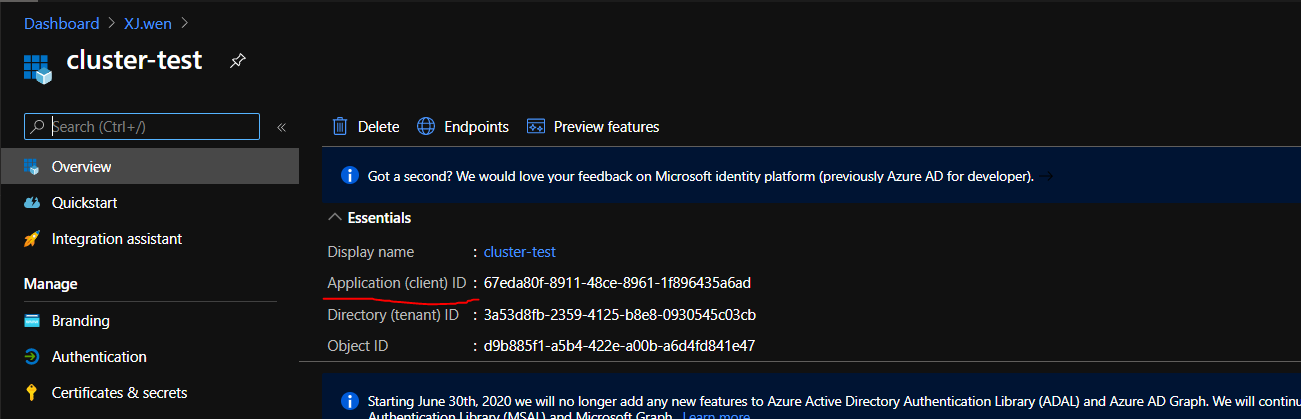


1. 下Azure上建一个service principal 的application，在CGI Gateway cluster中使用其App ID 和secret 完成API call。步骤如下：

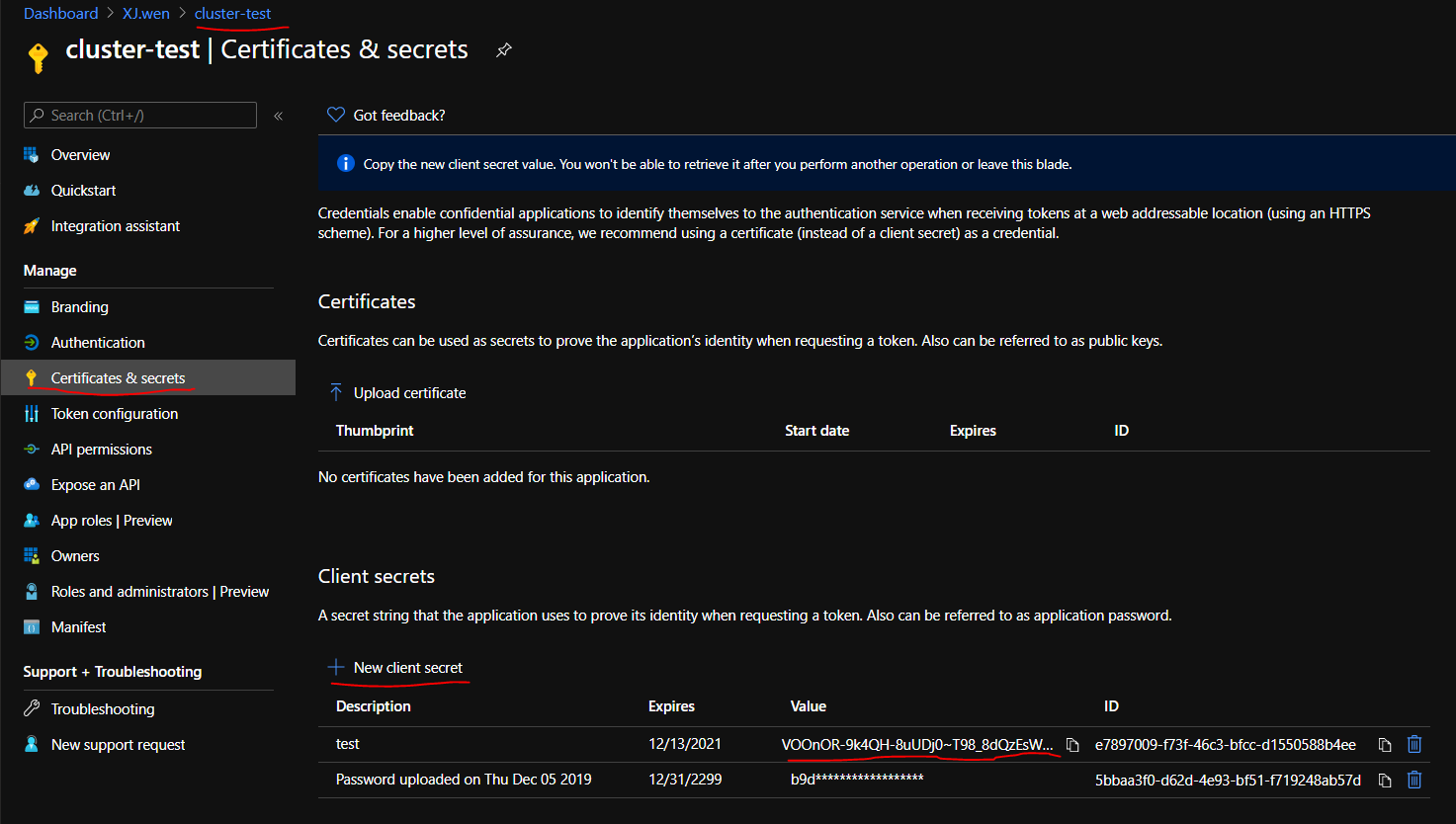
* Azure Active Directory --> app registration -->new registration



* 从新建的app-->Overview中copy “Application(client) ID” 作为第7步中的“client-ID”



* 在新建的app中，点击“Certificates&secrets”，点击“New client secret”，输入Description，copy该Description的“Value”作为第7步中的“client-secret”。

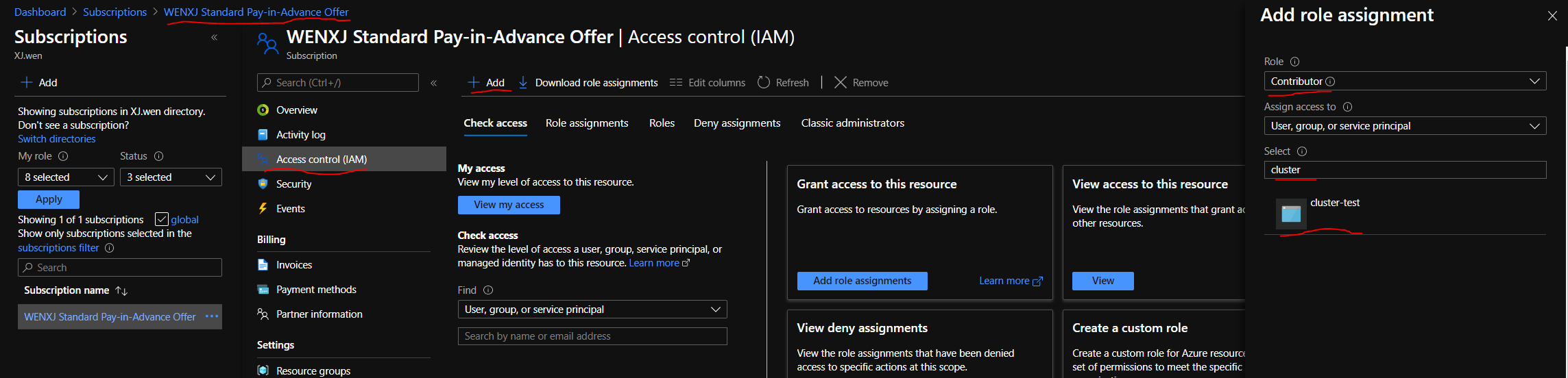


* subscriptions --> access control(IAM) -->Add (add role assignment)

role: distributor

assign access to: Azure AD user, group or service principal

select: app name (输入新建app名字)



3. 在Azure上创建resource group, security group, Vnet and subnet，至少两个网段。

4. 部署Cluster GW。在Create a resource中搜索“template”，在“template deployment”中创建新的template。（或者在Marketplace里搜索template服务也可以）。上传脚本文件<<mainTemplate-change-LB-MP-OK.json>>，输入响应参数。特别注意的是：

“'\_artifactsLocation' parameter”需要输入<https://vmss.blob.core.chinacloudapi.cn/ha-test/>, 必须以“/”结束。 可以参看“R80.30 VMSS and MGMT deployment instructions-1.docx”。具体参数如下：

Subscription: 选择订阅

Resource group: 选择部署的RG

Location：选择部署的区域，建议China East 2

Location：保持默认

Cloud Guard Version: 保持默认 （R80.30-Bring Your Own License）

Admin Password: 设置密码 （用户名缺省是admin）

Authentication Type: 保持默认 （password）

SSH Public Key: 保持空白

Vm Name：输入cluster的名字，两台防火墙分别在cluster名字后面加“0”和“1”

Vm Size：可以保持原有，也可以输入新的VM类型

Sic Key：输入SIC密码 （防火墙和管理服务器通信密码）

Virtual Network Name：输入部署的Vnet名字

Virtual Network Address Prefixes：输入Vnet的IP地址域

Subnet1Name：输入eth0的Vnet内的子网名字

Subnet1Prefix：输入eth0的子网前缀

Subnet1Start Address：输入eth0子网的第一个IP地址，0-4不要用

Subnet2Name：输入eth1的Vnet内的子网名字

Subnet2Prefix：输入eth1的子网前缀

Subnet2Start Address：输入eth1子网的第一个IP地址，0-4不要用

Vnet New or Existing：选择existing

Virtual Network Existing RG Name：输入Vnet RG名字

Bootstrap Script：保留空白

Allow Download From Upload To Check Point：选择True

Additional Disk Size GB：保留空白

Disk Type：保留默认Standard\_LRS

Preview：保留空白

Role：保留默认，Contributor

Managed System Assigned：保留默认，yes

Source Image Vhd URL：保留默认。（如果不适用marketplace，需要输入URL）

Availability Options：保留默认

\_artifacts Location： 输入步骤1中目录的URL，必须以“/”结束

\_artifacts Loacation Sas Token：保留空白

5. 检查所有interface的安全组是否开放了响应权限。

web登陆GW确保JHF为最新版本。

修改时区为中国。

6. 检查cluster文件：azure-ha.json，正确的见附件。

#cd $FWDIR/conf

#cat azure-ha.json

7. 输入App ID and client-secret 到文件azure-ha.json里。注意CLI中为两个横杠。

#azure-ha-conf --client-id 'Applicationid' --client-secret 'Password'

client-id: 参看第二步中创建的App中的“Application(client) ID”

client-secret: 参看第二步中subscription（订阅）中的client secret。

（example: azure-ha-conf --client-id 'b78cca0d-2f9b-4426-9c51-dd6bd9a081b7' --client-secret 'uzzCUqUn9n5UM5EDiu592AgnDEtaG/Lqq+HYZZ6tTyM='）

8. 输入中国环境参数到文件azure-ha.json里。

#azure-ha-conf --environment AzureChinaCloud

9. 检查azure-ha.json文件里的cluster信息，要和Azure Template脚本输入的名字一致。

"clusterNetworkInterfaces": {

"eth0": [

"private cluster IP",

" ha-0" (cluster name = public ip name)

]

},

10. 检查文件azure-ha.json，无输出为正确。

#python -m json.tool $FWDIR/conf/azure-ha.json

11. 重新加载cluster脚本。

#$FWDIR/scripts/azure\_ha\_cli.py reconf

12. 确认fwkern.conf内容：

#vi $FWDIR/boot/modules/fwkern.conf

fwha\_dead\_timeout\_multiplier=200

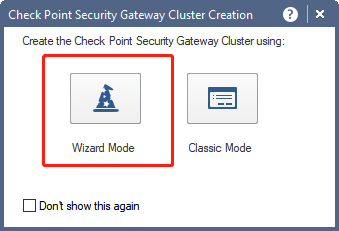
fwha\_if\_problem\_tolerance=200

cloud\_balancer\_ip1=0xa83f8110

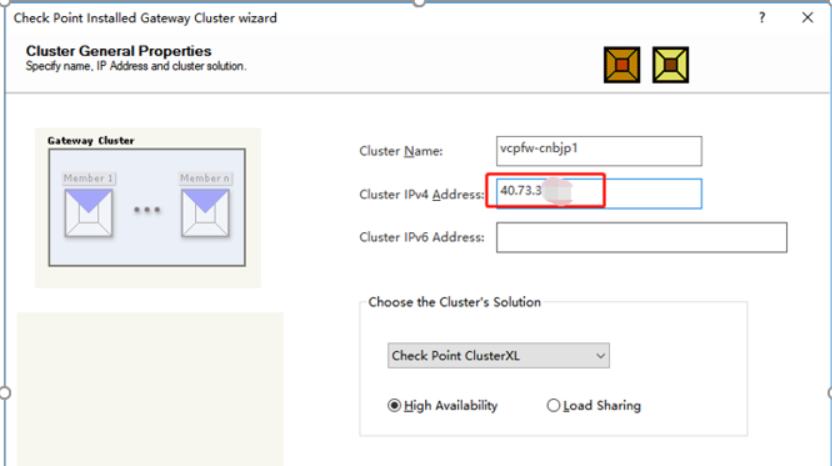
cloud\_balancer\_port=8117

13 在管理服务器中配置ClusterXL，如果没有管理服务器，建议部署在同一个vnet内。

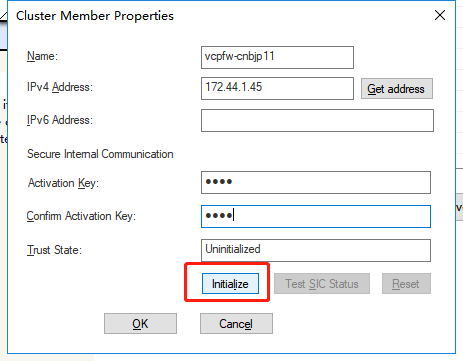
* 创建New Cluster，选择向导模式

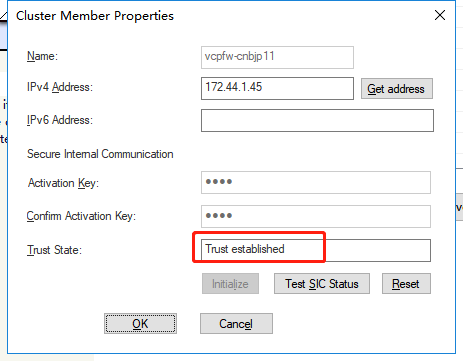


* 输入Cluster Name名字要和"azure-ha.json"文件中一致，即template脚本时输入的“Vm Name”；在Azure界面里“All resource”中找到第一台防火墙（通常为主设备）的主网卡（例如vcp-cnbjp11-eh0。vcp-cnbjp1为cluster名字，vcp-cnbjp11为第一台防火墙，vcp-cnbjp12为第二台防火墙），在网卡的“IP configuration”里可以看到两个IP，一个是member IP，即本机接口IP，一个是cluster IP。在下图的cluster IPv4 Address中输入公网的Cluster IP。然后点击下一步。

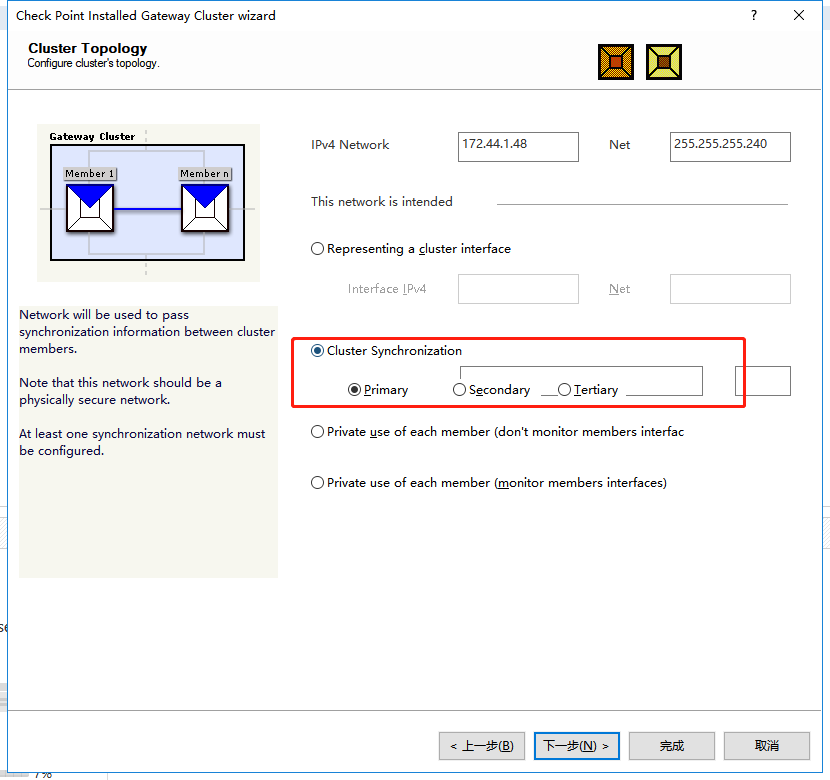


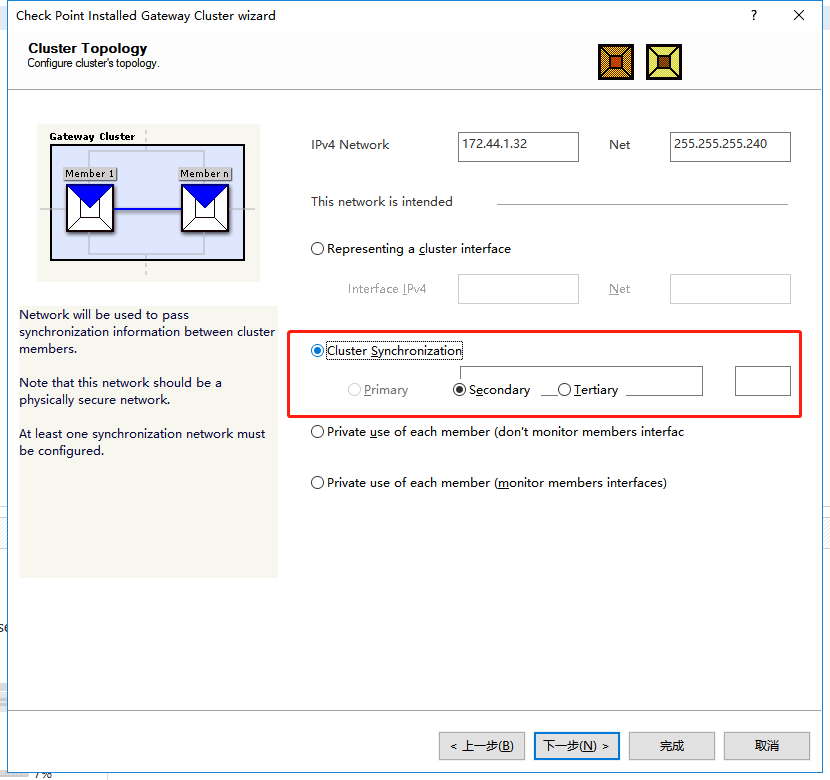
* 添加member1，Name为第一台防火墙的名字，IPv4为该防火墙的公网Member IP（Azure中在接口的IP configuration内）。Activation Key为SIC密码，Template脚本中已经输入。然后初始化管理服务器和防火墙的密钥连接。



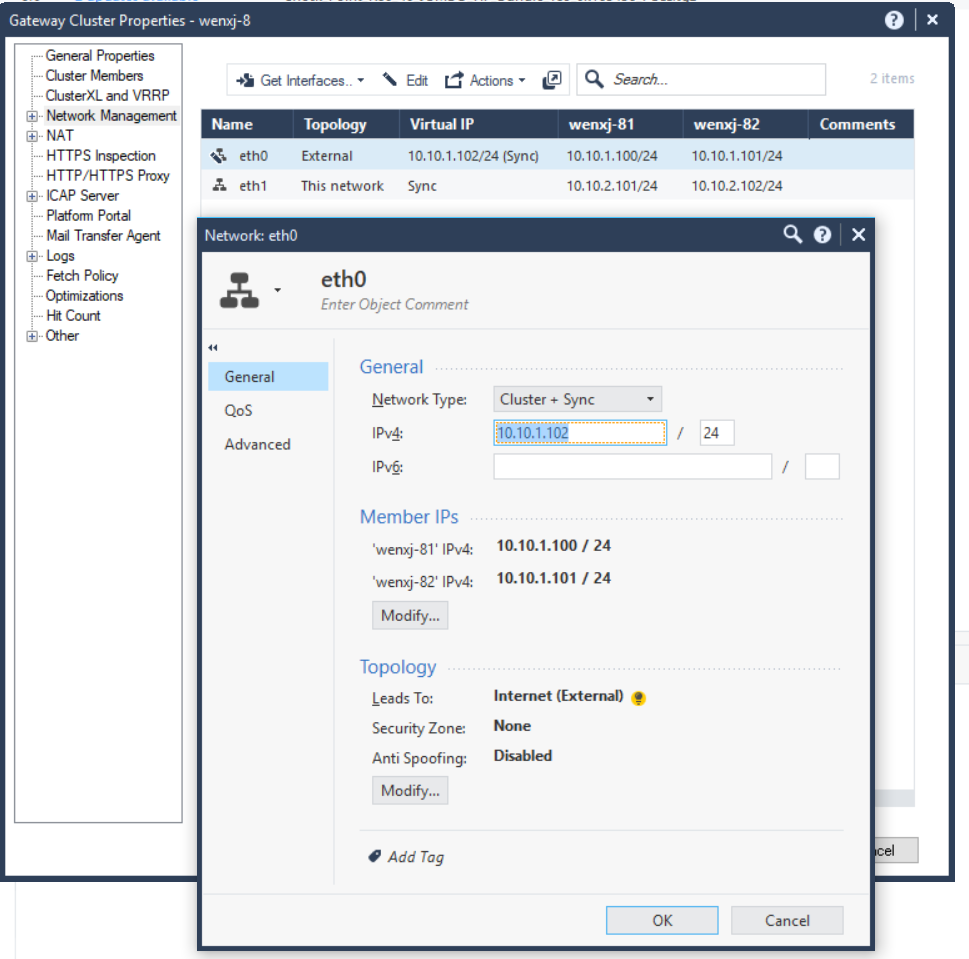


* 同理添加member2。
* 配置为Cluster Synchronization，选择内网卡eth1为Primary和外网卡eth0为Secondary，然后点击完成。

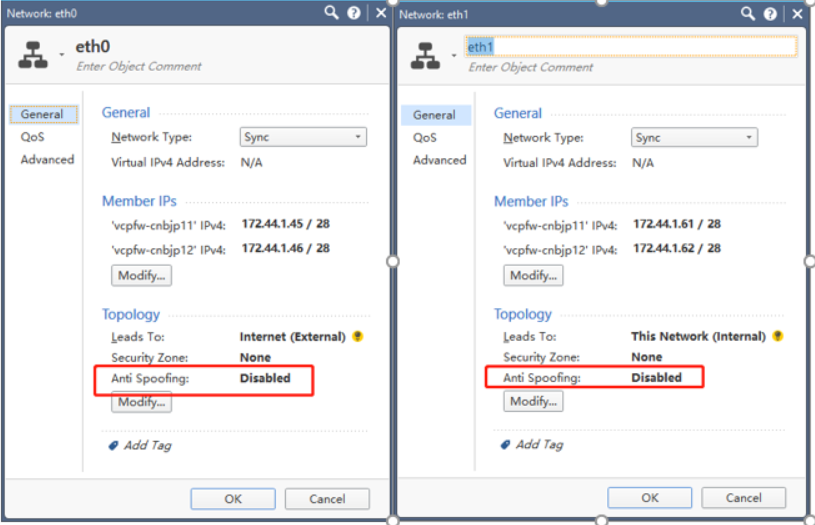




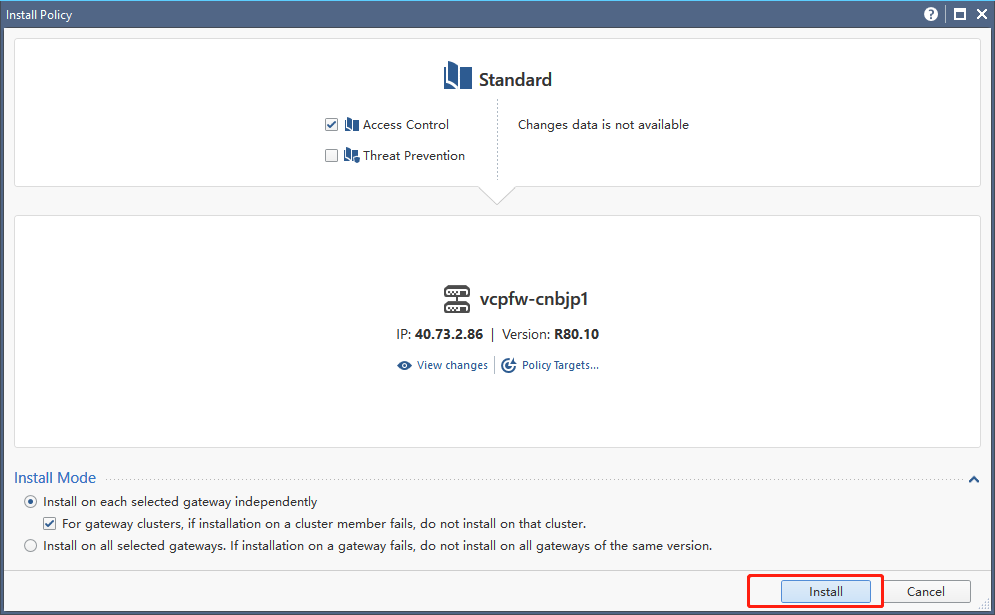
* Cluster建立完成后，在管理界面双击cluster的图标，进入“Gateway Cluster Properties”界面，点击networkmanagement，双击Eth0，修改其Network Type为“Cluster+Sync”，在IPv4栏中输入私有的VIP地址。



* Disable eth0和eth1接口的Anti snoofing。



* 初次配置管理服务器，需要修改缺省访问策略Drop为allow，然后下发策略。



14. 在两台防火墙上做cluster自测，没有报错，其输出结果最后为防火墙的IP地址。

#cd $FWDIR/scripts

#./azure\_ha\_test.py

在防火墙上检查Cluster状态，在主设备上用第二条命令实现fail-over切换，再次检查 cluster状态。

#cphaprob state (检查主备机状态)

#clusterXL\_admin down (fail-over 切换)

15. 自测失败可以查日志："tail -f $FWDIR/log/azure\_had.elg"

附录—azure-ha.json文件样本：

Expert@ha-01:0]# cat azure-ha.json

{

"debug": false,

"subscriptionId": "49ec1be9-c437-489a-8934-e20490b21260",

"resourceGroup": "vmss-test",

"credentials": {

"tenant": "3a53d8fb-2359-4125-b8e8-0930545c03cb",

"grant\_type": "client\_credentials",

"client\_id": "67eda80f-8911-48ce-8961-1f896435a6ad",

"client\_secret": "b9d47Y-kaJ2]UjLEuUbs?SesdBDXP]:q"

},

"clusterNetworkInterfaces": {

"eth0": [

"10.0.1.30",

" ha-0"

]

},

"proxy": "",

"virtualNetwork": "vnet-vmss",

"clusterName": "ha-0",

"lbName": "ha-elb",

"environment": "AzureChinaCloud"