UNIS ACG 系列应用控制网关

故障处理手册

目 录

1 部署方式故障处理

1.1 路由模式无法访问外网

1.1.1 故障描述

路由模式 ACG 部署在网络边界处，内网流量无法访问外网或无法使用某些服务等。

1.1.2 故障处理步骤

(1) 查看客户端 IP 等信息。保证用户 IP 地址正确。
(2) 检查接口地址是否正确，无法访问外网时内网间流量是否可以正常通信。
(3) 查看配置路由是否无误，网关地址、路由条目是否配置正确。
(4) 查看安全策略是否存在、匹配路由正确，默认策略是否放行。
(5) 查看 NAT 配置，保证 NAT 映射正确。

1.1.3 故障诊断命令

表1-1 故障诊断命令

命 令	说明
display interface	查看当前接口IP信息及接口状态
display ip route	查看路由表中路由条目及下一跳接口地址
display running-config policy	查看设备安全策略是否匹配及策略行为（permit/deny）
display ip nat source rule	查看设备NAT映射

1.2 透明模式无法访问外网

1.2.1 故障描述

使用透明模式 ACG 时，内网用户无法访问外部网络。

1.2.2 故障处理步骤

(1) 查看客户端 IP 等信息，测试内网连通性。
(2) 查看设备接口状态是否开启。
(3) 检测桥接口配置信息，确认要通信的网段都划入了桥接口下。
(4) 查看安全策略是否匹配（默认拒绝所有）。

1.2.3 故障诊断命令

表1-2 故障诊断命令

命 令	说明
display interface	查看当前接口IP信息及接口状态
display running-config interface	查看当前所有接口下的动作
display running-config policy	查看设备安全策略是否匹配及策略行为是否为放行（permit）

1.3 旁路模式无法对流量进行监听

1.3.1 故障描述

查看 ACG 监控日志无相应日志显示。

1.3.2 故障处理步骤

(1) 查看用户 IP 地址信息，无错误配置。

(2) 检查旁路模式接口启用情况。

(3) 查看用户地址对象匹配的网段是否正确。

(4) 检查安全策略是否被匹配。

1.3.3 故障诊断命令

表1-3 故障诊断命令

命 令	说明
display interface	查看当前接口IP信息及接口状态
display running-config interface	查看当前接口是否设置为旁路模式（deploy-mode listen enable）
display running-config policy	查看设备安全策略是否匹配及策略行为（permit/deny）
display address	查看IPV4地址对象网段是否正确匹配

2 升级异常维护指导

版本升级包括软件和特征库文件升级，升级的方式存在多种，在不同场景的实际应用中，可能会存在多种多样的问题，下面详细介绍一下系统升级管理员实际操作中的故障定位思路和方法。

2.1 主程序升级常见问题定位方法

进行主程序升级，常见问题包括：

- Web 界面下无法正常升级
- 命令行界面下无法正常升级
- Menuboot 下无法正常升级

下面将详细介绍各种常见问题的定位方法。

2.1.1 Web 界面下无法正常升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确保上传升级文件过程中网络正常，设备端需要提示上传成功。

(4) 升级文件上传成功后需要进行设备配置保存操作。

2.1.2 命令行界面下无法正常升级

(1) 首先检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 连接设备端口正确。

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定 TFTP 和 FTP 服务器正常，文件服务器路径设置正确。文件服务器登录名，密码与命令设置相同。

(4) 检查命令是否输入正确。

(5) 确保升级完成后 设备重启，用 **display version** 命令检查版本信息：

```
UNIS# display version
UNIS Uniware software,Version 1.10,Ess 6441, Build time is Apr 23 2018 09:47:39
System uptime: 0 days 0 hours 13 minutes
Firmware is UNISACG1000-IMW110-E6441.BIN

Application signature version: 20171208

Software S/N    : 18010070011804176511600l
Model           : ACG1000-G50
Platform        : PLATFORM_NC01

Basic Functionality                          : License valid
Application Audit and Control                : License valid
URL Category                                 : License valid
Malware URL Category                         : License valid
Virtual Private Network                      : License valid
```

2.1.3 Menuboot 下无法正常升级

(1) 首先检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 连接设备端口正确。

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 若设备无 CF 卡或 CF 卡中 menuboot 程序损坏，则需要在其他设备导入 menuboot 文件，例如，可以在连接设备的管理员 PC 上安装 3Cdemon 文件服务器，在 menuboot 中通过 **setenv** *serverip*，**setenv** *ipaddr*，**setenv loadfile** *menuboot.bin* 三个命令，分别设置文件服务器的 IP 地址，设备 IP 地址，与加载 menuboot 文件。

(4) 检查 menuboot 中各参数是否设置正确。

2.1.4 其他问题

其他问题如网线等物理层问题导致升级失败的请注意检查，如有其他问题请联系设备售后人员或咨询售后服务电话。

2.2 特征库升级常见问题定位方法

ACG 系统在线运行时需要周期性的更新特征库，才能更好进行应用识别控制和流量控制。在设备无法正常与互联网进行通信的情况下，可通过 WEB 页面进行特征库手动升级。若设备可正常与互联网进行通信，则可通过设置定期自动从服务器更新最新的特征库。

2.2.1 手动升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 检查升级文件是否正确，版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定在上传进度条完成后，WEB 界面提示上传成功，然后进行的下一步操作。

2.2.2 自动升级

(1) 自动升级需要设备接入互联网，检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）。

(2) 检查升级文件是否正确，版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 检查外网线路网络质量是否正常，检查设备 DNS 是否正确配置，若无配置，请将主备正确设置。

(4) 检查系统升级服务器，设定周期是否设置正常。

2.2.3 其他问题

特征库升级的前提是已经购买并导入授权升级许可，如未购买则无法进行升级，购买授权许可证可以联系厂商相关销售人员。

如有其他问题请联系咨询售后人员。

3 远程控制异常维护指导

不同场景的实际应用中，可能会存在多种多样的问题，下面详细介绍一下系统升级管理员实际操作中的故障定位思路和方法。

3.1 Web管理常见问题定位方法

(1) 检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 管理员 IP 与设备 IP 需要在同一网段下。

(3) 需要按照管理员需求，需改接口的访问权限，访问权限参考如下：

- https：允许 HTTPS 访问管理
- http：允许 HTTP 访问管理
- ssh：允许使用 SSH 方式管理
- telnet：允许使用 Telnet 设备管理地址访问管理
- ping：允许 Ping 此接口地址，如果不勾选，路由可达情况下 Ping 不通

(4) 检查浏览器是否正常。

3.2 命令行下管理常见问题定位方法

(1) 检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 检查 Console 线两端连接设备端口正确。

(2) 检查管理员 PC 的 COM 端口是否正常。

(3) 检查超级终端或 SecureCRT 配置正确，检查配置协议正确为“serial”，检查波特率配置正确为 9600。

(4) 连接建立后按回车打印显示信息。

3.3 其他问题

如有其他问题请联系设备售后人员或咨询售后服务电话。

3.4 常用调试命令

表3-1 常用调试命令

命令	使用说明
enable	进入特权模式
configure terminal	进入全局配置模式
display running-config	查看所有配置(空格键翻页)
save config	保存当前配置

命令	使用说明
erase startup-config	恢复出厂配置，需重启设备才能生效
reboot	重启系统，重启前会提示是否保存当前配置
display version	查看版本信息、系统运行时间、设备序列号/型号、功能授权状态等信息
display date	查看系统当前时间(local time)
display interface	查看接口相关信息，包括IP地址、链路状态、MAC地址和工作模式
display cpu usage	查看设备cpu使用率(当前值、1分钟/5分钟/15分钟平均值
display memory	查看设备内存使用率(控制面、数据面)

4 应用识别与审计故障处理

4.1 应用识别模式导致审计无法正确识别出应用特征

4.1.1 故障描述

查看应用识别或应用统计集，查看不到正确的应用

4.1.2 故障处理步骤

(1) 执行 **display app-ident mode** 查看是否模式为关闭

(2) 如果性能条件允许修改识别模式为 smart

4.2 网站日志无法记录

4.2.1 故障描述

访问网站，在 web 页面查看网站审计日志，未能查询到对应日志。

4.2.2 故障处理步骤

(1) 页面是否带有 content-type，类型是否为 text/html。

(2) HTTP 返回码是否为 200。

(3) 网页标题长度仅记录为 128 字符范围内（约为 40-60 个汉字）。

(4) URL 长度是否小于 512。

4.3 应用识别与审计不报日志

4.3.1 故障描述

配置应用审计策略，在 web 页面查看应用审计日志，未能查询到日志。

4.3.2 故障处理步骤

(1) 执行 **display running policy** 命令，检查应用审计策略是否正确。

(2) 执行 **display log config** 命令，查看应用审计日志是否记录。

(3) 执行 **debug app audit detail** 和 **debug application identify** 两个调试命令后，执行 **display log debug**+具体应用名称，如 **display log debug QQ**，查看应用审计与识别的细节信息，判断是否识别与审计成功。

(4) 通过查看首页应用流量排名统计来查看是否有误识别和漏识别情况。

(5) 执行 **display ip connection protocol** *protocol-name ip* **source** *source-addr* **dest** *dest-addr*，查看特定 IP 地址的会话的会话的 AppName 字段来确认是否为误识别。

4.4 远程syslog服务器收不到日志

4.4.1 故障描述

在本地可以查看到应用审计日志，配置日志服务器后，在 syslog 服务器端未能收到日志。

4.4.2 故障处理步骤

(1) 执行 **display log config** 命令，查看应用审计日志是否发送，日志服务器是否启用，服务器 IP 及端口是否正确。

(2) Syslog 服务器是否启动，端口是否与设备配置一致。

(3) 执行 **display ip route** 命令，查看路由是否正确，ping 服务器地址是否能 ping 通。

4.5 故障诊断命令

表4-1 故障诊断命令

命令	说明
display running policy	显示应用审计策略
display log config	显示日志配置情况
debug app audit detail	应用审计细节信息
debug application identify	应用识别细节信息
display log debug *app-name*	查看特定应用的debug信息
display ip connection protocol *protocol-name* **ip source** *source-addr* **dest** *dest-addr*	查看过滤特定地址的会话
display ip route	查看路由信息

5 QoS 故障处理

5.1 IPQoS带宽限制不生效问题

5.1.1 故障描述

配置了 IPQoS 带宽限制后发现远未达到所限带宽，流量就已不再增长。

5.1.2 故障处理步骤

检查接口配置的接口带宽与运营商提供的实际带宽是否一致，如：运营商提供 20M 带宽，但 QoS 的带宽显示为 50M，此时带宽已被运营商所提供带宽瓶颈所限制。

5.2 IPQoS最大带宽限速不生效

5.2.1 故障描述

配置了 IPQoS 最大带宽限制后发现未达到最大限速，或者超过了所配置限速值。

5.2.2 故障处理步骤

(1) 检查该 IP 是否超过限速的时间，如果只是一个瞬间的超速是正常的。
(2) 检查该 IP 是否在 QoS 白名单中。
(3) 执行 **display run qos-profile** 查看是否有该 IP 队列，正常情况下上下行都有 1 个队列。（或者 **display qos-profile statistics/display qos-profile**，查看数据包在该 QoS 的队列情况）。
(4) 检查设备是否有多个公网出口，而该 IP 只在某一个接口上做了限制。
(5) 若策略中限制的地址为 any，请改为具体 IP 地址。
(6) 每个策略中的地址薄条目数不超过 8 个。

5.3 应用QoS最大带宽限速不生效

5.3.1 故障描述

配置了应用 QoS 最大带宽限制后发现未达到最大限速，或者超过了所配置限速值。

5.3.2 故障处理步骤

(1) 检查是否开启了应用识别。
(2) 检查是否升级为最新应用特征库。
(3) 在统计集中查看该应用识别成何种应用，然后将该应用加入限制。
(4) 对于 FTP 等需要做 ALG 的环境，检查该应用的 ALG 是否做成功。

5.4 报文不受QoS限制

5.4.1 故障描述

报文未受 QoS 限制。

5.4.2 故障处理步骤

(1) 检查是否是本地报文。

(2) 检测报文是否为非 IPv4/IPv6 报文。

(3) 桥二层报文仅受物理接口的 QoS 限制，不受桥的 QoS 限制。

5.5 流量未匹配QoS策略

5.5.1 故障描述

流量未匹配所配置 QoS。

5.5.2 故障处理步骤

QoS 策略中当有多个对象限制时如：“Address”、“Service”、“APP”等时，为匹配所有对象时才可命中该 QoS 策略。

5.6 故障诊断命令

表5-1 故障诊断命令

命令	说明
clear qos-profile statistics	在定位前先删除已存在的数据包统计
display run qos-profile	显示qos的相关配置
display qos-profile	显示qos接口下的详细包数量
debug qos config	debug qos 相关配置
debug qos match	查看流量匹配qos队列
debug qos drop	所丢弃数据包由哪个qos队列丢弃

6 应用路由/ISP 路由

6.1 策略路由常见问题定位

6.1.1 配置了策略路由后，还是无法 Ping 通

- 原因可能是地址对象配置错误和下一跳配置错误。
- 解决方法：分清入口和报文源地址对象，并配置正确下一跳地址。

6.1.2 配置了策略路由后，直连接口无法通信

- 原因可能是错误配置了源接口、源地址、目的地址为 any 的策略路由导致。因为策略路由是优于所有其它路由的(包括直连路由)，错误的配置了这条策略路由后，会改变本地始发的数据包的出接口。
- 解决方法：分清入口和报文源地址对象，精确匹配策略路由引用的地址对象，尽量不要使用 any。

6.2 ISP路由无负载均衡

6.2.1 故障描述

当使用双 ISP 路由接入时，一段链路 down 掉，流量无法通过另一条链路访问外网。

6.2.2 故障处理步骤

(1) 查看 ISP 路由配置，保证 ISP 双运营商路由配置正确。

(2) 检查缺省路由配置，保证在路由表中拥有双 ISP 的缺省路由。

(3) 查看源 NAT 另一侧 ISP 路由出口填写正确。

6.3 故障诊断命令

表6-1 故障诊断命令

命 令	说明
display ip route	查看当前设备路由表
display ip nat source rule	查看当前设备NAT配置信息

6.4 ISP路由无法连接外网

6.4.1 故障描述

配置 ISP 路由后用户可以在内网互访，不能访问互联网。

6.4.2 故障处理步骤

(1) 检测 IPv4 地址对象所选网段是否配置正确。

(2) 查看路由表中是否存在双 ISP 的缺省路由。

(3) 查看源 NAT 地址对象是否配置正确。

(4) 查看安全策略是否放行匹配流量。

6.5 故障诊断命令

表6-2 故障诊断命令

命 令	说明
display address	查看IPV4地址对象所匹配的网段
display ip nat source rule	查看当前设备NAT配置信息
display ip route	查看当前设备路由表
display running-config policy	查看策略配置是否正确引入“IPv4地址对象”

7 IPsec VPN 维护指导

IPsec VPN 的主要问题定位手段是查看 IPsec 的配置、第一阶段 SA 的协商状态、第二阶段 SA 的协商状态、IPsec 协商的调试命令、检查路由、查看策略是否引用 IPsec、感兴趣流是否一致等等。下面详细介绍一下 IPsec VPN 在典型应用场景中的故障定位思路和方法。

7.1 IPsec VPN常见问题定位方法

IPsec VPN 在基于策略的使用时，常见问题包括：

- 第一阶段协商不成功；
- 第二阶段协商不成功；
- 保护子网不能通信；
- IPsec 协商起 100 条隧道，还有一部分没协商成功；
- 某些移动终端接入 VPN 不成功；
- NAT 环境下 IPsec 协商不成功；
- IPsec 建起连接后，一端断开后，IPsec 无法协商；
- 本端 SA 状态显示连接，流量无法转发；
- 当设备存在多出口时，其它参数正确，IPsec 协商失败；
- IPsec 使用国密证书协商不成功；
- 发起方保护子网范围比响应方子网范围大，二阶段无法协商成功；

下面将详细介绍各种常见问题的定位方法。

7.1.1 第一阶段协商不成功

第一阶段协商不成功，首先可以检查 IKE 的配置，查看两端的配置是否一致。其次检查路由，查看对端是否可达。如果一端配置对端网关配置的是动态，另一端配置静态对端网关，查看配置静态对端网关的一端，是否开启了自动连接，若未配置自动连接，流量需要从静态那一端发起，触发 IKE SA 的协商。

调试命令：**debug ipsec-VPN debug。**

7.1.2 第二阶段协商不成功

第二阶段协商不成功，首先可以检查 IPsec 的配置，查看两端的配置是否一致。检测感兴趣流，查看两端的感兴趣流是否一致。检测路由，查看对端是否可达。若是基于 tunnel 口，查看是否配置 tunnel 口的路由。

调试命令：**debug ipsec-VPN debug**。

7.1.3 保护子网不能通信

查看感兴趣流的方向性配置是否正确。隧道模式，查看是否配置策略。

若是感兴趣流的问题，可以通过以下命令查看：

- **display ike dump-tunn**，查看基于 tunnel 的 IPSec VPN 的 sp 状态是否建立成功。

7.1.4 IPsec 协商起 100 条隧道，还有一部分没协商成功

一条 IPsec VPN 隧道，配置多个网段的感兴趣流，最多支持 100 条，超过的不能协商成功。

7.1.5 某些移动终端接入 VPN 不成功

有些手机的 IKE 协商模式是野蛮模式，有些是主模式，所以一条 VPN 隧道不能保证所有的手机都能接入成功。同时手机发起的加密算法也各有不同，可以通过 **debug ipsec-vpn debug** 命令，查看协商不成功的原因，以及对端发来的加密算法是否与设置中的一致。

7.1.6 NAT 环境下 IPsec 协商不成功

搭建 IPsec 的环境中间有过 NAT 并且配置了 AH 认证导致 ipsec 无法协商成功，AH 封装的校验从 IP 头开始，如果 NAT 将 IP 的头部改动，AH 的校验就会失败，因此我们得出结论，AH 是无法与 NAT 共存的。此时去掉 AH 认证 IPsec 可以协商成功。

7.1.7 IPsec 建起连接后，一端断开后，IPsec 无法协商

IPsec 断开后对端设备并没有吧原先建立好的 SA 清除，就不再接受再次发起的协商请求，导致无法建立连接。解决方案：

(1) 在对端设备手动删除 SA。

(2) 双方启用 DPD 检测。

建议使用方案 2。

7.1.8 本端 SA 状态显示连接，流量无法转发

问题原因：

- 对端手动清除了 SA；
- 对端同时启用了按秒计时和按流量统计，本端只配置了按秒计时，如果流量过大，可能导致在按秒计时的生存周期内流量已经超出，导致对端 SA 端口连接。

排错：

- 双方把各自一阶段的 SA 生存期和二阶段 SA 生存周期改成一致；
- 一阶段启用 DPD 检测。

7.1.9 当设备存在多出口时，其它参数正确，IPsec 协商失败

当有多出口时，需要指定用于建立 IPsec 的本端 IP 地址。如果指定的是本地源接口，则使用该接口上的主 IP 作为本端 IP 地址。

7.1.10 IPsec 使用国密证书协商不成功

IPsec 认证方式选择国密认证后，需要填写本端证书、对端证书和 CA 证书。协商不成功需要检查本端证书与对端证书是否导入正确。

7.1.11 发起方保护子网范围比响应方子网范围大，二阶段无法协商成功

当 IPsec 发起方保护子网范围比响应方子网范围大，二阶段无法协商成功。此时需要修改 IPsec 保护子网范围一致。

8 IPsec 快速配置维护指导

IPsec 快速配置的主要问题定位手段是查看 IPsec 的配置、第一阶段 SA 的协商状态、第二阶段 SA 的协商状态、IPsec 协商的调试命令、检查路由等，由于 IPsec 配置被大大简化，一二阶段的配置均是自动生成，默认参数一致，且不支持修改。所以出现协商不起来的问题主要从配置检查和网络连通性方面着手。下面详细介绍一下 IPsec VPN 在典型应用场景中的故障定位思路和方法。

8.1 IPsec VPN常见问题定位方法

IPsec 快速配置在使用中，常见问题包括：

- 第一阶段协商不成功
- 保护子网不能通信
- IPsec 建起连接后，一端断开后，IPsec 无法协商
- 网段映射不生效
- 监控页面隧道名称为空

8.1.1 第一阶段协商不成功

第一阶段协商不成功，首先可以检查 IKE 的配置，查看两端的配置是否一致。其次检查路由，查看对端是否可达。

调试命令：**debug ipsec-VPN debug**

8.1.2 保护子网不能通信

1、保护子网之间不能通信，查看下两端是否配置了保护接口或保护子网，并查看下是否生成了保护子网的路由。2、检查两分支是否存在保护子网冲突，导致后接入的分支在中心端的路由覆盖了先接入的分支端设备的路由，解决分支网段冲突建议更改分支保护子网或者使用网段映射功能。

调试命令：**display ip route**

8.1.3 IPsec 建起连接后，一端断开后，IPsec 无法协商

IPsec 断开后对端设备并没有把原先建立好的 Sa 清除，就不再接受再次发起的协商请求，导致无法建立连接。解决方案：1、在对端设备手动删除 SA 2、双方启用 DPD 检测。建议使用方案 2。

调试命令：**debug ipsec-VPN debug**

8.1.4 监控页面隧道名称为空

分支端有选路策略，需要配置线路名称和对应的 IP，该线路名称会同步给中心端设备，显示为监控页面中的隧道名称，默认情况下不配置选路策略，就会出现隧道名称为空的情况，不影响功能，如果要显示名称，则在选路策略中定义线路即可。

调试命令：**debug ipsec-VPN debug**

9 组网特性故障处理

9.1 IPv6常见问题定位方法

9.1.1 IPv6 设备无法 Ping 通对端的地址

1. 故障现象

无法 Ping 通对端的 IPv6 地址。

2. 故障排除

(1) 在 enable 模式下，用 **display ipv6 interface** 命令检查接口配置的 IPv6 地址是否正确，接口状态是否为 up。

(2) 使用 **debug ipv6 packet** 命令打开 IPv6 报文调试开关，根据调试信息进行判断。**display log debug** 查看具体信息。

9.1.2 IPv6 发送前缀路由，对端 PC 无法接收，故障处理

1. 故障现象

发送前缀路由，对端 PC 无法接收到。

2. 故障排除

(1) 首先查看本地网卡是否已经接收到另一个前缀地址，并排查本地网络中是否有发送多个前缀的设备。

(2) 将网卡禁用再启用，再次获取查看。

9.1.3 IPv6 手动隧道无法通信，故障处理

1. 故障描述

手动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 手动隧道的源地址和目的地址都需要手动配置。

(2) 查看安全策略配置是否正确。

(3) 查看 IPv6 和 IPv4 路由是否正确。

9.1.4 IPv6 6to4 自动隧道无法通信，故障处理

1. 故障描述

6to4 自动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 首先分析设置的 6to4 隧道采用的地址是否正确，因为这个地址是一个特殊的地址，需要将 IPv4 公网通信接口的 IPv4 地址转化为 16 进制的 IPv6，o 为 2002:A.B.C.D::/64+EUI-64 格式，其中 2002 表示固定的 IPv6 地址前缀，A.B.C.D::/64 表示该 6to4 隧道对应的 32 位全球唯一的 IPv4 源地址，用 16 进制表示（如 1.1.1.1 可以表示为 0101:0101）。2002:A.B.C.D::/64 之后的部分唯一标识了一个主机在 6to4 网络内的位置。要算换一下此 IP 是否正确。

(2) 查看安全策略配置是否正确。

(3) 查看 IPv6 和 IPv4 路由是否正确。

9.1.5 IPv6 ISATAP 自动隧道故障处理

1. 故障描述

IPv6 ISATAP 自动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 首先要检查 ISATAP 隧道地址是否添写正确，这里的 ISATAP 隧道地址是经过换算得来的，使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。ISATAP 地址格式为：Prefix(64bit):0:5EFE:ip-address。其中，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀，ip-address 为 32 位 IPv4 源地址，换算成 16 进制后添在 IPv6 的后 32 位中。

(2) 路由前缀是否通信成功，在本地网卡上查看，可在 PC 端使用 wireshak 抓包。

(3) 查看安全策略配置是否正确。

(4) 查看 IPv6 和 IPv4 路由是否正确。

9.2 VRF故障处理

1. 故障描述

VRF 配置后无法通信。

2. 故障处理步骤

按照标准配置手册文档多次检查配置是否正确，例如排查路由、安全策略是否正确。若配置没有问题，错误依然存在，将配置导出并发给技术支援处理。

9.3 动态路由故障处理

9.3.1 OSPFv2 无法建立邻居定位方法

1. 故障描述

OSPF 邻居关系无法正常建立。

2. 故障处理步骤

如果物理连接和下层协议正常，则检查接口上配置的 OSPF 参数，必须保证与相邻路由器的参数一致，区域号相同，网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。

(1) 使用 **display ip ospf neighbor** 命令查看 OSPF 邻居状态。

(2) 使用 **display ip ospf interface** 命令查看 OSPF 接口的信息。

(3) 检查物理连接及下层协议是否正常运行，可通过 ping 命令测试。若从本地设备 Ping 对端设备不通，则表明物理连接和下层协议有问题。

(4) 检查 OSPF 定时器，在同一接口上邻居失效时间应至少为 Hello 报文发送时间间隔的 4 倍。

(5) 如果是 NBMA 网络，则应该使用 **peer** *ip-address* 命令手工指定邻居。

(6) 如果网络类型为广播网或 NBMA，则至少有一个接口的路由器优先级大于零。

9.3.2 OSPFv2 路由信息不正确

1. 故障描述

OSPF 不能发现其他区域的路由。

2. 故障处理步骤

应保证骨干区域与所有的区域相连接。若一台设备配置了两个以上的区域，则至少有一个区域应与骨干区域相连。骨干区域不能配置成 Stub 区域。

在 Stub 区域内的设备不能接收外部 AS 的路由。如果一个区域配置成 Stub 区域，则与这个区域相连的所有设备都应将此区域配置成 Stub 区域。

(1) 使用 **display ip ospf neighbor** 命令查看 OSPF 邻居状态。

(2) 使用 **display ip ospf interface** 命令查看 OSPF 接口的信息。

(3) 使用 **display ip ospf database** 查看数据库的信息是否完整。

(4) 使用 **display running-config ospf** 命令查看区域是否配置正确。若配置了两个以上的区域，则至少有一个区域与骨干区域相连。

(5) 如果某区域是 Stub 区域，则该区域中的所有设备都要配置 stub 命令；如果某区域是 NSSA 区域，则该区域中的所有设备都要配置 nssa 命令。

(6) 如果配置了虚连接，使用 **display ospf vlink** 命令查看 OSPF 虚连接是否正常。

9.3.3 OSPFv2 路由传递问题

1. 故障描述

查看 OSPFv2 邻居关系显示邻居关系已经 full 状态。但无法学习由 OSPF 邻居传递的路由。

2. 故障处理步骤

(1) 查看 OSPF 接口网络类型，保证建立邻居的接口在相同的网络类型内。

(2) 查看 OSPF 进程是否配置了 distribute 路由过滤。

(3) 查看 OSPF 进程是否设置了域间路由汇总 not-advertise 不通过路由。

(4) 查看 OSPF 进程是否设置了重分布路由不通告。

9.3.4 OSPFv3 无法建立邻居定位

1. 故障描述

查看 OSPFv3 邻居关系时无任何显示，无法与相邻设备建立 OSPFv3 邻居关系。

2. 故障处理步骤

(1) 查看双方直连接口 IPV6 地址，确定直连 IPV6 地址在相同网段内。

(2) 查看 OSPFv3 接口，保证建邻接口在相同 area 内。

(3) 检查建邻设备 router-id 是否冲突。

(4) 查看建邻接口 OSPF hello time 和 dead time 相同。

(5) 查看建邻接口 MTU 是否一致，MTU 一致后邻居关系才可到达 full 状态。

9.3.5 OSPFv3 学习路由条目故障处理

1. 故障描述

OSPFv3 邻居关系正常达到 full 状态，但是无法从 OSPFv3 邻居学习其他路由条目。

2. 故障处理步骤

(1) 查看 OSPFv3 口网络类型，保证建立邻居的接口在相同的网络类型内。

(2) 查看 OSPFv3 进程是否设置了域间路由汇总 not-advertise 不通过路由。

(3) 查看 OSPFv3 进程是否设置了重分布路由不通告。

9.4 HA常见问题定位方法

HA 在主备场景下使用时，常见问题包括：

- HA 无法协商

- HA 主备无法切换
- HA 无法同步

下面将详细介绍各种常见问题的定位方法。

9.4.1 HA 无法协商

要求作为 HA 的两台设备为同一个硬件型号、同一软件版本，选择同样的接口作为 HA 接口配置了抢占模式必须在主设备和备设备上分别配置，一台设备配置为抢占主，一台配置为抢占备。否则 HA 无法协商

9.4.2 HA 主备无法切换

- 备设备有接口处于 down 状态。
- 配置了抢占模式的 HA 设备无法手动切换 HA 状态。

9.4.3 HA 无法同步

- 两台设备型号或版本不同，不同型号的设备接口数目可能不一样，这样配置永远不相同。
- 某个需要 License 的模块主设备有而备份设备没有 License 或已过期，这可能导致配置不同。
- 未开启自动同步功能，导致主备配置不同。
- 在 HA 主设备上重启对端的备设备。HA 备设备可能出现配置和主设备冲突，无法同步的情况。这时可以重启备设备，使备设备抛弃错误配置，使用同步过去的最新配置。

9.4.4 HA 常用调试命令

表9-1 HA 常用调试命令

命令	说明
debug ha error	查看HA错误信息
debug ha event	查看HA事件信息
debug ha filesync	查看HA队列信息
debug ha recv	查看HA发包信息
debug ha send	查看HA收包信息
debug ha session	查看HA会话信息
debug ha sync	查看HA同步状态信息
debug ha recv	查看HA发包信息

9.5 HA联动故障处理

9.5.1 故障描述

ACG 配置 HA 并且关联 track，主备频繁切换。

9.5.2 故障处理步骤

(1) ACG 上查看 track 状态主要看超时时间和间隔设备

(2) ACG 上 HA 是否配置了自动抢占

(3) Track 超时时间建议配置默认值 10*4

(4) 关闭 HA 抢占

9.6 HA联动无法切换

9.6.1 故障描述

ACG 配置 HA 并且在主备墙都关联 track，导致主备无法切换。

9.6.2 故障处理步骤

(1) ACG 备墙上查看 HA 配置

(2) ACG 备墙上查看 HA 所关联 track 状态是否为 Failed

(3) ACG 备墙查看引用的 track 对象的探测目标是从哪个接口出去的

(4) ACG 备墙在探测目标的接口下配置管理 ip 地址

9.6.3 故障诊断命令

表9-2 故障诊断命令

命 令	说明
display running-config ha	查看HA配置
display track *name*	查看track详细信息

9.7 Bypass故障处理

9.7.1 故障描述

系统异常时、掉电时接口没有切换到 Bypass 状态。

9.7.2 故障处理步骤

正常情况下 Bypass 模块的触发机制分为硬件触发与软件触发，例如当设备没有通电的情况下，Bypass 功能会调整为开启，如果设备一旦通电后，系统启动成功时，Bypass 立即调整为关闭状态。当系统启动成功后，由于系统故障异常会导致重启时，Bypass 功能会调整为开启状态。当系统运行正常，突发掉电情况下，Bypass 软件会调整为开启状态。

(1) 当发现 Bypass 异常，首先需要判断接口是否属于同一 Bypass 接口。例如 UNIS ACG1000 PLATFORM_MC5200 平台默认是 GE6、GE7 属于 Bypass 接口对，当网线插入 GE5、GE6 时，系统掉电后无法正常通信，因为不是属于同一个接口对。

(2) 当判断网线插口属于正确的 Bypass 接口对时，查看当前配置是否为桥模式，因为 Bypass 仅对二层转发生效，不对三层模式生效。

(3) 由于 Bypass 属于芯片集成功能，由于硬件芯片所属环境如潮湿，干燥，静电也会导致芯片异常功能失效。

9.8 链路负载均衡

9.8.1 链路负载均衡不生效

1. 故障描述

出口设备使用带宽比的链路负载均衡不生效。

2. 故障处理步骤

(1) 查看负载均衡是否开启

(2) 检查属于负载均衡组下的接口状态是否 UP

(3) 检查负载均衡组下路由状态是否生效

(4) 检查路由的多下一跳出口是否分属不同的负载均衡组，对于这种存在冲突的情况，按照之前的路由选路方式进行，不再进行负载均衡

9.8.2 带宽比的负载方式不准确

1. 故障描述

带宽比的负载方式，负载不准确。

9.8.3 故障诊断命令

表9-3 故障诊断命令

命 令	说明
display mllb-group *NAME*	查看负载均衡组配置
display running-config mllb-group	查看负载均衡组配置
display interface	查看设备安全策略是否匹配及策略行为是否为放行（permit）
display ip route	查看路由状态

10 增强功能

10.1 配置会话限制后没有限制效果

10.1.1 故障描述

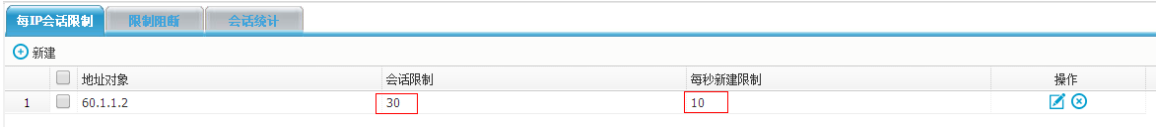
配置了会话限制，但是并没有对配置的地址对象下的会话进行限制。

10.1.2 故障处理步骤

由于配置的地址对象的对应的会话已经建立的数量大于配置的限制的会话数，导致并不能看到会话限制的效果。

比如配置会话限制数为 30，每秒新建限制为 10。

图10-1 会话限制配置



查看限制阻断，没有记录（此时 60.1.1.2 地址对象所对应的流量保持的会话数为 50）。

图10-2 会话限制阻断

查看当前会话统计，60.1.1.2 会话数大于 30。

图10-3 会话统计

如果该地址对象的会话一直有流量的话，会话不会老化，可以在命令下清除当前的会话，即可进行正常的会话限制。如果该地址对象的会话没有流量，可以等候会话老化，之后便能看到会话限制的效果。

```
UNIS# clear ip connection all
```

再查看阻断记录，能够正常阻断。

图10-4 清除会话后的阻断记录

10.1.3 故障诊断命令

表10-1 故障诊断命令

命令	说明
clear ip connection all	清除当前已经建立起来的会话

10.2 DNS代理对客户端请求没有进行处理

10.2.1 故障描述

- 设备开启了 DNS 代理功能，并且配置了 DNS 服务器。
- 客户端配置设备为 DNS 服务器，但是在发出 DNS 请求后收不到响应。

10.2.2 故障处理步骤

查看 CPU 是否过高，DNS 代理的过程通过 CPU0 来处理，CPU0 用作 CP，当 CPU0 偏高时，会产生丢包，执行 **display cpu usage** 命令查看 CPU 占用情况。

图10-5 查看 CPU 占用情况

```
host# display cpu usage
----------------------------------------------------------------
Name          Current       1Min          5Min          15Min
----------------------------------------------------------------
Average       0             0             0             0
CPU0          8             7             7             7
CPU1          0             0             0             0
CPU2          0             0             0             0
CPU3          0             0             0             0
CPU4          0             0             0             0
CPU5          0             0             0             0
CPU6          0             0             0             0
CPU7          0             0             0             0
CPU8          0             0             0             0
CPU9          0             0             0             0
CPU10         0             0             0             0
CPU11         0             0             0             0
CPU12         0             0             0             0
CPU13         0             0             0             0
CPU14         0             0             0             0
CPU15         0             0             0             0
```

查看是否是内存不足导致丢包，设备分配了一定的内存来作为 DNS 请求和转发的缓冲，大小约为 400K，客户端产生大量 DNS 请求时，将导致用于缓冲的内存部分用尽，产生丢包；命令为 **debug dp drop**，**display log debug**。

图10-6 查看是否是内存不足导致丢包

```
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
```

查看是否是 FPA 泄露，FPA 主要负责分配收发报文过程中的 packet work entry 以及 packet 的 data buffer，ACG1000 设备上的 FPA 存在于 FPA0-FPA3 上，数值会有上下浮动但不会持续下降，当 FPA 泄露完之后导致设备不会转发报文，命令 **display statistics fpa**。

图10-7 查看是否是 FPA 泄露

```
host#disp statistics fpa
FPA 0
    Pool Available      :       65411
    Pool Page Index     :       2041
FPA 1
    Pool Available      :       65475
    Pool Page Index     :       2043
FPA 2
    Pool Available      :       972
    Pool Page Index     :       27
FPA 3
    Pool Available      :       32
    Pool Page Index     :       0
```

10.2.3 故障诊断命令

表10-2 故障诊断命令

命令	说明
debug dp drop	查看转发过程中的丢包情况
display cpu usage	查看CPU 使用情况
display log debug	查看debug产生的日志
display statistics fpa	查看fpa状态

10.3 无法拦截DoS攻击

10.3.1 故障描述

配置了 DoS 攻击防护后发现无法拦截 DoS 攻击流量。

10.3.2 故障处理步骤

分析问题出现的原因。按正确的逻辑顺序，列出问题解决步骤。对于简单的解决方法，采用正文直接描述即可。

(1) 执行 **display running-config defend** 检查设置的 DoS 攻击防护是目的 IP 防御还是接口防御，其中目的 IP 防御是全局生效的，而接口防御仅对被设置的接口生效。

(2) 如果设置的是目的 IP 防御，检查该 IP 是否在设置的保护主机范围内。

(3) 如果设置的是接口防御，该接口是否是 DoS 攻击的入接口。

10.3.3 故障诊断命令

表10-3 故障诊断命令

命令	说明
display statistics interface	查看所有端口的统计信息
display running-config defend	查看安全防护配置信息
debug ip defend attack	debug安全防护丢包信息
debug ip packet receive	debug收到的数据包
debug ip packet send	debug转发的数据包
debug dp filter	设置debug过滤器

10.4 恶意URL白名单故障处理

10.4.1 故障描述

安全策略开启 URL 过滤后，某些网站无法访问，查看恶意 URL 日志，发现网页被阻断。配置了恶意 URL 白名单后重新访问网站还是不能访问。

10.4.2 故障处理步骤

(1) 查看访问的网站 URL 是否填写正确。

(2) 查看恶意 URL 日志，访问的网站是否有记录。

(3) 查看配置的恶意 URL 白名单是否正确，恶意 URL 白名单为精确匹配

(4) 修改恶意 URL 白名单后，重新访问网站

10.4.3 故障诊断命令

命 令	说明
display malware_whitelist	查看恶意URL白名单配置
malware-url *url*	添加恶意URL白名单

10.5 管理员无法登录Web页面

10.5.1 故障描述

无法使用新建的管理员账户登录设备。

10.5.2 故障处理步骤

(1) 查看新建管理员用户名、密码配置（可以使用默认的 admin 账户登录）。

(2) 查看新建管理员是否配置管理 IP 地址。

(3) RADIUS、LDAP 服务器是否正常。

10.5.3 故障诊断命令

表10-4 故障诊断命令

命 令	说明
display amdin-user（管理员名称）	查看ACG中该管理员是否存在及用户类型、用户状态、管理地址、管理员权限

10.6 断点续传故障处理

10.6.1 断点续传描述

属于断点续传的有服务器不可达/服务器 down/vtysh 超时退出（这种情况下，属于断点下载范围。当设备版本下载过程中断掉后，再次开始后从上一次的进度处开始下载）

10.6.2 故障描述

- 使用 FTP 方式下载版本文件，版本下载失败
- 使用 HTTP 方式下载版本文件，版本下载失败

10.6.3 故障处理步骤

(1) FTP 服务器是否开启，PC 端需要关闭防火墙。

(2) 查看版本文件是否放在 FTP 服务器正确的目录下。

(3) 查看 FTP 服务器是否设置了登录口令。

(4) 设备端下载版本文件名是否正确。

(5) 下载过程中，用户主动断掉（ctrl+c，这种情况不属于断点下载，需要重头开始下载）。

(6) HTTP 服务器是否开启，PC 端需要关闭防火墙。

(7) 查看版本文件是否放在了 HTTP 服务端的目录下。

(8) 设备端下载版本文件名是否正确。

(9) 下载过程中，用户主动断掉（ctrl+c，这种情况不属于断点下载， 需要重头开始下载）。

10.7 第三方用户存储认证故障处理

10.7.1 故障描述

ACG 配置 RADIUS/LDAP 第三方认证后访问外网无法重定向到认证页面。

10.7.2 故障处理步骤

(1) ACG 上 IPv4 策略是否将流量拒绝。

(2) 查看 ACG 上的用户策略是否正确。

(3) 查看 ACG 上的路由配置是否正确。

10.7.3 故障诊断命令

表10-5 故障诊断命令

命 令	说明
display running-config policy	查看ACG中IPv4策略
display user-policy	查看ACG中用户策略
display ip route	查看ACG中路由配置相关信息

10.8 第三方用户存储无法认证成功

10.8.1 故障描述

ACG 配置 RADIUS/LDAP 第三方认证后，在重定向页面内输入正确的用户名、密码，点击登录，页面提示“用户名或密码错误”。

10.8.2 故障处理步骤

(1) 在命令行 **debug aaa events**，根据相应的 debug 信息查看认证失败的原因，包括服务器没有回应、服务器密码错误、用户名或密码错误。根据这些相应的原因查看是否拓扑或路由错误导致服务器没有回应；RADIUS 服务器密码是否错误；输入的用户名及密码是否正确，此用户在 RADIUS/LDAP 服务器上是否存在。

(2) 查看相应的系统日志，查找故障原因。

10.8.3 故障诊断命令

表10-6 故障诊断命令

命 令	说明
debug aaa events **display log debug**	查看认证失败的相应debug信息
display log event all	查看ACG关于认证失败的日志信息

10.9 基于用户MAC的转发策略故障处理

10.9.1 故障描述

在 ACG 上配置有用户认证策略，并新建用户将 PC 的 MAC 地址绑定， PC 仍无法上网并重定向到认证页面。

10.9.2 故障处理步骤

PC 能够重定向到认证页面，说明设备的路由及 IPv4 策略是没有问题的。

(1) 首先查看绑定的 MAC 地址是否与 PC 的 MAC 地址一致；

(2) 再查看下组网方式，若是 ACG 通过三层交换机与内网 PC 相连，目前 ACG 没有跨三层 MAC 地址学习功能，则无法直接获取到内网 PC 的 MAC 地址，这样即使绑定了 MAC 地址，任然需要通过认证才能上网。

10.9.3 故障诊断命令

表10-7 故障诊断命令

命 令	说明
display user	查看ACG中绑定MAC的用户

10.10 三权分立

10.10.1 管理员无法登录 WEB 界面问题定位

(1) 检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 管理员 IP 与设备 IP 需要在同一网段下。

(3) 需要按照管理员需求，需改接口的访问权限，访问权限参考如下：

- https：允许 HTTPS 访问管理
- http：允许 HTTP 访问管理
- ssh：允许使用 SSH 方式管理
- telnet：允许使用 Telnet 设备管理地址访问管理
- ping：允许 Ping 此接口地址，如果不勾选，路由可达情况下 Ping 不通

(4) 检查浏览器是否正常。

10.10.2 系统管理员 Web 登录后看不到任何模块

1. 故障描述

在 Web 登录系统管理员账号后，看不到任何模块。

2. 故障处理步骤

(1) 登录权限管理员账号，查看是否给该系统管理员分配相应模块的权限。

(2) 如果权限管理员只给该系统管理员分配了 CLI 权限，那么登录系统管理员账号也不会显示该模块。

(3) 如果权限管理员只给该系统管理员分配了应用审计日志、网站访问日志模块，当设备没有硬盘时，那么登录系统管理员账号也不会显示该模块。

10.11 服务质量管理故障处理

10.11.1 服务质量探测结果一直为 0

10.11.2 故障描述

网络连通的情况下，服务质量条目探测结果一直为 0。

10.11.3 故障处理步骤

(1) 查看接口物理线路是否 ok

(2) 是否有去往探测目标的路由

(3) 如果服务质量管理探测的对象为域名，是否在设备上配置了 DNS。当探测内网 DNS 服务器时，需要将设备 DNS 服务器指向内网 DNS 服务器；探测外网的知名 DNS 时，首先确定设备是否配置了 DNS 服务器。

10.11.4 故障诊断命令

表10-8 故障诊断命令

命 令	说明
display interface	查看ACG接口状态
display ip route	查看是否有去往目标的路由
display running-config dns	查看是否配置DNS功能

11 应用/用户流量统计故障处理

11.1 应用/用户流量统计后台数据信息查看方法

后台执行 **display flow-account statistics** 可以查看到后台信息具体内容。

11.1.1 故障诊断命令

表11-1 故障诊断命令举例

命令	说明
display flow-account statistics	查看应用/用户流量统计具体信息内容
WorkState: enabled	当前功能开启
AccountPeriod: 1(centi-seconds)	统计周期为百万分之一秒
UserLost: 0	用户（IP或实名认证用户）没有统计出来的数据会显示在此行
UserTopOut: 0	用户没有进入TOP的数据报文计数

命令	说明
UserTopOldIn: 250	用户首次进入TopN统计的报文数量(N为不同硬件规格规定的上限)
UserTopNewIn: 198	后进入TopN的用户统计的报文数量(将首次进入ToP的数据顶出)
UserOverflow: 0	应用/用户流量统计保存的二维表(用户的应用)用户维度统计溢出计数，另一个是二维表应用维度统计溢出计数
AppLost: 0	用户应用没有统计出来的数据会显示在此行
AppTopOut: 0	应用没有进入TOP的数据报文计数
AppTopOldIn: 322	应用首次进入TOP时的报文计数
AppTopNewIn: 126	后进入TOPN的应用统计报文数量(将首次进入ToP的数据顶出)
AppOverflow: 0	应用/用户流量统计保存的二维表(应用的用户)应用维度统计溢出计数
MemLack: 0	内存分配失败的报文计数

12 地址探测故障处理

12.1 接口联动失败后接口down掉无法up起来

12.1.1 故障描述

ACG 配置接口联动，track 目标为下一跳地址，在该接口关联 track 对象，track 失败后，接口无法 up。

12.1.2 故障处理步骤

(1) ACG 上查看接口状是否为 TD（track-down）。

(2) 如果不是 TD 的话查看接口物理线路是否 ok。

(3) 如果是 TD 的话查看 track 对象的下一跳是否为直连接口。

(4) 确定 track 对象下一跳是直连接口后，在接口下删除 track。

12.1.3 故障诊断命令

表12-1 故障诊断命令

命 令	说明
display interface	查看ACG接口状态
display running-config interface	查看接口下关联的track
display track *name*	查看track详细信息
display running-config ha	查看HA配置

13 策略故障处理

13.1 无法访问外网

13.1.1 故障描述

ACG 配置策略后无法访问外网。

13.1.2 故障处理步骤

(1) 是否有去往外网的默认路由。

(2) 是否配置了源 NAT。

(3) ACG 上 IPv4 策略是否将流量拒绝。

13.1.3 故障诊断命令

表13-1 故障诊断命令

命 令	说明
display running-config policy	查看ACG中IPv4策略
display address	查看ACG中IPv4地址对象
debug policy	查看ACG中策略匹配信息
debug app audit detail	查看ACG中具体应用规则和URL规则匹配信息

14 IMC 联动故障处理

14.1 无法重定向认证页面

14.1.1 故障描述

ACG 配置 Portal 认证后访问外网无法重定向 IMC Portal 认证页面。

14.1.2 故障处理步骤

(1) ACG 上 IPv4 策略是否将流量拒绝。

(2) 查看 IPv4 地址对象是否配置正确。

(3) 用户策略中目的地址是否排除了 IMC 服务器地址、认证方式是否正确。

(4) ACG 中 Portal Server 页面的认证 URL 填写是否正确。

14.1.3 故障诊断命令

表14-1 故障诊断命令

命 令	说明
display running-config policy	查看ACG中IPv4策略
display address	查看ACG中IPv4地址对象
display user-policy	查看ACG中用户策略
display running-config user-portal-server	查看ACG中Portal Server配置信息

14.2 无法认证成功

14.2.1 故障描述

- ACG 配置 Portal 认证后，在重定向页面内输入正确的用户名、密码、服务类型，点击上线，页面报错“设备拒绝请求”。
- ACG 配置 Portal 认证后，在重定向页面内输入正确的用户名、密码、服务类型，点击上线，页面报错“向设备发送请求超时”。

14.2.2 故障处理步骤

(1) 查看 Portal Server 配置是否调用了正确的 RADIUS 服务器。

(2) 查看 RADIUS 服务器中服务器地址、服务器密码、端口是否配置正确。

14.2.3 故障诊断命令

表14-2 故障诊断命令

命 令	说明
display running-config user-portal-server	查看ACG中Portal Server配置信息
display radius-server	查看ACG中RADIUS服务器配置信息

14.3 微信认证无法成功

14.3.1 故障描述

- 微信认证失败，点击“我要上网”不弹微信认证界面。
- 微信认证失败，点击“我要上网”后设备在线用户列表中无微信认证用户，反复弹出 Portal 页面。

14.3.2 不弹微信认证界面故障处理步骤

(1) 查看微信认证里的信息是否填写正确。

注意：微信公众号的里 SSID 一定要是本地的 Wifi 名称，公众号里的 SSID 要和设备里配置微信认证的界面 Wifi 名称保持一致。

(2) 不知道应用秘钥怎么办？

可以在微信公众号最下角，选择“开发 > 基本配置 > 开发者密码 > 重置”，点击“重置”重置“应用密钥”（AppSecret）。

(3) 查看是否开启了认证策略：在“用户管理 > 认证策略”里查看。

(4) 在 IPV4 策略里放通所有流量。

(5) 保证客户端能获取到无线对应的 IP 地址，如果 AP 没有开 DHCP，那么一定要在设备接口下开启 DHCP 和 SNAT。

(6) 如果重试几次还没有，可以清除一下浏览器缓存，重新刷新页面。

(7) 微信认证的目的就是为了推广，所以要关注微信号，才能上网，不然会不断提示进行上网认证。

14.3.3 故障诊断命令

表14-3 故障诊断命令

命 令	说明
display user-policy	查看用户策略配置信息
display run dhcp	查看ACG中dhcp配置信息
display run user-wechat	查看微信配置信息

14.3.4 微信认证失败处理步骤

1. 现象描述：

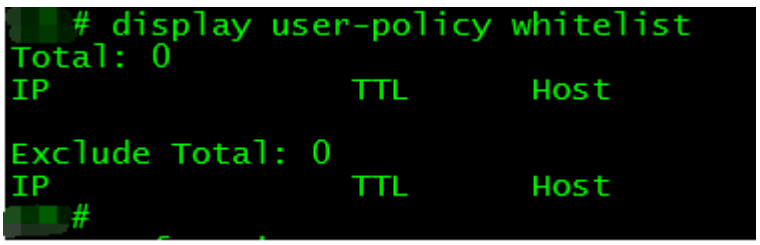
微信认证失败，点击“我要上网”后设备在线用户列表中无微信认证用户，反复弹 portal。

2. 处理步骤：

(1) 确认微信认证页面是否为动态页面，如无法从页面区分可以通过抓包来看用户点击“我要上网”时是否有对应的 HTTP 报文从微信中发出，如抓到报文，需确认该报文中的 HOST 字段是否与 ACG 中“微信认证弹出 URL”配置相同，区分大小写。

(2) 确认“微信认证 URL”是否与“web 认证 URL”配置相同（域名解析后的 IP 地址相同）。

(3) 查看是否有 URL 白名单配置且 URL 白名单中的配置是否与微信认证 URL 配置相同（HOST 相同），如下图应为正确：



当在该图中 Host 下方有微信认证 URL 则需要手动输入 **clear user-policy whitelist**

(4) 微信公众平台中配置的回复链接及 ACG 设备中微信认证 URL 配置是否有误，如：?openId=customer 格式是否正确，请严格遵照典配文档配置。

14.3.5 微信认证注意点

- 静态页面：

微信认证 URL 不可使用静态页面，例如：.html 的页面，建议使用.php、.asp 或嵌入动态脚本的页面，这些动态页面中要保证在 UI 上有变化（每次访问的页面都有差异，例如：嵌入时间或其他变量

- web 认证 URL 页面配置：

配置微信认证时“微信认证弹出 URL”不可与认证导航配置页面中的“web 认证 URL 页面”相同，例如：微信认证弹出 URL 配置 URL 为 www.baidu.com，web 认证 URL 页面配置不可为 www.baidu.com/XXX/XXX。建议配置举例：微信认证弹出 URL 配置 URL 为 www.baidu.com，web 认证 URL 页面配置为 www.sina.com.cn

- 确认应用特征库版本是否是最新的。
- 收集 debug user cfg 及微信认证 URL。
- 微信认证是为了做推广用的，所以需要关注后才能正常上网，否则有时会出现“反复提示认证”的提示。

15 用户中心故障处理

15.1 用户中心中用户无法审计

15.1.1 故障描述

设备接入成功后，特定的用户未在用户中心显示。

15.1.2 故障处理步骤

(1) 检查当前用户中心的用户是否超过规格限制。

(2) 若用户数达到规格，可以通过清除用户的内存缓存，使其识别新的用户。

(3) 若用户未达到规格，用户很多时，需要等几分钟再查看，因为用户根据设备型号不同，同步的时间也各不相同，当用户中心规格高于或等于 2w 时，每 15s 同步 250 个用户；低于 2w 时，每 30s 同步 100 个用户。

15.1.3 故障诊断命令

表15-1 故障诊断命令

命 令	说明
display capacity	查看当前用户中心的规格数UCC_USER即代表的用户中心的用户数，此规格限制是针对内存中对于用户的限制
clear ucc user	清除用户的内存缓存，使其识别新的用户，此时用户中心的页面显示的用户数会比规格数多

15.2 用户管理员密码无法登录设备

15.2.1 故障描述

用户忘记管理员密码导致设备无法进行登录管理。

15.2.2 故障处理步骤

(1) 重启设备，按 ctrl+B 进入 menuboot

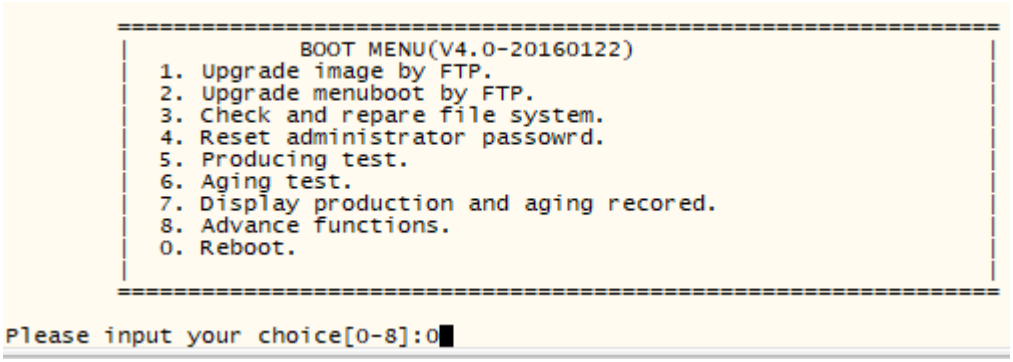
```
Flash boot bus region not enabled, skipping NOR flash config
PCIe: Port 0 not in PCIe mode, skipping
PCIe: Port 1 not in PCIe mode, skipping
PCIe: Port 2 not in PCIe mode, skipping
PCI console init succeeded, 1 consoles, 1024 bytes each
Press CTRL C to enter menuboot 0
reading menuboot
..................................................
54850768 bytes read in 9067 ms (5.8 MiB/s)
```

```
================================================================================
******** Please use the interface to communicate ge0********

        ================================================================
        |             BOOT MENU(V4.0-20160122)                         |
        |   1. Upgrade image by FTP.                                   |
        |   2. Upgrade menuboot by FTP.                                |
        |   3. Check and repare file system.                           |
        |   4. Reset administrator passowrd.                           |
        |   5. Producing test.                                         |
        |   6. Aging test.                                             |
        |   7. Display production and aging recored.                   |
        |   8. Advance functions.                                      |
        |   0. Reboot.                                                 |
        |                                                              |
        ================================================================
```

(2) 进入 menuboot 按选项 4，即可重置管理员密码，默认为 admin。显示“Reset admin password success”表示成功。

```
        ================================================================
        |             BOOT MENU(V4.0-20160122)                         |
        |   1. Upgrade image by FTP.                                   |
        |   2. Upgrade menuboot by FTP.                                |
        |   3. Check and repare file system.                           |
        |   4. Reset administrator passowrd.                           |
        |   5. Producing test.                                         |
        |   6. Aging test.                                             |
        |   7. Display production and aging recored.                   |
        |   8. Advance functions.                                      |
        |   0. Reboot.                                                 |
        |                                                              |
        ================================================================

Please input your choice[0-8]:4
Rest admin password success.
```

(3) 选择 0 重启设备



(4) 重新使用 admin 登录即可。

15.3 用户的应用行为不能记录到时间轴

15.3.1 故障描述

用户登录 QQ，账号可以记录到时间轴上，当该 qq 掉线，重新登录时，该行为不能被记录到时间轴上。

15.3.2 故障处理步骤

特定的时间间隔达到时，相同的应用才能再次被记录到时间轴上。

- 即时通讯类：时间间隔为 1 天，也就是 1 天内时间轴上只会记录不同即时通讯应用。
- 搜索类：时间间隔为 2 分钟
- 社区类：时间间隔为 1 分钟
- 邮件类：时间间隔为 1 分钟
- 视频类：时间间隔为 30 分钟
- 文件传输类：时间间隔为 150 秒
- 电子商务类：时间间隔为 150 秒

16 流量劫持维护指导

流量劫持的主要问题定位手段是查看流量劫持的配置以及 debug 调试命令。下面详细介绍一下流量劫持在典型应用场景中的故障定位思路和方法。

16.1 流量劫持常见问题定位方法

流量劫持在使用中，常见问题包括：

- 有时候不弹广告页面
- 广告页面弹速度较慢

- 访问网页被重置
- 同一个页面弹出多个广告图片

16.1.1 有时候不弹广告页面

不弹广告页面包括以下几种情况：

(1) 如果访问的是 https 网页，则不支持弹广告页面。

(2) 一个网页多次跳转后广告页面无法弹出原因是同一条连接发起了多个 get 请求只对第一个 get 请求作插入。

其他情况不弹广告页面通过调试命令 **debug http hijack** 查看 http 请求是否匹配到流量劫持。

调试命令：**debug http hijack**

16.1.2 广告页面弹出速度较慢

流量劫持广告弹出与网速带宽、广告过滤软件等都有关，网速慢的情况下图片加载就慢。

调试命令：**debug http hijack**

16.1.3 访问网页被重置

个别网站在开启流量劫持的情况下，网页停留一段时间后，提示网页已重置（网页邮箱）这类网站会定期向服务器端发送请求报文，与流量劫持插入代码冲突，导致网页显示重置，目前没有好的处理办法。建议，在域名白名单排除掉该网站

调试命令：**debug http hijack**

16.1.4 同一个页面弹出多个广告图片

一些网站结构为 frameset 框架布局，主界面里包含多个其它请求，广告图片会显示多个，目前暂无法处理，建议：此类网站加入域名白名单排除掉该网站。

调试命令：**debug http hijack**

17 日志信息收集方式

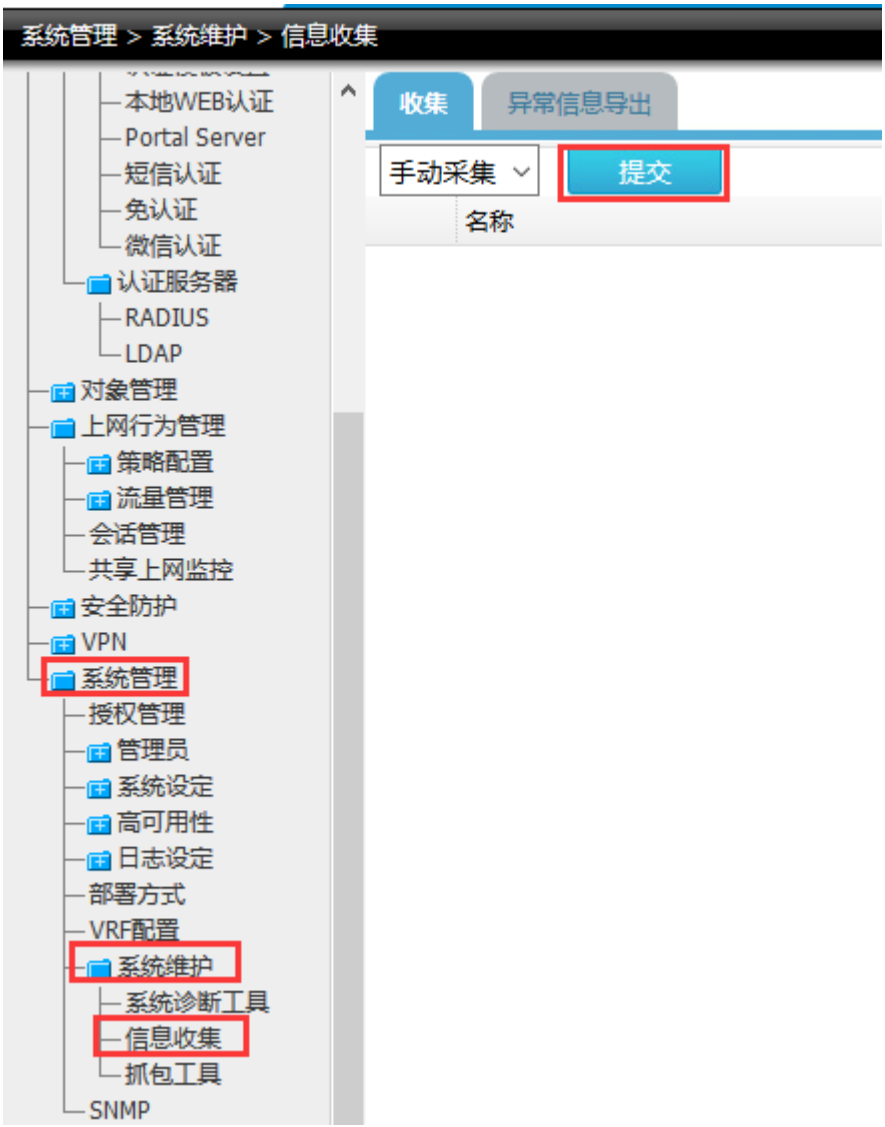
17.1 日志信息收集方式

17.1.1 故障描述

一些应用出现问题或者设备出现意外重启等问题，都会被日志记录下来（保证设备有硬盘或者充当硬盘的外置 U 盘），那么在排查问题的时候，日志收集是很重要的。

17.1.2 日志收集的方式

(1) 在 web 界面收集。



(2) 收集系统版本信息——web 和命令行。

尽量使用命令行收集，使信息更清晰：**display version**

(3) 使用 Debug 打印基本信息用来分析。

根据想抓取的应用或者服务进行 debug 调试信息（请参照 debug 手册进行）；通过 **display log debug** 来收集信息。

(4) 从 web 界面收集一些日志信息，尽量找到离事件发生最近的日志来分析，选中可以复制到 Word 文档中，提供给后端人员进行分析。

17.1.3 故障诊断命

表17-1 常用命令

命 令	说明
debug dp basic	查看数据的基本处理转发流程，以此为例；根据需求进行调整
display log debug	查看日志信息

18 日志分析与管理平台安装卸载故障处理

18.1 安装程序无法正常进行

18.1.1 故障描述

安装程序进行中断，提示端口 80 等被占用，无法正常进行。

18.1.2 故障处理步骤

(1) 在 CMD 模式下输入“**netstat –aon | findstr 80**”查找占用 80 端口的进程。

(2) 卸载该程序或停止占用端口的无关应用，释放端口。

(3) 重新加载安装程序。

(4) 查看安装程序是否可正常进行。

(5) 成功安装后查看控制面板——服务列表中 dnms_db、dnms_loader、dnms_logserver、dnms_reporter、dnms_web 各项服务是否均正常启动；查看日志分析与管理平台是否正常显示。

18.1.3 故障诊断命令

表18-1 常用命令

命 令	说明
netstat –aon | findstr 80	查找占用80端口的进程
tasklist | findstr 80	找到占用80端口的应用名
taskkill /f /im process-name	杀死进程
taskkill /f /pid 8000	杀死进程

18.1.4 其他注意事项

Win2003 服务器由于自带服务“World Wide Web Publishing Service”占用 80 端口所以请先停止该服务再安装。停止该服务操作步骤如下：

“控制面板->管理工具->服务”，打开服务找到“World Wide Web Publishing Service”右键选择停止即可。

18.2 卸载程序无法正常进行

18.2.1 故障描述

运行卸载日志分析与管理平台程序时，卸载程序无法正常进行，提示缺少指向文件等信息。

18.2.2 故障处理步骤

系统正常情况下图各项服务均为正常启动状态，如所示。若有没有正常启动的服务，先尝试把服务正常启动，再执行卸载程序。

图18-1 正常服务启动状态。

(1) 查看控制面板——服务列表中 dnms_db、dnms_loader、dnms_logserver、dnms_reporter、dnms_web 各项服务是否均正常启动。

(2) 未正常开启，尝试开启服务，正常开启后，正常卸载。

(3) 未正常开启，且开启服务失败后，停止所有服务，删除安装目录。

(4) 未正常开启，且开启、停止服务均失败后，删除安装目录，关机重新启动。

18.2.3 安装目录默认路径

系统安装路径默认为 C:\Program Files (x86)\dnms 并且在安装路径中不允许包含中文字符。

18.3 安装结束后提示错误信息

18.3.1 故障描述

安装程序结束，提示某某服务（如 dnms_loader）无法正常启动。

18.3.2 故障处理步骤

(1) 进入控制面板—服务，查看非正常启动的服务。
(2) 尝试手动启动该服务。
(3) 如手动启动失败，可能原因为安装不完整，请重新执行安装程序。

19 日志分析与管理平台设备管理维护指导

19.1 添加、导入设备常见问题分析

19.1.1 故障描述

通过界面添加设备或通过文件批量导入设备均可能会失败，原因多种多样，有些可通过提示信息直接判断失败原因，有些需要进一步排查，归纳主要分为几类。

19.1.2 故障处理步骤

请检查是否含有以下情况：

(1) 名称非法，名称中只能包含中文、英文、数字、空格、特殊字符（“#&%<>除外）
(2) 名称重复
(3) IP 地址非法
(4) 用户名或密码非法
(5) 各类字段字符超长或未达到最短长度等
(6) 未授权设备数量情况下，添加（导入）超过 9 台设备；授权后，添加超过 3000 台设备
(7) 导入文件必填项缺失（设备名称、IP、用户名、密码、设备类型）

19.2 设备状态显示故障定位

19.2.1 故障描述

设备显示为未上线状态。

19.2.2 故障处理步骤

正常情况下，设备状态显示设备当前连接状态，系统每隔一段时间后自动获取最新状态，当设备状态显示未上线时，从以下几个方面排查：

(1) 查看添加设备的用户名和密码是否正确匹配。

(2) 检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址是否可以连通。（设备接口允许 ping 的情况下）。

(3) 通过操作功能，手动重新连接设备，查看是否可以重新连接。

(4) 查看设备端是否允许数据分析与管理平台进行管理，进入到设备端系统，执行命令 **display running-config interface**，查看接口的配置下时候存在命令 **allow access center-monitor**，此配置用来。

20 日志分析与管理平台升级异常维护指导

版本升级包括系统文件和特征库文件升级，可能会存在一些问题，下面详细介绍一下管理员在实际操作中的故障定位思路和方法。

20.1 系统文件升级常见问题定位方法

20.1.1 系统文件无法正常升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。确保版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定升级过程中，网络连通正常，设备状态为在线状态。

20.1.2 其他问题

其他问题如网线等物理层问题导致升级失败的请注意检查，如有其他问题请联系设备售后人员或咨询售后服务电话。

20.2 特征库升级常见问题定位方法

ACG 系统在线运行时需要周期性的更新特征库，才能更好进行应用识别控制和流量控制。若设备可正常与互联网进行通信，则可通过日志分析与管理平台统一对管理的设备进行定期最新特征库。

20.2.1 特征库升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。

(2) 检查上传升级文件是否正确，url 分类特征库文件必须以 uuc 为后缀名，应用特征库文件必须以 uac 为后缀名，确保版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定升级过程中，网络连通正常，设备状态为在线状态。

20.2.2 其他问题

特征库升级的前提是已经购买并导入授权升级许可，如未购买则无法进行升级，购买授权许可证可以联系厂商相关销售人员。

如有其他问题请联系咨询售后人员。

21 日志分析与管理平台策略管理维护指导

21.1 下发策略失败原因分析

21.1.1 故障描述

下发策略提示下发失败。

21.1.2 故障处理步骤

(1) 确定在下发过程中设备在线，且网络连接正常。

(2) 查看下发的策略是否与设备端已有的策略冲突，如下图所示。

图21-1 配置冲突

21.2 对象升级异常

21.2.1 故障描述

应用对象或 URL 对象无法升级或升级后内容错误。

21.2.2 故障处理步骤

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。

(2) 检查升级文件是否正确，版本文件必须以.xml 为后缀名。确保版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确保上传升级文件及升级过程中网络正常。

21.3 各类对象常见故障

21.3.1 对象（组）无法删除

一般各类对象无法删除的原因是因为该对象目前正被引用，需要解除引用后再执行删除。

图21-2 地址被引用

(1) 查看是否被组对象引用（服务组可以引用服务对象，地址组可以引用地址对象）。

(2) 查看是否被其他对象引用（如循环对象中周计划可以引用日计划、服务组可以引用服务组、地址组可以引用地址组）。

(3) 查看是否被策略引用。

21.3.2 地址组（服务组）无法引用其他地址组（服务组）

地址组（服务组）比较特殊，可以引用其他地址组（服务组），因此系统在此设置了环路检测功能，禁止环路引用。

如地址 2 引用了地址 1，当编辑地址 1 引用地址 2 时，提示错误；

禁止环路引用，与设备端保持一致。

图21-3 环路检测

22 日志分析与管理平台日志接收故障处理

接收管理设备的发送日志是日志分析与管理平台的主要功能，导致日志不能接收的原因可能因为设备端配置，也可能因为日志分析与管理平台服务器的故障，总之可能会存在多种多样的问题，下面详细介绍定位日志接收失败的各类原因。

22.1 设备端问题定位

(1) 查看设备端“系统配置 > 日志设置 >日志服务器”是否启用。

(2) 查看日志服务器 IP 地址和端口是否设置为日志分析与管理平台正确的 IP 和端口。

(3) 查看设备端“系统配置 > 日志设置 > 日志过滤” 各类日志过滤设置是否正正确

(4) 设备端自身下发的安全策略（不是通过日志分析与管理平台下发的策略）设置的应用过滤和 URL 过滤是否选择了正确的日志记录类型。

(5) 执行 **display ip route** 命令，查看路由是否正确，ping 服务器地址是否能 ping 通。

22.2 日志分析与管理平台端问题定位

(1) 查看管理设定中 Syslog 端口是否同设备端保持一致，且该端口没被占用。

(2) 用抓包工具查看是否有设备端定时发送来的日志流量，如果没有，则问题一般在设备端或网络传输问题。

(3) 查看控制面板服务中 dnms 各项服务是否正常启动。

(4) 查看服务器中安装目录下（默认路径为 C:\Program Files (x86)\dnms\web\app\logserver\data）中的文件是否正常的写入写出，文件容量不是很大，且没有大容量的文件堆积。

22.3 其他问题

如果出现上述情况，则很可能是数据库文件损毁，建议联系咨询售后人员。

23 日志分析与管理平台服务器异常断电故障处理

23.1 服务器异常断线故障处理

23.1.1 故障描述

由于不可抗力的因素导致服务器或设备异常断电。

23.1.2 故障处理步骤

(1) 重启设备端，查看设备各项配置是否保存，恢复设备端的各项配置（包括日志配置）。

(2) 重启日志分析与管理平台服务器，系统将自动检查数据库文件是否有损坏，如有损坏，重新登录日志分析与管理平台管理系统后会提示损坏的数据库的信息，点击确认后系统自动修复数据库文件。

(3) 重新运行系统查看是否正常运行。

23.1.3 其他问题

如系统自修复后仍有数据库损坏问题，请联系咨询售后人员。

24 日志分析与管理平台报表故障处理

24.1 自定义报表设置不生效问题

24.1.1 故障描述

设置的报表任务在规定的时间内没有自动生成。

24.1.2 故障处理步骤

(1) 确保查看报表之前没有对日志分析与管理平台进行数据库还原操作，因为数据库还原将清空之前服务器上生成的所有报表文件。

(2) 查看报表生成的时间段内，日志分析与管理平台服务器是否正常运行。

(3) 查看报表设置的生成开始时间是否大于当前时间、或生成结束时间已过期。

(4) 若上述均无故障，立即执行该任务，查看是否生成，若无文件生成，重启 dnms_reporter 服务。

24.2 预定义报表不能生效

预定义报表一般已经填好了一些参数值，周计划报表每周六 17:00 自动生成，月计划报表每月最后一天生成）只需要用户设置设备、最后的生成文件格式、是否发送邮箱即可。

24.2.1 故障描述

不能自动生成预定义报表或报表无数据。

24.2.2 故障处理步骤

(1) 如果未自动生成报表，查看预定义报表是否已选择设备，查看服务器在生成时间内是否正常运行。

(2) 如果报表无数据请查询相关日志，确认是否有数据产生。

(3) 若上述均无故障，立即执行该报表，查看是否生成，若无文件生成，重启 dnms_reporter 服务。

24.3 报表不能发送到邮箱

24.3.1 故障描述

报表没有发送至任务指定的邮箱。

24.3.2 故障处理步骤

(1) 没有设置邮箱服务器。

(2) 邮箱服务器验证失败。

(3) 邮箱服务器至测试验证，未保存配置。

(4) 发送邮箱地址错误。

(5) 发送邮箱收件箱已满。

24.3.3 常用功能

(1) 设置邮箱服务器“系统管理 > 邮件服务器配置”。

(2) 添加常用邮箱，“系统管理 > 管理邮件列表”。

25 日志分析与管理平台系统管理故障处理

25.1 管理员权限

25.1.1 授予了角色设备管理的权限，该角色管理员登录不能维护设备

只有资源管理员具有维护设备的权限，授予其他角色的设备管理功能仅能查看设备信息。

25.1.2 新管理员登录后不能查看到设备

管理员只能管理被分配的管理组内的设备，且管理组和管理员为一对一的关系（资员管理除外，他管理所有设备组）。可能原因：新管理员未被分配设备组，新管理员被分配的设备组内没有设备。

25.1.3 编辑角色按钮不可用

可能原因：

- 管理员既不是配置管理员（编辑用户角色），也不是资源管理员（编辑用户管理设备组）。
- 配置管理员（或资源管理员）选择的是自己，不能为自己编辑角色。
- 配置管理员（或资源管理员）选择了多个用户，不能同时编辑多个用户角色。

25.1.4 管理员密码重置按钮不可用

确保执行管理员密码重置功能的用户有足够的权限。

25.2 邮件服务器配置失败

25.2.1 故障描述

邮件服务器连接失败。

25.2.2 故障处理步骤

(1) 查看发送邮箱地址是否正确。

(2) 查看邮箱服务器地址是否正确，并且邮箱服务器是否正常运行。

(3) 查看邮箱密码是否填写正确。

(4) 查看网络连接是否正常。

25.3 数据库备份还原

25.3.1 数据库不能正常备份

一般数据库不能正常备份可能的原因有以下几点：

- 填写的路径非法（包含空格、盘符不存在等原因）。
- 网络连接异常，或备份中网络中断。

- 备份的磁盘已满。
- 备份的磁盘损坏。

请根据以上原因逐项排查。

25.3.2 数据库自动备份没有执行

- 确保保存自动备份数据库的配置。
- 在执行数据库自动备份时服务全部正确开启。

25.3.3 数据库不能还原

数据库还原失败一般有以下几点原因：

- 填写的路径非法（包含空格、路径格式错误等）。
- 填写的目的文件不存在。
- 网络连接异常，或还原中网络中断。
- 用其他服务器上的备份文件还原数据库，系统检测到环境异常，不允许还原（系统规定：不允许不同服务器上的数据库相互还原）。

请根据以上原因逐项排查。

25.3.4 数据库还原后信息缺少

确保数据库还原时，是按照备份顺序来进行还原的，否则会出现部分数据没有还原的情况。

25.4 产品激活失败故障定位

25.4.1 故障描述

产品激活失败。

25.4.2 故障处理步骤

(1) 查看网络连接是否正常。

(2) 看激活码的正确性，确保激活码是从官网或者正规渠道获得的与系统 SN 唯一对应的正确的格式和内容。