VCFC控制器无法下发虚拟负载均衡问题

VCFC 郑启航 2021-03-03 发表

组网及说明

版本信息:

VCFC E2180P26

L5000C 8130P30

问题描述

现网环境下发VLB时控制器系统日志报错failed

过程分析

1、在控制器后台ping设备地址是否能通信；

2、查看 netconf诊断日志：

[2021-02-28 18:06:48.830] INFO http-nio-8443-exec-8 Time test : check context VLB_2240168060 .Thread:Thread[http-nio-8443-exec-8,5,main],time:0.

[2021-02-28 18:06:48.830] INFO http-nio-8443-exec-8 [NgfwmTemplateManager][getLeastCountDeviceResource]:Device LB500C max_number is null.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmKeystoreHelper][createPool]: Create resource pool in keystore.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [ngfwmBusHelper][sendCreatePool]: send MSG_NGFWM_RESOURCE_POOL_CREATE bus message.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [ngfwmBusHelper][sendBusMsg]: send bus message.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmPoolManager][updateContextCount]: Update context count successfully.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmContextManager][create]:Start to create context , increase context count 2.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmTemplateManager][allocIp]:start to alloc Ip from template LB5000.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmTemplateManager][allocIp]:The IpPool of template LB5000 and interface Route-Aggregation1 is null

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmTemplateManager][allocIp]:start to alloc Ip from template LB5000.

[2021-02-28 18:06:48.833] INFO http-nio-8443-exec-8 [NgfwmTemplateManager][allocIp]:The IpPool of template LB5000 and interface Route-Aggregation1 is null

提示端口信息为null

3、在L5K资源模板中查看不能识别到具体端口，查看设备上相关配置存在。

4、通过查看诊断日志原因在于netconf连接失败。

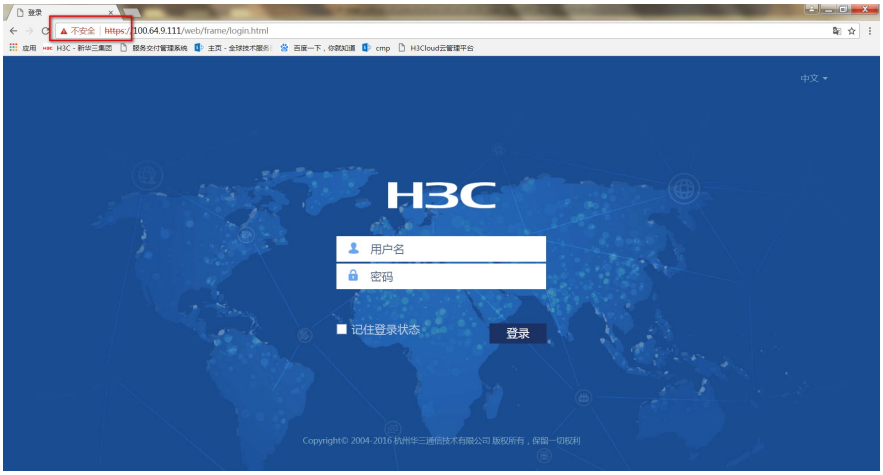
解决方法

1、在我司云网融合安全纳管解决方案中，大云平台需要调用VCFC进行纳管防火墙以及负载均衡设8110P08备的操作。VCFC产品从E0218P11版本开始支持使用iso镜像安装，其底层操作系统为CentOS7.3，VCFC基于该操作系统对如下不安全算法进行了禁用，其中包括MD5withRSA算法。

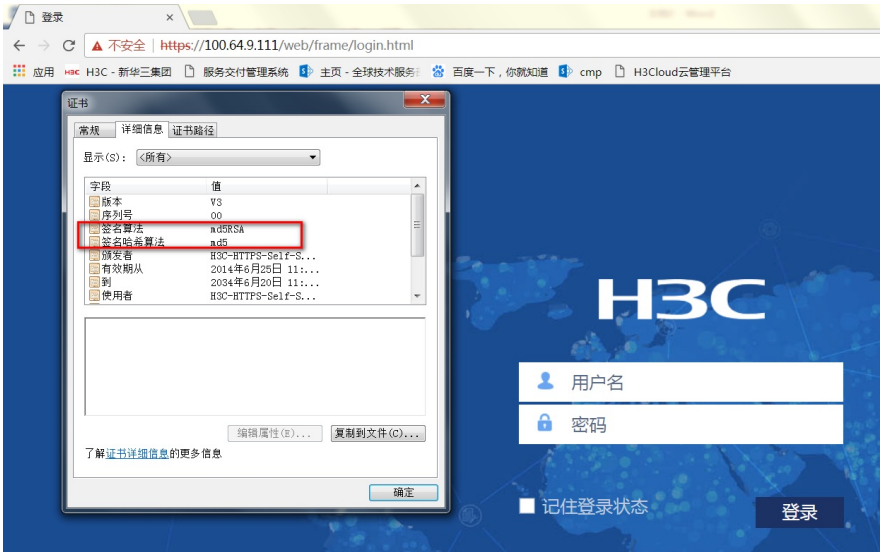
```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768, DHE
```

2、查看L5000-C的证书算法。

（1）通过https方式登录安全设备的web界面，点击“不安全”；



（2）点击“证书—详细信息”，如图所示，可看到该设备采用了md5RSA算法；



3、由于该设备是从较老的版本升级上来的，在升级过程中设备证书未更新，仍采用md5算法，因此不能被VCFC纳管。

1、Telnet登录L5000-C设备，使用dir命令查看设备文件，进入pki目录并删除该路径下的https-server.p12；


1 本地Shell
2 本地Shell
3 100.64.9.111:23
<L5000-C>dir