ADWAN网元无法注册上线问题的经验案例

ADWAN行业纵向网IP方案 陈楷铎 2018-06-30 发表

组网及说明

ADWAN网元无法注册上线问题排查

问题描述

ADWAN WEB界面上[规划部署/设备管理]中会显示网元节点状态。当节点状态为不可用时，表示网元未激活，此时将无法正常开展相关业务。

过程分析

网元状态为正常运行或者严重告警状态的要求是ADWAN服务器与网元之间的NETCONF和SNMP连接正常。网元未激活的问题定位故障排查思路如下：

步骤1：检查ADWAN服务器IP地址与网元的管理IP地址是否可达，若网络不可达，需排查网络问题。

步骤2：查看ADWAN上已导入的授权是否和网络场景对应，若授权和网络场景不对应需卸载已导入授权，导入对应网络场景的授权。

步骤3：通过自动发现设备添加设备时，如果为OpenFlow注册或者BGP-LS拓扑自动发现再添加设备，若加入设备列表中没有自动发现要添加的设备，则需检查ADWAN和网元上OpenFlow配置或BGP-LS配置。

步骤4：检查ADWAN与网元的NETCONF连接是否正常，查看网元设备与ADWAN之间通信的NETCONF端口号（默认TCP 830）是否放行。

步骤5：检查ADWAN与网元的SNMP连接是否正常，查看网元设备与ADWAN之间通信的SNMP端口号UDP_161和UDP_162是否放行。

步骤6：若还存在问题，请拨打400-810-0504寻求帮助。

解决方法

1、检查ADWAN服务器IP地址与网元的管理IP地址是否可达

ADWAN上网元状态正常的首要条件是网元的管理IP地址与ADWAN服务器IP地址路由可达，登录设备命令行或者ADWAN所在服务器操作系统命令行，执行ping操作来进行确认IP地址是否可达。

命令：*ping x.x.x.x*

例如：在ADWAN服务器操作系统命令行下执行ping操作，99.1.1.17为网元的地址，通过命令可查看到ADWAN服务器可以ping通网元。通过标红加粗部分字段可以看到，**0% packet loss**表示ADWAN服务器和网元管理IP地址可达。

```
[root@localhost ~]# ping 99.1.1.17
PING 99.1.1.17 (99.1.1.17) 56(84) bytes of data.
64 bytes from 99.1.1.17: icmp_seq=1 ttl=255 time=0.670 ms
64 bytes from 99.1.1.17: icmp_seq=2 ttl=255 time=0.615 ms
64 bytes from 99.1.1.17: icmp_seq=3 ttl=255 time=0.553 ms
64 bytes from 99.1.1.17: icmp_seq=4 ttl=255 time=0.599 ms
^C
--- 99.1.1.17 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.553/0.609/0.670/0.045 ms
```

2. 查看ADWAN上已导入的授权是否和网络场景对应

ADWAN支持以下两种License，其中试用版License仅做体验，所以不区分场景功能和节点数量License，默认包含了场景功能和节点数量；正式版License区分场景功能和节点数量，需要分开申请。同时ADWAN产品每种License对应一种网络场景，不能支持多网络场景的叠加。现有的网络场景有DCI场景、纵向网场景和企业分支场景。网络场景由安装的场景License自动配置，即如果安装的是纵向网的场景License，ADWAN软件就自动配置为纵向网场景。如下图所示：在ADWAN WEB页面上[系统管理/License管理/激活文件管理]查看已导入License，通过红框部分可见已导入DCI场景的临时License。

此时需要在ADWAN WEB页面上[规划部署/网络定义/基础网络管理]网络场景配置是否为DCI。如果不是现场要求网络场景的授权，则需要卸载已导入的授权重新导入正确的授权。如下图所示：通过红框部分可以网络场景配置为DCI场景。

3. 检查ADWAN和网元上OpenFlow配置或BGP-LS配置

通过自动发现设备功能添加设备时未自动发现需要添加的网元时，检查ADWAN和网元上OpenFlow配置或BGP-LS配置，如下图所示，在ADWAN WEB页面上[规划部署/设备管理]设备管理处点击自动发现设备按钮，如果发现如下图显示没有相应的记录，则需进行如下排查。

（1）排查是否通过OpenFlow注册来实现自动发现设备

在ADWAN WEB页面上[规划部署/设备管理/设备发现与认证]勾选OpenFlow注册来实现自动发现设备时，则需检查网元上的OpenFlow配置，如下图所示红框部分，已经勾选OpenFlow注册来实现自动发

现设备，此时需要检查网元上的OpenFlow配置是否进行如下配置。

```
设备OpenFlow基础配置：
openflow instance 1
 default table-miss permit    //配置Table Miss表项的缺省动作为允许

 classification port （vlan  XXX）    //配置OpenFlow实例对应的VLAN或者port生
效
 controller 1 address ip 99.1.1.220 （local address ip X.X.X.X）  （vrf XXX） //配置所连接的控制器i
p地址
 active instance //激活OpenFlow实例
#
MSR设备需按如下配置：
#
openflow instance 1
default table-miss permit      //配置Table Miss表项的缺省动作为允
许
 classification global        //配置OpenFlow实例类型为全局类型
 controller 1 address ip 99.1.1.220 （local address ip X.X.X.X）  （vrf XXX） //配置所连接的控制器i
p地址
 active instance     //激活OpenFlow实例
#
```

注：设备侧如果使用OpenFlow自动上报设备信息，设备上就需要配置OpenFlow实例，classfication port代表端口生效，对于CR16K设备要配置classfication vlan XXX，原因是CR16K配置了classfication port命令后，该设备会按照OpenFlow进行转发，不再使用路由转发；交换机设备需要配置classfication vlan XXX，且保证该vlan不是配置中涉及的vlan。_

MSR设备需配置default table-miss permit，表示若无匹配OpenFlow流表按照路由转发，原因是MSR设备只支持classification global，对全局生效，控制器不对设备下发流表，需设备按路由转发。Controller address ip配置的地址是控制器的ip地址，如果不配置 local address ip , OpenFlow会使用路由表中到控制器出接口地址来上报OpenFlow报文，如果配置了则使用配置的IP地址上报OpenFlow报文。如果管理地址所在端口有绑定VPN实例，则需要在配置中增加VRF参数配置。

（2）排查是否通过BGP-LS拓扑自动发现来实现自动发现设备

在ADWAN WEB上[规划部署/设备管理/设备发现与认证]中的设备发现，如下图所示红框部分，已经勾选BGP-LS拓扑自动发现来实现自动发现设备。

在ADWAN WEB上[规划部署/网络定义/基础配置]页面的BGP-LS配置,拓扑自动发现勾选BGP-LS拓扑自动发现，BGP-LS基础配置中AS ID配置BGP进程号，目前仅支持ADWAN与设备建立IBGP邻居，注意此处的AS的ID需要与BGP-LS设备上的AS号一致；BGP ID配置ADWAN的管理地址作为Router ID；BGP-LS 邻居配置：用来配置BGP-LS邻居的地址，也就是设备侧的地址，支持主备方式进行BGP-LS备份。如下图红框所示，拓扑自动发现勾选BGP-LS拓扑自动发现，BGP-LS基础配置配置AS ID为100，BGP ID配置为ADWAN的管理地址，在BGP-LS邻居配置设备侧的地址，可以配置主邻居HOST IP和备邻居HOST IP实现备份，如下图所示配置主邻居HOST IP为路由管理IP 99.1.1.161。

查看网元上的BGP-LS配置，如下所示：

```
#
ospf 1
 import-route direct
 distribute bgp-ls   // 配置允许设备将OSPF进程1的链路状态信息发布到BGP
 area 0.0.0.0
#
bgp 100
 peer 99.1.1.150 as-number 100  // 配置网元和ADWAN控制器建立IBGP邻居
 peer 99.1.1.150 connect-interface Loopback99
 #
 address-family link-state     //在链路状态地址族中使能邻居互连
  peer 99.1.1.150 enable
#
```

4. 检查网元和ADWAN上的NETCONF连接是否正常

（1）查看ADWAN上[规划部署/设备管理/设备发现与认证]中NETCONF方式管理配置

如下图红框所示：配置网元登陆用户名h3c，密码为h3c.com!，承载协议ssh，端口号为830。

查看网元设备上是否配置了相对应的正确的NETCONF配置，正确的配置请参考下面的配置片段。若配置不正确，请更正配置。查看到网元设备上已经配置了NETCONF的相关配置，如下图所示，网元设备需要进行如下配置。

```
 #
local-user h3c class manage
 password hash $h$6$/PxZzWgZUQG79nNi$Q9CcMYMd1Cag/bntBQ8mJfQEUuIt9TZjv4IP9
4tYSeEFEHJ1cqrZLYKKNOcHEGrhDNbLxq3ht0NL3E0XvUojyg==
 service-type ssh http https   //访问类型为ssh http https
 authorization-attribute user-role network-admin //用户权限为network-admin
 authorization-attribute user-role network-operator
#
 ssh server enable  //使能ssh server
netconf soap http enable      //使能NETCONF over http
 netconf soap https enable     //使能NETCONF over https
 netconf ssh server enable     //使能NETCONF over ssh
#
line vty 0 63
 authentication-mode scheme     //认证模式选择用户名和密码模式
 user-role network-admin        //用户权限为network-admin
#
```

（2）检查网元设备与ADWAN之间通信的NETCONF端口号是否放行

检查网元设备与ADWAN之间通信的NETCONF端口号是否放行，端口号可以在[规划部署/设备管理/设备发现与认证]中NETCONF方式管理配置里查看。

检查ADWAN服务器与网元之间是否开启防火墙，若未开启，可忽略本步骤。若开启，需要确保NETCONF所用的TCP端口为放行状态。首先确认是否开启防火墙，在操作系统输入systemctl status firewalld.service如下图红色加粗**active（running）**则表示已经开启防火墙。

```
[root@localhost ~]# systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
   Active: active (running) since Sun 2018-04-29 12:01:16 CST; 16min ago
 Main PID: 31269 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─31269 /usr/bin/python -Es /usr/sbin/firewalld --nofork –nopid
```

确认网元设备与ADWAN之间通信的NETCONF端口号是否已经防火墙放行，如果下图红色标粗显示为**yes**则已经放通，如果显示为**no**则还未放通。

```
[root@localhost ~]# firewall-cmd --query-port=830/tcp
yes
```

放通端口的配置方法如下：

```
在操作系统输入：firewall-cmd –-permanent --add-port=830/tcp 永久放行端口号使其操作系统重启也生效
[root@localhost ~]# firewall-cmd –-permanent --add-port=830/tcp
Success
再输入firewall-cmd --add-port=830/tcp 使放行端口号立即生效
[root@localhost ~]# firewall-cmd --add-port=830/tcp
Success
验证端口是否放行成功，显示yes表示放行成功：
[root@localhost ~]# firewall-cmd --query-port=830/tcp
yes
```

5. 检查网元和ADWAN上的SNMP连接是否正常

（1）检查ADWAN上[规划部署/设备管理]中[设备发现与认证]中SNMP方式管理配置

确认配置设备支持SNMP版本号和只读团体字和网元上配置的SNMP配置对应。如下图红框所示：勾选SNMP方式管理，设备支持的版本号为v2c，只读团体字为public。

在网元设备上查看是否配置了相对应的正确的SNMP配置，正确的配置请参考下面的配置片段。若配置不正确，请更正配置。如下所示：通过标红加粗部分字段可以看到，**read** 和**public**表示网元SNMP只读团体字为public，**v2c**表示网元配置SNMP版本为v2c。

```
#
snmp-agent
snmp-agent community write simple private
snmp-agent community read simple public
snmp-agent sys-info version v2c
#
备注：
1、ADWAN控制器支持SNMP v2c，v3三种协议，建议使用v2c。
```

（2）检查网元设备与ADWAN之间通信的SNMP端口号UDP161和UDP162是否放行

检查ADWAN服务器与网元之间是否开启防火墙，若未开启，可忽略本步骤。若开启，需要确保SNMP所用的UDP端口为放行状态。首先确认是否开启防火墙，在操作系统输入systemctl status firewalld.service如果下图所示红色加粗部分**active（running）**则已经开启防火墙。

```
[root@localhost ~]# systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
   Active: active (running) since Sun 2018-04-29 12:01:16 CST; 16min ago
 Main PID: 31269 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─31269 /usr/bin/python -Es /usr/sbin/firewalld --nofork –nopid
```

确认网元设备与ADWAN之间通信的SNMP端口号是否已经放行，如果显示为yes则已经放通，如果显示为no则还未放通，如下加红标粗**yes**表示检查UDP端口161和162已经放行。

```
[root@localhost ~]# firewall-cmd --query-port=161/udp
yes
[root@localhost ~]# firewall-cmd --query-port=162/udp
yes
```

如果显示为no，则需要放通端口，放通端口配置方法如下：

```
在操作系统输入：firewall-cmd —permanent --add-port=161/udp 永久放行端口号使其操作系统重启也生效
[root@localhost ~]# firewall-cmd —permanent --add-port=161/udp
Success
[root@localhost ~]# firewall-cmd —permanent --add-port=162/udp
Success
再输入firewall-cmd --add-port=161/udp 使放行端口号立即生效
[root@localhost ~]# firewall-cmd --add-port=161/udp
Success
[root@localhost ~]# firewall-cmd --add-port=162/udp
Success
验证端口是否放行成功，显示yes表示放行成功：
[root@localhost ~]# firewall-cmd --query-port=161/udp
   yes
[root@localhost ~]# firewall-cmd --query-port=161/udp
yes
```

6. 收集信息并拨打热线电话400-810-0504寻求帮助

如果以上问题都不存在，请收集网元设备上的配置，确认ADWAN网络场景以及已导入授权信息，然后拨打400-810-0504热线反馈测试结果寻求帮助。