ADCampus方案中如何在EIA服务器抓包

ADCampus解决方案 李淑娟 2022-09-02 发表

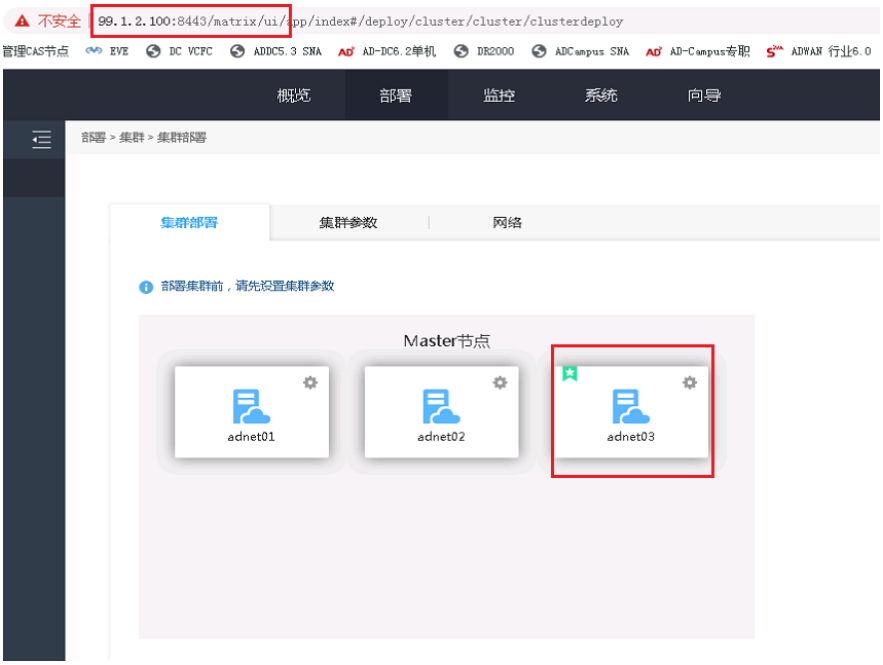
问题描述

ADCampus方案的组网中，使用部署在统一数字底盘上的EIA组件作为认证服务器进行认证，当出现认证问题时可能需要在EIA侧抓包，应当如何操作？

解决方法

1. 首先需要在统一数字底盘后台安装抓包工具，方法可参考：https://zhiliao.h3c.com/Theme/details/162948。

2. 由于EIA地址复用北向虚IP地址，该地址会落在集群的主Master节点上，因此**需要在集群的主Master服务器后台对物理网卡进行抓包。** 主Master节点可以在Matrix页面查看（https://x.x.x.x:8443/matrix/ui，其中x.x.x.x为北向虚IP），如下图adnet03节点为主Master节点，后台ip addr | grep x.x.x.x（北向虚IP地址）可看到北向虚IP落在该节点上。




```
[root@adnet03 ~]# ip addr | grep 99.1.2.100
    inet 99.1.2.100/32 scope global eth0
```

3. 通过ifconfig命令，查看该节点IP所在网卡名，如下图为eth0。

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 99.1.2.103  netmask 255.255.255.0  broadcast 99.1.2.255
      inet6 fe80::eda:41ff:fe1d:7437  prefixlen 64  scopeid 0x20<link>
      ether 0c:da:41:1d:74:37  txqueuelen 1000  (Ethernet)
      RX packets 315656267  bytes 388802758053 (362.1 GiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 329661172  bytes 357902418131 (333.3 GiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4. 使用tcpdump命令抓包：tcpdump –i eth0 *（以现场实际网卡名为准）* “port 1812 or 1813” *（仅抓取与认证相关端口的报文）* –w zhuabao.pcap

```
[root@adnet03 ~]# tcpdump -i eth0 "port 1812 or 1813" -w zhuabao.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4 packets captured
275 packets received by filter
179 packets dropped by kernel
```

5.确认抓包成功。

```
[root@adnet03 ~]# ll | grep zhuabao
-rw-r--r--. 1 tcpdump tcpdump 283570190 4月  21 14:37 zhuabaodhc33p.pcapng
-rw-r--r--. 1 tcpdump tcpdump    565011 4月  21 15:16 zhuabaodhcp22.pcapng
-rw-r--r--. 1 root    root         1454 9月   2 15:40 zhuabao.pcap
```

6.将抓包文件通过ftp等方式导出到本地即可查看。