**NSD CLOUD DAY04**

1. [案例1：创建虚拟私有云](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case1)
2. [案例2：购买云主机](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case2)
3. [案例3：弹性公网IP与安全组案例](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case3)
4. [案例4：配置华为云YUM源](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case4)
5. [案例5：创建模板机和跳板机](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case5)
6. [案例6：部署网站实战案例](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/CLOUD/DAY04/CASE/01/index.html#case6)

**1 案例1：创建虚拟私有云**

**1.1 问题**

本案例要求：

* 创建虚拟私有云

**1.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：创建虚拟私有云，如图-1



图-1

选择区域，名称等，如图-2：

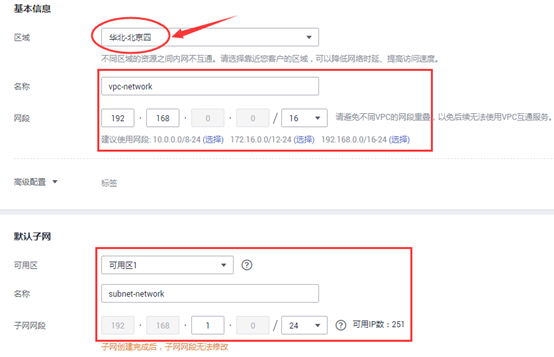


图-2

**2 案例2：购买云主机**

**2.1 问题**

本案例要求在华为云上购买 2 台云主机实现如下操作：

* 云主机 ecs-proxy（登录方式，密码）
* 云主机 ecs-host （登录方式，密钥）

**2.2 步骤**

实现此案例需要按照如下步骤进行。

选择弹性云服务器ECS，如图-3



图-3

选择按需购买ECS，选择型号和系统后，查看价格，如图-4，图-5所示。



图-4



图-5

网络配置，如图-6



图-6

设置密码，如图-7

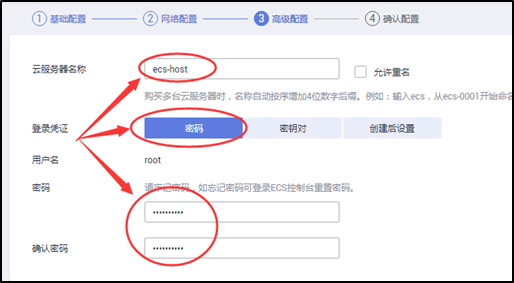


图-7

使用云主机，如图-8、图-9所示。



图-8

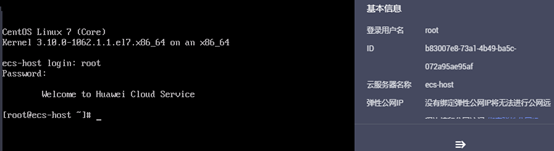


图-9

**3 案例3：弹性公网IP与安全组案例**

**3.1 问题**

本案例要求购买弹性公网 IP 和带宽：

* 让云主机可以访问互联网
* 配置安全组
* 允许互联网用户访问云主机服务

**3.2 步骤**

实现此案例需要按照如下步骤进行。

购买弹性公网IP，如图-10、图-11所示。



图-10



图-11

绑定公网IP，如图-12

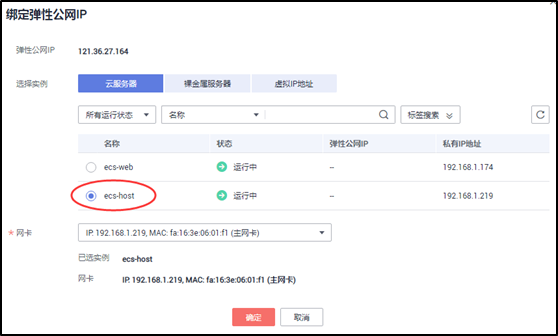


图-12

设置安全组，如图-13、图-14、图-15所示。

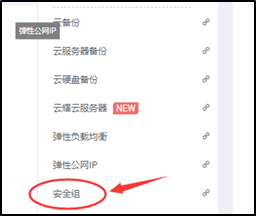


图-13



图-14

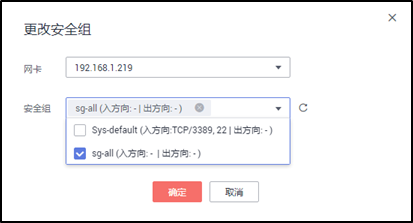


图-15

连接公网IP，如图-16

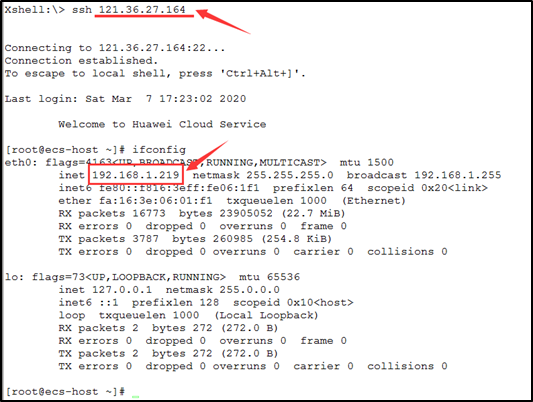


图-16

**4 案例4：配置华为云YUM源**

**4.1 问题**

本案例要求购买弹性公网 IP 和带宽：

* 测试云主机访问网络
* 在云主机上配置 华为云私网Yum 源
* 安装软件测试 bash-completion

**4.2 步骤**

实现此案例需要按照如下步骤进行。

1)配置yum源，并测试

1. [root@localhost ~]# rm -rf /etc/yum.repos.d/\*.repo
2. [[root@localhost](mailto:root@localhost) ~]# curl -o \
3. /etc/yum.repos.d/CentOS-Base.repo \
4. <http://mirrors.myhuaweicloud.com/repo/CentOS-Base-7.repo>
5. [[root@localhost](mailto:root@localhost) ~]# yum install –y bash-completion

**5 案例5：创建模板机和跳板机**

**5.1 问题**

本案例要求创建模板机和跳板机：

* ecs-proxy 跳板机
* ecs-host 模板

**5.2 步骤**

实现此案例需要按照如下步骤进行。

1. 配置yum源
2. [root@localhost ~]# rm -rf /etc/yum.repos.d/\*.repo
3. [[root@localhost](mailto:root@localhost) ~]# curl \
4. -o /etc/yum.repos.d/CentOS-Base.repo \
5. <http://mirrors.myhuaweicloud.com/repo/CentOS-Base-7.repo>
6. 安装常用工具软件包
7. [[root@localhost](mailto:root@localhost) ~]# yum install -y net-tools lftp rsync psmisc \
8. vim bash-completion createrepo vsftpd ansible lrzsz
9. ... ...
10. [[root@localhost](mailto:root@localhost) ~]# mkdir /var/ftp/localrepo
11. [[root@localhost](mailto:root@localhost) ~]# cd /var/ftp/localrepo
12. [[root@localhost](mailto:root@localhost) ~]# createrepo .
13. [[root@localhost](mailto:root@localhost) ~]# systemctl enable --now vsftpd
14. 添加 chrony 服务
15. [[root@localhost](mailto:root@localhost) ~]# systemctl stop postfix ntpd
16. [[root@localhost](mailto:root@localhost) ~]# yum remove -y postfix ntp
17. [[root@localhost](mailto:root@localhost) ~]# yum install -y install chrony
18. [[root@localhost](mailto:root@localhost) ~]# vim /etc/chrony.conf # 编辑配置文件
19. [[root@localhost](mailto:root@localhost) ~]# systemctl enable --now chronyd
20. 上传共享密钥：私钥上传到跳板机，更改权限
21. [[root@localhost](mailto:root@localhost) ~]# chmod 0400 /root/.ssh/id\_rsa

2）配置模板机

1. 设置密码
2. [root@localhost ~]# passwd root
3. [root@localhost ~]# rm -rf /etc/yum.repos.d/\*.repo
4. [[root@localhost](mailto:root@localhost) ~]# curl -o /etc/yum.repos.d/CentOS-Base.repo <http://mirrors.myhuaweicloud.com/repo/CentOS-Base-7.repo>
5. [[root@localhost](mailto:root@localhost) ~]# cat >/etc/yum.repos.d/local.repo <<EOF
6. [local\_repo]
7. name=CentOS-$releasever – Localrepo
8. baseurl=”<ftp://192.168.1.252/localrepo>”
9. enabled=1
10. gpgcheck=0
11. EOF
12. 创建镜像
13. [[root@localhost](mailto:root@localhost) ~]# yum install net-tools vim-enhanced bash-completion lftp rsync psmisc iproute
14. [[root@localhost](mailto:root@localhost) ~]# systemctl stop postfix ntpd
15. [[root@localhost](mailto:root@localhost) ~]# yum remove –y postfix ntp
16. [[root@localhost](mailto:root@localhost) ~]# yum install –y install chrony
17. [[root@localhost](mailto:root@localhost) ~]# vim /etc/chrony.conf         #编辑配置文件
18. [[root@localhost](mailto:root@localhost) ~]# systemctl enable --now chronyd
19. [[root@localhost](mailto:root@localhost) ~]# vim /etc/cloud/cloud.cfg     #编辑配置文件
20. #manage\_etc\_hosts: localhost         #注释该行
21. 注：配置完成以后，关机，在华为云主机管理菜单中把模板主机系统硬盘做成镜像，供以后使用

**6 案例6：部署网站实战案例**

**6.1 问题**

本案例要求部署网站：

* 购买3台云主机（web服务器）
* 安装配置 web 集群（推荐playbook方式）

**6.2 步骤**

实现此案例需要按照如下步骤进行。

1. [root@localhost ~]# vim web\_install.yaml
2. ---
3. - name: web 集群安装
4. hosts: web
5. tasks:
6. - name: 安装 apache 服务
7. yum:
8. name: httpd,bash-completion
9. state: latest
10. update\_cache: yes
11. - name: 配置 httpd 服务
12. service:
13. name: httpd
14. state: started
15. enabled: yes
16. - name: 部署网站网页
17. unarchive:
18. src: files/webhome.tar.gz
19. dest: /var/www/html/
20. copy: yes
21. owner: apache
22. group: apache
23. [root@localhost ~]# ansible-playbook web\_install.yaml

部署完成之后，购买弹性负载均衡ELB，如图-17



图-17

添加监听器和后端服务器，如图-18、图-19所示。

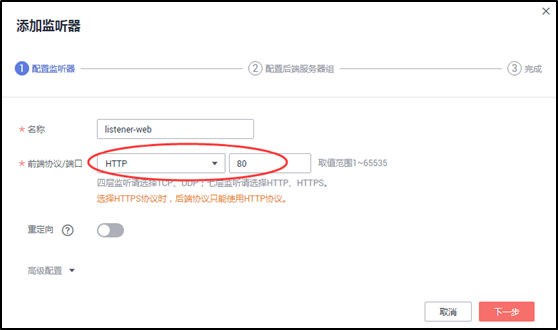


图-18



图-19

绑定公网IP，测试访问，如图-20



拓展：

* 1. 华为云高可用

绑定服务器虚拟ip地址

虚拟私有云—》点进子网—》申请虚拟ip—》绑定服务器与公网ip地址









* 1. 如何获取真实ip地址

Log/access\_log

awk ‘{A[$1++]}END{for （a in A）print A[a],a}’log/access\_log

华为云四层与7层方法如下：

**七层服务**

针对七层（HTTP协议）服务，需要对应用服务器进行配置，然后使用X-Forwarded-For的方式获取来访者的真实IP地址。

真实的来访者IP会被负载均衡放在HTTP头部的X-Forwarded-For字段，格式如下：

X-Forwarded-For: 来访者真实IP, 代理服务器1-IP, 代理服务器2-IP, ...

当使用此方式获取来访者真实IP时，获取的第一个地址就是来访者真实IP。

**配置Apache服务器**

1. 安装Apache 2.4。

例如在CentOS 7.5环境下，可以执行如下命令执行安装：

yum install httpd

1. 修改Apache的配置文件/etc/httpd/conf/httpd.conf，在最末尾添加以下配置信息。
2. LoadModule remoteip\_module modules/mod\_remoteip.so
3. RemoteIPHeader X-Forwarded-For

RemoteIPInternalProxy ***100.125.0.0/16***

图1 修改Apache的配置文件示例图  


说明：

将代理服务器的网段添加到 RemoteIPInternalProxy <IP\_address>，如负载均衡的IP地址段 100.125.0.0/16（100.125.0.0/16 是负载均衡服务保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用逗号分隔。

1. 修改Apache的配置文件/etc/httpd/conf/httpd.conf，将日志输出格式修改为如下所示（%a代表源IP地址）：

LogFormat "***%a*** %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

1. 重启Apache。

service httpd restart

1. 查看httpd的访问日志，您可以获取真实的来访者IP。

**配置Nginx服务器**

1. 运行以下命令安装http\_realip\_module。
2. wget http://nginx.org/download/nginx-1.17.0.tar.gz
3. tar zxvf nginx-1.17.0.tar.gz
4. cd nginx-1.17.0
5. ./configure --user=www --group=www --prefix=/path/server/nginx --with-http\_stub\_status\_module --without-http-cache --with-http\_ssl\_module --with-http\_realip\_module
6. make
7. make install
8. kill -USR2 `cat /path/server/nginx/logs/nginx.pid`

kill -QUIT `cat /path/server/nginx/logs/ nginx.pid.oldbin`

1. 打开nginx.conf文件。

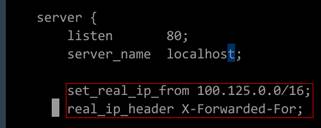
vi /path/server/nginx/conf/nginx.conf

1. 在以下配置信息后添加新的配置字段和信息。

在http或者server处，需要添加的配置字段和信息：

set\_real\_ip\_from ***100.125.0.0/16***;

real\_ip\_header X-Forwarded-For;

图2 添加配置字段和信息示例图  


说明：

将代理服务器的网段添加到 set\_real\_ip\_from <IP\_address>，如负载均衡的IP地址段 100.125.0.0/16（100.125.0.0/16 是负载均衡服务保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用逗号分隔。

1. 重启Nginx。

/path/server/nginx/sbin/nginx -s reload

1. 查看Nginx的访问日志，您可以获取真实的来访者IP。

**配置Windows IIS服务器**

本教程以Windows Server 2012配置IIS7为例介绍，其他版本操作可能略有不同。

1. 下载并安装IIS。

[https://www.microsoft.com/zh-cn/download/confirmation.aspx?id=1038](https://www.microsoft.com/zh-cn/download/confirmation.aspx?id=1038" \t "_blank)

1. 自行下载F5XForwardedFor.dll插件，并根将获取到x86和x64目录下的F5XForwardedFor.dll插件拷贝到IIS服务具有访问权限的目录下，例如C:\F5XForwardedFor2008。
2. 打开IIS管理器，选择“模块 > 配置本机模块”注册拷贝的2个插件。

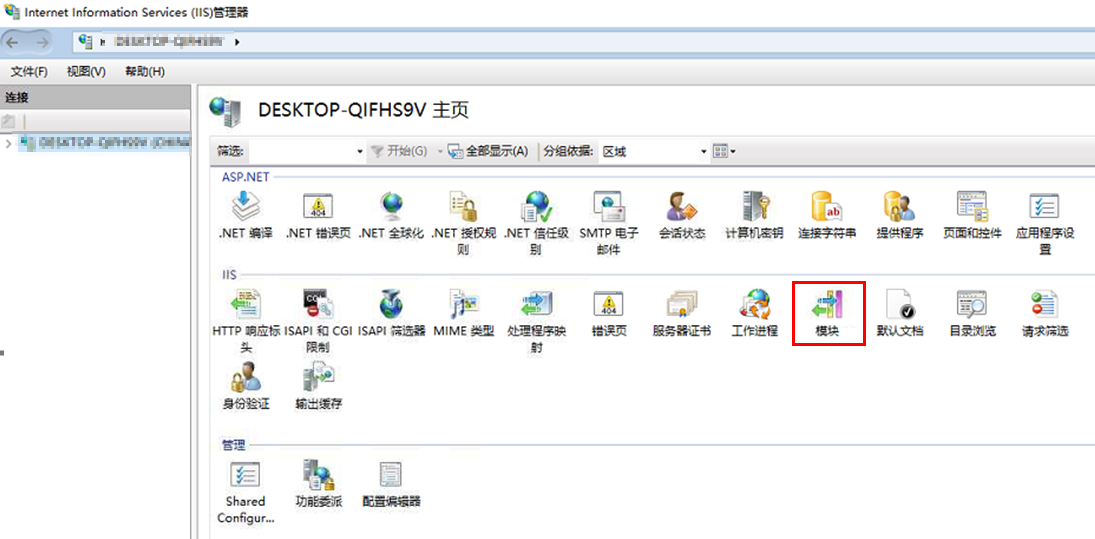
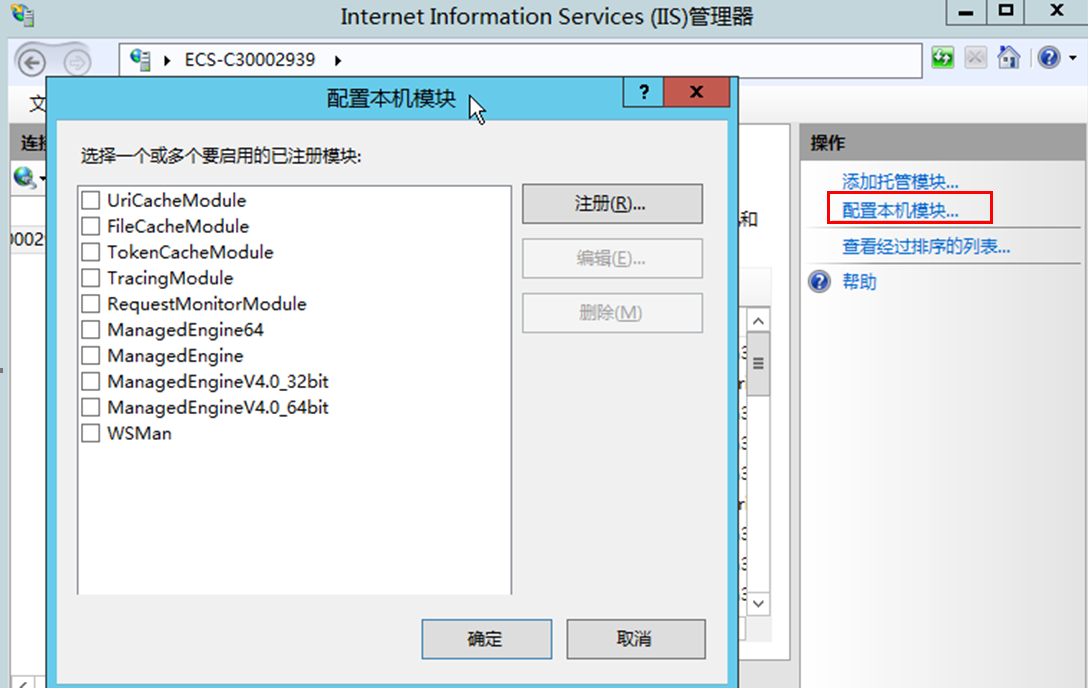
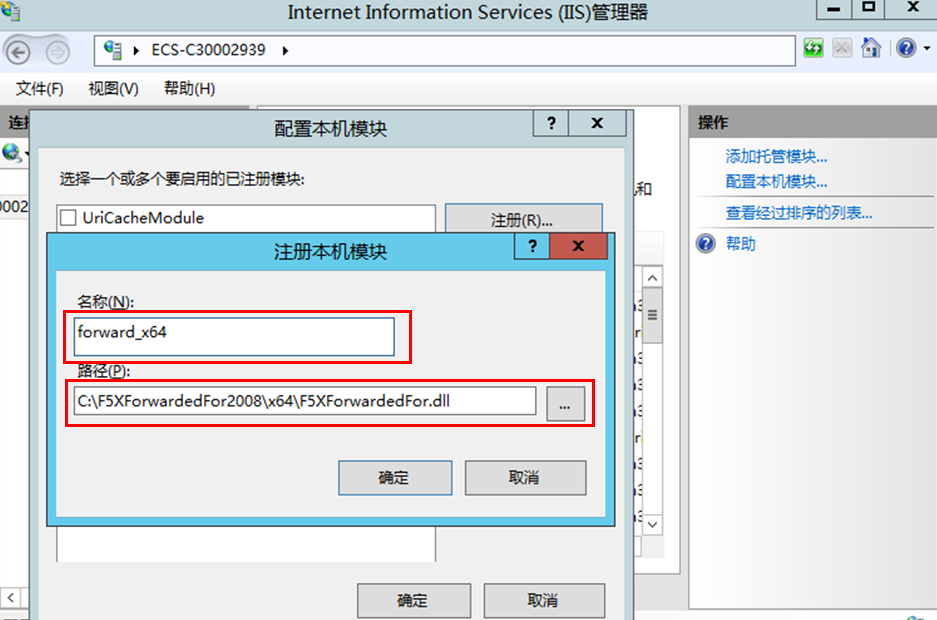
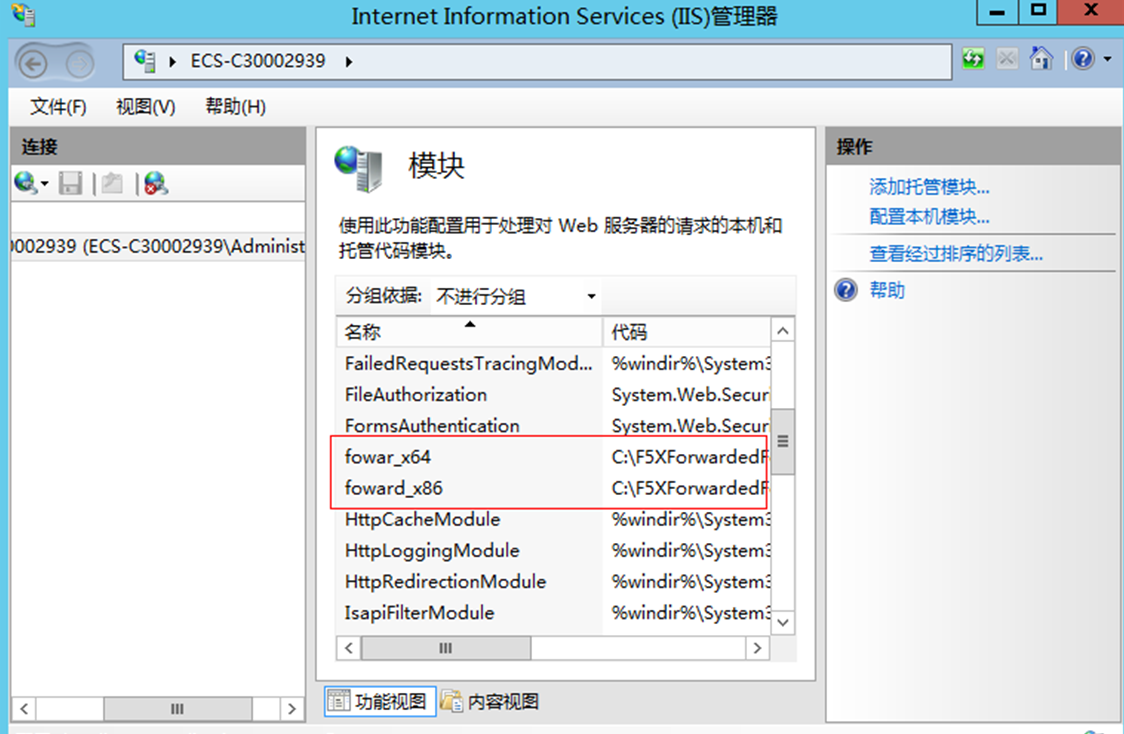
图3 选择模块选项  


图4 配置本机模块  


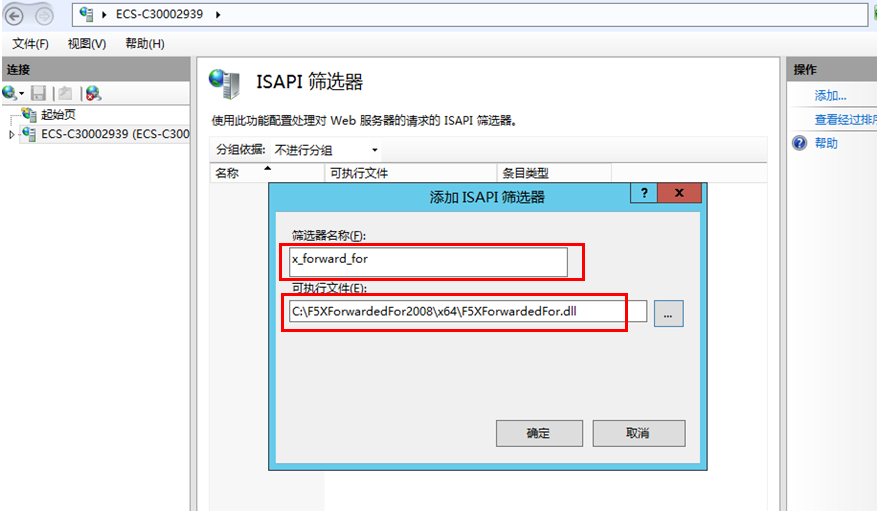
1. 单击“注册”，分别注册x86和x64插件。

图5 注册插件  


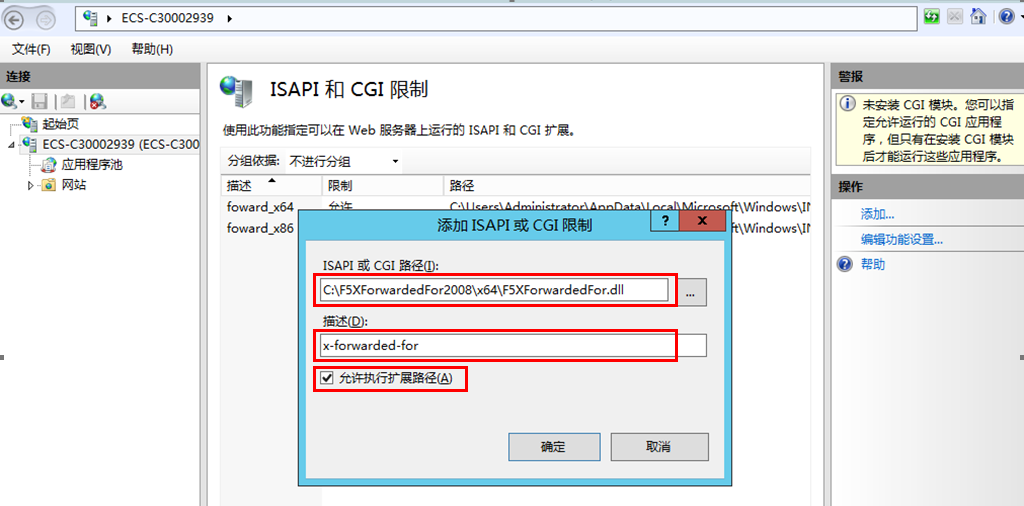
1. 在“模块”页面，确认注册的模块名称出现在列表中。

图6 确认注册成功  


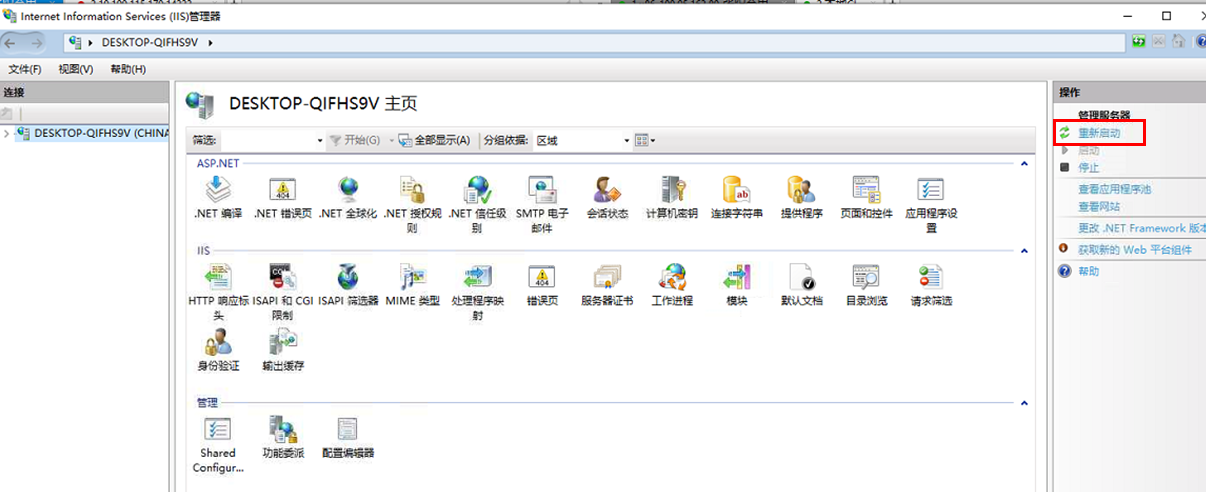
1. 选择IIS管理器主页的“ISAPI筛选器”，为2个插件授权运行ISAPI和CGI扩展。

图7 添加授权  


1. 选择“ISAPI和CGI限制”，为2个插件设置执行权限。

图8 允许执行  


1. 单击主页的“重新启动”，重启IIS服务，重启后配置生效。

图9 重启IIS服务  


**四层服务**

针对四层服务（TPC/UDP协议），有两种方式可以获取客户端的真实IP。

* **方式一（TCP/UDP协议）**：开启监听器的“获取客户端IP”功能。

**注意：**

* + c1，c2，s1，m1，e1，e2，et2，h1，hc1，g1，g2类型的弹性云服务器不支持此功能。
  + 裸金属服务器（BMS）不支持此功能。
  + 开启此功能后，执行后端服务器迁移任务时，可能出现流量中断（例如单向下载、推送类型的流量）。所以后端服务器迁移完成后，需要通过报文重传来恢复流量。
  + 监听器开启此功能后，后端服务器不能作为客户端访问此监听器。
  + 如果监听器之前已经添加了后端服务器、并且开启了健康检查功能，开启“获取客户端IP”功能会重新上线后端服务器，新建流量会有1-2个健康检查周期的中断。
  + 为保证后端服务器能够直接接受客户端IP的访问，请确保放通对应的安全规则，包括后端服务器的安全组、网络ACL、操作系统和软件的安全规则。
  + 开启监听器的“获取客户端IP”功能。
    1. 登录管理控制台。
    2. 在管理控制台左上角单击图标，选择区域和项目。
    3. 选择“服务列表 > 网络 > 弹性负载均衡”。
    4. 在“负载均衡器”界面，单击需要操作的负载均衡名称。
    5. 切换到“监听器”页签。
       - 新增场景：单击“添加监听器”。
       - 修改场景：单击需要修改的监听器名称右侧的。
    6. 开启“获取客户端IP”开关。

图10 开启开关  


* + 设置后端服务器的安全组、网络ACL、操作系统和软件的安全规则，使客户端的IP地址能够访问后端服务器。
* **方式二（TCP协议）**：配置TOA插件获取。

针对四层（TCP协议）服务，需要配置TOA插件获取。需要配置TOA插件获取。配置TOA插件请参考[TOA插件配置](https://support.huaweicloud.com/usermanual-elb/zh_cn_elb_06_0001.html)。