**腾讯专有云**

**网络入侵防护系统（NIPS）**

**部署操作手册**

**文档版本：05**

**发布日期：2021年12月22日**

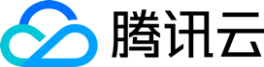
|  |  |
| --- | --- |
| 腾讯云计算（北京）有限责任公司 |  |

**【版权声明】**

本文档著作权归腾讯云计算（北京）有限责任公司（以下简称“腾讯云”）单独所有，未经腾讯云事先书面许可，任何主体不得以任何方式或理由使用本文档，包括但不限于复制、修改、传播、公开、剽窃全部或部分本文档内容。

本文档及其所含内容均属腾讯云内部资料，并且仅供腾讯云指定的主体查看。如果您非经腾讯云授权而获得本文档的全部或部分内容，敬请予以删除，切勿以复制、披露、传播等任何方式使用本文档或其任何内容，亦请切勿依本文档或其任何内容而采取任何行动。

**【商标声明】**

“腾讯”、“腾讯云”及其它腾讯云服务相关的商标、标识等均为腾讯云及其关联公司各自所有。若本文档涉及第三方主体的商标，则应依法由其权利人所有。

**【免责声明】**

本文档旨在向客户介绍本文档撰写时，腾讯云相关产品、服务的当时的整体概况，部分产品或服务在后续可能因技术调整或项目设计等任何原因，导致其服务内容、标准等有所调整。因此，本文档仅供参考，腾讯云不对其准确性、适用性或完整性等做任何保证。您所购买、使用的腾讯云产品、服务的种类、内容、服务标准等，应以您和腾讯云之间签署的合同约定为准，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【修订记录】

| 编号 | 修改日期 | 修改人 | 更新内容 |
| --- | --- | --- | --- |
| 05 | 2021-12-22 | v\_ichzhou | 第3章系统环境、6.6.4章NIPS探针服务器内核版本检查章节内容有更新。 |
| 04 | 2021-12-08 | v\_ichzhou | 新增8.6部署后探针状态排查 |
| 03 | 2021-12-02 | huanxiong | 新增6.1前置处理、6.5挂在/DATA盘 |
| 02 | 2021-06-30 | songafeng | 增加6.1多region多az的处理 |
| 01 | 2021-01-08 | liangxiong | 第一次发布。更新成CSIG标准模板。 |

目 录

[【修订记录】 1](#_Toc91152684)

[目 录 2](#_Toc91152685)

[1 物料 4](#_Toc91152686)

[2 机器资源 5](#_Toc91152687)

[2.1 在CMDB中将主机转移到NIPS云产品业务模块树下 5](#_Toc91152688)

[2.2 云产品业务模块树介绍 5](#_Toc91152689)

[2.3 查找待分配主机 5](#_Toc91152690)

[2.4 分配主机到云产品 6](#_Toc91152691)

[2.5 分配主机到具体业务模块树 7](#_Toc91152692)

[2.6 修改主机业务状态 8](#_Toc91152693)

[3 系统环境 10](#_Toc91152694)

[4 依赖检查 12](#_Toc91152695)

[4.1 支撑检查 12](#_Toc91152696)

[4.2 网络资源依赖 12](#_Toc91152697)

[5 NIPS组网方案 13](#_Toc91152698)

[6 部署 14](#_Toc91152699)

[6.1 前置处理 14](#_Toc91152700)

[6.2 交换机配置 15](#_Toc91152701)

[6.2.1 WC端口规划 15](#_Toc91152702)

[6.2.2 NFVW&NFVL&MA（10G）规划 15](#_Toc91152703)

[6.2.3 MIRROR端口规划 16](#_Toc91152704)

[6.3 prepare\_pkg 16](#_Toc91152705)

[6.4 dcos\_install\_machine 17](#_Toc91152706)

[6.5 挂载/data盘 18](#_Toc91152707)

[6.6 安装前机器配置检查 19](#_Toc91152708)

[6.6.1 NIPS探针网卡配置检查 19](#_Toc91152709)

[6.6.2 NIPS探针网卡路由检查 22](#_Toc91152710)

[6.6.3 NIPS探针服务器端口要求 23](#_Toc91152711)

[6.6.4 NIPS探针服务器内核版本检查 23](#_Toc91152712)

[6.6.5 NIPS服务器DNS和时间服务器检查 23](#_Toc91152713)

[6.6.6 NIPS服务器提前安装软件 24](#_Toc91152714)

[6.7 push\_images 24](#_Toc91152715)

[6.8 update\_config 24](#_Toc91152716)

[6.9 upgrade\_images 25](#_Toc91152717)

[6.10 import\_yunapi 25](#_Toc91152718)

[6.11 install-product-psg 26](#_Toc91152719)

[6.12 安装imgcache组件包 26](#_Toc91152720)

[6.13 import\_dbsq 26](#_Toc91152721)

[7 部署完验证 28](#_Toc91152722)

[7.1 配置NIPS探针出入流量识别配置文件 （所有探针均须操作） 28](#_Toc91152723)

[7.2 检查管控镜像运行状态 29](#_Toc91152724)

[7.3 检查生产组件运行状态 29](#_Toc91152725)

[7.4 检查TCE运营端控制台页面 30](#_Toc91152726)

[7.5 检查策略运行状态 30](#_Toc91152727)

[7.6 OPT交换机到探针镜像流量对账（含出入双向） 31](#_Toc91152728)

[7.7 配置NIPSIDS策略为观察模式 31](#_Toc91152729)

[7.8 事件告警与指标监控 31](#_Toc91152730)

[7.9 NIPS与御界联动配置 31](#_Toc91152731)

[8 附录 33](#_Toc91152732)

[8.1 查看NIPS提供给第三方安全产品阻断API的key密钥 33](#_Toc91152733)

[8.2 NIPS如何新增第三方安全产品对接生产key和密钥 33](#_Toc91152734)

[8.3 NIPS探针平行扩容方案 34](#_Toc91152735)

[8.3.1 交换机扩容配置修改 34](#_Toc91152736)

[8.3.2 NIPS探针服务器扩容部署 35](#_Toc91152737)

[8.4 NIPS基本功能测试验证方案 36](#_Toc91152738)

[8.4.1 管控-全局访问控制 36](#_Toc91152739)

[8.4.2 管控-系统调用规则 42](#_Toc91152740)

[8.5 交换机配置 44](#_Toc91152741)

[8.5.1 WC1-10G配置 44](#_Toc91152742)

[8.5.2 WC2-10G配置 58](#_Toc91152743)

[8.5.3 MIRROR光配置 71](#_Toc91152744)

[8.5.4 NFVW1交换机配置 80](#_Toc91152745)

[8.5.5 NFVW2交换机配置 103](#_Toc91152746)

[8.6 部署常见错误 125](#_Toc91152747)

[8.6.1 生产组件部署常见错误 125](#_Toc91152748)

物料

|  |  |  |
| --- | --- | --- |
| **类别** | **路径** | **物料id** |
| 镜像 | /data/tce\_dc/software/latest/image | ocloud-psg-console  ocloud-psg-console-frontend |
| dbsql | /data/tce\_dc/software/latest/dbsql | dbsql-psg-argus |
| 生产组件 | /data/tce\_dc/software/latest/product | product-psg-ll  product-frontend-imgcache-ocloud-psg |
| yunapi | /data/tce\_dc/software/latest/yunapi | yunapi-psg |
| preset | /data/tce\_dc/software/latest/preset | preset-psg-cam-ocloud-psg |

机器资源

探针（高可用情况下，至少2台物理机），一般情况TCE适配的机型组合如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **平台** | **角色** | **机型** | **数量** | **现有机型配置** |
| v6 | NIPS探针 | DS4-100G | 2台 | 2个24核CPU(8255C), 384G内存, 1\*480G sataSSD, 2\*10GE(电口)，2\*100G(SinglePort(光口)) |

备注：在平行扩容方案中，探针可以继续新增部署，新增探针安装依照下述生产组件安装步骤重新部署完成即可。

在CMDB中将主机转移到NIPS云产品业务模块树下

确定了云产品使用的主机信息后，在实际部署云产品之前，需要在业务CMDB系统中，将主机分配到对应的业务模块树下，以保证业务CMDB记录的资源使用信息和云产品实际使用一致。

云产品业务模块树介绍

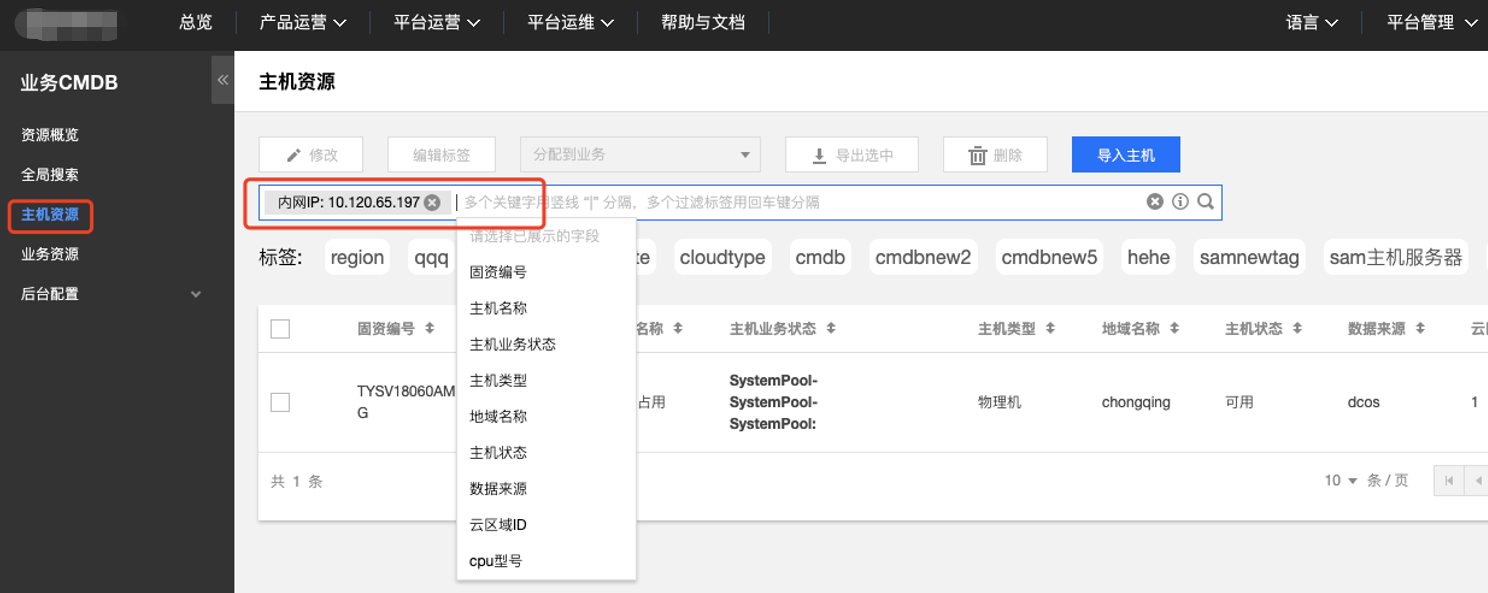
|  |  |  |
| --- | --- | --- |
| **业务** | 集群 | 模块 |
| **NIPS** | mirror | mirror |
| manager | manager |

备注：下述截图仅供参考，请替换为具体的云产品业务业务模块树

查找待分配主机

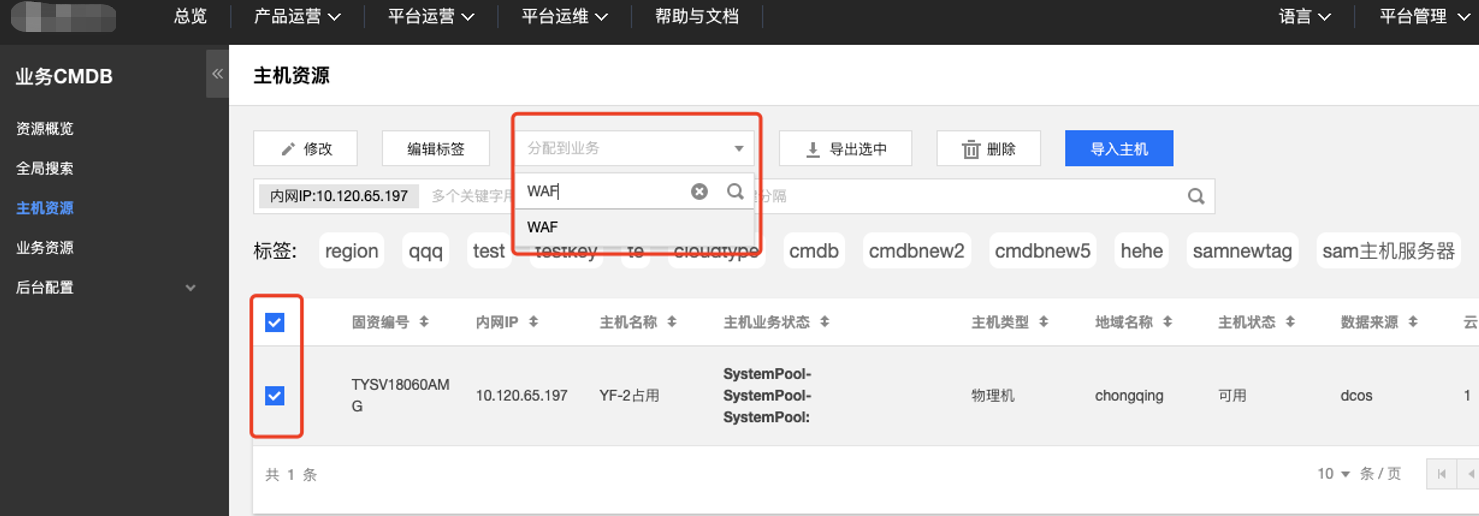


1. 如上图，在TCE运营端控制台，进入业务CMDB系统页面。



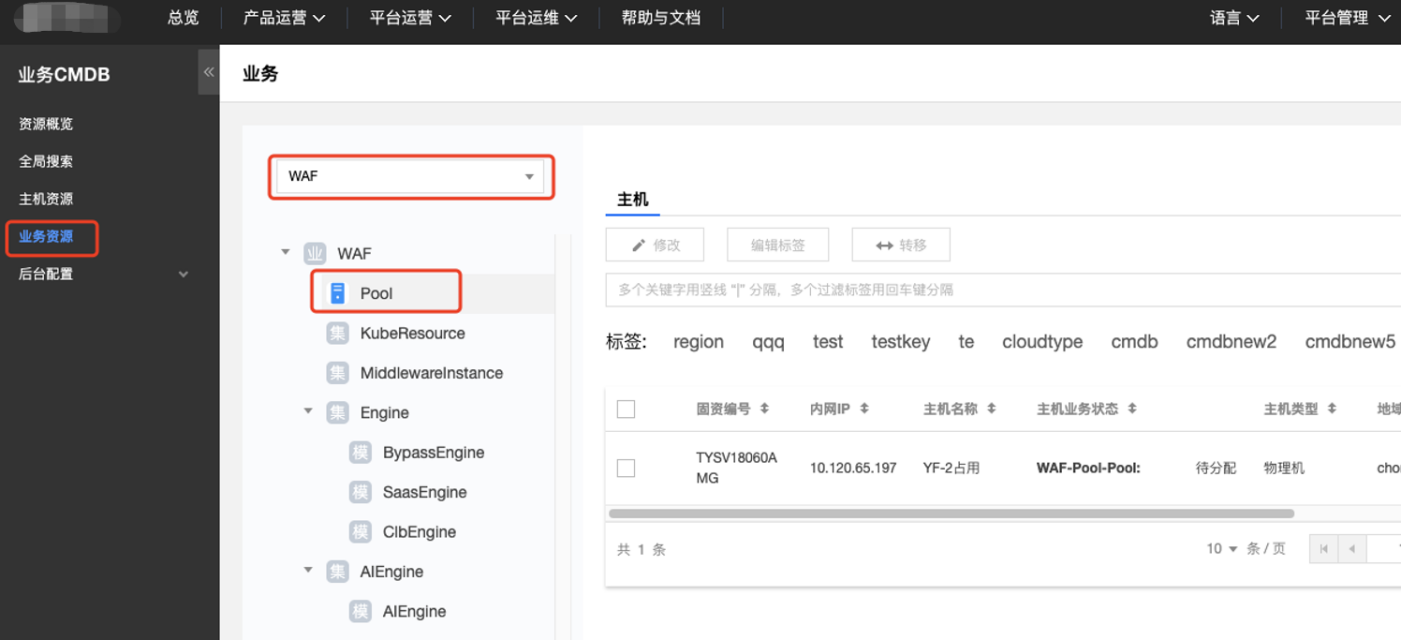
1. 在主机资源页面输入入IP地址查找到分配给云产品的主机信息。

分配主机到云产品

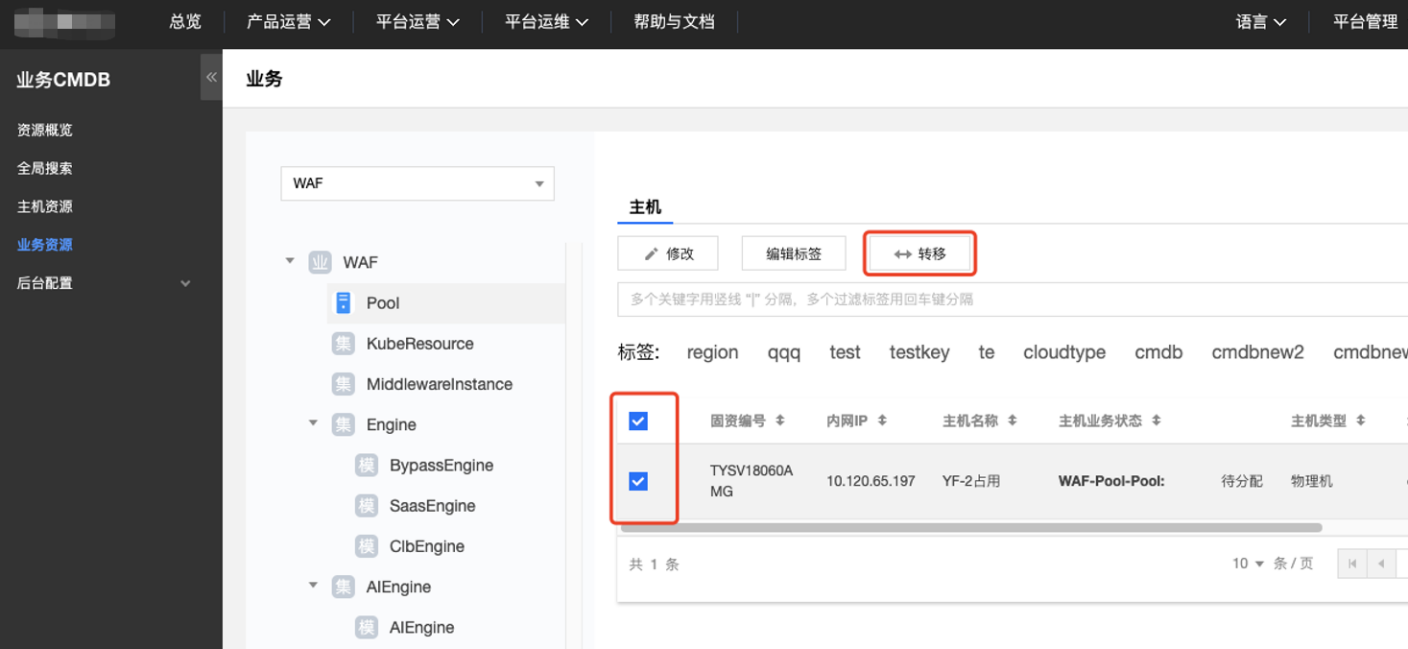


多选待分配主机，然后选择对应的云产品，将此主机分配给云产品。

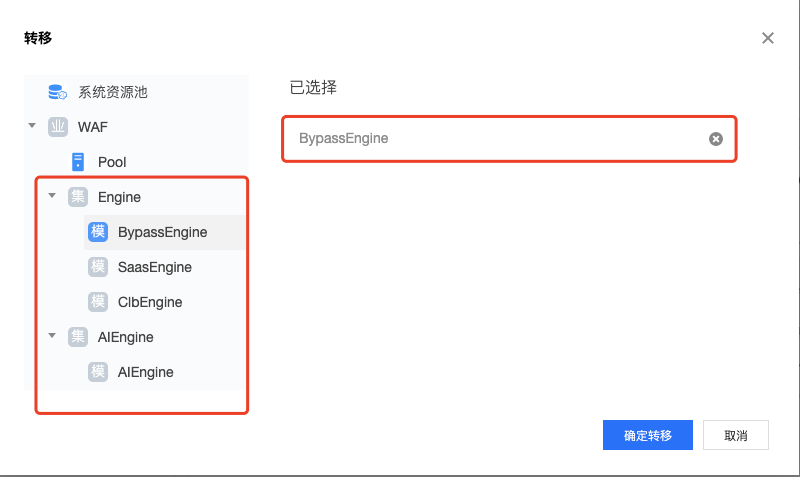
分配主机到具体业务模块树



1. 进入业务页面，选择云产品，进入云产品的资源池模块（上述截图的Pool模块），可以看到刚刚分配给云产品的所有主机。

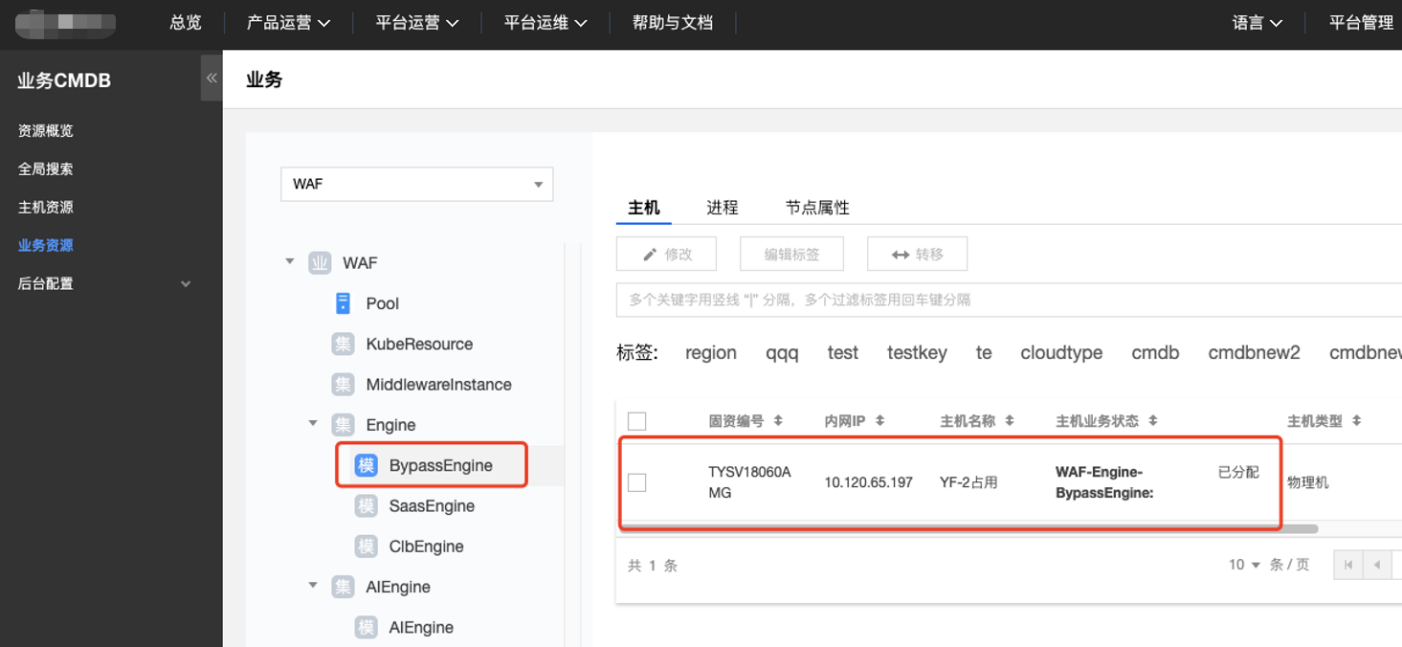


1. 选择待分配的主机（相同业务模块树的主机可多选），然后点击转移按钮。

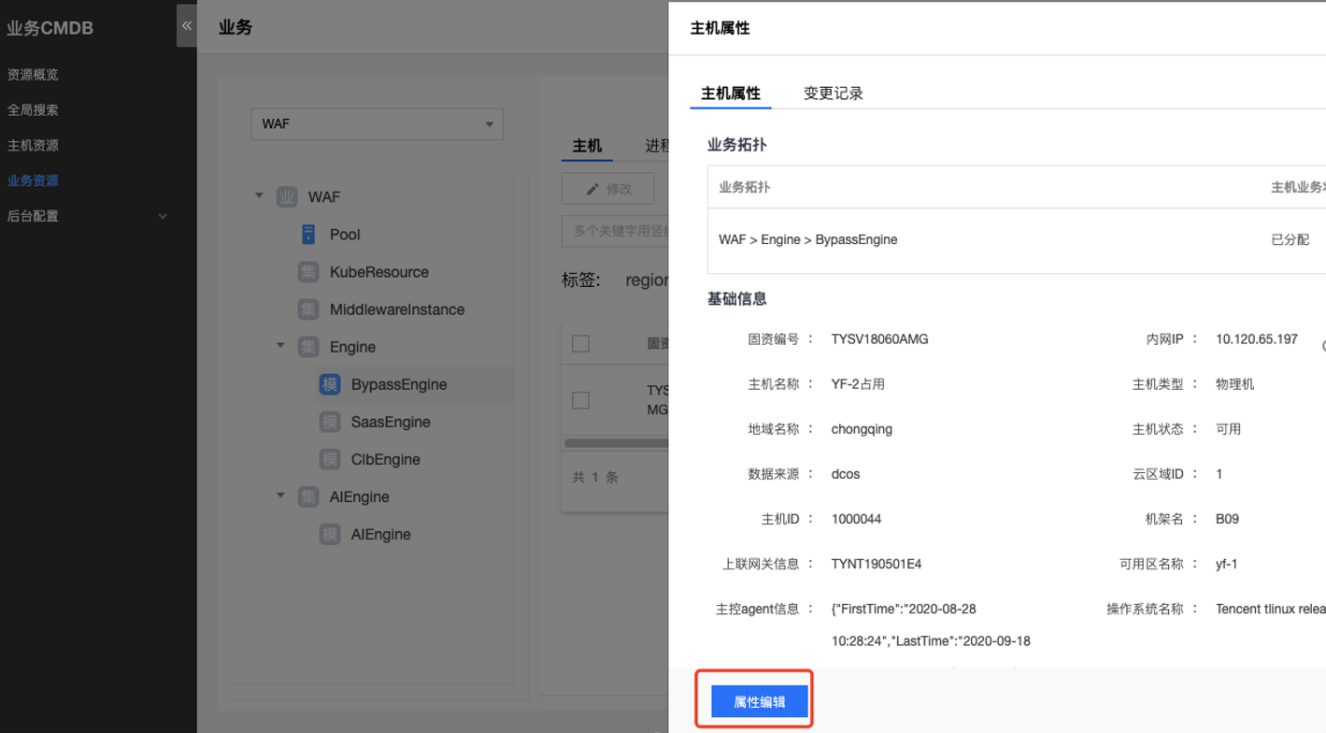


1. 在转移对话框，选择目标的业务模块树（支持多选），在右侧展示当前已经选择模块信息，确认无误后，请点击确认转移。

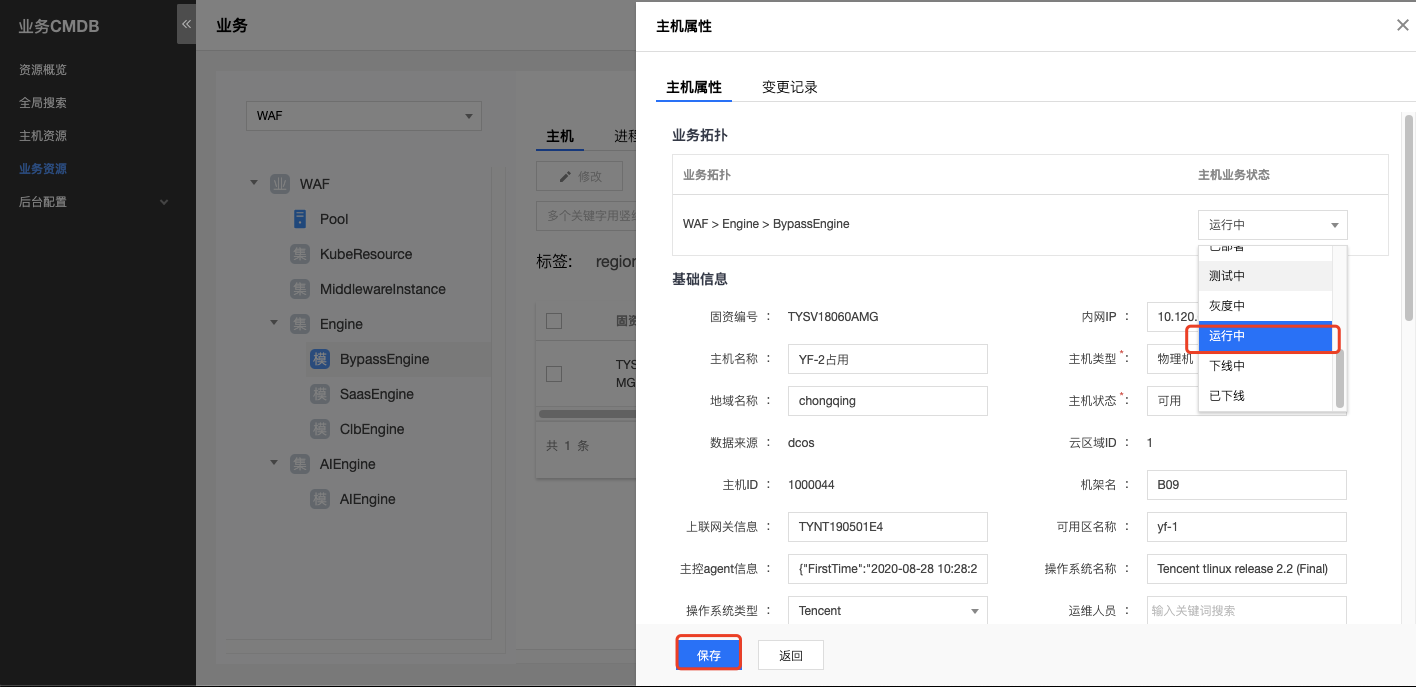
修改主机业务状态



1. 主机分配给业务模块后，点击左侧业务模块，右侧会展示此业务模块下关联的所有主机。



1. 点击右侧主机单元格，弹出主机属性详情页，点击左下角“属性编辑”按钮，进入主机属性编辑页面。



1. 修改此主机业务状态为“运行中”。

系统环境

NIPS探针环境要求

探针内核版本必须是严格匹配，执行

uname -r

检查探针内核版本是否匹配

X86:

|  |  |
| --- | --- |
| **操作系统说明** | - |
| **系统名称** | TencentOS Server 2.2 (TK3) |
| **探针内核版本** | 4.14.105-1-tlinux3-0011 |

1、通过dcos安装TencentOS Server 2.2 (TK3) 0011内核版本的操作系统（x86），如果dcos不支持，需要手动安装，通过带外或者u盘的方式安装系统。

TencentOS Server 2.2 (TK3) iso下载地址: （dcos不支持的情况下，可下载安装）

<https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/tlinux-2.2%20iso/tlinux_4in1_20200106.iso>

TencentOS Server 2.2 (TK3) 内核包下载地址：

<https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/tlinux-2.2%20iso/kernel-tlinux3-4.14.105-1.0011.tl2.x86_64.rpm>

需要使用iso镜像安装系统，然后对系统内核进行降级，降级步骤看下面（2）步骤。

2、检查NIPS两台探针服务器内核版本命令： uname -r 查看内核是否为4.14.105-1-tlinux3-0011。如果不是，请降级内核为0011版本（x86）。 降级步骤如下：

（1）上传kernel-tlinux3-4.14.105-1.0011.tl2.x86\_64.rpm到探针服务器；

（2）内核版本降级安装命令： rpm -ivh kernel-tlinux3-4.14.105-1.0011.tl2.x86\_64.rpm --force

（3）内核版本降级操作完毕后，需重启服务器生效，执行命令: reboot

（4）机器重启完毕后，重新执行命令：uname -r ，观察内部版本是否为4.14.105-1-tlinux3-0011，以确保内核降级成功。

Arm:

|  |  |
| --- | --- |
| **操作系统说明** | 定制化内核版本 |
| **系统名称** | TencentOS Server 2.4 (TK3) |
| **探针内核版本** | 5.4.109-19-0005.xfrm |

5.4.109-19-0005.xfrm 内核包下载地址：

https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/log4j/kernel-5.4.109-19.0005.xfrm.tmanager.tl2.aarch64.rpm

<https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/log4j/kernel-debuginfo-common-5.4.109-19.0005.xfrm.tmanager.tl2.aarch64.rpm>

下载后使用命令安装内核（自动使用新版本内核，重启后生效）：

rpm -ivh kernel-5.4.109-19.0005.xfrm.tmanager.tl2.aarch64.rpm kernel-debuginfo-common-5.4.109-19.0005.xfrm.tmanager.tl2.aarch64.rpm

依赖检查

支撑检查

NIPS目前依赖的TCE支撑组件包括如下： （1）TCE CDB/TDSQL（要求5.6版本或以上，容量要求500G或以上）；（2）CKV+\CRedis；（3）zookeeper；（4）Kafka（1.1.1版本）；（5）ElasticSearch（5.6.4版本，容量要求2T或以上）；（6）ntp时间服务器节点信息。

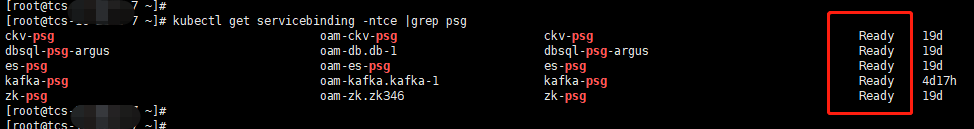
支撑级别：tdsql为region级别，其余都是zone级别

350及以上版本tcs会自动根据服务申明创建支撑实例，无需部署者手动部署。

支撑检查命令如下：

kubectl get servicebinding -ntce |grep psg

如果部署前检查不到实例，不用担心，部署好镜像和生产组件后再检查一遍，确保状态都是ready。



网络资源依赖

* 管理口地址规划

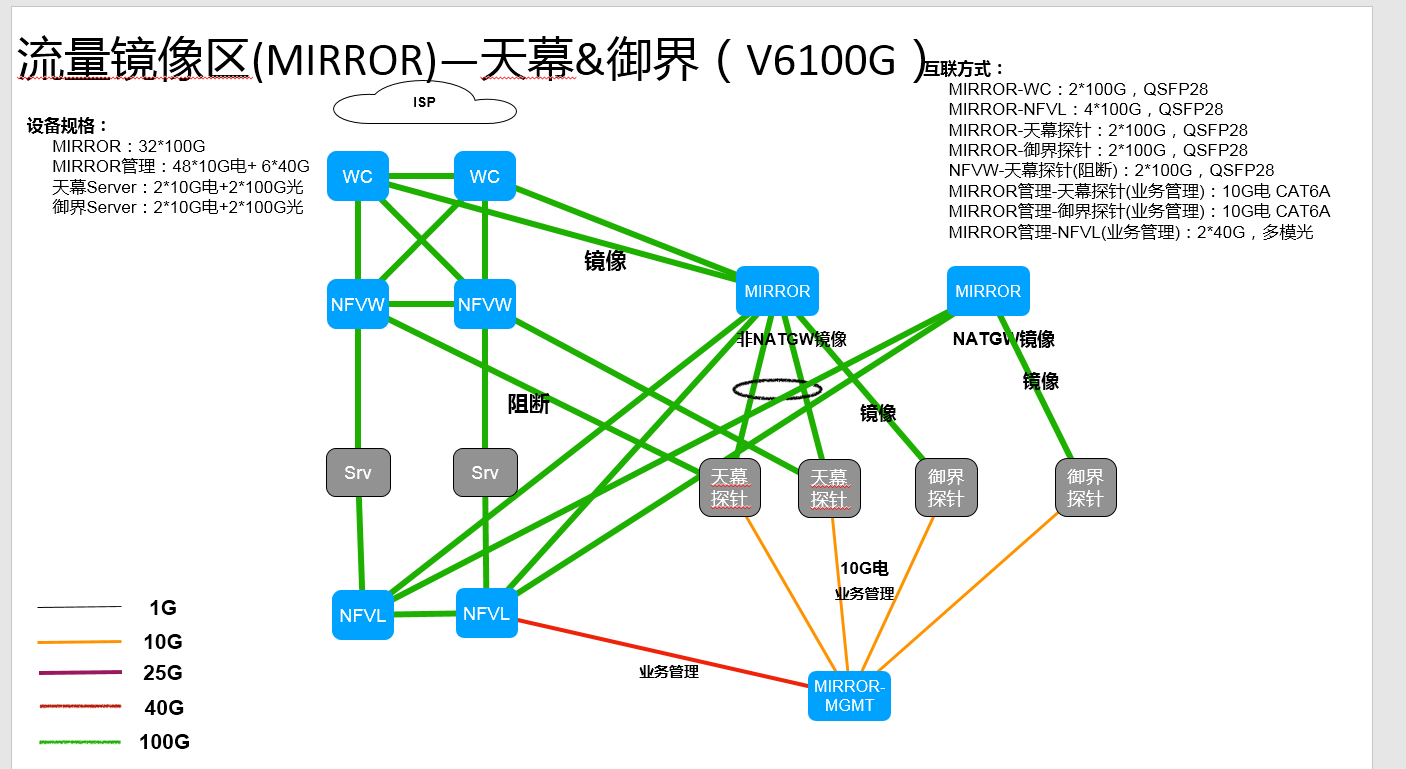
探针管理网口从NFVL-VLAN 263网段分配而来；

* 阻断口地址规划

阻断口地址从NFVW交换机上VLAN/VRF 100~103分配而来，分配地址的同时，需给出GW地址，参考配置如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **探针/阻断IP** | **CT-100** | **CU-101** | **CM-102** | **BGP-103** |
| 10.27.36.135 | 10.27.110.135 | 10.27.111.5 | 10.27.111.135 | 10.27.112.5 |
| GW10.27.83.253 | 10.27.110.129/25 | 10.27.111.1/25 | 10.27.111.129/25 | 10.27.112.1/25 |
| 10.27.36.136 | 10.27.110.136 | 10.27.111.6 | 10.27.111.136 | 10.27.112.6 |
| GW10.27.84.125 | 10.27.110.130/25 | 10.27.111.2/25 | 10.27.111.130/25 | 10.27.112.2/25 |

NIPS组网方案



WC将南北向流量镜像到MIRROR光口交换机，MIRROR光口交换机根据源IP+目的IP作HASH将镜像流量负载均衡转发到NIPS探针服务器镜像口；NFVW给NIPS探针服务器阻断口划分一个单独的VLAN，以实现NIPS伪造的RST包可以直达NFVW，NFVW根据伪造的RST包的目的IP作路由转发实现对外、对内阻断tcp会话链接的效果；NIPS探针管理口直连MIRROR电1，MIRROR电1连接NFVL以实现业务管理（包括跟TCE支撑组件通信）。 NIPS探针支持平行扩容。

部署

前置处理

背景：由于客户对TCE架构需求不一，为满足不同场景下，天幕交付兼容性部署，特提供灵活处理方案如下：

1、单region单az、单region多az场景：参考文档部署即可。

2、单region多az部署（部分az不部署）场景：

（2.1）只剩余1个az场景下：登录天幕数据库实例，对dw\_soc\_threat\_data\_region1\_az1 ~az5 里面的region\_config进行部分记录delete删除，只保留主az的那一条记录，在对应主az区域进行天幕控制台ocloud-psg-console 和 ocloud-psg-console-frontend 容器拉起部署；

（2.2）剩余多个az场景下：登录天幕数据库实例，对dw\_soc\_threat\_data\_region1\_az1 ~az5 里面的region\_config进行部分记录delete删除，只保留主az和需要实际部署az的多条记录，在对应az区域进行天幕控制台ocloud-psg-console 和 ocloud-psg-console-frontend 容器拉起部署；

3、多region多az场景下：

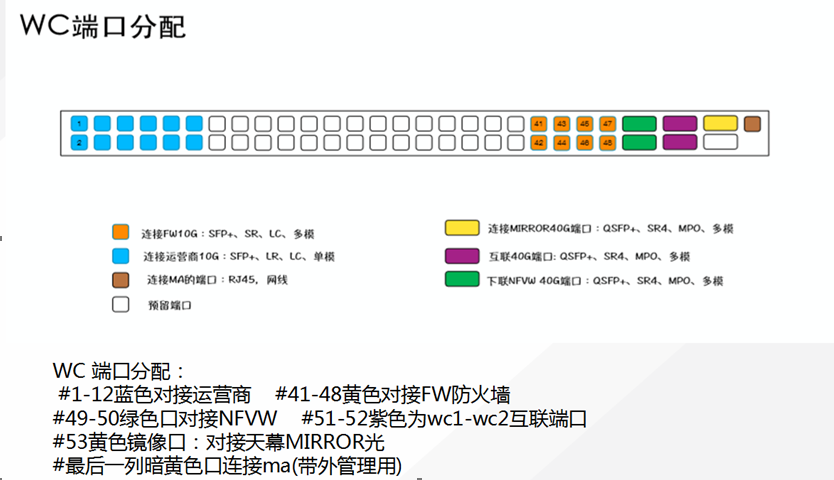
（3.1）只在主region主az部署天幕控制台ocloud-psg-console 和 ocloud-psg-console-frontend，在主region主az的tcs master 部署探针的时候，统一输入多个region多个az的探针IP列表来统一管控。

（3.2）登录天幕数据库实例，对dw\_soc\_threat\_data\_region1\_az1 ~az5 里面的region\_config进行部分记录delete删除，只保留主az的那条记录，其余全部删除掉；在对应主az区域进行天幕控制台ocloud-psg-console 和 ocloud-psg-console-frontend 容器拉起部署；

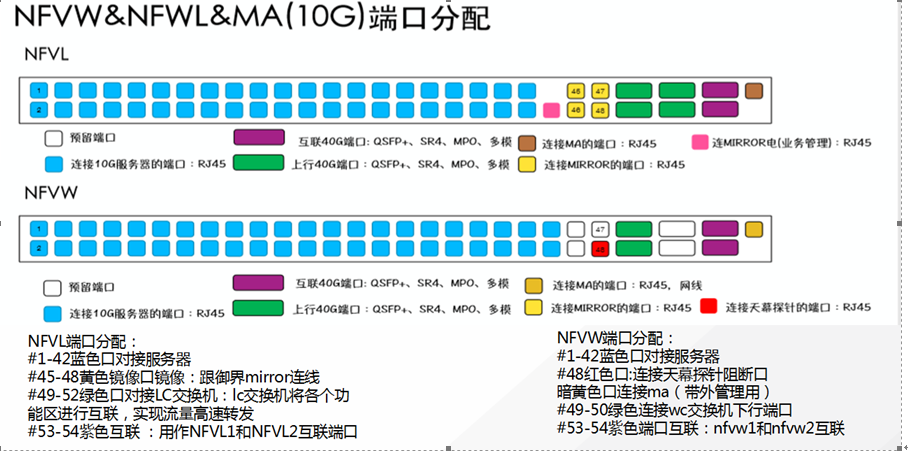
（3.3）在product-psg-ll 生产组件的config/mul\_deploy.conf 配置文件对应的psg\_host 里面填写多个region多个az的IP信息。

交换机配置

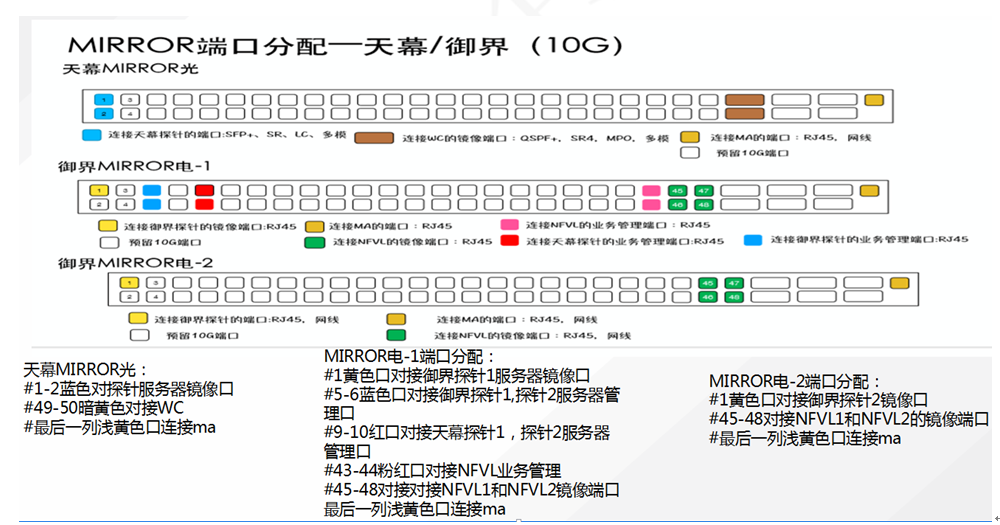
WC端口规划



NFVW&NFVL&MA（10G）规划



MIRROR端口规划



**交换机详细配置**

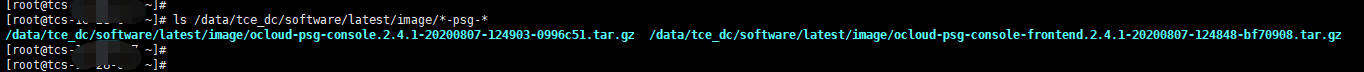
因交换机配置命令较多，与NIPS相关的交换机有wc1，wc2，nfvw1，nfvw2，mirror光，具体配置放到附录交换机配置

prepare\_pkg

1. 镜像包检查

ls /data/tce\_dc/software/latest/image/\*-psg-\*

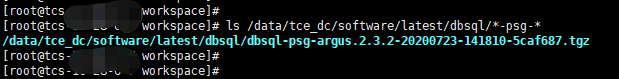
希望结果：



1. dbsql包检查

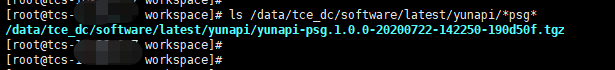
ls /data/tce\_dc/software/latest/dbsql/\*-psg-\*

希望结果：



1. yunapi包检查

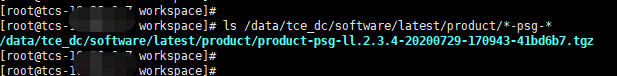
ls /data/tce\_dc/software/latest/yunapi/\*psg\*



1. 生产组件包检查

ls /data/tce\_dc/software/latest/product/\*-psg-\*

希望结果：



dcos\_install\_machine

操作对象

|  |  |  |  |
| --- | --- | --- | --- |
| **组件** | **ip** | **固资** | **dcos安装配置** |
| NIPS探针 | 以环境分配的为准 | 以环境分配的为准 | 系统参见3章节  网络方案不需要bond，NORAID  监控Agent：默认安装 |

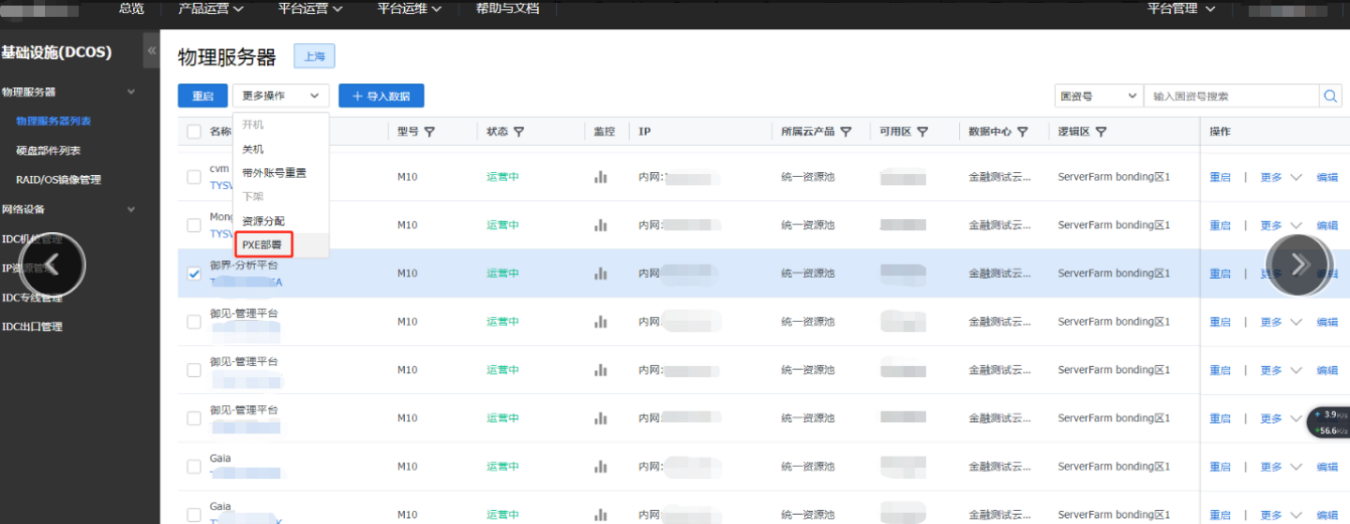
执行装机

登入运营端DCOS页面

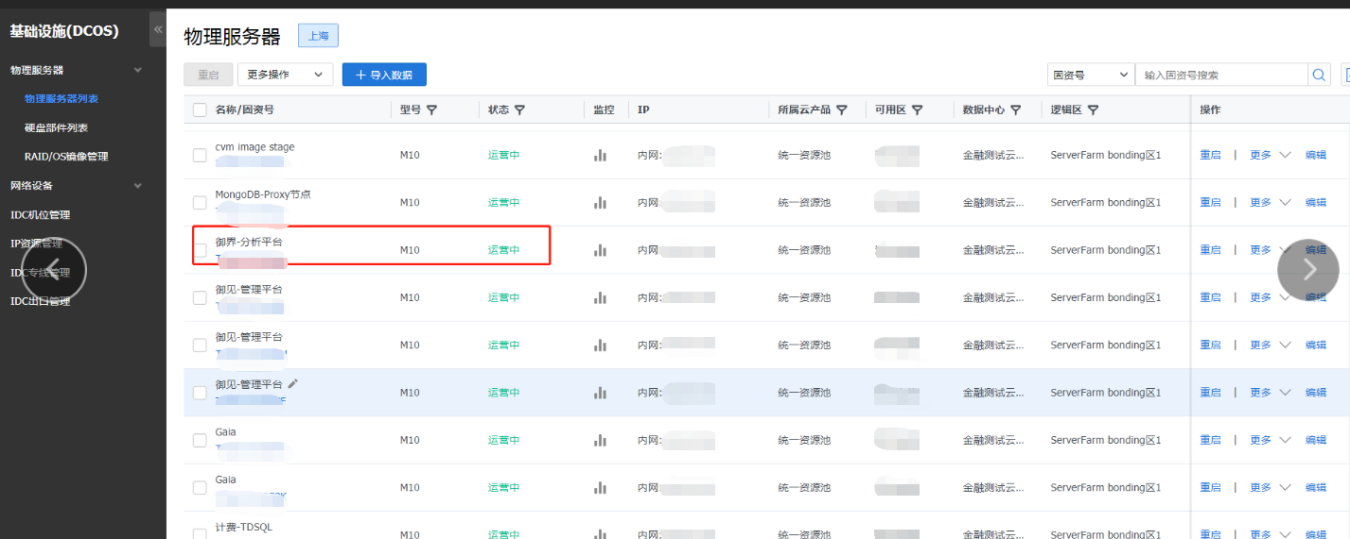
按固资号找到物理机器执行PXE装机选项安装系统

如果带外账号不正常，尝试重置带外账号，未解决则找网络（机房）同学解决





装完系统后看机器状态是否是运营中，ssh能远程登录机器.



挂载/data盘

ssh到机器执行

1. fdisk -l ，此处以/dev/vdb为例，部署时请根据实际情况选择合适的盘。
2. mkfs.ext4 /dev/vdb
3. mount /dev/vdb /data
4. 并写入/etc/fstab中，写入后重启CVM保证fstab可以正常加载
5. df -h查看是否挂载成功

Text

Description automatically generated

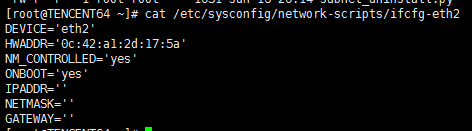
安装前机器配置检查

NIPS探针网卡配置检查

1、NIPS探针服务器的带内管理口接线必须要绑定在eth1口（即要求管理IP配置在eth1）、阻断口接线必须要绑定在eth0口（即阻断口IP配置在eth0.xxx，由于350版本以后存在三网合一的需求，因此需要针对不同的运营商出口增加不同的vlan子接口）。请提前记录好2台探针服务器的管理口IP以及网关地址、2台探针服务器的阻断口IP以及网关地址（每个运营商对应一个vlan子接口）。

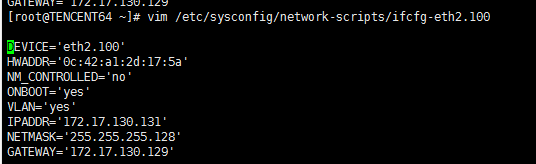
2、检查探针网卡配置文件方法如下： （截图示例以eth2为阻断口）

vim /etc/sysconfig/network-scripts/ifcfg-eth0  （阻断口配置）



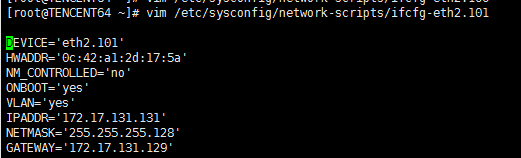
ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， IP\_ADDR、NETMASK、GATEWAY无需填写。

vim /etc/sysconfig/network-scripts/ifcfg-eth0.100  （vlan为100的阻断子接口配置）



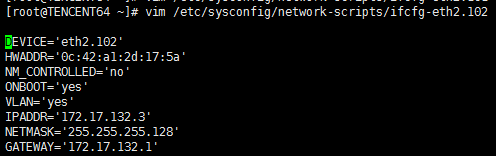
ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， DEVICE字段设置为对应的eth0.100，NM\_CONTROLLED设置为no, VLAN字段为yes，HWADDR地址保持跟eth0的HWADDR地址一致，IP\_ADDR、NETMASK、GATEWAY根据客户实际情况填写（必须填写）；

vim /etc/sysconfig/network-scripts/ifcfg-eth0.101  （vlan为101的阻断子接口配置）



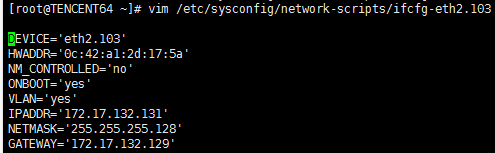
ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， DEVICE字段设置为对应的eth0.101，NM\_CONTROLLED设置为no, VLAN字段为yes，HWADDR地址保持跟eth0的HWADDR地址一致，IP\_ADDR、NETMASK、GATEWAY根据客户实际情况填写（必须填写）；

vim /etc/sysconfig/network-scripts/ifcfg-eth0.102  （vlan为102的阻断子接口配置）



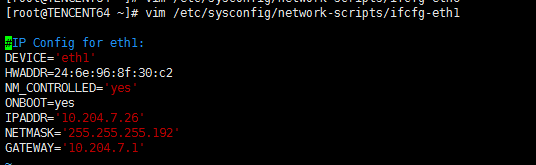
ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， DEVICE字段设置为对应的eth0.102，NM\_CONTROLLED设置为no, VLAN字段为yes，HWADDR地址保持跟eth0的HWADDR地址一致，IP\_ADDR、NETMASK、GATEWAY根据客户实际情况填写（必须填写）；

vim /etc/sysconfig/network-scripts/ifcfg-eth0.103  （vlan为103的阻断子接口配置）



ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， DEVICE字段设置为对应的eth0.103，NM\_CONTROLLED设置为no, VLAN字段为yes，HWADDR地址保持跟eth0的HWADDR地址一致，IP\_ADDR、NETMASK、GATEWAY根据客户实际情况填写（必须填写）；

vim /etc/sysconfig/net work-scripts/ifcfg-eth1 （带内管理口配置）



ONBOOT 字段必须设为yes（保证开机启动网卡正常启动）， IP\_ADDR、NETMASK、GATEWAY根据客户实际情况填写（必须填写）；

vim /etc/sysconfig/network-scripts/ifcfg-eth2  （镜像口配置）

vim /etc/sysconfig/network-scripts/ifcfg-eth3  （镜像口配置）

ONBOOT 字段必须设为yes（保证开机启动网卡正常启动），镜像口默认无需配置IP信息。

**探针策略路由添加**：（**重要**，参考示例如下）



以10.2.50.133这台探针为例，那么我们给探针添加的策略路由命令是：

python subnet\_install.py eth0 10010.2.130.131 25 10.2.130.129 101 10.2.131.131 25 10.2.131.129 102 10.2.132.3 2510.2.132.1 103 10.2.132.131 25 10.2.132.129

 其中,eth0代表阻断口网口；100、101、102、103代表各运营商映射的阻断网段vlan id；10.2.130.131、10.2.131.131、10.2.132.3、10.2.132.131代表分配给天幕的阻断vlan子接口的ip地址；25代表掩码位，10.2.130.129、10.2.131.129、10.2.132.1、10.2.132.129代表分配给天幕的阻断vlan子接口的ip网关。

**删除策略路由的命令**：（应急备用）

  python subnet\_uninstall.py eth0 100 101 102 103

其中，eth0代表阻断口网口;100、101、102、103代表各运营商映射的阻断网段vlan id。

subnet\_install.py和subnet\_uninstall.py脚本下载链接：

<https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/subnet/subnet_install.py>

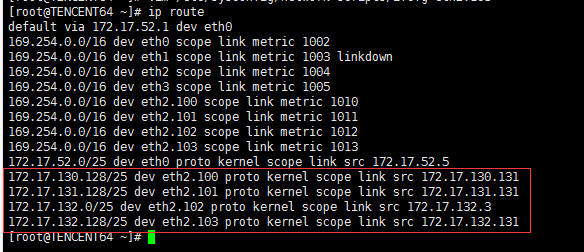
<https://tianmu-1258877907.cos.ap-chengdu.myqcloud.com/TIANMU-release/subnet/subnet_uninstall.py>

NIPS探针网卡路由检查

1. 通过ping命令检查是否可以ping通带内管理口网关，通过ping命令检查是否可以ping通每个vlan子接口对应阻断口网关，通过ping命令检查探针服务器之间的带内管理口是否可以互相ping通。
2. 在探针服务器分别执行命令：ethtool eth0、ethtool eth1、ethtool eth2、ethtool eth3检查Link detected 状态是否为yes。如果Link detected状态为no，可以使用命令ifconfig ethX up来开启；如果执行ifconfig ethX up后，运行ethtool ethX依然显示Link detected 状态为no，则需要进一步检查服务器物理接线是否正常接上（例如接触不良等）。
3. NIPS探针默认路由指向带内管理口（eth1）的网关。

在两台探针服务器分别检查路由指向，执行命令：route -n，默认路由指向带内管理口网关，目的是通过跳板机实现探针服务器SSH登录管理、与NIPS依赖TCE的支撑组件实现网络通信（NIPS具体依赖的TCE支撑组件清单请查阅上述1.1节，**特别需要提醒的是，NIPS探针对时间敏感，必须要保证探针与ntp时间服务器ip网段可通便于及时同步更新时间**）。

在两台探针服务器分别检查路由指向，执行命令：ip route，确认是否存在如下信息。



在两台探针服务器分别检查路由指向，执行命令：ip rule，确认是否存在如下信息。



NIPS探针服务器端口要求

NIPS探针服务器需要对外开放的端口号包括：80/36000/56000。其中，80是主要预留用于http接口服务，36000/56000主要是用于SSH登录管理，36000/56000开通其中一个即可，优先使用36000端口。

其余端口是TCE支撑组件和NIPS探针服务器之间内部互访的，探针服务器iptables配置默认已经做好内部放开。

NIPS探针服务器内核版本检查

执行命令：uname -r 检查是否匹配目录3 系统环境。

如果不匹配必须执行3 系统环境要求，升降级内核版本到指定版本号。

NIPS服务器DNS和时间服务器检查

1、DNS

TCE环境有内部的DNS地址，需要确认在新安装的NIPS服务器上已完成正确的配置，查看执行命令：

cat /etc/resolv.conf

显示类似nameserverxxx.xxx.xxx.xxx (xxx为DNS服务器地址)

如果NIPS2台探针服务器的/etc/resolv.conf文件为空或者与TCE 内部的DNS地址不符，请对该文件添加/修改为TCE的内部DNS地址。

2、ntp时间服务器

NIPS2台探针服务器在作生产组件部署时，默认会读取TCE 配置中心的时间服务器IP地址，因此无需作特殊配置操作。

NIPS服务器提前安装软件

1. TK

yum install -y tk

push\_images

1. 操作步骤

kaleido\_image load /data/tce\_dc/software/latest/image --filter psg

1. check

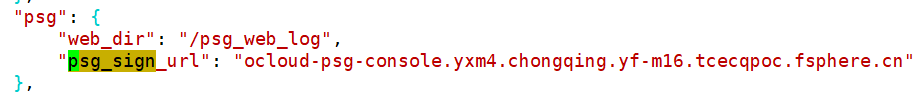
# 脚本输出未push成功的镜像，无输出表示全部push到仓库

kaleido\_image check push /data/tce\_dc/software/latest/yaml psg

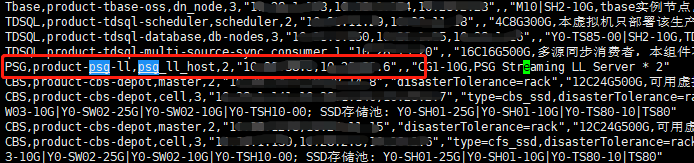
update\_config

1. 修改私有变量/data/tce\_dc/config/self/private.json：

修改psg\_sign\_url变量，将PSG对第三方提供的阻断服务的签名服务修改为当前环境的域名信息，默认为"ll.psg.yun.ccb.com";



1. 根据规划将生产节点ip添加到/data/tce\_dc/config/self/iplist.csv 。添加方法：根据产品名，组件ID，模块/地址组名称找到对应行，将ip添加到“分配IP（逗号分割）”列



1. 生成iplist.env

$ kaleido\_refresh iplist

刷新配置

cd /data/tce\_dc/software/latest/image

ls \*-**psg**-\* | grep -oP '^[^.]+' > /tmp/**psg**.list

kaleido config update /tmp/**psg**.list

1. 将配置包中的文件合并到/data/tce\_dc/config/目录中，执行以下命令：

kaleido\_config update --prepare

upgrade\_images

1. 操作步骤

# 拉起镜像并开启健康检查

kaleido\_image upgrade --yaml /data/tce\_dc/software/latest/yaml/ --filter psg

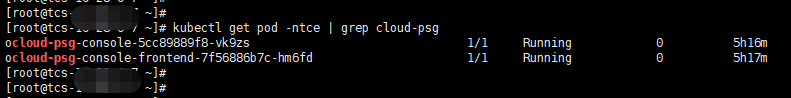
1. check

检查镜像拉起状态

# 查看已拉起镜像状态，pod状态为Running

kubectl get pod -ntce | grep cloud-psg

希望结果:



import\_yunapi

kaleido\_yunapi update yunapi-psg

install-product-psg

1. 解压组件包并渲染：

kaleido\_product install product-psg-ll --action=trender

1. 检查配置文件：

Cat /data/tce\_dc/workspace/product-psg-ll/config/mul\_deploy.conf | grep psg\_host

返回:  psg\_host=（这里应该出现两台探针的ip） 说明无误，继续往下执行

备注：必须先检查支撑组件域名联通性才可执行生产组件部署：

登录生产组件：**错误!超链接引用无效。**配置文件中渲染出的 zk，es，ckv，kafka对应的域名**错误!超链接引用无效。**，确认可达后才能进行生产组件的deploy；

1. 部署 product-psg-ll：

kaleido\_product install product-psg-ll --action=deploy

等待NIPS探针生产节点执行软件服务安装，当探针服务器安装完软件服务后会执行自动reboot重启操作（时间约5~10分钟左右），必须等到机器重启完毕后再执行下面操作。

1. 安装后服务检查和IDS策略导入命令：

cd /data/tce\_dc/workspace/product-psg-ll/TCE; sh allocate.sh

备注：如果导入失败，可以重复执行多次安装直到成功为止。

安装imgcache组件包

从380版本开始，imgcache组件由每个产品单独部署；

kaleido\_product install /data/tce\_dc/software/latest/product/product-frontend-imgcache-ocloud-psg\*

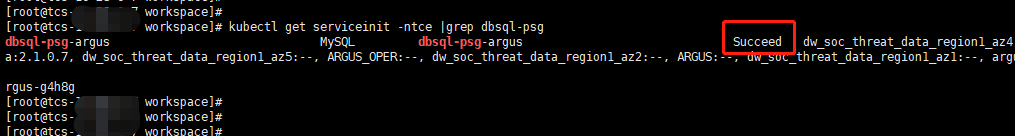
import\_dbsq

350在采用tcs底座之后会按照组件的依赖申明自动刷dbsql，也就是说在拉起镜像或者部署生产组件的时候如果有依赖dbsql的会自动刷好dbsql。

我们需要做的是先检查dbsql有没刷好

可以执行以下命令查看，状态为Succeed即为刷成功了

kubectl get serviceinit -ntce |grep dbsql-psg



如果出现其他的状态，如Error则表示刷失败了。

重刷的命令如下

kaleido\_dbsql update dbsql-psg-argus

附：[刷dbsql失败排查办法](http://tapd.oa.com/OneBank/markdown_wikis/view/)

部署完验证

配置NIPS探针出入流量识别配置文件 （所有探针均须操作）

1. 在每台探针服务器上操作识别出流量的配置文件的配置，主要是提供给RecvServer服务使用。

注：此配置文件用于识别出入流量，如置空或配置不当，会导致镜像流量中的出方向流量误判作入方向流量处理，直接影响NIPSIDS策略执行（如FTP爆破检测逻辑无法工作等）。可联系TCE网络规划人员获取所有TCE云平台对外出口IP网段列表。

vi/home/oicq/argus/RecvServer/conf/local\_ip\_net.conf

把TCE云平台对外出口IP网段列表全部添加进去，例如：

10.27.3.182/32

10.27.3.183/32

10.27.3.181/32

10.27.2.0/24

特别注意：如果是单个ip，也要带上/32的掩码；如果是子网段，需要带上对应的/xx的掩码位，而且每一行末尾不能留有空格等特殊符号，否则RecvServer服务无法正常启动。

1. 由于TCE网络架构中，WC和NFVW划分给天幕的vlan id不是相同的关系，那么需要对WC 和NFVW的vlan id作映射配置。举个例子，假如对于移动运营商， WC镜像给天幕探针流量的vlan id 是200， NFVW 给天幕阻断口的vlan id 是100，那么需要在每台探针的配置文件补充：

vim /home/oicq/argus/RecvServer/conf/flow\_label.conf

每行4个值：wc\_vlan\_tag\_in,nfvw\_vlan\_tag\_out,0,2

即：

200,100,0,2

201,101,0,2

202,102,0,2

203,103,0,2

1. 添加完出口IP网段清单和vlan映射关系在配置文件后，需重启服务：

cd /home/oicq/argus/RecvServer/scripts;sh svr.sh restart

1. 确认RecvServer服务正常启动，执行命令：

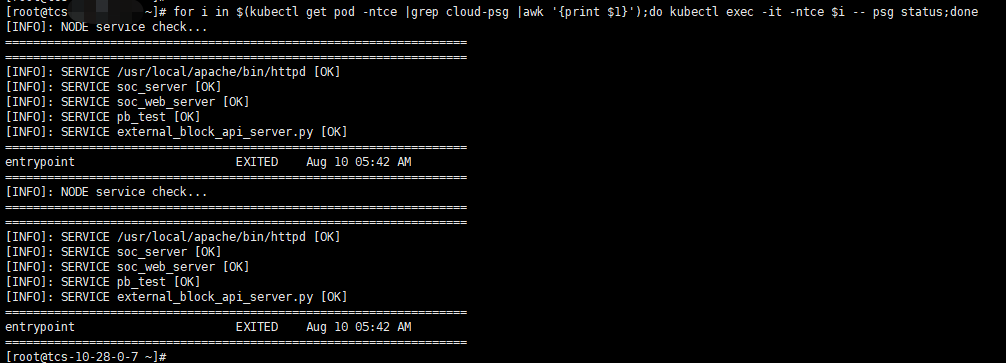
ps -elf |grep RecvServer

检查管控镜像运行状态

以下步骤在TCE部署机执行：

for i in $(kubectl get pod -ntce |grep cloud-psg |awk '{print $1}');do kubectl exec -it -ntce $i -- psg status;done

全部返回【OK】状态



检查生产组件运行状态

ssh 分别登录2台NIPS探针服务器，执行命令： psg status，检查是否为ok状态

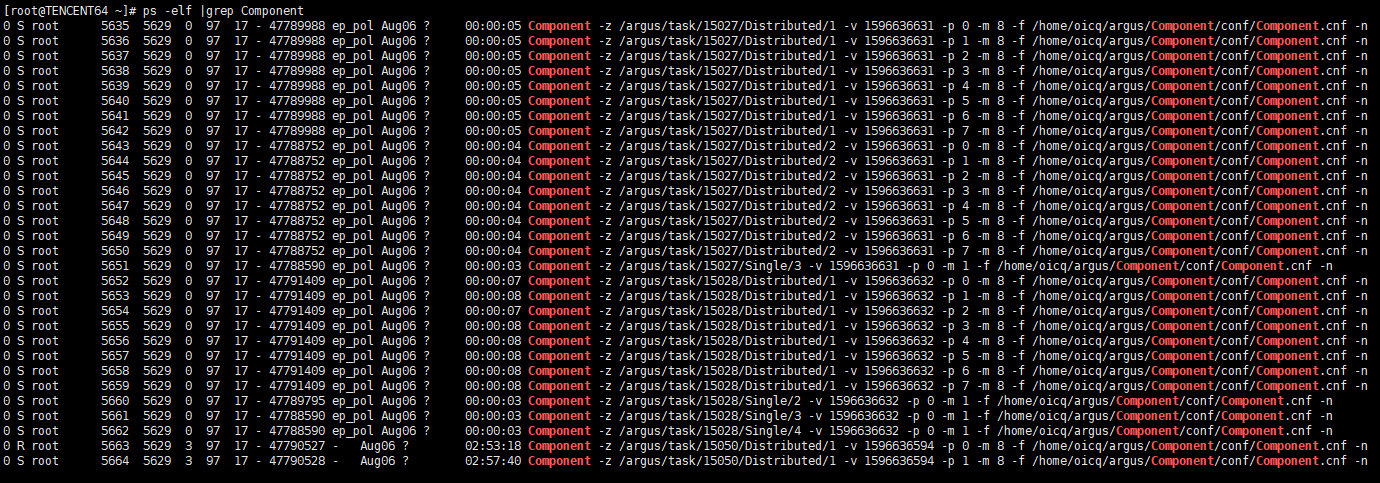


检查TCE运营端控制台页面

登录TCE运营端（cmgt），从运营端页面点击进入NIPS控制台，点击总览、报表、其他管控等入口，查看各个页面展示是否有异常，如无异常报错返回即可。

检查策略运行状态

确认策略是否导入正常，执行命令：ps -elf |grep Component，有进程存活则证明导入正常。

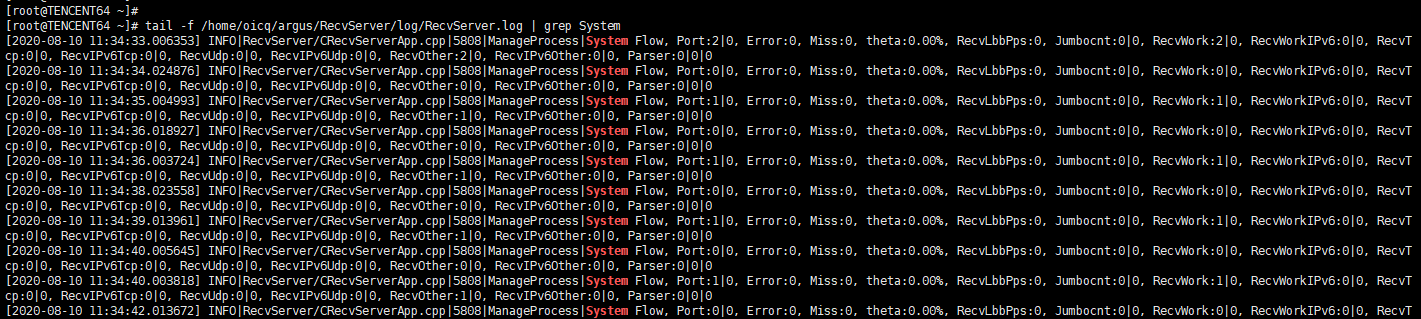


OPT交换机到探针镜像流量对账（含出入双向）

ssh登录各台NIPS探针服务器，执行命令：

tail -f /home/oicq/argus/RecvServer/log/RecvServer.log| grep System

关注关键字：Flow,Port:2462929|9069 ， 其中2462929 这一列指的是出入双方向每秒总包量（单位：个），9069这一列指的是出入双方向每秒总流量（单位：Mbps）



根据上述两个字段，与客户驻场网络工程师作出入双方向流量对账，建议抽样5~10个时间点作对比，抽样结果一致即可，如不一致，请联系客户驻场网络工程师再次确认是否已将出入双向流量转发至NIPS探针服务器

配置NIPSIDS策略为观察模式

NIPS部署完毕后，IDS策略默认开启拦截模式，正常情况下需要客户授权后才能开启IDS拦截模式以避免发生误拦情况（正常情况下误拦率低于0.1%）。

操作NIPSIDS策略开启观察模式的方法：

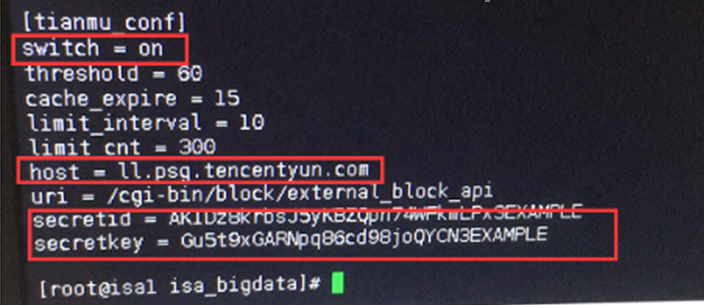
使用浏览器登录TCE运营端（cmgt）： 进入NIPS控制台左侧菜单栏：管控 - 其他设置 - 攻击拦截开关，将攻击拦截开关置为关闭状态。

事件告警与指标监控

目前NIPS版本还没有实现对接TCE的告警统一管控平台，可以通过使用浏览器登录TCE运营端（cmgt）： 进入NIPS控制台左侧菜单栏：更多 - 故障日志来查看NIPS系统运营告警。

NIPS与御界联动配置

这部分已在御界操作部署手册记录，涉及到NIPS部分见下图，需要确认host与secretid与secretkey的部分，secretid与secretkey需要咨询客户，host域名见以下操作步骤。



host域名修改方式：

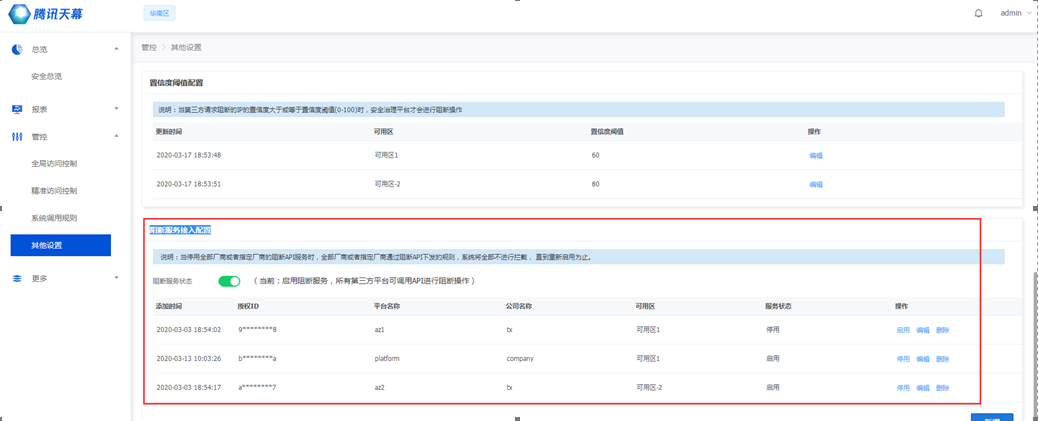
host会通过tce配置中心自动获取，需要确认host是否正确，正确的话域名为客户现场的格式。获取正确host的方式，可以向NIPS负责人询问或查询NIPS控制台，登录NIPS控制台的容器，登录容器 ocloud-psg-console

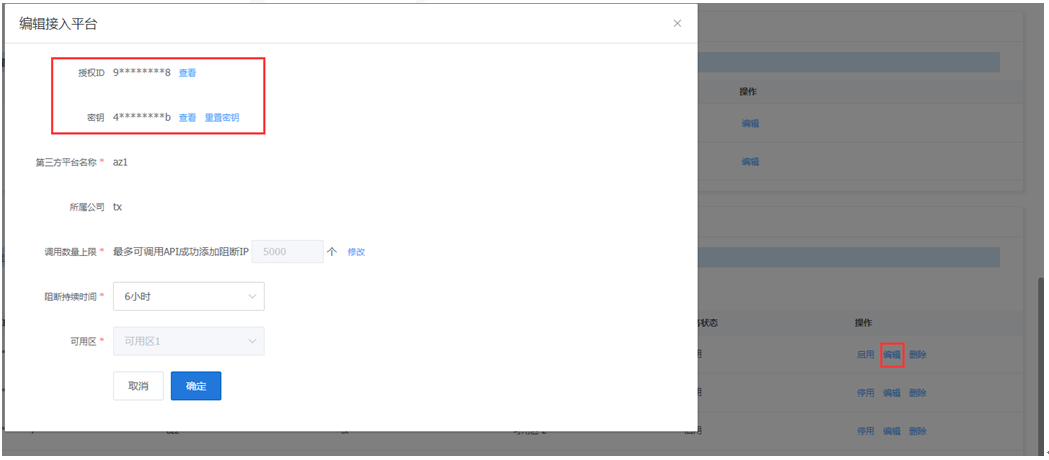
执行命令： cat /etc/psg/psg.ini |grep ll\_host  就能看到host域名。

附录

查看NIPS提供给第三方安全产品阻断API的key密钥

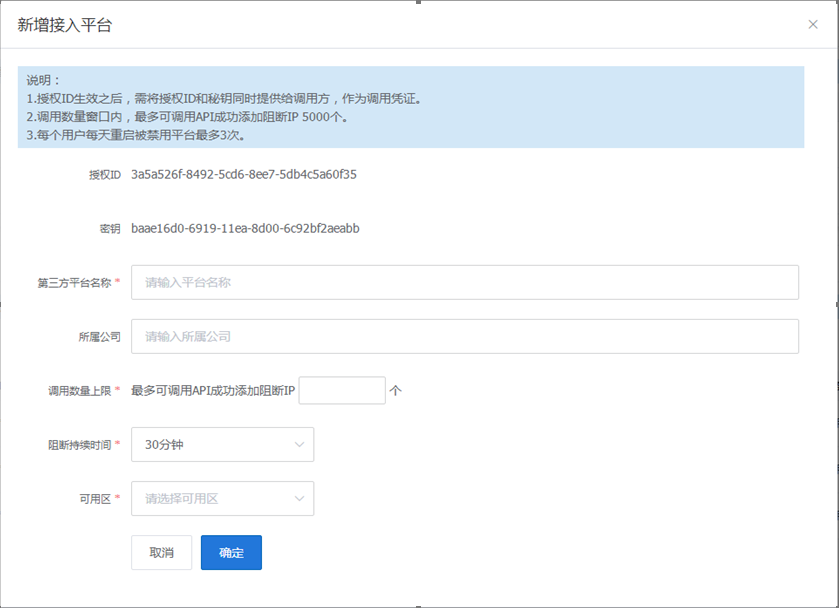
使用浏览器登录TCE运营端（cmgt）： 进入NIPS控制台左侧菜单栏：管控 - 其他设置 - 阻断服务接入配置，如果是已有接入产品，可以根据公司名称+平台名称查看对接安全产品，点击对应的编辑按钮可显示出来key和密钥信息。（例如跟御界产品的对接等等）





NIPS如何新增第三方安全产品对接生产key和密钥

使用浏览器登录TCE运营端（cmgt）： 进入NIPS控制台左侧菜单栏：管控 - 其他设置 - 阻断服务接入配置，点击右下方 新增按钮，输入对应的第三方安全产品名称、所属公司、调用数量上限（默认为5000个），阻断持续时间等内容，点击 确定以生产出来 授权ID 和 密钥信息。



NIPS探针平行扩容方案

交换机扩容配置修改

bgp 【bgp\_as】

 ip vpn-instance Outside\_WC

  address-family ipv4 unicast

  network 【WAN\_network】【WAN\_network\_mask】

ipprefix-list BGP\_ADV index 20 permit 【WAN\_network】 【WAN\_network\_mask】

iproute-static vpn-instance Outside\_WC 【WAN\_address】 【mask】Vlan-interface101 【FW\_OUT\_VIP】 preference 5 tag 5000 descriptionTo-BFW-Outside

acl advanced3200

 description YUJIE\_mirroring\_subnet

 rule  permit ip source 【WAN\_network】 【inverse mask】

 rule  comment 【mirror-port】-source

 rule  permit ip destination 【WAN\_network】 【inverse mask】

 rule  comment 【mirror-port】-destination

 rule 100 deny ip

NIPS探针服务器扩容部署

1. 新增NIPS探针服务器操作系统安装，操作系统版本说明请查阅上述3.2小节内容；
2. NIPS探针服务器安装部署前检查，请严格按照上述3.3节中的3.3.1、3.3.2、3.3.3、3.3.4 等4小节内容作详细配置检查。
3. 配置新增扩容探针的服务器IP到iplist

登录TCE部署机部署机，在iplist.csv文件中添加NIPS探针服务器3的IP。

vim /data/tce\_dc/config/self/iplist.csv

找到 PSG 开头的这一行，确保信息如下，如果不是，修改为如下：

PSG,product-psg-ll,psg\_ll\_host,1,"探针3 IP"

1. 部署NIPS探针生产组件，可参考4.8节内容。以下步骤在TCE部署机执行。假设新增的1台探针服务器3带内管理IP为：10.250.36.141

（1）解压组件包并渲染：

kaleido\_product install product-psg-ll--action=trender

（2）检查配置文件：

cat /data/tce\_dc/workspace/product-psg-ll/./config/mul\_deploy.conf  | grep psg\_host

返回:  psg\_host=10.250.36.141 说明无误，继续往下执行

（3）部署product-psg-ll：

kaleido\_product install product-psg-ll--action=deploy

等待NIPS探针生产节点执行软件服务安装，当探针服务器安装完软件服务后会执行自动reboot重启操作（时间约5~10分钟左右），必须等到机器重启完毕后再执行下面操作：

（4）安装后服务检查和IDS策略导入命令：

cd /data/tce\_dc/workspace/product-psg-ll/TCE;sh allocate.sh

备注：如果导入失败，可以重复执行多次安装直到成功为止。

1. 部署后验证，请参照上述第5节的5.1、5.2、5.3、5.4、5.5、5.6、5.7小节内容进行详细验证。

NIPS基本功能测试验证方案

管控-全局访问控制

1.黑名单设置

|  |  |
| --- | --- |
| **用例编号** | PSG\_全局访问控制 \_E001 |
| **用例名称** | 新增、停用、启用、删除、查询黑名单 |
| **测试耗时** | 0.5h |
| **测试目的** | 验证黑名单功能是否生效 |
| **预置条件** | 靶机和攻击机已就绪，都配置有公网IP，且网络互通，靶机http服务已开启（可以安装nginx或者apache服务），端口为80，攻击机对靶机攻击请求已报备 |
| **测试过程** | 1、登录网络入侵防护系统平台，在左侧导航处， 点击“管控-全局访问控制-黑名单设置 “， 右上角点击”新增“，黑名单配置如下，“选择类型”字段选仅源IP，“匹配类型”选择阻断， 来源平台无选项时，需要先通过管理来源平台添加1个：    点击“确认“后，新增黑名单后如下：    2、登录攻击机，向靶机发送正常http请求，请求被阻断。    3、左侧导航栏点击，”报表-安全告警“，在搜索框填写攻击机公网IP，然后回车确认，查看是否有黑名单“精准匹配源IP”已拦截告警，并记录“累计告警次数”：    4、左侧导航，点击 “管控-全局访问控制-黑名单设置”，停用“精准匹配源IP” 规则—确定：    停用后，查看名单状态是否已失效,操作动作由停用变为启用    5、登录攻击机，等待10s左右，向靶机发送正常http请求，确认请求正常，不再被拦截    6、左侧导航，点击“报表-安全告警“，搜索框输入攻击机公网IP，查看“累计告警次数”没有增加    7、左侧导航，点击“管控-全局访问控制-黑名单设置“，启用“精准匹配源IP”规则—确定：    启用后，查看状态是否“正在使用”，操作由“启用”变为“停用”：    8、登陆攻击机，等待10s后，发送正常HTTP请求到靶机，请求被阻断    9、左侧导航，点击“报表-安全告警”，搜索框输入攻击机公网IP，确认“累计告警次数”增加。    10、左侧导航，点击“管控-全局访问控制-黑名单设置”，删除” 精准匹配源IP”规则—确定    删除后，在搜索框搜索：攻击机公网IP，确认不再有该规则的记录显示：    11、登陆攻击机，等待10s后，向靶机发送正常HTTP请求，确认请求正常？    12、左侧导航，点击“报表-安全告警”，搜索框输入攻击机公网IP，确认“累计告警次数”不再增加 |
| **预期结果** | 1、新增黑名单后阻断生效，安全告警显示有黑名单的已拦截告警信息  2、停用黑名单后，阻断失效，“累计告警次数”没有增加  3、启用黑名单后，阻断生效，“累计告警次数”增加（规则为：10s内的告警会被压制1条，因此为了保证累计告警会增加，请确保每次 http请求，间隔10s以上）  4、删除黑名单后，黑名单查询不到删除后的黑名单，阻断失效，“累计告警次数”没有增加 |
| **测试结果** |  |
| **备注** |  |

2.白名单设置

|  |  |
| --- | --- |
| **用例编号** | PSG\_全局访问控制 \_E002 |
| **用例名称** | 新增、编辑、启用、停用、删除和查询白名单 |
| **测试耗时** | 0.5h |
| **测试目的** | 验证白名单功能是否生效 |
| **预置条件** | 靶机和攻击机已就绪，都配置有公网IP，且网络互通，靶机http服务已开启（可以安装nginx或者apache服务），端口为80，攻击机对靶机攻击请求已报备 |
| **测试过程** | 1、 登陆攻击机，向靶机以频率1s1次发送http攻击报文5次，  curl http://$server\_ip:$server\_port/vuln\_base/B001/sql\_test.php?a1=1 and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,md5(3.1415),0x7e))) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)    第2次请求被拦截    2、左侧导航，点击“报表-安全告警”，搜索框输入攻击机公网IP，查询有拦截规则“已下发”告警，最新告警时间与实际攻击时间匹配，并记录“累计告警次数”    3、左侧导航，点击“管控-全局访问控制-白名单设置”， 然后右上角点击“新增”，白名单配置如下，“选择类型”字段选仅源IP，“匹配类型”选择放行， 来源平台无选项时，需要先通过管理来源平台添加1个：    确认后，白名单如下：    4、登陆攻击机，向靶机发送http攻击报文，请求正常，不再被拦截    5、停用“白名单精准匹配源IP”规则    确定停用后，如下：    6、 登陆攻击机，向靶机发送http攻击报文，请求被阻断    7、启用“白名单精准匹配源IP”规则：    启用后如下：    8、登陆攻击机，向靶机发送http攻击报文，请求被放过    9、删除“白名单精准匹配源IP”规则：    确认删除后，在输入框输入之前配置的源IP，查询不到该白名单记录，如下：    10、登陆攻击机，向靶机发送http攻击报文，请求被阻断 |
| **预期结果** | 1、新增白名单后，阻断不生效  2、停用白名单后，阻断生效，会产生默认规则的攻击告警  3、启用黑名单后，阻断不生效  4、删除白名单后，黑名单查询不到删除后的白名单，阻断生效，产生默认规则的攻击告警 |
| **测试结果** |  |
| **备注** |  |

管控-系统调用规则

IDS规则管理

|  |  |
| --- | --- |
| **用例编号** | PSG\_系统调用规则\_E003 |
| **用例名称** | IDS规则管理 |
| **测试耗时** | 10min |
| **测试目的** | 验证平台IDS规则的阻断功能 |
| **预置条件** | 靶机和攻击机已就绪，都配置有公网IP，且网络互通，靶机http服务已开启（可以安装nginx或者apache服务），端口为80，攻击机对靶机攻击请求已报备 |
| **测试过程** | 1、左侧导航，点击“管控-其他设置”，找到“攻击拦截配置”栏，打开拦截开关，设置“攻击拦截状态”为“当前：已开启拦截，拦截模式”，默认拉黑时长为2分钟，如下：    2、登陆攻击机，向靶机发送2次mysql注入攻击请求，频率为1s 1次，第二次请求被阻断。  请求内容如下：  curl "http://$server\_ip:$server\_port/vuln\_base/B001/sql\_test.php?a1=1 and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,md5(3.1415),0x7e))) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)"    3、左侧导航，点击“报表-安全告警”，搜索框输入攻击机IP，新增1次相关阻断规则“已下发”告警，最新告警时间与实际攻击时间一致    4、点击“管控—系统调用规则”，搜索框输入靶机IP—点击查询，列表中新增1条ids规则，规则ID格式为“IDSxxxxx”    5、等待2分钟后，ids规则失效，向靶机发送HTTP正常请求，确认请求被放行： |
|  |  |
| **预期结果** | 1、发送HTTP SQL注入攻击请求2次后，阻断规则被下发，IP被加黑，等待配置的拉黑时长过后，拉黑失效，再次发送请求被放行 |
| **测试结果** |  |
| **备注** |  |

交换机配置

WC1-10G配置

聚合组：

三层

#10为对接其他AZ-WC聚合组编号

二层

#100为对接BFW聚合组编号

#128为互联聚合组编号

#48为镜像聚合组编号

端口分配：

#1-12对接运营商

#13-40，预留端口

#41-48对接BFW

#49-50对接NFVW

#51-52互联

#53镜像

#54对接其他AZ-WC

#管理口（M-GE0/0/0）

-------------------------------------

!!刷配置前设置后重启生效命令

 max-ecmp-num 16

 y

 hardware-resource routing-mode ipv6-128

 y

 #

 public-keylocal create rsa

 1024

 #

 public-keylocal create dsa

 1024

 #

 save force

 reboot

 y

#

-------------------------------------

!!设备配置脚本

#

 sysname 【sysname】

#

 clocktimezone BeiJing add 08:00:00

#

ip vpn-instance Inside\_WC

 route-distinguisher 100:0

#

ip vpn-instance Outside\_WC

 route-distinguisher 200:0

#

ip vpn-instance mgt\_vrf

 route-distinguisher 2:1

#

 irfmac-address persistent timer

 irfauto-update enable

 undo irflink-delay

 irf member1 priority 1

#

 parity-error unrecoverable log enable

#

 ipunreachables enable

 ipttl-expires enable

#

 ipload-sharing mode per-flow dest-ip src-ip ip-pro dest-port src-port global

#

 lldpignore-pvid-inconsistency

 lldp globalenable

#

 fanprefer-direction slot 1 port-to-power

 password-recovery enable

#

vlan 100

 descriptionInside\_WC

#

vlan 101

 descriptionOutside\_WC

#

vlan 500

 descriptionWC\_IBGP

#

stp region-configuration

 region-nameWC

 revision-level 1

 activeregion-configuration

#

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation100

 description【BFW1\_description】               //例如：To-XXX-BFW-01-BAGG100

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 link-aggregation mode dynamic

 undo stpenable

 undoshutdown

#

interface Bridge-Aggregation128

 description【WC2\_description】                //例如：To-XXX-WC-01-BAGG128

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 link-aggregation mode dynamic

 undoshutdown

#

interface Route-Aggregation10                   //AZ间WC互联聚合口编号待定义

 undo shutdown

#

interface Route-Aggregation10.1                //AZ间WC互联子接口号待定义

 description【other-WC1\_description】

 ip bindingvpn-instance Inside\_WC                 // Inside互通

 ip address 【WC1\_address】255.255.255.254

 ipv6address 【WC1\_ipv6-address】

 undo shutdown

#

interface Route-Aggregation10.2                //AZ间WC互联子接口号待定义

 description【other-WC1\_description】

 ip bindingvpn-instance Outside\_WC              //Outside互通

 ip address 【WC1\_address】255.255.255.254

 ipv6address 【WC1\_ipv6-address】

 undo shutdown

#

interface LoopBack0

 ip address 【loopback】255.255.255.255

 ip address 【loopback-ipv6】

#

interface Vlan-interface100

 descriptionInside\_BFW

 ip bindingvpn-instance Inside\_WC

 ip address 【vrrp\_address1】255.255.255.248

 vrrpversion 2

 vrrp vrid 1virtual-ip 【vrrp\_vip\_1】

 vrrp vrid 1authentication-mode md5 plain 【vrrp\_auth】      //【vrrp\_auth】取值不能超过8位

 vrrp vrid 1priority 200

 vrrp vrid 1preempt-mode delay 3

 ipv6address【vrrp\_ipv6-address1】

 vrrp ipv6vrid 1 virtual-ip 【vrrp\_ipv6-address1】 link-local

 vrrp ipv6vrid 1 priority 200

 vrrp ipv6vrid 1 preempt-mode delay 3

 undoshutdown

#

interface Vlan-interface101

 descriptionOutside\_BFW

 ip bindingvpn-instance Outside\_WC

 ip address 【vrrp\_address1】255.255.255.248

 vrrpversion 2

 vrrp vrid 1virtual-ip 【vrrp\_vip\_1】

 vrrp vrid 1authentication-mode md5 plain 【vrrp\_auth】      //【vrrp\_auth】取值不能超过8位

 vrrp vrid 1priority 200

 vrrp vrid 1preempt-mode delay 3

 ipv6address【vrrp\_ipv6-address1】

 vrrp ipv6vrid 1 virtual-ip 【vrrp\_ipv6-address1】 link-local

 vrrp ipv6vrid 1 priority 200

 vrrp ipv6vrid 1 preempt-mode delay 3

 undoshutdown

#

interface Vlan-interface500

 description【WC2\_description】

 ip bindingvpn-instance Outside\_WC

 ip address 【WC1\_address】255.255.255.254

 ipv6address 【WC1\_ipv6-address】

 undoshutdown

#

interface FortyGigE1/0/49

 portlink-mode route

 description【NFVW1\_description】

 flow-interval 30

 ip bindingvpn-instance Inside\_WC

 ip address 【WC1\_address】255.255.255.254

 ipv6address 【WC1\_ipv6-address】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/50

 portlink-mode route

 description【NFVW2\_description】

 flow-interval 30

 ip bindingvpn-instance Inside\_WC

 ip address 【WC1\_address】255.255.255.254

 ipv6address 【WC1\_ipv6-address】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/51

 portlink-mode bridge

 description【WC2\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/52

 portlink-mode bridge

 description【WC2\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/53                           //镜像端口，配置详见尾部镜像配置

#

interface FortyGigE1/0/54

 portlink-mode route

 description【other-WC1\_description】

 flow-interval 30

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 lacp periodshort

 portlink-aggregation group 10

 undoshutdown

#

interface Ten-GigabitEthernet1/0/47

 portlink-mode bridge

 description【BFW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 portlink-aggregation group 100

 undoshutdown

#

interface Ten-GigabitEthernet1/0/48

 portlink-mode bridge

 description【BFW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 portlink-aggregation group 100

 undoshutdown

#

interface M-GigabitEthernet0/0/0

 descriptionOut-Of-Band-Management

 ip bindingvpn-instance mgt\_vrf

 ip address 【MGT\_address】255.255.255.128

 undoshutdown

#

interface Ten-GigabitEthernet1/0/1

 portlink-mode route

 ip bindingvpn-instance Outside\_WC

 descriptionTIX

 ip address 【WC1-TIX\_address】【mask】

 ipv6address 【WC1-TIX\_ipv6-address】

 undoshutdown

#

bgp 【bgp\_as】

 non-stop-routing

 router-id 【loopback】

 compare-different-as-med

#

 ipvpn-instance Inside\_WC

  router-id 【loopback】

 compare-different-as-med

  group 【NFVW】 external

  peer 【NFVW】 passwordsimple 【peer\_password】

  group 【NFVW-IPv6】 external

  peer 【NFVW-IPv6】 passwordsimple 【peer\_password】

  group 【other-WC】 external

  peer 【other-WC】 password simple 【other-WC-peer\_password】

  group 【other-WC-IPv6】 external

  peer 【other-WC-IPv6】 passwordsimple 【other-WC-peer\_password】

  peer 【peer\_nfvw1\_address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw1\_address】 group 【NFVW】

  peer 【peer\_nfvw1\_address】 description 【peer\_nfvw1\_description】

  peer 【peer\_nfvw2\_address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw2\_address】 group 【NFVW】

  peer 【peer\_nfvw2\_address】 description 【peer\_nfvw2\_description】

  peer 【peer\_other-WC\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_address】 group 【other-WC】

  peer 【peer\_other-WC\_address】 description 【peer-other-WC-description】

  peer 【peer\_nfvw1\_ipv6-address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw1\_ipv6-address】 groupNFVW-IPv6

  peer 【peer\_nfvw1\_ipv6-address】 description 【peer\_nfvw1\_description】

  peer 【peer\_nfvw2\_ipv6-address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw2\_ipv6-address】 groupNFVW-IPv6

  peer 【peer\_nfvw2\_ipv6-address】 description 【peer\_nfvw2\_description】

  peer 【peer\_other-WC\_ipv6\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_ipv6\_address】 group 【other-WC-ipv6】

  peer 【peer\_other-WC\_ipv6\_address】 description 【peer-other-WC-description】

#

 address-family ipv4 unicast

   balance16

  preference 10 100 100

   peer 【NFVW】 enable

   peer 【NFVW】 route-policyFrom-NFVW import

   peer 【NFVW】 route-policyTo-NFVW export

   peer 【NFVW】default-route-advertise route-policy SetComm-2/2

   peer 【NFVW】advertise-community

   peer 【other-WC】 enable

   peer 【other-WC】route-policy 【From-other-WC】 import

   peer 【other-WC】 route-policy【To-other-WC】  export

   peer 【other-WC】advertise-community

  #

 address-family ipv6 unicast

   balance16

  preference 10 100 100

   network 【IPV6 network】 route-policySetComm-1/4

   peer 【NFVW-IPv6】 enable

   peer 【NFVW-IPv6】 route-policyFrom-NFVW-IPV6 import

   peer 【NFVW-IPv6】 route-policyTo-NFVW-IPV6 export

   peer 【NFVW-IPv6】default-route-advertise route-policy SetComm-2/2

   peer 【NFVW-IPv6】advertise-community

   peer 【other-WC-IPv6】 enable

   peer 【other-WC-IPv6】 route-policy 【From-other-WC-IPV6】 import

   peer 【other-WC-IPv6】 route-policy 【To-other-WC-IPV6】 export

   peer 【other-WC-IPv6】advertise-community

 #

 ipvpn-instance Outside\_BGP

  router-id 【loopback】

 compare-different-as-med

  group 【QCPL】 external

  peer 【QCPL】 password simple【peer\_password】

  group 【QCPL-IPv6】 external

  peer 【QCPL-IPv6】 passwordsimple 【peer\_password】

  group 【WC】 internal

  peer 【WC】 passwordsimple 【peer\_password】

  group 【WC-IPv6】 internal

  peer 【WC-IPv6】 passwordsimple 【peer\_password】

  group 【other-WC】 external

  peer 【other-WC】 passwordsimple 【other-WC-peer\_password】

  group 【other-WC-IPv6】 external

  peer 【other-WC-IPv6】 passwordsimple 【other-WC-peer\_password】

  peer 【peer\_QCPL\_address】 as-number 【qcpl-as】

  peer 【peer\_QCPL\_address】 group 【QCPL】

  peer 【peer\_QCPL\_address】 description 【peer\_QCPL\_description】

  peer 【peer\_WC\_address】 group 【WC】

  peer 【peer\_WC\_address】 description 【peer\_WC\_description】

  peer 【peer\_other-WC\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_address】 group 【other-WC】

  peer 【peer\_other-WC\_address】 description 【peer\_other-WC\_description】

  peer 【peer\_QCPL\_ipv6\_address】 as-number 【qcpl-as】

  peer 【peer\_QCPL\_ipv6\_address】 group 【QCPL-IPv6】

  peer 【peer\_QCPL\_ipv6\_address】 description 【peer\_QCPL\_description】

  peer 【peer\_WC\_ipv6\_address】 group 【WC-IPv6】

  peer 【peer\_WC\_ipv6\_address】 description 【peer\_WC\_description】

  peer 【peer\_other-WC\_ipv6\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_ipv6\_address】 group 【other-WC-IPv6】

  peer 【peer\_other-WC\_ipv6\_address】 description 【peer\_other-WC\_description】

  #

 address-family ipv4 unicast

   balance16

  preference 10 100 100

   network 【WAN\_network】【WAN\_network\_mask】

   peer 【QCPL】 enable

   peer 【QCPL】 route-policyFrom-QCPL import

   peer 【QCPL】 route-policyTo-QCPL export

   peer 【WC】 enable

   peer 【WC】advertise-community

   peer 【WC】 next-hop-local

   peer 【other-WC】 enable

   peer 【other-WC】route-policy 【From-other-WC】 import

   peer 【other-WC】 route-policy【To-other-WC】  export

   peer 【other-WC】 advertise-community

  #

 address-family ipv6 unicast

   balance16

  preference 10 100 100

   network 【IPV6 network】 route-policySetComm-1/4

   peer 【QCPL-IPv6】 enable

   peer 【QCPL-IPv6】 route-policyFrom-QCPL-IPV6 import

   peer 【QCPL-IPv6】 route-policyTo-QCPL-IPV6 export

   peer 【WC-IPv6】 enable

   peer 【WC-IPv6】advertise-community

   peer 【WC-IPv6】 next-hop-local

   peer 【other-WC-IPv6】 enable

   peer 【other-WC-IPv6】 route-policy 【From-other-WC-IPV6】 import

   peer 【other-WC-IPv6】 route-policy 【To-other-WC-IPV6】 export

   peer 【other-WC-IPv6】advertise-community

#

route-policy From-NFVW permit node 5

#

route-policy From-NFVW-IPV6 permit node 5

#

route-policy From-QCPL permit node 5

#

route-policy From-QCPL-IPV6 permit node 5

#

route-policy 【From-other-WC】 permit node 5

#

route-policy 【From-other-WC-IPV6】 permit node 5

#

route-policy SetComm-1/1 permit node 5

 applycommunity 1:1

#

route-policy SetComm-1/4 permit node 5

 applycommunity 1:4

#

route-policy SetComm-2/2 permit node 5

 applycommunity 2:2

#

route-policy To-NFVW permit node 5

#

route-policy To-NFVW-IPV6 permit node 5

#

route-policy To-QCPL permit node 5

 if-match ipaddress prefix-list BGP\_ADV

#

route-policy To-QCPL deny node 10

#

route-policy To-QCPL-IPV6 permit node 5

 if-matchipv6 address prefix-list BGP-IPV6\_ADV

#

route-policy To-QCPL-IPV6 deny node 10

#

route-policy 【To-other-WC】 permit node 5

 if-matchcommunity 10

#

route-policy 【To-other-WC-IPV6】 permit node 5

 if-matchcommunity 10

#

 ipcommunity-list 10 permit 3:1

#

 ipprefix-list BGP\_ADV index 10 permit 【WAN\_network】 【WAN\_network\_mask】

 ipv6 prefix-listBGP-IPV6\_ADV index 10 permit 【WAN-IPV6\_network】

#

 schedulerlogfile size 16

#

line class aux

 user-rolenetwork-admin

#

line class vty

 user-rolenetwork-operator

#

line aux 0

 authentication-mode scheme

 user-rolenetwork-admin

#

line vty 0 63

 authentication-modescheme

 user-rolenetwork-admin

 user-rolenetwork-operator

 idle-timeout 5 0

#

#

 iproute-static vpn-instance mgt\_vrf 0.0.0.0 0 M-GigabitEthernet0/0/0 【MA\_address】 preference 5description Out-Of-Band-Management

 iproute-static vpn-instance Inside\_WC 0.0.0.0 0 Vlan-interface100 【FW\_IN\_VIP】 preference 5tag 6000 description To-BFW-Inside

 iproute-static vpn-instance Outside\_WC 【WAN\_address】 【mask】 Vlan-interface101【FW\_OUT\_VIP】 preference 5 tag 5000 descriptionTo-BFW-Outside

 ipv6 route-staticvpn-instance Inside\_WC 0.0.0.0 0 Vlan-interface100 【FW\_IN\_VIP-IPV6】 preference 5tag 6000 description To-BFW-Inside-IPV6

 ipv6route-static vpn-instance Outside\_WC 【WAN-ipv6\_address】 【mask】Vlan-interface101 【FW\_OUT\_VIP-IPV6】 preference 5 tag 5000 descriptionTo-BFW-Outside-IPV6

#

 info-centerlogbuffer size 1024

 info-centerloghost source M-GigabitEthernet0/0/0

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_1】 facilitylocal2

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_2】 facilitylocal2

 info-centersource SHELL logbuffer deny

#

 snmp-agentcommunity read 【community】 acl 2001

 snmp-agentsys-info version v2c

 undosnmp-agent sys-info version v3

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_1】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_2】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttrap source M-GigabitEthernet0/0/0

 snmp-agentpacket max-size 17940

#

 ssh serverenable

 ssh serveracl 2000

#

 arp timeraging 5

#

 ntp-serviceenable

 ntp-servicesource M-GigabitEthernet0/0/0

 ntp-serviceunicast-server 【ntp\_address\_1】 vpn-instance mgt\_vrf

 ntp-serviceunicast-server 【ntp\_address\_2】 vpn-instance mgt\_vrf

#

acl basic 2000

 descriptionLogin-Filter

 rule  permit vpn-instance mgt\_vrf source 【gaya\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【cloud\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AAA\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【NTP\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AZ-network】 0

#

acl basic 2001

 descriptionSNMP-Filter

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_2】 0

#

 headerlogin %

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

             Authorized Access Only!

Disconnect IMMEDIATELY as you are not anauthorized user!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%

#

local-user 【local\_user】 class manage

 passwordsimple 【local\_password】

 service-type ssh terminal

 authorization-attribute user-rolenetwork-admin

#

return

#

save force

#

-----------------3A配置------------------------

#

hwtacacs scheme 【hwtacacs\_scheme】

 primaryauthentication 【first\_3A】

 primaryauthorization 【first\_3A】

 primaryaccounting 【first\_3A】

 secondaryauthentication 【second\_3A】

 secondaryauthorization 【second\_3A】

 secondaryaccounting 【second\_3A】

 keyauthentication simple 【3A\_key】

 keyauthorization simple 【3A\_key】

 keyaccounting simple 【3A\_key】

 user-name-format without-domain

 nas-ip 【nas\_ip】

 vpn-instance mgt\_vrf

#

domain 【hwtacacs\_domain】

 authentication login hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization login hwtacacs-scheme 【hwtacacs\_scheme】 local

 accountinglogin hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization command hwtacacs-scheme 【hwtacacs\_scheme】 none

 accountingcommand hwtacacs-scheme 【hwtacacs\_scheme】

#

domain system

 state block

#

 domaindefault enable 【hwtacacs\_domain】

#

line vty 0 63

command authorization

command accounting

#

line aux 0

command accounting

#

save force

#

-----------------镜像配置------------------------

#

#需根据需求是否配置

#

 mirroring-group 1 local

#

acl basic 2200

 rule 0 deny

#

acl advanced 3200                                                 //根据实际情况设定镜像源端口及地址

 descriptionYUJIE\_mirroring\_subnet

 rule   permit ip source 【mirror\_network】 【inverse mask】

 rule   comment 【mirror-port】-source

 rule   permit ip destination 【mirror\_network】 【inverse mask】

 rule   comment 【mirror-port】-destination

 rule 100deny ip

#

mirroring-group 1 mirroring-port 【source\_port】  inbound     //镜像源端口；WC对接QCPL端口

mirroring-group 1 mirroring-port 【source\_port】  inbound     //镜像源端口；WC对接BFW端口

mirroring-group 1 monitor-portBridge-Aggregation48             //镜像目的端口；WC对接MIRROR光交换机端口

#

vlan 10

 namemonitor-server

#

stp region-configuration

 region-nameWC

 revision-level 1

 instance 1vlan 500

 instance 2vlan 10

 activeregion-configuration

#

 stpinstance 1 root primary

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation48

 description【OPT\_description】

 port accessvlan 10

 undoshutdown

#

interface FortyGigE1/0/53

 portlink-mode bridge

 description【OPT\_description】

 port accessvlan 10

 flow-interval 30

 packet-filter 2200 inbound

 packet-filter3200 outbound

 portlink-aggregation group 48

 undoshutdown

#

save force

WC2-10G配置

聚合组：

三层

#10为对接其他AZ-WC聚合组编号

二层

#100为对接BFW聚合组编号

#128为互联聚合组编号

#48为镜像聚合组编号

端口分配：

#1-12对接运营商

#13-40，预留端口

#41-48对接BFW

#49-50对接NFVW

#51-52互联

#53镜像

#54对接其他AZ-WC

#管理口（M-GE0/0/0）

-------------------------------------

!!刷配置前设置后重启生效命令

 max-ecmp-num 16

 y

 hardware-resource routing-mode ipv6-128

 y

 #

 public-keylocal create rsa

 1024

 #

 public-keylocal create dsa

 1024

 #

 save force

 reboot

 y

#

-------------------------------------

!!设备配置脚本

#

 sysname 【sysname】

#

 clocktimezone BeiJing add 08:00:00

#

ip vpn-instance Inside\_WC

 route-distinguisher 100:0

#

ip vpn-instance Outside\_WC

 route-distinguisher 200:0

#

ip vpn-instance mgt\_vrf

 route-distinguisher 2:1

#

 irfmac-address persistent timer

 irfauto-update enable

 undo irflink-delay

 irf member1 priority 1

#

 parity-error unrecoverable log enable

#

 ipunreachables enable

 ipttl-expires enable

#

 ipload-sharing mode per-flow dest-ip src-ip ip-pro dest-port src-port global

#

 lldpignore-pvid-inconsistency

 lldp globalenable

#

 fanprefer-direction slot 1 port-to-power

 password-recovery enable

#

vlan 100

 descriptionInside\_WC

#

vlan 101

 descriptionOutside\_WC

#

vlan 500

 descriptionWC\_IBGP

#

stp region-configuration

 region-nameWC

 revision-level 1

 activeregion-configuration

#

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation100

 description【BFW2\_description】                //例如：To-XXX-BFW-01-BAGG100

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 link-aggregation mode dynamic

 undo stpenable

 undoshutdown

#

interface Bridge-Aggregation128

 description【WC1\_description】                //例如：To-XXX-WC-01-BAGG128

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 link-aggregation mode dynamic

 undoshutdown

#

interface Route-Aggregation10                   //AZ间WC互联聚合口编号待定义

 undoshutdown

#

interface Route-Aggregation10.1                //AZ间WC互联子接口号待定义

 description【other-WC2\_description】

 ip bindingvpn-instance Inside\_WC                 // Inside互通

 ip address 【WC2\_address】255.255.255.254

 ipv6address 【WC2\_ipv6-address】

 undoshutdown

#

interface Route-Aggregation10.2                //AZ间WC互联子接口号待定义

 description【other-WC2\_description】

 ip bindingvpn-instance Outside\_WC              //Outside互通

 ip address 【WC2\_address】255.255.255.254

 ipv6address 【WC2\_ipv6-address】

 undoshutdown

#

interface LoopBack0

 ip address 【loopback】255.255.255.255

 ip address 【loopback-ipv6】

#

interface Vlan-interface100

 descriptionInside\_BFW

 ip bindingvpn-instance Inside\_WC

 ip address 【vrrp\_address2】255.255.255.248

 vrrp version2

 vrrp vrid 1virtual-ip 【vrrp\_vip\_2】

 vrrp vrid 1authentication-mode md5 plain 【vrrp\_auth】      //【vrrp\_auth】取值不能超过8位

 vrrp vrid 1priority 150

 vrrp vrid 1preempt-mode delay 3

 ipv6address【vrrp\_ipv6-address2】

 vrrp ipv6vrid 1 virtual-ip 【vrrp\_ipv6-address2】 link-local

 vrrp ipv6vrid 1 priority 150

 vrrp ipv6vrid 1 preempt-mode delay 3

 undoshutdown

#

interface Vlan-interface101

 descriptionOutside\_BFW

 ip bindingvpn-instance Outside\_WC

 ip address 【vrrp\_address2】255.255.255.248

 vrrpversion 2

 vrrp vrid 1virtual-ip 【vrrp\_vip\_2】

 vrrp vrid 1authentication-mode md5 plain 【vrrp\_auth】      //【vrrp\_auth】取值不能超过8位

 vrrp vrid 1priority 150

 vrrp vrid 1preempt-mode delay 3

 ipv6address【vrrp\_ipv6-address2】

 vrrp ipv6vrid 1 virtual-ip 【vrrp\_ipv6-address2】 link-local

 vrrp ipv6vrid 1 priority 200

 vrrp ipv6vrid 1 preempt-mode delay 3

 undoshutdown

#

interface Vlan-interface500

 description【WC1\_description】

 ip bindingvpn-instance Outside\_WC

 ip address 【WC2\_address】255.255.255.254

 ipv6 address【WC1\_ipv6-address】

 undoshutdown

#

interface FortyGigE1/0/49

 portlink-mode route

 description【NFVW1\_description】

 flow-interval 30

 ip bindingvpn-instance Inside\_WC

 ip address 【WC2\_address】255.255.255.254

 ipv6address 【WC2\_ipv6-address】

 lldp tlv-enablebasic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/50

 portlink-mode route

 description【NFVW2\_description】

 flow-interval 30

 ip bindingvpn-instance Inside\_WC

 ip address 【WC2\_address】 255.255.255.254

 ipv6address 【WC2\_ipv6-address】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/51

 portlink-mode bridge

 description【WC1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/52

 portlink-mode bridge

 description【WC1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101 500

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/53                           //镜像端口，配置详见尾部镜像配置

#

interface FortyGigE1/0/54

 portlink-mode route

 description【other-WC2\_description】

 flow-interval 30

 lldp tlv-enablebasic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 lacp periodshort

 portlink-aggregation group 10

 undoshutdown

#

interface Ten-GigabitEthernet1/0/47

 portlink-mode bridge

 description【BFW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 portlink-aggregation group 100

 undoshutdown

#

interface Ten-GigabitEthernet1/0/48

 portlink-mode bridge

 description【BFW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 100 to 101

 portlink-aggregation group 100

 undoshutdown

#

interface M-GigabitEthernet0/0/0

 descriptionOut-Of-Band-Management

 ip bindingvpn-instance mgt\_vrf

 ip address 【MGT\_address】255.255.255.128

 undoshutdown

#

interface Ten-GigabitEthernet1/0/1

 portlink-mode route

 ip bindingvpn-instance Outside\_WC

 descriptionTIX

 ip address 【WC1-TIX\_address】【mask】

 ipv6address 【WC1-TIX\_ipv6-address】

 undoshutdown

#

bgp 【bgp\_as】

 non-stop-routing

 router-id 【loopback】

 compare-different-as-med

#

 ipvpn-instance Inside\_WC

  router-id 【loopback】

 compare-different-as-med

  group 【NFVW】 external

  peer 【NFVW】 passwordsimple 【peer\_password】

  group 【NFVW-IPv6】 external

  peer 【NFVW-IPv6】 passwordsimple 【peer\_password】

  group 【other-WC】 external

  peer 【other-WC】 passwordsimple 【other-WC-peer\_password】

  group 【other-WC-IPv6】 external

  peer 【other-WC-IPv6】 passwordsimple 【other-WC-peer\_password】

  peer 【peer\_nfvw1\_address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw1\_address】 group 【NFVW】

  peer 【peer\_nfvw1\_address】 description 【peer\_nfvw1\_description】

  peer 【peer\_nfvw2\_address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw2\_address】 group 【NFVW】

  peer 【peer\_nfvw2\_address】 description 【peer\_nfvw2\_description】

  peer 【peer\_other-WC\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_address】 group 【other-WC】

  peer 【peer\_other-WC\_address】 description 【peer-other-WC-description】

  peer 【peer\_nfvw1\_ipv6-address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw1\_ipv6-address】 groupNFVW-IPv6

  peer 【peer\_nfvw1\_ipv6-address】 description 【peer\_nfvw1\_description】

  peer 【peer\_nfvw2\_ipv6-address】 as-number 【nfvw\_as】

  peer 【peer\_nfvw2\_ipv6-address】 groupNFVW-IPv6

  peer 【peer\_nfvw2\_ipv6-address】 description 【peer\_nfvw2\_description】

  peer 【peer\_other-WC\_ipv6\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_ipv6\_address】 group 【other-WC-ipv6】

  peer 【peer\_other-WC\_ipv6\_address】 description 【peer-other-WC-description】

  #

 address-family ipv4 unicast

   balance16

  preference 10 100 100

   peer 【NFVW】 enable

   peer 【NFVW】 route-policyFrom-NFVW import

   peer 【NFVW】 route-policyTo-NFVW export

   peer 【NFVW】default-route-advertise route-policy SetComm-2/2

   peer 【NFVW】advertise-community

   peer 【other-WC】 enable

   peer 【other-WC】route-policy 【From-other-WC】 import

   peer 【other-WC】 route-policy【To-other-WC】  export

   peer 【other-WC】advertise-community

  #

 address-family ipv6 unicast

   balance16

  preference 10 100 100

   network 【IPV6 network】 route-policySetComm-1/4

   peer 【NFVW-IPv6】 enable

   peer 【NFVW-IPv6】 route-policyFrom-NFVW-IPV6 import

   peer 【NFVW-IPv6】 route-policyTo-NFVW-IPV6 export

   peer 【NFVW-IPv6】default-route-advertise route-policy SetComm-2/2

   peer 【NFVW-IPv6】advertise-community

   peer 【other-WC-IPv6】 enable

   peer 【other-WC-IPv6】 route-policy 【From-other-WC-IPV6】 import

   peer 【other-WC-IPv6】 route-policy 【To-other-WC-IPV6】 export

   peer 【other-WC-IPv6】advertise-community

 #

 ipvpn-instance Outside\_BGP

  router-id 【loopback】

 compare-different-as-med

  group 【QCPL】 external

  peer 【QCPL】 passwordsimple 【peer\_password】

  group 【QCPL-IPv6】 external

  peer 【QCPL-IPv6】 passwordsimple 【peer\_password】

  group 【WC】 internal

  peer 【WC】 passwordsimple 【peer\_password】

  group 【WC-IPv6】 internal

  peer 【WC-IPv6】 passwordsimple 【peer\_password】

  group 【other-WC】 external

  peer 【other-WC】 password simple【other-WC-peer\_password】

  group 【other-WC-IPv6】 external

  peer 【other-WC-IPv6】 passwordsimple 【other-WC-peer\_password】

  peer 【peer\_QCPL\_address】 as-number 【qcpl-as】

  peer 【peer\_QCPL\_address】 group 【QCPL】

  peer 【peer\_QCPL\_address】 description 【peer\_QCPL\_description】

  peer 【peer\_WC\_address】 group 【WC】

  peer 【peer\_WC\_address】 description 【peer\_WC\_description】

  peer 【peer\_other-WC\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_address】 group 【other-WC】

  peer 【peer\_other-WC\_address】 description 【peer\_other-WC\_description】

  peer 【peer\_QCPL\_ipv6\_address】 as-number 【qcpl-as】

  peer 【peer\_QCPL\_ipv6\_address】 group 【QCPL-IPv6】

  peer 【peer\_QCPL\_ipv6\_address】 description 【peer\_QCPL\_description】

  peer 【peer\_WC\_ipv6\_address】 group 【WC-IPv6】

  peer 【peer\_WC\_ipv6\_address】 description 【peer\_WC\_description】

  peer 【peer\_other-WC\_ipv6\_address】 as-number 【other-WC\_as】

  peer 【peer\_other-WC\_ipv6\_address】 group 【other-WC-IPv6】

  peer 【peer\_other-WC\_ipv6\_address】 description 【peer\_other-WC\_description】

  #

 address-family ipv4 unicast

   balance16

  preference 10 100 100

   network 【WAN\_network】【WAN\_network\_mask】

   peer 【QCPL】 enable

   peer 【QCPL】 route-policyFrom-QCPL import

   peer 【QCPL】 route-policyTo-QCPL export

   peer 【WC】 enable

   peer 【WC】 advertise-community

   peer 【WC】 next-hop-local

   peer 【other-WC】 enable

   peer 【other-WC】route-policy 【From-other-WC】 import

   peer 【other-WC】 route-policy【To-other-WC】  export

   peer 【other-WC】advertise-community

  #

 address-family ipv6 unicast

   balance16

  preference 10 100 100

   network 【IPV6 network】 route-policySetComm-1/4

   peer 【QCPL-IPv6】 enable

   peer 【QCPL-IPv6】 route-policyFrom-QCPL-IPV6 import

   peer 【QCPL-IPv6】 route-policy To-QCPL-IPV6 export

   peer 【WC-IPv6】 enable

   peer 【WC-IPv6】 advertise-community

   peer 【WC-IPv6】 next-hop-local

   peer 【other-WC-IPv6】 enable

   peer 【other-WC-IPv6】 route-policy 【From-other-WC-IPV6】 import

   peer 【other-WC-IPv6】 route-policy 【To-other-WC-IPV6】 export

   peer 【other-WC-IPv6】 advertise-community

#

route-policy From-NFVW permit node 5

#

route-policy From-NFVW-IPV6 permit node 5

#

route-policy From-QCPL permit node 5

#

route-policy From-QCPL-IPV6 permit node 5

#

route-policy 【From-other-WC】 permit node 5

#

route-policy 【From-other-WC-IPV6】 permitnode 5

#

route-policy SetComm-1/1 permit node 5

 applycommunity 1:1

#

route-policy SetComm-1/4 permit node 5

 applycommunity 1:4

#

route-policy SetComm-2/2 permit node 5

 applycommunity 2:2

#

route-policy To-NFVW permit node 5

#

route-policy To-NFVW-IPV6 permit node 5

#

route-policy To-QCPL permit node 5

 if-match ipaddress prefix-list BGP\_ADV

#

route-policy To-QCPL deny node 10

#

route-policy To-QCPL-IPV6 permit node 5

 if-matchipv6 address prefix-list BGP-IPV6\_ADV

#

route-policy To-QCPL-IPV6 deny node 10

#

route-policy 【To-other-WC】 permit node 5

 if-matchcommunity 10

#

route-policy 【To-other-WC-IPV6】 permit node 5

 if-matchcommunity 10

#

 ipcommunity-list 10 permit 3:1

#

 ipprefix-list BGP\_ADV index 10 permit 【WAN\_network】 【WAN\_network\_mask】

 ipv6 prefix-listBGP-IPV6\_ADV index 10 permit 【WAN-IPV6\_network】

#

 schedulerlogfile size 16

#

line class aux

 user-rolenetwork-admin

#

line class vty

 user-rolenetwork-operator

#

line aux 0

 authentication-mode scheme

 user-rolenetwork-admin

#

line vty 0 63

 authentication-modescheme

 user-rolenetwork-admin

 user-rolenetwork-operator

 idle-timeout 5 0

#

#

 iproute-static vpn-instance mgt\_vrf 0.0.0.0 0 M-GigabitEthernet0/0/0 【MA\_address】 preference 5description Out-Of-Band-Management

 ip route-staticvpn-instance Inside\_WC 0.0.0.0 0 Vlan-interface100 【FW\_IN\_VIP】 preference 5tag 6000 description To-BFW-Inside

 iproute-static vpn-instance Outside\_WC 【WAN\_address】 【mask】Vlan-interface101 【FW\_OUT\_VIP】 preference 5 tag 5000 descriptionTo-BFW-Outside

 ipv6 route-staticvpn-instance Inside\_WC 0.0.0.0 0 Vlan-interface100 【FW\_IN\_VIP-IPV6】 preference 5tag 6000 description To-BFW-Inside-IPV6

 ipv6route-static vpn-instance Outside\_WC 【WAN-ipv6\_address】 【mask】Vlan-interface101 【FW\_OUT\_VIP-IPV6】 preference 5 tag 5000 descriptionTo-BFW-Outside-IPV6

#

 info-centerlogbuffer size 1024

 info-centerloghost source M-GigabitEthernet0/0/0

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_1】 facilitylocal2

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_2】 facilitylocal2

 info-centersource SHELL logbuffer deny

#

 snmp-agentcommunity read 【community】 acl 2001

 snmp-agentsys-info version v2c

 undosnmp-agent sys-info version v3

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_1】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_2】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttrap source M-GigabitEthernet0/0/0

 snmp-agentpacket max-size 17940

#

 ssh serverenable

 ssh serveracl 2000

#

 arp timeraging 5

#

 ntp-serviceenable

 ntp-servicesource M-GigabitEthernet0/0/0

 ntp-serviceunicast-server 【ntp\_address\_1】 vpn-instance mgt\_vrf

 ntp-serviceunicast-server 【ntp\_address\_2】 vpn-instance mgt\_vrf

#

acl basic 2000

 descriptionLogin-Filter

 rule  permit vpn-instance mgt\_vrf source 【gaya\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【cloud\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AAA\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【NTP\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AZ-network】 0

#

acl basic 2001

 descriptionSNMP-Filter

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_2】 0

#

 headerlogin %

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

             Authorized Access Only!

Disconnect IMMEDIATELY as you are not anauthorized user!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%

#

local-user 【local\_user】 class manage

 passwordsimple 【local\_password】

 service-type ssh terminal

 authorization-attribute user-rolenetwork-admin

#

return

#

save force

#

-----------------3A配置------------------------

#

hwtacacs scheme 【hwtacacs\_scheme】

 primaryauthentication 【first\_3A】

 primaryauthorization 【first\_3A】

 primaryaccounting 【first\_3A】

 secondaryauthentication 【second\_3A】

 secondaryauthorization 【second\_3A】

 secondaryaccounting 【second\_3A】

 keyauthentication simple 【3A\_key】

 keyauthorization simple 【3A\_key】

 keyaccounting simple 【3A\_key】

 user-name-format without-domain

 nas-ip 【nas\_ip】

 vpn-instance mgt\_vrf

#

domain 【hwtacacs\_domain】

 authentication login hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization login hwtacacs-scheme 【hwtacacs\_scheme】 local

 accountinglogin hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization command hwtacacs-scheme 【hwtacacs\_scheme】 none

 accountingcommand hwtacacs-scheme 【hwtacacs\_scheme】

#

domain system

 state block

#

 domaindefault enable 【hwtacacs\_domain】

#

line vty 0 63

command authorization

command accounting

#

line aux 0

command accounting

#

save force

#

-----------------镜像配置------------------------

#

#需根据需求是否配置

#

 mirroring-group 1 local

#

acl basic 2200

 rule 0 deny

#

acl advanced 3200                                                 //根据实际情况设定镜像源端口及地址

 descriptionYUJIE\_mirroring\_subnet

 rule   permit ip source 【mirror\_network】 【inverse mask】

 rule   comment 【mirror-port】-source

 rule   permit ip destination 【mirror\_network】 【inverse mask】

 rule   comment 【mirror-port】-destination

 rule 100deny ip

#

mirroring-group 1 mirroring-port 【source\_port】  inbound     //镜像源端口；WC对接QCPL端口

mirroring-group 1 mirroring-port 【source\_port】  inbound     //镜像源端口；WC对接BFW端口

mirroring-group 1 monitor-portBridge-Aggregation48             //镜像目的端口；WC对接MIRROR光交换机端口

#

vlan 10

 namemonitor-server

#

stp region-configuration

 region-nameWC

 revision-level 1

 instance 1vlan 500

 instance 2vlan 10

 activeregion-configuration

#

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation48

 description【OPT\_description】

 port accessvlan 10

 undoshutdown

#

interface FortyGigE1/0/53

 portlink-mode bridge

 description【OPT\_description】

 port accessvlan 10

 flow-interval 30

 packet-filter 2200 inbound

 packet-filter 3200 outbound

 portlink-aggregation group 48

 undoshutdown

#

save force

MIRROR光配置

聚合组：

二层

#1-2为对接WC聚合组编号

#3为对接镜像服务器聚合组编号

端口分配：

#1-2对接镜像服务器

#3-48，预留端口

#49-50对接WC

#51-54，预留端口

#管理口（M-GE0/0/0）

------------------------------------

!!刷配置前设置后重启生效命令

max-ecmp-num 16

 y

hardware-resource routing-mode ipv6-128

 y

#

public-key local create rsa

public-key local create dsa

save force

 reboot

 y

-------------------------------------

!!设备配置脚本

systeam

#

 sysname 【hostname】

#

 clocktimezone BeiJing add 08:00:00

#

ip vpn-instance mgt\_vrf

 route-distinguisher 2:1

#

 ipunreachables enable

 ipttl-expires enable

#

interface Bridge-Aggregation1

undo shutdown

#

interface Bridge-Aggregation2

undo shutdown

#

interface Bridge-Aggregation3

undo shutdown

#

mirroring-group 1 local

#

mirroring-group 1 mirroring-portBridge-Aggregation1   inbound

mirroring-group 1 mirroring-portBridge-Aggregation2  inbound

mirroring-group 1 monitor-port Bridge-Aggregation3

#

 lldp globalenable

#

 burst-modeenable

#

 fanprefer-direction slot 1 port-to-power

 password-recovery enable

#

vlan 1

#

vlan 10

 descriptionmonitor-server

#

stp region-configuration

 region-nameOPT

 revision-level 1

 instance 2vlan 10

 activeregion-configuration

#

 stpinstance 2 root primary

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation1

 description【WC1\_description】

 port accessvlan 10

 undo stpenable

#

interface Bridge-Aggregation2

 description【WC2\_description】

 port accessvlan 10

 undo stpenable

#

interface Bridge-Aggregation3

 descriptionmonitor-server

 port accessvlan 10

 link-aggregationload-sharing mode destination-ip source-ip

#

interface NULL0

#

interface LoopBack0

 ip address 【loopback】255.255.255.255

#

interface FortyGigE1/0/49     //对接WC镜像端口；源端口

 portlink-mode bridge

 description【WC1\_description】

 port accessvlan 10

 flow-interval 10

 packet-filter 2200 outbound

 portlink-aggregation group 1

#

interface FortyGigE1/0/50     //对接WC镜像端口；源端口

 portlink-mode bridge

 description【WC2\_description】

 port accessvlan 10

 flow-interval 10

 packet-filter 2200 outbound

 port link-aggregationgroup 2

#

interface FortyGigE1/0/51

 portlink-mode bridge

#

interface FortyGigE1/0/52

 portlink-mode bridge

#

interface FortyGigE1/0/53

 portlink-mode bridge

#

interface FortyGigE1/0/54

 portlink-mode bridge

#

interface M-GigabitEthernet0/0/0

 descriptionOut-Of-Band-Management

 ip bindingvpn-instance mgt\_vrf

 ip address 【MGT\_address】255.255.255.128

#

interface M-GigabitEthernet0/0/1

#

interface Ten-GigabitEthernet1/0/1   //对接NIPS服务器镜像端口；目的端口

 portlink-mode bridge

 descriptionTo-monitor-server

 port accessvlan 10

 flow-interval 10

 packet-filter 2200 inbound

 portlink-aggregation group 3

#

interface Ten-GigabitEthernet1/0/2   //对接NIPS服务器镜像端口；目的端口

 portlink-mode bridge

 descriptionTo-montior-server

 port accessvlan 10

 flow-interval 10

 packet-filter 2200 inbound

 portlink-aggregation group 3

#

interface Ten-GigabitEthernet1/0/3

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/4

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/5

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/6

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/7

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/8

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/9

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/10

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/11

 port link-modebridge

#

interface Ten-GigabitEthernet1/0/12

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/13

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/14

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/15

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/16

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/17

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/18

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/19

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/20

 port link-modebridge

#

interface Ten-GigabitEthernet1/0/21

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/22

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/23

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/24

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/25

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/26

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/27

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/28

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/29

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/30

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/31

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/32

 port link-modebridge

#

interface Ten-GigabitEthernet1/0/33

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/34

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/35

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/36

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/37

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/38

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/39

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/40

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/41

 port link-modebridge

#

interface Ten-GigabitEthernet1/0/42

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/43

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/44

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/45

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/46

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/47

 portlink-mode bridge

#

interface Ten-GigabitEthernet1/0/48

 portlink-mode bridge

#

 schedulerlogfile size 16

#

line class aux

 user-rolenetwork-admin

#

line class vty

 user-rolenetwork-operator

#

line aux 0

 authentication-mode scheme

 user-rolenetwork-admin

#

line vty 0 63

 authentication-mode scheme

 user-rolenetwork-admin

 user-rolenetwork-operator

 idle-timeout5 0

#

 iproute-static vpn-instance mgt\_vrf 0.0.0.0 0 M-GigabitEthernet0/0/0 【MA\_address】 preference 5tag 2002 description Out-Of-Band-Management

#

 info-centerlogbuffer size 1024

 info-centerloghost source M-GigabitEthernet0/0/0

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_1】 facilitylocal2

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_2】 facilitylocal2

 info-centersource SHELL logbuffer deny

#

 snmp-agent

 snmp-agentcommunity read 【community】 acl 2001

 snmp-agentsys-info version v2c

 undosnmp-agent sys-info version v3

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_1】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_2】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttrap source M-GigabitEthernet0/0/0

 snmp-agentpacket max-size 17940

#

 ssh serverenable

 ssh serveracl 2000

#

 arp timeraging 5

#

 ntp-serviceenable

 ntp-servicesource M-GigabitEthernet0/0/0

 ntp-serviceunicast-server 【ntp\_address\_1】 vpn-instance mgt\_vrf

 ntp-serviceunicast-server 【ntp\_address\_2】 vpn-instance mgt\_vrf

#

acl basic 2000

 descriptionLogin-Filter

 rule  permit vpn-instance mgt\_vrf source 【gaya\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【cloud\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AAA\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【NTP\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AZ-network】 0

#

acl basic 2001

 descriptionSNMP-Filter

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_2】 0

#

acl basic 2200

 rule 0 deny

#

 headerlogin %

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

             Authorized Access Only!

Disconnect IMMEDIATELY as you are not anauthorized user!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%

#

local-user 【local\_user】 class manage

 passwordsimple 【local\_password】

 service-type ssh terminal

 authorization-attribute user-role network-admin

#

return

-----------------3A配置------------------------

#

hwtacacs scheme 【hwtacacs\_scheme】

 primaryauthentication 【first\_3A】

 primaryauthorization 【first\_3A】

 primaryaccounting 【first\_3A】

 secondaryauthentication 【second\_3A】

 secondaryauthorization 【second\_3A】

 secondaryaccounting 【second\_3A】

 keyauthentication simple 【3A\_key】

 keyauthorization simple 【3A\_key】

 keyaccounting simple 【3A\_key】

 user-name-format without-domain

 nas-ip 【nas\_ip】

 vpn-instance mgt\_vrf

#

domain 【hwtacacs\_domain】

 authentication login hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization login hwtacacs-scheme 【hwtacacs\_scheme】 local

 accountinglogin hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization command hwtacacs-scheme 【hwtacacs\_scheme】 none

 accountingcommand hwtacacs-scheme 【hwtacacs\_scheme】

#

domain system

 state block

#

 domaindefault enable 【hwtacacs\_domain】

#

line vty 0 63

command authorization

command accounting

#

line aux 0

command accounting

NFVW1交换机配置

nfvw只是增加一个vlan接入网关，没有镜像配置

聚合组：

二层

#128为互联聚合组编号

端口分配：

#1-44对接服务器

#45-47，预留端口

#48对接探针

#49-50对接WC

#53-54互联

#管理口（M-GE0/0/0）

-------------------------------------

!!刷配置前设置后重启生效命令

 max-ecmp-num 16

 y

 hardware-resource routing-mode ipv6-128

 y

 #

 public-keylocal create rsa

 1024

 #

 public-keylocal create dsa

 1024

 #

 save force

 reboot

 y

-------------------------------------

!!设备配置脚本

#

 sysname 【sysname】

#

 clocktimezone BeiJing add 08:00:00

#

ip vpn-instance mgt\_vrf

 route-distinguisher 2:1

#

 irfmac-address persistent timer

 irf auto-updateenable

 undo irflink-delay

 irf member1 priority 1

#

#

ospf 203 router-id 【loopback】

 log-peer-change

 descriptionTGW-Route-Access

 non-stop-routing

 preference30

 preferencease 35

 spf-schedule-interval 1 50 200

 lsa-generation-interval 1 50 200

 bandwidth-reference 100000

 filter-policy prefix-list TGW-Route import

 area0.0.0.203

  network 【PM\_network】 0.0.0.127

#

ospfv3 203

 router-id 【loopback】

 log-peer-change

 non-stop-routing

 lsa-generation-interval 5 1000

 spf-schedule-interval 5 1000

 preference30

 preferencease 35

 bandwidth-reference100000

 area0.0.0.203

#

 ipunreachables enable

 ipttl-expires enable

#

 ipload-sharing mode per-flow dest-ip src-ip global

#

 lldpignore-pvid-inconsistency

 lldp globalenable

#

 burst-modeenable

#

 fanprefer-direction slot 1 port-to-power

 password-recovery enable

#

vlan 203

 descriptionTGW-Route-Access

#

vlan 252

 descriptionTGW-Underlay-NAT

#

vlan 263

 descriptionmirror-Access

#

vlan 250 to 300

#

stp region-configuration

 region-nameNFVW

 revision-level1

 activeregion-configuration

#

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation128

 description【NFVW2\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 link-aggregation mode dynamic

 undoshutdown

#

interface LoopBack0

 ip address 【loopback】255.255.255.255

 ipv6address 【ipv6\_loopback】

#

interface Vlan-interface203

 descriptionTGW-Route-Access

 ip address 【PM\_network】255.255.255.128

 ospfauthentication-mode md5 1 plain 【ospf\_password】

 ospf timerhello 1

 ospf timerdead 10

 ospfdr-priority 255

 ospfv3 203area 0.0.0.203

 ospfv3dr-priority 255

 ospfv3timer hello 1

 ospfv3timer dead 10

 ospfv3mtu-ignore

 ipv6address 【PM\_ipv6-address】

 undoshutdown

#

interface Vlan-interface252

 descriptionTGW-Underlay-NAT

 ip address 【PM\_network】255.255.255.128

 ipv6address 【PM\_ipv6-address】

 undoshutdown

#

interface Vlan-interface263

 descriptionmirror-Access

 ip address 【PM\_Gateway】  【mask】

 undoshutdown

#

interface FortyGigE1/0/49

 portlink-mode route

 description【WC1\_description】

 flow-interval 30

 ip address 【NFVW1\_address】255.255.255.254

 ipv6address 【NFVW1\_ipv6-address】 【mask】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undo shutdown

#

interface FortyGigE1/0/50

 port link-moderoute

 description【WC2\_description】

 flow-interval 30

 ip address 【NFVW1\_address】255.255.255.254

 ipv6address 【NFVW1\_ipv6-address】 【mask】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/51

 portlink-mode bridge

#

interface FortyGigE1/0/52

 portlink-mode bridge

#

interface FortyGigE1/0/53

 portlink-mode bridge

 description【NFVW2\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 flow-interval 30

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/54

 portlink-mode bridge

 description【NFVW2\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 flow-interval 30

 portlink-aggregation group 128

 undoshutdown

#

interface M-GigabitEthernet0/0/0

 descriptionOut-Of-Band-Management

 ip bindingvpn-instance mgt\_vrf

 ip address 【MGT\_address】255.255.255.128

#

###以下端口用作对接相应服务器，具体端口号对应VLAN需依据使用情况进行分配####

#

interface Ten-GigabitEthernet1/0/1

 portlink-mode bridge

 port accessvlan 【】                                        //VLAN待定

 description【】                                               //依据VLAN使用，进行相关描述

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/2

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/3

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/4

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/5

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/6

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/7

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/8

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/9

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/10

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/11

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/12

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/13

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/14

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/15

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/16

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/17

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/18

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/19

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/20

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/21

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/22

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/23

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/24

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trust dscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/25

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/26

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/27

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/28

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/29

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/30

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/31

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/32

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/33

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/34

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/35

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/36

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/37

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/38

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/39

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trust dscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/40

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/41

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/42

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/43

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/44

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/45

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/46

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/47

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/48

 portlink-mode bridge

 port accessvlan 263                                                     //镜像阻断VLAN

 descriptionmirror-Access

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undo shutdown

#

bgp 【bgp\_as】

 non-stop-routing

 router-id 【loopback】

 compare-different-as-med

 group NFVWinternal

 peer NFVWpassword simple 【peer\_password】

 groupNFVW-IPv6 internal

 peerNFVW-IPv6 simple 【peer\_password】

 group WCexternal

 peer WCas-number 【WC\_AS】

 peer WCpassword simple 【peer\_password】

 groupWC-IPv6 external

 peerWC-IPv6 as-number 【WC\_AS】

 peerWC-IPv6 password simple 【peer\_password】

 peer 【peer\_NFVW\_address】 group NFVW

 peer 【peer\_NFVW\_address】 description 【peer\_NFVW\_description】

 peer 【peer\_WC1\_address】 group WC

 peer 【peer\_WC1\_address】 description 【peer\_WC1\_description】

 peer 【peer\_WC2\_address】 group WC

 peer 【peer\_WC2\_address】 description 【peer\_WC2\_description】

 peer 【peer\_NFVW\_ipv6-address】 group NFVW-IPv6

 peer 【peer\_NFVW\_ipv6-address】 description【peer\_NFVW\_description】

 peer 【peer\_WC1\_ipv6-address】 group WC-IPv6

 peer 【peer\_WC1\_ipv6-address】 description 【peer\_WC1\_description】

 peer 【peer\_WC2\_ipv6-address】 group WC-IPv6

 peer 【peer\_WC2\_ipv6-address】 description 【peer\_WC2\_description】

 #

 address-family ipv4 unicast

  balance 16

  preference10 100 100

 import-route ospf 203 route-policy Match-Odd-Even

  network 【loopback】255.255.255.255 route-policy SetComm-1/4

  network 【PM\_network1】 【PM\_network1\_mask】 route-policySetComm-1/1

  network 【PM\_network2】 【PM\_network2\_mask】 route-policySetComm-1/1

  network 【WAN\_network】 【WAN\_network\_mask】

  peer WCenable

  peer WCroute-policy From-WC import

  peer WCroute-policy To-WC export

  peer WCadvertise-community

  peer NFVWenable

  peer NFVWroute-policy From-NFVW import

  peer NFVWroute-policy To-NFVW export

  peer NFVWadvertise-community

  peer NFVWnext-hop-local

 #

 address-family ipv6 unicast

  balance 16

  preference10 100 100

 import-route ospfv3 252 route-policy Match-Odd-Even-IPv6

  network 【ipv6\_loopback】 128route-policy SetComm-1/4

  network 【PM\_ipv6-network1】 route-policySetComm-1/1

  network 【PM\_ipv6-network2】 route-policySetComm-1/1

  network 【WAN\_ipv6-network】

  peerNFVW-IPv6 enable

  peerNFVW-IPv6 route-policy From-NFVW-IPv6 import

  peerNFVW-IPv6 route-policy To-NFVW-IPv6 export

  peerNFVW-IPv6 advertise-community

  peerNFVW-IPv6 next-hop-local

  peerWC-IPv6 enable

  peerWC-IPv6 route-policy From-WC-IPv6 import

  peer WC-IPv6route-policy To-WC-IPv6 export

  peer WC-IPv6advertise-community

#

route-policy From-NFVW permit node 5

#

route-policy From-NFVW-IPV6 permit node 5

#

route-policy From-WC permit node 5

#

route-policy From-WC-IPV6 permit node 5

#

route-policy Match-Odd-Even permit node 5

 if-match ipaddress  acl 3001

 applycommunity 3:1

 apply cost1000

#

route-policy Match-Odd-Even permit node 10

 if-match ipaddress  acl 3002

 applycommunity 3:1

 apply cost2000

#

route-policy Match-Odd-Even permit node 15

 if-match ipaddress acl 3000

 applycommunity 1:7

 apply cost1000

#

route-policy Match-Odd-Even permit node 20

 applycommunity 1:7

 apply cost2000

#

route-policy Match-Odd-Even-IPv6 permit node 5

 if-matchipv6 address acl 3000

 applycommunity 1:7

 apply cost1000

#

route-policy Match-Odd-Even-IPv6 permit node 10

 applycommunity 1:7

 apply cost2000

#

route-policy SetComm-1/1 permit node 5

 applycommunity 1:1

#

route-policy SetComm-1/4 permit node 5

 applycommunity 1:4

#

route-policy To-NFVW permit node 5

#

route-policy To-NFVW-IPV6 permit node 5

#

route-policy To-WC permit node 5

#

route-policy To-WC-IPV6 permit node 5

#

#掩码长度根据实际情况确定

------------------------

ip prefix-list TGW-Route index 5 permit   【VLAN203-PM\_network】 25greater-equal 32

ip prefix-list TGW-Route index 10 permit 【WAN\_network】  【mask】 greater-equal 32

ip prefix-list TGW-Route index 15 permit 【WAN\_network】  【mask】 greater-equal 28  less-equal 28

ip prefix-list TGW-Route index 20 permit 【WAN\_network】  【mask】 greater-equal 27  less-equal 27

#

 schedulerlogfile size 16

#

line class aux

 user-rolenetwork-admin

#

line class vty

 user-rolenetwork-operator

#

line aux 0

 authentication-mode scheme

 user-rolenetwork-admin

#

line vty 0 63

 authentication-mode scheme

 user-rolenetwork-admin

 user-rolenetwork-operator

 idle-timeout 5 0

#

 iproute-static vpn-instance mgt\_vrf 0.0.0.0 0 M-GigabitEthernet0/0/0 【MA\_address】 preference 5tag 2002description Out-Of-Band-Management

#

 info-centerlogbuffer size 1024

 info-centerloghost source M-GigabitEthernet0/0/0

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_1】 facilitylocal2

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_2】 facilitylocal2

 info-centersource SHELL logbuffer deny

#

 snmp-agentcommunity read 【community】 acl 2001

 snmp-agentsys-info version v2c

 undo snmp-agentsys-info version v3

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_1】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_2】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttrap source M-GigabitEthernet0/0/0

 snmp-agentpacket max-size 17940

#

 ssh serverenable

 ssh serveracl 2000

#

 ntp-serviceenable

 ntp-servicesource M-GigabitEthernet0/0/0

 ntp-serviceunicast-server 【ntp\_address\_1】 vpn-instance mgt\_vrf

 ntp-serviceunicast-server 【ntp\_address\_2】 vpn-instance mgt\_vrf

#

 arp timeraging 5

#

acl basic 2000

 descriptionLogin-Filter

 rule  permit vpn-instance mgt\_vrf source 【gaya\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【cloud\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AAA\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【NTP\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AZ-network】 0

#

acl basic 2001

 descriptionSNMP-Filter

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_2】 0

#

acl number 3000

 descriptionMatch-Odd-Even

 rule  permit ip source 0.0.0.1 255.255.255.254destination 255.255.255.255 0

#

acl number 3001

 descriptionMatch-Front-Mask28andMask27

 rule  permit ip source 0.0.0.0 255.255.255.239destination 255.255.255.240 0.0.0.0   //掩码前/28

 rule  permit ip source 0.0.0.0 255.255.255.255destination 255.255.255.224 0.0.0.0   //掩码/27

#

acl number 3002

 descriptionMatch-Rear-Mask28

 rule  permit ip source 0.0.0.16 255.255.255.239destination 255.255.255.240 0.0.0.0  //掩码后/28

#

acl ipv6 advanced 3000

 descriptionMatch-Odd-Even-IPv6

 rule 0permit ipv6 source 【ipv6\_address】

#

 header login%

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

             Authorized Access Only!

Disconnect IMMEDIATELY as you are not anauthorized user!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%

#

local-user 【local\_user】 class manage

 passwordsimple 【local\_password】

 service-typessh terminal

 authorization-attribute user-rolenetwork-admin

#

return

#

save force

-----------------3A配置------------------------

#

hwtacacs scheme 【hwtacacs\_scheme】

 primaryauthentication 【first\_3A】

 primary authorization【first\_3A】

 primaryaccounting 【first\_3A】

 secondaryauthentication 【second\_3A】

 secondaryauthorization 【second\_3A】

 secondaryaccounting 【second\_3A】

 keyauthentication simple 【3A\_key】

 keyauthorization simple 【3A\_key】

 keyaccounting simple 【3A\_key】

 user-name-format without-domain

 nas-ip 【nas\_ip】

 vpn-instance mgt\_vrf

#

domain 【hwtacacs\_domain】

 authentication login hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization login hwtacacs-scheme 【hwtacacs\_scheme】 local

 accountinglogin hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorizationcommand hwtacacs-scheme 【hwtacacs\_scheme】 none

 accountingcommand hwtacacs-scheme 【hwtacacs\_scheme】

#

domain system

 state block

#

 domaindefault enable 【hwtacacs\_domain】

#

line vty 0 63

command authorization

command accounting

#

line aux 0

command accounting

#

save force

#

NFVW2交换机配置

聚合组：

二层

#128为互联聚合组编号

端口分配：

#1-44对接服务器

#45-47，预留端口

#48对接探针

#49-50对接WC

#53-54互联

#管理口（M-GE0/0/0）

-------------------------------------

!!刷配置前设置后重启生效命令

 max-ecmp-num 16

 y

 hardware-resourcerouting-mode ipv6-128

 y

 #

 public-keylocal create rsa

 1024

 #

 public-keylocal create dsa

 1024

 #

 save force

 reboot

 y

-------------------------------------

!!设备配置脚本

#

 sysname 【sysname】

#

 clocktimezone BeiJing add 08:00:00

#

ip vpn-instance mgt\_vrf

 route-distinguisher 2:1

#

 irfmac-address persistent timer

 irfauto-update enable

 undo irflink-delay

 irf member1 priority 1

#

#

ospf 203 router-id 【loopback】

 log-peer-change

 descriptionTGW-Route-Access

 non-stop-routing

 preference30

 preferencease 35

 spf-schedule-interval1 50 200

 lsa-generation-interval 1 50 200

 bandwidth-reference 100000

 filter-policy prefix-list TGW-Route import

 area0.0.0.203

  network 【PM\_network】 0.0.0.127

#

ospfv3 203

 router-id 【loopback】

 log-peer-change

 non-stop-routing

 lsa-generation-interval5 1000

 spf-schedule-interval 5 1000

 preference30

 preferencease 35

 bandwidth-reference 100000

 area0.0.0.203

#

 ipunreachables enable

 ipttl-expires enable

#

 ipload-sharing mode per-flow dest-ip src-ip global

#

 lldpignore-pvid-inconsistency

 lldp globalenable

#

 burst-modeenable

#

 fanprefer-direction slot 1 port-to-power

 password-recovery enable

#

vlan 203

 descriptionTGW-Route-Access

#

vlan 252

 descriptionTGW-Underlay-NAT

#

vlan 263

 descriptionmirror-Access

#

vlan 250 to 300

#

stp region-configuration

 region-nameNFVW

 revision-level 1

 activeregion-configuration

#

 stpbpdu-protection

 stp globalenable

#

interface Bridge-Aggregation128

 description【NFVW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 link-aggregation mode dynamic

 undoshutdown

#

interface LoopBack0

 ip address 【loopback】255.255.255.255

 ipv6address 【ipv6\_loopback】

#

interface Vlan-interface203

 descriptionTGW-Route-Access

 ip address 【PM\_network】255.255.255.128

 ospfauthentication-mode md5 1 plain 【ospf\_password】

 ospf timerhello 1

 ospf timerdead 10

 ospfdr-priority 254

 ospfv3 203area 0.0.0.203

 ospfv3dr-priority 254

 ospfv3timer hello 1

 ospfv3timer dead 10

 ospfv3mtu-ignore

 ipv6 address【PM\_ipv6-address】

 undoshutdown

#

interface Vlan-interface252

 descriptionTGW-Underlay-NAT

 ip address 【PM\_network】255.255.255.128

 ipv6address 【PM\_ipv6-address】

 undoshutdown

#

interface Vlan-interface263

 descriptionmirror-Access

 ip address 【PM\_Gateway】  【mask】

 undoshutdown

#

interface FortyGigE1/0/49

 portlink-mode route

 description【WC1\_description】

 flow-interval 30

 ip address 【NFVW2\_address】255.255.255.254

 ipv6address 【NFVW2\_ipv6-address】 【mask】

 lldptlv-enable basic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/50

 portlink-mode route

 description【WC2\_description】

 flow-interval 30

 ip address 【NFVW2\_address】255.255.255.254

 ipv6 address【NFVW2\_ipv6-address】 【mask】

 lldp tlv-enablebasic-tlv management-address-tlv 【MGT\_address】

 qos trustdscp

 undoshutdown

#

interface FortyGigE1/0/51

 portlink-mode bridge

#

interface FortyGigE1/0/52

 portlink-mode bridge

#

interface FortyGigE1/0/53

 portlink-mode bridge

 description【NFVW1\_description】

 portlink-type trunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 flow-interval 30

 portlink-aggregation group 128

 undoshutdown

#

interface FortyGigE1/0/54

 portlink-mode bridge

 description【NFVW1\_description】

 port link-typetrunk

 undo porttrunk permit vlan 1

 port trunkpermit vlan 203 252

 flow-interval 30

 portlink-aggregation group 128

 undoshutdown

#

interface M-GigabitEthernet0/0/0

 descriptionOut-Of-Band-Management

 ip bindingvpn-instance mgt\_vrf

 ip address 【MGT\_address】255.255.255.128

#

###以下端口用作对接相应服务器，具体端口号对应VLAN需依据使用情况进行分配####

#

interface Ten-GigabitEthernet1/0/1

 portlink-mode bridge

 port accessvlan 【】                                        //VLAN待定

 description【】                                                //依据VLAN使用，进行相关描述

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/2

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/3

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/4

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/5

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/6

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/7

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/8

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/9

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/10

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/11

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/12

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/13

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/14

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/15

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/16

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/17

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/18

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/19

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/20

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/21

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/22

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/23

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/24

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/25

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/26

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/27

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trust dscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/28

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/29

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/30

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/31

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/32

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/33

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/34

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/35

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/36

 portlink-mode bridge

 flow-interval30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/37

 portlink-mode bridge

 flow-interval 30

 broadcast-suppressionkbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/38

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/39

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppressionkbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/40

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/41

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/42

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stp edged-port

 lldpadmin-status rx

 qos trust dscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/43

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldp admin-statusrx

 qos trustdscp

 undo shutdown

#

interface Ten-GigabitEthernet1/0/44

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/45

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/46

 portlink-mode bridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/47

 port link-modebridge

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

interface Ten-GigabitEthernet1/0/48

 portlink-mode bridge

 port accessvlan 263                                                    //镜像阻断VLAN

 descriptionmirror-Access

 flow-interval 30

 broadcast-suppression kbps 10000

 unicast-suppression kbps 10000

 multicast-suppression 1

 stpedged-port

 lldpadmin-status rx

 qos trustdscp

 undoshutdown

#

bgp 【bgp\_as】

 non-stop-routing

 router-id 【loopback】

 compare-different-as-med

 group NFVWinternal

 peer NFVWpassword simple 【peer\_password】

 group NFVW-IPv6internal

 peerNFVW-IPv6 simple 【peer\_password】

 group WCexternal

 peer WCas-number 【WC\_AS】

 peer WCpassword simple 【peer\_password】

 groupWC-IPv6 external

 peerWC-IPv6 as-number 【WC\_AS】

 peerWC-IPv6 password simple 【peer\_password】

 peer 【peer\_NFVW\_address】 group NFVW

 peer 【peer\_NFVW\_address】 description 【peer\_NFVW\_description】

 peer 【peer\_WC1\_address】 group WC

 peer 【peer\_WC1\_address】 description 【peer\_WC1\_description】

 peer 【peer\_WC2\_address】 group WC

 peer 【peer\_WC2\_address】 description 【peer\_WC2\_description】

 peer 【peer\_NFVW\_ipv6-address】 groupNFVW-IPv6

 peer 【peer\_NFVW\_ipv6-address】 description【peer\_NFVW\_description】

 peer 【peer\_WC1\_ipv6-address】 group WC-IPv6

 peer 【peer\_WC1\_ipv6-address】 description 【peer\_WC1\_description】

 peer 【peer\_WC2\_ipv6-address】 group WC-IPv6

 peer 【peer\_WC2\_ipv6-address】 description 【peer\_WC2\_description】

 #

 address-family ipv4 unicast

  balance 16

  preference10 100 100

 import-route ospf 203 route-policy Match-Odd-Even

  network 【loopback】 255.255.255.255 route-policySetComm-1/4

  network 【PM\_network1】 【PM\_network1\_mask】 route-policySetComm-1/1

  network 【PM\_network2】 【PM\_network2\_mask】 route-policySetComm-1/1

  network 【WAN\_network】 【WAN\_network\_mask】

  peer WC enable

  peer WCroute-policy From-WC import

  peer WCroute-policy To-WC export

  peer WCadvertise-community

  peer NFVWenable

  peer NFVWroute-policy From-NFVW import

  peer NFVWroute-policy To-NFVW export

  peer NFVWadvertise-community

  peer NFVWnext-hop-local

 #

 address-family ipv6 unicast

  balance 16

  preference10 100 100

 import-route ospfv3 252 route-policy Match-Odd-Even-IPv6

  network 【ipv6\_loopback】 128route-policy SetComm-1/4

  network 【PM\_ipv6-network1】 route-policySetComm-1/1

  network 【PM\_ipv6-network2】 route-policySetComm-1/1

  network 【WAN\_ipv6-network】

  peerNFVW-IPv6 enable

  peerNFVW-IPv6 route-policy From-NFVW-IPv6 import

  peerNFVW-IPv6 route-policy To-NFVW-IPv6 export

  peerNFVW-IPv6 advertise-community

  peerNFVW-IPv6 next-hop-local

  peerWC-IPv6 enable

  peer WC-IPv6route-policy From-WC-IPv6 import

  peerWC-IPv6 route-policy To-WC-IPv6 export

  peerWC-IPv6 advertise-community

#

route-policy From-NFVW permit node 5

#

route-policy From-NFVW-IPV6 permit node 5

#

route-policy From-WC permit node 5

#

route-policy From-WC-IPV6 permit node 5

#

route-policy Match-Odd-Even permit node 5

 if-match ipaddress  acl 3001

 applycommunity 3:1

 apply cost2000

#

route-policy Match-Odd-Even permit node 10

 if-match ipaddress  acl 3002

 applycommunity 3:1

 apply cost1000

#

route-policy Match-Odd-Even permit node 15

 if-match ipaddress acl 3000

 applycommunity 1:7

 apply cost1000

#

route-policy Match-Odd-Even permit node 20

 applycommunity 1:7

 apply cost2000

#

route-policy Match-Odd-Even-IPv6 permit node 5

 if-match ipv6address acl 3000

 applycommunity 1:7

 apply cost1000

#

route-policy Match-Odd-Even-IPv6 permit node 10

 applycommunity 1:7

 apply cost2000

#

route-policy SetComm-1/1 permit node 5

 applycommunity 1:1

#

route-policy SetComm-1/4 permit node 5

 applycommunity 1:4

#

route-policy To-NFVW permit node 5

#

route-policy To-NFVW-IPV6 permit node 5

#

route-policy To-WC permit node 5

#

route-policy To-WC-IPV6 permit node 5

#

#掩码长度根据实际情况确定

------------------------

ip prefix-list TGW-Route index 5 permit   【VLAN203-PM\_network】 25greater-equal 32

ip prefix-list TGW-Route index 10 permit 【WAN\_network】  【mask】 greater-equal 32

ip prefix-list TGW-Route index 15 permit 【WAN\_network】  【mask】 greater-equal 28  less-equal 28

ip prefix-list TGW-Route index 20 permit 【WAN\_network】  【mask】 greater-equal 27  less-equal 27

#

 schedulerlogfile size 16

#

line class aux

 user-rolenetwork-admin

#

line class vty

 user-rolenetwork-operator

#

line aux 0

 authentication-mode scheme

 user-rolenetwork-admin

#

line vty 0 63

 authentication-modescheme

 user-rolenetwork-admin

 user-rolenetwork-operator

 idle-timeout 5 0

#

 iproute-static vpn-instance mgt\_vrf 0.0.0.0 0 M-GigabitEthernet0/0/0 【MA\_address】 preference 5tag 2002description Out-Of-Band-Management

#

 info-centerlogbuffer size 1024

 info-centerloghost source M-GigabitEthernet0/0/0

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_1】 facilitylocal2

 info-centerloghost vpn-instance mgt\_vrf 【log\_address\_2】 facility local2

 info-centersource SHELL logbuffer deny

#

 snmp-agentcommunity read 【community】 acl 2001

 snmp-agentsys-info version v2c

 undosnmp-agent sys-info version v3

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_1】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttarget-host trap address udp-domain 【snmp\_address\_2】 vpn-instancemgt\_vrf params securityname 【community】 v2c

 snmp-agenttrap source M-GigabitEthernet0/0/0

 snmp-agentpacket max-size 17940

#

 ssh serverenable

 ssh serveracl 2000

#

 ntp-serviceenable

 ntp-servicesource M-GigabitEthernet0/0/0

 ntp-serviceunicast-server 【ntp\_address\_1】 vpn-instance mgt\_vrf

 ntp-serviceunicast-server 【ntp\_address\_2】 vpn-instance mgt\_vrf

#

 arp timeraging 5

#

acl basic 2000

 descriptionLogin-Filter

 rule  permit vpn-instance mgt\_vrf source 【gaya\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【cloud\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AAA\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【NTP\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【AZ-network】 0

#

acl basic 2001

 descriptionSNMP-Filter

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_1】 0

 rule  permit vpn-instance mgt\_vrf source 【snmp\_address\_2】 0

#

acl number 3000

 descriptionMatch-Odd-Even

 rule  permit ip source 0.0.0.0 255.255.255.254destination 255.255.255.255 0

#

acl number 3001

 descriptionMatch-Front-Mask28andMask27

 rule  permit ip source 0.0.0.0 255.255.255.239destination 255.255.255.240 0.0.0.0   //掩码前/28

 rule  permit ip source 0.0.0.0 255.255.255.255destination 255.255.255.224 0.0.0.0   //掩码/27

#

acl number 3002

 descriptionMatch-Rear-Mask28

 rule  permit ip source 0.0.0.16 255.255.255.239destination 255.255.255.240 0.0.0.0  //掩码后/28

#

acl ipv6 advanced 3000

 descriptionMatch-Odd-Even-IPv6

 rule 0permit ipv6 source 【ipv6\_address】

#

 headerlogin %

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

             Authorized Access Only!

Disconnect IMMEDIATELY as you are not anauthorized user!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*%

#

local-user 【local\_user】 class manage

 passwordsimple 【local\_password】

 service-type ssh terminal

 authorization-attribute user-rolenetwork-admin

#

return

#

save force

-----------------3A配置------------------------

#

hwtacacs scheme 【hwtacacs\_scheme】

 primaryauthentication 【first\_3A】

 primaryauthorization 【first\_3A】

 primaryaccounting 【first\_3A】

 secondaryauthentication 【second\_3A】

 secondaryauthorization 【second\_3A】

 secondaryaccounting 【second\_3A】

 keyauthentication simple 【3A\_key】

 keyauthorization simple 【3A\_key】

 keyaccounting simple 【3A\_key】

 user-name-format without-domain

 nas-ip 【nas\_ip】

 vpn-instance mgt\_vrf

#

domain 【hwtacacs\_domain】

 authentication login hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization login hwtacacs-scheme 【hwtacacs\_scheme】 local

 accountinglogin hwtacacs-scheme 【hwtacacs\_scheme】 local

 authorization command hwtacacs-scheme 【hwtacacs\_scheme】 none

 accountingcommand hwtacacs-scheme 【hwtacacs\_scheme】

#

domain system

 state block

#

 domaindefault enable 【hwtacacs\_domain】

#

line vty 0 63

command authorization

command accounting

#

line aux 0

command accounting

#

save force

#

部署常见错误

生产组件部署常见错误

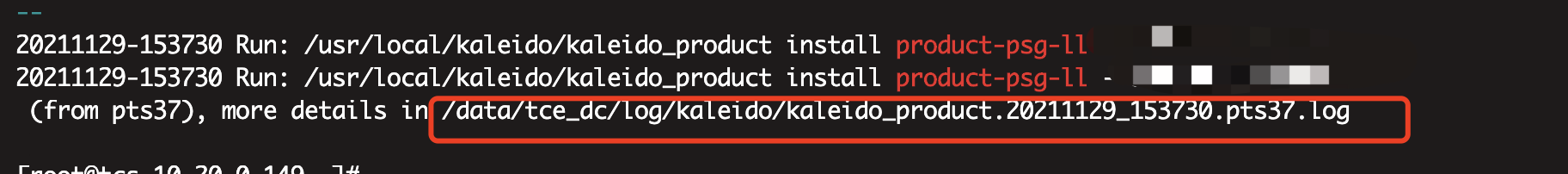
主动排查错误

1. kaleido部署日志

在master机器上使用命令查询部署生产组件后是否产生错误

kaleido\_history |grep -A2 psg

返回



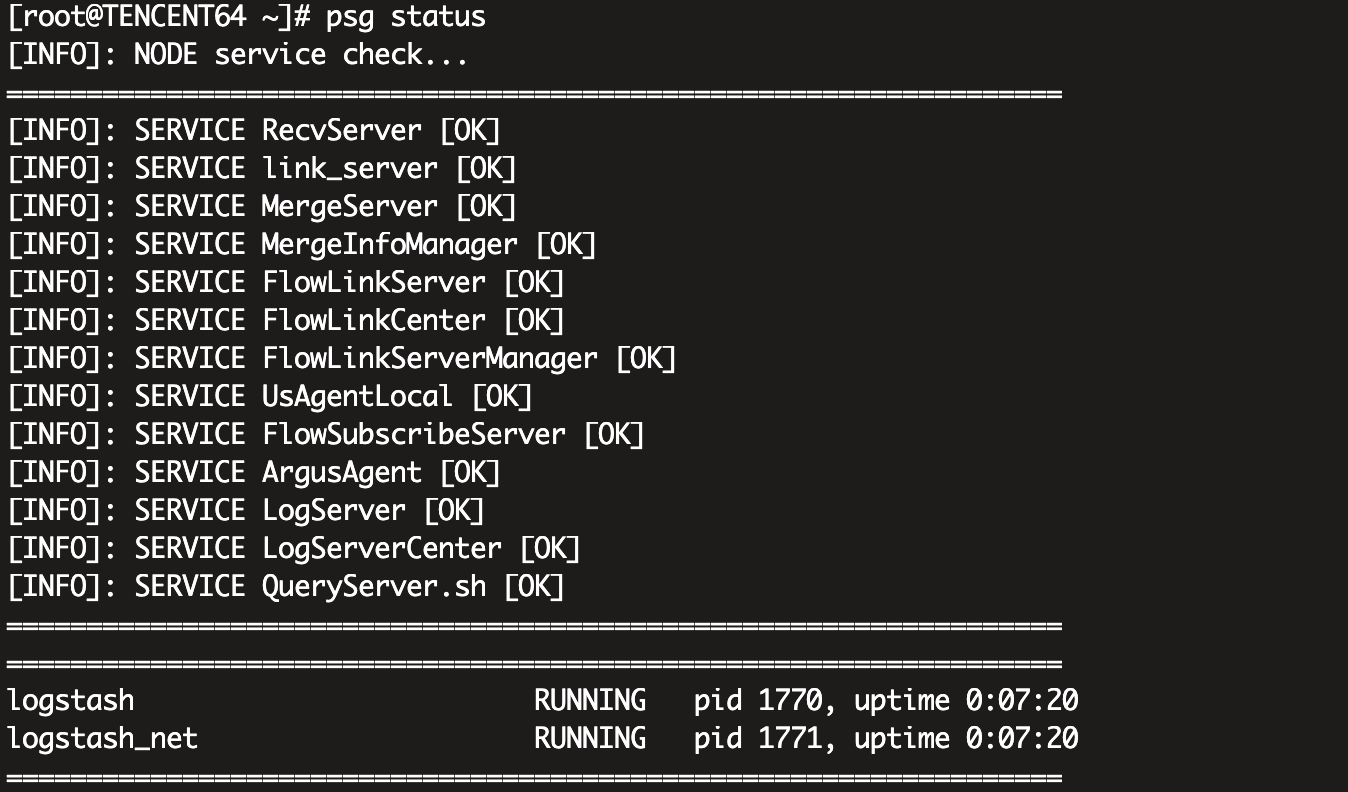
然后查看红框的log内容，发现部署过程中明显报错，根据报错内容进行排查和反馈。

1. 生产组件（探针服务器）服务状态

执行命令查看服务状态

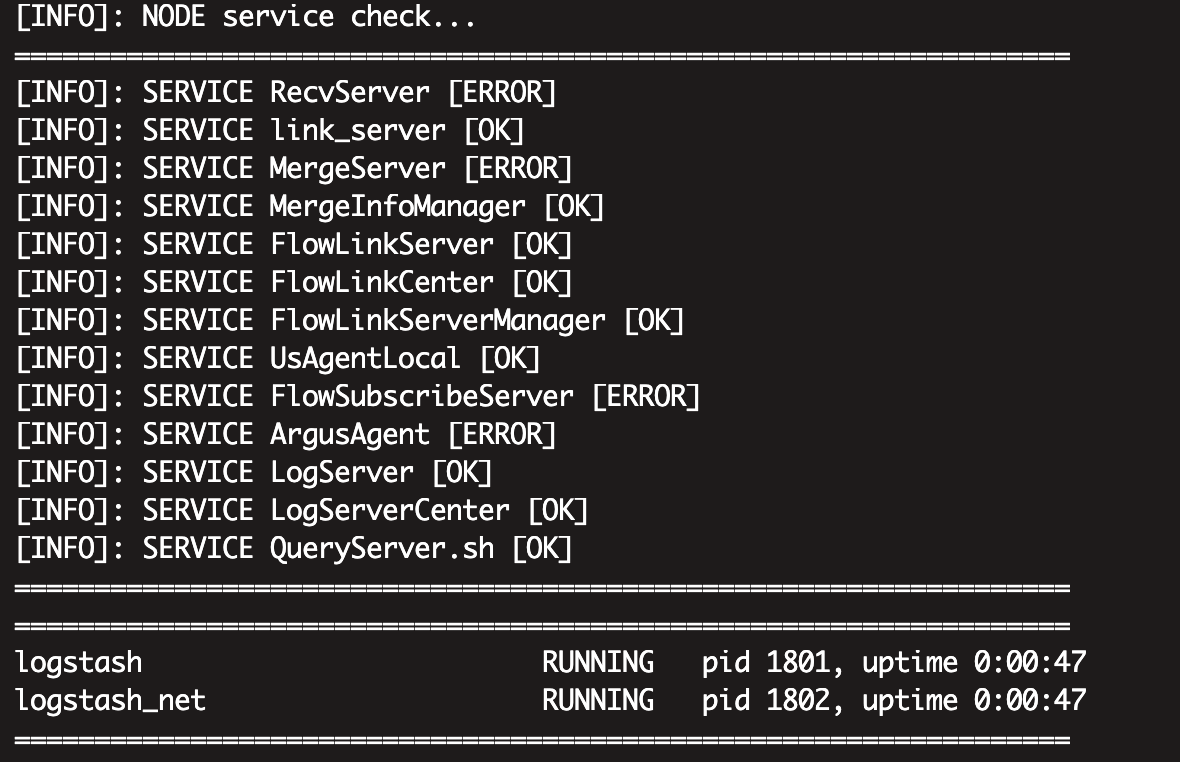
psg status

查看返回



一般来说，RecvServer如果ok，那么代表探针服务状态正常，

服务器开机后并不是马上全部都ok，会逐步变成ok。recvserver状态正常的稍慢。



然后recvserver 正常后mergerserver和argusAgent会正常，强依赖关系。



1. recvserver服务状态

查看recvserver的日志内容判断探针状态

tail -f /home/oicq/argus/RecvServer/log/RecvServer.log| grep System

查看recvserver启动显示内容判断探针状态

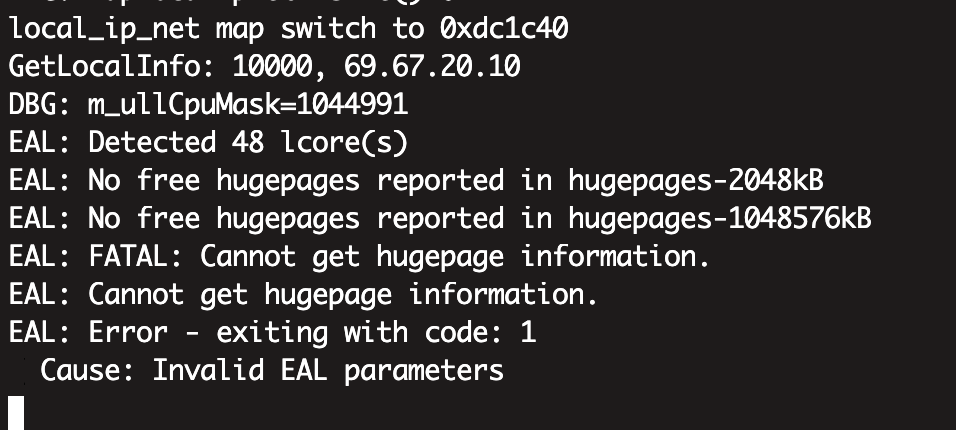
cd /home/oicq/argus/RecvServer/scripts;./svr.sh restart

常见报错

1. recvserver启动报错，大页内存（hugepage）报错

报错来源 8.6.1.1 3 recvserver服务状态，启动探针报错

关键字 hugepage



问题原因：

服务器及系统问题，hugepage设置和recvserver要求不匹配，执行命令查询当前hugepage内存设置

grep Huge /proc/meminfo



上图是正常的值，如果值不是很大，比如2000kb，就是错误的，没有正确被设置。

解决办法：

X86:

grep 'huge' /etc/default/grub

编辑这行，后边加上 default\_hugepagesz=1G hugepagesz=1G hugepages=92



然后执行

grub2-mkconfig -o /boot/grub2/grub.cfg

重启服务器，使大页内存设置生效。

ARM：

grep 'huge' /etc/default/grub

编辑这行，后边加上 default\_hugepagesz=512M hugepagesz=512M hugepages=200



然后执行

grub2-mkconfig -o /boot/grub2/grub.cfg

重启服务器，使大页内存设置生效。

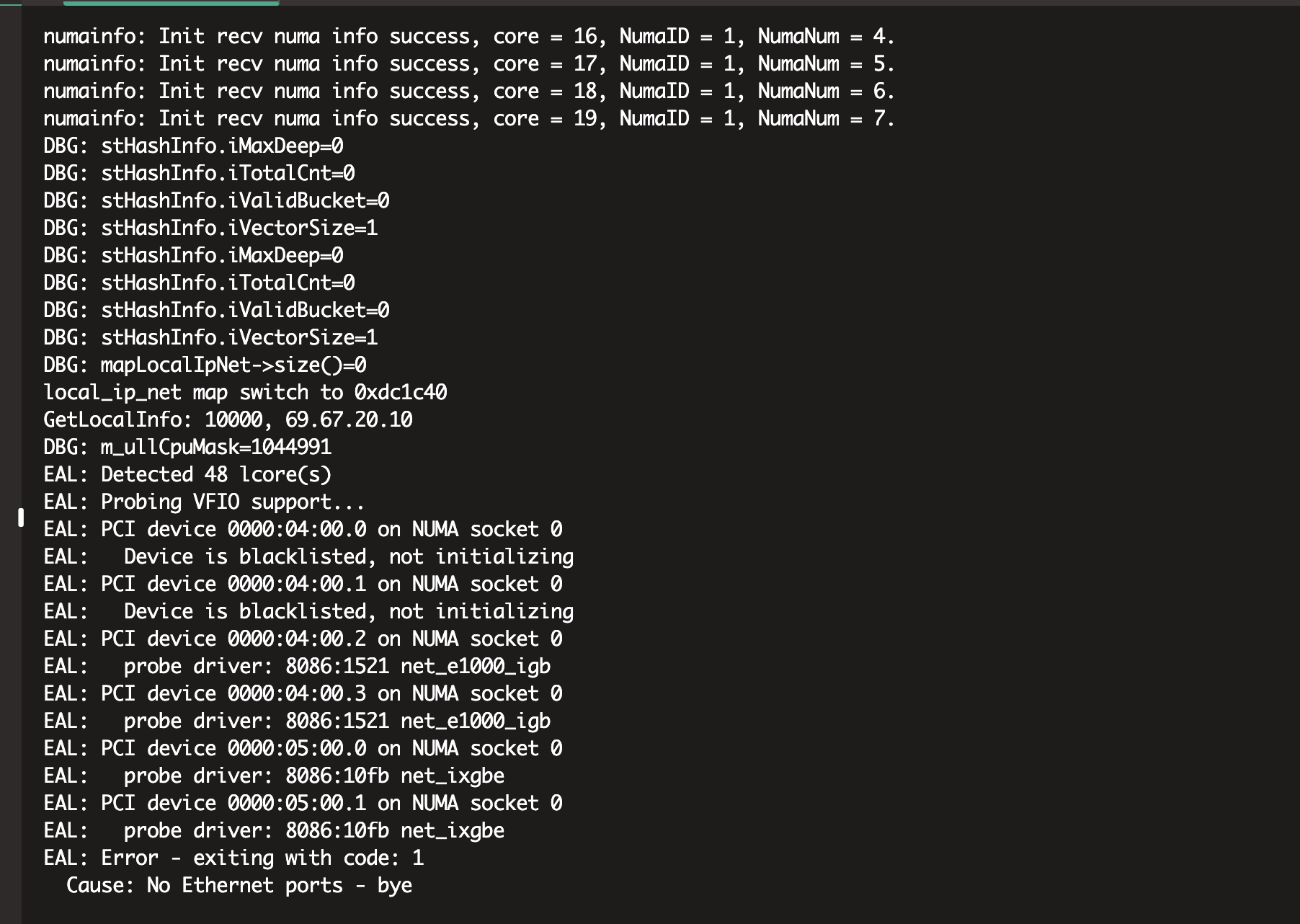
1. recvserver启动报错，no eth port

报错来源 8.6.1.1 3 recvserver服务状态，启动探针报错或日志包含此关键字

关键字 no eth port

No Ethernet ports





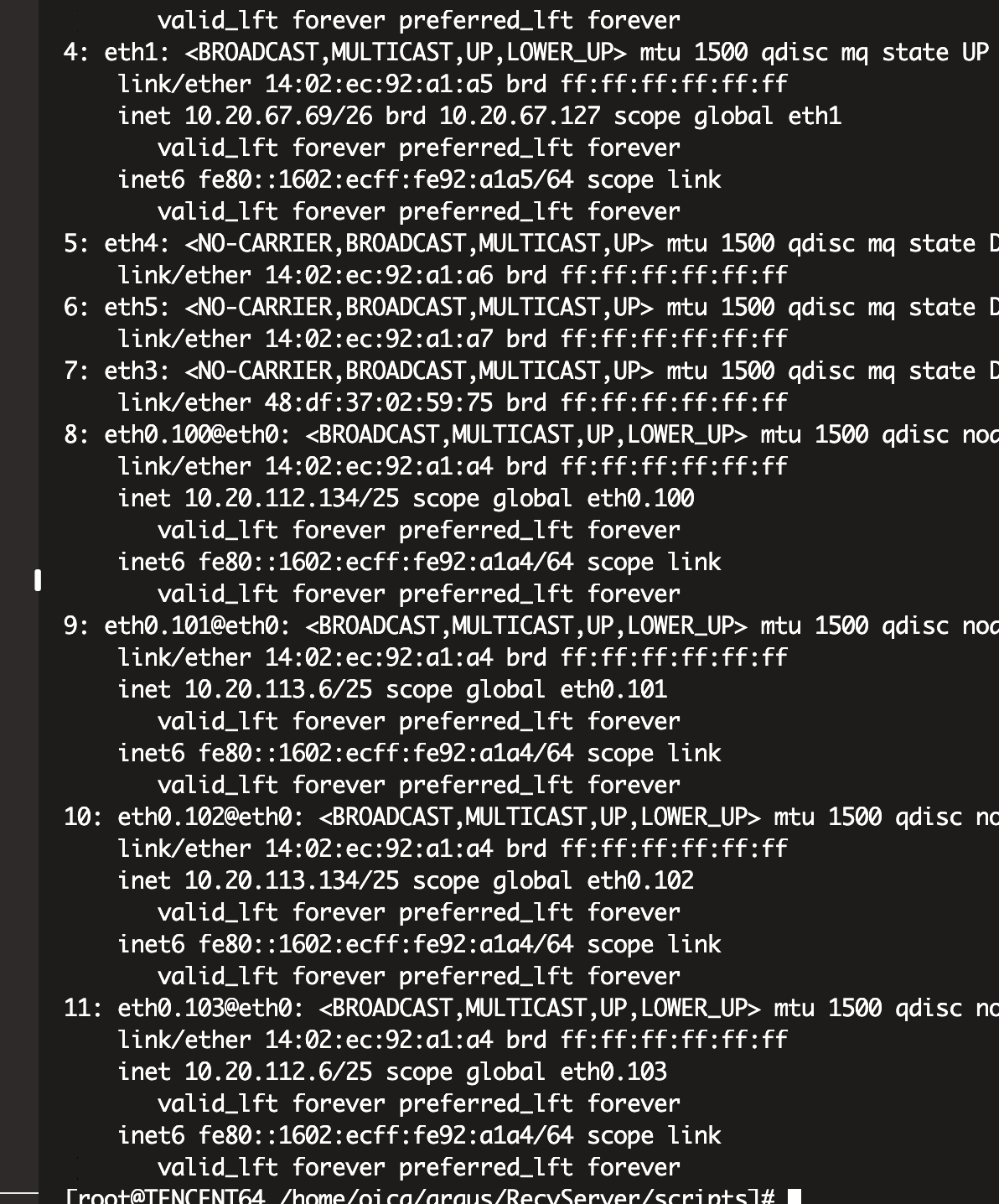
问题原因：

出现这个报错，一般是阻断网卡没有正常工作，网卡驱动没有加载成功

排查：

查看网卡配置的ip状态

ip a

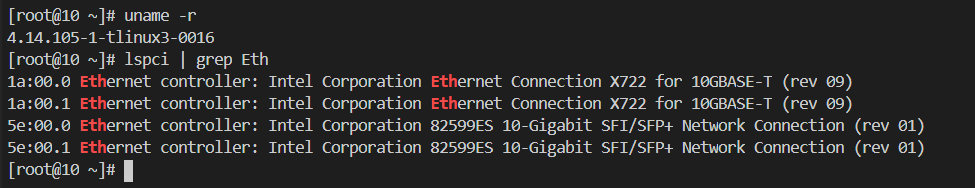


可以看到eth0阻断网卡的ip是正常的。

X86:

查看网卡型号：

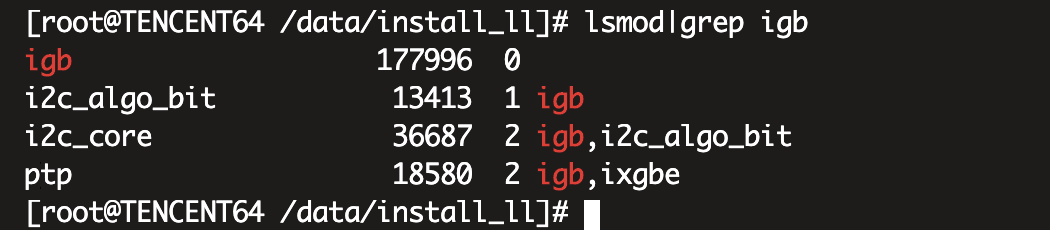
lspci |grep Eth



咨询产研是否支持过该网卡，这里的是支持的.

如果支持，查看驱动是否正常加载

lsmod |grep igb



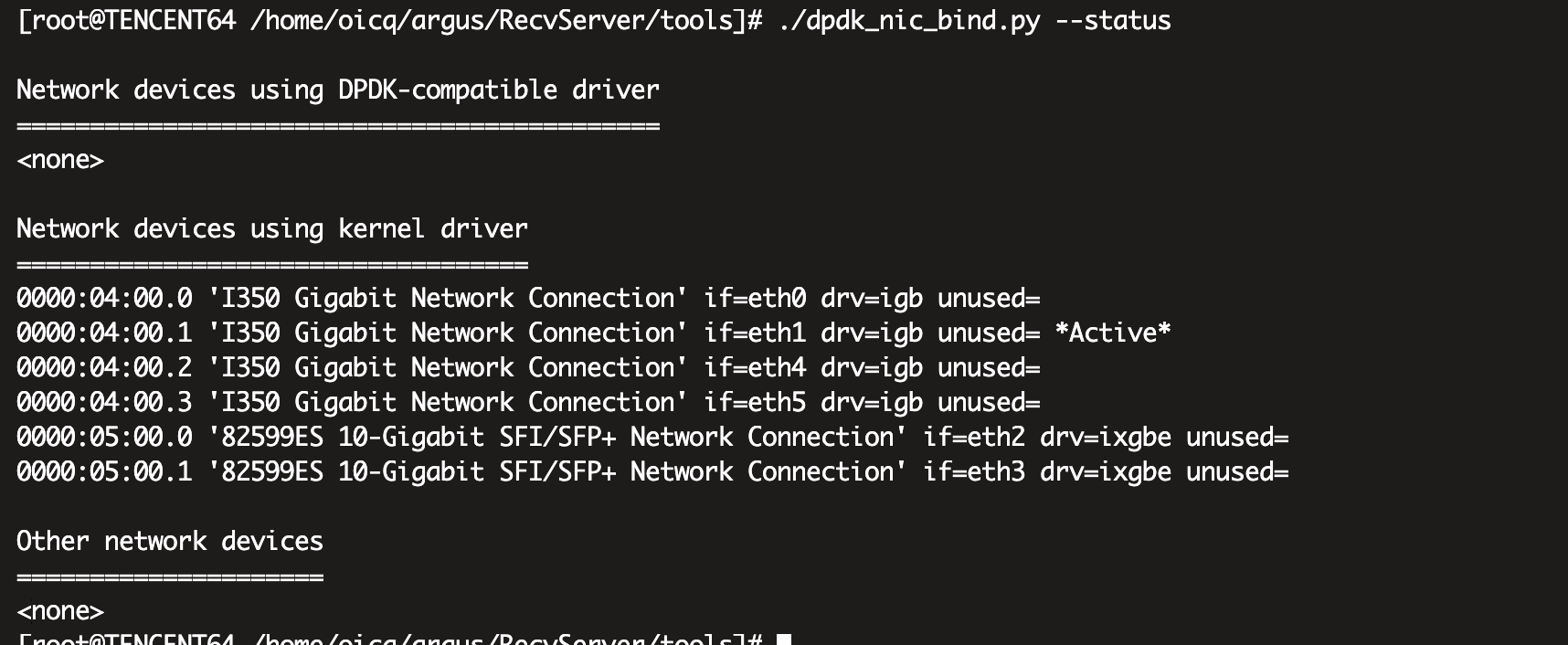
这里有正常的显示，是正常的，如果没显示的话，安装的驱动可能存在问题。

然后使用脚本查询网卡与驱动的绑定状态

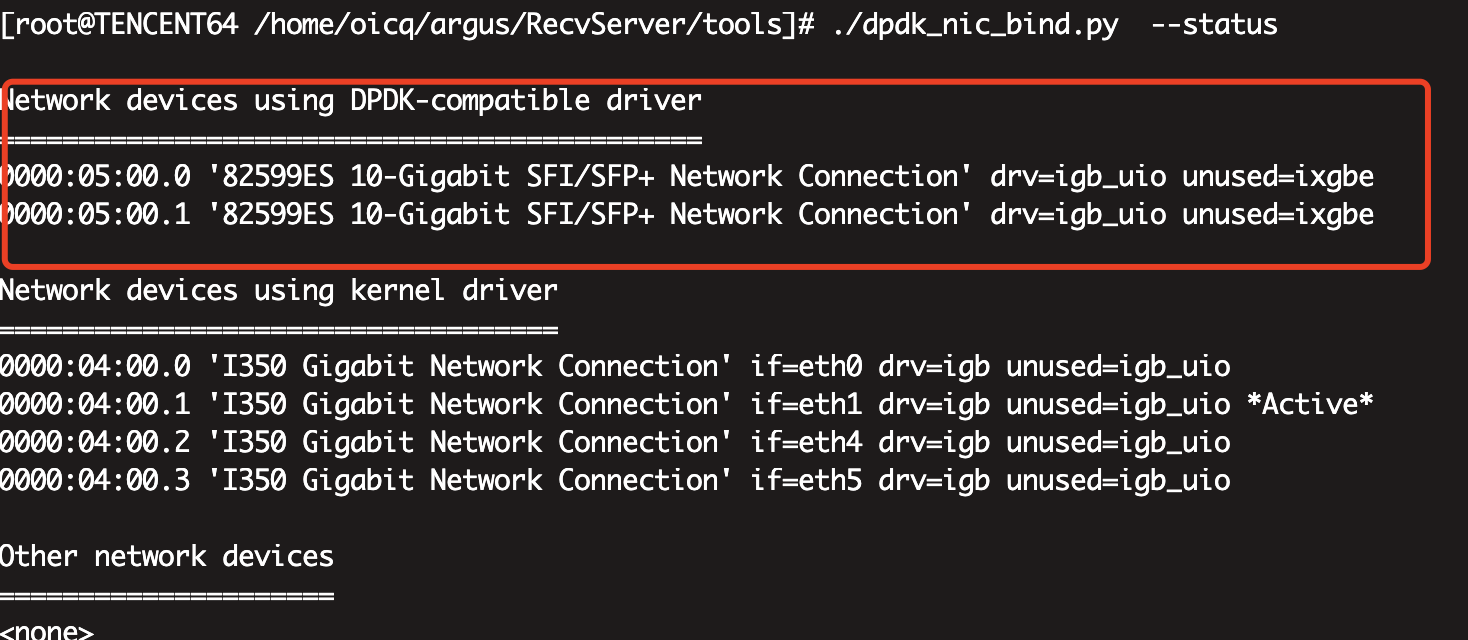
cd /home/oicq/argus/RecvServer/tools/

./dpdk\_nic\_bind.py --status

有可能不正常（intel网卡如下）：



正常：



如果不正常则代表驱动未与网卡绑定，执行命令尝试

cd /home/oicq/argus/RecvServer/tools

./dpdk\_nic\_bind.py --bind=igb\_uio eth0



出现此错误代表驱动无法绑定网卡

可能内核版本不匹配

uname -a

查询文档上方内核版本要求，并安装正确网卡，可以解决。