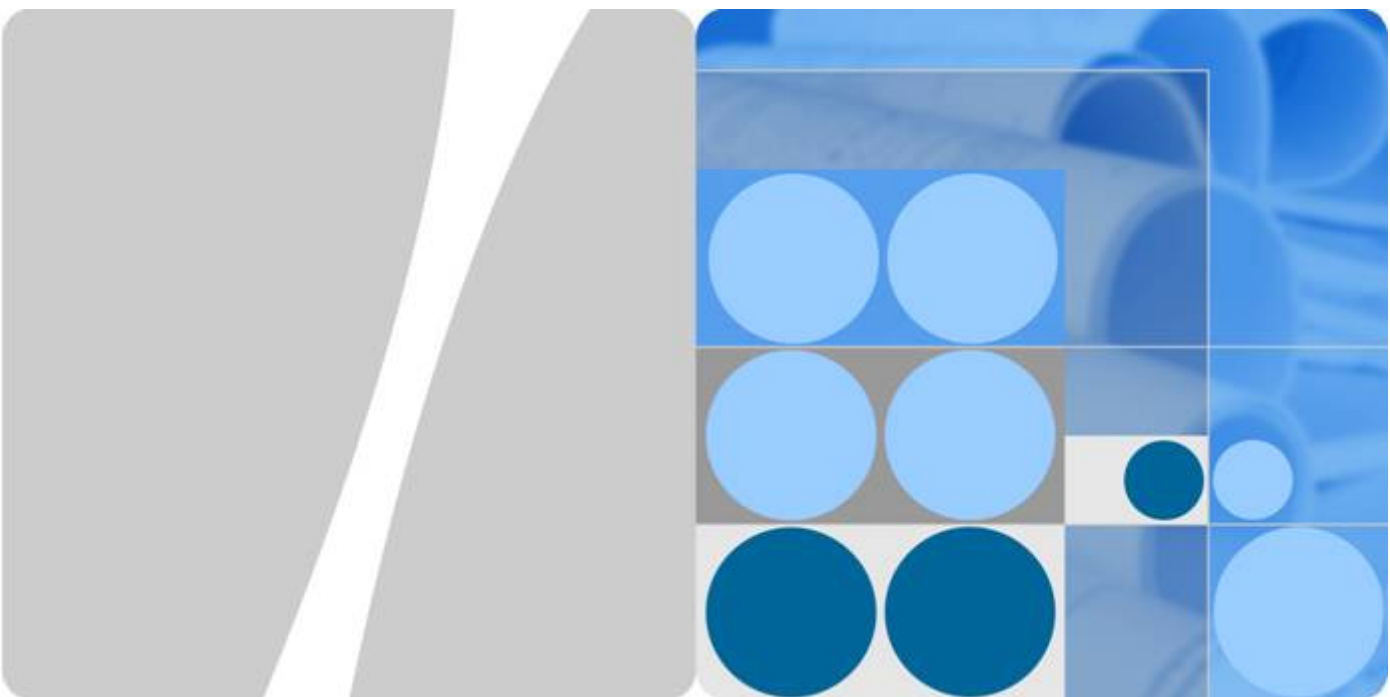




Huawei eSight
V200R002C00

操作指南

文档版本 02
发布日期 2012-03-15

版权所有 © 华为技术有限公司 2012。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：<http://www.huawei.com>

客户服务邮箱：support@huawei.com

客户服务电话：4008302118

目 录

1 从这里开始.....	1
1.1 基础调测.....	2
1.1.1 调测流程.....	2
1.1.2 确认网管所需端口.....	3
1.1.2.1 服务端口介绍.....	3
1.1.2.2 服务器与网元之间的端口.....	4
1.1.2.3 服务器与客户端之间的端口.....	5
1.1.2.4 服务器和 OSS 之间的端口.....	6
1.1.2.5 服务器内部进程间的端口.....	6
1.1.2.6 其他方向的端口.....	9
1.1.3 确认 License 容量.....	10
1.1.4 运行环境要求.....	11
1.1.5 登录和退出 eSight.....	11
1.1.6 了解 eSight 主界面.....	12
1.1.7 添加用户并设置权限.....	13
1.1.8 添加网元.....	15
1.1.8.1 设置网元侧 SNMP 参数.....	15
1.1.8.2 手工创建单个网元.....	16
1.1.8.3 设置网管侧 SNMP 参数.....	17
1.1.8.4 设置网管侧 Telnet 参数.....	18
1.1.9 备份设备配置文件.....	19
1.1.10 添加下级网管.....	19
1.2 基本概念.....	20
1.2.1 安全基本概念.....	20
1.2.2 拓扑基本概念.....	23
1.2.3 资源基本概念.....	26
1.2.4 故障基本概念.....	26
1.2.5 性能基本概念.....	28
1.2.6 报表基本概念.....	28
1.2.7 网元管理基本概念.....	29
1.2.8 业务管理基本概念.....	30
1.2.8.1 IPSec VPN 管理基本概念.....	30
1.2.9 智能配置工具基本概念.....	31

1.2.10 设备配置文件基本概念.....	32
1.2.11 自定义设备管理基本概念.....	32
2 安全管理.....	34
2.1 安全操作全景图.....	35
2.2 安全策略管理.....	37
2.2.1 设置帐号策略.....	37
2.2.2 设置密码策略.....	37
2.2.3 设置访问控制策略.....	38
2.2.3.1 设置登录时间控制策略.....	38
2.2.3.2 设置登录 IP 地址控制策略.....	39
2.2.4 设置客户端自动注销.....	40
2.2.5 修改用户密码.....	41
2.3 配置用户并分配权限.....	44
2.3.1 操作系统用户及权限.....	45
2.3.2 eSight 用户及权限.....	45
2.3.3 设置自定义管理域.....	46
2.3.4 创建角色.....	47
2.3.5 创建用户.....	48
2.4 监控用户.....	50
2.4.1 监控用户会话.....	50
2.4.2 强制用户注销.....	51
2.5 示例：安全管理典型操作.....	51
3 资源管理.....	55
3.1 资源操作全景图.....	57
3.2 自动发现网元.....	58
3.3 创建子网.....	60
3.4 手工创建单个网元.....	62
3.5 手工批量导入网元.....	63
3.6 调整网元所属子网.....	65
3.7 调整子网.....	66
3.8 物理资源管理.....	66
3.9 链路管理.....	67
3.10 电子标签管理.....	69
3.11 示例：资源管理典型操作.....	70
4 拓扑管理.....	72
4.1 拓扑操作全景图.....	73
4.2 物理拓扑管理.....	75
4.2.1 设计物理视图.....	75
4.2.2 调整物理视图.....	75
4.2.2.1 调整网元位置.....	75
4.2.2.2 调整子网位置.....	76

4.2.2.3 设置拓扑背景图.....	76
4.2.2.4 布局拓扑对象.....	77
4.2.3 浏览物理视图.....	78
4.2.3.1 查找拓扑对象.....	78
4.2.3.2 缩放物理视图.....	78
4.2.3.3 保存物理视图.....	79
4.2.3.4 全屏/鸟瞰查看拓扑视图.....	79
4.2.3.5 显示拓扑图例.....	80
4.2.3.6 设置设备标签.....	80
4.2.3.7 打印物理视图.....	81
4.2.3.8 导出物理视图.....	81
4.2.4 示例：拓扑管理典型操作.....	81
4.3 IP 拓扑管理.....	83
4.3.1 IP 拓扑管理功能.....	83
4.3.2 IP 拓扑基本操作.....	84
4.3.3 示例：IP 拓扑管理典型操作.....	85
5 故障管理.....	87
5.1 故障操作全景图.....	88
5.2 设置告警远程通知.....	90
5.2.1 远程通知设置流程.....	90
5.2.2 设置邮箱服务器.....	92
5.2.3 设置短消息服务器.....	92
5.2.4 设置内容模板.....	93
5.2.5 设置用户组.....	94
5.2.6 设置远程通知规则.....	95
5.2.7 按具体告警创建远程通知规则.....	97
5.3 设置故障监控规则.....	98
5.3.1 创建告警屏蔽规则.....	98
5.3.2 设置告警声音.....	100
5.3.3 设置告警自定义过滤条件.....	101
5.4 监控告警.....	102
5.4.1 浏览当前告警.....	102
5.4.2 通过告警板监控告警.....	104
5.4.3 通过拓扑视图监控告警.....	105
5.4.4 通过网元管理器监控告警.....	105
5.4.5 处理告警.....	106
5.4.5.1 告警处理流程.....	106
5.4.5.2 查看告警详情.....	108
5.4.5.3 确认告警.....	110
5.4.5.4 清除告警.....	110
5.5 统计分析.....	111
5.5.1 查询历史告警.....	111

5.5.2 查询事件.....	112
5.5.3 查询被屏蔽告警.....	113
5.6 示例：故障管理典型操作.....	113
6 性能管理.....	117
6.1 性能操作全景图.....	118
6.2 性能监视流程.....	119
6.3 设置性能监视参数.....	121
6.3.1 设置性能监视模板.....	121
6.3.2 创建性能监视任务.....	122
6.3.3 添加性能监视视图.....	124
6.4 浏览性能监视数据.....	125
6.4.1 查询实时性能数据.....	125
6.4.2 查询历史性能数据.....	126
6.4.3 查看网元性能概况.....	127
6.5 示例：性能管理典型操作.....	128
7 报表管理.....	130
7.1 报表操作全景图.....	131
7.2 配置报表的系统参数.....	132
7.2.1 设置数据源.....	132
7.2.2 报表系统配置.....	132
7.3 创建报表.....	133
7.4 查看报表.....	134
7.5 维护报表系统.....	134
7.5.1 修改报表任务.....	134
7.5.2 管理报表存储空间.....	135
7.5.3 管理报表任务的状态.....	135
8 网元管理器.....	136
8.1 网元管理全景图.....	137
8.2 查看网元.....	138
8.2.1 查看基本信息.....	138
8.2.2 查看设备面板.....	139
8.2.3 查看告警列表.....	139
8.2.4 查看性能状态.....	141
8.3 配置网元.....	142
8.3.1 配置网元的 web 网管.....	142
8.3.2 配置协议参数.....	142
8.3.2.1 配置网管侧网元 Telnet 参数.....	142
8.3.2.2 配置网管侧网元 SNMP 参数.....	143
8.3.3 接口管理.....	144
8.3.3.1 了解接口.....	144
8.3.3.2 配置接口.....	144

8.3.3.3 查询接口参数.....	144
8.3.4 查询 IP 地址.....	145
8.3.5 配置文件管理.....	145
9 业务管理.....	146
9.1 IPsec VPN 监控管理.....	147
9.1.1 IPsec VPN 应用.....	147
9.1.2 IPsec VPN 操作全景图.....	147
9.1.3 新建网络域.....	148
9.1.4 发现网络域 IPsec VPN 业务.....	149
9.1.5 监控 IPsec VPN 业务.....	149
9.1.5.1 查看 IPsec VPN 业务拓扑结构.....	149
9.1.5.2 查看 IPsec VPN 业务运行状态.....	149
9.2 WLAN 管理.....	150
9.2.1 WLAN 基本概念.....	150
9.2.2 WLAN 的组网方案及原理介绍.....	150
9.2.3 WLAN 功能全景图.....	155
9.2.4 WLAN 配置任务.....	156
9.2.4.1 向导式配置 WLAN 业务.....	156
9.2.4.2 配置 AC 基本信息.....	157
9.2.4.3 配置 AP 上线.....	158
9.2.4.4 配置 AP 模板.....	159
9.2.4.5 配置射频模板.....	160
9.2.4.6 配置 ESS 模板.....	160
9.2.4.7 配置 AP 域.....	161
9.2.4.8 配置 AP 绑定的模板.....	162
9.2.5 WLAN 维护任务.....	162
9.2.5.1 查看 AC 信息.....	162
9.2.5.2 查看 AP 信息.....	163
9.2.5.3 浏览 STA.....	164
9.2.5.4 浏览全网 SSID.....	165
9.2.5.5 管理 Rogue AP.....	165
9.2.5.6 查看业务拓扑.....	166
9.2.5.7 故障诊断.....	166
9.2.5.8 AP 故障恢复.....	167
9.2.5.9 查看位置拓扑.....	168
9.2.6 示例：WLAN 管理典型操作.....	170
9.3 BGP/MPLS VPN 管理.....	173
9.3.1 了解 BGP/MPLS VPN.....	173
9.3.1.1 基本概念.....	173
9.3.1.2 功能.....	175
9.3.1.3 应用场景.....	175
9.3.2 全景图.....	180

9.3.3 业务自动发现.....	182
9.3.3.1 自动发现流程.....	182
9.3.3.2 自动发现.....	183
9.3.3.3 业务调整.....	184
9.3.4 业务监控.....	185
9.3.4.1 查看业务列表.....	185
9.3.4.2 业务拓扑.....	186
9.3.4.3 区域管理.....	188
9.3.4.4 告警管理.....	190
9.3.4.5 性能管理.....	191
9.3.4.6 报表管理.....	192
9.3.4.7 业务质量审计.....	193
9.3.5 业务故障诊断.....	193
9.3.6 示例：BGP/MPLS VPN 管理典型操作.....	195
9.4 SLA 管理.....	198
9.4.1 了解 SLA.....	198
9.4.1.1 SLA 基本概念.....	198
9.4.1.2 SLA 功能简介.....	199
9.4.1.3 SLA 术语及系统默认设置.....	200
9.4.2 SLA 管理全景图.....	213
9.4.3 配置 SLA 任务.....	214
9.4.3.1 新建服务.....	214
9.4.3.2 新建任务.....	215
9.4.3.3 快速诊断.....	216
9.4.4 监控 SLA 任务.....	216
9.4.4.1 查看 SLA 任务管理界面.....	216
9.4.4.2 查看 SLA 单任务历史数据统计界面.....	217
9.4.5 SLA 配置举例.....	217
9.4.5.1 示例：创建系统预定义视频监测任务.....	218
9.4.5.2 示例：创建用户自定义监测任务.....	218
10 智能配置工具.....	220
10.1 智能配置工具全景图.....	221
10.2 智能配置工具功能.....	222
10.3 智能配置工具流程介绍.....	223
10.3.1 按模板下发.....	223
10.3.2 按规划表下发.....	224
10.3.3 下发记录管理.....	225
10.4 智能配置工具配置任务.....	226
10.4.1 模板管理与下发.....	226
10.4.1.1 新建模板.....	226
10.4.1.2 部署模板.....	227
10.4.1.3 导出规划表.....	227

10.4.2 规划表管理与下发.....	228
10.5 智能配置工具配置示例.....	228
10.5.1 示例：按模板下发场景.....	229
10.5.2 示例：按规划表下发场景.....	229
11 设备配置文件管理.....	231
11.1 设备配置文件管理全景图.....	232
11.2 设置 FTP 参数.....	233
11.3 备份网元配置数据.....	234
11.3.1 使用备份任务备份网元配置数据.....	234
11.3.1.1 新建备份任务.....	234
11.3.1.2 启用备份任务.....	234
11.3.1.3 维护备份任务.....	235
11.3.2 手工备份网元配置数据.....	235
11.4 管理网元配置数据.....	236
11.4.1 查看网元配置数据文件.....	236
11.4.2 浏览网元配置数据文件备份列表.....	237
11.4.3 比较网元配置数据文件.....	237
11.4.4 基线化网元配置数据文件.....	237
11.4.5 设置备份文件上限.....	238
11.5 恢复网元配置数据.....	239
12 自定义设备管理.....	240
12.1 自定义设备管理全景图.....	241
12.2 自定义设备功能介绍.....	242
12.3 自定义设备配置流程.....	246
12.4 发现自定义设备.....	246
12.4.1 手工添加自定义设备.....	246
12.4.2 自动发现自定义设备.....	248
12.4.3 批量导入自定义设备.....	249
12.5 自定义厂商和设备类型.....	251
12.6 设备管理能力定制.....	252
12.6.1 自定义告警参数.....	252
12.6.2 自定义性能指标.....	254
12.6.3 自定义设备配置文件.....	255
12.6.4 自定义设备面板.....	255
12.7 检测自定义设备网络状态.....	257
12.7.1 执行 Ping 测试.....	257
12.7.2 执行 Trace 测试.....	257
12.7.3 查询接口基本信息.....	258
12.7.4 查看 IP 地址表.....	258
12.8 调用自定义设备的 Web 网管.....	258
13 系统管理.....	260

13.1 系统操作全景图.....	261
13.2 设置 eSight 数据溢出转储.....	263
13.2.1 设置日志数据库溢出转储.....	263
13.2.2 设置告警数据库溢出转储.....	264
13.2.3 设置性能数据库溢出转储.....	265
13.2.4 设置 SLA 数据库溢出转储.....	266
13.3 查询日志.....	267
13.3.1 日志类型.....	267
13.3.2 查询安全日志.....	267
13.3.3 查询系统日志.....	268
13.3.4 查询操作日志.....	268
13.4 下级网管.....	269
13.4.1 了解下级网管.....	269
13.4.1.1 下级网管的应用.....	269
13.4.1.2 下级网管相关功能.....	270
13.4.2 管理下级网管.....	270
13.4.2.1 增加下级网管.....	270
13.4.2.2 查看下级网管信息.....	271
13.4.2.3 测试下级网管连通性状态.....	271
13.5 管理 License.....	271
13.5.1 查看 eSight 当前 License.....	272
13.5.2 获取 ESN.....	273
13.5.3 导入 License.....	273
13.6 备份/恢复数据库.....	274
13.7 网元包组件管理.....	274
14 例行维护.....	276
14.1 维护项目列表.....	277
14.2 如何获取技术支持.....	277
14.3 每日维护操作.....	278
14.3.1 浏览当前网管告警.....	278
14.3.2 查询安全日志.....	280
14.3.3 备份/恢复数据库.....	280
14.4 每周维护操作.....	281
14.4.1 检查服务器磁盘状态.....	281
14.4.2 检查服务器磁盘空间.....	282
14.4.3 检查 Oracle 数据库日志.....	282
14.4.4 检查防病毒软件运行状态.....	282
14.4.5 检查操作系统日志.....	283
14.4.6 检查 MySQL 数据库日志.....	284
14.5 每月维护操作.....	284
14.5.1 修改 eSight 当前用户密码.....	284
14.5.2 检查 eSight 服务器时间.....	284

14.5.3 清理 eSight 服务器磁盘空间.....	285
14.6 每季度维护操作.....	286
14.6.1 检查机房环境.....	286
14.6.2 检查服务器供电情况.....	287
14.6.3 检查服务器硬件和外设.....	287
15 命令参考.....	289
15.1 eSight 命令参考.....	290
15.1.1 启动 eSight 进程和帮助进程.....	290
15.1.2 停止 eSight 进程和帮助进程.....	292
15.1.3 查看日志级别.....	293
15.1.4 修改日志级别.....	299
15.1.5 查看 eSight 启动状态.....	303
15.1.6 查看 eSight 进程状态.....	304
15.1.7 查看 SBus 服务信息.....	305
15.2 Oracle 命令参考.....	316
15.2.1 sqlplus 命令.....	316
15.2.2 startup 命令.....	317
15.2.3 shutdown 命令.....	318
15.2.4 show 命令.....	319
15.2.5 alter 命令.....	321
16 FAQ.....	323
16.1 如何解决通过 IE8 操作 eSight 时系统提示未选中告警声音复选框的问题.....	324
16.2 如何解决登录 eSight 时发生安全证书错误的问题.....	324
16.3 如何解决登录 eSight 时发生的安全警告问题.....	332
16.4 如何解决使用中文版本的 Firefox 浏览器访问 eSight 英文界面时，个别英文字段无法完全显示的问题.....	337
16.5 如何解决在 IE 浏览器中安装 eSight 提供的 Adobe Flash Player 时安装失败问题.....	340
16.6 如何解决使用 Firefox 浏览器访问 eSight 的 Flash 页面时，提示 Flash 插件已崩溃问题.....	341
16.7 如何解决复制某些阿拉伯字符显示为乱码的问题.....	342
16.8 如何根据网管所需端口情况，自定义端口连接规则.....	342
16.9 如何解决因数据库异常停止使网元出现垃圾数据而导致网管无法管理该网元的问题.....	343
16.10 如何解决 eSight 界面无法正常显示，注销时出现整页程序代码的问题.....	345
16.11 如何配置服务器 SNMP 参数.....	345
16.12 如何解决因修改 eSight 服务器系统时间对 eSight 产生的影响.....	346
A 术语.....	348

1 从这里开始

关于本章

如果您需要了解新安装完成的网管需要做哪些基础调测或需要整体了解 eSight 的功能特点及界面构成，请阅该部分。

1.1 基础调测

1.2 基本概念

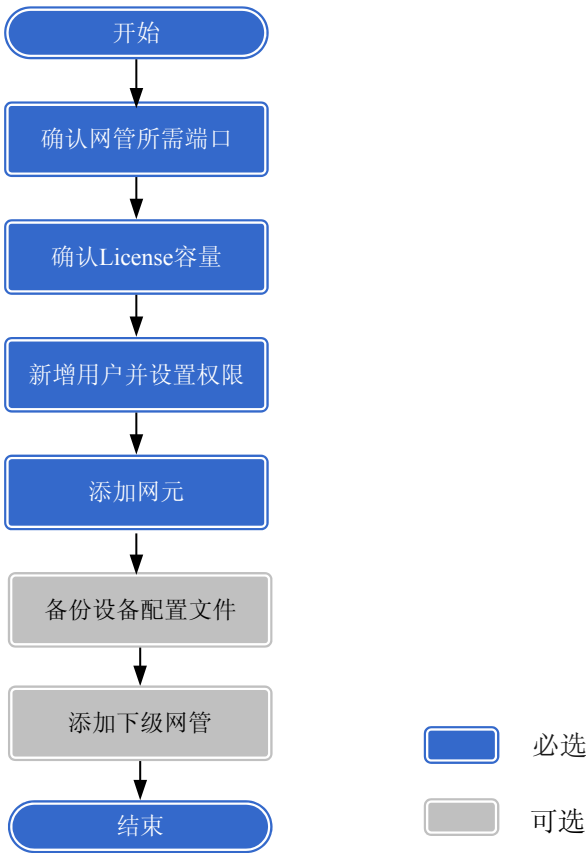
在使用 eSight 前，需要了解 eSight 各个模块的基本概念，包括资源、拓扑、安全、故障和性能基本概念。理解这些概念可以更快速、更准确地操作 eSight。

1.1 基础调测

1.1.1 调测流程

通过调测完成网管基本功能的配置验证。
调测流程如图 1-1 所示。

图 1-1 调测流程图



操作	备注
1、1.1.2 确认网管所需端口	根据网管所需端口列表检查相应端口占用情况，以确保网管可以正常使用这些端口而不发生冲突。
2、1.1.3 确认 License 容量	确认 License 容量，以确保网管的功能项可以正常使用。

操作	备注
3、 1.1.7 添加用户并设置权限	为网络设备的维护人员创建用户帐号，设置用户的基本信息和操作权限，不同的维护人员分配不同的操作权限，提高网管操作的安全管理。
4、 1.1.8.2 手工创建单个网元	将网元添加到网管，并进行管理。
5、(可选) 1.1.9 备份设备配置文件	及时对设备配置文件进行备份，以防止意外操作导致当前配置文件不可用，使用备份的配置文件进行恢复，提高网管对配置文件的安全管理。
6、(可选) 1.1.10 添加下级网管	在分级网管的场景下，可以通过逐级定义下级网管来实现对于下游网管性能、告警等信息的监控。

1.1.2 确认网管所需端口

根据网管所需端口列表检查相应端口的使用情况，确保网管可以正常使用这些端口而不发生冲突。

1.1.2.1 服务端口介绍

介绍 eSight 使用的服务端口。eSight 对各服务的端口号进行统一分配，避免了端口使用冲突的情况。所有端口采用 TCP 或 UDP 协议在服务器端和客户端之间进行通信。

eSight 服务端口简述

在防火墙的安全策略中，需要结合 IP 地址和 TCP(Transmission Control Protocol)/UDP (User Datagram Protocol)的端口号来进行流量过滤。

TCP/UDP 端口号可以用来分离数据包，并将相应的数据包传递给正确的应用程序。

TCP/UDP 端口号范围从 0 ~ 65535，被划分为如下 3 段：

- 0 ~ 1023，被用来标识一些标准的服务，如 FTP、Telnet、TFTP(Trivial File Transfer Protocol)等。
- 1024 ~ 49151，因特网地址分配组织 IANA(Internet Assigned Number Authority)分配给已注册的应用进程。
- 32768 ~ 65535，作为私有端口号，可以被动态分配给任何应用。

eSight 服务端口包含多种类型，具体如下：

- [服务器和网元之间的端口\(服务器侧\)](#)
- [服务器和客户端之间的端口\(服务器侧\)](#)
- [服务器和 OSS 系统之间的端口\(服务器侧\)](#)
- [服务器和 OSS 系统之间的端口\(OSS 侧\)](#)
- [服务器内部进程间的端口](#)

1.1.2.2 服务器与网元之间的端口

介绍 eSight 服务器和网元之间使用的端口。

当 eSight 服务器和网元之间部署防火墙时，需要按照如下要求开放端口：

网元的任意端口能透过防火墙和表 1-1 中所列的端口建立连接。

表 1-1 eSight 服务器连接网元时服务器侧需要打开的端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	网元	23	Telnet 端口，配置网元业务时需要使用，必须打开。	是
eSight 服务器	大于 1024 的随机端口	UDP	网元	161	设备接收 SNMP 请求的端口，配置网元业务时需要使用，必须打开。	是
网元	大于 1024 的随机端口	TCP	eSight 服务器	21	FTP 服务器用于传输文件。	是
网元	大于 1024 的随机端口	SNMP	eSight 服务器	162	接收被管理设备 trap。	是
网元	大于 1024 的随机端口	SNMP	eSight 服务器	10162	接收被管理设备 trap，eSight 接收告警的端口。	否
网元	大于 1024 的随机端口	TCP	eSight 服务器	39008	Mediation 的 soap 协议适配器。	否
网元	大于 1024 的随机端口	TCP	eSight 服务器	31022	SFTP 服务器用于传输文件。	是
网元	大于 1024 的随机端口	TCP	eSight 服务器	31023	FTPS 服务器用于传输文件。	是

1.1.2.3 服务器与客户端之间的端口

介绍 eSight 服务器和客户端之间使用的端口。

当 eSight 服务器和客户端之间部署防火墙时，需要使能 eSight 服务器的端口，使客户端能透过防火墙和表 1-2 中所列的服务器侧端口建立连接。

表 1-2 用于连接 eSight 客户端的服务器侧端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTP	eSight 服务器	8080	eSightWeb 服务使用的端口。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTPS	eSight 服务器	8443	用于登录界面，登录时安全通讯的端口。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTPS	eSight 服务器	8445	维护工具登录时安全通讯的端口。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTP	eSight 服务器	8888	图形化命令行 http 访问端口，批量配置、网元管理需要使用。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTP	eSight 服务器	8889	eSight 维护工具 Web 服务使用的端口。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTP	eSight 服务器	38080	联机帮助、故障采集工具和报表下载的共用访问端口。	是
WEB 浏览器 (eSight)	大于 1024 的随机端口	HTTPS	eSight 服务器	38443	用于联机帮助登录界面。	是

1.1.2.4 服务器和 OSS 之间的端口

介绍 eSight 服务器和 OSS（Operation Support System）之间使用的端口。

当 eSight 服务器和 OSS 之间部署防火墙时，需要保证 OSS 的任意端口能透过防火墙和表 1-3 中所列的端口建立连接。

表 1-3 连接 OSS 时 eSight 服务器侧需要打开的端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	6666	UDP	OSS	任意端口	向北向发送 trap 源端口	是

eSight 服务器和 OSS 系统之间(OSS 侧)的端口如表 1-4 所示。

表 1-4 eSight 服务器和 OSS 系统之间(OSS 侧)的端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
OSS	大于 1024 的随机端口	TCP	eSight 服务器	21	ftp 接口，用于向北向传输文件	是
OSS	大于 1024 的随机端口	UDP	eSight 服务器	4700	北向接收上级网管下发的 SNMP 命令的端口	是

1.1.2.5 服务器内部进程间的端口

介绍 eSight 服务器内部进程间的端口。

eSight 服务器内部进程间的端口仅用于 eSight 内部进程通信，不与外部通信。可以通过端口扫描工具查看，但是不需要在防火墙配置。

服务器内部进程间的端口如表 1-5 所示。

表 1-5 eSight 服务器内部进程间的端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	30999	Virgo 的 shell 端口	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	31000	OSGI 调试端口	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	31003	SSO Server 访问安全管理	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	31004	JSON 总线端口	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	31005	Hession 总线端口	否
eSight Med Node	31007	TCP	eSight Med Center	31006	Med Node 和 Med Center 连接	否
eSight 服务器	31009 , 31011	TCP	eSight 服务器	31010 , 31012	Socket 端口, 用于 license 服务	否
eSight 服务器	10001 , 10003	TCP	eSight 服务器	10002 , 10004	Socket 端口, 用于 license 服务	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	32403	检测网管启停状态的端口	否
eSight 服务器	任意端口	TCP	eSight 服务器	33306	MySQL 进程, 用于数据库连接	是
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	38085	Hedex web 服务停止端口	否

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	40000	jmx 端口	否
eSight 服务器	5656	TCP	eSight 服务器	5656	eSight 与智能配置工具 Socket 通讯端口	是
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	8081	Web 服务端口(用于维护工具和服务器的交互)	是
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	8444	用于登录界面(用于维护工具和服务器的交互)	是
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	32001	OSGI 调试端口(用于维护工具和服务器的交互)	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	32006	检测网管启停状态的端口(用于维护工具和服务器的交互)	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	40001	jmx 端口(用于维护工具和服务器的交互)	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	32004	OSGI 调试端口（用于维护工具）	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	32008	检测网管启停状态的端口（用于维护工具）	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	33336	JSON 总线端口（用于维护工具）	否

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	33337	Hession 总线端口（用于维护工具）	否
eSight 服务器	大于 1024 的随机端口	TCP	eSight 服务器	40002	jmx 端口（用于维护工具）	否

1.1.2.6 其他方向的端口

介绍 eSight 服务器与周边其他应用通信的端口。

eSight 服务器与周边其他应用通信的端口如表 1-6 所示。

表 1-6 其他方向的端口

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	Email 服务器	25	SMTP 协议端口	是
eSight 服务器	大于 1024 的随机端口	TCP	短信网关	5018	SMPP3.3/3.4 协议端口	是
eSight 服务器	大于 1024 的随机端口	TCP	短信中心	5090	SMPP3.3/3.4 协议端口	是
eSight 服务器	大于 1024 的随机端口	TCP	短信网关	7890	CMPP2.0/2.1 协议端口	是
eSight 服务器	大于 1024 的随机端口	TCP	短信网关	7891	CMPP3.0 协议端口	是

源端	源端口	协议类型	目的端	目的端口	端口说明	目的侧防火墙是否要打开此端口
eSight 服务器	大于 1024 的随机端口	TCP	短信网关	8801	SGIP1.2 协议端口	是

1.1.3 确认 License 容量

确认 License 容量是否满足现网需求。

前提条件

已导入 License。

背景信息

License 信息详细说明如表 1-7 所示。

表 1-7 License 信息

类别	属性	说明	举例
基本信息	License 失效时间	License 的失效时间	2011-04-14
	失效前提醒时间(天)	提示您 License 在此时间后失效并产生告警，您需导入新的 License	15
资源控制	资源名称	License 管理的资源的名称	客户端数
	License 使用状态	License 管理的资源的使用情况	30/2000 表示 License 能够管理的此类资源为 2000，当前已使用 30
	重要告警阈值	当资源使用率超过设定的告警阈值时，系统产生告警。	80%
功能控制	功能名称	eSight 提供的功能	故障管理
	是否支持	License 是否支持用户使用此功能	支持

操作步骤

- 步骤 1** 选择“系统 > License 管理”。
- 系统显示当前 License 的所有信息。

----结束

1.1.4 运行环境要求

为了使用户更好的在客户端中浏览并操作 eSight，PC 机需要满足特定的运行环境要求。

eSight 运行环境要求，如表 1-8 所示。

表 1-8 eSight 运行环境要求

配置项	基本配置要求
计算机硬件配置	Inter(R) Pentium(R) Dual CPU E2180 @ 2.00GHz、2G 内存
操作系统	Windows XP、Windows 7、Windows 2008
浏览器	Firefox 3.6、Internet Explorer 8 说明 ● 若使用 Internet Explorer 8，则需要设置 Internet Explorer 8 的浏览模式。设置方法如下： 1. 在 Internet Explorer 8 浏览器菜单栏中，选择“工具 > 兼容性视图设置”。 2. 在“兼容性视图设置”对话框中，选中“在兼容性视图中显示 Intranet 站点”和“在兼容性视图中显示所有网站”。 ● 由于 Windows 2008 操作系统默认具有较高的安全策略，使用 Windows 2008 操作系统的客户端无法使用 Internet Explorer 8 登录非本客户端的网管系统。如有需要可以联系操作系统管理员，降低系统安全策略。
分辨率	1024 x 768

1.1.5 登录和退出 eSight

介绍如何登录和退出 eSight。

前提条件

eSight 采用浏览器/服务器的工作模式。登录前请确保当前 PC 机和 eSight 服务器之间的网络连接正常，并且 eSight 服务器工作正常。

背景信息

eSight 缺省提供一个初始用户 admin，初始密码为 Changeme123。此用户拥有 eSight 所有管理对象的所有操作权限。



注意

- 第一次成功登录 eSight 后，请修改密码以确保 eSight 的访问安全性。
- 操作过程中如果需要回退，请不要使用浏览器自带的返回功能，否则会丢失正在操作的数据并会退出 eSight。

登录 eSight

步骤 1 在浏览器地址栏中输入 `http://eSight 服务器的 IP 地址:eSight 服务器端口号/`（例如 `http://12.10.10.1:8086/`），按“Enter”。

系统显示 eSight 登录页面。



- eSight 默认端口号为“8086”。
- 在登录 eSight 提示 License 不合法时，可以在提示信息页面选择更新 License、直接登录或获取 ESN 号以申请新 License。如何更新导入 License 请参见 [13.5.3 导入 License](#)，如何获取 ESN 请参见 [13.5.2 获取 ESN](#)。

步骤 2 输入登录“用户名”和“密码”。

步骤 3 单击“登录”。



- 当密码将要超过有效期时，eSight 会提示需在有效期内修改密码。
- 若在线用户数已经达到 eSight 当前版本支持的最大数，eSight 会提示用户不能登录，此时请联系系统管理员。

----结束

退出 eSight

步骤 1 单击 eSight 客户端右上角的。
退出 eSight。

----结束

1.1.6 了解 eSight 主界面

指导您快速了解企业网网管的界面构成。

eSight 的主界面如[图 1-2](#)所示。

图 1-2 eSight 主界面



1、主菜单	主菜单主要包括“系统”、“资源”、“报表”、“性能”、“网络应用”、“操作维护”和“故障”。
2、常用信息及按钮	显示当前登录的用户名、网管帮助按钮、注销按钮。
3、告警指示灯区	显示告警的条数和级别。
4、新增 Portlet	自定义首页。
5、统计区	显示统计图，统计图包括。 ● TOP 故障网元统计 ● 下级网管 ● TOP10 CPU 利用率 ● TOP10 内存利用率 ● TOP10 接口流入带宽利用率 ● TOP10 接口流出带宽利用率 ● 子网列表

1.1.7 添加用户并设置权限

当 eSight 缺省提供的用户已不能满足当前网络管理需求时，可以根据实际需要创建新的用户。

前提条件

- 已具备“安全管理”的操作权限。
- 已了解用户帐号策略和密码策略，即帐号和密码的设置要求、合法条件。
帐号策略和密码策略请参见 [2.2.1 设置帐号策略](#)和 [2.2.2 设置密码策略](#)。

背景信息

新用户各项属性除了用户名和密码在新建用户过程中必须设置以外，其他属性可使用缺省值或在新建用户以后设置。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“权限分配 > 用户”。

步骤 3 在“用户”页面中，单击“创建”。

步骤 4 在“创建用户”页面中，设置基本信息。

1. 在“基本信息”步骤中，设置“用户名”、“密码”、“确认密码”和“描述”，并设置“账号使用状态”为“启用”。
2. 单击“下一步”。

步骤 5 在“创建用户”页面中，设置所属角色，使用户拥有角色的管理权限和操作权限。

1. 在“所属角色”步骤中，选中用户所属角色名前的复选框。



说明

单击“角色名”列中的角色名，在“查看角色”对话框中可查看角色的详细信息。

2. 单击“下一步”。

步骤 6 在“创建用户”页面中，设置访问控制，使用户只能在特定时间段、从特定 IP 地址登录 eSight。

1. 在“访问控制”步骤中，选择登录时间控制策略和限制可登录的 IP 地址区间，以限制用户的可登录时间和可登录 IP 地址区间，确保 eSight 的访问安全性。



说明

- 若“时间策略”列表中不存在所需的登录时间控制策略，单击“创建”，可创建所需的登录时间控制策略。如何创建登录时间控制策略请参见 [2.2.3.1 设置登录时间控制策略](#)。
- 若“允许访问的 IP 地址区间”列表中不存在所需的登录 IP 地址控制策略，单击“创建”，可创建所需的登录 IP 地址控制策略。如何创建登录 IP 地址控制策略请参见 [2.2.3.2 设置登录 IP 地址控制策略](#)。

2. 单击“完成”。

----结束

后续处理

创建用户后，在“用户”页面中可以执行如下操作。

维护用户	操作方法
查看用户	通过查看用户，可了解用户的详细信息。 单击“用户名”列中的目标用户名，在“查看用户”页面中可查看目标用户的详细信息。
修改用户	当需要适当调整用户信息时，可修改用户的相关信息。 1. 单击目标用户所在“操作”栏中的  ，可以修改用户的相关信息。 2. 在“修改用户”页面中，修改“基本信息”、“所属角色”、“访问控制”。修改“基本信息”可参见 步骤 4 ，修改“所属角色”可参见 步骤 5 ，修改“访问控制”可参见 步骤 6 。 3. 单击“确定”。
删除用户	当不再使用某用户时，可删除该用户。 1. 单击目标用户所在“操作”列中的  。 2. 在“确认”对话框中单击“是”。
重置密码	当用户登录 eSight 时忘记密码，可在重置密码后，让用户使用新密码登录 eSight。 1. 单击目标用户所在“操作”列中的  。 2. 在“重置密码”对话框中，根据下方的密码规则设置“新密码”、“确认密码”。 3. 单击“确定”。
启用用户	帐号长时间未使用且达到帐号策略设置的帐号连续未使用天数时，帐号会被停用。若需重新使用该用户时，可启用被停用的用户。 单击目标用户所在“操作”列中的  ，可启用被停用的用户。
停用用户	当暂时不使用某用户时，可停用该用户。 单击目标用户所在“操作”列中的  ，可以停用用户。

1.1.8 添加网元

将网元添加到网管进行管理。

1.1.8.1 设置网元侧 SNMP 参数

在网管系统中创建网元之前，需要通过命令行设置网元侧的 SNMP 参数。

背景信息

网管系统能够通过 SNMP 协议发现并管理网元的前提是：

- 网元侧配置了正确的 SNMP 参数。
- 网管侧配置的 SNMP 参数与网元侧配置的 SNMP 参数一致。

操作步骤

步骤 1 执行 **system-view** 命令，进入系统视图。

步骤 2 执行 **snmp-agent** 命令，启动 SNMP Agent 服务。

步骤 3 对于 SNMPv1/v2c，请执行该步骤，对于 SNMPv3，请跳过该步骤，执行**步骤 4**。

1. 执行 **snmp-agent sys-info version { { v1 | v2c } * }** 命令，设置 SNMP 协议版本。
2. 执行如下命令，设置读团体名。

```
snmp-agent community read community-name [ [ mib-view view-name ] | [ acl acl-number ] ]*
```

3. 执行如下命令，设置写团体名。

```
snmp-agent community write community-name [ [ mib-view view-name ] | [ acl acl-number ] ]*
```

步骤 4 对于 SNMPv3，请执行该步骤。

1. 执行 **snmp-agent sys-info version v3** 命令，设置 SNMP 协议版本。
2. 执行如下命令，设置 SNMP 用户组：

```
snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view | [ write-view write-view ] | [ notify-view notify-view ] | [ acl acl-number ]
```

3. 执行如下命令，为 SNMPv3 组添加新用户：

```
snmp-agent usm-user v3 user-name group-name [ [ authentication-mode { md5 | sha } password ] | [ privacy-mode des56 password ] ] | [ acl acl-number ]
```

----结束

1.1.8.2 手工创建单个网元

当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。

前提条件

已具备“资源接入”的操作权限。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口的导航树中，选择新增网元的父对象，在右侧页面单击“单个创建”。

步骤 3 在“选择类型”页面的“物理设备类”中，选择待创建网元的类型。

步骤 4 在“配置参数”页面中，设置待创建网元的基本信息和 SNMP 协议参数。

 说明

对于需要配置 SNMP 协议参数的网元，可配置完 SNMP 协议参数后单击“保存协议模板”，作为 SNMP 协议参数的配置模板。当再次需要配置 SNMP 协议参数时可直接单击“选择协议模板”，应用已保存的协议模板。

步骤 5 单击“确定”。

 说明

- 单击“应用”，可继续创建网元。
- 如果网元创建成功，在管理对象列表中可查看到新增网元。
 - 如果网元创建失败，则会弹出“错误”提示框，说明网元添加失败的原因。单击“确定”，重新配置参数。

----结束

后续处理

通过手工单个创建网元功能增加网元到 eSight 后，在“资源管理”窗口中可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 1. 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 1. 在“搜索类型”下拉框中选择搜索类型。 2. 在“搜索条件”文本框中输入搜索条件。 2. 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的 . 2. 在修改网元信息页面修改网元的名称。 3. 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 1. 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的 . ● 批量删除：选择需要删除的网元，单击“批量删除”。 2. 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理窗口。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的 . 2. 在弹出的网元管理器窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

1.1.8.3 设置网管侧 SNMP 参数

当网管与网元之间使用 SNMP 协议进行通信且网元侧的 SNMP 参数有变化时，需要同步修改网管侧网元的 SNMP 参数。

前提条件

网管上已添加网元。

背景信息

eSight 可通过 SNMP 协议访问被管理网元。当手动或自动创建 SNMP 网元时，eSight 使用缺省 SNMP 参数模板完成到指定网元的适配，以确定被管理网元所支持的 SNMP 协议参数。适配成功的缺省 SNMP 参数模板即成为该网元对应网管侧的 SNMP 参数配置，其后对该网元的全部管理操作都通过此 SNMP 参数进行。当网元访问协议的参数发生变化时，需要修改指定网元的访问协议参数。

操作步骤

步骤 1 在主菜单中选择“资源 > 物理资源”。

步骤 2 选中一台或多台设备，单击“设置 SNMP 参数”。

步骤 3 在弹出的“设置 SNMP 参数”窗口中设置 SNMP 相关参数。

- **SNMP 协议版本：**当前支持 SNMPv1、SNMPv2c、SNMPv3 三个版本，SNMPv3 应用在通讯参数安全级别要求比较高的场景下。
- **读团体字：**网管系统在向设备发送读操作请求时候的团体名。只有与该设备认可的读团体名相同时，才能进行读操作。
- **写团体字：**网管系统在向设备发送写操作请求时候的团体名，只有与该设备认可的写团体名相同时，才能进行写操作。
- **超时时间（秒）：**网管系统在向设备发送操作请求时的等待响应的时间。
- **重发次数：**网管系统在向设备进行一次 SNMP 参数设置过程中，超时情况下重复发送操作请求的最大次数，超过该次数即认为操作失败。
- **网元端口：**该网元的 SNMP 协议通信端口。
- **安全名：**访问设备时所使用的设备用户名。
- **上下文名称：**上下文引擎名称。
- **上下文引擎：**代表一个 SNMP 引擎的管理性唯一标识符。和环境名称一起使用唯一地标识一个 SNMP 实体的环境，只有发送端的环境和接收端的环境完全匹配才对 SNMP 消息包进行处理，否则 SNMP 消息包被丢弃。
- **鉴权协议：**用于消息验证时采用的协议。可选择 HMACMD5、HMACSHA 协议或不使用协议。选择了 HMACMD5 或 HMACSHA 协议时，需要设置授权认证密码。
- **私有协议：**数据封装时所采用的加密协议。可选择 DES、AES 加密协议或不加密。选择了 DES 或 AES 加密协议时需要设置加密密码。

步骤 4 单击“确定”。

----结束

1.1.8.4 设置网管侧 Telnet 参数

当网管与网元之间使用 Telnet 协议进行通信且网元侧 Telnet 参数有变化时，需要同步设置网管侧网元的 Telnet 参数。

前提条件

网管上已添加设备。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 物理资源”。
- 步骤 2** 选中一台或多台设备，单击“设置 Telnet 参数”。
- 步骤 3** 在弹出的“设置 Telnet 参数”窗口中，设置 Telnet 相关参数。
- 步骤 4** 单击“确定”。

----结束

1.1.9 备份设备配置文件

需要对网元的配置文件进行即时备份时，可以使用手工备份网元配置数据的方法，即时执行备份操作。

前提条件

网管与网元通信正常。

已配置并启动 FTP 服务，配置 FTP 操作请参考 [11.2 设置 FTP 参数](#)。

配置网管侧和网元侧的 Telnet 参数为相同值。

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树上选择“设备配置管理 > 配置文件”。
- 步骤 3** 如果选中一个或多个设备，选择“备份 > 备份选中”，备份选中设备的相关信息；如果需要备份全部可以直接单击“备份 > 备份所有”，若设置了搜索条件，只能备份该搜索条件下的所有设备的相关信息。

----结束

操作结果

当设备上正在运行的配置文件与已备份的配置文件相同时，网管默认保留原有的配置文件，丢弃刚备份的配置文件。

当设备上正在运行的配置文件与已备份的配置文件不同，且备份的文件已达到上限时，则网管默认丢弃最早的非基线配置文件。

1.1.10 添加下级网管

可以通过增加下级网管操作，实现上级网管管理下级网管。

前提条件

下级网管运行正常。

具备增加下级网管的权限。

操作步骤

步骤 1 在主菜单中选择“系统 > 下级网管”。

步骤 2 单击“创建”，在弹出的窗口中，设置“网管名称”、“IP 地址”、“端口号”、“备注”。

步骤 3 单击“确定”。

----结束

1.2 基本概念

在使用 eSight 前，需要了解 eSight 各个模块的基本概念，包括资源、拓扑、安全、故障和性能基本概念。理解这些概念可以更快速、更准确地操作 eSight。

1.2.1 安全基本概念

在进行安全管理操作前，需要了解安全管理的基本概念，如用户、角色、操作权限和访问控制。理解这些概念可以更快速地进行安全管理的操作。

安全的基本概念如表 1-9 所示。

表 1-9 安全基本概念

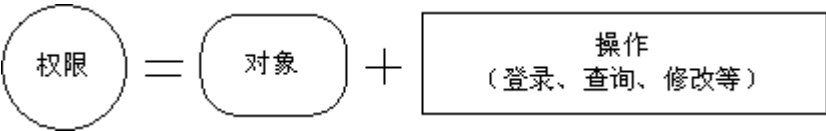
概念	说明
用户	用户及其密码的唯一性确定了相应的操作管理权限。 admin 是 eSight 缺省提供的超级管理员，能管理所有的设备并具有所有的操作权限。
角色	角色是权限的集合，用于对用户进行授权。 角色拥有系统管理、故障管理、性能管理等应用级操作权限。通过角色来管理用户权限可以使权限管理更有条理，避免权限管理的混乱。 Administrators 是 eSight 缺省提供的超级管理员角色，拥有所有管理域的所有操作权限。
管理域	管理域是管理对象的集合。 用户拥有管理域的操作权限才可对在其管理域内的管理对象执行相应操作。
操作权限	操作权限是指用户可以执行某项具体操作的权限。操作权限分配给用户后表示该用户可以执行该具体操作。 操作权限和管理域是相关的，用户只有拥有相应的管理网元权限才能对在其管理域内的网元进行操作。
访问控制	访问权限用于限制用户只能在特定时间或特定 IP 地址登录 eSight。 通过访问控制，在某些情况下即使用户帐号与密码被盗，盗用者也无法使用被盗帐号从访问控制外的其他地址登录到服务器，从而提高了 eSight 的访问安全性。

什么是权限

简单来说，权限就是定义“在什么对象上执行哪些操作”，不同用户在不同对象上的操作可以是不同的。

权限要素包括对象和操作，如图 1-3 所示。

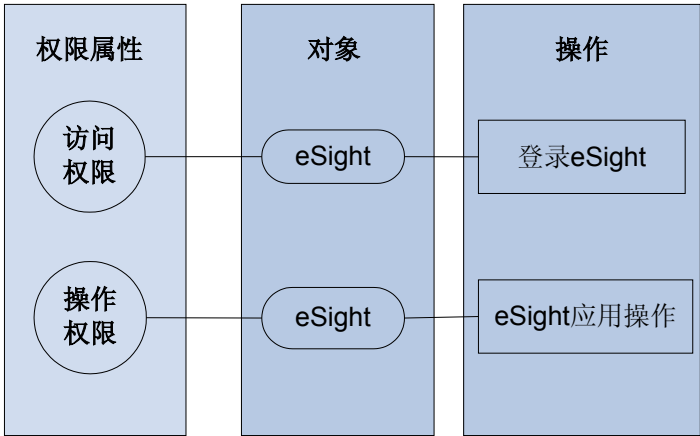
图 1-3 权限要素示意图



eSight 用户必须拥有 eSight 的访问权限和操作权限，才能对 eSight 进行操作。

用户可对 eSight 执行的操作如图 1-4 所示。

图 1-4 eSight 和网元操作权限组成



eSight 用户的权限说明如表 1-10 所示。

表 1-10 权限说明

权限属性	操作	操作说明
访问权限	登录 eSight	用户需拥有合法的用户帐号和密码，才能成功登录 eSight。
操作权限	eSight 应用操作	用户需要拥有相关操作权限，才能在 eSight 客户端中进行相关管理操作，例如查询系统日志、创建拓扑对象等。执行操作前用户需先登录 eSight。

授权原理

授权是将权限分配给用户，定义“谁可以对什么对象进行哪些操作”。

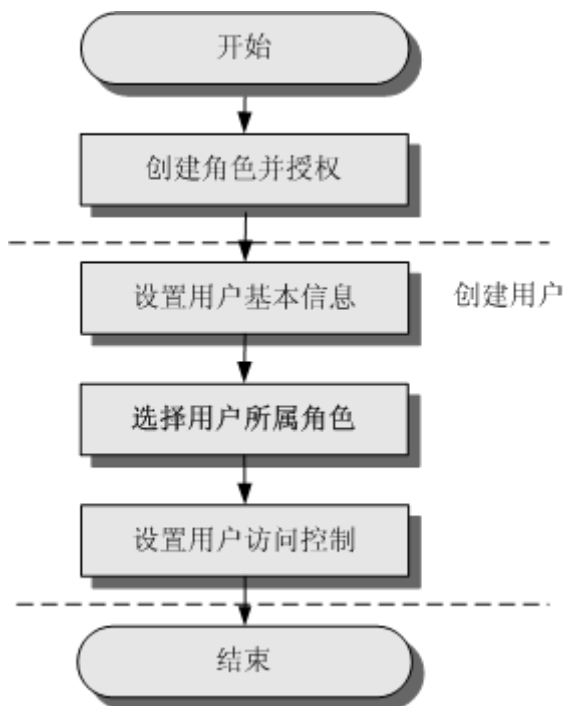
授权就是为用户分配 eSight 操作权限。eSight 是通过将用户加入到角色中来给用户授权的。

将操作、对象分配给角色，使角色拥有某些对象的某些操作的权限。通过将用户加入到角色，使用户具有该角色的权限。eSight 支持“创建用户时选择角色”和“创建角色时选择用户”两种授权方式。

- 创建用户时选择角色

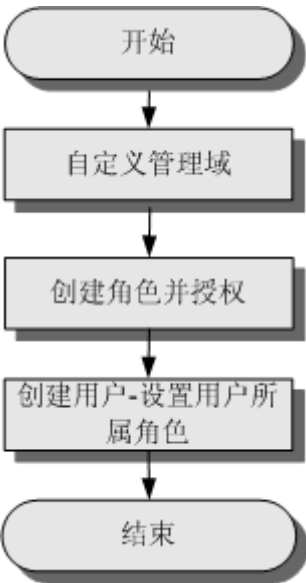
已创建好角色。在创建用户时选择用户所属角色，用户创建成功后将拥有选择角色的权限。“创建用户时选择角色”授权方式的一般授权流程如图 1-5 所示。

图 1-5 一般授权流程



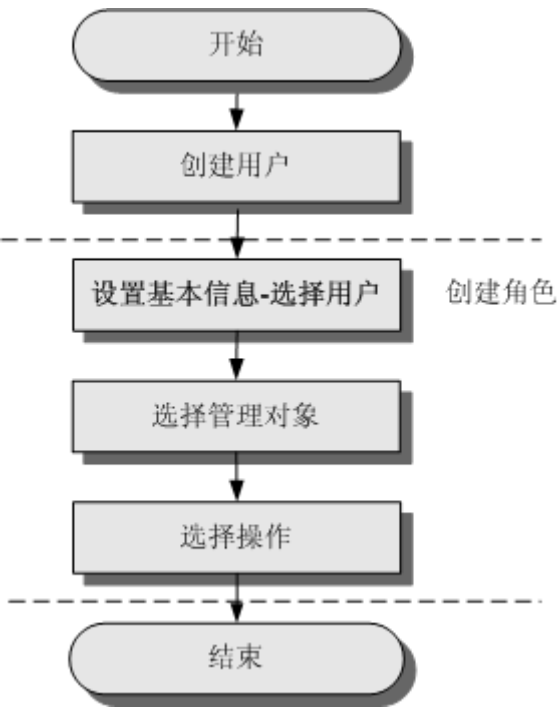
按图 1-5 所示流程授权时，对象和操作需逐一指定给角色。如果对象很多，授权操作会比较繁琐，但如果在授权前规划好管理域，可提高授权效率。当需要通过新建管理域来授权时请参见图 1-6。

图 1-6 完整授权流程



- 创建角色时选择用户
已创建好用户。在创建角色时选择用户，角色创建成功后，选择的用户将拥有该角色的权限。“创建角色时选择用户”授权方式的流程如图 1-7 所示。

图 1-7 创建角色时选择用户



1.2.2 拓扑基本概念

在进行拓扑管理操作时，需要了解拓扑管理的基本概念，如拓扑对象和物理视图等。理解这些概念可以更快速和准确地进行拓扑管理的操作。

拓扑对象

拓扑对象表示网络中的事物，eSight 所管理的每一个元素称为一个对象。一个对象可以是一个子网、一个网元或网元间的链路。拓扑对象的基本概念如表 1-11 所示。

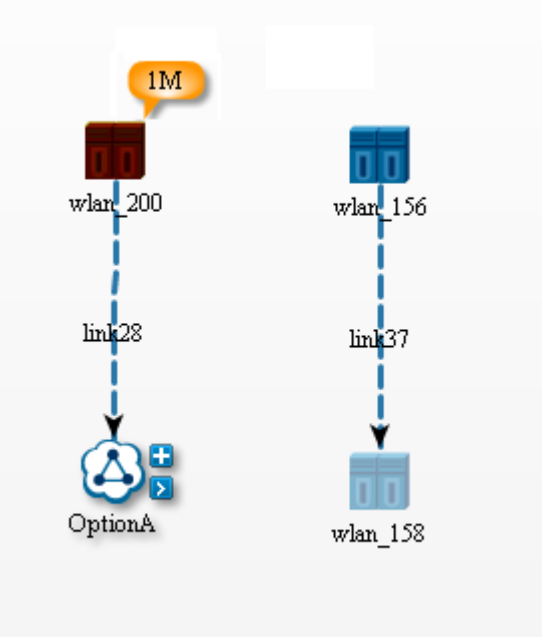
表 1-11 拓扑对象

概念	说明
子网	按照某种原则（如按地域划分），将一个比较大的网络结构分解为几个相对较小的网络结构，以便于网络管理。这种相对较小的网络结构在 eSight 中称为子网。
空子网	子网中不包含任何设备是被称为空子网。
三层视图	三层视图可以展现三层设备、子网及三层设备和子网间 IP 链路的实时信息。 说明 三层视图中子网的划分规则是按照网段划分的，即在同一个网段内的设备将被划分到同一子网中。
二层视图	二层视图是系统根据网桥协议和邻居协议（LLDP、NDP、CDP、STP）构建的拓扑图，展现了子网中各设备之间的二层连接关系、链路状态、设备状态等网络结构和状态信息。
网元	网元用于标识具体的实体设备，分为物理网元和虚拟网元。 ● 物理网元：可以通过 eSight 进行管理的网元，如业务网络中的 SEE、USAU 网元，物理网络中的主机、ATAE 网元、路由器等。
链路	链路是网元之间的连接在拓扑中的映射，eSight 中的链路都为虚拟链路。虚拟链路是指两个网元（包括物理网元和虚拟网元）之间存在逻辑通信，需要用户在 eSight 中手工创建。

物理视图

eSight 的拓扑视图类型包括物理视图。在物理视图中，eSight 使用不同的图标来表示子网、网元、链路以及它们的状态。物理视图如图 1-8 所示。

图 1-8 物理视图



在物理视图中，eSight 使用不同的图标来表示子网、网元、链路等对象。拓扑对象图标说明如表 1-12 所示。

表 1-12 拓扑对象图标

图标	含义
	子网
	网元

在物理视图中，网元的告警状态由不同颜色的告警冒泡图标表示。当物理网元产生告警时，网元上的告警冒泡图标表示发生相应级别的告警。如果一个网元同时产生多个告警，告警冒泡图标将显示为最高级别告警对应的颜色，告警冒泡图标中的数字表示最高级别告警的数量。告警冒泡图标说明如表 1-13 所示。

表 1-13 告警冒泡图标

颜色	含义	说明
	紧急	网元发生紧急告警。
	重要	网元发生重要告警。
	次要	网元发生次要告警。
	提示	网元发生提示告警。

1.2.3 资源基本概念

在进行资源管理操作前，需要了解资源管理的基本概念，如子网、网元等。理解这些概念可以更快速和准确地进行资源管理的操作。

资源的基本概念如表 1-14 所示。

表 1-14 资源基本概念

概念	说明
子网	按照某种原则（如按地域划分）将一个比较大的网络结构分解为几个相对较小的网络结构，使网络便于管理。在 eSight 中，把这种相对较小的网络结构称为子网。
网元	一台实际存在的物理设备，具有 IP 地址、登录端口号、用户名、密码等基本信息。

1.2.4 故障基本概念

在进行故障管理操作前，需要了解故障管理的基本概念，如告警级别、告警状态。理解这些概念可以更快速和准确地进行故障管理的操作。

告警级别

根据影响业务的严重性，告警级别分为紧急、重要、次要和提示，如表 1-15 所示。根据不同的告警级别可以采取对应的处理策略。

表 1-15 告警级别

告警级别	说明
紧急	已经影响业务，需要立即采取纠正措施的告警。
重要	已经影响业务，如果不及时处理会产生较为严重后果的告警。
次要	目前对业务没有影响，但需要采取纠正措施，以防止产生严重故障的告警。
提示	检测到潜在的或即将发生的影响业务的故障，但是目前对业务还没有影响的告警。

告警状态

告警状态包括告警的确认状态和清除状态。针对不同状态的告警可以采取相应的处理措施。

- 告警状态分类
根据告警是否被确认以及清除，告警可分为不同的状态。告警状态的分类如表 1-16 所示。

表 1-16 告警状态分类

告警类别	告警状态
当前告警	未确认未清除
	已确认未清除
	未确认已清除
历史告警	已确认已清除

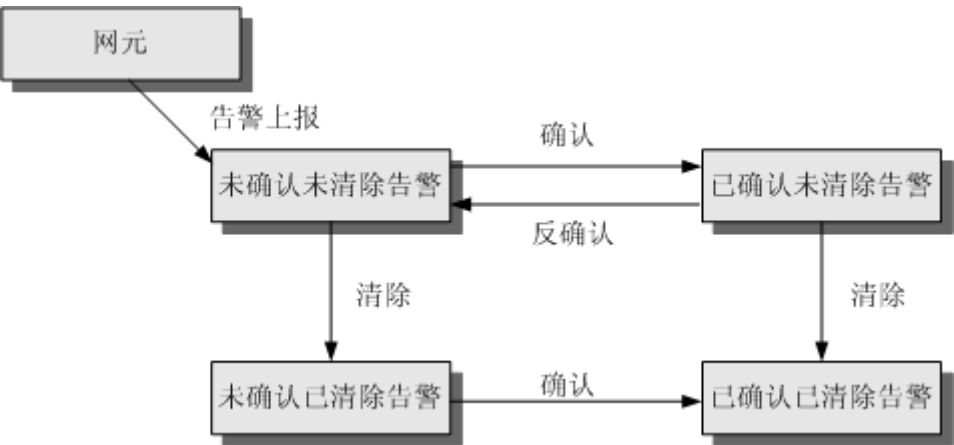
- 告警状态转换
告警状态转换分类的说明如表 1-17 所示。

表 1-17 告警状态转换分类

告警状态转换类别	说明
清除状态转换	当告警产生的条件消除，网元恢复正常，此时网元将上报对应的清除告警，告警由未清除状态变成清除状态。
确认状态转换	对告警进行确认表示告警即将或已经被处理。告警被确认后，由未确认状态变成已确认状态。 如果要重新关注已确认的告警，可以对该告警进行反确认操作。告警被反确认后，由已确认状态变成未确认状态。

告警状态转换关系模型如图 1-9 所示。

图 1-9 告警状态转换关系模型



故障、告警和事件

- 故障和告警

告警是系统检测到故障而产生的通知。并不是系统中所有故障都会产生告警，只有系统能够检测到的故障才会产生告警，对于不能检测到的故障，不会产生告警，但是该故障依然存在。

- 告警和事件的相同点
在 eSight 中，告警和事件都是指 eSight 检测到被管理的对象发生变化后，通过告警或事件的方式呈现出来。
- 告警和事件的区别
告警是指 eSight 检测到故障而产生的通知。
事件是指被管对象除故障外发生变化的统称。
两者的区别在于：
 - 告警是事件的特例。用户必须处理发生的告警，否则会导致由于 eSight 或网元异常而引起业务的异常。
 - 事件的发生只是告诉用户被管对象发生了变化，但是不一定会引起业务的异常。

1.2.5 性能基本概念

在进行性能管理操作前，需要了解性能管理的基本概念，如性能指标、指标阈值。理解这些概念可以更快速地进行性能管理的操作。

性能的基本概念如表 1-18 所示。

表 1-18 性能基本概念

概念	说明
性能指标	测量指标用来监视资源的性能，如 CPU、内存是资源，CPU 占用率、内存占用率是测量指标。通过监视网元测量指标可以提前发现业务处理质量劣化的趋势，并在故障发生前解决这些隐患。
指标阈值	指标阈值用来配置是否上报告警以及上报的告警级别。 当某一测量指标测量值超出设置的阈值时，测量对象就会产生一个 Qos 告警，说明性能劣化趋势已经达到需要用户关注并处理的程度。而当测量值降低到指标阈值允许的范围内时，产生的 Qos 告警会被清除。 合理设置指标阈值能保证业务正常运行。正常情况下，设置指标阈值时需要预留一定的余量，以保证可以提前发现问题。
测量对象	测量对象用来指定测量指标对应的物理或者逻辑资源，当管理对象的某项资源存在多个时（如一个设备中会存在多个 CPU），需要为该资源的测量指标指定具体的资源。
采集周期	采集周期用来配置采集数据间隔时间，如采集周期为 1min，eSight 每隔 1min 对测量对象的测量指标进行一次数据采集。

1.2.6 报表基本概念

报表系统提供了基于设计文件的报表开发和基于 Web 的报表生成、转发、管理等一整套灵活、方便的报表应用服务。通过强大的报表系统来支持对网络性能、存量、告警的

监控、分析、优化和决策。报表系统不仅支持手工报表和周期报表，还拥有完善的报表 Email 转发机制，具有强大的数据采集功能和呈现能力。

手工报表和周期报表

报表系统提供手工报表管理功能，并且能生成周期报表。

- 手工报表
报表系统提供手工报表管理功能，可以直接手工导出 excel、word、pdf 或 ppt 格式的手工报表。
- 周期报表
周期任务可以周期运行，手工导出 excel、word、pdf 或 ppt 格式的周期报表，周期任务有以下几种类型：日报、周报、月报、季报、半年报、年报。

报表转发机制

发送报表到外部 Email 邮箱，报表转发机制方便易用。

报表存储和管理功能

报表系统提供报表存储管理功能，可以进行如下操作：

- 将报表保存到报表存储区中。
- 周期报表保存到报表存储区的报表文件夹中，手工报表不保存。
- 设置存储区的空间大小。
- 在报表系统中打印报表存储区的报表。

1.2.7 网元管理基本概念

介绍网元管理器的基本概念。

功能特性	说明
面板管理	支持单板、端口状态的联动显示。
告警	支持对查看网元的告警列表，并对其告警进行锁定、解锁、确认、反确认、清除、屏蔽、拓扑定位、导出、查看告警详细信息、查看告警日志信息操作。
性能	支持将网元的关键性能以图表的方式进行展示。
接口管理	支持查看接口的基本信息。
IP 地址管理	支持对网元的 IP 地址及网元上各接口 IP 地址进行管理。
配置文件管理	支持对设备的配置文件进行查看、比较、恢复操作。

功能特性	说明
协议参数管理	支持对网管侧网元的 SNMP 协议参数及 Telnet 参数进行配置，实现网管和网元的通信正常。

1.2.8 业务管理基本概念

1.2.8.1 IPSec VPN 管理基本概念

在使用网管配置和管理 IPSec VPN 业务之前，需要掌握 IPSec VPN 业务的基本概念，保证相关操作顺利完成。

数据流（Data Flow）

为一组具有某些共同特征的数据的集合，由源地址/掩码、目的地址/掩码、IP 报文中封装上层协议的协议号、源端口号、目的端口号等来规定。

通常，一个数据流采用一个访问控制列表（access-list）来定义，经访问控制列表匹配的所有报文在逻辑上作为一个数据流。一个数据流可以是两台主机之间单一的 TCP 连接，也可以是两个子网之间所有的数据流量。

IPSec VPN 能够对不同的数据流施加不同的安全保护，例如对不同的数据流使用不同的安全协议、算法或密钥。

安全联盟（Security Association，简称 SA）

使用 IPSec VPN 保护数据流，必须先建立一个安全联盟（SA），SA 可以通过手工创建或自动协商方式建立。

IKE 用于自动协商创建 SA。IPSec VPN 安全联盟是要建立 IPSec VPN 隧道的通信双方对隧道参数的约定，包括隧道两端的 IP 地址、隧道采用的验证方式、验证算法、验证密钥、加密算法、加密密钥、共享密钥以及密钥的生存周期等一系列参数。

为了建立 IPSec VPN 隧道，通信双方需要协商隧道参数，即建立安全联盟。安全联盟是单向的，通信双方间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

安全联盟的协商方式

IPSec VPN 安全联盟的协商方式有以下两种：

- ISAKMP 协商方式

IKE 自动协商（ISAKMP）方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 ISAKMP 自动协商来创建和维护安全联盟。

 说明

ISAKMP 定义了协商、建立、修改和删除 SA 的过程和包格式。IKE 使用 ISAKMP 协议定义密钥交换，为 Internet 上需要加密和认证的通信协议提供算法和密钥协商服务。

- 手工方式

手工配置协商建立安全联盟的优点是可以不依赖 ISAKMP 而单独实现 IPSec VPN 功能，缺点是创建安全联盟所需的全部信息都必须手工配置，配置比较复杂，并且不支持密钥定时更新等高级特性。

当进行通信的对端设备数量较少时，或是在小型静态环境中，手工配置安全联盟是可行的。在中型和大型的动态网络环境中，推荐使用 IKE 自动协商方式建立安全联盟。

IPSec VPN 数据保护方式

IPSec VPN 通过 IP 认证头协议（AH）和 IP 封装安全载荷协议（ESP）两个安全协议为 IP 数据报提供高质量、可互操作、基于密码学的安全性。

AH（Authentication Header）协议提供数据完整性保护，ESP（Encapsulating Security Payload）协议提供数据私有性和完整性保护。

- AH 报文验证方式
 - 数据完整性校验
 - 数据源验证
 - 防报文重放功能
- ESP 保护方式
 - 数据完整性校验
 - 数据加密
 - 数据源验证
 - 防报文重放功能

1.2.9 智能配置工具基本概念

在进行智能配置工具操作前，需要了解智能配置工具的基本概念，如模板、规划表、校验。理解这些概念可以更快速和准确地进行智能配置工具的操作。

智能配置工具的相关概念如表 1-19 所示

表 1-19 智能配置工具相关概念

概念	说明
模板	模板为命令的集合，系统预置了基于配置场景的通用模板，用户直接选择模板填入参数即可下发设备。
规划表	规划表为用户利用同一模板对多设备下发多个参数所用的表单，可以将模板导出生成规划表，可对规划表内不同设备配置不同参数，再将规划表导入，工具会根据规划信息自动生成脚本并下发到设备。
校验	在离线的情況下编写命令行模板，自动对用户制作的脚本进行校验，并且以彩色显示校验结果，确保所有的配置符合命令行规范，提高下发设备的成功率。

1.2.10 设备配置文件基本概念

为避免事故或误操作导致的配置文件恢复失败，eSight 支持配置文件的备份。

设备配置文件基本概念如表 1-20 所示。

表 1-20 设备配置文件基本概念

概念	说明
配置文件的备份	为了保证设备配置的安全性，避免设备问题导致配置丢失，且方便设备间配置相互复制，用户需要将设备上的配置文件备份到网管上。 配置文件的备份传输通道仅支持 FTP 方式。
配置文件的恢复	设备的配置文件备份到网管上后，一旦设备出现问题，设备上的配置文件遭到破坏，需要从网管获取该设备的配置文件进行恢复。网管支持批量恢复设备上的配置文件。
配置文件基线化	将指定备份的配置文件保存成基线文件，对设备进行配置文件恢复时，可以将现有的配置文件恢复到基线文件。

1.2.11 自定义设备管理基本概念

eSight 可以对自定义设备完成性能监控管理、配置文件管理、拓扑管理、网元面板管理、告警管理和资源管理。

性能监控

- CPU 利用率（包括单板 CPU）。
- 内存利用率（包括单板内存）。
- 设备响应时间，设备当天不可达比例。
- 基于 RFC1213 标准 MIB(Management Information Base)的指标统计：IP 报文统计，接口报文统计，路由地址丢弃率，TCP 报文统计，UDP 报文统计，SNMP 报文统计，PPP 报文统计。
- 扩展对自定义设备性能的监控，通过定制方式可导入指标，支持基本计算公式（能够对多个 MIB 节点计算得到指标）。

配置文件管理

配置文件备份/恢复，支持脚本实现配置文件的备份/恢复。

拓扑管理

支持对自定义设备的拓扑展示，不同的设备能根据设备的图标进行展示，能够判断设备类型，并根据设备类型提供不同的操作。

网元面板

提供默认图片根据公有 MIB 展示网络设备（打印机、PC 机、服务器等非网络设备不提供仿真面板功能）的面板信息。提供针对自定义设备面板的扩展功能，根据实体的照片

或者仿真图绘制模板，使面板显示的效果更接近真实的设备。支持在面板上显示非华为设备私有 mib 信息，并能够在面板上对接口进行激活/去激活操作、查询告警信息操作。

告警管理

系统默认解析自定义设备的标准告警。对于自定义设备的私有告警，需要用户通过提供的定制工具定制私有告警参数，系统根据私有告警参数解析私有告警。

资源管理

支持对基于标准 MIB 的特性的操作，基于 RFC1213 实现对于接口的基本管理，查询和修改设备基本信息，支持对 IP 地址表（IPv4）、IP 路由表的查询，支持查询实体数据。可以自定义设备厂商基本信息、厂商图标和设备型号等。

2 安全管理

关于本章

安全管理包括对用户权限、eSight 安全策略等的管理。合理设置安全参数，有效避免非法用户对 eSight 的入侵，保证了 eSight 数据的安全性。

2.1 安全操作全景图

通过安全操作全景图可以了解安全管理的所有操作，并根据实际情况，选择操作方式。

2.2 安全策略管理

安全策略是为管理用户而制定的“帐户策略”、“密码策略”和“访问控制策略”等。在初始安装时应进行必要的安全策略规划和配置，以提高 eSight 的访问安全性。

2.3 配置用户并分配权限

eSight 提供根据实际需要创建用户、角色和自定义管理域的功能。在创建用户、设置用户的基本信息并分配权限后，即让用户拥有了对指定管理域的操作权限。

2.4 监控用户

通过监控已登录 eSight 用户的会话、操作，可以了解用户的会话信息和操作信息。为了保证 eSight 的安全，eSight 提供强制退出可能影响 eSight 安全用户的功能，以主动预防用户可能发生的非法会话或非法操作。

2.5 示例：安全管理典型操作

在 eSight 中，某用户只有属于某一特定角色后，才能拥有该角色在其管理域中的所有操作权限。安全管理典型操作介绍如何创建 eSight 用户并分配权限。

2.1 安全操作全景图

通过安全操作全景图可以了解安全管理的所有操作，并根据实际情况，选择操作方式。

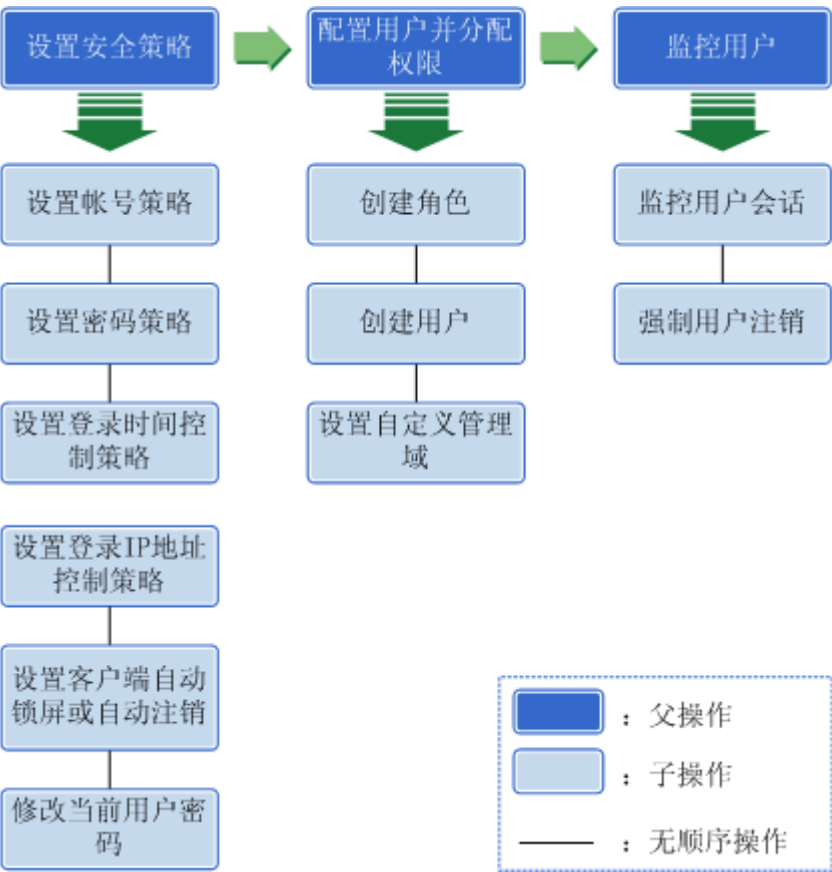
背景信息

在进行安全管理操作前，若需要了解安全管理的基本概念，如用户、角色、操作权限和访问控制等，请参见 [1.2.1 安全基本概念](#)。理解这些概念可以更快速地进行安全管理的操作。

安全操作全景图

安全操作全景图，如 [图 2-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 2-1 安全操作全景图



安全操作的简要说明如[表 2-1](#)所示。

表 2-1 操作简要说明

操作	说明	操作入口
2.2.1 设置帐号策略	合理设置帐号名的长度和与用户登录相关的策略，可提高 eSight 访问安全性。	“系统 > 安全管理 > 安全策略 > 帐号策略”
2.2.2 设置密码策略	合理设置用户密码复杂度、更新周期和字符限制的策略，避免了用户设置过于简单的密码或长时间未修改密码。使用密码策略可提高 eSight 访问安全性。	“系统 > 安全管理 > 安全策略 > 密码策略”
2.2.3.1 设置登录时间控制策略	通过设置登录时间控制策略，限制用户只能在特定的时间段内登录 eSight，以确保 eSight 访问安全性。	“系统 > 安全管理 > 访问控制 > 登录时间控制”
2.2.3.2 设置登录 IP 地址控制策略	通过设置允许访问的 IP 地址区间，限制用户只能从特定 IP 地址区间登录 eSight，以确保 eSight 访问安全性。	“系统 > 安全管理 > 访问控制 > 登录 IP 地址控制”
2.2.4 设置客户端自动注销	为了防止其他人员在用户离开时进行非法操作，eSight 提供设置客户端自动注销的功能。如果在指定时间段内不做任何操作，客户端将被自动注销。	“系统 > 用户设置 > 基本设置 > 闲置操作设置”
2.2.5 修改用户密码	第一次登录需要修改初始密码以确保用户账号的安全性。周期性的修改密码，可提高用户信息的安全性。	“系统 > 用户设置 > 基本设置 > 修改密码”
2.3.4 创建角色	当 eSight 缺省提供的角色不能满足用户授权需求时，为了确保 eSight 的访问安全性和管理条理性，可以根据实际需要创建新的角色。	“系统 > 安全管理 > 权限分配 > 角色”
2.3.5 创建用户	当 eSight 缺省提供的用户已不能满足当前网络管理需求时，可以根据实际需要创建新的用户。	“系统 > 安全管理 > 权限分配 > 用户”
2.3.3 设置自定义管理域	用户可根据实际需要设置自定义管理域。设置自定义管理域之后，为角色分配自定义管理域，角色即可管理指定自定义管理域中的所有对象，从而提高了为角色分配管理对象时的工作效率。	“系统 > 安全管理 > 高级 > 自定义管理域”
2.4.1 监控用户会话	通过监视用户会话，能了解当前登录 eSight 的用户信息。	“系统 > 安全管理 > 安全监控 > 监控用户会话”
2.4.2 强制用户注销	在监控用户操作或会话时，若发现一些危险操作或非法会话，可以强制将产生会话的用户帐号注销。	“系统 > 安全管理 > 安全监控 > 监控用户会话”

2.2 安全策略管理

安全策略是为管理用户而制定的“帐户策略”、“密码策略”和“访问控制策略”等。在初始安装时应进行必要的安全策略规划和配置，以提高 eSight 的访问安全性。

2.2.1 设置帐号策略

合理设置帐号名的长度和与用户登录相关的策略，可提高 eSight 访问安全性。

前提条件

已具备“安全管理”的操作权限。

背景信息

- 帐号策略适用于所有用户。
- eSight 提供默认配置，配置后可根据管理需要适当调整。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“安全策略 > 帐号策略”。

步骤 3 在“帐号策略”页面中，根据需要设置帐号策略。

步骤 4 单击“应用”。

----结束

后续处理

设置帐号策略后，若用户被停用或被锁定，可以进行如下操作。

名称	操作方法
启用用户	1. 选择“权限分配 > 用户”。 2. 单击目标用户所在“操作”列中的  .
解锁用户	● 解锁被锁定时长限制的用户。 超过锁定时长限制时间后，用户可自行解锁。 ● 解锁被永久锁定的用户。 - 选择“权限分配 > 用户”。 - 单击目标用户所在“操作”列中的 .

2.2.2 设置密码策略

合理设置用户密码复杂度、更新周期和字符限制的策略，避免了用户设置过于简单的密码或长时间未修改密码。使用密码策略可提高 eSight 访问安全性。

前提条件

已具备“安全管理”的操作权限。

背景信息

- 密码策略设置后将对 eSight 所有用户立即生效。例如：设置用户密码长度的最小值并生效后，若某个在线用户需修改其密码，密码的最小长度需符合新的密码长度的最小值要求。
- 创建用户时，必须按照密码策略设置密码。
- 新的密码策略对已经设置的密码无影响。
- eSight 提供默认配置，配置后可根据管理需要适当调整。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“安全策略 > 密码策略”。

步骤 3 在“密码策略”页面中，根据需要设置密码策略。

步骤 4 单击“应用”。

----结束

2.2.3 设置访问控制策略

访问控制包括登录时间控制和登录 IP 地址控制。设置访问控制策略，使用户只能在特定时间段、从特定 IP 地址登录 eSight，以确保 eSight 访问安全性。

2.2.3.1 设置登录时间控制策略

通过设置登录时间控制策略，限制用户只能在特定的时间段内登录 eSight，以确保 eSight 访问安全性。

前提条件

已具备“安全管理”的操作权限。

背景信息

- 默认策略不限制登录时间。
- 默认用户 admin 不受任何时间控制策略限制。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“访问控制 > 登录时间控制”。

步骤 3 在“登录时间控制”页面中可以执行如下操作。

设置登录时间控制策略	操作方法
创建登录时间控制策略	当默认策略不能满足管理需要时，可根据实际需要创建登录时间控制策略。 1. 单击“创建”。 2. 在“创建登录时间控制”页面中，设置“登录时间策略名称”、“起止日期”、“每日起止时间”、“星期”和“描述”。 3. 单击“确定”。
查看登录时间控制策略	通过查看登录时间控制策略，可以了解登录时间控制策略的详细信息。 单击“时间策略”列中的目标策略名，在“查看登录时间控制”页面中可查看目标策略的详细信息。
修改登录时间控制策略	当需要适当调整登录时间控制策略时，可修改登录时间控制策略的相关信息。 1. 单击目标策略所在“操作”列中的. 2. 在“修改登录时间控制”页面中，修改“起止日期”、“每日起止时间”、“星期”和“描述”。 3. 单击“确定”。 说明 默认策略不可以修改。
删除登录时间控制策略	当不再使用某登录时间控制策略时，可删除该登录时间控制策略。 1. 单击目标策略所在“操作”列中的. 2. 在“确认”对话框中，单击“是”。 说明 默认策略不可以删除。

---结束

2.2.3.2 设置登录 IP 地址控制策略

通过设置允许访问的 IP 地址区间，限制用户只能从特定 IP 地址区间登录 eSight，以确保 eSight 访问安全性。

前提条件

已具备“安全管理”的操作权限。

背景信息

可以给默认用户 admin 设置登录 IP 地址控制，以限制 admin 只能从特定 IP 地址区间登录 eSight。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“访问控制 > 登录 IP 地址控制”。

步骤 3 在“登录 IP 地址控制”页面中可以执行如下操作。

设置登录 IP 地址控制策略	操作方法
创建登录 IP 地址控制策略	可根据实际需要创建登录 IP 地址控制策略，以限制用户只能从特定 IP 地址登录 eSight。 - 单击“创建”。 - 在“创建登录 IP 地址控制”页面中，设置“起始 IP 地址”、“终止 IP 地址”和“描述”。 - 单击“确定”。
查看登录 IP 地址控制策略	通过查看登录 IP 地址控制策略，可以了解登录 IP 地址控制策略的详细信息。 单击“允许访问的 IP 地址区间”列中的目标 IP 地址区间，在“查看登录 IP 地址控制”页面中可查看目标策略的详细信息。
修改登录 IP 地址控制策略	当需要适当调整登录 IP 地址控制策略时，可修改登录 IP 地址控制策略的相关信息。 - 单击目标策略所在“操作”列中的. - 在“修改登录 IP 地址控制”页面中，修改登录 IP 地址策略参数。 - 单击“确定”。
删除登录 IP 地址控制策略	当不再使用某登录 IP 地址控制策略时，可删除该登录 IP 地址控制策略。 - 单击目标策略所在“操作”列中的. - 在“确认”对话框中，单击“是”。

----结束

2.2.4 设置客户端自动注销

为了防止其他人员在用户离开时进行非法操作，eSight 提供设置客户端自动注销的功能。如果在指定时间段内不做任何操作，客户端将被自动注销。

背景信息

该操作只对当前用户生效。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 用户设置”。
- 步骤 2** 在“用户设置”窗口的导航区中，选择“基本设置 > 闲置操作设置”。
- 步骤 3** 在“闲置操作设置”页面中，选中“闲置时间”前的复选框。
- 步骤 4** 在“闲置时间”后的文本框中输入值或使用微调按钮选择值。
- 步骤 5** 单击“应用”。

----结束

后续处理

客户端被自动注销后，当前用户需重新登录 eSight。

2.2.5 修改用户密码

第一次登录需要修改初始密码以确保用户账号的安全性。周期性的修改密码，可提高用户信息的安全性。

需要修改如下用户密码。

- [修改 eSight 用户密码](#)
- [修改 Windows 操作系统 Administrator 用户密码](#)
- [修改 Linux 操作系统 root 用户密码](#)
- [修改 FTP/FTPS 账户密码](#)
- [修改 SBUS 默认账户密码](#)
- [修改北向 SNMP V3 账户密码](#)

修改 eSight 用户密码

第一次登录 eSight 后，需要修改初始密码以确保 eSight 的安全性。周期性的修改 eSight 用户密码，可提高用户信息的安全性。

背景信息

eSight 缺省提供一个初始用户“admin”，初始密码为“Changeme123”。此用户拥有 eSight 所有管理域的所有操作权限。

操作步骤

- 修改初始密码
当第一次登录 eSight 时，会自动进入修改初始密码的页面。
 1. 在“修改密码”页面中，设置“旧密码”、“新密码”和“确认密码”。
 2. 单击“应用”。
- 周期性修改密码
 1. 在主菜单中选择“系统 > 用户设置”。
 2. 在“用户设置”窗口的导航区中，选择“基本设置 > 修改密码”。
 3. 在“修改密码”页面中，设置“旧密码”、“新密码”和“确认密码”。

4. 单击“应用”。

----结束

修改 Windows 操作系统 Administrator 用户密码

第一次登录 Windows 操作系统的服务器后，建议修改初始密码以确保用户账号的安全性。周期性的修改 Windows 操作系统用户密码，可提高用户信息的安全性。

前提条件

以“Administrator”用户身份登录服务器。

操作步骤

- 步骤 1** 按“Ctrl+Alt+Delete”组合键锁定当前登录用户界面。
- 步骤 2** 单击“更改密码”。
- 步骤 3** 在弹出的对话框中依次输入“Administrator”用户的“旧密码”、“新密码”、“确认新密码”。
- 步骤 4** 单击“确定”。

----结束

修改 Linux 操作系统 root 用户密码

第一次登录 Linux 操作系统的服务器后，建议修改初始密码以确保用户账号的安全性。周期性的修改 Linux 操作系统 root 用户密码，可提高用户信息的安全性。

前提条件

以“root”用户身份登录服务器。

操作步骤

- 步骤 1** 执行如下命令，更改“root”用户密码。
`# passwd`
- 步骤 2** 根据提示输入新密码和确认新密码。

----结束

修改 FTP/FTPS 账户密码

通过使用 BME 加密工具生成密文，复制到配置文件中，以修改 FTP/FTPS 账户密码。

背景信息

- FTP/FTPS 的初始账户为 admin，初始密码为 admin。
- 加密工具的目录为 eSight_ROOT\AppBase\tools\encrypt。



说明

“eSight_ROOT”为 eSight 的安装目录。

- FTP/FTPS 的账户密码存储位置为 eSight_ROOT\AppBase\etc\ftpusers.properties。



“eSight_ROOT”为 eSight 的安装目录。

步骤 1 执行如下命令进入加密工具 encrypt 的目录。

```
cd /d eSight_ROOT\AppData\tools\encrypt
```



“eSight_ROOT”为 eSight 的安装目录。

步骤 2 执行如下命令生成密文。

```
encrypt.bat 0 旧密码
```

步骤 3 将生成的密码替换口令存储位置中的密码。



打开配置文件 eSight_ROOT\AppData\etc\ftpusers.properties，将生成的密码替换 ftpusers.properties 文件中的 “admin.password” 的值。

步骤 4 重启 eSight。

----结束

修改 SBUS 默认账户密码

通过使用 BME 加密工具生成密文，复制到配置文件中，以修改 SBUS 账户密码。

背景信息

- SBUS 的初始密码为 admin。
- 加密工具的目录为 eSight_ROOT\AppData\tools\encrypt。



“eSight_ROOT”为 eSight 的安装目录。

- SBUS 的账户密码存储位置为 eSight_ROOT\AppData\etc\oms.xml。



“eSight_ROOT”为 eSight 的安装目录。

操作步骤

步骤 1 执行如下命令进入加密工具 encrypt 的目录。

```
cd /d eSight_ROOT\AppData\tools\encrypt
```



“eSight_ROOT”为 eSight 的安装目录。

步骤 2 执行如下命令生成密文。

```
encrypt.bat 0 密码
```

步骤 3 将生成的密码替换口令存储位置中的密码。



打开配置文件 eSight_ROOT\AppData\etc\oms.xml，将生成的密码替换 oms.xml 文件中的 “name=password” 的值。

步骤 4 重启 eSight。

----结束

修改北向 SNMP V3 账户密码

通过使用 BME 加密工具生成密文，复制到配置文件中，以修改 SNMP V3 账户密码。

背景信息

- 北向 SNMP V3 的初始账户为 nbi，初始密码为 12345678。
- 加密工具的目录为 eSight_ROOT\AppBase\tools\encrypt。



“eSight_ROOT”为 eSight 的安装目录。

- 北向 SNMP V3 的账户密码存储位置为 eSight_ROOT\AppBase\etc\oms.nbi\nbi.xml。



“eSight_ROOT”为 eSight 的安装目录。

- 北向 SNMP V3 的密码包括鉴权密钥和私有密钥。

操作步骤

- 修改鉴权密钥
 1. 执行如下命令进入加密工具 encrypt 的目录。

```
cd /d eSight_ROOT\AppBase\tools\encrypt
```

2. 执行如下命令生成密文。

```
encrypt.bat 0 密码
```

3. 将生成的密码替换口令存储位置中的密码。



打开配置文件 eSight_ROOT\AppBase\etc\oms.nbi\nbi.xml，将生成的密码替换 nbi.xml 文件中的“V3AuthPwd”的值。

4. 重启 eSight。

- 修改私有密钥

1. 执行如下命令进入加密工具 encrypt 的目录。

```
cd /d eSight_ROOT\AppBase\tools\encrypt
```

2. 执行如下命令生成密文。

```
encrypt.bat 0 密码
```

3. 将生成的密码替换口令存储位置中的密码。



打开配置文件 eSight_ROOT\AppBase\etc\oms.nbi\nbi.xml，将生成的密码替换 nbi.xml 文件中的“V3PrivPwd”的值。

4. 重启 eSight。

----结束

2.3 配置用户并分配权限

eSight 提供根据实际需要创建用户、角色和自定义管理域的功能。在创建用户、设置用户的基本信息并分配权限后，即让用户拥有了对指定管理域的操作权限。

2.3.1 操作系统用户及权限

介绍与 eSight 相关的操作系统用户及其权限。

Windows 操作系统用户及权限

与 eSight 相关的 Windows 操作系统用户及权限如表 2-2 所示。

表 2-2 与 eSight 相关的 Windows 操作系统用户

用户	说明
Administrator	Administrator 是操作系统默认用户帐户，即系统管理员，具有操作系统的最高权限。Administrator 用户能够控制所有操作系统资源，创建其他用户和赋予其他用户权限，执行操作系统提供的所有操作功能。eSight 服务器应用程序的安装和卸载，以及 eSight 服务的启动和停止都由 Administrator 用户执行。

Linux 操作系统用户及权限

与 eSight 相关的 Linux 操作系统用户及权限如表 2-3 所示。

表 2-3 与 eSight 相关的 Linux 操作系统用户

用户	说明
root	root 是操作系统默认用户帐户，即系统管理员，具有操作系统的最高权限。root 用户能够控制所有操作系统资源，创建其他用户和赋予其他用户权限，执行操作系统提供的所有操作功能。 eSight 服务器应用程序的安装和卸载是由 root 用户执行。
root	缺省密码为“Changeme123”。使用该用户对 eSight 服务器进行日常操作和维护。

2.3.2 eSight 用户及权限

介绍 eSight 用户及其权限。eSight 用户主要用于 eSight 客户端操作。

eSight 的用户及权限如表 2-4 所示。

表 2-4 eSight 用户及权限

用户	说明
admin	admin 是 eSight 缺省提供的超级用户，初始密码为“Changeme123”。admin 具有所有设备的管理权限和所有 eSight 客户端的操作权限。

2.3.3 设置自定义管理域

用户可根据实际需要设置自定义管理域。设置自定义管理域之后，为角色分配自定义管理域，角色即可管理指定自定义管理域中的所有对象，从而提高了为角色分配管理对象时的工作效率。

前提条件

已具备“安全管理”的操作权限。

背景信息

在创建和维护角色时，可以从管理域列表中选择自定义管理域。

操作步骤

- 步骤 1 在主菜单中选择“系统 > 安全管理”。
- 步骤 2 在“安全管理”窗口的导航区中，选择“高级 > 自定义管理域”。
- 步骤 3 在“自定义管理域”页面中可以执行如下操作。

操作名称	操作方法
创建自定义管理域	可根据实际管理需求创建自定义管理域，便于对管理对象进行管理。 1. 单击“创建”。 2. 在“创建自定义管理域”页面中，设置“管理域名称”、“描述”。 3. 单击“增加”，在“选择管理对象”对话框中选择管理对象。 4. 单击“确定”。
查看自定义管理域	通过查看自定义管理域，可了解自定义管理域的详细信息。 单击“管理域名称”列中的目标管理域名，在“查看自定义管理域”页面中可查看目标管理域的详细信息。

操作名称	操作方法
修改自定义管理域	当需要适当调整自定义管理域时，可修改自定义管理域的相关信息。 1. 单击目标管理域所在“操作”列中的. 2. 在“修改自定义管理域”页面中，修改自定义管理域的相关信息。 3. 单击“确定”。
删除自定义管理域	当不再使用自定义管理域时，可删除自定义管理域。 1. 单击目标管理域所在“操作”列中的. 2. 在“确认”对话框中单击“是”。

----结束

2.3.4 创建角色

当 eSight 缺省提供的角色不能满足用户授权需求时，为了确保 eSight 的访问安全性和管理条理性，可以根据实际需要创建新的角色。

前提条件

已具备“安全管理”的操作权限。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“权限分配 > 角色”。

步骤 3 在“角色”页面中，单击“创建”。

步骤 4 在“创建角色”页面中，设置基本信息。

1. 在“基本信息”中，设置“角色名”、“描述”。

2. **可选:** 选择用户。

- 可在用户列表中选择用户，让指定用户在角色被创建完成后，就立即拥有该角色的管理权限和操作权限。

说明

选择用户的时候，可以在列表中选择用户，也可以输入用户名进行搜索选择用户。在已选择用户列表中可以删除已选用户。

- 也可创建完角色后，在创建用户时，通过分配角色，让用户拥有角色的管理权限和操作权限。

3. 单击“下一步”。

步骤 5 在“创建角色”页面中，选择管理对象，使该角色拥有指定管理域的管理权限。

1. 在“选择管理对象”中，单击“增加”。



- 说明
- 在选择管理对象时，可选择默认管理域中的管理对象，也可选择自定义管理域中的管理对象。如需创建自定义管理域，请参见 [2.3.3 设置自定义管理域](#)。
- 在“选择管理对象”对话框中选择管理对象。
 - 单击“下一步”。

步骤 6 在“创建角色”页面中，选择操作，使该角色拥有指定的操作权限。

- 在“选择操作”中，单击“增加”。
- 在“选择操作”对话框中选择操作权限。
- 单击“下一步”。

步骤 7 在“创建角色”页面中，确认结果。

- 在“结果确认”中，核对角色创建的所有信息。
- 单击“完成”。

---结束

后续处理

创建角色后，在“角色”页面中可以执行如下操作。

维护角色	操作方法
查看角色	通过查看角色，可了解角色的详细信息。 单击“角色名”列中的目标角色名，在“查看角色”页面中可以查看目标角色的详细信息。
修改角色	当需要适当调整角色信息时，可修改角色的相关信息。 - 单击目标角色所在“操作”列中的 - 在“修改角色”页面中可修改“描述”、“用户列表”、“管理对象”、“操作权限”。修改“用户列表”可参见步骤 4，修改“管理对象”可参见步骤 5，修改“操作权限”可参见步骤 6。 说明 角色名不可以修改。 - 单击“确定”。
删除角色	当不再使用某角色时，可删除该角色。 - 单击目标角色所在“操作”列中的 - 在“确认”对话框中单击“是”。

2.3.5 创建用户

当 eSight 缺省提供的用户已不能满足当前网络管理需求时，可以根据实际需要创建新的用户。

前提条件

- 已具备“安全管理”的操作权限。

- 已了解用户帐号策略和密码策略，即帐号和密码的设置要求、合法条件。
帐号策略和密码策略请参见 [2.2.1 设置帐号策略](#)和 [2.2.2 设置密码策略](#)。

背景信息

新用户各项属性除了用户名和密码在新建用户过程中必须设置以外，其他属性可使用缺省值或在新建用户以后设置。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“权限分配 > 用户”。

步骤 3 在“用户”页面中，单击“创建”。

步骤 4 在“创建用户”页面中，设置基本信息。

1. 在“基本信息”步骤中，设置“用户名”、“密码”、“确认密码”和“描述”，并设置“账号使用状态”为“启用”。
2. 单击“下一步”。

步骤 5 在“创建用户”页面中，设置所属角色，使用户拥有角色的管理权限和操作权限。

1. 在“所属角色”步骤中，选中用户所属角色名前的复选框。



说明

单击“角色名”列中的角色名，在“查看角色”对话框中可查看角色的详细信息。

2. 单击“下一步”。

步骤 6 在“创建用户”页面中，设置访问控制，使用户只能在特定时间段、从特定 IP 地址登录 eSight。

1. 在“访问控制”步骤中，选择登录时间控制策略和限制可登录的 IP 地址区间，以限制用户的可登录时间和可登录 IP 地址区间，确保 eSight 的访问安全性。



说明

- 若“时间策略”列表中不存在所需的登录时间控制策略，单击“创建”，可创建所需的登录时间控制策略。如何创建登录时间控制策略请参见 [2.2.3.1 设置登录时间控制策略](#)。
- 若“允许访问的 IP 地址区间”列表中不存在所需的登录 IP 地址控制策略，单击“创建”，可创建所需的登录 IP 地址控制策略。如何创建登录 IP 地址控制策略请参见 [2.2.3.2 设置登录 IP 地址控制策略](#)。

2. 单击“完成”。

----结束

后续处理

创建用户后，在“用户”页面中可以执行如下操作。

维护用户	操作方法
查看用户	通过查看用户，可了解用户的详细信息。 单击“用户名”列中的目标用户名，在“查看用户”页面中可查看目标用户的详细信息。

维护用户	操作方法
修改用户	当需要适当调整用户信息时，可修改用户的相关信息。 - 单击目标用户所在“操作”栏中的，可以修改用户的相关信息。 - 在“修改用户”页面中，修改“基本信息”、“所属角色”、“访问控制”。修改“基本信息”可参见步骤 4，修改“所属角色”可参见步骤 5，修改“访问控制”可参见步骤 6。 - 单击“确定”。
删除用户	当不再使用某用户时，可删除该用户。 - 单击目标用户所在“操作”列中的. - 在“确认”对话框中单击“是”。
重置密码	当用户登录 eSight 时忘记密码，可在重置密码后，让用户使用新密码登录 eSight。 - 单击目标用户所在“操作”列中的. - 在“重置密码”对话框中，根据下方的密码规则设置“新密码”、“确认密码”。 - 单击“确定”。
启用用户	帐号长时间未使用且达到帐号策略设置的帐号连续未使用天数时，帐号会被停用。若需重新使用该用户时，可启用被停用的用户。 单击目标用户所在“操作”列中的，可启用被停用的用户。
停用用户	当暂时不使用某用户时，可停用该用户。 单击目标用户所在“操作”列中的，可以停用用户。

2.4 监控用户

通过监控已登录 eSight 用户的会话、操作，可以了解用户的会话信息和操作信息。为了保证 eSight 的安全，eSight 提供强制退出可能影响 eSight 安全用户的功能，以主动预防用户可能发生的非法会话或非法操作。

2.4.1 监控用户会话

通过监视用户会话，能了解当前登录 eSight 的用户信息。

前提条件

已具备“安全管理”的操作权限。

背景信息

- 会话是客户端和服务端建立的连接。会话在客户端登录时开始，在客户端注销时结束。
- 一个用户帐号可以产生多个会话。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“安全监控 > 监控用户会话”。

步骤 3 在“监控用户会话”页面中，可查看在线的用户会话信息。



说明

单击“刷新”，可更新最新用户会话信息。

----结束

2.4.2 强制用户注销

在监控用户操作或会话时，若发现一些危险操作或非法会话，可以强制将产生会话的用户帐号注销。

前提条件

已具备“安全管理”的操作权限。

背景信息

- 强制注销操作只注销产生对应会话的用户帐号。
- 当前登录用户不能强制自己注销。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在“安全管理”窗口的导航区中，选择“安全监控 > 监控用户会话”。

步骤 3 单击目标用户所在“操作”列中的  强制注销。

步骤 4 在“确认”对话框中单击“是”。

----结束

2.5 示例：安全管理典型操作

在 eSight 中，某用户只有属于某一特定角色后，才能拥有该角色在其管理域中的所有操作权限。安全管理典型操作介绍如何创建 eSight 用户并分配权限。

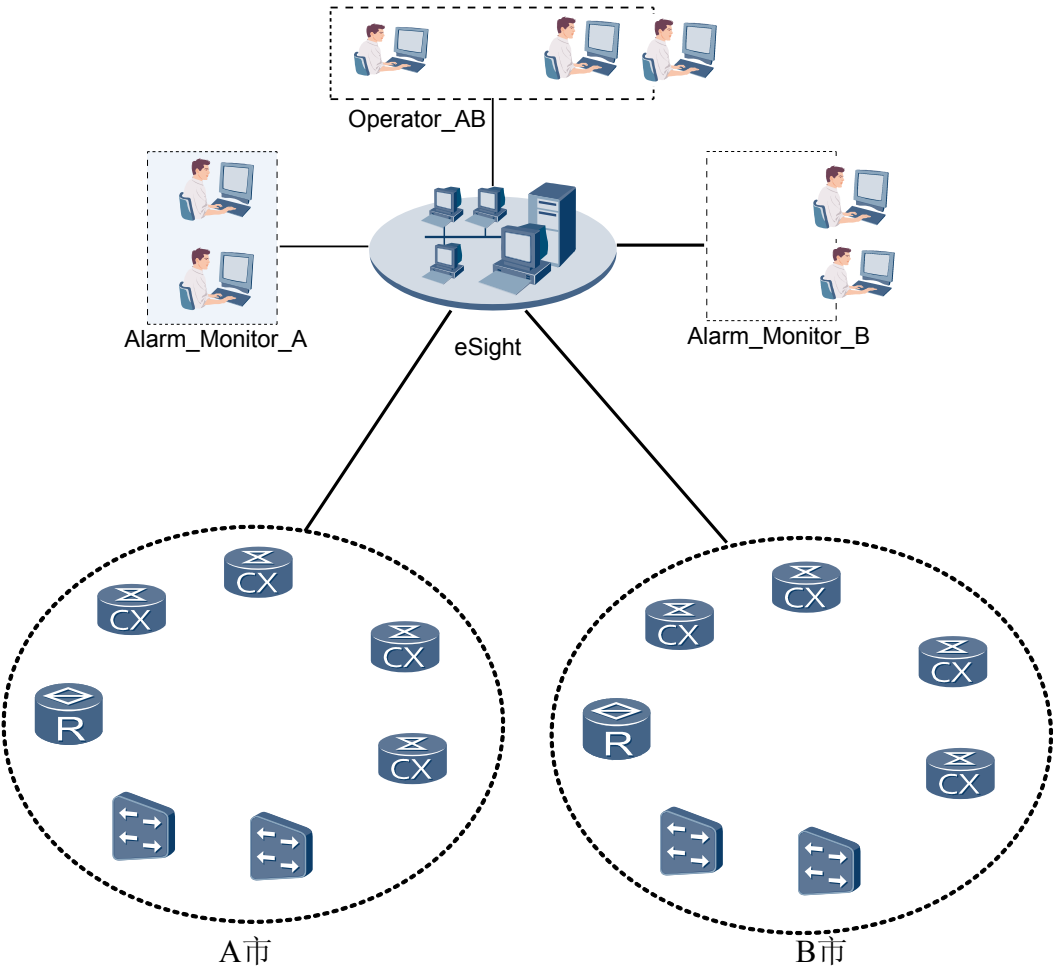
场景介绍

通过 eSight 可集中监控管理某局点的网元。将该局点所管理的网元按照地域划分至 A 市和 B 市两个自定义管理域，分别由不同的人员负责对这些网元进行监控和维护。为了使

不同的人员能够通过 eSight 对网元进行监控和维护，需要为不同人员分配相应的 eSight 用户帐号及权限。

该场景的组网图如图 2-2 所示。

图 2-2 分权分域组网图



数据规划

根据地域划分，规划 A 市和 B 市两个自定义管理域，便于集中监控和维护管理域中的网元。

根据角色职责的划分，规划以下 3 个角色。

表 2-5 角色规划

角色名称	职责说明	管理域	操作权限
Administrators	负责 A 和 B 市网元的操作维护	A 市和 B 市网元	拥有 eSight 超级管理员权限

角色名称	职责说明	管理域	操作权限
A 市告警监视员	负责 A 市网元的告警监控维护	A 市网元	浏览被屏蔽告警 浏览历史告警 浏览事件列表
B 市告警监视员	负责 B 市网元的告警监控维护	B 市网元	浏览被屏蔽告警 浏览历史告警 浏览事件列表

根据用户职责的划分，规划以下 3 个用户。

表 2-6 用户规划

用户名称	职责说明	所属角色
Operator_AB	负责 A 和 B 市网元的维护	Administrators
Alarm_Monitor_A	负责 A 市网元的告警监控	A 市告警监视员
Alarm_Monitor_B	负责 B 市网元的告警监控	B 市告警监视员

配置过程

创建 eSight 用户并分配相应权限的过程如下。

- 分别创建 A 市和 B 市自定义管理域。
 - 在主菜单中选择“系统 > 安全管理”。
 - 在“安全管理”窗口的导航区中，选择“高级 > 自定义管理域”。
 - 在“自定义管理域”页面中单击“创建”。设置“管理域名称”为“A 市”，单击“增加”。
 - 在“选择管理对象”对话框中，选择 A 市所有网元。
 - 单击“确定”。将 A 市的所有网元添加到 A 市自定义管理域中。
 - 参考 1.1 至 1.5，创建 B 市自定义管理域并将 B 市的网元添加到 B 市管理域中。
- 分别创建 A 市告警监视员和 B 市告警监视员角色，并分配角色的管理域和操作权限。
 - 在主菜单中选择“系统 > 安全管理”，在“安全管理”窗口的导航区中，选择“权限分配 > 角色”。
 - 在“角色”页面中单击“创建”，在“基本信息”步骤中设置“角色名”为“A 市告警监视员”，单击“下一步”。
 - 在“选择管理对象”步骤中，单击“增加”，在“选择管理对象”对话框的右侧选择 A 市自定义管理域，单击“确定”。
 - 单击“下一步”。

- e. 单击“增加”，参考表 2-5 给出的操作权限，在“选择操作”对话框中选择相应的操作权限，单击“确定”。
- f. 单击“下一步”。
- g. 单击“完成”，角色 A 市告警监视员创建成功。
- h. 参考 2.1 至 2.7，创建 B 市告警监视员角色。



说明

Administrators 是 eSight 默认的角色，管理域默认是全部网元，默认拥有所有的操作权限，故不需要单独创建。

3. 分别创建用户 Operator_AB、Alarm_Monitor_A 和 Alarm_Monitor_B，设置用户所属的角色，使各用户具有角色的管理域和操作权限。
 - a. 在“安全管理”窗口的导航区中，选择“权限分配 > 用户”。
 - b. 在“用户”页面中单击“创建”，在“基本信息”步骤中设置“用户名”为“Operator_AB”，同时设置该用户的“密码”和“确认密码”。单击“下一步”。
 - c. 在“所属角色”步骤中设置所属角色为“Administrators”，单击“下一步”。
 - d. （可选）为了保证 eSight 的安全，在“访问控制”步骤中，可进行如下设置：
 - 根据人员班次不同的情况设置不同的可登录时间。
 - 根据各区域工作站 IP 地址绑定帐户可登录的 IP 地址。
 - e. 单击“完成”。用户 Operator_AB 创建成功。
 - f. 参考 3.1 至 3.5，分别创建用户 Alarm_Monitor_A、Alarm_Monitor_B，并将其所属角色设置为 A 市告警监视员、B 市告警监视员。

完成以上配置后，就可以将用户帐号提供给相应的人员使用了。

3 资源管理

关于本章

资源管理用于将资源添加到 eSight 并对这些资源进行管理。

3.1 资源操作全景图

通过资源操作全景图可以了解资源管理的所有操作，并根据实际情况，选择操作方式。

3.2 自动发现网元

通过网元自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。当指定网段中的所有网元都需要增加到 eSight 时，该功能可以实现批量操作，节省时间。

3.3 创建子网

按照某种原则（如按地域或按设备类型划分）将一个比较大的网络结构分解为几个相对较小的网络结构，使网络便于管理。在 eSight 中，把这种相对较小的网络结构称为子网。通过创建子网，可以根据用户的自定义逻辑将网元归类管理。

3.4 手工创建单个网元

当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。

3.5 手工批量导入网元

当开局或设备扩容时，被管设备较多，以创建单个网元方式增加网元比较繁琐，可以选择手工批量导入网元方式批量增加网元。

3.6 调整网元所属子网

当网络结构发生变动时，可以根据实际情况，调整网元所属子网，以便正确的体现网元和子网之间的关系。

3.7 调整子网

当网络结构发生变动时，可以根据实际情况，调整子网，以便正确的体现子网和子网之间的关系。

3.8 物理资源管理

物理资源管理提供了对现网中资产统一查询、统计的入口，为现网维护、改造、扩容提供数据依据。

3.9 链路管理

通过链路管理，可以及时查看链路的状态，便于对网络链路进行维护。同时链路在拓扑视图上进行展现，用户可以根据网管链路拓扑了解现网中的网络拓扑结构的变化。

3.10 电子标签管理

电子标签可以应用于客户的网络设计、规划和维护、资产管理（含备件管理）、订单、帐务管理、清算、投资跟踪、保修等业务活动中。eSight 系统支持查看、导出电子标签操作。

3.11 示例：资源管理典型操作

本主题通过资源管理操作的示例，展示了资源管理的流程和方法。通过本示例，可以了解资源管理的基本流程和操作。

3.1 资源操作全景图

通过资源操作全景图可以了解资源管理的所有操作，并根据实际情况，选择操作方式。

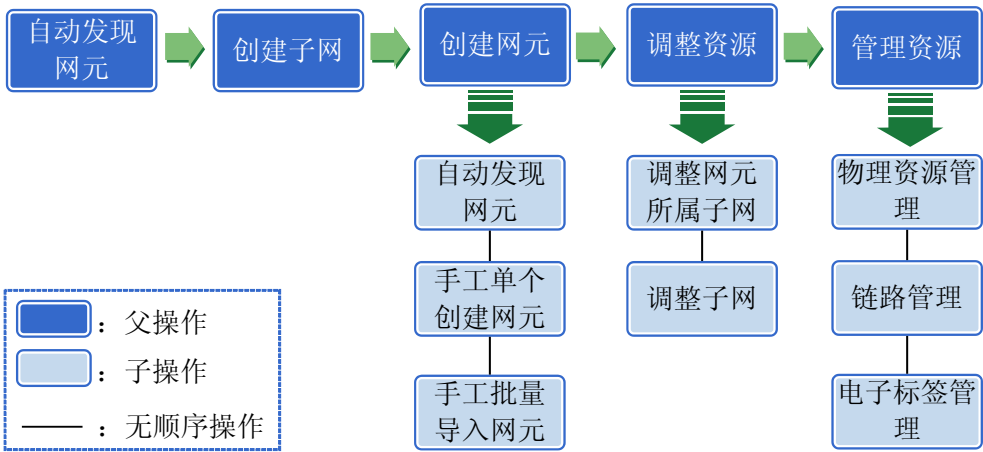
背景信息

在进行资源管理操作前，若需要了解资源管理的基本概念，如子网、网元，请参见 [1.2.3 资源基本概念](#)。理解这些概念可以更快速和准确地进行资源管理的操作。

资源操作全景图

资源操作全景图，如 [图 3-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 3-1 资源操作全景图



资源操作的简要说明如 [表 3-1](#) 所示。

表 3-1 资源操作简要说明

操作	说明	操作入口
3.2 自动发现网元	通过网元自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。当指定网段中的所有网元都需要增加到 eSight 时，该功能可以实现批量操作，节省时间。	“资源 > 资源管理”

操作	说明	操作入口
3.3 创建子网	按照某种原则（如按地域或按设备类型划分）将一个比较大的网络结构分解为几个相对较小的网络结构，使网络便于管理。在 eSight 中，把这种相对较小的网络结构称为子网。通过创建子网，可以根据用户的自定义逻辑将网元归类管理。	“资源 > 资源管理”
3.4 手工创建单个网元	当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。	“资源 > 资源管理”
3.5 手工批量导入网元	当开局或设备扩容时，被管设备较多，以创建单个网元方式增加网元比较繁琐，可以选择手工批量导入网元方式批量增加网元。	“资源 > 资源管理”
3.6 调整网元所属子网	当网络结构发生变动时，可以根据实际情况，调整网元所属子网，以便正确的体现网元和子网之间的关系。	“资源 > 资源管理”
3.7 调整子网	当网络结构发生变动时，可以根据实际情况，调整子网，以便正确的体现子网和子网之间的关系。	“资源 > 资源管理”
物理资源管理	物理资源管理提供了对现网中资产统一查询、统计的入口，为现网维护、改造、扩容提供数据依据。	“资源 > 物理资源”
链路管理	通过链路管理，可以及时查看链路的状态，便于对网络链路进行维护。同时链路在拓扑视图上进行展现，用户可以根据网管链路拓扑了解现网中的网络拓扑结构的变化。	“资源 > 链路管理”
电子标签管理	电子标签可以应用于客户的网络设计、规划和维护、资产管理（含备件管理）、订单、帐务管理、清算、投资跟踪、保修等业务活动中。eSight 系统支持查看、导出电子标签操作。	“资源 > 电子标签”

3.2 自动发现网元

通过网元自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。当指定网段中的所有网元都需要增加到 eSight 时，该功能可以实现批量操作，节省时间。

前提条件

- 已具备“资源接入”的操作权限。
- 网元支持 eSight 指定的 SNMP 协议。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口右侧页面中，单击“自动发现”。

步骤 3 在自动发现页面中，单击“网段发现”。

步骤 4 在“网段发现”页面中，设置网段发现参数和 SNMP 协议参数。

为了操作快捷，可以通过单击“选择协议模板”使用已保存的 SNMP 协议模板来设置 SNMP 协议参数。详情请参见[手工创建单个网元](#)页面中的[保存协议模板](#)。

步骤 5 可选：选中“发现的对象自动添加到本网管系统中”。

 说明

- 如果选择了“发现的对象自动添加到本网管系统中”，发现的网元将自动进行添加操作，不需要执行[步骤 7](#)。
- 如果不选择“发现的对象自动添加到本网管系统中”，需要您执行[步骤 7](#)，增加发现的网元。

步骤 6 单击“开始发现”。

发现结果列表中显示自动发现的网元信息以及增加结果。

 说明

发现过程中，可单击“停止发现”，暂停发现操作。

步骤 7 在列表中选择网元，单击“创建”。

如果选择了“发现的对象自动添加到本网管系统中”，此步骤省略。

- 如果网元添加成功，“添加结果”列显示“添加成功”。
- 如果网元添加失败，“添加结果”列显示失败原因。

步骤 8 单击“完成”。

返回“资源管理”窗口，右侧管理对象列表中可查看到添加的网元信息。

----结束

后续处理

通过自动发现网元功能增加网元到 eSight 后，在“资源管理”窗口中可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 - 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 - 在“搜索类型”下拉框中选择搜索类型。 - 在“搜索条件”文本框中输入搜索条件。 - 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在修改网元信息页面修改网元的名称。 - 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 - 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的. ● 批量删除：选择需要删除的网元，单击“批量删除”。 - 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理窗口。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在弹出的网元管理器窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

3.3 创建子网

按照某种原则（如按地域或按设备类型划分）将一个比较大的网络结构分解为几个相对较小的网络结构，使网络便于管理。在 eSight 中，把这种相对较小的网络结构称为子网。通过创建子网，可以根据用户的自定义逻辑将网元归类管理。

前提条件

已具备“资源接入”的操作权限。

背景信息

- 子网下可以嵌套创建子网。
- 创建完子网后，可以通过单击将网元移动到新增子网中。详情请参见 [3.6 调整网元所属子网](#)。
- 子网的层级不能超过 10 层。但是可以通过移动来追加层级。

- 每个子网中的网元数量不能超过 500 个。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”。
- 步骤 2** 在“资源管理”窗口的导航树中，选择新增子网的父对象，在右侧页面中单击“单个创建”。
- 步骤 3** 在“选择类型”页面的“子网与解决方案类”中选择要创建的子网类型。
- 步骤 4** 在“配置参数”页面中设置待创建子网的“子网名”和“描述信息”。
- 步骤 5** 单击“确定”。



说明

单击“应用”，可继续创建同类型子网。

- 如果子网创建成功，在导航树和管理对象列表中可查看到新增的子网。
- 如果子网创建失败，则 eSight 提示子网创建失败的原因。单击“确认”，重新配置参数。

----结束

后续处理

创建子网成功后，在“资源管理”窗口中可以执行如下操作。

维护子网	操作方法
查看子网信息	在 eSight 中可以方便的查看子网信息，包括子网的基本信息和协议信息等。 1. 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 1. 在“搜索类型”下拉框中选择搜索类型。 2. 在“搜索条件”文本框中输入搜索条件。 2. 单击目标子网的名称，eSight 显示此子网的所有信息。
修改子网信息	在 eSight 中可以方便的修改子网的属性，例如子网名称等。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标子网所在“操作”列中的 . 2. 在修改子网信息页面修改子网的配置参数。 3. 单击“确定”。
删除子网	当网络结构调整，不再需要 eSight 管理某些子网，可以删除。 1. 在“资源管理”窗口右侧的管理对象列表中，删除子网。 ● 单个删除：单击目标子网所在“操作”列中的 . ● 批量删除：选择需要删除的子网，单击“批量删除”。 2. 在“确认”对话框中，单击“是”。

3.4 手工创建单个网元

当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。

前提条件

已具备“资源接入”的操作权限。

操作步骤

- 步骤 1 在主菜单中选择“资源 > 资源管理”。
- 步骤 2 在“资源管理”窗口的导航树中，选择新增网元的父对象，在右侧页面单击“单个创建”。
- 步骤 3 在“选择类型”页面的“物理设备类”中，选择待创建网元的类型。
- 步骤 4 在“配置参数”页面中，设置待创建网元的基本信息和 SNMP 协议参数。

 说明

对于需要配置 SNMP 协议参数的网元，可配置完 SNMP 协议参数后单击“保存协议模板”，作为 SNMP 协议参数的配置模板。当再次需要配置 SNMP 协议参数时可直接单击“选择协议模板”，应用已保存的协议模板。

- 步骤 5 单击“确定”。
-  说明
- 单击“应用”，可继续创建网元。
- 如果网元创建成功，在管理对象列表中可查看到新增网元。
 - 如果网元创建失败，则会弹出“错误”提示框，说明网元添加失败的原因。单击“确定”，重新配置参数。

----结束

后续处理

通过手工单个创建网元功能增加网元到 eSight 后，在“资源管理”窗口中可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 1. 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 1. 在“搜索类型”下拉框中选择搜索类型。 2. 在“搜索条件”文本框中输入搜索条件。 2. 单击目标网元的网元名称，eSight 显示此网元的所有信息。

维护网元	操作方法
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. 2. 在修改网元信息页面修改网元的名称。 3. 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 1. 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的. ● 批量删除：选择需要删除的网元，单击“批量删除”。 2. 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理窗口。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. 2. 在弹出的网元管理器窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

3.5 手工批量导入网元

当开局或设备扩容时，被管设备较多，以创建单个网元方式增加网元比较繁琐，可以选择手工批量导入网元方式批量增加网元。

前提条件

已具备“资源接入”的操作权限。

背景信息

手工批量导入网元是通过导入 Excel 模板资源文件增加网元。

表 3-2 对 Excel 模板中的各个字段进行了说明。

表 3-2 Excel 模板信息

字段名称	设置说明
IP	例如 10.123.124.115。
名称（可选）	1 - 128 位字符，不能包含#%&+;/<=>? \特殊字符。
协议类型	设置为“SNMP”。
协议版本	需与设备的 SNMP 协议版本一致。取值为“V1”或“V2c”。

字段名称	设置说明
端口	需与设备的 SNMP 协议的端口号一致，如“161”。
读团体字	需与设备的 SNMP 协议的读团体字一致，如“public”。
写团体字	需与设备的 SNMP 协议的写团体字一致，如“private”。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口右侧页面中，单击“批量导入”。

步骤 3 在“选择批量导入类型”页面中，选择“导入主机及网络类设备”。

步骤 4 在“导入主机及网络类设备”中，单击“模板下载”后的  模板.xls，下载 Excel 模板到本地。

步骤 5 打开模板，填入网元信息，保存文件。

步骤 6 在批量导入页面单击“待导入的模版资源文件”后的 ，选择所保存的 Excel 文件。

如果需要导入其他文件，可以单击  清除已选择的文件。

步骤 7 单击 ，上传文件。

“待导入的资源列表”中显示文件中各网元的信息以及校验结果。“结果”列为空白，表示网元校验通过。

步骤 8 在待导入资源列表中选择网元，单击“创建”，

eSight 开始导入网元。

- 如果网元创建成功，“结果”列显示“创建成功”。
- 如果网元创建失败，“结果”列显示失败原因。请根据失败原因提示解决问题，尝试重新导入。如果不能解决，请联系技术支持人员。

----结束

后续处理

通过手工批量导入网元功能增加网元到 eSight 后，在“资源管理”窗口可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 - 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 - 在“搜索类型”下拉框中选择搜索类型。 - 在“搜索条件”文本框中输入搜索条件。 - 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在修改网元信息页面修改网元的名称。 - 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 - 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的. ● 批量删除：选择需要删除的网元，单击“批量删除”。 - 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理页面。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在弹出的网元管理窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

3.6 调整网元所属子网

当网络结构发生变动时，可以根据实际情况，调整网元所属子网，以便正确的体现网元和子网之间的关系。

前提条件

已具备“资源接入”的操作权限。

背景信息

网元不能移入到容器网元，但是可以将网元移出子网。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口的导航树中，选择需要调整的网元，单击。

步骤 3 在“移动树节点”对话框中的“要移动的节点”区域框中，选择需要移动的网元，在“目标容器节点”区域框中选择目标子网。

步骤 4 单击“确定”。

返回“资源管理”窗口，在导航树中可查看到所调整的网元已经在目标子网下。

----结束

3.7 调整子网

当网络结构发生变动时，可以根据实际情况，调整子网，以便正确的体现子网和子网之间的关系。

前提条件

已具备“资源接入”的操作权限。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口的导航树中，选择需要调整的子网，单击。

步骤 3 在“移动树节点”对话框中的“要移动的节点”区域框中，选择需要移动的子网，在“目标容器节点”区域框中选择目标子网。

步骤 4 单击“确定”。

返回“资源管理”窗口，在导航树中可查看到所调整的子网已经在目标子网下。

----结束

3.8 物理资源管理

物理资源管理提供了对现网中资产统一查询、统计的入口，为现网维护、改造、扩容提供数据依据。

资源管理模块管理的对象有：设备、机框、单板、子卡、端口、服务器。各资源支持操作见表 3-3。

表 3-3 资源支持的操作

子域名称	界面入口	支持操作
设备资源	在主菜单中选择“资源>物理资源”。在左侧导航单击“设备资源”。	“导出”：将设备信息导出到文件。 “同步”：将设备侧数据同步到网管上。 “设置 SNMP 参数”：可批量设置网管侧的网元 SNMP 参数。 “设置 Telnet 参数”：设置登录到该设备的 Telnet 参数。 “修改”：单击  修改设备的维保和备注信息。 打开网元管理器：单击设备的“名称”，网管自动打开对于设备的网元管理器。
机框资源	在主菜单中选择“资源>物理资源”。在左侧导航单击“机框资源”。	“导出”：将机框信息导出到文件。 “修改备注”：单击  修改机框的备注信息。
单板资源	在主菜单中选择“资源>物理资源”。在左侧导航单击“单板资源”。	“导出”：将单板信息导出到文件。 “修改备注” 修改备注：单击  修改单板的备注信息。
子卡资源	在主菜单中选择“资源>物理资源”。在左侧导航单击“子卡资源”。	“导出”：将子卡信息导出到文件。 “修改备注”：单击  修改子卡的备注信息。
端口资源	在主菜单中选择“资源>物理资源”。在左侧导航单击“端口资源”。	“导出”：将端口信息导出到文件。 “修改备注”：单击  修改端口的备注信息。

3.9 链路管理

通过链路管理，可以及时查看链路的状态，便于对网络链路进行维护。同时链路在拓扑视图上进行展现，用户可以根据网管链路拓扑了解现网中的网络拓扑结构的变化。

前提条件

已配置网管侧和网元侧的 Telnet 参数。

背景信息

当网元被创建到网管上后，网元之间的链路会自动发现到网管上，并展现在拓扑中。

现网中的链路信息是实时变化的，故在网管上进行链路管理相关操作之前，必须先执行“链路发现”操作，将现网中的链路及时发现到网管上，保持网管和现网中的数据一致。

操作步骤

- 步骤 1 在主菜单中选择“资源 > 链路管理”。
- 步骤 2 可选: 在窗口上方设置过滤参数，单击“搜索”。
- 步骤 3 单击“链路发现”，在左侧的窗口中选择需要发现的链路两端的设备，选中“下发命令”，单击“开始发现”，发现完成后，被发现到网管上的链路会在右侧窗口中显示，单击“确定”。

表 3-4 发现 LLDP 链路命令

命令	说明
snmp-agent community read #{readvalue} mib-view iso-view	增加 MIB 和 ISO 视图中#{readvalue}团体的读权限。
snmp-agent community write #{writevalue} mib-view iso-view	增加 MIB 和 ISO 视图中#{readvalue}团体的写权限。
lldp enable	使能接口的 LLDP 功能，使能了 LLDP 功能的邻居节点间交互 LLDP 报文，从而让本端接口既可以接收到来自相邻节点的状态信息，同时也将本端的状态信息传递到相邻节点，从而获取网管系统拓扑发现所需的所有数据。
snmp-agent packet max-size 12200	Agent 能接收和发送的 SNMP 消息包最大值为 12200 字节。
snmp-agent mib-view included iso-view iso	创建一个视图包含 ISO 对象。

说明

以上下发的命令仅用于 LLDP 链路发现，不影响设备其它功能。

对于 LLDP 链路。

- 若设备上未配置过表 3-4 所示的命令，则需要配置网管侧和设备侧的 Telnet 参数，同时勾选“下发命令”，执行链路发现完毕后，可单击“下发命令结果”查看命令下发执行结果。
- 若设备上已配置表 3-4 所示的命令，则无需勾选“下发命令”，可以直接将链路发现到网管上。

对于 Side by Side 链路，无需勾选“下发命令”，可以直接将链路发现到网管上。

- 步骤 4 可选: 创建用户指定的链路。
1. 单击“创建链路”，创建指定的链路。

2. 分别选择“源网元”、“源端口”、“宿网元”和“宿端口”后，单击“确定”。

- 步骤 5** 将网管中的链路导出到客户端上，以.doc、.xls、.pdf 或.ppt 格式的文件进行保存查看。
- 单击“导出 > 导出选中”，在弹出的窗口中单击“保存”。
 - 单击“导出 > 导出全部”，在弹出的窗口中单击“保存”。
- 结束

后续处理

成功添加链路后，可以执行如下操作。

维护链路	操作方法
修改显示规则	可根据需要设置链路的显示规则。 1. 在“链路管理”窗口中，单击“显示规则”，设置链路的显示规则。 ● 在“名称规则”下设置链路名称的显示字段。 ● 在“Tips 规则”下设置链路 Tips 显示字段。 说明 Tips 规则会在拓扑管理界面中展现，鼠标放在链路上等待一段时间，则链路的 Tips 信息会展现给客户。
删除链路	可根据需要删除链路。 1. 在“链路管理”窗口中，选择待删除的链路，单击“删除”。 2. 在弹出的确认对话框中，单击“是”。 说明 该处删除的是网管上的链路，可以通过链路发现操作，重新将网元上的链路数据上载到网管上。

3.10 电子标签管理

电子标签可以应用于客户的网络设计、规划和维护、资产管理（含备件管理）、订单、帐务管理、清算、投资跟踪、保修等业务活动中。eSight 系统支持查看、导出电子标签操作。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 电子标签”。
- 步骤 2** 单击“获取电子标签”，选择相应的网元，单击“获取”，查询各物理资源的电子标签。
-  **说明**
获取全网电子标签耗时较长，建议在业务较空闲的时候进行操作。
- 步骤 3** 导出电子标签。

- 单击“导出 > 导出选中”，在弹出的窗口中单击“保存”。
- 单击“导出 > 导出全部”，在弹出的窗口中单击“保存”。

----结束

3.11 示例：资源管理典型操作

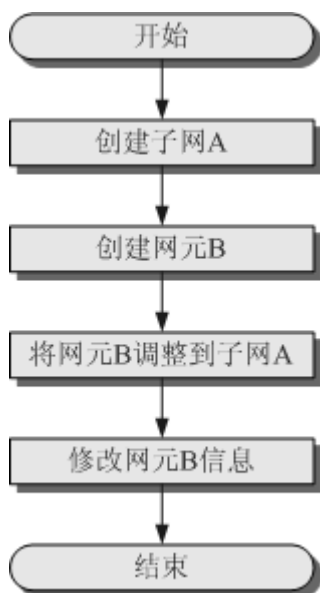
本主题通过资源管理操作的示例，展示了资源管理的流程和方法。通过本示例，可以了解资源管理的基本流程和操作。

背景信息

X 企业由于业务的增加，新增了一套设备，管理员小李需要将设备添加到 eSight 中，通过 eSight 管理这些设备。

小李规划好的操作流程如图 3-2 所示。

图 3-2 操作流程



操作步骤

步骤 1 创建子网 A

1. 在主菜单中选择“资源 > 资源管理”。
2. 在“资源管理”窗口的导航树中选择 Root，在右侧管理对象页面中，单击“单个创建”。
3. 在“选择类型”页面中，选择“子网与解决方案类 > 子网”。
4. 在“配置参数”页面中，设置子网 A 的名称和描述信息。
5. 单击“确定”。

步骤 2 创建网元 B

1. 在“资源管理”窗口的导航树中选择 Root，在右侧管理对象页面中，单击“单个创建”。

2. 在“选择类型”页面中，选择“物理设备类 > Snmp 网络设备”。
3. 在“配置参数”页面中，设置网元 B 的基本信息和 SNMP 协议参数。
4. 单击“确定”。

步骤 3 将网元 B 调整到子网 A

1. 在“资源管理”窗口的导航区中，单击 。
2. 在“移动树节点”对话框中的“要移动的节点”区域框中选择网元 B，在“目标容器节点”区域框中选择子网 A。
3. 单击“确定”。

步骤 4 修改网元 B 信息

1. 在“资源管理”窗口的导航树中选择子网 A。
2. 在右侧管理对象页面中，单击网元 B 所在“操作”列中的 .
3. 修改网元 B 的名称。
4. 单击“确定”。

----结束

4 拓扑管理

关于本章

拓扑管理用于构造并管理整个网络的拓扑结构，以反映设备的组网情况和运行状态。通过物理视图中网元图标所显示的颜色及状态，可以实时监控整个网络的运行情况。

4.1 拓扑操作全景图

通过拓扑操作全景图可以了解拓扑管理的所有操作，并根据实际情况，选择操作方式。

4.2 物理拓扑管理

4.3 IP 拓扑管理

IP 拓扑是以 IP 层协议的角度，对网络系统所管理的网络进行分析和计算所形成的视图(拓扑图)。在 IP 拓扑中，由于三层设备通过路由接口与子网连接，因此视图可以直观的展现出网络中路由和子网的划分情况，同时视图中也能展现二层设备之间的链路关系。

4.1 拓扑操作全景图

通过拓扑操作全景图可以了解拓扑管理的所有操作，并根据实际情况，选择操作方式。

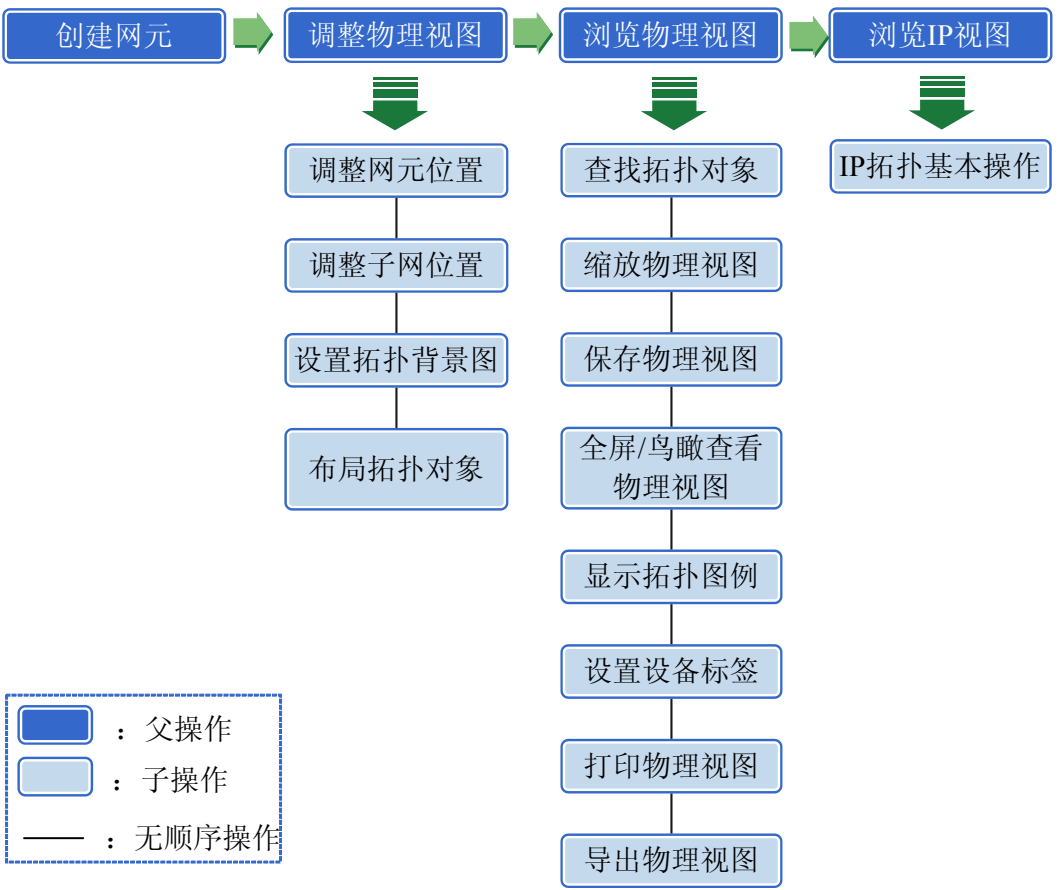
背景信息

在进行拓扑管理操作前，若需要了解拓扑管理的基本概念，请参见 [1.2.2 拓扑基本概念](#)。理解这些概念可以更快速和准确地进行拓扑管理的操作。

拓扑操作全景图

拓扑操作全景图，如 [图 4-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 4-1 拓扑操作全景图



拓扑操作的简要说明如 [表 4-1](#) 所示。

表 4-1 拓扑操作简要说明

操作名称	说明	操作入口
调整网元位置	当网元的物理位置发生变化时，可以调整其在物理视图中的位置，以便正确地体现它与其他拓扑对象的关系。	“资源 > 拓扑管理”
调整子网位置	当子网的物理位置发生变化时，可以调整其在物理视图中的位置，以便正确地体现它与其他拓扑对象的关系。	“资源 > 拓扑管理”
设置拓扑背景图	根据拓扑对象的布局设置合适的背景图，通过背景图和拓扑对象位置的恰当设置，可以直观地了解拓扑对象所在的位置。	“资源 > 拓扑管理”
布局拓扑对象	当物理视图中的子网或者网元的展示混乱时，可以通过拓扑布局功能对拓扑对象进行重新布局，以便清晰的了解拓扑对象之间的关系。	“资源 > 拓扑管理”
查找拓扑对象	利用查找的方式快速定位到所关注的网元、链路、子网等拓扑对象。	“资源 > 拓扑管理”
缩放物理视图	物理视图可以根据需要，放大、缩小、还原显示、适合屏幕显示或全屏显示。	“资源 > 拓扑管理”
保存物理视图	当物理视图中拓扑对象位置发生改变后，可以对改变后的物理视图进行保存。	“资源 > 拓扑管理”
全屏/鸟瞰查看物理视图	eSight 支持通过鸟瞰图查看物理视图，浏览物理视图的全貌，并定位拓扑窗口所显示的区域，也可以全屏显示查看物理视图。	“资源 > 拓扑管理”
显示拓扑图例	通过显示拓扑图例，可以了解拓扑视图中拓扑对象的告警状态和运行状态等。	1. “资源 > 拓扑管理” 2. 在“拓扑管理”窗口的拓扑工具栏中，选择“  > 显示图例”
设置设备标签	通过设置设备标签，在设备图标下显示设备的名称和 IP 地址等，以便直观的了解设备基本信息。	1. “资源 > 拓扑管理”。 2. 在“拓扑管理”窗口的拓扑工具栏中，选择“  设置设备标签”
打印物理视图	打印物理视图功能可以将物理视图打印到纸件或文件中。	“资源 > 拓扑管理”

操作名称	说明	操作入口
导出物理视图	导出物理视图功能，可以将物理视图导出到本地。	“资源 > 拓扑管理”
IP 拓扑基本操作	在日常维护中，通过 IP 拓扑管理可查看二层视图、三层视图，进而了解二层/三层设备、LLDP 链路、IP 链路和各子网实时信息。	“资源 > IP 拓扑管理”

4.2 物理拓扑管理

4.2.1 设计物理视图

在物理视图中部署网元之前，应该设计好物理视图。物理视图在反映实际通信网络拓扑结构的同时，应尽可能方便操作人员的日常操作。

按实际组网，eSight 提供了以下几种划分物理视图的方式，以满足不同的管理需求：

- 按地域划分：根据网元所在的区域划分。
- 按网元类型划分：根据网元的类型划分。
- 按 IP 地址划分：根据网元的 IP 地址所在网段划分。
- 按管理的责任人划分：根据网元的责任人划分。

4.2.2 调整物理视图

在构建物理视图后，可以根据实际情况调整物理视图。调整物理视图包括调整拓扑对象和设置拓扑背景图等。

4.2.2.1 调整网元位置

当网元的物理位置发生变化时，可以调整其在物理视图中的位置，以便正确地体现它与其他拓扑对象的关系。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

如果不具备“拓扑编辑”的操作权限，只能在本地调整网元在物理视图中的位置，不能保存。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的物理视图中，调整网元位置。

- 单个移动网元：在物理视图中单击需要调整的单个网元，将网元拖动至指定位置。
- 批量移动网元：按住“Ctrl”，在物理视图中选择需要调整的多个网元，将网元拖动至指定位置。

步骤 3 在拓扑工具栏中单击 ，保存调整后的网元位置。

----结束

4.2.2.2 调整子网位置

当子网的物理位置发生变化时，可以调整其在物理视图中的位置，以便正确地体现它与其他拓扑对象的关系。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

如果不具备“拓扑编辑”的操作权限，只能在本地调整子网在物理视图中的位置，不能保存。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的物理视图中，调整子网位置。

- 单个移动子网：在物理视图中单击需要调整的单个子网，将子网拖动至指定位置。
- 批量移动子网：按住“Ctrl”，在物理视图中选择需要调整的多个子网，将子网拖动至指定位置。

步骤 3 在拓扑工具栏中单击 ，保存调整后的子网位置。

----结束

4.2.2.3 设置拓扑背景图

根据拓扑对象的布局设置合适的背景图，通过背景图和拓扑对象位置的恰当设置，可以直观地了解拓扑对象所在的位置。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

导入拓扑背景图时，eSight 支持的图片文件格式：*.jpg、*.jpeg、*.gif、*.png。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的拓扑工具栏中，单击.

步骤 3 导入图片文件。

1. 在“设置背景图”对话框中，选中“显示背景图”。

2. 单击，导入目标图片文件。

 说明

如果设置的背景图不需要显示在拓扑视图中，请选中“不显示背景图”。

步骤 4 单击“确定”。

拓扑背景图显示为设置后的图片。

----结束

4.2.2.4 布局拓扑对象

当物理视图中的子网或者网元的展示混乱时，可以通过拓扑布局功能对拓扑对象进行重新布局，以便清晰的了解拓扑对象之间的关系。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

- 如果不具备“拓扑编辑”的操作权限，只能在本地布局拓扑对象，不能保存。
- 选择部分拓扑对象，针对选择的拓扑对象进行布局。
- 没有选择任何拓扑对象，则对物理视图中所有的拓扑对象进行布局。
- eSight 提供以下几种布局：
 - 环形：将拓扑对象排列成环形。
 - 对称：将拓扑对象排列成对称。
 - 上下树形：将拓扑对象排列成上下树形。
 - 下上树形：将拓扑对象排列成下上树形。
 - 左右树形：将拓扑对象排列成左右树形。
 - 右左树形：将拓扑对象排列成右左树形。



注意

eSight 提供的如上排序方式按照自己提供的规则进行排序，有可能破坏已有的排序样式，请谨慎使用。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的物理视图中，选择需要布局的拓扑对象，单击拓扑工具栏中的



，选择拓扑对象布局方式。

物理视图中的拓扑对象将按照选定的布局方式进行布局。

步骤 3 单击 ，保存布局后拓扑对象新的位置。

----结束

4.2.3 浏览物理视图

介绍多种浏览物理视图的方式，以便了解物理视图的整体结构信息。

4.2.3.1 查找拓扑对象

利用查找的方式快速定位到所关注的网元、链路、子网等拓扑对象。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在拓扑工具栏中的  前设置搜索条件。

1. 在下拉框中选择搜索条件。
2. 在文本框中输入搜索的值。

步骤 3 单击 。

eSight 根据设置的条件对拓扑对象进行查找，并在“搜索结果”对话框中列出查询到的拓扑对象。

步骤 4 在“搜索结果”对话框中单击关注的拓扑对象的名称，在物理视图和拓扑导航树上快速定位到此对象。

----结束

4.2.3.2 缩放物理视图

物理视图可以根据需要，放大、缩小、还原显示、适合屏幕显示或全屏显示。

前提条件

已具备“拓扑编辑”的操作权限。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口中，可以选择以下方式缩放物理视图。

- 单击拓扑工具栏中的 ，放大物理视图。
- 单击拓扑工具栏中的 ，缩小物理视图。
- 单击拓扑工具栏中的 ，还原显示物理视图。
- 单击拓扑工具栏中的 ，适合屏幕显示物理视图。

- 单击拓扑工具栏中的，全屏显示物理视图。
- 通过鸟瞰图缩放物理视图。详情请参见 [4.2.3.4 全屏/鸟瞰查看拓扑视图](#)。
 - 在鸟瞰图中，向前滚动鼠标滚轮，放大物理视图。
 - 在鸟瞰图中，向后滚动鼠标滚轮，缩小物理视图。

----结束

4.2.3.3 保存物理视图

当物理视图中拓扑对象位置发生改变后，可以对改变后的物理视图进行保存。

前提条件

已具备“拓扑编辑”的操作权限。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 拓扑管理”。
- 步骤 2** 在“拓扑管理”窗口的物理视图中，调整拓扑对象位置。
- 步骤 3** 单击拓扑工具栏中的，保存物理视图。

----结束

4.2.3.4 全屏/鸟瞰查看拓扑视图

eSight 支持通过鸟瞰图查看物理视图，浏览物理视图的全貌，并定位拓扑窗口所显示的区域，也可以全屏显示查看物理视图。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 拓扑管理”。
- 步骤 2** 在“拓扑管理”窗口中，单击拓扑视图右下角的。

eSight 显示鸟瞰图，如下图所示，其中的白色矩形区域为当前视图的可见范围。
- 步骤 3 可选:** 在鸟瞰图中，按住鼠标左键并拖动其中的矩形区域，可更改当前视图的显示区域。
- 步骤 4 可选:** 通过鸟瞰图，缩放拓扑视图。
 - 在鸟瞰图中，向前滚动鼠标滚轮，放大拓扑视图。
 - 在鸟瞰图中，向后滚动鼠标滚轮，缩小拓扑视图。
- 步骤 5** 单击，关闭鸟瞰图。
- 步骤 6** 单击拓扑工具栏中的，全屏显示拓扑视图。

 说明

- 单击  后，eSight 可能改变拓扑对象的大小比例，但不会改变其坐标位置和形状。
- 当拓扑视图全屏显示时，不支持以下功能：
 - 创建虚拟网元
 - 创建虚拟链路
 - 查找拓扑对象
 - 设置拓扑背景图

----结束

4.2.3.5 显示拓扑图例

通过显示拓扑图例，可以了解拓扑视图中拓扑对象的告警状态和运行状态等。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

操作步骤中所涉及的操作界面所处的计算机分辨率大小为 1024*768 像素。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的拓扑工具栏中，选择“ > 显示图例”。

eSight 显示拓扑图例，如下图所示。



----结束

4.2.3.6 设置设备标签

通过设置设备标签，在设备图标下显示设备的名称和 IP 地址等，以便直观的了解设备基本信息。

前提条件

已具备“拓扑编辑”的操作权限。

背景信息

- 操作步骤中所涉及的操作界面所处的计算机分辨率大小为 1024*768 像素。
- 当所选择的设备标签内容未配置时，eSight 缺省显示设备的名称。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的拓扑工具栏中，选择“ > 设备标签”。

步骤 3 在“设置设备标签”对话框中，选择设备标签内容。

步骤 4 单击“确定”。

在设备图标下显示所选择的设备标签内容。

----结束

4.2.3.7 打印物理视图

打印物理视图功能可以将物理视图打印到纸件或文件中。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的拓扑工具栏中，单击.

步骤 3 设置打印参数。

步骤 4 单击“打印”。

----结束

4.2.3.8 导出物理视图

导出物理视图功能，可以将物理视图导出到本地。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口的拓扑工具栏中，单击.

步骤 3 选择物理视图的保存路径和文件格式。

步骤 4 单击“保存”。

----结束

4.2.4 示例：拓扑管理典型操作

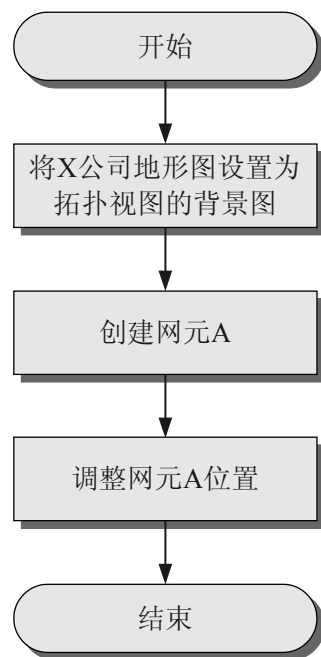
本主题通过拓扑管理操作的示例，展示了构建拓扑视图的流程和方法。通过本示例，可以了解在 eSight 如何构建拓扑视图。

背景信息

X 公司由于业务的增长，新增了一批设备，管理员小王需要将这些设备加入到 eSight 的拓扑视图中，以便通过 eSight 管理这些设备。

小王规划好的操作流程如图 4-2 所示。

图 4-2 操作流程



操作步骤

步骤 1 将 X 公司的地形图设置为拓扑视图的背景图

1. 在主菜单中选择“资源 > 拓扑管理”。
2. 在“拓扑管理”窗口的拓扑工具栏中，单击 .
3. 在“设置背景图”对话框中，选中“显示背景图”，单击 .
4. 选择 X 公司的地形图文件，单击“打开”。
5. 单击“确定”。

步骤 2 创建网元 A

1. 在“资源管理”窗口的导航树中选择 Root，在右侧管理对象页面中，单击“单个创建”。
2. 在“选择类型”页面中，选择“物理设备类 > Snmp 网络设备”。
3. 在“配置参数”页面中，设置网元 A 的基本信息和 SNMP 协议参数。
4. 单击“确定”。

步骤 3 调整网元 A 位置

1. 在拓扑视图中单击网元 A，将网元 A 拖动至指定位置。

2. 在拓扑工具栏中单击, 保存调整后的网元 A 的位置。

----结束

4.3 IP 拓扑管理

IP 拓扑是以 IP 层协议的角度, 对网络系统所管理的网络进行分析和计算所形成的视图(拓扑图)。在 IP 拓扑中, 由于三层设备通过路由接口与子网连接, 因此视图可以直观的展现出网络中路由和子网的划分情况, 同时视图中也能展现二层设备之间的链路关系。

IP 拓扑工具栏中常用菜单的操作请参见 [4.2.2 调整物理视图](#)和 [4.2.3 浏览物理视图](#)。

4.3.1 IP 拓扑管理功能

IP 拓扑由二层和三层视图组成, 二层视图以二层链路作为连接的载体, 展现子网中所有设备及它们之间的物理连接; 三层视图以 IP 链路作为连接的载体, 展现三层设备之间以及三层设备与子网之间的连接关系。在日常维护中, 通过 IP 拓扑管理可查看二层视图、三层视图, 进而了解二层/三层设备、LLDP 链路、IP 链路和各子网实时信息。

IP 拓扑管理的基本功能如[表 4-2](#)所示。

表 4-2 IP 拓扑管理功能

功能		描述
IP 拓扑监控	展现设备、子网和链路告警	● 设备告警: 通过设备的颜色展示该设备上产生的最高级别的告警。 ● 链路告警: 通过链路的颜色识别链路上产生的告警, 链路告警级别由链路两端的端口告警级别决定。 ● 子网告警: 通过子网的颜色展示其告警, 子网告警由子网内设备的最高级别决定。 说明 拓扑中的设备、链路、子网会根据当前最高级别告警实时刷新相关状态。
	展现链路运行状态	● 支持在二层视图上展示 LLDP 链路的运行状态。 ● 支持在三层视图上展示 IP 链路的运行状态。
	查看链路和设备的详细信息	把鼠标放置在设备/链路的图标上, 拓扑视图以标签的形式显示设备/链路的详细信息。
	查看全网当前告警	在 IP 拓扑管理界面的空白处单击右键, 选择“当前告警”。
	查看设备当前告警	在 IP 拓扑管理界面中, 右键单击设备, 选择“告警列表”。

功能		描述
IP 拓扑管理	二层/三层设备自动识别	eSight 根据路由功能的支持情况将设备划分为二层设备和三层设备。如果一个设备支持路由转发且存在两个以上配置了 IP 地址的接口（包括物理接口和逻辑接口），则被识别为三层设备，否则将被识别为二层设备。 说明 网管添加设备后，新增的设备会被及时刷新到 IP 拓扑中。
	显示/隐藏空子网	不包含任何设备的子网为空子网，eSight 可以控制空子网的显示和隐藏。
	IP 变更管理	● IP 变更通知：eSight 会实时监控设备的 IP 变化，当设备的 IP 有变更时，eSight 会以图标形式提示用户。 ● 清除 IP 变更通知：如果此条 IP 变更通知无需关注，可清除 IP 变更通知。 ● IP 变更列表：如果设备上提示 IP 变更通知，可通过查看 IP 变更列表了解变更的详细信息。 ● IP 变更汇总：IP 变更汇总中包含了当前全网所有 IP 变更的详细信息。 ● 清除全网 IP 变更通知：如果当前所有 IP 变更通知都无需关注，可清除全网 IP 变更通知。

4.3.2 IP 拓扑基本操作

在 IP 拓扑上，通过相关操作，可以实现对设备的状态、链路连接情况进行监控。

前提条件

- 网管已添加设备。
- 清除 IP 变更通知操作，需具备“操作员”及以上的网管用户权限。

操作步骤

- 查看三层拓扑视图
 1. 在主菜单中选择“资源 > IP 拓扑管理”。
三层拓扑视图将展现在右边窗口中。
 2. **可选：**查看三层拓扑视图，在快捷图标栏单击对当前拓扑进行排序，三层拓扑图展现三层设备之间以及三层设备与子网之间的连接关系。
 3. **可选：**设置显示/隐藏空子网，在三层拓扑视图的快捷图标栏中，单击显示空子网，单击隐藏空子网。
- 查看二层拓扑视图
 1. 在主菜单中选择“资源 > IP 拓扑管理”。
 2. 有两种方法查看二层拓扑视图：

- 在三层拓扑视图中，双击子网图标，进入二层拓扑视图，查看二层拓扑视图中各设备之间的物理连接。
- 在三层拓扑视图中，单击子网图标后，单击展开二层拓扑视图，查看二层拓扑视图中各设备之间的物理连接。

● IP 变更管理

1. 查看 IP 变更通知。在 IP 拓扑管理界面中，如果设备上方出现，说明该设备上 IP 有变更。
2. 查看设备变更列表。在 IP 拓扑管理界面中，右键单击存在 IP 变更通知的设备，选择“IP 变更列表”。



说明

如果想查看全网 IP 变更情况，可在 IP 拓扑管理界面的空白处单击右键，选择“IP 变更汇总”。

3. 清除 IP 变更通知。在 IP 拓扑管理界面中，右键单击存在 IP 变更通知的设备，选择“清除 IP 变更通知”。



说明

如果想清除全网 IP 变更的通知，可在 IP 拓扑管理界面的空白处单击右键，选择“清除全网 IP 变更通知”。

● 查看设备和链路的详细信息

1. 在主菜单中选择“资源 > IP 拓扑管理”。
2. 将鼠标放在对应的设备或链路上，拓扑上会显示其详细信息。

● 查看告警

- 查看设备告警。在 IP 拓扑管理界面中，右键单击设备，选择“告警列表”。
- 查看全网告警。在 IP 拓扑管理界面的空白处单击右键，选择“当前告警”。

----结束

4.3.3 示例：IP 拓扑管理典型操作

本示例结合配置组网场景给出了详细的操作流程。通过学习本示例，用户可以独立完成 IP 拓扑网络的构建。

前提条件

网管已添加设备。

场景介绍

由于业务增长的需要，某公司 A 现网中新增了一批设备，且这些设备被划分在同一网段（10.137.51.0）内。先需要将这些设备添加到 IP 拓扑中进行管理和查看。

操作流程

操作步骤	操作说明
设备自动识别	网管添加设备后，IP 拓扑会自动识别设备并将设备划分到相应的子网中。

操作步骤	操作说明
查看三层拓扑视图	通过 IP 拓扑，查看三层拓扑视图。
查看二层拓扑视图	通过 IP 拓扑，查看二层拓扑视图。

操作步骤

- 步骤 1 设备自动识别
- 步骤 2 查看三层拓扑视图
 - 在主菜单中选择“资源 > IP 拓扑管理”。
 - 在拓扑图中找到命名为 10.137.51.0 的子网，即为新创建子网。
- 步骤 3 查看二层拓扑视图。在三层拓扑视图中，双击命名为 10.137.51.0 的子网，进入二层拓扑视图，查看二层拓扑视图中各设备之间的物理连接。
- 结束

5 故障管理

关于本章

为了更快的发现、定位并解决网络或设备故障，eSight 提供了监控网络告警、查询告警/事件和设置告警远程通知等管理功能。

5.1 故障操作全景图

通过故障操作全景图可以了解故障管理的所有操作，并根据实际情况，选择操作方式。

5.2 设置告警远程通知

通过设置告警远程通知规则，包括通知条件、通知时间和通知方式，符合条件的告警将被发送给维护人员，便于不在现场的维护人员及时了解到系统服务器上的告警信息从而采取相应措施。

5.3 设置故障监控规则

eSight 提供告警屏蔽、声音、过滤条件监控故障，了解各规则的使用效果有助于用户合理设置故障监控规则。

5.4 监控告警

在 eSight 中，可以通过拓扑视图、告警板和告警柱状图等方式监控网络告警，实时了解网络中的告警状况并采取相应的措施。

5.5 统计分析

通过查询并分析历史告警、事件和被屏蔽告警可以了解网元告警趋势，以便对网元进行升级。

5.6 示例：故障管理典型操作

本主题通过故障管理操作的示例，展示了故障管理的流程和方法。通过本示例，可以更好的了解故障管理的基本流程和操作。

5.1 故障操作全景图

通过故障操作全景图可以了解故障管理的所有操作，并根据实际情况，选择操作方式。

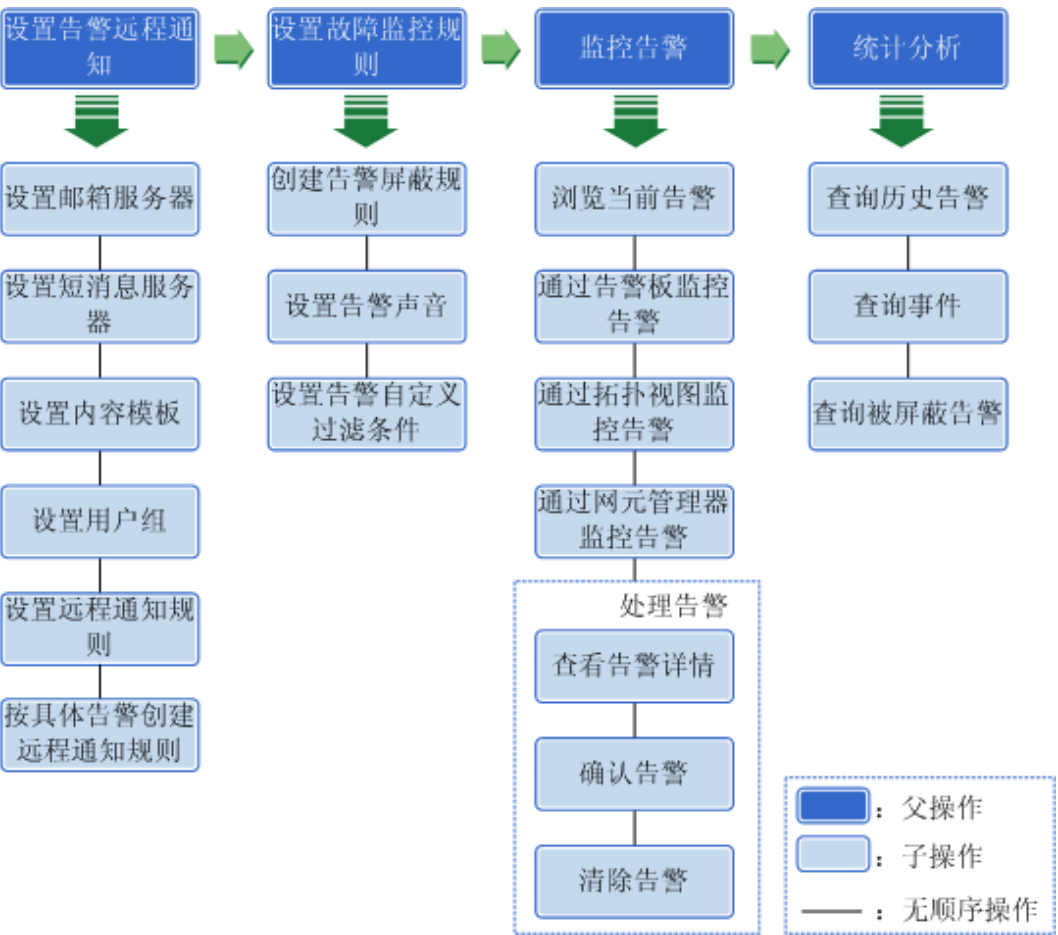
背景信息

在进行故障管理操作时，若需要了解故障管理的基本概念，如告警级别、告警状态等，请参见 [1.2.4 故障基本概念](#)。理解这些概念可以更快速和准确地进行故障管理的操作。

故障操作全景图

故障操作全景图，如 [图 5-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 5-1 故障操作全景图



故障操作的简要说明如[表 5-1](#) 所示。

表 5-1 操作简要说明

操作	说明	操作入口
5.2.2 设置邮箱服务器	设置远程通知设备的邮箱服务器参数，当设备上报告警时，可以通过发送邮件的方式通知远程设备用户。	“故障 > 告警设置 > 远程通知 > 邮箱服务器”
5.2.3 设置短消息服务器	设置远程通知设备的短消息服务器参数，当设备上报告警时，可以通过发送短消息的方式通知远程设备用户。	“故障 > 告警设置 > 远程通知 > 短消息服务器”
5.2.4 设置内容模板	通过定制远程通知告警或事件的信息内容模板，eSight 按该内容模板，将满足远程通知规则的告警或事件以邮件或短消息的方式发送给用户。	“故障 > 告警设置 > 远程通知 > 通知内容模版”
5.2.5 设置用户组	在设置告警远程通知时，需要设置远程通知的用户组。	“故障 > 告警设置 > 远程通知 > 通知用户组”
5.2.6 设置远程通知规则	通过设置告警远程通知规则，eSight 按照该通知规则将符合一定条件的告警，以电子邮件或短消息的方式通知维护人员。	“故障 > 告警设置 > 远程通知 > 远程通知规则”
5.2.7 按具体告警创建远程通知规则	通过选择具体的告警源、告警/事件和通知用户组来创建通知规则。	“故障 > 告警设置 > 远程通知 > 远程通知规则”
5.3.1 创建告警屏蔽规则	对于网元上报的且不需要关注的告警，可以通过在 eSight 中创建屏蔽规则将告警列入到被屏蔽告警列表中。被屏蔽的告警不会显示在当前告警列表中，使用户在当前告警列表中能更迅速地发现自己关注的告警。	“故障 > 告警设置 > 基础设置 > 屏蔽规则”
5.3.2 设置告警声音	可以为不同级别的告警指定告警提示声音。当告警发生时，主机上的音箱会发出对应的声音。	“故障 > 告警设置 > 基础设置 > 告警声音”
5.3.3 设置告警自定义过滤条件	将常用的告警查询过滤条件保存为自定义过滤条件，可以直接使用自定义过滤条件进行查询。	“故障 > 当前告警 > 过滤条件 > 自定义过滤条件”
5.4.1 浏览当前告警	通过在当前告警中设置过滤条件和搜索告警，查看当前需要关注和处理的告警。	“故障 > 当前告警”
5.4.2 通过告警板监控告警	通过告警板可以了解不同级别告警的数目，还可以通过告警板和告警声音了解当前告警状况。	eSight 客户端主界面

操作	说明	操作入口
5.4.3 通过拓扑视图监控告警	通过查看拓扑视图，可以实时监控网元的告警情况。	“资源 > 拓扑管理”
5.4.4 通过网元管理器监控告警	通过在网元管理中查看 eSight 所管理网元的告警信息，可以了解网元当前运行状况，以便及早发现并解决异常。	“资源 > 资源管理”
5.4.5.2 查看告警详情	在 eSight 系统中可以查看当前告警详情、历史告警详情和被屏蔽告警详情。查看告警详情可以获取告警名称、修复建议和定位信息等告警信息。	“故障 > 当前告警”
5.4.5.3 确认告警	标识某条告警已有用户处理，不必过多关注。	“故障 > 当前告警”
5.4.5.4 清除告警	当告警无法自动清除或已确认网元上不存在该告警的时候，可以手工进行清除。告警被清除说明导致告警的故障已被排除。	“故障 > 当前告警”
5.5.1 查询历史告警	通过设置历史告警查询条件，可以快速找到所关注的历史告警。	“故障 > 历史告警”
5.5.2 查询事件	通过查询事件信息，可以查看到设备侧向 eSight 发送的具体事件消息。	“故障 > 事件列表”
5.5.3 查询被屏蔽告警	通过设置被屏蔽告警查询条件，可以快速找到所关注的被屏蔽告警。	“故障 > 被屏蔽告警”

5.2 设置告警远程通知

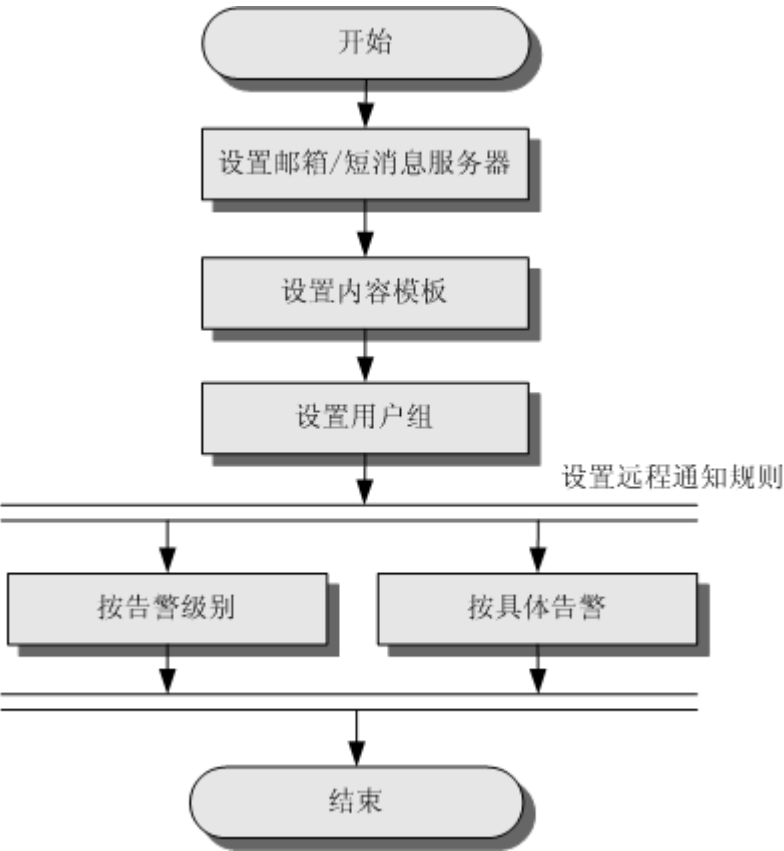
通过设置告警远程通知规则，包括通知条件、通知时间和通知方式，符合条件的告警将被发送给维护人员，便于不在现场的维护人员及时了解到系统服务器上的告警信息从而采取相应措施。

5.2.1 远程通知设置流程

介绍远程通知设置流程，在 eSight 系统中发现告警后，将符合设置的远程通知规则的告警信息发送给维护人员，便于不在现场的维护人员及时了解到系统服务器上的告警信息从而采取相应措施。

远程通知设置流程图

图 5-2 远程通知设置流程



流程说明

表 5-2 远程通知设置流程说明

步骤	操作	说明
1	设置邮箱/短消息服务器	正确设置远程通知设备的邮箱/短消息服务器参数，eSight 将满足远程通知规则的告警或事件信息以邮件或短消息的方式发送给用户。
2	设置内容模板	定制远程通知告警或事件的信息内容模板。eSight 按该内容模板，将满足远程通知规则的告警或事件信息以邮件或短消息的方式发送给用户。
3	设置用户组	设置远程通知用户的用户名、手机号码和邮箱地址。eSight 将满足远程通知规则的告警或事件信息以邮件或短消息的方式发送给指定的用户。

步骤	操作	说明
4	设置远程通知规则	eSight 支持“按告警级别设置”和“按具体告警设置”两种方式新增通知规则。eSight 按照通知规则将符合一定条件的告警，以电子邮件或短消息的方式通知维护人员。

5.2.2 设置邮箱服务器

设置远程通知设备的邮箱服务器参数，当设备上报告警时，可以通过发送邮件的方式通知远程设备用户。

前提条件

- 已具备“告警设置”的操作权限。
- 已获取 SMTP 服务器 IP 地址和发件箱地址。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“远程通知 > 邮箱服务器”。

步骤 3 在“邮箱服务器设置”页面中，设置 SMTP 服务器和发件箱地址。

- “SMTP 服务器”：SMTP（Simple Mail Transfer Protocol）邮件服务器的主机名称或者 IP 地址。

 说明

为了避免因域名解析失败而导致无法与邮件服务器连接，建议直接使用邮件服务器的 IP 地址。SMTP 的缺省端口是 25，请确保邮件服务器上的 SMTP 端口可用。

- “发件箱地址”：发送者的电子邮件地址。
- “需要检查权限”：若 SMTP 服务器需要权限验证，选中“需要检查权限”复选框，设置 SMTP 服务器的用户名和密码。选中需要检查权限后，检查当前用户是否可以发送邮件。

步骤 4 单击“应用”。

 说明

- 单击“测试”，检测与该邮箱服务器是否连通，系统将会弹出连通与否的提示信息。在测试连接服务器时，如果输入的参数有误，系统可能反应较慢，需等待一会。
- 设置邮箱服务器参数后，请单击“应用”保存设置。由于邮箱服务器参数中涉及帐户和密码，为保证安全性，用户没有单击“应用”进行页面切换时，eSight 不会提示保存数据。

----结束

5.2.3 设置短消息服务器

设置远程通知设备的短消息服务器参数，当设备上报告警时，可以通过发送短消息的方式通知远程设备用户。

前提条件

- 已具备“告警设置”的操作权限。
- 已获取短消息服务器的主机名、端口、编码协议和主叫号码信息。

操作步骤

- 步骤 1** 在主菜单中选择“故障 > 告警设置”。
- 步骤 2** 在“告警设置”窗口的导航区中，选择“远程通知 > 短消息服务器”。
- 步骤 3** 在“短消息服务器设置”页面中，设置主机名、端口和短消息通知主叫号码等信息。
- 主机名：短消息中心的主机名或 IP 地址。
 - 端口：短消息中心的端口号，根据实际场景进行设置。
 - 编码协议：短消息中心的编码协议。

如果需要支持长短信和状态回复，单击“高级设置”进行选择。

选择不同协议支持的短信长度不一样。

表 5-3 是否支持长短信

协议类型	是否支持长短信
SMPP3_3/SMPP3_4	● 是 发短信方发送的 1 条短信无论包含多少个字符，收短信方都可以收到 1 条短信。 ● 否 发短信方发送的 1 条短信如果超过 70 个字符，则系统以每 70 个字符分割短信，收短信方收到多条分割的短信。
CMPP2_x/ CMPP3_x	
SGIP	● 是 发短信方发送的 1 条短信无论包含多少个字符，收短信方都可以收到 1 条短信。 ● 否 发短信方发送的 1 条短信如果超过 80 个字符，则系统以每 80 个字符分割短信，收短信方收到多条分割的短信。

- 步骤 4** 单击“应用”。

 说明

- 单击“测试”，检测与该短消息服务器是否连通，系统将会弹出连通与否的提示信息。在测试连接服务器时，如果输入的参数有误，系统可能反应较慢，需等待一会。
- 设置短消息服务器参数后，请单击“应用”保存设置。由于短消息服务器参数中涉及帐户和密码，为保证安全性，用户没有单击“应用”进行页面切换时，eSight 不会提示保存数据。

----结束

5.2.4 设置内容模板

通过定制远程通知告警或事件的信息内容模板，eSight 按该内容模板，将满足远程通知规则的告警或事件以邮件或短消息的方式发送给用户。

前提条件

已具备“告警设置”的操作权限。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“远程通知 > 通知内容模板”。

步骤 3 在“通知内容模板设置”页面中，设置告警内容模板和事件内容模板。

- 设置告警内容模板：

在“告警内容模板”页签的“可选择的告警字段”区域框中，选中需要添加的告警字段，单击 ，将该字段添加到“已选择的告警字段”区域列表中。

在“已选择的告警字段”区域列表中，单击  或 ，调整字段显示的位置。

- 设置事件内容模板：

在“事件内容模板”页签的“可选择的事件字段”区域框中，选中需要添加的事件字段，单击 ，将该字段添加到“已选择的事件字段”区域列表中。

在“已选择的事件字段”区域列表中，单击  或 ，调整字段显示的位置。

在“已选择的告警字段”或“已选择的事件字段”区域中，可以对“字段名”设置前缀信息，在告警或事件发送短信通知用户时，设置的前缀信息会加到通知信息字段名的前面发送给用户。

步骤 4 单击“应用”。

----结束

5.2.5 设置用户组

在设置告警远程通知时，需要设置远程通知的用户组。

前提条件

已具备“告警设置”的操作权限。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“远程通知 > 通知用户组”。

步骤 3 在“通知用户组”页面中可以执行如下操作。

设置用户组	操作方法
新增用户组及组内成员	1. 单击“创建”。 2. 在“创建用户组”页面中设置用户组名、描述和添加组内成员。 添加组内成员： a. 在“创建用户组”页面中单击“创建”。 b. 在“创建成员”对话框中设置用户名、手机号码和邮箱地址。 c. 单击“确定”。 在“创建用户组”页面的成员列表中，通过单击目标成员所在“操作”列的或可以修改或删除成员。 3. 在“创建用户组”页面中单击“保存”。
查看用户组及组内成员	1. 单击目标用户组的“用户组名”。 2. 在“查看用户组”页面中，查看用户组信息和组内成员信息。
修改用户组及组内成员	1. 单击目标用户组所在“操作”列中的. 2. 在“修改用户组”页面中修改用户组名、描述和组内成员。 修改成员，包括对成员进行增、删、改操作。
删除用户组	1. 单击目标用户组所在“操作”列中的. 2. 在“确认”对话框中单击“是”。

----结束

5.2.6 设置远程通知规则

通过设置告警远程通知规则，eSight 按照该通知规则将符合一定条件的告警，以电子邮件或短消息的方式通知维护人员。

前提条件

已具备“告警设置”的操作权限。

背景信息

eSight 支持“按告警级别”和“按具体告警”两种方式来创建通知规则。

- 按告警级别：当指定级别的告警产生或清除时，eSight 向指定的用户组发送远程通知。
- 按具体告警：当指定设备的指定告警产生或清除时，eSight 向指定的用户组发送远程通知。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“远程通知 > 远程通知规则”。

步骤 3 在“远程通知规则”页面中可以执行如下操作。

设置远程通知规则	操作方法
创建远程通知规则	通过创建告警远程通知规则，符合条件的告警将被发送给维护人员，便于不在现场的维护人员及时了解到 eSight 服务器上的告警信息从而采取相应措施。 eSight 提供“按告警级别”和“按具体告警”两种方式创建通知规则。 远程通知规则创建完成后，缺省为启用状态。 ● 按告警级别： 1. 选择“创建 > 按告警级别”。 2. 在“按告警级别创建”窗口中，设置“规则名称”、“告警级别”和“通知用户组”信息。 说明 ● 设置通知用户组，可以单击  增加多个通知用户组。 ● 在“用户组”下拉框中选择通知用户组，可以添加用户组，请参见 5.2.5 设置用户组。 3. 单击“保存”。 ● 按具体告警： 请参见：5.2.7 按具体告警创建远程通知规则
启用远程通知规则	启用被停用的远程通知规则可以继续使用该规则。 选择一条或者多条远程通知规则，单击“启用”，启用远程通知规则。
停用远程通知规则	将暂时不使用的远程通知规则停用，下次需要时再启用。 选择一条或者多条远程通知规则，单击“停用”，停用远程通知规则。
修改远程通知规则	修改远程通知规则以满足最新的管理要求。 1. 单击目标远程通知规则所在“操作”列中的 . 2. 在“按告警级别修改”或“按具体告警修改”页面中，修改远程通知规则信息。
删除远程通知规则	删除冗余的远程通知规则，确保服务器有足够内存，运行畅通。 1. 单击目标远程通知规则所在“操作”列中的 . 2. 在“确认”对话框中单击“是”。

---结束

5.2.7 按具体告警创建远程通知规则

通过选择具体的告警源、告警/事件和通知用户组来创建通知规则。

前提条件

已具备“告警设置”的操作权限。

背景信息

需要知道通知的告警所属子网、告警源和事件等信息。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“远程通知 > 远程通知规则”。

步骤 3 在“远程通知规则”页面中，选择“创建 > 按具体告警”。

步骤 4 选择告警源。

1. 在“按具体告警创建”页面的“告警源选择”步骤中，设置“规则名称”，单击“添加告警源”。
2. 在“添加告警源”对话框的“子网列表”中，选择子网。
 - 选择“Root”节点，在“告警源”中，显示所有的网元。
 - 选择具体子网，在“告警源”中，显示该子网下所有的网元。
 - 在子网中选择具体的网元后，在子网右上方会显示红星号，表示在该子网下选择了告警源。
3. 在“添加告警源”对话框的“告警源”中，选择网元。
 - 单击“全选”或“清空”，将选中或清空选中“告警源”中的所有告警源。
 - 根据需要可以选择多个子网下的多个告警源，已经选择过的告警源将不会出现在“告警源”中。
4. 单击“确定”。
5. 单击“下一步”。

步骤 5 选择告警/事件。

1. 在“按具体告警创建”页面的“告警/事件选择”步骤中，单击“添加告警和事件”。
2. 在“添加告警和事件”对话框的“设备类型”中，选择设备类型。
 - 选择具体设备类型，右侧页面显示该设备类型下的告警/事件。
 - 在选中的设备类型右上方会显示红星号，表示在该设备类型下选择了告警/事件。
3. 在“添加告警和事件”对话框的“告警列表”或“事件列表”中，选择具体的告警/事件。
 - 单击“全选”或“清空”，将选中或清空选中“告警列表”或“事件列表”中的所有告警/事件。
 - 根据需要可以选择多个设备类型下的多个告警/事件，已经选择过的告警/事件将不会出现在列表中。
 - 在“告警列表”中，设置告警级别列出告警，选择需要关注的告警。

- 在“事件列表”中，选择需要关注的事件。
- 4. 单击“确定”。
- 5. 单击“下一步”。

步骤 6 选择通知用户组。

在“按具体告警创建”页面的“通知用户组选择”步骤中，设置接收远程通知的用户组和告警清除时是否发送远程通知。

步骤 7 单击“完成”。

远程通知规则创建完成后，缺省为启用状态。

----结束

5.3 设置故障监控规则

eSight 提供告警屏蔽、声音、过滤条件监控故障，了解各规则的使用效果有助于用户合理设置故障监控规则。

5.3.1 创建告警屏蔽规则

对于网元上报的且不需要关注的告警，可以通过在 eSight 中创建屏蔽规则将告警列入到被屏蔽告警列表中。被屏蔽的告警不会显示在当前告警列表中，使用户在当前告警列表中能更迅速地发现自己关注的告警。

前提条件

已具备“告警设置”的操作权限。

背景信息

“时间”分为“全时段”和“分时段”：

- 全时段：在设置的“日期”内，屏蔽规则在所有时间生效。
- 分时段：在设置的“日期”内，屏蔽规则每日在指定的分时段生效，最多可以设置 5 个分时段。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“基础设置 > 屏蔽规则”。

步骤 3 在“屏蔽规则”页面中，单击“创建”。

步骤 4 设置基本信息。

1. 在“创建告警屏蔽规则”页面的“基本信息”步骤中，设置“规则名称”、“日期”和“时间”。
2. 单击“下一步”。

步骤 5 选择告警源。

1. 在“创建告警屏蔽规则”页面的“告警源选择”步骤中，单击“添加告警源”。

2. 在“添加告警源”对话框的“子网列表”中，选择子网。
 - 选择“Root”节点，在“告警源”中，显示所有的网元。
 - 选择具体子网，在“告警源”中，显示该子网下所有的网元。
 - 在子网中选择具体的网元后，在子网右上方会显示红星号，表示在该子网下选择了网元。
3. 在“添加告警源”对话框的“告警源”中，选择具体的网元。
 - 单击“全选”或“清空”，将选中或清空选中“告警源”中的所有告警源。
 - 根据需要可以选择多个子网下的多个告警源，已经选择过的告警源将不会出现在“告警源”中。
4. 单击“确定”。
5. 单击“下一步”。

步骤6 选择告警。

1. 在“创建告警屏蔽规则”页面的“告警选择”步骤中，单击“添加告警”。
2. 在“添加告警”对话框的“设备类型”中，选择设备类型。
 - 选择具体设备类型，在“设备类型”中，显示该子网下所有设备类型。
 - 在选中的设备类型右上方会显示红色的星号，表示在该设备类型下选择了告警。
3. 在“添加告警”对话框的右侧区域框中，选择具体的告警。
 - 单击“全选”或“清空”，将选中或清空选中所有告警。
 - 根据需要可以选择多个子网下的多个告警，已经选择过的告警将不会出现在子网中。
 - 在右侧区域框中，设置告警级别列出告警，选择需要关注的告警。
4. 单击“确定”。

步骤7 单击“完成”。

告警屏蔽规则创建完成后，缺省为启用状态。

---结束

后续处理

告警屏蔽规则创建后可以对屏蔽规则执行如下操作。

设置告警屏蔽规则	操作方法
启用告警屏蔽规则	启用被停用的屏蔽规则可以继续使用该屏蔽规则。 在“屏蔽规则”页面中选择一条或多条屏蔽规则，单击“启用”。 屏蔽规则的“启用状态”列显示为“已启用”，表示该屏蔽规则已启用，后续上报的告警会按照此规则进行屏蔽。
停用告警屏蔽规则	将暂时不使用的屏蔽规则停用。 在“屏蔽规则”页面中选择一条或多条屏蔽规则，单击“停用”。 屏蔽规则的“启用状态”列显示为“未启用”，表示该屏蔽规则处于停用状态。

设置告警屏蔽规则	操作方法
删除告警屏蔽规则	删除冗余的屏蔽规则，确保服务器有足够内存，运行畅通。 1. 在“屏蔽规则”页面中，单击目标屏蔽规则所在“操作”列中的  。 2. 在“确认”对话框中单击“是”。
修改告警屏蔽规则	修改告警屏蔽规则以满足最新的管理要求。 1. 在“屏蔽规则”页面中，单击目标屏蔽规则所在“操作”列中的  。 2. 在“修改告警屏蔽规则”页面中，修改屏蔽规则的名称、基本信息、告警源和屏蔽的告警。

5.3.2 设置告警声音

可以为不同级别的告警指定告警提示声音。当告警发生时，主机上的音箱会发出对应的声音。

前提条件

已具备“告警设置”的操作权限。

背景信息

- 系统缺省告警声音为“已启用”。
- 系统分别为不同级别的告警声音值缺省设置为：
 - “紧急”：“Critical.mp3”
 - “重要”：“Major.mp3”
 - “次要”：“Minor.mp3”
 - “提示”：“Warning.mp3”

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在“告警设置”窗口的导航区中，选择“基础设置 > 告警声音”。

步骤 3 在“告警声音”页面中可以执行如下操作。

设置告警声音	操作方法
停用告警声音	选中目标告警声音“告警级别”前面的复选框，单击“停用”，停止使用该告警级别的告警声音。
启用告警声音	选中目标告警声音“告警级别”前面的复选框，单击“启用”，启用该告警级别的告警声音。

设置告警声音	操作方法
试听告警声音	单击目标声音所在“试听”列中的  , 试听告警声音。
修改告警声音	单击目标声音所在“操作”列中的  , 在“告警声音设置”页面中, 修改“告警声音”和“播放次数”, 单击“保存”。
恢复默认设置	单击“恢复默认设置”将所有告警声音恢复为初始化设置。

----结束

5.3.3 设置告警自定义过滤条件

将常用的告警查询过滤条件保存为自定义过滤条件, 可以直接使用自定义过滤条件进行查询。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

eSight 缺省提供以下过滤条件:

- 所有告警
- 未确认的紧急告警
- 未确认的重要告警
- 未清除的紧急告警
- 未清除的重要告警
- 最近一天的告警

 说明

系统缺省提供的过滤条件不可以删除和修改。

操作步骤

- 步骤 1** 在主菜单中选择“故障 > 当前告警”。
- 步骤 2** 在“当前告警”窗口工具栏上的“过滤条件”下拉框中, 选择“自定义过滤条件”。
- 步骤 3** 在“设置告警过滤条件”对话框中可以执行如下操作。

设置告警自定义过滤条件	操作方法
创建告警自定义过滤条件	当 eSight 缺省提供的过滤条件无法满足当前管理要求时，可以创建自定义过滤条件以满足管理要求。 - 单击“创建”，在右边页面中设置名称、告警级别、确认状态、清除状态、事件类型和首次发生时间。 - 单击“保存”。
删除告警自定义过滤条件	删除冗余的自定义过滤条件，确保服务器有足够内存，运行畅通。 - 在左边过滤条件列表中选中用户自定义过滤条件，单击“删除”。 - 在“确认”对话框中单击“是”。
修改告警自定义过滤条件	通过修改自定义过滤条件以满足最新管理要求。 - 在左边过滤条件列表中选中用户自定义过滤条件，在右边窗口中修改名称、告警级别、确认状态、清除状态、事件类型和首次发生时间。 - 单击“保存”。
复制告警自定义过滤条件	复制自定义过滤条件可以方便、快速的创建自定义过滤条件。 - 在左边过滤条件列表中选中过滤条件，单击“复制”，在右边窗口中修改名称、告警级别、确认状态、清除状态、事件类型和首次发生时间。 - 单击“保存”。

----结束

5.4 监控股警

在 eSight 中，可以通过拓扑视图、告警板和告警柱状图等方式监控网络告警，实时了解网络中的告警状况并采取相应的措施。

5.4.1 浏览当前告警

通过在当前告警中设置过滤条件和搜索告警，查看当前需要关注 and 处理的告警。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

- 当前告警列表是告警归并后的展示。对于新上报的告警，只要当前告警列表中存在符合归并规则的告警记录，都将新上报的告警归并到原有的告警记录中，归并后告

警次数加一；若当前告警列表中不存在符合归并规则的告警记录，新上报的告警以一条新记录显示在当前告警列表中。

告警归并规则：当告警源、定位信息和告警标识相同时会归并成一条告警记录。

- 当修改了当前设置的过滤条件时，系统即按照新的过滤条件进行搜索。

操作步骤

步骤 1 在主菜单中选择“故障 > 当前告警”。

步骤 2 在“当前告警”窗口的“过滤条件”下拉菜单中，选择条件进行查询。若当前的过滤条件不满足需求可以自定义过滤条件，请参见 [5.3.3 设置告警自定义过滤条件](#)。

步骤 3 在“当前告警”窗口中可以执行如下操作。

管理告警	操作方法	说明
锁定告警	在窗口中单击“锁定”，当前列表中的告警处于锁定状态。 此时“锁定”按钮自动更新为“解锁”按钮。	当告警处于锁定状态时需要注意： ● 新上报的告警不会更新到当前列表中，解锁后才会更新到当前列表中。 ● 当告警处于可选状态时，可以进行确认、清除和查看详细信息等操作。处于不可选状态的告警，不可以做任何操作。 ● 在锁定状态下确认、清除告警，该告警不会列入到历史告警列表，解锁后才会更新到历史列表中。
解锁告警	在窗口中单击“解锁”，系统会自动上报告警到当前列表中。 此时“解锁”按钮自动更新为“锁定”按钮。	当告警处于解锁状态时，不能选择条件范围进行搜索，锁定后才能进行搜索。
搜索告警	在窗口中支持如下搜索方式： ● 不设置任何条件直接单击“搜索”，在当前列表中显示所有告警。 ● 当告警处于锁定状态时，在下拉框中选择搜索范围，在文本框中输入搜索的值，单击“搜索”，在当前列表中显示搜索的告警。	-
确认告警	在窗口中选中一条或多条告警，单击“确认”。	● 已确认告警：在“确认用户”列中显示确认用户。 ● 未确认告警：在“确认用户”列中显示.

管理告警	操作方法	说明
反确认告警	在窗口中选中一条或多条告警，选择“更多 > 反确认”。	通过反确认后，告警由确认状态变成未确认状态。
清除告警	在窗口中选中一条或多条未清除的告警，单击“清除”。	● 已清除告警：告警背景颜色为绿色。 ● 未清除告警：告警背景颜色为白色。
屏蔽告警	1. 在窗口中单击目标告警所在“操作”列中的，选择“屏蔽规则”。 2. 在“屏蔽规则”对话框中设置规则名称和日期，单击“确定”。	● 新增的告警屏蔽规则默认为启用状态。 ● 屏蔽规则只对屏蔽规则启用且处于生效期间上报的告警生效。屏蔽规则对屏蔽规则设置前上报的告警不生效。 ● 性能告警和已清除的告警不可以设置屏蔽规则。
定制告警列表显示列	单击  ，在打开的页面中设置告警列表显示列，单击“确定”。	-
定位拓扑	在窗口中单击目标告警所在“操作”列中的  .	eSight 将该告警记录定位到拓扑视图中产生告警的对象。
查看告警详情	在窗口中单击需要查看详细信息的“告警名称”。	在“告警详情”对话框中显示了所选告警的名称、告警可能原因和修复建议等信息。
查看告警日志信息	在窗口中单击需要查看日志信息的“告警次数”。	在“告警日志信息”对话框中显示了与该条记录相关的告警日志。
导出告警信息	在窗口中选择一条或多条告警，选择“导出 > 导出选中”，导出选择告警的相关信息。 如果需要导出全部可以直接选择“导出 > 导出全部”。	-

---结束

5.4.2 通过告警板监控告警

通过告警板可以了解不同级别告警的数目，还可以通过告警板和告警声音了解当前告警状况。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

在系统右上角显示告警板，告警板从左到右依次显示未清除紧急告警、未清除重要告警、未清除次要告警、未清除提示告警和已清除告警信息。

说明

在首页可以定制当前告警柱状图，显示未清除的紧急告警、重要告警、次要告警和提示告警信息。显示次数与告警板中显示的次数存在联动关系。

操作步骤

步骤 1 在主界面右上方的告警板中，查看未清除紧急告警、未清除重要告警、未清除次要告警、未清除提示告警和已清除告警信息。

----结束

5.4.3 通过拓扑视图监控告警

通过查看拓扑视图，可以实时监控网元的告警情况。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

在拓扑视图中，网元的图标上会显示告警级别对应的颜色。如果该网元同时产生多个告警，网元图标上将显示最高级别告警对应的颜色。

操作步骤

步骤 1 在主菜单中选择“资源 > 拓扑管理”。

步骤 2 在“拓扑管理”窗口中，可以查看到产生告警的 Tips 信息和网元位置。

- 通过 Tips 信息了解到告警的最高级别以及该网元上产生的最高级别的告警总数。
- 通过网元位置信息了解到与其它网元关系，以便能及时处理告警。

步骤 3 在“拓扑管理”窗口中，选择一个发生告警的网元图标。单击该网元右下角的，选择“告警列表”。

步骤 4 在网元管理器窗口中，可以查看该网元的当前告警。

----结束

5.4.4 通过网元管理器监控告警

通过在网元管理中查看 eSight 所管理网元的告警信息，可以了解网元当前运行状况，以便及早发现并解决异常。

前提条件

- 已具备“当前告警管理”的操作权限。
- 被监控告警的网元支持资源管理器管理，且支持告警管理。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 可选: 设置搜索条件搜索网元。

1. 在“资源管理”窗口中，设置“搜索类型”和“搜索条件”。
2. 单击“搜索”。

步骤 3 可选: 在“资源管理”窗口的导航树中，选择一个网元或子网。

步骤 4 在“资源管理”窗口的右边网元列表中，单击目标网元所在“操作”列中的。

步骤 5 在网元管理器窗口中，可以查看该网元的当前告警。

---结束

5.4.5 处理告警

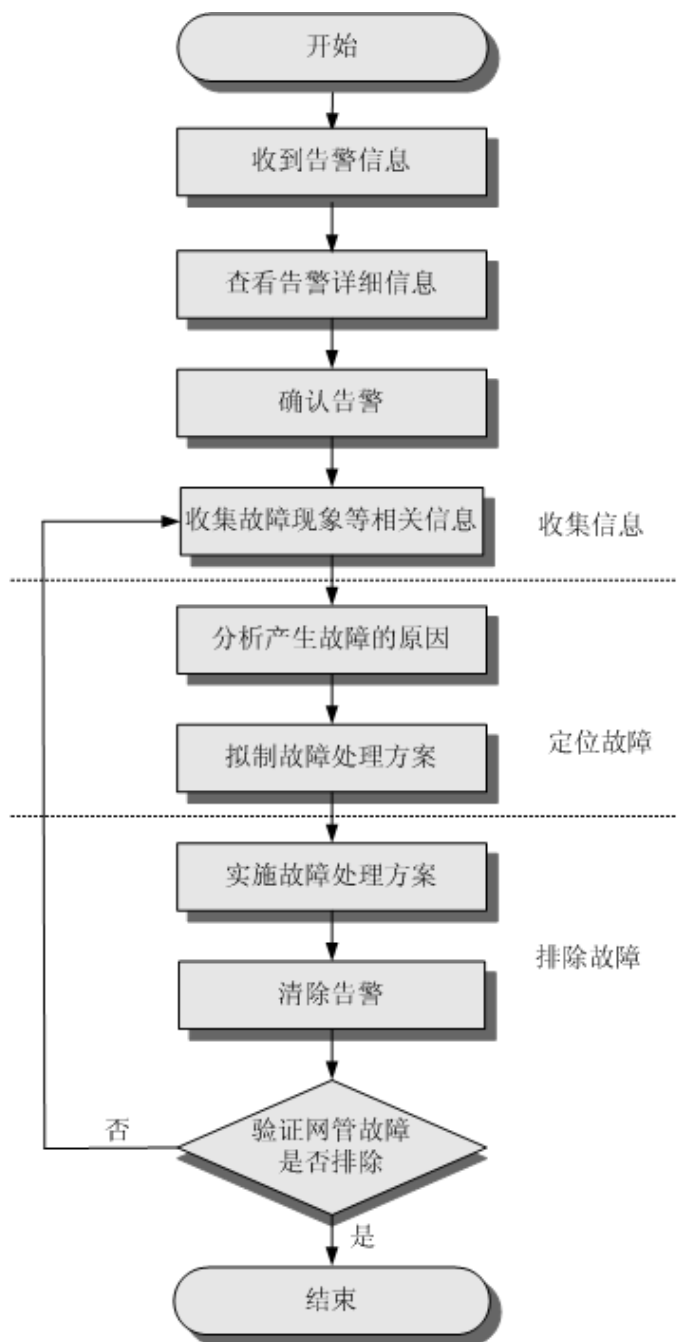
在发现告警信息后，需要按照流程来处理告警以排除故障。处理告警的操作包括查看告警详细信息、确认告警和清除告警等。

5.4.5.1 告警处理流程

介绍告警处理流程，在 eSight 中发现告警后，根据告警处理流程及时处理。

告警处理流程图

图 5-3 告警处理流程



流程说明

表 5-4 告警处理流程说明

步骤	操作	说明
1	收到告警信息	收到告警信息后，启动告警处理流程。为保证故障发生后能及时通知到相关操作员，需要先在 eSight 中配置告警通知方式。 如何配置告警通知方式请参见 5.2 设置告警远程通知 。
2	查看告警详细信息	故障处理的第一步，就是查看告警的详细信息，包括告警的定位信息、告警可能原因和告警处理建议等。
3	确认告警	为避免他人同时对此告警进行处理，需确认该告警，表示已有人跟进处理该告警。
4	收集故障现象等相关信息	通过定位告警，查询告警信息等操作，收集产生的故障现象。
5	分析产生故障的原因	根据故障现象相关信息，分析产生故障的具体原因。
6	拟制故障处理方案	根据告警详细信息，再参考对应网元的相关手册和网络运行情况，以及告警处理建议，拟制故障处理方案。
7	实施故障处理方案	根据拟制的故障处理方案，排除产生告警的故障。
8	清除告警	告警产生的条件消除。如果告警产生的原因已经排除，eSight 上将收到对应的清除告警。
9	验证网管故障是否排除	故障排除后，需要验证故障处理效果。

5.4.5.2 查看告警详情

在 eSight 系统中可以查看当前告警详情、历史告警详情和被屏蔽告警详情。查看告警详情可以获取告警名称、修复建议和定位信息等告警信息。

告警详情参数列表

在“告警详情”对话框中显示了所选告警的名称、告警可能原因和修复建议等信息。

表 5-5 告警详情参数

参数	说明
告警名称	告警的名称。根据告警名称可以快速定位告警的大致情况。 如：License 已经过期，根据名称即可知道是由于 License 文件过期而产生了该告警。

参数	说明
定位信息	通过定位信息可以快速地定位告警产生的原因，分析告警处理的方法。
告警级别	对应故障的严重程度。从严重程度由高到低分为：紧急、重要、次要、提示。
修复建议	查看该告警修复建议，有利于快速定位及解决告警。
告警次数	告警产生的次数。
告警源	发生告警的设备。
最后发生时间	被管对象最后一次产生该告警的时间。
首次发生时间	被管对象第一次产生该告警的时间。
清除时间	管理对象产生清除告警的时间。
清除状态	告警的当前清除状态，如：“未清除”、“已清除”。
清除用户	手动清除告警的用户，如 admin。当网元自动清除告警时，该参数值不存在。
确认状态	告警的当前确认状态，如：“未确认”、“已确认”。
确认时间	告警确认状态改变的发生时间。
告警流水号	告警的唯一索引。在 eSight 系统内，唯一标识一条告警记录。
设备流水号	在同一个设备上，可根据设备流水号唯一确定一条告警。
清除类别	该告警应该采用何种方式清除。 ● ADAC 该告警中描述的故障是一个 ADAC 故障，即该故障修复后，系统会自动检测到已修复，并会有对应的清除告警上报。 ● ADMC 该告警中描述的故障是一个 ADMC 故障，即该故障修复后，系统无法检测到修复信息，因此不会上报清除告警，需要人工清除。
清除类型	一条告警的清除类型。如：“正常清除”、“复位清除”、“手动清除”、“配置清除”、“相关性清除”。
告警标识	告警的 ID。它是告警静态信息表的主关键字，在管理范围内，唯一标识一条静态定义的告警项。
网元名称	产生该告警的网元名称。
网元类型	网络中网元的类型，每个网元对应一种网元类型。
事件类型	承载告警的事件报告的类型。
告警可能原因	系统为何要上报该告警的可能原因，即告警的触发条件。

参数	说明
附加信息	用来记录告警的一些附加参数。主要是记录动态信息，增强告警信息的扩展性。
附加文本	是一个字符串文本，用来对告警信息进行附加描述，可增强告警内容的扩展性。
阈值信息	用来记录阈值越限告警与阈值门限相关信息。 说明 性能告警和 SLA 告警提供阈值信息。
告警通知号	在上报告警相关的信息（包括告警的产生、清除、确认状态改变和告警级别变化等）时，都会带一个告警通知号。网元上报或展示的告警通知号应在网元内部唯一，而资源管理系统上报或展示的告警通知号则应在资源管理系统内部唯一。

5.4.5.3 确认告警

标识某条告警已有用户处理，不必过多关注。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

- 已确认告警：在“确认用户”列中显示确认用户名。
- 未确认告警：在“确认用户”列中显示.

操作步骤

- 步骤 1 在主菜单中选择“故障 > 当前告警”。
- 步骤 2 在“当前告警”窗口中选择过滤条件进行查询，如果不满足需求可以自定义过滤条件，请参见 [5.3.3 设置告警自定义过滤条件](#)
- 步骤 3 在搜索结果窗口中，选中一条或多条告警，单击“确认”。
在“确认用户”列显示确认用户名。
- 结束

后续处理

如果要重新确认该告警，选择“更多 > 反确认”对该告警进行反确认操作。

5.4.5.4 清除告警

当告警无法自动清除或已确认网元上不存在该告警的时候，可以手工进行清除。告警被清除说明导致告警的故障已被排除。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

- 用户对告警执行手工清除后，清除告警命令会被 eSight 下发到网元，网元会清除自己相应的告警。
- 清除告警与告警是相对应的。当设备发生故障时，产生告警；当故障排除后，产生清除告警，原告警被清除。
- 可以通过告警背景颜色辨别告警是否清除如下：
 - 已清除告警：告警背景颜色为绿色。
 - 未清除告警：告警背景颜色为白色。

操作步骤

步骤 1 在主菜单中选择“故障 > 当前告警”。

步骤 2 在“当前告警”窗口中选择过滤条件进行查询，如果不满足需求可以自定义过滤条件，请参见 [5.3.3 设置告警自定义过滤条件](#)

步骤 3 在“当前告警”窗口中，选中一条或多条告警单击“清除”。
清除操作成功后，该告警背景颜色变成绿色。

----结束

5.5 统计分析

通过查询并分析历史告警、事件和被屏蔽告警可以了解网元告警趋势，以便对网元进行升级。

5.5.1 查询历史告警

通过设置历史告警查询条件，可以快速找到所关注的历史告警。

前提条件

已具备“浏览历史告警”的操作权限。

背景信息

- 处于已确认已清除状态的告警成为历史告警，显示在历史告警列表中。
- 查询结果都基于数据库中的现有数据。如果数据库为空，则查询结果无显示内容。
- 在查询历史告警时，可以通过下面设置查看所需告警信息：
 - 通过单击  定制显示列。
 - 通过单击  组合排序 在“组合排序”对话框中设置告警排序。

操作步骤

- 步骤 1 在主菜单中选择“故障 > 历史告警”。
- 步骤 2 可选: 在“历史告警”窗口的搜索栏中设置搜索信息，单击“搜索”。
 - “子网或网元”：单击，在“选择子网或网元”对话框中选择告警源。当选择子网时，告警源为该子网下的网元。

说明

当选择错误或者需要重新选择时，单击清除当前选择的告警源。
 - “告警名称”：设置查询的历史告警名称。
 - “首次发生时间”：从下拉框中选择需要查询告警的月份和所选月份的起止日期。
 - “告警级别”：设置查询历史告警的级别。
- 步骤 3 在“历史告警”窗口中可以执行如下操作。

查询历史告警	操作方法
查看告警详情	1. 单击目标告警的“告警名称”。 2. 在“告警详情”对话框中查看告警级别、告警可能原因和修复建议等信息。
导出告警信息	选择一条或多条告警，选择“导出 > 导出选中”，导出选择告警的相关信息。 说明 如果需要导出全部可以直接单击“导出 > 导出全部”。若设置了搜索条件，只能导出该搜索条件下的所有历史告警。

----结束

5.5.2 查询事件

通过查询事件信息，可以查看到设备侧向 eSight 发送的具体事件消息。

前提条件

已具备“浏览事件列表”的操作权限。

背景信息

事件是指设备侧上报 eSight 的事件通知。

操作步骤

- 步骤 1 在主菜单中选择“故障 > 事件列表”。
- 步骤 2 可选: 在“事件列表”窗口的搜索栏中设置搜索信息，单击“搜索”。
 - “子网或网元”：单击，在“选择子网或网元”对话框中选择事件源。当选择子网时，事件源为该子网下的网元。



当选择错误或者需要重新选择时，单击  清除当前选择的事件源。

- “事件名称”：设置查询的事件名称。
- “发生时间”：从下拉框中选择需要查询事件的月份和所选月份的起止日期。

步骤 3 在“事件列表”窗口中，可以查看事件信息。

----结束

5.5.3 查询被屏蔽告警

通过设置被屏蔽告警查询条件，可以快速找到所关注的被屏蔽告警。

前提条件

已具备“浏览被屏蔽告警”的操作权限。

背景信息

在查询被屏蔽告警时，可以通过下面设置查看所需告警信息。

- 通过单击  定制显示列。
- 通过单击  组合排序 在“组合排序”对话框中设置告警排序。

操作步骤

步骤 1 在主菜单中选择“故障 > 被屏蔽告警”。

步骤 2 在“被屏蔽告警”窗口的搜索栏中设置搜索信息，单击“搜索”。

- “子网或网元”：单击 ，在“选择子网或网元”对话框中选择需要查询的告警源。



当选择错误或者需要重新选择，单击 ，清除当前选择的告警源。

- “告警名称”：设置查询的被屏蔽告警名称。
- “首次发生时间”：设置告警第一次被屏蔽的时间。
- “告警级别”：设置需要查询被屏蔽告警的级别。

步骤 3 在告警列表中单击需要查看的告警名称。

在“告警详情”对话框中显示了所选告警的名称、告警可能原因和修复建议等信息。

----结束

5.6 示例：故障管理典型操作

本主题通过故障管理操作的示例，展示了故障管理的流程和方法。通过本示例，可以更好的了解故障管理的基本流程和操作。

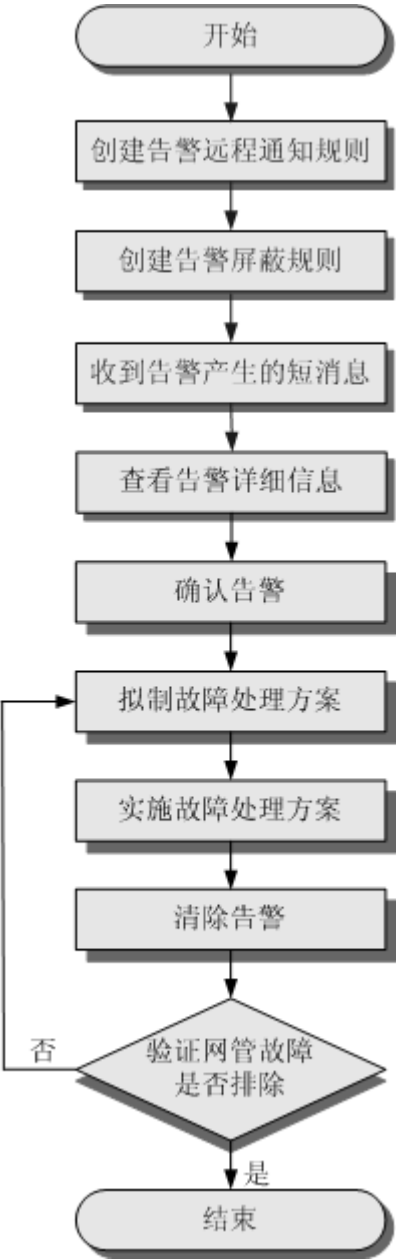
背景信息

管理员小李 2011-12-25 需外出处理个人事务，为了在外出时间能够实时监控并能及时处理网元 eSight、A、B、C 的故障，小李需要设置故障监控规则后，方可放心处理个人事务。补充信息：网元 B 在 2011-12-25 16：00 - 2011-12-26 10：00 进行升级。

网元升级时会上报大量不需要关注的告警，通过创建告警屏蔽规则将不需要关注的告警列入到被屏蔽告警列表中。

在操作前，小李需要先规划好操作流程，规划好的操作流程如图 5-4 所示。

图 5-4 操作流程



操作步骤

步骤 1 创建告警远程通知规则。

管理员小李觉得短消息通知方便些。通过创建告警远程通知规则，eSight 将当前告警列表中 eSight、网元 A、网元 B、网元 C 的告警信息发送到小李的手机。

1. 在主菜单中选择“故障 > 告警设置”。
参考 [5.2.1 远程通知设置流程](#) 设置短消息服务器、内容模板。
2. 新建通知用户组 xef，并增加成员小李。
 - a. 在“告警设置”窗口的导航区中，选择“远程通知 > 通知用户组”。
 - b. 在“通知用户组”页面中，单击“创建”。
 - c. 在“创建用户组”页面中，设置用户组名为“xef”。单击“创建”。
 - d. 在“创建成员”对话框中，设置用户名为“小李”，输入小李的手机号。单击“确定”。
 - e. 单击“保存”。
3. 创建告警远程通知规则“alarm”。
 - a. 在“告警设置”窗口的导航区中，选择“远程通知 > 远程通知规则”。
 - b. 在“远程通知规则”页面中，选择“创建 > 按具体告警”。
 - c. 在“按具体告警创建”页面中，设置规则名称为“alarm”。单击“添加告警源”。
 - d. 在“添加告警源”对话框的“告警源”中，选择网元 eSight、A、B、C。单击“确定”。
 - e. 单击“下一步”，在“告警/事件选择”步骤中，单击“添加告警和事件”。
 - f. 在“添加告警和事件”对话框的“设备类型”中，选择设备。在右边的“告警列表”页签中，选择所有告警级别，单击“全选”。在“事件列表”页签中单击“全选”。
按照此操作依次设置其他设备。单击“确定”。
 - g. 单击“下一步”，在“通知用户组”区域框的“用户组”下拉列框中选择“xef”。
 - h. 单击“完成”。

新创建的远程通知规则，缺省为启用状态。

步骤 2 创建屏蔽规则“NE_B”。

网元升级时会上报大量不需要关注的告警，通过创建告警屏蔽规则，eSight 将网元 B 在升级时间段上报的告警列入到被屏蔽告警列表中，不在当前告警列表中显示。

1. 在“告警设置”窗口的导航区中，选择“基础设置 > 屏蔽规则”。
2. 在“屏蔽规则”页面中单击“创建”。
3. 在“创建屏蔽规则”页面中，设置如下参数。
 - 规则名称：NE_B
 - 日期：2011-12-25 16: 00 到 2011-12-26 10: 00
 - 时间：全时段
4. 单击“下一步”，在“告警源选择”步骤中单击“添加告警源”。
5. 在“添加告警源”对话框的“子网列表”中选择网元 B 所属的子网。在“告警源”中选择网元 B，单击“确定”。

6. 单击“下一步”，在“告警选择”步骤中单击“添加告警”。
7. 在“添加告警”对话框的“设备类型”中选择设备类型。在右边区域中选择所有告警级别，单击“全选”。单击“确定”。
8. 单击“完成”。

新创建的告警屏蔽规则，缺省为启用状态。

步骤 3 小李的手机收到 eSight “License 不合法”告警短消息。

步骤 4 查看告警详情。

1. [登录 eSight](#)。
2. 选择“故障 > 当前告警”，在“当前告警”窗口中发现有“License 不合法”。
3. 单击该告警名称，在“详细信息”对话框中查看告警的详细信息。

步骤 5 确认告警。

根据告警详细信息判断产生告警的故障可以被清除，该告警可得到妥善处理，因此可以确认该告警。在当前告警窗口中选中该告警，单击“确认”，该告警被确认。

步骤 6 拟制告警处理方法。

根据告警详细信息中的修复建议，参考 eSight 的实际运行情况，处理该告警。

步骤 7 排除告警故障。

联系管理员申请新的 License 并导入 eSight。

步骤 8 验证处理结果。

选择“故障 > 历史告警”，可以查看到原来的“License 不合法”告警。

----结束

6 性能管理

关于本章

性能管理能为网络维护人员提供一种监视手段，检查和监视过去一段时间内网络或者业务的运行情况，了解网络运行的性能趋势，对网络进行性能优化，保证网络的正常运行。

6.1 性能操作全景图

通过性能操作全景图可以了解性能管理的所有操作，并根据实际情况，选择操作方式。

6.2 性能监视流程

网管能够从管理的网元中采集网元性能测量数据，提供给用户做报表分析和数据展示。本节介绍性能数据的监视与上报流程。

6.3 设置性能监视参数

监视并采集网元或者网络的性能数据，可以帮助用户提前发现网络运行隐患，规避网络故障风险。

6.4 浏览性能监视数据

用户通过浏览性能监视数据可以及时掌握网络运行质量，提早发现网络故障隐患。

6.5 示例：性能管理典型操作

性能管理操作示例展示了性能管理的流程和方法。通过性能管理可以了解性能管理的基本流程和操作。

6.1 性能操作全景图

通过性能操作全景图可以了解性能管理的所有操作，并根据实际情况，选择操作方式。

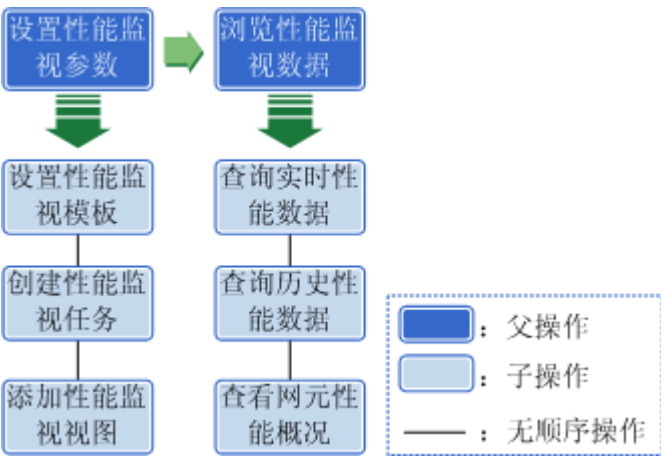
背景信息

在进行性能管理操作时，若需要了解性能管理的基本概念，如性能指标、指标阈值，请参见 [1.2.5 性能基本概念](#)。理解这些概念可以更快速和准确地进行性能管理的操作。

性能操作全景图

性能操作全景图，如 [图 6-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 6-1 性能操作全景图



性能操作的简要说明如[表 6-1](#) 所示。

表 6-1 操作简要说明

操作	说明	操作入口
6.3.1 设置性能监视模板	性能监视模板能够提供对设备关键性能数据的自动采集功能，网元创建后 eSight 能够根据设置的模板自动创建网元性能采集任务，以及采集数据和产生告警。	“性能 > 性能监视模板设置”
6.3.2 创建性能监视任务	用户创建性能监视任务后，就能够启动性能监视任务对网元的性能指标进行监视与数据采集。	“性能 > 性能监视设置”

操作	说明	操作入口
6.3.3 添加性能监视视图	性能监视视图能提供关键性能指标图形化的实时监视，可以是针对同一指标的多个对象监视，也可以是一个对象的多个相关指标监视。	“性能 > 性能监视视图”
6.4.1 查询实时性能数据	性能监视视图中能够实时监控性能指标数据，并图形化展示指标数据的变化情况。	“性能 > 性能监视视图”
6.4.2 查询历史性能数据	按照指定时间段查询性能统计数据，能帮助用户了解一段时间内网络或者业务的运行情况。	“性能 > 性能历史数据”
6.4.3 查看网元性能概况	eSight 支持对网元关键 KPI 指标的实时监视，通过不同的图表形式向用户展示网元当前的性能状况。	“资源 > 资源管理”

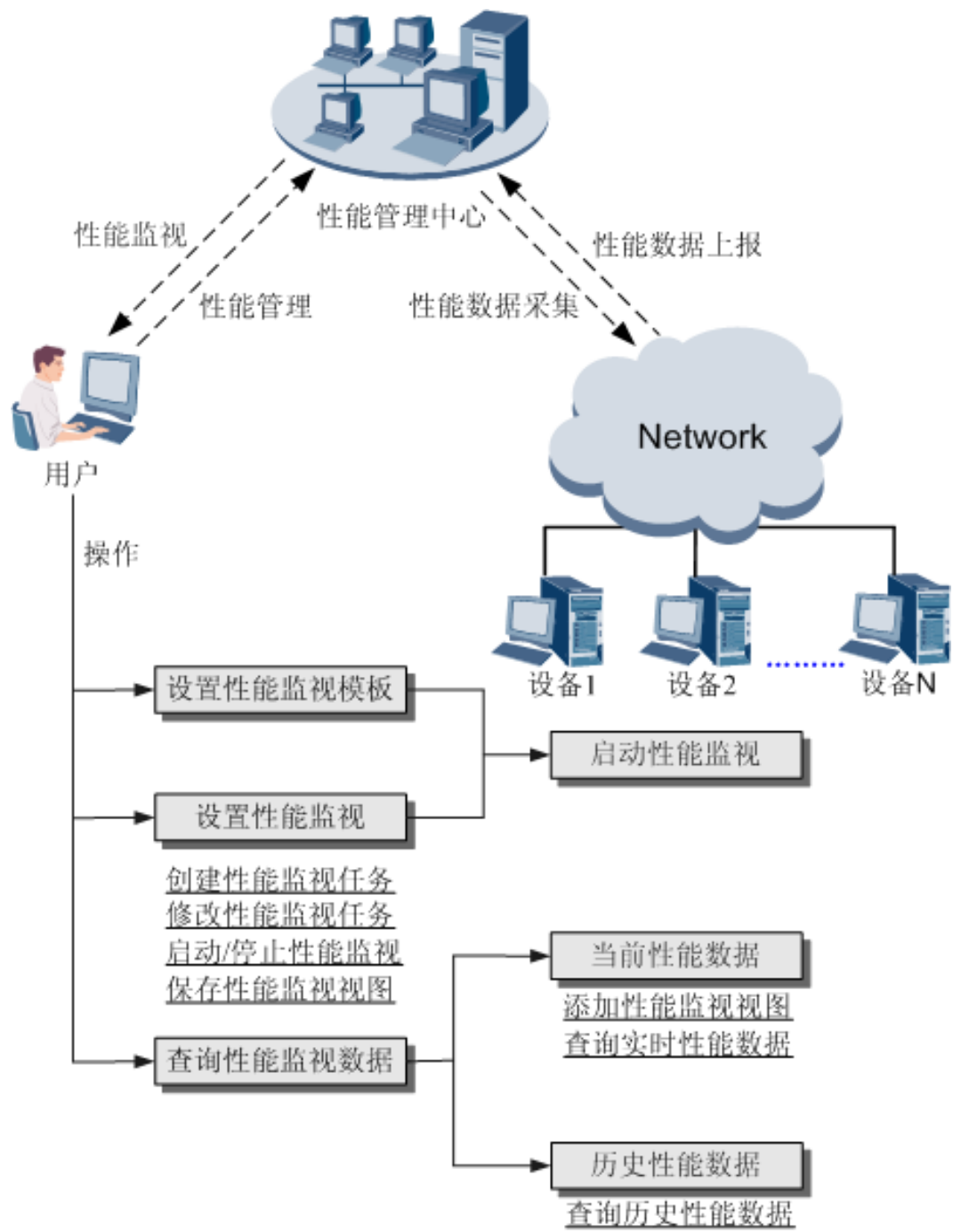
6.2 性能监视流程

网管能够从管理的网元中采集网元性能测量数据，提供给用户做报表分析和数据展示。本节介绍性能数据的监视与上报流程。

性能监视流程

性能监视的流程如图 6-2 所示，在网管两侧分别为用户侧和网元侧。用户侧能够从网管启动性能监视，网管侧从网元上采集性能数据并展示给用户查看。

图 6-2 性能监视流程



用户侧性能监视的流程

- 6.3.1 设置性能监视模板:** 由于同类型网元具有相同的属性,可以在一个模板中提前预置性能监视参数, eSight 根据模板的设置自动在“性能监视设置”窗口中增加监视任务,进行性能数据的采集并上报产生的告警。

2. **6.3.2 创建性能监视任务**：在需要进行性能监视的对象上创建一个性能监视任务，通过启/停性能监视任务实现对性能指标数据的采集。支持对已监视对象的属性进行修改，实现了对所有性能监视任务当前采集状态与告警状态的集中监视。
3. 查询性能监视数据：从网元上报的性能监视数据都保存在网管的性能数据库中，性能监视数据分为实时性能数据和历史性能数据。
 - **实时性能数据**：通过性能监视视图可以实时监控网元性能指标数据，并图形化展示指标数据的变化情况。
 - **历史性能数据**：支持查询指定时间段的性能数据，以了解一段时间内网络或者业务的运行情况。历史性能数据支持列表和曲线图方式展示。

6.3 设置性能监视参数

监视并采集网元或者网络的性能数据，可以帮助用户提前发现网络运行隐患，规避网络故障风险。

6.3.1 设置性能监视模板

性能监视模板能够提供对设备关键性能数据的自动采集功能，网元创建后 eSight 能够根据设置的模板自动创建网元性能采集任务，以及采集数据和产生告警。

前提条件

已具备“性能监视模板设置”的操作权限。

背景信息

由于同类型网元具有相同的属性，将这些属性设置为一个性能监视模板并设置为缺省监视后，当有新网元接入时，会自动继承模板中的设置，从而提供默认的监视和告警能力。性能监视模板中的设置能够批量应用到网元上，通过这种全局应用，可以提高性能采集任务的创建和下发效率。

操作步骤

- 步骤 1** 在主菜单中选择“性能 > 性能监视模板设置”。
- 步骤 2** 在“性能监视模板设置”窗口的左侧导航树中，选择一个网元类型，右侧折叠状态联动显示网元类型对应的所有性能指标。
- 步骤 3** 单击，展开折叠对象下的性能指标。
- 步骤 4** 单击，在“修改阈值”对话框中设置告警产生/恢复条件和重复次数。单击“确定”。



注意

修改阈值条件后，该阈值修改前产生的告警将被清除。

例如“重复次数”设置为 3 时，表示设备连续 3 个性能采集周期的性能值都超过阈值时，设备才会上报该告警。

步骤 5 设置采集周期。

步骤 6 设置性能指标的“缺省监视”。

- 选中“缺省监视”。

当该网元类型有新网元接入时，eSight 会自动在“性能监视设置”窗口中增加该性能指标的监视任务。

- 去选中“缺省监视”。

在设置指标属性时，可以设置为启用模板直接引用性能模板的设置。

步骤 7 单击“应用”，对应性能指标的采集任务会随模板一起下发到网元上。

----结束

操作结果

设置告警阈值后，当告警条件满足时，系统会自动产生告警，并发送到当前告警窗口中。

6.3.2 创建性能监视任务

用户创建性能监视任务后，就能够启动性能监视任务对网元的性能指标进行监视与数据采集。

前提条件

已具备“性能监视设置”的操作权限。

背景信息

eSight 支持用户手工输入测量对象和给出具体的测量对象供用户选择。

操作步骤

步骤 1 在主菜单中选择“性能 > 性能监视设置”。

步骤 2 在“性能监视设置”窗口中，单击“创建”。

步骤 3 选择管理对象。

1. 在“创建监视任务”页面中，单击“选择管理对象”。
2. 在“选择管理对象”对话框的“子网列表”中，选择一个子网。
3. 在“管理对象”中选择对象，单击“确定”。

步骤 4 选择指标。

1. 在“创建监视任务”页面中，单击“选择指标”。
2. 在“选择指标”对话框的“对象类型”中，选择一个对象类型。
3. 在“指标列表”中选择指标，单击“确定”。

步骤 5 可选: 用户可以自定义性能监视的采集周期、阈值条件。

1. 在“创建监视任务”页面中，单击“修改属性”。
2. 在“修改属性”对话框中，去选中目标指标所在“是否启用模板”列中的复选框。

 说明

- 如果启用模板设置，监视任务的属性会使用对应模板中设置的值，且全部灰化不能修改，只有去掉启用模板设置才能手动修改。
- 如果启用模板设置，后续在性能监视模板中调整属性时，相应的指标会自动采用新的模板值。
- 列表中只按指标项显示，修改属性的结果会自动对监视该指标的多个网元都生效。

3. 单击目标指标所在“修改阈值”列中的.
4. 在“修改阈值”对话框中，修改告警上报或恢复的阈值条件和重复次数。单击“确定”。



注意

修改阈值条件后，该阈值修改前产生的告警将被清除。

例如“重复次数”设置为3时，表示设备连续3个采集周期的性能值都超过阈值时，设备才会上报该告警。

5. 在“修改属性”对话框中单击“确定”。

步骤 6 选择测量对象。

所有已选指标必须选择测量对象，没有测量对象的指标不用进行选择。

1. 单击已选指标所在“测量对象”列中的.
2. 在“选择测量对象”对话框中选择测量对象。
 - 直接选择测量对象：
 - a. 在“选择测量对象”对话框的“可选择测量对象”页签中，选择测量对象。在“测量对象名称”文本框中输入关键字，单击“搜索”，可以搜索出符合条件的测量对象。
 - b. 在“已选择测量对象”页签中查看已经选择的测量对象。在“已选择测量对象”页签中选择一个或多个测量对象，单击“删除”可以取消选择已选择的测量对象。
 - c. 单击“确定”。
 - 支持手工输入测量对象：
 - a. 在“选择测量对象”对话框中，在 eSight 缺省提供的测量对象中选择测量对象。
 - b. 单击，在打开的文本框中输入测量对象信息（如电话号码）。
单击手工输入的测量对象对应的可以删除该测量对象。不能删除 eSight 缺省提供的测量对象。
 - c. 单击“确定”。

 说明

“手工输入测量对象”功能需要在“自定义设备管理 > 设备管理能力定制 > 性能指标定制”中定制“测量对象类型”为“未指定对象指标组”的指标，当针对该指标创建性能监视任务时有效。

步骤 7 在“创建监视任务”页面中单击“确定”。

步骤 8 在“操作结果列表”页面中单击“完成”。

监视任务创建完成后，默认立即启动。在监视任务列表中可以查看监视任务的数据采集状态。

----结束

后续处理

性能监视任务创建后可以对性能监视任务执行如下操作。

设置性能监视任务	操作方法
修改性能监视任务	修改性能监视任务以满足最新管理要求。 - 在“性能监视设置”窗口中，选择一条或多条任务，单击“修改”。 - 在“修改属性”对话框中修改任务指标属性，如修改告警上报的阈值条件。 注意 修改阈值条件后，该阈值修改前产生的告警将被清除。
删除性能监视任务	删除冗余的性能监视任务，确保服务器有足够内存，运行顺畅。 在“性能监视设置”窗口中，选择一条或多条任务，单击“删除”。
启动性能监视任务	启动性能监视任务，网元按照任务设置的信息对性能指标进行监视与数据采集，并上报告警。 在“性能监视设置”窗口中，选择一条或多条“采集状态”为“停止”的任务，单击“启动”。
停止性能监视任务	停止不需要关注的任务，确保服务器有足够内存，运行顺畅。 在“性能监视设置”窗口中，选择一条或多条任务，单击“停止”。

6.3.3 添加性能监视视图

性能监视视图能提供关键性能指标图形化的实时监视，可以是针对同一指标的多个对象监视，也可以是一个对象的多个相关指标监视。

前提条件

- 已具备“性能监视设置”和“性能监视视图”的操作权限。
- 至少存在 1 个性能监视任务。

背景信息

- 添加性能监视视图的指标只支持数值类型。
- 对同一个用户而言，添加性能监视视图的个数不能超过 10 个，且同一性能监视视图的指标不能超过 6 个。

操作步骤

- 从主菜单直接进入性能监视视图。
 1. 在主菜单中选择“性能 > 性能监视视图”。
 2. 在“性能监视视图”窗口中，单击“增加监视视图”。
 3. 在“增加监视视图”对话框中设置视图名称，在“管理对象”中选择管理对象。
 4. 在“指标实例”中选择需要添加到性能监视视图的指标，单击“确定”。
- 在性能监视列表中直接将监视任务保存为性能监视视图。
 1. 在主菜单中选择“性能 > 性能监视设置”。
 2. **可选:** 在“性能监视设置”窗口中，根据需要设置过滤条件，单击“搜索”，界面显示符合特定查询条件的性能监视任务。
 3. 在“性能监视设置”窗口的性能监视列表中，选择一条或多条监视任务，单击“保存为监视视图”。
 4. 在“增加监视视图”窗口中设置视图名称，单击“确定”。
 5. 在主菜单中选择“性能 > 性能监视视图”，在“性能监视视图”窗口中查看保存的视图。

----结束

后续处理

添加性能监视视图后可以对性能监视视图执行如下操作。

设置性能监视视图	操作方法
修改性能监视视图	修改性能监视视图以满足最新管理要求。 1. 在“性能监视视图”窗口中，单击目标监视视图对应的. 2. 在“修改监视视图”窗口中，修改视图名称，并对视图中监视的指标实例进行增删。
删除性能监视视图	删除冗余的性能监视视图，释放资源以创建新的性能监视视图。 在“性能监视视图”窗口中，单击目标监视视图对应的  .

 说明

用户修改或删除监视视图后，若同一用户正在另一客户端中查看监视视图，此时会提示监视视图的状态发生改变需要更新，在提示对话框中单击“确定”更新监视视图。

6.4 浏览性能监视数据

用户通过浏览性能监视数据可以及时掌握网络运行质量，提早发现网络故障隐患。

6.4.1 查询实时性能数据

性能监视视图中能够实时监控性能指标数据，并图形化展示指标数据的变化情况。

前提条件

- 已具备“性能监视视图”的操作权限。
- 待查看的性能指标已添加性能监视视图。

操作步骤

步骤 1 在主菜单中选择“性能 > 性能监视视图”。

步骤 2 单击，展开查看对应的性能监视视图。

----结束

6.4.2 查询历史性能数据

按照指定时间段查询性能统计数据，能帮助用户了解一段时间内网络或者业务的运行情况。

前提条件

已具备“性能历史数据查询”的操作权限。

操作步骤

步骤 1 在主菜单中选择“性能 > 性能历史数据”。

步骤 2 在“性能历史数据”窗口中单击“选择管理对象”。

步骤 3 在“选择管理对象”对话框中，单击“对象类型”后的，在“选择对象类型”对话框中选择查询的对象类型。

步骤 4 在“选择对象类型”对话框中单击“确定”。

在“选择管理对象”对话框的管理对象列表中，显示该类型下的所有管理对象。

步骤 5 在“子网列表”中选择一个子网，在“管理对象”中选择该子网下的一个或多个管理对象，单击“确定”。

“性能历史数据”窗口左侧的“管理对象”中显示选择的管理对象。

步骤 6 设置查询的“指标组”和“时间范围”，单击“搜索”。“数据列表”中显示与搜索条件匹配的性能监视数据。

 说明

选择网元或者测量对象，可以在搜索结果中过滤，列表中只显示特定网元或者测量对象的性能监视数据。

只有当查询的管理对象带测量对象时，测量对象下拉框激活可操作，否则灰化。

步骤 7 可选：设置数据曲线图显示性能监视数据。

1. 在“数据曲线图”页签中单击“选择实例”。
2. 在“选择实例”对话框中选择与指标相关的对象实例，单击“确定”。

“数据曲线图”页签显示性能指标的数据曲线图。

最多可以选择 6 个对象实例，曲线图以不同颜色的曲线表示不同实例的性能指标。

----结束

后续处理

在“数据列表”页签中单击“导出所有数据”，将采集到的性能测量数据保存到 csv 格式的本地文件中。

6.4.3 查看网元性能概况

eSight 支持对网元关键 KPI 指标的实时监视，通过不同的图表形式向用户展示网元当前的性能状况。

前提条件

- 已具备“性能监视设置”和“性能 KPI 浏览”的操作权限。
- 查看的网元支持资源管理器管理，且支持性能管理。

背景信息

eSight 提供“资源管理”和“性能管理”两个入口查看网元性能概况。

操作步骤

步骤 1 进入网元管理窗口。

- 通过“资源管理”进入网元管理窗口。
 1. 在主菜单中选择“资源 > 资源管理”。
 2. 在“资源管理”窗口的导航树中，选择一个网元。
 3. 在右侧单击网元所在“操作”列中的，进入网元管理窗口。
- 通过“性能管理”进入网元管理窗口。
 1. 在主菜单中选择“性能 > 性能监视设置”。
 2. 在“性能监视设置”窗口的性能监视列表中，单击目标监视任务所在“管理对象”列的名称，进入网元管理窗口。

步骤 2 查看网元基本信息和性能 KPI。

1. 在“基本信息”页签中查看网元基本信息和性能 KPI 信息。
2. 设置图形化显示的 KPI 指标。

最多可以选择 20 个 KPI 指标。

 - a. 单击“性能 KPI”区域框标题所在行中的“设置”。
 - b. 在“设置”对话框中选择需要在“性能 KPI”中图形化显示的 KPI 指标，单击“确定”。

 窍门

- 单击目标 KPI 指标视图对应的，可以删除该性能指标的图形化显示。
- 单击目标 KPI 指标视图对应的，选择“指标详情”，在“KPI 指标详情”页签中自动展开对应指标的数据曲线图，查看各个性能采集时间点指标数据的变化情况。
- 当指标带有多个测量对象时，单击目标 KPI 指标视图对应的，选择“测量对象”，在弹出窗口中增加和删除图表中显示的测量对象。

步骤 3 网元监视设置。

1. 在主菜单中，选择“性能 > 性能监视设置”。
2. 在“性能监视设置”页签中可以管理监视任务并将监视任务保存为性能监视视图，详细操作请参见 [6.3.2 创建性能监视任务](#)和 [6.3.3 添加性能监视视图](#)。

步骤 4 查看指标详情。

1. 在网元管理窗口的导航区中，选择“性能状态”，可查看各性能指标的数据曲线图。
2. 在“性能状态”页签中，单击目标性能指标区域框标题所在行中的展开并查看性能指标的数据曲线图。
3. 单击目标性能指标区域框标题所在行中的，在“请选择测量对象”对话框中选择测量对象，详细操作请参见 [6.3.2 创建性能监视任务](#)中的**步骤 6**。
每个测量对象的性能指标详情在性能视图中显示一条线，多个测量对象就显示多条线。
4. 单击目标性能指标区域框标题所在行中的，在“修改属性”对话框中修改性能指标的采集周期、阈值条件。详细操作请参见 [6.3.2 创建性能监视任务](#)中的**步骤 5**。

----结束

6.5 示例：性能管理典型操作

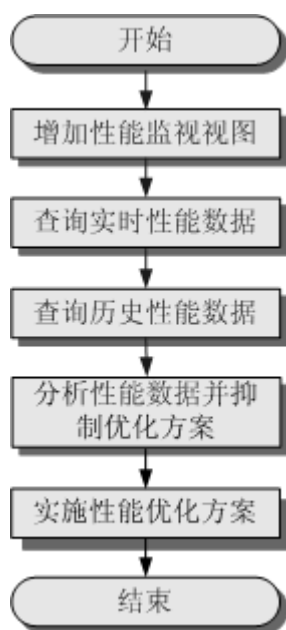
性能管理操作示例展示了性能管理的流程和方法。通过性能管理可以了解性能管理的基本流程和操作。

背景信息

维护工程师小王最近发现设备 A 的业务处理质量较差，怀疑设备 A 的性能较低不能满足业务运行要求。小王收集设备 A 的性能数据来分析。

在操作前，小王需要先规划好操作流程，规划好的操作流程如[图 6-3](#)所示。

图 6-3 操作流程图



操作步骤

步骤 1 增加设备 A 的性能监视视图

1. 在主菜单中选择“性能 > 性能监视视图”。
2. 在“性能监视视图”窗口中，单击“增加监视视图”。
3. 在“增加监视视图”对话框中设置视图名称，在“管理对象”中选择设备 A。
4. 在“指标实例”中选择需要收集性能数据的指标，单击“确定”。

步骤 2 在增加的性能监视视图中，查看设备 A 的实时性能数据。

步骤 3 查询设备 A 的历史性能数据

1. 在主菜单中选择“性能 > 性能历史数据”。
2. 在“性能历史数据”窗口中单击“选择管理对象”。
3. 在“选择管理对象”对话框中选择设备 A，单击“确定”。
4. 设置查询的“指标组”和“时间范围”，单击“搜索”。

步骤 4 分析并抑制优化方案

根据搜集的性能数据，判断是否设备 A 的性能已不能满足业务运行要求。并给出优化方案。

步骤 5 实施性能优化方案。

----结束

7 报表管理

关于本章

报表为客户提供对全网存量资源、告警资源、业务资源、资源监控、系统性能数据的查询与统计。

7.1 报表操作全景图

通过报表操作全景图可以了解报表管理的所有操作，并根据实际情况，选择相应操作。

7.2 配置报表的系统参数

当客户需要对报表的存储容量、LOGO 及数据源有特殊要求时，支持对这些配置项进行定制。

7.3 创建报表

用户可以创建报表任务来执行报表。报表任务生成报表后，会自动将报表保存到存储区中，并且根据配置，触发 E-Mail 转发操作。

7.4 查看报表

网管根据报表任务生成报表后，可以根据需要查看报表的内容，完成对现网的维护。

7.5 维护报表系统

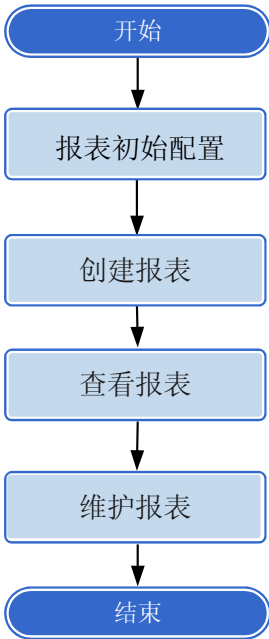
根据需要，定期对报表系统进行维护。

7.1 报表操作全景图

通过报表操作全景图可以了解报表管理的所有操作，并根据实际情况，选择相应操作。

报表操作全景图，如图 7-1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 7-1 报表操作全景图



报表操作的简要说明如表 7-1 所示。

表 7-1 操作简要说明

操作	说明
1、 报表初始配置	网管默认为报表提供了系统配置，当客户需要对报表的存储容量、LOGO 及数据源有特殊要求时，支持对这些配置项进行定制。 ● 配置报表存储区容量。 ● 定制报表客户的 LOGO。 ● 配置监控报表的数据源。
2、 创建报表	eSight 根据报表任务生成报表，并自动将周期报表保存到存储区，并根据配置将报表以 Email 方式发送给客户。
3、 查看报表	查看报表内容。

操作	说明
4、 维护报表	维护报表任务包括： ● 修改报表任务。 ● 配置报表存储区域。 ● 导出报表。 ● 管理报表任务状态。

7.2 配置报表的系统参数

当客户需要对报表的存储容量、LOGO 及数据源有特殊要求时，支持对这些配置项进行定制。

7.2.1 设置数据源

当监控的数据源和网管服务器不在同一台机器上，可以通过设置数据源，将其在网管上生成报表，展现给用户。

背景信息

当上级网管需要监控下级网管的报表时，需要在上级网管上设置报表数据源为下级网管的数据库。

操作步骤

- 步骤 1** 在主菜单中选择“报表 > 报表系统配置”。
- 步骤 2** 选择“数据源”，单击“创建”，在弹出的窗口中设置数据源相关参数。
- 步骤 3** 单击“测试连接”，测试成功后，单击“保存”。

----结束

后续处理

将数据源指定给设计文件：

1. 在主菜单中选择“报表 > 报表任务管理”。
2. 单击“创建”，选择相应的设计文件，单击，设置设计文件的数据源，单击“确定”。

7.2.2 报表系统配置

通过报表系统配置，可以配置报表存储区的空间和客户的信息。

操作步骤

- 步骤 1** 在主菜单中选择“报表 > 报表系统配置”。

- 步骤 2** 在左侧导航树中选择“报表系统配置 > 存储区”，在右侧窗口中设置存储区容量的上限值，单击“保存”。
该窗口下可查看存储区使用情况。
- 步骤 3** 在左侧导航树中选择“报表系统配置 > 客户信息”，在右侧窗口中单击选择客户 LOGO 图片，单击“上传”。
 窍门
 - 当选择了不适合的图片且未上传时，可单击清除后，再重新选择图片。
 - 需要对已上传的图片进行替换时，可重新选择新图片并上传。

----结束

7.3 创建报表

用户可以创建报表任务来执行报表。报表任务生成报表后，会自动将报表保存到存储区中，并且根据配置，触发 E-Mail 转发操作。

操作步骤

- 步骤 1** 在主菜单中选择“报表 > 报表任务管理”。
- 步骤 2** 单击“创建”，选择相应的设计文件。
 窍门

当设计文件较多时，可以设置“设计文件分类”或“文件名”后单击“查询”，可将需要的设计文件过滤显示在下方列表中。

单击“上传设计文件”，在弹出的窗口中配置自定义设计文件相关信息，单击“确定”，上传自定义的设计文件。
- 步骤 3** 可选: 根据需要，单击，设置设计文件的数据源，单击“确定”。
- 步骤 4** 单击“下一步”，根据需要设置相关参数。

设计文件分类:	性能报表
设计文件名:	网元CPU使用率统计报表
* 任务名:	网元CPU使用率统计报表
* 类型:	 在每月指定的时间生成报表，统计上个月或近30天的数据。 ☐ 手工报表 ☒ 周期报表， 每 月 第 1 天生成。
* 统计范围:	近30天

表 7-2 参数说明

名称	说明
类型	- 手工报表：创建手工报表，任务创建成功后手工执行，生成手工报表。 - 周期报表：创建周期报表，任务创建成功后根据设置的周期，生成周期报表。 说明 默认情况下，eSight 会在当天的凌晨 4 点生成周期报表。如需修改生成周期报表的时间，在 eSight 服务器安装路径\AppBase\bin\runtime.center\config\report\report_conf.xml 中设置。修改后，需重启 eSight 服务才能生效。
统计范围	设置周期报表统计的范围，两种范围。 以月报为例：创建报表任务的日期为 2011 - 05 - 11，若统计范围选择“近 1 月”，则统计的是 2011 - 04 - 11 至 2011 - 05 - 10 之间的数据；若统计范围选择的是“上月”，则统计的是 2011 - 04 - 01 至 2011 - 04 - 30 之间的数据。

步骤 5 可选：勾选“通过 Email 转发”，设置 Email 转发的相关参数，将报表以邮件的方式发送给用户。

步骤 6 设置任务参数，单击“完成”。
设计文件不同，配置参数也不同。

----结束

7.4 查看报表

网管根据报表任务生成报表后，可以根据需要查看报表的内容，完成对现网的维护。

操作步骤

步骤 1 在主菜单中选择“报表 > 报表任务管理”。

步骤 2 查看报表。

- 对于周期报表，在相应的报表后，单击，在弹出的窗口中查看报表相关信息。
- 对于手工报表，在相应的报表后，单击，在弹出窗口中查看报表相关信息。

----结束

7.5 维护报表系统

根据需要，定期对报表系统进行维护。

7.5.1 修改报表任务

根据需要，对报表任务进行修改。

操作步骤

步骤 1 在主菜单中选择“报表 > 报表任务管理”。

步骤 2 可选: 在界面的上方设置报表任务的过滤条件，单击“搜索”，搜索出相应的报表任务。

步骤 3 在“操作”下单击.

步骤 4 在“修改任务”界面，根据需要修改报表任务相关参数，单击“保存”。

----结束

7.5.2 管理报表存储空间

当报表存存储容量达到临界值时，需要定期清理存储区内的报表，释放存储空间。

操作步骤

步骤 1 在主菜单中选择“报表 > 报表系统配置”。

步骤 2 选择“存储区”，调整“容量上限”，单击“保存”。

步骤 3 在主菜单中选择“报表 > 报表任务管理”。

步骤 4 对于周期报表任务，单击，勾选待清理的报表，单击“导出”，选择导出报表的文件格式，在弹出的窗口中，单击“确定”。

 说明

手工报表不存库。

导出手工报表方法：单击，在弹出的窗口中单击“导出报表”导出相应的报表。

步骤 5 根据需要，单击“删除”，在存储区中删除该报表。

----结束

7.5.3 管理报表任务的状态

根据需要，定期对报表系统进行维护。

操作步骤

步骤 1 在主菜单中选择“报表 > 报表任务管理”。

步骤 2 可选: 在界面的上方设置报表任务的过滤条件，单击“搜索”，搜索出相应的报表任务。

步骤 3 查看报表的状态信息，根据需要。

- 对于周期报表任务，可单击启动任务。
- 对于周期报表任务，可单击禁止任务。
- 对于手工报表任务，可单击立即执行任务。

----结束

8 网元管理器

关于本章

eSight 提供设备基本信息管理、设备面板的查看、设备接口信息管理、IP 地址信息查看等功能。

8.1 网元管理全景图

通过网元管理操作全景图可以了解网元管理的所有操作，并根据实际情况，选择操作方式。

8.2 查看网元

通过查看网元的基本信息、面板、告警和性能，实现对网元的监控。

8.3 配置网元

通过对网元的配置方式的设置、协议参数的配置、接口及 IP 地址配置以及网元配置文件的备份与恢复，完成对网元的配置操作。

8.1 网元管理全景图

通过网元管理操作全景图可以了解网元管理的所有操作，并根据实际情况，选择操作方式。

背景信息

在进行网元管理操作前，若需要了解网元管理的基本概念，请参见 [1.2.7 网元管理基本概念](#)。理解这些概念可以更快速和准确地进行资源管理的操作。

网元管理全景图

网元管理全景图，如 [图 8-1](#) 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 8-1 网元管理全景图



网元管理的操作简要说明如 [表 8-1](#) 所示。

表 8-1 操作简要说明

操作	说明	操作入口
查看基本信息	通过查看网元基本信息，了解网元的基本情况。	“资源 > 资源管理”
查看设备面板	在设备面板上可以查看到网元的槽位、单板、子卡和端口相关参数。	“资源 > 资源管理”
查看告警列表	通过查看网元告警列表，了解网元的当前相关告警信息。	“资源 > 资源管理”
查看性能状态	通过查看性能状态，了解网元当前的性能相关信息。	“资源 > 资源管理”

操作	说明	操作入口
配置 Telnet 参数	当网管与网元之间使用 Telnet 协议进行通信且网元侧的 Telnet 参数发生变化时，需同步设置网管侧网元的 Telnet 参数。	“资源 > 资源管理”
配置 SNMP 参数	当网管与网元之间使用 SNMP 协议通信且网元侧的 SNMP 参数有变化时，需要同步修改网管侧网元的 SNMP 参数。	“资源 > 资源管理”
配置接口	可以对接口进行激活/去激活和修改接口别名的操作。	“资源 > 资源管理”
查看接口参数	网管支持对接口的索引、接口描述、接口 IP 地址、接口类型、接口状态、接口速率、接口别名等信息查询。	“资源 > 资源管理”
查询 IP 地址	在进行业务配置及网络规划时，需要查询网元及其接口的 IP 地址，eSight 支持对网元的 IP 地址以及接口的 IP 地址进行查询。	“资源 > 资源管理”
配置文件管理	eSight 支持将网元的配置文件进行恢复，当配置文件数据遭到破坏时，可以通过恢复操作，对网元上的配置文件进行保护。	“资源 > 资源管理”

8.2 查看网元

通过查看网元的基本信息、面板、告警和性能，实现对网元的监控。

8.2.1 查看基本信息

通过查看网元基本信息，了解网元的基本情况。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 查看网元的基本信息。

在“基本信息”中，可执行如下操作：

- 单击“修改”，在弹出的窗口修改网元的基本信息，单击“确定”。



说明

如果修改网元信息失败，可能是网元实际支持的参数长度小于页面参数提示长度，或者 SNMP 参数设置错误。

- 单击“刷新”，网管同步网元的基本信息并刷新网元的状态。

- 单击“Telnet”：登录设备。

执行该操作前需要配置 Telnet 参数，详细操作请参见 [8.3.2.1 配置网管侧网元 Telnet 参数](#)。

- 单击“Ping”，在弹出的窗口中设置 ping 信息，单击“Ping”，测试完成后，可在“Ping”中查看测试结果，Ping 测试验证网管与设备之间的连通性。
- 单击“Trace”，在弹出的对话框中查看测试结果。Trace 测试验证网管与设备之间的连通性，并追踪其路由信息。
- 单击“同步设备数据”，将设备的数据同步到网管侧，在弹出窗口中的详细信息中查看同步设备的数据详细情况。
- 在“性能 KPI”中，查看网元当前的关键性能信息。
- 在“TOP10 告警”中，查看网元当前的 TOP10 告警信息。
- 在“接口流量”中，查看网元的接口流量信息。

----结束

8.2.2 查看设备面板

在设备面板上可以查看到网元的槽位、单板、子卡和端口相关参数。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“查看 > 设备面板”。

步骤 3 将鼠标放在对应的单板、子卡或端口上，网管上会显示其相应的参数。

步骤 4 可选：可单击“缩小”、“放大”、“刷新”、“显示图例”，执行相应的操作。



步骤 5 可选：将鼠标放在设备面板上，右键单击鼠标，弹出可选菜单项：

- “浏览告警”：用于查看该网元的告警信息，掌握网元当前运行状况，具体可参见 [5.4.4 通过网元管理器监控告警](#)。
- “创建新样式”：可通过手绘图方式对设备面板进行定制，具体可参见 [12.6.4 自定义设备面板](#)。
- “绑定样式”：可将所创建的设备面板图与该网元进行绑定。

----结束

8.2.3 查看告警列表

通过查看网元告警列表，了解网元的当前相关告警信息。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“查看 > 告警列表”。

步骤 3 在“告警列表”窗口中，可进行如下操作。

操作名称	操作方法
锁定	在窗口中单击“锁定”，当前列表中的告警处于锁定状态。 当告警处于锁定状态时需要注意： ● 新上报的告警不会更新到当前列表中，解锁后才会更新到当前列表中。 ● 当告警处于可选状态时，可以进行确认、清除和查看详细信息等操作。处于不可选状态的告警，不可以做任何操作。 说明 ● 在锁定状态下确认、清除告警，该告警不会列入到历史告警列表，解锁后才会更新到历史列表中。 ● 可选状态：可选中告警，且在勾选框中可以选择。 ● 不可选状态：不可勾选该告警，且勾选框处于灰化状态。
解锁	在窗口中单击“解锁”，系统会自动上报告警到当前列表中。
搜索	在窗口中支持两种搜索方式： ● 不设置任何条件直接单击“刷新”，在当前列表中显示所有告警。 ● 当窗口处于锁定状态时，在“选择搜索范围”下拉菜单中选择搜索范围，单击“搜索”。
告警确认	在窗口中选中一条或多条告警，单击“确认”。 说明 ● 已确认告警：在“确认用户”栏中显示确认用户。 ● 未确认告警：在“确认用户”栏中显示.
告警反确认	在窗口中选中一条或多条告警，选择“更多 > 反确认”。 说明 通过反确认后，告警由确认状态变成未确认状态。

操作名称	操作方法
告警清除	在窗口中选中一条或多条未清除的告警，单击“清除”。 说明 ● 已清除告警：告警背景颜色为绿色。 ● 未清除告警：告警背景颜色为白色。
告警屏蔽	1. 在窗口中选中一条告警，在操作栏中单击  图标，选择“屏蔽”。 2. 在“屏蔽告警”对话框中设置规则名称、屏蔽时间和定位信息，单击“确定”。 说明 ● 在当前告警窗口中，新增的告警屏蔽规则默认为启用状态。 ● 屏蔽规则只对屏蔽规则启用且处于生效期间上报的告警生效。屏蔽规则对屏蔽规则设置前上报的告警不生效。 ● 性能告警和已清除的告警不可以设置屏蔽规则。
拓扑定位	在窗口中选择一条告警，在操作栏中单击  。 说明 eSight 将该告警记录定位到拓扑视图中产生告警的对象。
查看告警详细信息	在窗口中选择需要查看的告警，单击该“告警名称”。 在“告警详情”对话框中显示了所选告警的名称、告警可能原因和修复建议等信息。
查看告警日志信息	在窗口中选择需要查看的告警，单击该“告警次数”。 在“告警日志信息”对话框中显示了与该条记录相关的告警日志。
导出告警信息	在窗口中选择一条或多条告警，单击“导出 > 导出选中”，导出选择告警的相关信息。 如果需要导出全部可以直接单击“导出 > 导出全部”。

----结束

8.2.4 查看性能状态

通过查看性能状态，了解网元当前的性能相关信息。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“查看 > 性能状态”。

步骤 3 可选: 在相应性能标题右侧单击  定制性能属性。

----结束

8.3 配置网元

通过对网元的配置方式的设置、协议参数的配置、接口及 IP 地址配置以及网元配置文件的备份与恢复，完成对网元的配置操作。

8.3.1 配置网元的 web 网管

eSight 系统集成了网元的 web 网管及智能配置工具，通过 web 网管可以对网元进行相关配置。

前提条件

网元支持 web 网管。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“配置 > web 网管”。

----结束

8.3.2 配置协议参数

实现网管与网元之间正常通信，需配置网管的协议参数。

8.3.2.1 配置网管侧网元 Telnet 参数

当网管与网元之间使用 Telnet 协议进行通信且网元侧的 Telnet 参数发生变化时，需同步设置网管侧网元的 Telnet 参数。

前提条件

要实现网管与网元的正常通信，必须保持网管与网元的 Telnet 参数配置相同。

网管上已添加设备。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“协议参数 > Telnet 参数”。

步骤 3 在右侧的窗口中配置 Telnet 的相关参数，单击“测试”，测试成功后，单击“应用”。

----结束

8.3.2.2 配置网管侧网元 SNMP 参数

当网管与网元之间使用 SNMP 协议通信且网元侧的 SNMP 参数有变化时，需要同步修改网管侧网元的 SNMP 参数。

前提条件

要实现网管与网元之间正常通信，需保证网管侧网元 SNMP 参数与网元侧一致。

网管上已添加设备。

背景信息

eSight 可通过 SNMP 协议访问被管理网元。当手动或自动创建 SNMP 网元时，eSight 使用缺省 SNMP 参数模板完成到指定网元的适配，以确定被管理网元所支持的 SNMP 协议参数。适配成功的缺省 SNMP 参数模板即成为该网元对应网管侧的 SNMP 参数配置，其后对该网元的全部管理操作都通过此 SNMP 参数进行。当网元访问协议的参数发生变化时，需要修改指定网元的访问协议参数。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的导航树上选择“协议参数 > SNMP 参数”。

步骤 3 在右侧的窗口中设置 SNMP 相关参数。

- **SNMP 协议版本**：当前支持 SNMPv1、SNMPv2c、SNMPv3 三个版本，SNMPv3 应用在通讯参数安全级别要求比较高的场景下。
- **读团体字**：网管系统在向设备发送读操作请求时候的团体名。只有与该设备认可的读团体名相同时，才能进行读操作。
- **写团体字**：网管系统在向设备发送写操作请求时候的团体名，只有与该设备认可的写团体名相同时，才能进行写操作。
- **超时时间（秒）**：网管系统在向设备发送操作请求时的等待响应的的时间。
- **重发次数**：网管系统在向设备进行一次 SNMP 参数设置过程中，超时情况下重复发送操作请求的最大次数，超过该次数即认为操作失败。
- **网元端口**：该网元的 SNMP 协议通信端口。
- **安全名**：访问设备时所使用的设备用户名。
- **上下文名称**：上下文引擎名称。
- **上下文引擎**：代表一个 SNMP 引擎的管理性唯一标识符。和环境名称一起使用唯一地标识一个 SNMP 实体的环境，只有发送端的环境和接收端的环境完全匹配才对 SNMP 消息包进行处理，否则 SNMP 消息包被丢弃。
- **鉴权协议**：用于消息验证时采用的协议。可选择 HMACMD5、HMACSHA 协议或不使用协议。选择了 HMACMD5 或 HMACSHA 协议时，需要设置授权认证密码。
- **私有协议**：数据封装时所采用的加密协议。可选择 DES、AES 加密协议或不加密。选择了 DES 或 AES 加密协议时需要设置加密密码。

步骤 4 单击“测试”，测试成功后，单击“应用”。

----结束

8.3.3 接口管理

用户在管理设备的时候，需要了解设备的接口基本信息和状态。

8.3.3.1 了解接口

介绍接口的相关重要参数。

属性	说明
速率（bps）	接口对经过自身的数据报文处理速率。
管理状态	表示接口的物理状态，用户是否关闭接口。
运行状态	表示接口的逻辑状态，是端口的管理态和协议状态的交集，其中任一状态为 down，接口运行态即为 down。

8.3.3.2 配置接口

可以对接口进行激活/去激活和修改接口别名的操作。

前提条件

已配置 SNMP 写权限。

操作步骤

- 步骤 1

在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2

在左侧导航树单击“设备配置 > 接口管理”。
- 步骤 3

单击“同步”，弹出“同步进度”对话框，待同步任务完成后，单击“确定”。
- 步骤 4



配置接口相关参数。

说明

在设置接口别名时，建议使用英文别名，部分网元接口别名不支持设置为空。
- 步骤 5

可同时选中多个端口，单击“启用”、“禁用”、“禁止上报告警”或“恢复上报告警”批量操作。

说明

设置了禁止上报告警的接口，该接口监控的告警均不上报网管。
仅 S 系列的交换机支持告警的禁止上报和恢复上报操作。
- 结束

8.3.3.3 查询接口参数

网管支持接口信息查询。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧导航树单击“设备配置 > 接口管理”。
- 步骤 3** 在窗口上方设置过滤参数，单击“搜索”。
- 步骤 4** 在下方的窗格中查看接口相关参数。

----结束

8.3.4 查询 IP 地址

在进行业务配置及网络规划时，需要查询网元及其接口的 IP 地址，eSight 支持对网元的 IP 地址以及接口的 IP 地址进行查询。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧导航树单击“设备配置 > IP 地址管理”。
- 步骤 3** 单击“同步”，待同步结束，在“同步进度”窗口中查看详细信息，单击“确定”，将设备上的 IP 地址参数同步到网管上。
- 步骤 4** 在窗口上方设置过滤参数，单击“搜索”。在下方的窗格中查看 IP 地址的相关参数。

----结束

8.3.5 配置文件管理

eSight 支持将网元的配置文件进行恢复，当配置文件数据遭到破坏时，可以通过恢复操作，对网元上的配置文件进行保护。

前提条件

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧导航树选择“设备配置 > 配置文件”。
- 步骤 3** 在“操作”下单击“恢复”执行恢复操作。

----结束

后续处理

备份配置文件请参见 [11.3.2 手工备份网元配置数据](#)。

9 业务管理

关于本章

eSight 提供对 WLAN、IPSec VPN、SLA、BGP/MPLS VPN 业务管理。

9.1 IPSec VPN 监控管理

eSight 支持对 IPSec VPN（IP Security VPN）的监控管理，包括同步网络域隧道、查看网络域详细信息（隧道列表、网络域拓扑）。

9.2 WLAN 管理

本节介绍 WLAN（Wireless Local Area Network）的基本概念和配置方法。

9.3 BGP/MPLS VPN 管理

本节介绍 eSight 对 BGP/MPLS VPN（Border Gate Protocol Multi protocol Label Switch VPN）业务管理的基本概念、主要功能和典型配置示例。

9.4 SLA 管理

eSight 支持对 SLA 的监控和管理，包括 SLA 概述、SLA 服务、SLA 任务和快速诊断。

9.1 IPSec VPN 监控管理

eSight 支持对 IPSec VPN（IP Security VPN）的监控管理，包括同步网络域隧道、查看网络域详细信息（隧道列表、网络域拓扑）。

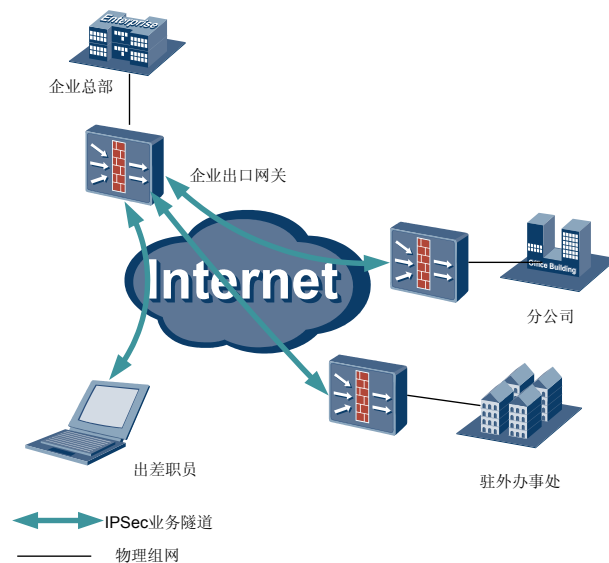
9.1.1 IPSec VPN 应用

IPSec VPN 为处于不同物理地域的企业和用户提供了建立安全通信隧道的方式，防止数据在通过公网传输时被非法查看或篡改。

随着 Internet 的迅速发展，越来越多的公司和个人利用互联网来进行通信。当分布于不同地域的企业或个人通过 Internet 进行通信时，由于处于不同的物理地域，它们之间进行通信的绝大部分流量都需要穿越 Internet 上的未知网络，无法保证在网络上发送和接收数据的安全性。IPSec 提供了一种建立和管理安全隧道的方式，通过对要传输的数据报文提供认证和加密服务来防止数据通过公网传输时被非法查看或篡改，相当于为位于不同地域的用户创建了一条安全的通信隧道。

如图 9-1 所示，企业中心和企业各分部通过 Internet 实现网络互通，可以在公司总部的出口网关与分公司的出口网关、驻外办事处的出口网关之间建立 IPSec VPN 隧道，出差职员也可以通过 PC 直接发起 IPSec VPN 隧道接入公司总部的出口网关。企业所有用户的异地互访数据流都通过安全的 IPSec VPN 隧道来承载，虽然是在公网上传输，但都得到了加密和认证保护，保证了数据传输的安全性。

图 9-1 IPSec VPN 典型应用场景

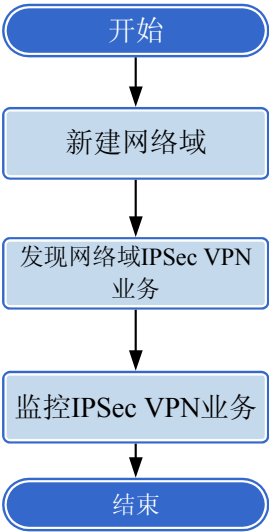


9.1.2 IPSec VPN 操作全景图

通过 IPSec VPN 操作全景图可以了解 IPSec VPN 监控管理的所有操作，并根据实际情况，选择相应操作。

IPSec VPN 操作全景图，如图 1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 9-2 IPSec VPN 操作全景图



IPSec VPN 操作的简要说明如表 9-1 所示。

表 9-1 操作简要说明

操作		说明
新建网络域		用户可以对某一区域的 IPSec VPN 业务进行集中管理，需要新建一个网络域，然后根据管理的需求，在网络域中新增设备。
发现网络域 IPSec VPN 业务		用户创建网络域之后，需要将设备上的隧道信息同步到 eSight，便于网管对隧道的连通性进行监控。
监控 IPSec VPN 业务	查看 IPSec VPN 业务拓扑结构	用户在 eSight 执行查看网络域的拓扑结构操作，可以在拓扑图展示了当前网络域的节点之间的隧道以及隧道的状态信息。
	查看 IPSec VPN 业务运行状态	对 IPSec VPN 业务进行维护时，需要定时查看其运行状态。

9.1.3 新建网络域

用户可以对某一区域的 IPSec VPN 业务进行集中管理，需要新建一个网络域，然后根据管理的需求，在网络域中新增设备。

操作步骤

- 步骤 1 在主菜单中选择“网络应用 > IPSec VPN 业务管理”。
- 步骤 2 在基本信息窗格，单击“新建”。

步骤 3 在弹出的窗口中，设置“网络域名称”和“网络域描述”。

步骤 4 在网元列表中单击“创建”，选择网元，单击“确定”。

----结束

9.1.4 发现网络域 IPsec VPN 业务

用户创建网络域之后，需要将设备上的隧道信息同步到 eSight，便于网管对隧道的连通性进行监控。

前提条件

已配置网管侧及网元侧的 Telnet 参数。

操作步骤

步骤 1 在主菜单中选择“网络应用 > IPsec VPN 业务管理”。

步骤 2 在左侧导航树中选择“IPsec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPsec VPN 业务的网络域。

步骤 3 单击“同步”，将设备上的 IPsec VPN 隧道同步到 eSight。

----结束

9.1.5 监控 IPsec VPN 业务

介绍对 IPsec VPN 网络域性能的监控操作。

9.1.5.1 查看 IPsec VPN 业务拓扑结构

用户在 eSight 执行查看网络域的拓扑结构操作，可以在拓扑图展示了当前网络域的节点之间的隧道以及隧道的状态信息。

操作步骤

步骤 1 在主菜单中选择“网络应用 > IPsec VPN 业务管理”。

步骤 2 在左侧导航树中选择“IPsec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPsec VPN 业务的网络域。

步骤 3 在“隧道拓扑”窗格中查看 IPsec VPN 业务的拓扑信息。

拓扑上用颜色区分隧道的连通性状态。

- 绿色表示连通
- 红色表示未连通

----结束

9.1.5.2 查看 IPsec VPN 业务运行状态

对 IPsec VPN 业务进行维护时，需要定时查看其运行状态。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > IPsec VPN 业务管理”。
- 步骤 2** 在左侧导航树中选择“IPsec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPsec VPN 业务的网络域。
- 步骤 3** 可选：单击“同步”，将设备上的 IPsec VPN 隧道同步到 eSight。
- 步骤 4** 在“隧道列表”中查看“隧道状态”的值。

----结束

9.2 WLAN 管理

本节介绍 WLAN（Wireless Local Area Network）的基本概念和配置方法。

9.2.1 WLAN 基本概念

WLAN（Wireless Local Area Network）无线局域网是指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。

无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。和传统的有线接入方式相比，无线局域网的启动和实施相对简单，维护的成本低廉，一般只要安放一个或多个接入点设备就可建立覆盖整个建筑或地区的局域网络。WLAN 以无线多址信道作为传输媒介，利用电磁波完成数据交互，实现传统有线局域网的功能。WLAN 技术现在已经广泛的应用在商务区，大学，机场，及其他公共区域。

WLAN 中的相关概念

- AP（Access Point）接入点：提供无线工作站到局域网的桥接功能，提供无线到有线和有线到无线的帧转换。
- 瘦 AP（FIT AP）：也叫集中控制型 AP，不能独立工作，需要与 AC 配合完成 WLAN 业务接入功能。
- AC（Access Controller）无线控制器：无线控制器对无线局域网中的所有 AP 进行控制和管理。无线控制器还可以通过同认证服务器交互信息，来为 WLAN 用户提供认证服务。
- CAPWAP（Control And Provisioning of Wireless Access Points）无线接入点控制协议：是 AP 与 AC 之间传输管理报文和数据报文的隧道。
- SSID（Service Set Identifier，服务组合识别码）：无线终端可以先扫描所有网络，然后选择特定的 SSID 接入某个指定无线网络。
- VAP（virtual Access Point，虚拟接入点）：VAP 是 AP 上的业务功能实体。用户可以在 AP 的每个射频上创建不同的 VAP，通过为 AP 的指定射频绑定服务集，就可以创建 VAP。

9.2.2 WLAN 的组网方案及原理介绍

WLAN 的组网方案主要有瘦 AP+AC 直连式组网、瘦 AP+AC 旁挂式组网。

瘦 AP+AC 直连式组网

直连式组网是指 AC 挂在 BRAS 下面，AP 的数据业务和管理业务都由 AC 集中转发和处理。在直连式组网模式下，AC 需具有很强的转发能力，能胜任汇聚层功能。适用于大规模集中部署的 WLAN 网络，并可以简化网络架构。

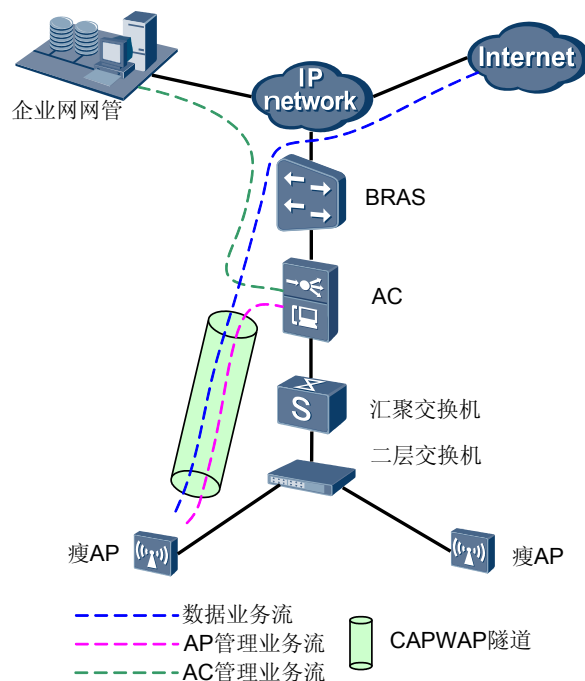
直连式组网方案中，AP 和 AC 建立 CAPWAP 隧道，管理流必须封装在 CAPWAP 隧道中，数据业务流可以选择是否封装在 CAPWAP 隧道中。

根据数据业务是否封装在 CAPWAP 隧道中，有两种配置场景：

- 数据业务流封装在 CAPWAP 隧道中

所有的管理流和数据业务流均要封装在 CAPWAP 协议的隧道中，包括所有的 AP 管理流、终端用户数据流等。如图 9-3 所示，所有数据业务流和 AP 管理流都通过 CAPWAP 封装，用不同的 VLAN 区分业务流。

图 9-3 数据业务流封装在 CAPWAP 隧道

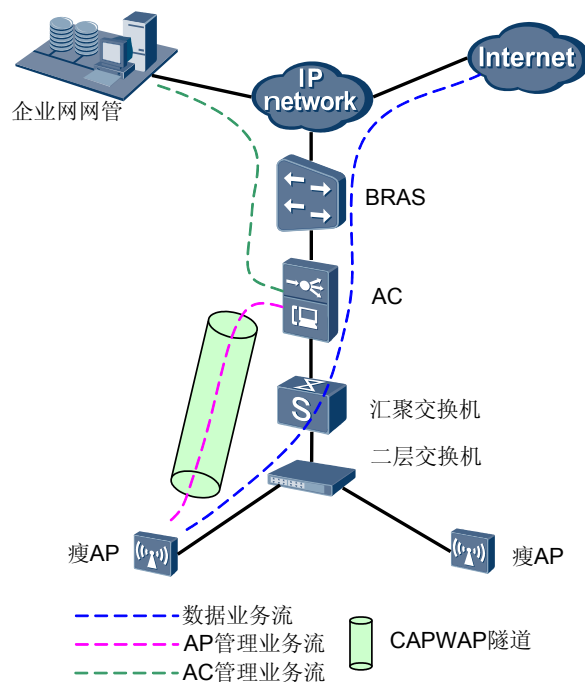


在这种方式下，只需预先在交换机配置管理 VLAN，无需配置数据 VLAN。AP 管理 VLAN 用于 AP 与 AC 间的对接。

- 数据业务流不封装在 CAPWAP 隧道中

AP 的管理流封装在 CAPWAP 协议的隧道中，而 AP 的数据业务流不封装在 CAPWAP 的协议隧道中，直接由 AP 发送到 AC，再由 AC 转发至上层设备中。如图 9-4 所示，所有数据业务流不使用 CAPWAP 隧道封装，通过 AC 转发至上层设备，AP 管理流使用 CAPWAP 隧道封装，用不同的 VLAN 区分业务流。

图 9-4 数据业务流不封装在 CAPWAP 隧道



在这种方式下，需预先在交换机配置管理 VLAN，还需要配置数据 VLAN，用于区分不同的 WLAN 业务流。

- AP 至 AC 的交换机上，配置 AP 管理 VLAN，用于 AP 与 AC 间的对接。
- AP 至 AC 之上的交换机上，配置用户的数据 VLAN，用于区分不同的 WLAN 业务流。

瘦 AP+AC 旁挂式组网

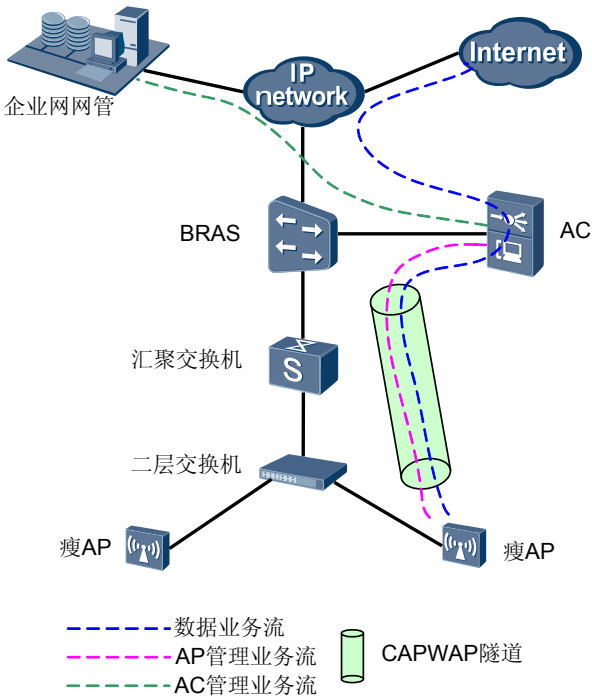
旁挂式组网是指 AC 旁挂在 BRAS 旁边，实现对 AP 的 WLAN 业务管理。在旁挂式组网模式下，BRAS 设备管辖范围内部署的 AP 都由 BRAS 旁挂的 AC 管理，AC 部署相对集中，适合于 AP 比较分散的全城热点部署的组网应用。

根据数据业务是否封装在 CAPWAP 隧道中，有两种配置场景：

- 数据业务封装在 CAPWAP 隧道中

所有的管理流和数据业务流均要封装在 CAPWAP 协议的隧道中，包括所有的 AP 管理流、终端用户数据流等。如图 9-5 所示，所有数据流和 AP 管理流都通过 CAPWAP 封装，用不同的 VLAN 区分业务流。

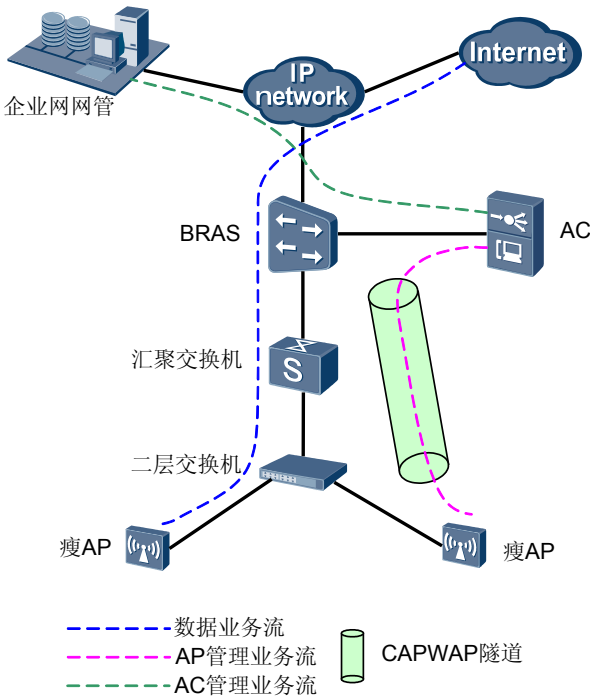
图 9-5 数据业务流封装在 CAPWAP 隧道



在这种方式下，只需预先在交换机配置管理 VLAN，无需配置数据 VLAN。AP 管理 VLAN 用于 AP 与 AC 间的对接。

- 数据业务不封装在 CAPWAP 隧道中
AC 只承载对 AP 的管理功能，管理流封装在 CAPWAP 隧道中传输。数据业务流不经过 AC，直接转发，经汇聚交换机由 BRAS 设备传输至上层网络。组网图如图 9-6 所示。

图 9-6 数据业务不封装在 CAPWAP 隧道中



- AC 旁挂在 BRAS 旁边，仅完成对 AP 的管理。所有的 AP 管理流必须全部到达 AC。

BRAS 启动 DHCP Server 功能给 AP 分配 IP 地址，AP 通过 DNS 或 DHCP Option43/option60 的方式发现 AC。或者是，AC 作为 AP 的 DHCP 服务器，直接为 AP 分配 IP 地址，AP 接入的 VLAN 对应的 VLANIF 使能 DHCP Server 功能。

- AP 的数据业务流不经过 AC，直接本地转发。

终端用户可根据不同的 SSID 配置不同的业务 VLAN，配置二层交换机和汇聚交换机识别这些业务 VLAN，转发到上层 BRAS 上，业务 VLAN 由 BRAS 终结，由 BRAS 对终端用户进行接入控制和 IP 地址的分配等。根据认证方式对用户进行身份验证，验证通过后，用户报文可以进入 Internet 网络。

AC 直连、旁挂组网方案对比

AC 的组网方式可以直连在 BRAS 下面，也可以挂在 BRAS 旁边，主要特性区别如表 9-2 所示。

表 9-2 AC 直连、旁挂组网方案对比

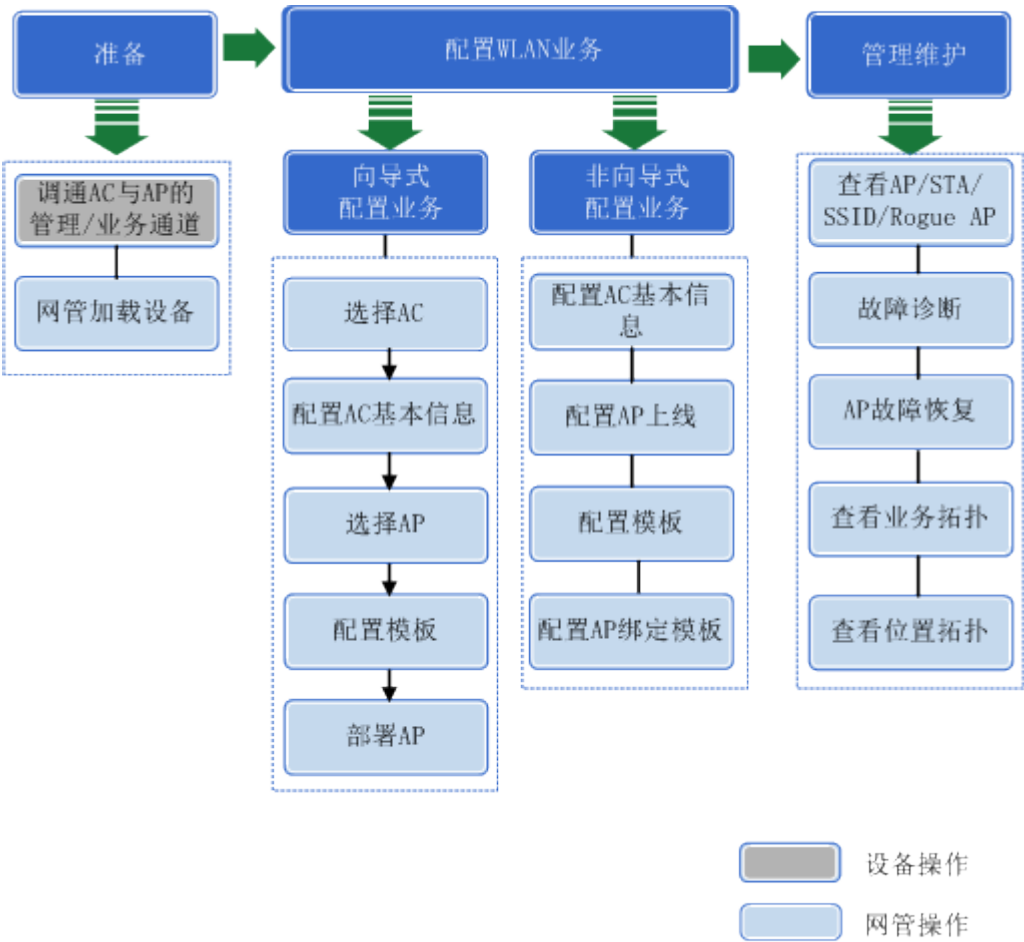
对比项	AC 直连组网方案	AC 旁挂组网方案
实现方式	直连式组网是指 AC 挂在 BRAS 下面，AP 的数据业务和管理业务都由 AC 集中转发和处理。	旁挂式组网是指 AC 旁挂在 BRAS 旁边，实现对 AP 的 WLAN 业务管理。

对比项	AC 直连组网方案	AC 旁挂组网方案
适用场景	AC 需具有很强的转发能力，能胜任汇聚层功能。适用于大规模集中部署的 WLAN 网络，并可以简化网络架构。	BRAS 设备管辖范围内部署的 AP 都由 BRAS 旁挂的 AC 管理，AC 部署相对集中，适合于 AP 比较分散的全城热点部署的组网应用。

9.2.3 WLAN 功能全景图

介绍 WLAN 配置全景图，根据实际情况选择操作方式。
WLAN 功能全景图如图 9-7 所示。

图 9-7 WLAN 配置全景图



WLAN 业务功能操作详细描述如表 9-3 所示。

表 9-3 WLAN 配置流程

阶段	操作说明
准备	准备阶段的操作，是网管配置管理 WLAN 业务的前提。 ● 调通 AC 与 AP 之间的管理/业务通道，需要在设备上配置。 ● 网管加载设备，将 AC 设备添加到网管上。
配置 WLAN 业务	向导式配置 WLAN 业务给出了配置 WLAN 业务的完整步骤。 非向导式配置 WLAN 业务的步骤： 1. 配置 AC 基本信息：创建 AC 并配置 AC 的接口，认证方式和转发类型。 2. 配置 AP 上线：添加 AP 到网管上。 3. 配置模板：配置 AP 模板、射频模板和 ESS 模板。 4. 配置 AP 绑定模板：将模板绑定到 AP 上，完成对 AP 的业务配置。
管理维护 WLAN 业务	● 查看 AP/STA/SSID/Rogue AP: eSight 提供浏览全网的 AP、STA、SSID 和 Rogue AP 的详细信息。 ● 故障诊断: eSight 提供故障诊断能力，有效定位业务的故障点。 ● AP 故障恢复: eSight 提供对 AP 进行恢复出厂配置，重启和替换 AP 操作，快速完成故障恢复。 ● 查看业务拓扑: 通过查看 WLAN 的业务拓扑，可了解 WLAN 业务中 AC 与 AP、非法 AP、终端用户信息之间的逻辑关系。 ● 查看位置拓扑: 通过位置拓扑，可以查看当前信号的覆盖范围、设备的当前状态，同时可根据网络环境的实际情况，在位置拓扑中构建出虚拟的仿真网络环境，便于日常维护和查看。

9.2.4 WLAN 配置任务

介绍完成 WLAN 业务配置管理的相关操作任务。

9.2.4.1 向导式配置 WLAN 业务

向导式配置 WLAN 业务包含了 WLAN 业务的完整配置步骤，有效指导用户配置 WLAN 业务。

前提条件

- 已在网管中创建 AC 设备。
- AP 和 AC 之间网络连接正常。
- 已配置 SNMP 读写权限。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“业务管理 > 配置向导”。

步骤 3 选择 AC，选中相应的 AC，单击“下一步”。

 说明

- 选中 AC 后，可单击“同步”，使网管与现网中 WLAN 业务保持一致。
- 网管添加 AP 采用批量导入的方式时，可单击“下载规划表单”，将待导入的 AP 设备相关信息填写到规划表单中。

步骤 4 配置 AC 基本属性，配置 AC 的“接口名称”、“AP 认证方式”、“转发类型”。

- “转发类型”为“ESS”时，AP 将以在绑定的 ESS 模板中设置的用户数据作为转发模式，转发用户数据。
- “转发类型”为“AP”时，AP 将以自定义设置的用户数据作为转发模式，转发用户数据。

 说明

如果系统中存在已确认的 AP，将不能修改 AC 的基本属性。

步骤 5 选择 AP。单击“增加 AP”，选择相应的 AP，单击“确定”。单击“下一步”。

 说明

同时支持以下两种增加 AP 的方式：

- 可单击“新增 AP 设备 > 离线创建”，离线创建 AP 设备。
- 可单击“新增 AP 设备 > 批量导入”，使用 AP 规划表单批量创建 AP 设备。

步骤 6 配置模板。分别配置 AP 模板、射频配置及 ESS 模板，将其绑定到 AP 上，单击“下一步”。

 说明

一个 AP 上可配置多个 ESS 模板。

步骤 7 可选：选中“加入白名单”，单击“部署”。

步骤 8 待业务部署完成后，单击“完成”。

----结束

9.2.4.2 配置 AC 基本信息

配置 AC 基本信息，为网管加载 AP 做好准备。

前提条件

已配置 SNMP 写权限。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”。

步骤 3 在右侧的窗口中，单击“创建”，在弹出的窗口中，单击“选择”，在弹出窗口中选择 AC 设备，单击“确定”，新建 AC 设备。

 说明

当选择的 AC 设备是 SPU 的类型时，如果 AC 设备不是运行 WLAN 业务，则创建不会成功。

步骤 4 在“创建”窗口中，单击“确定”，AC 创建成功。

步骤 5 单击设置 AC 的基本参数。

步骤 6 在“接口名称”后单击“选择”，选择相应接口，单击“确定”。

 说明

WS6603 不支持配置接口。

步骤 7 配置“AP 认证方式”和“转发类型”参数。

 说明

当 AP 认证方式设置为“不认证”，AP 将自动上线。

当 AP 认证方式设置为“MAC”或“SN”时，用户需要手工导入 AP 设备、离线创建 AP、在白名单中增加 AP 的 MAC 或 SN、在未授权 AP 中对 AP 进行上线确认。

转发类型为 ESS 时，AP 以其绑定的 ESS 模板设置的用户数据转发模式转发数据。

转发类型为 AP 时，AP 以其设置的数据转发模式转发数据。

----结束

后续处理

配置完 AC 后，可单击相应 AC 的“名称”，在弹出的“AC 基本信息”窗口中查看 AC 的相关信息。

9.2.4.3 配置 AP 上线

配置 AC 设备管理的 AP 上线，可以通过离线添加、白名单添加和手工确认未授权 AP 方式配置 AP 上线。

前提条件

已配置相关 VLAN。

已配置 AC 设备基本功能。

AP 和 AC 之间网络连接正常。

已配置 AC 设备上报告警到网管服务器。

已配置 SNMP 写权限。

背景信息

AP 上线的一般流程如下：

- 如果某 AP 已经离线添加，则该 AP 可以直接上线。
- 如果没有离线添加 AP，但 AP 的认证模式为“不认证”，或者 AP 的 MAC 或 SN 在已设置的“白名单”中，则该 AP 可以自动添加并上线。
- 如果 AP 设备不存在于白名单或 AP 列表中，且其认证模式非“不认证”情况下，则该 AP 设备存在于未认证 AP 列表之中。可通过确认未认证 AP 列表中的 AP 设备方式添加 AP 设备。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”。

有根据现网的情况分别参考[离线添加 AP](#)、[白名单上添加 AP](#)或[确认未授权 AP](#)选择配置 AP 上线的方式。

步骤 3 离线添加 AP。

1. 在右侧窗口中对应的“操作”下单击，单击“创建”。
2. 配置 AP 相关参数。
 - 在“AP 域”或“AP 模板”后单击选择，设置其参数。
 - 在“射频模板”和“ESS 模板”后单击“绑定”，分别绑定对应的模板。
 - 单击“确定”。

步骤 4 白名单上添加 AP。

1. 在右侧窗口中对应的“操作”下单击“更多 > AP 白名单”。
2. 单击“创建”，设置 AP 的“MAC”或“SN”，单击“确定”。

步骤 5 确认未授权 AP。

1. 在右侧窗口中对应的“操作”下单击“更多 > 未授权 AP”。
2. 在选中未授权 AP，单击“上线确认”。

----结束

9.2.4.4 配置 AP 模板

AP 模板是对 AP 配置的集合，网管会自动为 AP 绑定默认的 AP 模板，用户可以根据需要修改 AP 绑定的 AP 模板。

前提条件

已配置 SNMP 写权限。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中对应的“操作”下单击“更多 > AP 模板”。

步骤 3 单击“创建”，在弹出的窗口中设置 AP 模板相关参数。

步骤 4 单击“确定”，新增 AP 模板在列表中显示。

 说明

可单击  修改 AP 模板的相关参数。

----结束

9.2.4.5 配置射频模板

AP 设备与客户端设备之间通过无线频道进行通信，配置射频模板绑定到 AP 设备上，使 AP 设备可以正常工作，而不受干扰。

前提条件

已配置 SNMP 写权限。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中对应的“操作”下单击“更多 > 射频模板”。

步骤 3 单击“创建”，在弹出的窗口中设置射频模板相关参数。

- 信道管理模式设置为自动，AP 将自动选择未使用过的信道。当在同一区域中有多个接入点时，相邻接入点设置的信道至少间隔 5 个信道，以避免互相干扰。
- 功率管理模式设置为自动，AP 将自动选择发射功率，发射功率越高，传输距离就越远。功率选择不只是覆盖范围和支持最多客户端数的平衡，它还应考虑到在同一区域内不会影响到其他无线设备。
- 速率值：接入点可支持的最大数据速率。最大传输距离会受到数据速率的影响。越低的数据速率，则越远的数据传输距离。

步骤 4 单击“确定”，新增射频模板在列表中显示。

 说明

可单击  修改射频模板的相关参数。

----结束

9.2.4.6 配置 ESS 模板

ESS（Extended Service Set）扩展服务集是一类业务参数的集合，当它被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP(virtual Access Point)虚拟接入点，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

前提条件

已配置 SNMP 写权限。

仅支持创建 32 个 ESS 模板。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中对应的“操作”下单击“更多 > ESS 模板”。

步骤 3 单击“创建”，在弹出的窗口中设置 ESS 模板相关参数。

- 最大用户数：ESS 模板绑定到的射频上可以接入的最大用户数据。
- 关联超时时间：AP 发送无线的报文让区域内 STA 感应到有无无线网络连接，STA 接收到 AP 发的报文后，回应请求连接报文。报文交互过程需要的时间就是关联时间，若关联时间超过设定的值，则关联没有建立。
- SSID 隐藏：若设置隐藏 SSID，则客户端需要输入接入 AP 的 SSID 才能上线。

步骤 4 单击“确定”，新增 ESS 模板在列表中显示。

 说明

可单击  修改 ESS 模板的相关参数。

----结束

9.2.4.7 配置 AP 域

新建 AP 域，将 AP 增加到对应的 AP 域上，便于对 AP 进行集中管理。

前提条件

已配置 SNMP 写权限。

背景信息

- 1 个 AP 只能且必须加入 1 个 AP 域才能正常上线。
- 系统缺省存在 1 个 AP 域，当 AP 上线自动确认时，将自动加入缺省域。用户可以指定任何一个已存在的 AP 域为缺省域。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中对应的“操作”下单击“更多 > AP 域”。

步骤 3 单击“创建”，在弹出的窗口中设置 AP 域的相关参数。

布放类型取值原则如下。

- 离散布放:表示域中 AP 的布放非常独立，AP 间信号无任何干扰，此时相当于一个 AP 就是一个域，如果为每个这样的 AP 都创建一个域，用户配置将非常繁琐，因此可以创建一个特殊的域来包含所有的这类 AP，这个域内的 AP 都不需要调优，每个射频都以最大发送功率工作即可。
- 普通布放: 域内各 AP 之间分布比较稀疏，为满足基本的业务需求，每个射频的发送功率要求至少达到其最大发送功率的 50%。

- 密集布放: 域内各 AP 之间分布比较密集, 为满足基本的业务需求, 每个射频的发送功率最小可以只达到其最大发送功率的 25%。

步骤 4 单击“确定”, 新增 AP 域在列表中显示。

 说明

可单击  修改 AP 域的相关参数。

可单击  **设置默认域**, 将对应的 AP 域设置为默认 AP 域。

当该 AP 域 AP 出现大面积 AP 信号劣化时, 可单击  **射频调优**, 将 AP 域内 AP 的射频进行调优。

----结束

9.2.4.8 配置 AP 绑定的模板

通过将相关的 AP 模板、射频模板和 ESS 模板绑定对应的 AP 设备上, 完成 AP 业务的发放。

前提条件

已配置 SNMP 写权限。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”, 在右侧的窗口中单击对应的“操作”下单击  AP。

步骤 3 选择相应的 AP, 单击“绑定模板”, 弹出对话框提示批量处理绑定模板已生效的 AP, 可能会导致已上线用户下线, 单击“是”。

步骤 4 在“绑定模板”界面, 根据需要设置 AP 绑定的模板。

 说明

在绑定“射频模板”和“ESS 模板”时, 首先要配置“射频 ID”。

 窍门

某些 AP 设备可能支持多个射频, 用户根据需要可以在多个射频上分别绑定射频模板和 ESS 模板。

----结束

9.2.5 WLAN 维护任务

介绍 WLAN 维护管理相关操作任务。

9.2.5.1 查看 AC 信息

配置 WLAN 业务后, 可以查看所有 AC 基本信息、AC 管理的 AP 信息、域信息、AP 和 AC 中的告警、用户在线统计信息。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > WLAN 管理”。
- 步骤 2** 在左侧的导航树中选择“资源管理 > AC”。
- 步骤 3** 在右侧的窗口名称列中单击一个 AC 的名称，浏览该 AC 的基本信息、AC 管理的 AP 信息、域信息、AP 和 AC 中的告警、用户在线统计信息。

----结束

后续处理

系统默认提供一小时内的统计信息，每 30 分钟刷新一次。可设置不同的时间范围和刷新时间。

1. 在“用户在线统计”区域单击右上角.
2. 单击“设置”。
3. 选择“时间范围”和“刷新时间”。
4. 单击“确认”，保存设置的值。

统计图中会按照新设置的值刷新显示结果。

9.2.5.2 查看 AP 信息

配置 AP 上线后，可以通过该操作查看网管管理的所有 AP 设备信息。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > WLAN 管理”。
- 步骤 2** 在左侧的导航树中选择“资源管理 > Fit AP”。
- 步骤 3** 在右侧的窗口中单击“同步”，将 AP 设备相关信息同步到网管上。
- 步骤 4** 在“Fit AP”页签下单击 AP “名称”，查看 AP 的相关参数。

表 9-4 重要参数介绍

参数	说明
数据转发模式	● 直接转发：AP 不会对数据报文进行任何处理，发送原始报文。 ● 隧道转发：将数据报文封装在 CAPWAP 隧道中，转发到上层网络，提供报文转发的安全性。
AP 域	域是个逻辑概念，可以将一组 AP 划归在一个域里。域的划分由客户根据实际部署进行规划。 可以指定某个 AP 域为默认域，当 AP 为自动上线（即无需认证）的模式时，AP 将加入默认域。
天线选择	AP 发射信号选择天线的模式，当 AP 的信号质量不佳时，可以将当前模式修改为另一种模式。

参数	说明
信道频宽	为了避免相邻 AP 设备相互干扰，需要将相邻 AP 设备的射频信道设置为不同值。 当信道频宽为 20MHz 时，传输速率慢，但可选信道多，可以有效的避免相邻 AP 设备之间的干扰；当信道频宽为 40-MHz 和 40+MHz 时，传输速率快，但可选信道少。40-MHz 和 40+MHz 具有相同的传输速率，只是可选信道不同。
管理信道数	设置管理的信道数。 设置原则： 2.4G 频段 ● 20MHz: 1-13 ● 40MHz-minus: 5-11 ● 40MHz-plus: 1-7 5G 频段 ● 20MHz: 149, 153, 157, 161, 165 ● 40MHz-minus: 153, 161 ● 40MHz-plus: 149, 157
运行信道数	显示当前运行的信道数。 说明 在 AP 绑定的射频模板中，如果参数“信道管理模式”设置为“手动”，则“运行信道数”与“管理信道数”保持一致；如果参数“信道管理模式”设置为“自动”，则“运行信道数”由系统分配。
运行功率值	显示当前运行功率值。 说明 运行功率值决定位置拓扑中信号覆盖范围的显示。
发送功率等级	取值范围：0-15。 0 表示满功率，功率值由 AP 类型决定，数值越大，功率越低。
可用天线数	可用天线数必须小于或等于实际天线数。 关闭某些无用天线可节省电力。

----结束

9.2.5.3 浏览 STA

用户浏览当前网络中所有无线终端的信息。

背景信息

STA 是 station 的缩写，指带有无线网卡的台式电脑或便携式笔记本电脑等终端。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > WLAN 管理”。
- 步骤 2** 在左侧的导航树中选择“资源管理 > STA”。
- 步骤 3** 单击“同步”，浏览当前网络中的所有无线用户的信息。

----结束

9.2.5.4 浏览全网 SSID

SSID 可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > WLAN 管理”。
- 步骤 2** 在左侧的导航树中选择“资源管理 > SSID”。
- 步骤 3** 单击“同步”，浏览当前网络中的所有 SSID 的信息。

----结束

9.2.5.5 管理 Rogue AP

Rogue AP 即非法 AP，是未经授权加入无线网络的接入点，或不具有正确安全配置的接入点。非法 AP 可以允许非授权的网络访问，造成无线终端在不知情的情况下错误地接入到非法 AP，从而造成网络资源的浪费。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > WLAN 管理”。
- 步骤 2** 在左侧的导航树中选择“资源管理 > Rogue AP”。
- 步骤 3** 单击“同步”，浏览当前网络中的所有 Rogue AP 的信息。

概念	说明
BSSID	非法 AP 的 BSSID。BSSID 由运营商 ID +AC ID+AP ID+RF ID+WLAN ID 按照一定格式组成。
信道	接入点之间通过无线频道通信。当在同一区域中有多个接入点时，相邻接入点设置的信道至少要间隔 5 个信道，以避免互相干扰。
RSSI	（Received Signal Strength Indicator）接收信号强度指示。

----结束

9.2.5.6 查看业务拓扑

用户可以通过业务拓扑，查看 AC、AP、非法 AP 及终端用户之间的逻辑关系。

背景信息

网管上添加的 AC 设备会自动展现在业务拓扑上。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树选择“WLAN 拓扑 > WLAN 业务拓扑”。

步骤 3 查看 WLAN 的业务拓扑。



- 方法一：选中 ，单击  展开 WLAN 业务拓扑，单击  收缩 WLAN 业务拓扑。



- 方法二：双击 ，进入 WLAN 业务拓扑。

步骤 4 选中设备，单击右键选择执行相关操作。

- “同步”：将 AC 设备上的数据同步到 eSight 上。
- “查看物理拓扑”：查看 AC 设备的物理拓扑视图。
- “查看告警”：查看 AC 设备或 AP 对应的 AC 设备的告警列表视图。
- “详细信息”：查看设备的详细信息。
- “Ping”：用于检查两个网络设备间的连通性，用一个 AP 设备去 Ping 另一个网络设备。
- “查看用户”：若此 AP 设备上有用户连接，在视图中显示连接的用户。
- “隐藏用户”：在视图中隐藏与此 AP 设备连接的用户。

----结束

9.2.5.7 故障诊断

eSight 支持对 AP 与 AC 以及 AP 与 AP 之间进行连通性测试。

前提条件

执行连通性测试的 AP 或 AC 必须处于在线状态。

已正确配置 AC 的 Telnet 参数。

背景信息

Ping 用于向远端的主机发送 ping 包，检查网络主机是否可达。当需要检测网络连接是否出现故障或检查网络线路质量时，使用此功能。

Tracert 用于测试数据包从发送主机到达目的主机所经过的路由。当需要跟踪发送数据包经过的路由，检查网络故障发生在何处时，使用此功能。

当用 Ping 功能测试发现网络出现故障后，可以用 Tracert 功能定位网络何处有故障。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树选择“WLAN 拓扑 > WLAN 业务拓扑”。



步骤 3 双击 ，进入 WLAN 业务拓扑。

步骤 4 根据场景选择需要的诊断方式：

诊断方式	应用场景	操作
AP 设备上执行 Ping	● 用于检查两个网络设备间的连通性的。用一个 AP 设备去 Ping 一个网络设备。 ● 升级过程中，用于检测 AP 与 FTP 服务器的互通。	1. 选中 AP 设备，单击 ，选择“Ping”。 2. 在“AP Ping”窗口中输入目的设备的 IP 地址，单击“ping”。Ping 测试的结果展现在窗口中。
在 AP 与 AC 隧道上执行 Ping 或 Tracert	● APPing 受 AP 状态正常约束，因此提供 AC 的诊断，AC 下行 Ping，可诊断 AC 至 AP 隧道通断。 ● Ping 用于检测 AP 与 AC 隧道上是否出现故障或检查网络线路质量。 ● Tracert 用于在 Ping 功能测试发现网络出现故障后，定位网络故障所在。	1. 选中 AP 与 AC 之间隧道，单击 ，选择“Ping”或“Tracert”。 2. Ping 或 Tracert 的测试结果显示在窗口中，单击“确定”，关闭窗口。

----结束

9.2.5.8 AP 故障恢复

网络中 AP 出现配置异常、硬件故障或升级调优时，需要可对 AP 进行恢复出厂配置、替换 AP 及 AP 重启操作。

背景信息

- 恢复出厂配置：当 AP 出现配置数据异常或执行网络调优时，需批量执行该操作。
- AP 重启：当 AP 在线升级完成后或网络调优过程中，需要批量执行该操作。

- AP 替换：当网络中某个 AP 出现硬件故障时，为避免重新配置数据，用户通过配置 AP 替换快速完成 AP 的替换。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧导航树选择“资源管理 > AC”，在右侧的窗口对于的“操作”下单击  AP。
根据需要，参考执行重启 AP，恢复 AP 出厂配置或替换 AP。

步骤 3 重启 AP，选中一个或多个 AP，单击“重启”，弹出“确认”对话框提示重启 AP 会导致业务中断，单击“是”。

步骤 4 恢复 AP 出厂配置，选中一个或多个 AP，单击“恢复出厂配置”，弹出“确认”对话框提示恢复 AP 出厂配置会导致业务中断，单击“是”。

步骤 5 替换 AP，选中相应的 AP，单击 ，输入新 AP 的“SN”和“MAC”的值，单击“确定”。

----结束

9.2.5.9 查看位置拓扑

用户可以根据管理需要，创建位置拓扑，并将 AP 设备加入该位置拓扑中。通过位置拓扑，可以查看 AP 当前信号的覆盖范围、当前状态，AP 间信道是否冲突，同时可根据网络环境的实际情况，在位置拓扑中构建出虚拟的仿真网络环境，便于日常维护和查看。

操作步骤

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中，选择“WLAN 拓扑 > WLAN 位置拓扑”。

步骤 3 在右边拓扑中，单击右键选择“增加区域位置”。在弹出的对话框中设置区域位置的“名称”和“属性”，单击“确认”。

 说明

- 位置拓扑可以支持多层次的子位置拓扑，即一级位置拓扑中还可以包含子位置拓扑。支持的最大层次数为 9 层。
- 一个位置视图可以包含多个设备。

步骤 4 双击新建的区域位置图标，单击快捷图标栏中的“设置背景图”。在弹出的对话框中，选中“显示背景图”，根据网络环境的实际情况，选择合适的图片。

 说明

图片为网络物理环境的平面图，图片文件格式支持 GIF、JPG、JPEG、PNG，图片大小不能超过 2M。

步骤 5 在位置拓扑中，单击右键选择“增加 AP”，在弹出的对话框中，选择需要增加的 AP，单击“确定”。

 说明

只有在已创建的底层区域位置中，才能增加 AP。

步骤 6 在位置拓扑中，单击右键选择“设置比例尺”，设置起点和终点后，输入两点之间的实际长度，单击“确定”，完成对比例尺的初始化设置。设置完毕后，查看背景图左上角的比例尺大小，比例尺大小建议大于下表中的可用最小值。

根据 AP 个数和信号覆盖范围显示方式的不同，给出对应比例尺的可用最小值（单位为米），如表 9-5 所示。

表 9-5 比例尺最小值

AP 个数	信号强度	信号强度 (有障碍物)	速率	速率（有 障碍物）	信道（有 冲突域）	信道（有 冲突域和 障碍物）
10	0.2	10	0.2	10	40	50
20	0.2	20	0.2	20	80	90
30	0.2	40	0.2	40	100	120
40	0.2	50	0.2	50	150	160
50	0.2	60	0.2	60	200	250

 说明

如果出现设置比例尺不生效等问题，请重新打开位置拓扑或先清空浏览器缓存再重新打开位置拓扑。

- 步骤 7** 在位置拓扑中，单击右键选择“显示信号覆盖范围”，根据需要选择需要显示的模式。
- 步骤 8** 单击快捷图标栏中的“保存位置”，将位置拓扑保存。
- 步骤 9 可选：**单击快捷图标栏中的“导出图片”，将位置拓扑图导出本地保存。
- 步骤 10 可选：**单击快捷图标栏中的“打印”，将位置拓扑图打印。

----结束

右键菜单说明

操作	说明	设置
增加区域位置	可根据现网设备所在物理位置的实际情况，通过增加区域位置，将其层级关系映射到位置拓扑中。	在位置拓扑中，单击右键，选择“增加区域位置”。 说明 在位置拓扑中，增加 AP 后，将不能再增加区域位置。
设置信道颜色	可根据自己需要设置信道颜色。	在位置拓扑中，单击右键，选择“设置信道颜色”。 说明 只显示运行信道：当不选中时将显示全部的信道。

操作	说明	设置
显示信号覆盖范围	信号覆盖范围有三种显示方式：按信号强度、按速率、按信道。 说明 信号覆盖范围的显示是否正常由射频模板中的运行功率值决定。如果信号覆盖范围不能正常显示，请查看射频模板中的运行功率值是否正常。 窍门 如果要查看信道是否冲突，可按单个信道显示。	在位置拓扑中，单击右键，选择“显示信号覆盖范围”。
隐藏信号覆盖范围	将信号的覆盖范围隐藏。	在位置拓扑中，单击右键，选择“隐藏信号覆盖范围”。
设置比例尺	根据网络布局的实际大小，通过设置比例尺，可完成网络布局到位置拓扑的映射。	在位置拓扑中，单击右键，选择“设置比例尺”。 说明 在位置拓扑中初次使用比例尺，要进行初始化，目的是为了使比例尺的比例与背景图中的比例一致。
增加障碍物	通过增加障碍物，可以达到以下目的： ● 使位置拓扑图与真实的网络布局一致。 ● 控制信号的衰减。	在位置拓扑中，单击右键，选择“增加障碍物”。 说明 根据比例尺和障碍物的厚度计算得出的障碍物宽度超过 50 个像素时，将按 50 像素显示。

9.2.6 示例：WLAN 管理典型操作

通过学习本示例，您可参照示例中的步骤，独立完成 WLAN 业务的配置。

前提条件

- 已在网管中创建 AC 设备。
- AP 和 AC 之间网络连接正常。
- 已配置 SNMP 读写权限。
- 已配置 AC 的源接口。
- 已开启 AC 的 DHCP server。

场景介绍

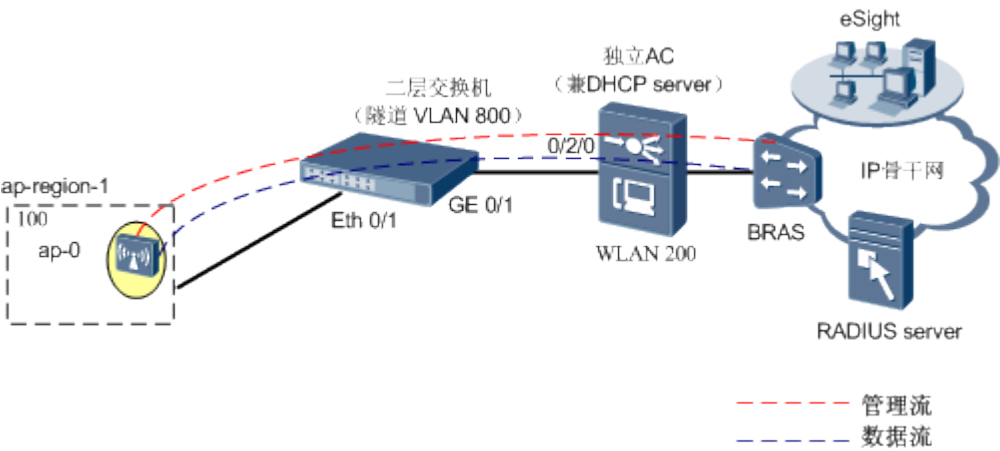
网络供应商为小区域 ap-region-1 提供 WLAN 上网服务，ap0 为 ap-region-1 提供 WLAN 业务。

组网说明

AC 和 AP 之间采用“直连式”的二层网络组网，AC 同时作为 DHCP server 给 AP 分配 IP 地址，IP 地址池中的接口为 Vlanif88。

ap-0 上业务数据采用直接转发模式。上网业务由 VLAN ID(100)分配，由 AC 转发。

图 9-8 配置组网图



数据规划

- AC 配置数据

名称	IP 地址	接口名称	类型	AP 认证方式	转发方式
WLAN200	10.137.59.200	Vlanif88	SPU	不认证	ESS

- AP 配置数据

AP 名称	SN	MAC	类型	天线选择	转发类型
ap-0	AA48005562	00-25-9E-EB-FF-D4	WA603DN	自动	直接转发模式

- AP 模板

名称	MTU	日志备份服务器 IP
ap_template	1500	10.67.38.52

- 射频配置

射频 ID	射频模板	工作状态	信道频宽	管理信道值	发送功率等级	可用天线数	ESS 模板
0	template	打开	20MHz	1	1	全部	ess_template

● 射频模板

名称	射频类型	速率模式	速率值 (Mbps)	信道管理模式	功率管理模式
template	802.11bg	自动	54	自动	自动

● ESS 模板

名称	类型	SSID	ESS 接口	VLAN ID	SSID 隐藏
ess_template	业务型	100	Wlan-Ess630	100	否

用户二层隔离	最大用户数	关联超时时间	IGMP 模式	用户数据转发模式	认证加密方式
否	32	5	关闭	直接转发	WEP 开放系统

配置流程

序号	配置步骤	配置说明
1	选择 AC	根据数据规划选择相应 AC 设备。 说明 网络中新增 AC 设备时，将其在网管上创建后，AC 设备会被自动发现到 WLAN 管理中。
2	配置 AC 基本属性	配置 AC 主要的鉴权和转发模式。
3	选择 AP	如果已经存在 AP 设备，可直接选择需要的 AP。如果不存在 AP 设备，需创建 AP 设备，创建 AP 设备的方式有两种：批量导入和离线创建。本例中采用离线创建。
4	配置模板	通过配置 AP 模板、射频模板、和 ESS 模板并将这些模板与 AP 进行绑定，完成对 AP 的业务配置。
5	部署到 AP	将已配置的业务部署到 AP。

操作步骤

步骤 1 选择 AC:

- 在主菜单中选择“网络应用 > WLAN 管理”。
- 在左侧的导航树中选择“业务管理 > 配置向导”。
- 根据数据规划表，选中名称为“WLAN200”的 AC 设备。单击“下一步”。

步骤 2 配置 AC 基本属性：根据数据规划中的 AC 配置数据，设置相应参数后，单击“下一步”。

步骤 3 选择 AP：

1. 单击“增加 AP”，在弹出的“选择 AP”窗口中，选择“新增 AP 设备 > 离线创建”。
2. 在弹出的“离线创建”窗口中，根据数据规划中的 AP 配置数据，设置相应参数后，两次单击“确定”后，完成选择 AP。单击“下一步”。

步骤 4 配置模板：

1. 根据数据规划中的 AP 模板、射频模板、ESS 模板，分别完成各模板的创建。
2. 根据数据规划中的射频配置，选择相应模板，设置相应参数后，单击“下一步”。

步骤 5 部署 AP：单击“部署”，可在“部署状态”中，查询执行状态。
部署的相关信息显示在“部署结果”中。

步骤 6 单击“完成”。

----结束

9.3 BGP/MPLS VPN 管理

本节介绍 eSight 对 BGP/MPLS VPN（Border Gate Protocol Multi protocol Label Switch VPN）业务管理的基本概念、主要功能和典型配置示例。

9.3.1 了解 BGP/MPLS VPN

BGP/MPLS VPN 是一种 L3VPN（Layer 3 Virtual Private Network）。它使用 BGP（Border Gateway Protocol）在服务提供商骨干网上发布 VPN 路由，使用 MPLS（Multi protocol Label Switch）在服务提供商骨干网上转发 VPN 报文。

企业或者业务提供商通过使用和管理 BGP/MPLS VPN 业务承载数据、语音和视频等增值业务。

9.3.1.1 基本概念

在进行 BGP/MPLS VPN 管理之前，需要了解 BGP/MPLS VPN 管理的基本概念，如 CE、PE、P 等。理解这些概念可以更快速和准确地进行 BGP/MPLS VPN 管理的操作。

基本概念请参见表 9-6。

表 9-6 基本概念

概念	说明
CE (Customer Edge)	用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE “感知”不到 VPN 的存在，也不需要支持 MPLS。

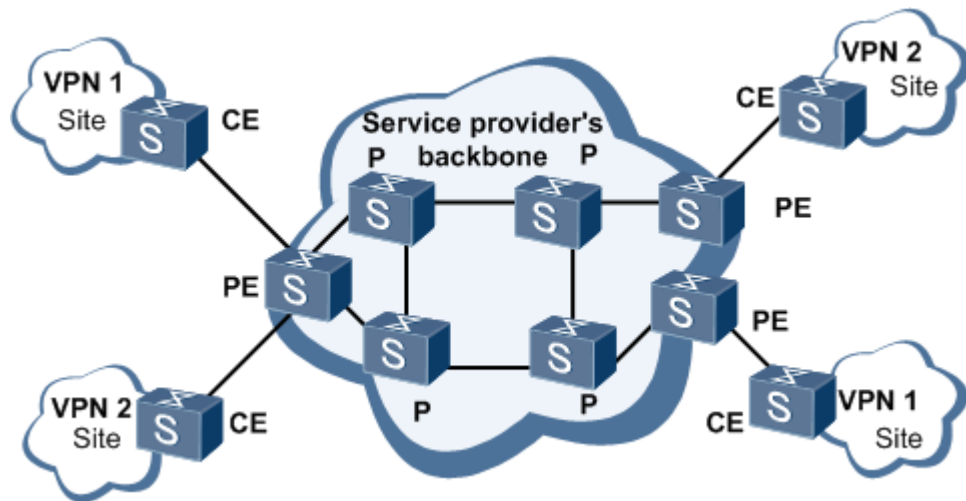
概念	说明
PE (Provider Edge)	是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上，对 PE 性能要求较高。 一台 PE 设备可以接入多台 CE 设备。一台 CE 设备也可以连接属于相同或不同服务提供商的多台 PE 设备。
P (Provider)	服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。
Site	也称为站点，是指相互之间具备 IP 连通性的一组 IP 系统，并且这组 IP 系统的 IP 连通性不需通过服务提供商网络实现。Site 是构成 VPN 的基本单元。
AS	自治系统（AS，autonomous system）是指在一个（有时是多个）实体管辖下的所有 IP 网络和路由器的全体，它们对互联网执行共同的路由策略。
VPN 实例 (VPN-instance)	也称为 VPN 路由转发表（VPN Routing and Forwarding table）。
VPN Target	实现直连 site 及远端 site 的 VPN 成员关系和路由规则控制。每个 VPN 实例关联一个或多个 VPN Target 属性（如一个 site 同属于不同的 VPN）。有两类 VPN Target 属性： ● Export Target: 本地 PE 从直接相连 site 学到 IPv4 路由后，转换为 VPN IPv4 路由，并为这些路由设置 Export Target 属性。Export Target 属性作为 BGP 的扩展团体属性随路由发布。 ● Import Target: PE 收到其它 PE 发布的 VPN-IPv4 路由时，检查其 Export Target 属性。当此属性与 PE 上某个 VPN 实例的 Import Target 匹配时，PE 就把路由加入到该 VPN 实例的路由表。 也就是说，VPN Target 属性定义了一条 VPN 路由可以为哪些 site 所接收，以及 PE 可以接收哪些 site 发送来的路由。 当收到直连 CE 传过来的路由时，PE 将该路由与一个或多个 Export Target 属性关联。Export Target 属性将和 VPN-IPv4 路由一起由 BGP 发布给其他相关的 PE。当这些相关的 PE 收到该 VPN-IPv4 路由时，将其 Export Target 属性与本设备所有的 VPN 实例的 Import Target 属性值比较。如果相等，就将该路由注入到该 VPN 路由表。

BGP/MPLS VPN 基本模型

单域和跨域的组网都是以 BGP/MPLS VPN 基本模型为基础。BGP/MPLS VPN 的基本模型由三部分组成：CE、PE 和 P。

BGP/MPLS VPN 基本模型如图 9-9 所示。

图 9-9 BGP/MPLS VPN 基本模型



9.3.1.2 功能

BGP/MPLS VPN 管理组件提供了网络的自动发现、业务监控（业务信息查看、业务拓扑展现、性能管理、报表管理、业务质量审计）和故障定位等功能，支持华为全系列路由器、交换机和主流的非华为设备。

- 自动发现：对于网络中已经运行的业务提供自动发现功能，快速将现网的业务发现到网管中，进行统一的管理、监控。
- 业务监控：可以通过各种方法监控业务的运行状态和质量，包括查看业务拓扑、监控业务性能、查看业务报表及审计业务质量等。
- 故障定位：包括告警查看和故障诊断。告警查看，在业务拓扑和业务列表中集中显示。故障诊断，用户根据选定的业务或者在拓扑界面上选择链路生成诊断任务，显示检测结果，主要用于检测网络连通性和定位故障。

9.3.1.3 应用场景

BGP/MPLS VPN 的组网主要有单域和跨域两类组网方式。

单域组网主要包括：

- Full-Mesh
- Hub-Spoke
- MCE
- HoVPN

跨域组网主要包括：

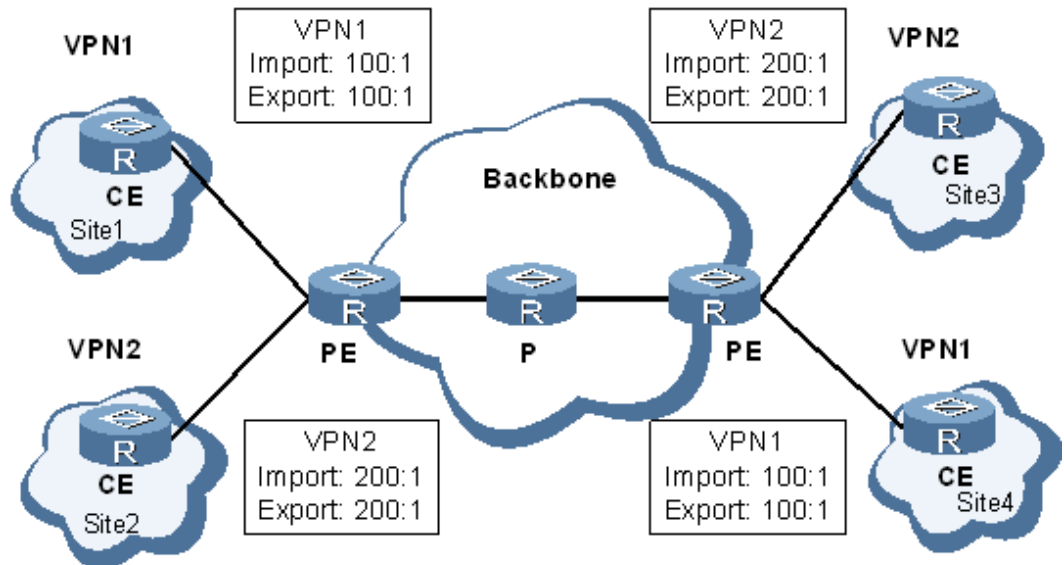
- 跨域 VPN-OptionA
- 跨域 VPN-OptionB

Full-Mesh 组网

一个 VPN 中的所有用户形成闭合用户群，相互之间能够进行流量转发，VPN 中的用户不能与任何本 VPN 以外的用户通信。需要为每个 VPN 分配一个 VPN Target，作为该 VPN 的 Export Target 和 Import Target，并且此 VPN Target 不能被其他 VPN 使用。

Full-Mesh 组网如图 9-10 所示。

图 9-10 Full-Mesh 组网



Hub-Spoke 组网

如果希望在 VPN 中设置中心访问控制设备，其它用户的互访都通过中心访问控制设备进行，可以使用 Hub-Spoke 组网方案。其中，中心访问控制设备所在站点称为 Hub 站点，其他用户站点称为 Spoke 站点。Hub 站点侧接入 VPN 骨干网的设备叫 Hub-CE；Spoke 站点侧接入 VPN 骨干网的设备叫 Spoke-CE。VPN 骨干网侧接入 Hub 站点的设备叫 Hub-PE，接入 Spoke 站点的设备叫 Spoke-PE。

Spoke 站点需要把路由发布给 Hub 站点，再通过 Hub 站点发布给其他 Spoke 站点。Spoke 站点之间不直接发布路由。Hub 站点对 Spoke 站点之间的通讯进行集中控制。

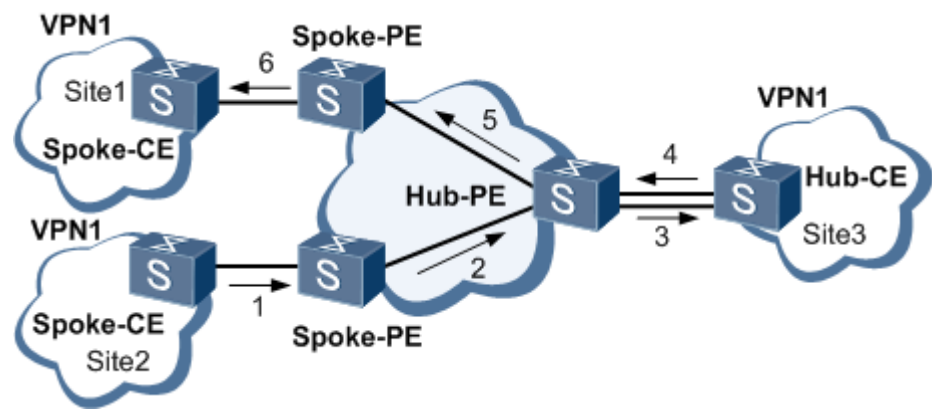
对于这种组网情况，需要设置两个 VPN Target，一个表示“Hub”，另一个表示“Spoke”。

各 site 在 PE 上的 VPN 实例的 VPN Target 设置规则为：

- 连接 Spoke 站点的 PE（Spoke-PE）：Export Target 为“Spoke”，Import Target 为“Hub”，任意 Spoke-PE 的 Import Route Target 属性不与其它 Spoke-PE 的 Export Route Target 属性相同；
- 连接 Hub 站点的 PE（Hub-PE）：Hub-PE 上需要使用两个接口或子接口，一个用于接收 Spoke-PE 发来的路由，其 VPN 实例的 Import Target 为“Spoke”；另一个用于向 Spoke-PE 发布路由，其 VPN 实例的 Export Target 为“Hub”。

Hub-Spoke 组网如图 9-11 所示。

图 9-11 Hub-Spoke 组网



MCE 组网

传统的 BGP/MPLS IP VPN 架构要求每个 VPN 实例单独使用一个 CE 与 PE 相连。

随着用户业务的不断细化和安全需求的提高，一个私有网络内的用户需要划分成多个 VPN，不同 VPN 用户间的业务需要完全隔离。通过建立 MCE 的组网方式，使用多 VPN 实例的 CE 设备（MCE：Multi-VPN-Instance CE ）允许多个 VPN 同时接入，实现不同业务或用户的隔离。

该组网中，PE 与传统的没有区别，主要实现如下能力：

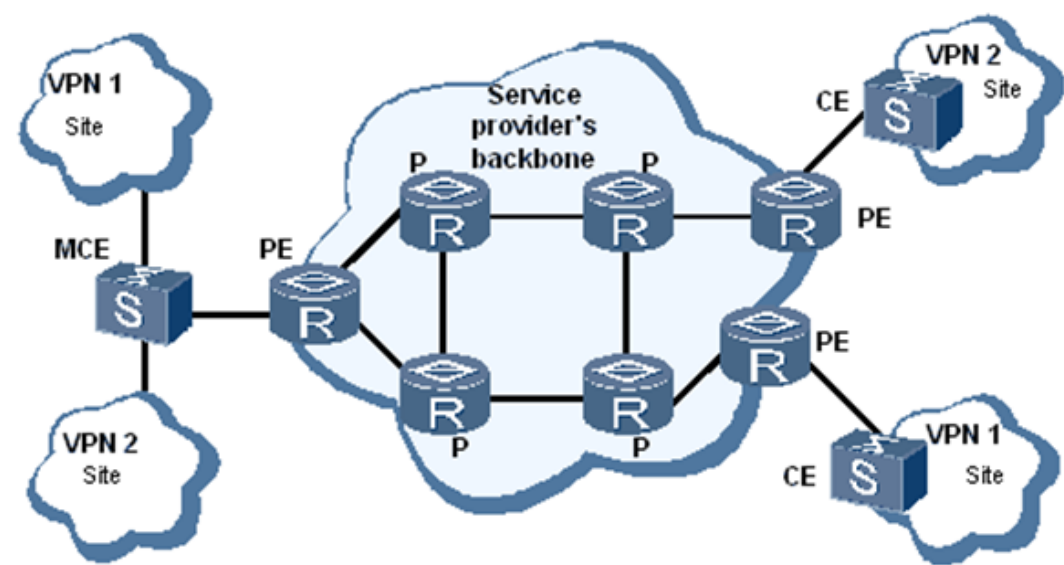
- 为每个 VPN 创建和维护独立的路由转发表（Multi-VRF）。
- 对 VPN 的所有处理都发生在 PE 上。

MCE 主要实现如下能力：

- 为每个 VPN 创建和维护独立的路由转发表（Multi-VRF）。
- 使用 CE 设备本身的 VLAN 接口与 VPN(VRF)进行绑定，实现不同 VPN 之间的业务完全隔离。

MCE 组网如图 9-12 所示。

图 9-12 MCE 组网



HoVPN 组网

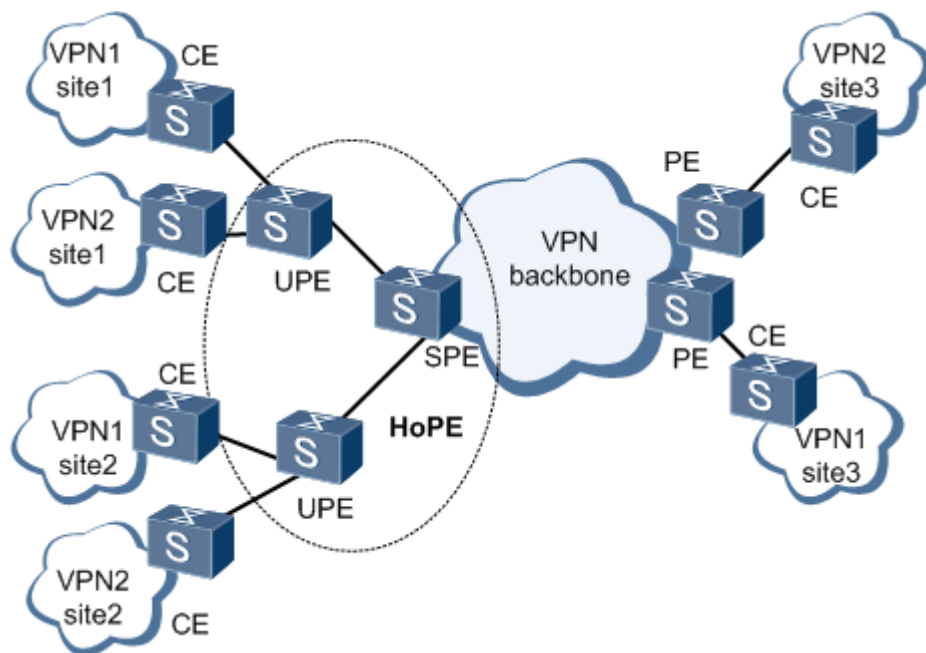
分层 VPN（Hierarchy of VPN，简称 HoVPN）将 PE 的功能分布到多个 PE 设备上，多个 PE 承担不同的角色，并形成层次结构，共同完成一个 PE 的功能，也称分层 PE（Hierarchy of PE，HoPE）。

在 BGP/MPLS VPN 中，PE 设备最为关键，它完成两方面的功能：

- 为用户提供接入功能，这需要 PE 具有大量接口；
- 管理和发布 VPN 路由，处理用户报文，这需要 PE 设备具有大容量内存和高转发能力。

HoVPN 组网如图 9-13 所示。

图 9-13 HoVPN 组网



根据所在位置，将 PE 做如下划分：

- UPE：连接用户的 PE 设备，主要负责用户接入。维护直接相连的 VPN site 路由，但不维护 VPN 中其它远端 site 的路由；为直接相连的 site 路由分配内层标签；通过 MP-BGP 随 VPN 路由发布此标签给 SPE。
- SPE：连接运营商的 PE 设备，主要负责 VPN 路由的管理和发布。维护其通过 UPE 连接的 VPN 所有路由，包括本地和远端 site 的路由；SPE 只向 UPE 发布 VPN 实例的缺省路由，并携带标签。

跨域 VPN-OptionA 组网

随着 MPLS VPN 解决方案的广泛应用，国内运营商的不同城域网之间，或相互协作的运营商的骨干网之间都存在着跨越不同自治域的情况。

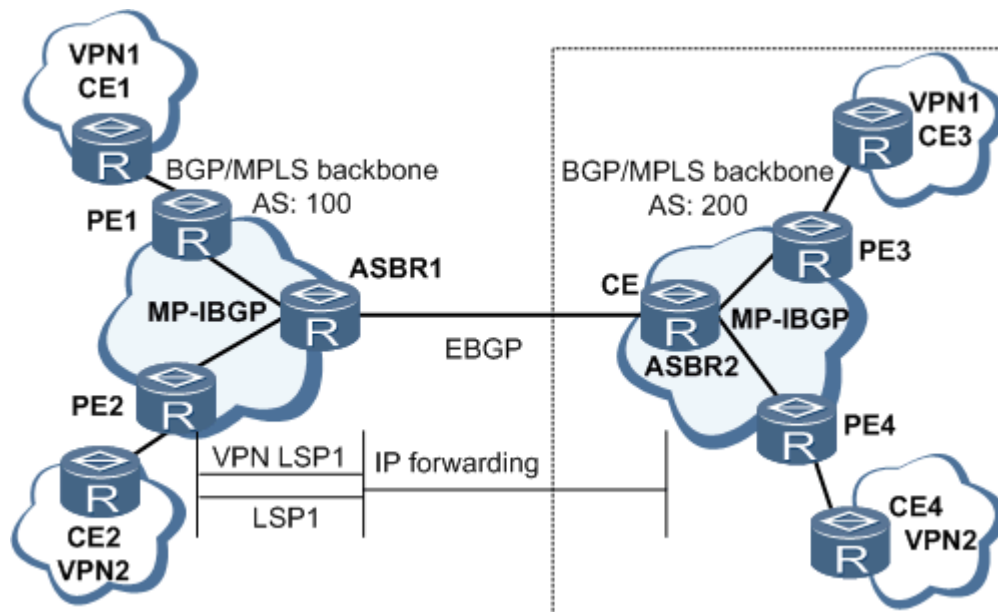
一般的 MPLS VPN 体系结构都是在一个自治系统内运行，任何 VPN 的路由信息都是只能在一个自治系统内按需扩散，没有提供自治系统内的 VPN 信息向其他自治系统扩散的功能。因此，为了支持运营商之间的 VPN 路由信息交换，就需要扩展现有的协议和修改 MPLS VPN 体系框架，提供一个不同于基本的 MPLS VPN 体系结构所提供的互连

模型——跨域（Inter-AS）的 MPLS VPN，以便可以穿过运营商间的链路来发布路由前缀和标签信息。

跨域 VPN-OptionA 是基本 BGP/MPLS VPN 在跨域环境下的应用，ASBR 之间不需要运行 MPLS，也不需要为跨域进行特殊配置。这种方式下，两个 AS 的边界交换机 ASBR 直接相连，ASBR 同时也是各自所在自治系统的 PE。两个 ASBR 都把对端 ASBR 看作自己的 CE 设备，使用 EBGP 方式向对端发布 IPv4 路由。

跨域 VPN-OptionA 组网如图 9-14 所示。

图 9-14 跨域 VPN-OptionA 组网



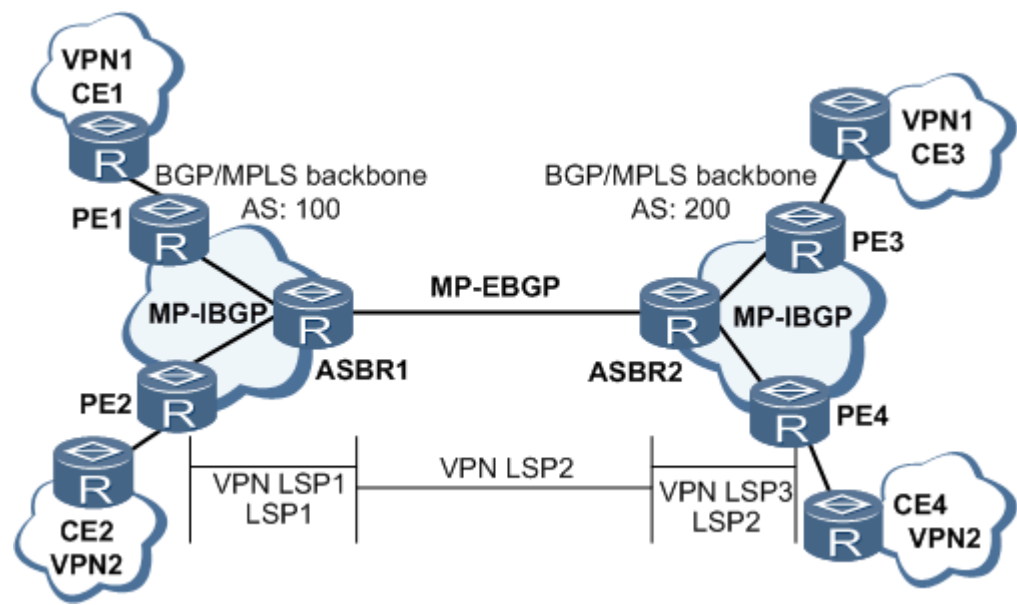
上图中，对于 AS100 的 ASBR1 来说，AS200 的 ASBR2 只是它的一台 CE 设备；同样，对于 ASBR2，ASBR1 也只是一台接入的 CE 设备。

跨域 VPN-OptionB 组网

跨域 VPN-OptionB 中，两个 ASBR 通过 MP-EBGP 交换它们从各自 AS 的 PE 设备接收的标签 VPN-IPv4 路由。

跨域 VPN-OptionB 组网如图 9-15 所示。

图 9-15 跨域 VPN-OptionB 组网



两种跨域方式的比较

两种跨域方式的比较请参见表 9-7。

表 9-7 两种跨域方式的比较

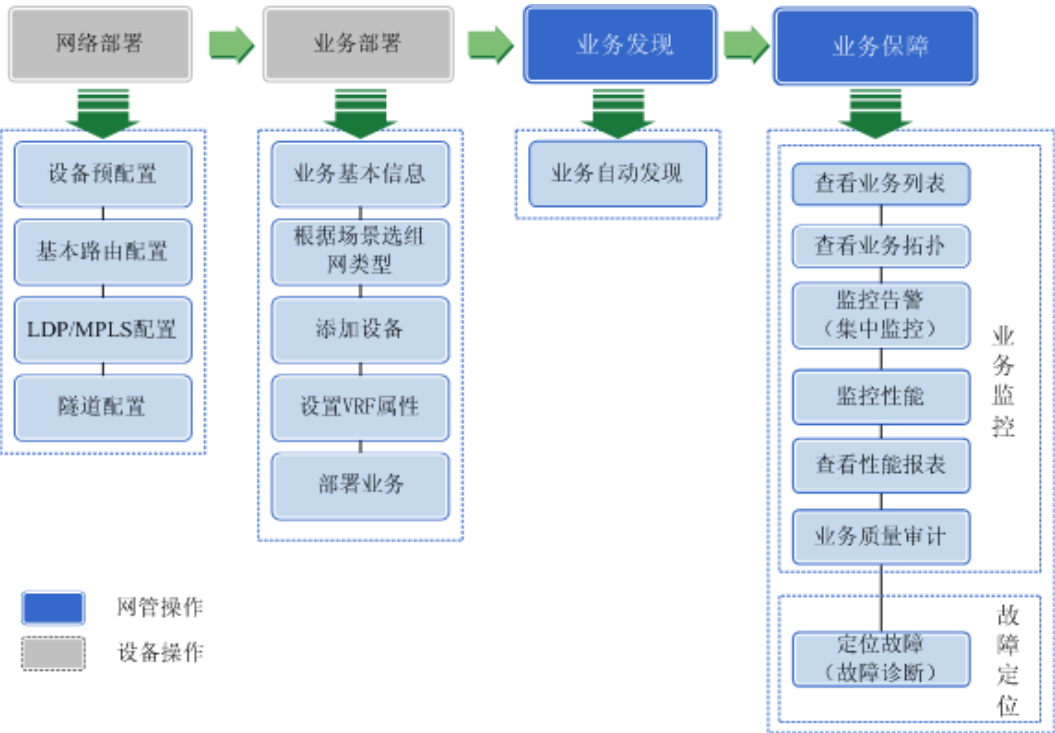
跨域 VPN	特点
OptionA	优点是配置简单：由于 ASBR 之间不需要运行 MPLS，也不需要为跨域进行特殊配置。缺点是可扩展性差：由于 ASBR 需要管理所有 VPN 路由，需要为每个 VPN 创建 VPN 实例。这将导致 PE 上的 VPN-IPv4 路由数量过大。并且，由于 ASBR 间是普通的 IP 转发，要求为每个跨域的 VPN 使用不同的接口（可以是子接口、物理接口、捆绑的逻辑接口），从而提高了对 PE 设备的要求。如果跨越多个自治域，中间域必须支持 VPN 业务，不仅配置量大，而且对中间域影响大。在需要跨域的 VPN 数量比较少的情况，可以优先考虑使用。
OptionB	不同于 OptionA，OptionB 方案不受 ASBR 之间互连链路数目的限制。局限性：VPN 的路由信息是通过 AS 之间的 ASBR 路由器来保存和扩散的，当 VPN 路由较多时，ASBR 负担重，容易成为故障点。因此在 MP-EBGP 方案中，需要维护 VPN 路由信息的 ASBR 一般不再负责公网 IP 转发。

9.3.2 全景图

介绍 BGP/MPLS VPN 管理流程，包括网络部署、业务部署、业务发现、业务保障。

BGP/MPLS VPN 管理流程如图 9-16 所示。

图 9-16 BGP/MPLS VPN 管理流程



详细管理流程请参见表 9-8。

表 9-8 BGP/MPLS VPN 管理流程

操作		备注
网络部署		该任务是部署 L3VPN 业务的前提配置。该部分包括设备预配置、基本路由配置、LDP/MPLS 配置、隧道配置等。该功能需要在设备上操作。
业务部署		在设备上创建并配置业务，创建业务前可以通过查看业务资源了解当前已存在的 VRF 信息。该功能需要在设备上操作。
业务发现		发现网络中已存在的业务到 eSight 进行统一管理。该功能可以在 eSight 上操作。
业务保障	业务监控	包括监控业务告警、性能、业务质量监控和性能报表，查看业务拓扑等。业务拓扑提供了丰富的业务操作入口，可以通过拓扑颜色直观的发现业务告警并支持通过拓扑入口跳转查看相应告警。该功能可以在 eSight 上操作。
	故障定位	通过监控发现业务告警后，在业务列表或者业务拓扑中集中显示，可以通过单击具体业务的告警查看具体的告警明细；通过业务诊断定位具体故障点。该功能可以在 eSight 上操作。

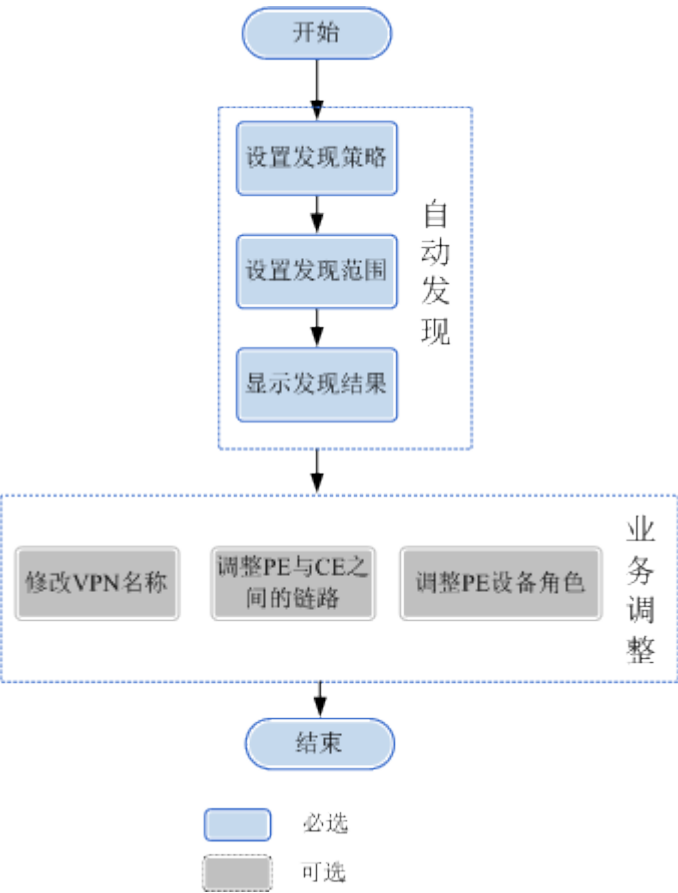
9.3.3 业务自动发现

当网络上完成 BGP MPLS VPN 的业务部署或者业务发生变更时，可以通过 BGP/MPLS VPN 自动发现功能将 L3VPN 业务发现到网管。

9.3.3.1 自动发现流程

以流程图的形式展示 BGP/MPLS VPN 的自动发现流程。
自动发现流程如图 9-17 所示。

图 9-17 自动发现流程



详细发现流程请参见表 9-9。

表 9-9 自动发现流程

操作	备注
自动发现	通过设置发现策略、发现范围，将已经完成网络部署和业务部署的设备上的 L3VPN 业务发现到 eSight 上。 自动发现包含：设置发现策略、设置发现范围、显示发现结果。 1. 设置发现策略：发现策略，主要包括：通过 VRF 连通性发现、通过 VRF 名称发现。 当 VPN 中 VRF 名称一致时，可使用通过 VRF 名称发现。 2. 设置发现范围：发现范围，主要有两种方式：选择设备、全网 PE/CE。 3. 显示发现结果：显示 VPN 名称、发现状态和操作。
业务调整	业务发现上来，可以对 L3VPN 名称、设备角色或者业务链路进行发现结果的调整。 业务调整包含：修改 L3VPN 名称、调整 PE 与 CE 间链路、调整 PE 设备角色。 1. 修改 L3VPN 名称：对发现上来的 L3VPN 名称进行调整。 2. 调整 PE 与 CE 间链路：PE 与 CE 之间，通过 OSPF、ISIS、或者 EBGp 交换私网路由，eSight 能够自动发现 PE 与 CE 之间的业务链路；其他通过静态路由或者 RIP 交换私网路由的链路，eSight 无法发现，此时需要通过手工方式对 PE 与 CE 之间的链路进行调整，包括：“添加 CE”、“删除 CE”、“修改 CE”。 3. 调整 PE 设备角色：用户根据实际组网需求，可以任意调整 PE 设备的角色，主要包括：“PE”、“UPE”和“SPE”。

9.3.3.2 自动发现

通过设置发现策略、发现范围，将已经完成网络部署和业务部署的设备上的 L3VPN 业务发现到 eSight 上。

前提条件

- 具有设备管理权限、“操作员”及以上的网管用户权限。
- 在设备上已经完成网络部署和业务部署。

背景信息

自动发现 BGP/MPLS VPN 业务不影响网元的配置数据，仅上载或更新 eSight 上 BGP/MPLS VPN 业务的数据信息。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。
- 步骤 2** 在左侧导航树中，选择“业务管理 > 业务列表”，单击“自动发现”。
- 步骤 3** 选择发现策略和发现范围。

发现策略:

- 选择“通过 VRF 连通性发现”，将路由策略相同（设备 A 的 Import RT 与设备 B 的 Export RT 相同）的 VRF 发现为一个业务。
- 选择“通过 VRF 名称发现”，将名称相同的 VRF 发现为一个业务。

发现范围:

- 选择“选择设备”，单击 ，在弹出的对话框中，选择一个或多个网元，然后单击“确定”，对特定网元进行业务发现。
- 选择“全网 PE/CE”，对网络中支持 L3VPN 业务的设备进行业务发现。

步骤 4 单击“自动发现”，先进行数据同步再根据如上的发现策略和发现范围的设置进行自动发现。数据同步和业务自动发现的进度以进度条的形式显示。

 说明

数据同步过程中，如果需要中断自动发现，可以单击“取消发现”。

----结束

操作结果

自动发现的结果，在发现结果列表中显示。

“VPN 名称”：显示发现的 L3VPN 业务名称，通过单击某个业务的名称进行业务调整。

 说明

“VPN 名称” 拼写规则：BGP/MPLS VPN_时间_序号。

“发现状态”主要分为如下三种类型：

- “新增业务”：通过自动发现操作，新增加到网管侧的业务。
- “变更业务”：网管侧有此业务，但与设备侧不一致，如 PE 与 PE 之间链路变更或者 PE 与 CE 之间链路变更。通过自动发现操作，由设备侧同步到网管侧的业务。
- “删除业务”：如果设备侧的业务被删除，通过自动发现操作，网管侧的该业务同步删除。

后续处理

自动发现成功后，可在“自动发现”页面进行如下操作。

名称	操作方法
修改业务名称	单击某个业务的  。
查看业务拓扑	单击某个业务的  。

9.3.3.3 业务调整

业务发现上来，可以对 L3VPN 名称、设备角色或者业务链路进行发现结果的调整。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。
- 步骤 2** 在左侧导航树中，选择“业务管理 > 业务列表”，单击  选择 ，修改 L3VPN 业务名称。
- 步骤 3** 在“业务列表”或者在自动发现的发现结果中，单击需要调整的 L3VPN 业务，进入业务调整界面进行业务调整。
- 步骤 4** 在“CE 管理”列表中，单击“增加 CE”、“删除 CE”或者“修改 CE”，调整 PE 与 CE 之间的链路。
-  **说明**
调整 PE 与 CE 之间的链路主要场景：PE 与 CE 之间，通过 OSPF、ISIS、或者 EBGp 交换私网路由，eSight 能够自动发现 PE 与 CE 之间的业务链路；其他通过静态路由或者 RIP 交换私网路由的链路，eSight 无法发现，此时需要通过手工方式在 eSight 上进行增加、删除或者修改 CE 设备。
- 步骤 5** 在“业务链路”列表中，单击“修改设备角色”，用户根据实际组网需求，可以任意调整 PE 设备的角色，主要包括：“UPE”、“SPE”和“PE”。

----结束

9.3.4 业务监控

当通过自动发现功能将 BGP/MPLS VPN 的业务发现到 eSight 时，可以通过各种方法监控业务的运行状态。

9.3.4.1 查看业务列表

查看 L3VPN 业务列表和 L3VPN 业务详细信息。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

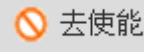
操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。
- 步骤 2** 在左侧导航树中，选择“业务管理 > 业务列表”，显示 L3VPN 业务列表，包括如下信息：“VPN 名称”、“运行状态”、“使能状态”、“告警级别”等。
-  **说明**
运行状态：PE 与 CE 之间链路状态和 VRF 的运行状态。
使能状态：PE 接入接口的管理态。
告警级别：显示 L3VPN 告警的最高级别。L3VPN 告警，主要是设备产生的告警以及 L3VPN 系统内部产生的告警，包括：PE/CE 设备与业务有关的接口 UP/DOWN 告警、VRF 的 up/down 告警、L3VPN 业务的性能指标告警、设备离线告警、L3VPN 业务 SLA 告警。
- 步骤 3** 单击具体的 L3VPN 业务，可以查看该业务的详细信息，包括：“CE 管理”、“业务链路”、“VRF 实例”和“路由配置”信息。

----结束

后续处理

在 L3VPN 业务列表中，同时还可以进行如下操作。

名称	操作方法
使能 L3VPN 业务	单击  使能。L3VPN 状态变为“使能”状态。
去使能 L3VPN 业务	单击  去使能。L3VPN 状态变为“去使能”状态。 说明 去使能操作成功后，业务中断。
删除 L3VPN 业务	单击  删除，将网管上 L3VPN 的数据删除。

9.3.4.2 业务拓扑

通过浏览拓扑视图，可实时了解拓扑结构和业务的运行状态，本节介绍了查看 L3VPN 业务拓扑视图的方法。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 通过如下任意一个操作，查看全网的业务拓扑。

- 在左侧导航树中，选择“业务管理 > 业务列表”，选任意一个 L3VPN 业务，单击 ，弹出“业务拓扑”窗口。
- 在左侧导航树中，选择“业务管理 > 业务拓扑”，弹出“业务拓扑”窗口。

步骤 3 在“业务拓扑”窗口中，显示全网的 L3VPN 拓扑。

- 单个 L3VPN 业务的拓扑，如 [图 9-18](#) 所示。

图 9-18 L3VPN 业务拓扑



- L3VPN 告警级别，当有 L3VPN 告警产生时，会以框进行标识，并且以颜色标识 L3VPN 告警的最高级别，如 [图 9-19](#) 所示。

图 9-19 L3VPN 告警



 说明

L3VPN 告警，即设备产生的告警以及 L3VPN 系统内部产生的告警，包括：PE/CE 设备与业务有关的接口 UP/DOWN 告警、VRF 的 up/down 告警、L3VPN 业务的性能指标告警、设备离线告警、L3VPN 业务 SLA 告警。

L3VPN 告警级别：以框的颜色进行标识。红色，表示紧急告警；橙色，表示重要告警；黄色，表示次要告警；蓝色，表示提示告警。

- 拓扑图例，可以了解拓扑对象的告警状态和运行状态等，单击 ，显示拓扑图例，如图 9-20 所示。

图 9-20 拓扑图例



步骤 4 在“业务拓扑”窗口中，选中任意一个 L3VPN 业务，可以进行如下操作：

- 性能查看，单击右键，选择 **性能指标**。
- 业务快速诊断，单击右键，选择 **快速诊断**。
- 业务质量监控，单击右键，选择 **业务质量监控**。
- 详细信息查看，单击右键，选择 **详细信息**。
- 展开/收缩业务拓扑，单击 ，展开业务拓扑；单击  收缩业务拓扑。

步骤 5 在“业务拓扑”窗口中，选中任意一个 L3VPN 业务，双击查看单个业务的详细拓扑。

在单个业务拓扑中，可以查看到源端和宿端的 PE 信息、与 PE 相连的 CE 信息和 PE 与 PE、PE 与 CE 之间的链路的信息。

 说明

如果业务自动发现时，没有选择相应 CE，在查看 PE-CE 之间的链路信息时，会导致有些链路只显示 PE 信息而不显示 CE 信息。

在单个业务拓扑中，可以进行如下操作：

- 设备基本信息查看，选中设备，单击右键，选择 **管理**，弹出“管理”窗口。
- 设备告警查看，即查看选中设备的所有设备告警和网管告警。选中设备，单击右键，选择 **查看告警**，弹出“查看告警”窗口。
- 链路诊断，对 PE 与 PE 之间、PE 与 CE 之间的链路进行快速诊断。选中链路，单击右键，选择 **链路诊断**，弹出“快速诊断”窗口。
- 链路性能，查看 L3VPN 的性能趋势图。选中 PE 与 CE 之间的链路，单击右键，选择 **链路性能**，弹出“链路性能”窗口。
- 设备 L3VPN 告警级别显示，在 PE/CE 设备上以冒泡的形式显示设备的 L3VPN 告警级别，如图 9-21 所示。

图 9-21 设备 L3VPN 告警显示



说明

设备 L3VPN 告警级别。当设备上有 L3VPN 告警产生时，会以冒泡的形式显示；冒泡的颜色，标识设备 L3VPN 告警的最高级别。红色，表示紧急告警；橙色，表示重要告警；黄色，表示次要告警；蓝色，表示提示告警。

- 链路查看，以直线形式显示 PE 与 CE、PE 与 PE、PE 与区域、CE 与区域的连接关系。
- 链路状态查看，任意两台设备之间的链路的状态以链路的颜色标识。

说明

链路的颜色，标识链路状态。绿色，表示正常；蓝色，表示未知；灰色，表示链路两端的有设备离线或者接口 down。

- 区域信息显示，如图 9-22 所示。如果区域中有 L3VPN 告警产生时，会以框进行标识。

图 9-22 区域信息显示



双击区域图标，可以查看区域中所包含的设备及设备之间的链路信息。

说明

只有在区域管理中导入了该 L3VPN 业务所涉及的设备，才会在拓扑中显示区域。

---结束

9.3.4.3 区域管理

区域，可以看作处于相同地理位置内网络设备的集合。可以通过区域管理实现网络设备的分层次管理。

前提条件

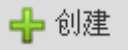
已经通过自动发现功能将 L3VPN 业务发现到 eSight。

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 在左侧导航树中，选择“业务管理 > 区域管理”，显示区域管理列表。

在区域管理列表中，可以进行如下操作。

1. 创建区域，单击 。
2. 修改区域，在“操作”列中，单击 。
3. 导入物理拓扑，将物理拓扑上已经创建的子网作为区域导入到区域管理中，子网中的设备作为区域中的设备随子网导入。单击 。
4. 删除区域，先勾选需要删除的区域，再单击 。
5. 查看区域信息，在“区域/设备名称”列中，单击任意一条数据，查看区域的详细信息。

----结束

后续处理

- 在区域的详细信息中，可以进行如下操作。

操作名称	操作方法
增加子区域	单击  。 说明 ● 增加子区域，只能在已有区域或者子区域中增加。 ● 一个区域中，最多支持创建 9 级的子区域。
切换区域	选择子区域中的设备，单击  ，完成设备所属区域的切换。 说明 不支持子区域切换到其他区域。
导入设备	先勾选需要删除的子区域/设备，再单击  ，完成删除操作。
删除子区域/设备	选择子区域中的设备，单击  ，完成设备所属区域的切换。
查看子区域信息	在“子区域/设备名称”列中，单击任意一条数据，查看子区域的详细信息。

- 在子区域的详细信息中，可以进行如下操作。

操作名称	操作方法
增加子区域	单击  增加子区域。
切换区域	选择子区域中的设备，单击  切换区域，完成设备所属区域的切换。
导入设备	单击  导入设备。
删除子区域/设备	先勾选需要删除的子区域/设备，再单击  删除，完成删除操作。
查看子区域信息	在“子区域/设备名称”列中，单击任意一条数据，查看子区域的详细信息。

9.3.4.4 告警管理

通过监控 L3VPN 告警，及时了解 L3VPN 业务的运行状态，并保证业务的正常运行。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

背景信息

L3VPN 告警，即设备产生的告警以及 L3VPN 系统内部产生的告警，包括：PE/CE 设备与业务有关的接口 UP/DOWN 告警、VRF 的 up/down 告警、L3VPN 业务的性能指标告警、设备离线告警、L3VPN 业务 SLA 告警。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。
- 步骤 2** 在左侧导航树中，选择“业务管理 > 业务列表”，显示全网的 L3VPN 列表。
- 步骤 3** 通过如下操作，查看 L3VPN 告警信息。
- 在左侧导航树中，选择“业务管理 > 业务列表”，选择任意一条 L3VPN 数据，选择 ，弹出“查看告警”，显示当前 L3VPN 的告警。
- 步骤 4** 通过如下任意一个操作，查看 L3VPN 的告警级别。
- 在左侧导航树中，选择“业务管理 > 业务列表”，在“告警级别”列中，显示当前业务告警的最高级别。
 - 在左侧导航树中，选择“业务管理 > 接入拓扑”，显示全网的业务拓扑。当有 L3VPN 告警产生时，会以框进行标识，并且以颜色标识 L3VPN 告警的最高级别，如 [图 9-23](#) 所示。

图 9-23 L3VPN 告警



说明

L3VPN 告警级别：以框的颜色进行标识。红色，表示紧急告警；橙色，表示重要告警；黄色，表示次要告警；蓝色，表示提示告警。

----结束

9.3.4.5 性能管理

查看 L3VPN 业务的历史性能及趋势图。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

背景信息

对于自动发现到 eSight 的 L3VPN 业务，eSight 会默认统计如下指标：

- 接口流入流量
- 接口流出流量
- VRF 接收字节数
- VRF 发送字节数
- VRF 接收字节速率
- VRF 发送字节速率
- VRF 活跃路由数
- VRF 配置路由数
- VRF 活跃路由百分比

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 通过如下任意操作，进入“性能指标”页面。

1. 在左侧导航树中，选择“业务管理 > 业务列表”，显示 L3VPN 业务列表。选择任意一个 L3VPN，在“操作”列中，单击 ，弹出“性能指标”。
2. 在左侧导航树中，选择“业务管理 > 接入拓扑”，显示 L3VPN 业务全网拓扑。选择任意一个 L3VPN，单击 ，选择 **性能指标**，弹出“性能指标”。

说明

L3VPN 的性能，主要包括接口性能和 VRF 性能。如果系统默认统计的性能指标无法满足实际需要，可以在性能管理功能中补充性能统计指标。

L3VPN 支持的测量对象和指标组详见 [表 9-10](#)。

表 9-10 L3VPN 支持的测量对象和指标组

测量对象	指标列表
接口	“接口高级统计”、“接口流量统计”、“接口统计指标”，即设备对接口支持的指标。
VRF	“L3VPN 基础统计指标”
	“VRF 路由数统计”

步骤 3 在“性能指标”中，显示历史性能。

1. 设置“时间范围”内选项，单击“确定”，查看选中范围内的历史性能。
2. 在“TOP VPN 性能”中，单击 ，选择要显示的 L3VPN TOP 性能图示。
3. 在“接入接口性能明细”、“VRF 流量性能明细”、“VRF 路由性能明细”中，选择任意一条 VRF，单击 ，查看 L3VPN 的性能明细。

----结束

9.3.4.6 报表管理

查看 L3VPN 报表数据。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

背景信息

对于自动发现到 eSight 的 L3VPN 业务，eSight 会默认创建如下报表任务：

- 接口流量性能统计报表
- 业务 VRF 统计报表
- VRF 流量统计报表

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 在左侧导航树中，选择“报表管理 > 报表管理”，显示 L3VPN 业务报表。

步骤 3 查看接口流量性能统计报表。

1. 选择任意一个 L3VPN，在“接口流量性能统计报表”列中，单击 。
弹出“统计时间段”。
2. 设置“开始时间”、“结束时间”，单击“确定”。
弹出“接口流量性能统计报表”，显示指定时间范围内的接口流量性能统计报表数据。

步骤 4 查看业务 VRF 统计报表。

1. 选择任意一个 L3VPN，在“业务 VRF 统计报表”列中，单击 。
弹出“统计时间段”。
2. 设置“开始时间”、“结束时间”，单击“确定”。
弹出“业务 VRF 统计报表”，显示指定时间范围内的业务 VRF 统计报表数据。

步骤 5 查看 VRF 流量统计报表。

1. 选择任意一个 L3VPN，在“VRF 流量统计报表”列中，单击 。
弹出“统计时间段”。
2. 设置“开始时间”、“结束时间”，单击“确定”。
弹出“VRF 流量统计报表”，显示指定时间范围内的 VRF 流量统计报表数据。

----结束

9.3.4.7 业务质量审计

查看 L3VPN 的业务质量数据。

前提条件

- eSight 已经安装并启动 SLA 组件。
- 已经通过自动发现功能将 L3VPN 业务发现到 eSight。
- SLA 任务已启动(默认情况下，SLA 任务为停止状态。)

背景信息

- 对于自动发现到 eSight 的 L3VPN 业务，并且有 PE-PE 或者 PE-CE 之间的链路时，eSight 会自动创建 SLA 任务。
- 该功能对源设备为非华为设备不支持。

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 在左侧导航树中，选择“业务管理 > 业务列表”，选择任意一个 L3VPN，选择 ，弹出“业务质量监控”。

步骤 3 “业务质量监控”中，显示“TOP 业务质量最低符合度”和“SLA 业务列表”。

----结束

9.3.5 业务故障诊断

当需要了解 L3VPN 运行状况、或者 L3VPN 业务产生告警时，无需配置任何诊断任务，使用此功能对 L3VPN 中的业务链路进行检测，从而快速了解网络连通性并定位具体故障点。

前提条件

已经通过自动发现功能将 L3VPN 业务发现到 eSight。

背景信息

- eSight 支持对 BGP/MPLS VPN 进行多种类型的诊断，可以根据需要或故障现象，采用分段（PE-PE、PE-CE）、分层（网络层次）的思路进行检查。不同诊断选项/工具的使用场景详见表 9-11。

表 9-11 L3VPN 诊断选项/工具的使用场景

诊断选项/工具	功能	应用场景
VRF Ping	检测 L3VPN 中业务链路的连通性。	用于检测 L3VPN 网络中的私网的连通性。
LSP Ping	检测 LSP 的连通性。	用于检测 L3VPN 网络中 LSP 的连通性。
ICMP Ping	检测网络层的连通性。通过执行结果查看丢包率、时延等信息，了解当前网络状况。	通常情况下，先排除业务层面的故障后，再通过此诊断检测公网或私网的连通性。

- 除此之外，BGP/MPLS VPN 业务还支持 VRF Traceroute、LSP Traceroute 和 ICMP Traceroute，应用场景与对应的 Ping 诊断类似。
不同在于，Traceroute 支持检测从源到宿所经过的中间节点，得到从源到这些中间节点的丢包率、时延信息，从而获取具体故障点；而 Ping 只能获取源到宿的连通性。在具体应用上，可以先通过 Ping 诊断源宿之间的连通性，当出现连通性故障时，再使用 Traceroute 进一步分析具体故障点。
- 不同链路类型支持的诊断选项/工具不同，如下表用“Y”表示，当前链路支持的诊断选项/工具，详见表 9-12。

表 9-12 诊断选项/工具与链路类型的对应关系

诊断选项/工具	链路类型			
	PE-PE	CE-CE	PE-RemoteCE	PE-CE
ICMP Ping	Y	Y	-	-
VRF Ping	Y	-	Y	Y
LSP Ping	Y	-	-	-
ICMP TraceRoute	Y	Y	-	-
VRF TraceRoute	Y	-	Y	Y

诊断选项/工具	链路类型			
	PE-PE	CE-CE	PE-RemoteCE	PE-CE
LSP TraceRoute	Y	-	-	-
查询公网路由	Y	-	-	-
查询私网路由	Y	-	Y	Y
查询 BGP VPNV4 对等体	Y	-	-	-
查询 VPNV4 路由	Y	-	-	-
查询 VRF FIB	Y	-	Y	Y
查询 LSP 信息	Y	-	-	-

- 该功能对非华为设备不支持。

操作步骤

步骤 1 在主菜单中选择“网络应用 > BGP/MPLS VPN 业务管理”。

步骤 2 在左侧导航树中，选择“业务管理 > 业务列表”，选择任意一条 L3VPN 数据，单击 ，弹出“快速诊断”窗口。

步骤 3 在“选择诊断对象”中，根据需要设置“链路类型”和“选择条件”，单击“搜索”，查询结果区显示所有符合条件的诊断对象。

步骤 4 在查询结果区中，选择需要诊断的链路。

步骤 5 选择诊断选项/工具，在“诊断选项/工具”中进行选择。

单击“高级”，可以设置诊断选项参数。

步骤 6 单击“快速诊断”。根据“链路类型”支持的诊断项，在“诊断结果”中，显示“Ping 结果”、“采集信息”和“Trace 结果”。

----结束

9.3.6 示例：BGP/MPLS VPN 管理典型操作

通过学习本示例，您可参照示例中的步骤，熟悉完成 Hub-spoke VPN 自动发现和查看拓扑及详细信息的过程。

前提条件

- 具有设备管理权限、“操作员”及以上的网管用户权限。
- 在设备上已经完成网络部署和业务部署。

- 设备已成功添加到网管，并已配置 telnet 参数。

场景介绍

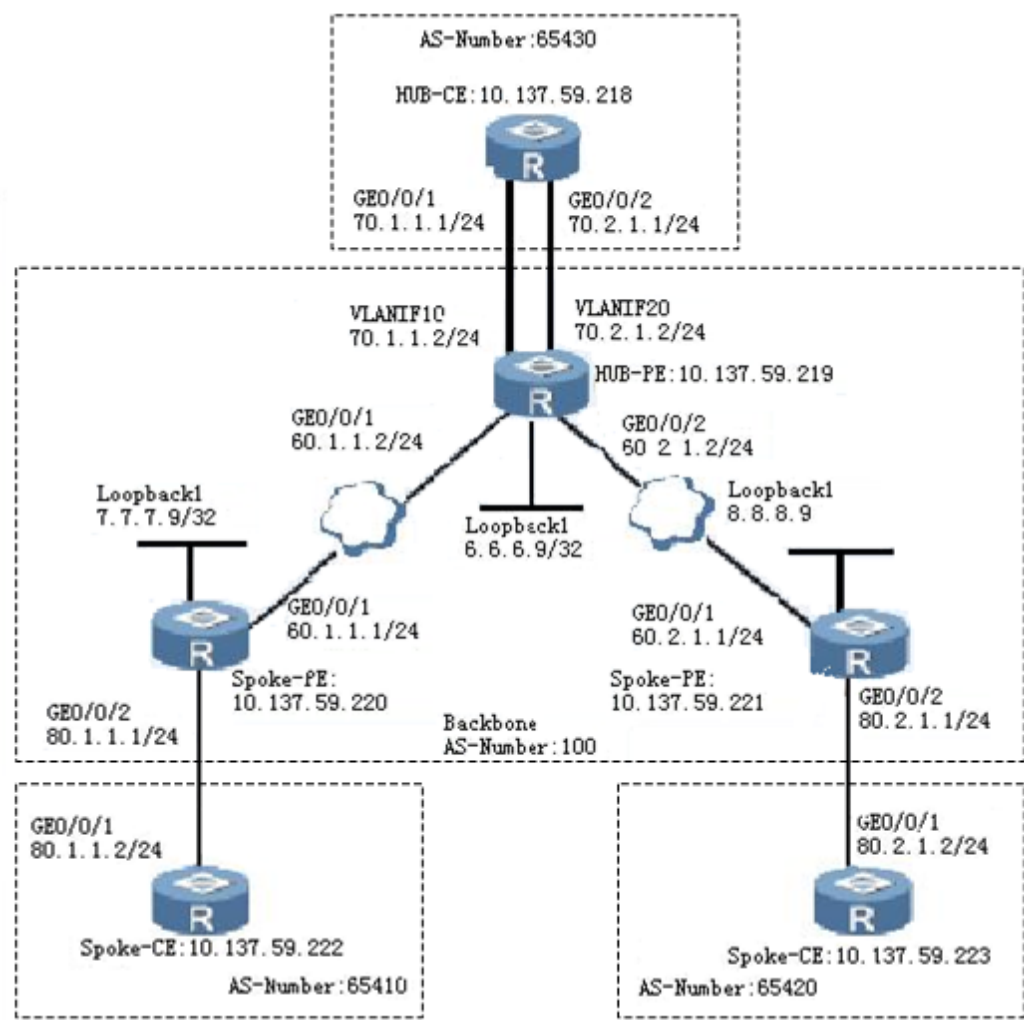
某大型企业总公司下有多个分公司，建有网管、BOSS、OA 等业务系统，这些业务系统分属不同的部门维护和管理，各业务系统所有的业务服务器及核心设备均集中在总公司。在全公司建有一张整个的 MPLS 骨干网络来承载所有的内部业务，不同的业务系统通过划分 VPN 来实现互访与隔离。

组网说明

分公司和总公司都部署相应的 PE 设备，分公司 1 的 PE 设备（10.137.59.220）和分公司 2 的 PE 设备（10.137.59.221）用来连接分公司的各业务系统网络，总公司的 PE 设备（10.137.59.219）用来连接各业务系统的服务器。

配置组网如图 9-24 所示。

图 9-24 配置组网图



数据规划

数据规划表请参见表 9-13。

表 9-13 数据规划表

设备名称	网元类型	网元 IP	设备角色	位置
AR3260_218_1	AR3260	10.137.59.218	HUB-CE	总部
AR2240_219_1	AR2240	10.137.59.219	HUB-PE	总部
AR2240_220_1	AR2240	10.137.59.220	SPOKE-PE	分部
AR2240_221_1	AR2240	10.137.59.221	SPOKE-PE	分部
AR3260_222_1	AR3260	10.137.59.222	SPOKE-CE	分部
AR3260_223_1	AR3260	10.137.59.223	SPOKE-CE	分部

操作步骤

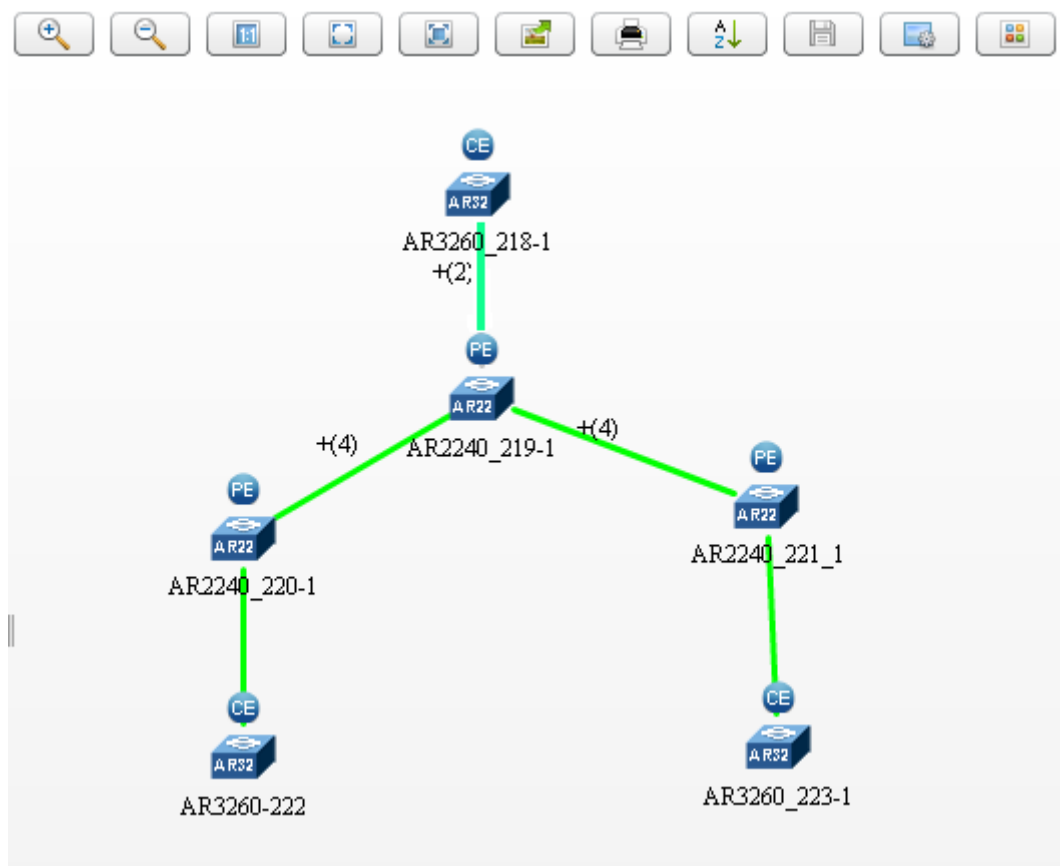
步骤 1 VPN 业务自动发现

1. 在主菜单中选择“网络应用 > BGP/MPLS VPN 管理”。
2. 在左侧导航树中，选择“业务管理 > 业务列表”，单击“自动发现”。
3. 选择“发现策略”为“通过 VRF 连通性发现”。
4. 在“发现范围”后单击“选择设备”。并在弹出的“选择设备”对话框中选中 IP 地址为 10.137.59.218 至 10.137.59.223 地址段的设备，单击“确定”。
5. 单击“自动发现”，发现出的 VPN 业务即展示在界面的下方表格中。
6. 在“发现结果”的表格区域，单击操作区的“修改名称”，修改对应的 VPN 名称。

步骤 2 查看 VPN 拓扑

1. 在“发现结果”的表格区域，单击操作区的“接入拓扑”，即进入全网 VPN 的拓扑界面。
2. 在全网 VPN 拓扑的界面，查找到对应的 VPN 名称，双击图标，进入该条 VPN 的拓扑界面。
 - 在拓扑界面上单击 ，即可选择不同的排序方式，调整设备在拓扑中的位置。
 - 设备图标上方的蓝色标识，标注出该设备的角色，如 、。
 - 将鼠标移到设备或者链路上，将会提示对应的设备信息和链路信息。
3. 调整后的 topo 如 [图 9-25](#) 所示：

图 9-25 VPN 业务拓扑



步骤 3 查看 VPN 业务详细信息

1. 在左侧导航树中，选择“业务管理 > 业务列表”。
2. 在展开的管理页面中，单击该条 VPN 名称，即可查看该业务的详细信息，包括：“CE 管理”、“业务链路”、“VRF 实例”和“路由配置”信息。

----结束

9.4 SLA 管理

eSight 支持对 SLA 的监控和管理，包括 SLA 概述、SLA 服务、SLA 任务和快速诊断。

9.4.1 了解 SLA

SLA 服务水平协议（SLA: Service Level Agreement）是在一定开销下为保障服务的性能和可靠性，服务提供商与用户间定义的一种双方认可的协定。

9.4.1.1 SLA 基本概念

在使用 SLA 之前，需要掌握 SLA 业务的基本概念，如 SLA 服务、任务、服务星级、符合度等，理解这些概念可以更快速、更准确地使用 SLA。

表 9-14 SLA 基本概念

概念	说明
SLA 服务	SLA 服务是业务、业务质量、测试例三者的融合体，业务即通常所说的语音视频等常见应用；测试例即设备的 UDP Echo、FTP 等诊断测试功能；业务质量可由对测试例指标所设置阈值的高低衡量出来。
SLA 任务	SLA 任务是为监控具体的网络链路及其上承载的业务质量的测试任务实例。
服务星级	反应了服务的质量标杆。星级越高，说明对某服务的丢包率、时延、抖动等指标控制得越严格。
符合度	反映网络质量和用户预期对比的一个百分比评估值。

9.4.1.2 SLA 功能简介

SLA 是一个网络性能度量与诊断工具，它通过主动在多个网元或链路之间发送诊断报文来实现对网络性能的度量。本章介绍了 SLA 业务的业务功能和流程，以指导用户能够熟悉和使用 SLA 组件。

SLA 的优点：

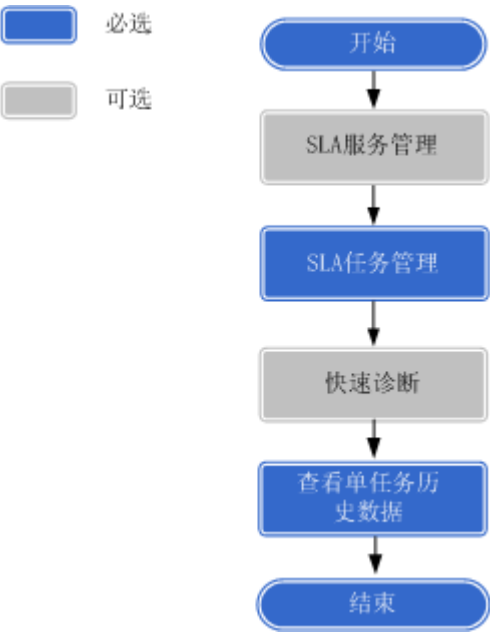
- 通过 SLA 的度量，用户可以确认网络应用按照需要的方式运行。
- 网络有问题时可以预先提醒用户。
- 可以连续的、周期性的度量网络的性能。
- 检测与确认服务质量，实现差别服务。

SLA 的能力：

- 测量能力：可以测量十种测试例（如 UDPEcho、TCPConnect、HTTP、DNS、ICMP Jitter 等）的多种指标（如时延、抖动、丢包率等）。
- 符合度：按用户设置的指标、阈值和权重，计算对应的 SLA 符合度，以图形化方式呈现给用户。
- 指标告警：用户可根据需要自定义 SLA 监视阈值，超过阈值将产生告警。
- 符合度告警：符合度低于用户的预期，将产生告警。
- 周期性监控：可以按用户指定的日期进行灵活的周期性监控。
- 历史情况查询：用户可查询任意一段时间的测量结果，并输出报表。

SLA 管理流程：

图 9-26 SLA 管理流程



- SLA 服务管理：用户可以用服务管理来定义某种业务所需的测试手段及树立该业务质量的标杆。系统预定义了十余种常见服务供用户选择，用户也可以根据需求自定义。
- SLA 任务管理：反应某链路的网络质量评价。用户选择某段链路，周期性的对某种服务进行定制测试，计算其 SLA 符合度并触发告警。
- 查看单任务历史数据：记录该任务在指定时间内的符合度曲线图，也可查询到用户指定测试例指标的阈值和实际测试值的对比曲线图。

9.4.1.3 SLA 术语及系统默认设置

在使用 SLA 之前，需要掌握 SLA 业务的基本概念和系统的默认设置，保证相关操作顺利完成。

系统支持的 SLA 服务

系统提供了默认的服务及其等级，可供用户在创建任务的时候选择。

典型业务	测试例	星级
视频	UDP Jitter、ICMP Jitter、UDP Echo	四星
语音	UDP Jitter	五星
数据	TCP Connect	三星
网页浏览	HTTP	四星
ftp 应用	FTP、ICMP Echo	四星
网络管理	SNMP	四星
实时应用	UDP Jitter、ICMP Jitter	四星

典型业务	测试例	星级
门户网站	HTTP、DNS、TCP Connect	四星
客户端服务器通信、数据库交易	TCP Connect、ICMP Echo	四星
电子商务、IM	UDP Echo、ICMP Echo	四星

系统支持的指标计算方法

- 抖动：报文接收时间减去报文发送时间。
- 时延：相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。
- 丢包率：（发包总数-收包数）/发包总数 * 100%。



说明

对于 TCP、FTP 测试例，丢包率=（探测总次数-成功探测次数）/探测总次数 * 100%。

系统支持的测试例及指标

指标	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
丢包率	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
往返时延最大值	Y	Y	Y	Y	Y	Y	Y	Y	N	N
往返时延平均值	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
抖动平均值	N	Y	N	Y	N	N	N	N	N	N
超时次数	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
源到目的单向时延最大值	N	Y	N	Y	N	N	N	N	N	N
目的到源单向时延最大值	N	Y	N	Y	N	N	N	N	N	N
源到目的方向抖动值平均值	N	Y	N	Y	N	N	N	N	N	N
目的到源方向抖动值平均值	N	Y	N	Y	N	N	N	N	N	N
MOS 值	N	N	N	Y	N	N	N	N	N	N
FTP 控制连接建立的最大时间	N	N	N	N	N	N	N	N	N	Y
FTP 数据传输最大的时间	N	N	N	N	N	N	N	N	N	Y

指标	IC MP Echo	IC MP Jitter	UD P Echo	UD P Jitter	TCP Connect	SN MP	DN S	DH CP	HT TP	FTP
FTP 探测所消耗的最大时间	N	N	N	N	N	N	N	N	N	Y
FTP 传输被强制终止的次数	N	N	N	N	N	N	N	N	N	Y
RTT 统计失败次数	N	N	N	N	N	N	Y	N	N	N
报文序号错误数	N	N	N	N	N	N	Y	N	N	N
初始化或资源申请失败（busy）次数	N	N	N	N	N	N	Y	N	N	Y
最大 HTTP 测试总时间	N	N	N	N	N	N	N	N	Y	N
最大 HTTP 交易时间	N	N	N	N	N	N	N	N	Y	N
HTTP 其它出错计数	N	N	N	N	N	N	N	N	Y	N
最大 TCP 连接往返时间	N	N	N	N	N	N	N	N	Y	N
TCP 连接出错计数	N	N	N	N	N	N	N	N	Y	N
TCP 连接超时计数	N	N	N	N	N	N	N	N	Y	N
最大 DNS 往返时间	N	N	N	N	N	N	N	N	Y	N
DNS 解析操作失败计数	N	N	N	N	N	N	N	N	Y	N

设备支持的测试例

设备系列	设备版本	IC MP Echo	IC MP Jitter	UD P Echo	UD P Jitter	TCP Connect	SN MP	DNS	DHCP	HTTP	FTP
S2300	V100 R005 C00 、 V100 R005 C01、 V100 R006 C00 、 V100 R006 C01 、 V200 R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
	V100 R003 C00 、 V100 R003 C01	Y	N	Y	Y	Y	Y	Y	N	Y	N
S2700	V100 R005 C01 、 V100 R006 C00 、 V100 R006 C01 、 V200 R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y

设备系列	设备版本	IC MP Echo	IC MP Jitter	UD P Echo	UD P Jitter	TCP Connect	SN MP	DNS	DHCP	HTTP	FTP
S3300	V100R003C00 、 V100R003C01 、 V100R005C00 、 V100R005C01 、 V100R006C00 、 V100R006C01 、 V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S3700	V100R005C01 、 V100R006C00 、 V100R006C01 、 V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S5300	V100R003C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
	V100R003C01、 V100R005C00、 V100R005C01、 V100R006C00、 V100R006C01	Y	N	Y	Y	Y	Y	Y	N	Y	Y
	V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S5700	V100R005C01、 V100R006C00、 V100R006C01、 V200R001	Y	N	Y	Y	Y	Y	Y	N	Y	Y
S6300	V100R006C00、 V100R006C01、 V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
S6700	V100R006C00 、 V100R006C01 、 V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S9300	V100R003C00 、 V100R003C01 、 V100R006C00 、 V100R006C01 、 V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S9700	V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
S7700	V100R003C01 、 V100R006C00 、 V100R006C01 、 V200R001	Y	Y	Y	Y	Y	Y	Y	N	Y	Y

设备系列	设备版本	IC MP Echo	IC MP Jitter	UD P Echo	UD P Jitter	TCP Connect	SN MP	DN S	DH CP	HT TP	FTP
NE20	V200 R005 C01 、 V200 R005 C02 、 V200 R005 C03 、 V200 R005 C05	Y	N	Y	Y	Y	Y	Y	Y	Y	N
NE20 E-8	V200 R003 C00 、 V200 R003 C01 、 V200 R005 C00 、 V200 R005 C01 、 V200 R005 C02 、 V200 R005 C03 、 V200 R005 C05	Y	N	Y	Y	Y	Y	Y	Y	Y	N
NE20 E-X6	V600 R003 C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
NE40	V300R002C00 、 V300R002C01 、 V300R003C00 、 V300R003C01 、 V300R003C02 、 V300R005C00 、 V300R005C01	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
NE40E	V300R001C00	N	N	N	N	N	N	N	N	N	N
	V300R002C00 、 V300R003C00 、 V300R003C01 、 V300R003C02	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

设备系列	设备版本	IC MP Echo	IC MP Jitter	UD P Echo	UD P Jitter	TCP Connect	SN MP	DNS	DHCP	HTTP	FTP
	V300 R006 C00 、 V300 R006 C01 、 V600 R001 C00 、 V600 R001 C01 、 V600 R003 C00 、 V600 R003 C01 、 V600 R003 C02 、 V600 R003 C03 、 V600 R003 C05	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NE40 E-4	V300 R003 C00 、 V300 R003 C01 、 V300 R003 C02	N	N	N	N	N	N	N	N	N	N

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
NE40E-X3	V300R006C00 、 V300R006C01	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
NE80	V300R002C00 、 V300R002C01 、 V300R003C00 、 V300R003C01 、 V300R003C02 、 V300R005C00 、 V300R005C01	Y	N	Y	Y	Y	Y	Y	Y	Y	N
NE80E	V100R002C00 、 V300R001C00	N	N	N	N	N	N	N	N	N	N
	V300R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	N

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
	V300R003C00 、 V300R003C01 、 V300R003C02	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
	V300R006C00 、 V300R006C01 、 V600R001C00 、 V600R001C01	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
AR1200	V200R001C00 、 V200R001C01 、 V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

设备系列	设备版本	ICMP Echo	ICMP Jitter	UDP Echo	UDP Jitter	TCP Connect	SNMP	DNS	DHCP	HTTP	FTP
AR2200	V200R001C00 、 V200R001C01 、 V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR3200	V200R001C00 、 V200R001C01 、 V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR150	V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AR200	V200R002C00	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

 说明

- 对于 UDP Echo 和 UDP Jitter 测试例，必须在目的设备上启动 UDP 服务。

执行如下命令启动 UDP 服务：

<Huawei> **system-view**

[Huawei] **nqa-server udpecho 10.137.61.39 33434**

其中“10.137.61.39”是目的设备 IP 地址，“33434”是 UDP 端口号。

- 对于 TCP Connect 测试例，必须在目的设备上启动 TCP 服务。

执行如下命令启动 TCP 服务：

<Huawei> **system-view**

[Huawei] **nqa-server tcpconnect 10.137.61.39 33433**

其中“10.137.61.39”是目的设备 IP 地址，“33433”是 TCP 端口号。

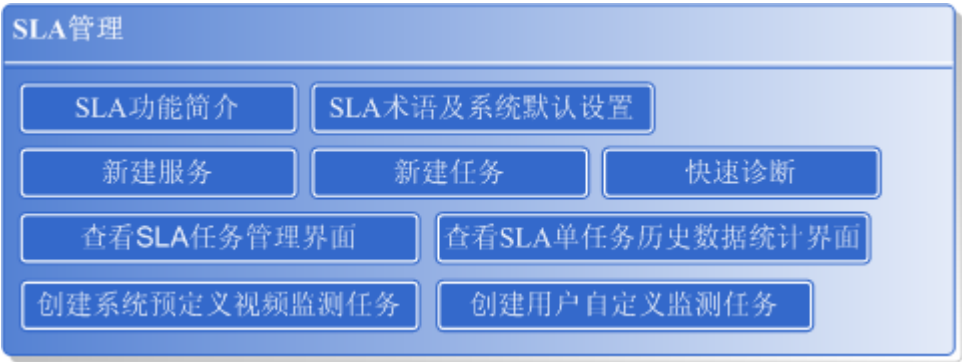
9.4.2 SLA 管理全景图

通过 SLA 全景图可以了解 SLA 管理的所有操作，并根据实际情况，选择操作方式。

SLA 管理全景图，如图 9-27 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

SLA 管理全景图

图 9-27 SLA 管理全景图



SLA 操作的简要说明如表 9-15 所示。

表 9-15 操作简要说明

操作	说明	操作入口
9.4.1.2 SLA 功能简介	SLA 是一个网络性能度量与诊断工具，它通过主动在多个网元或链路之间发送诊断报文来实现对网络性能的度量。	“网络应用 > SLA 管理 > SLA 概述”
9.4.1.3 SLA 术语及系统默认设置	在使用 SLA 之前，需要掌握 SLA 业务的基本概念和系统的默认设置，保证相关操作顺利完成。	“网络应用 > SLA 管理 > SLA 概述”
9.4.3.1 新建服务	SLA 服务：SLA 服务是业务、业务质量、测试例三者的融合体，业务即通常所说的语音视频等常见应用；测试例即设备的 UDP Echo、FTP 等诊断测试功能；业务质量可由对测试例指标所设置阈值的高低反映出来。	“网络应用 > SLA 管理 > SLA 服务管理”
9.4.3.2 新建任务	SLA 任务是为测试具体的网络链路及其质量的测试任务实例。	“网络应用 > SLA 管理 > SLA 任务管理”

操作	说明	操作入口
9.4.3.3 快速诊断	快速诊断功能用来诊断 SLA 任务所监控的链路之间的通断。	“网络应用 > SLA 管理 > 快速诊断”
9.4.4.1 查看 SLA 任务管理界面	用户浏览系统中存在的 SLA 任务的总体信息。该 SLA 任务管理界面可作为用户长期监控 SLA 的界面。	“网络应用 > SLA 管理 > SLA 任务管理”
9.4.4.2 查看 SLA 单任务历史数据统计界面	SLA 单任务详细信息的界面可展示出该条 SLA 任务下发到设备后，测试例返回的指标值在某时间范围内的曲线图。	“网络应用 > SLA 管理 > SLA 任务管理”
9.4.5.1 示例：创建系统预定义视频监测任务	通过学习本示例，您可参照示例中的步骤，独立完成系统预定义任务的创建。	“网络应用 > SLA 管理 > SLA 任务管理”
9.4.5.2 示例：创建用户自定义监测任务	通过学习本示例，您可参照示例中的步骤，独立完成自定义任务的创建。	“网络应用 > SLA 管理 > SLA 任务管理”

9.4.3 配置 SLA 任务

介绍配置 SLA 任务的操作方法。

9.4.3.1 新建服务

SLA 服务是业务、业务质量、测试例三者的融合体，业务即通常所说的语音视频等常见应用；测试例即设备的 UDP Echo、FTP 等诊断测试功能；用户期望的业务质量可由对测试例指标所设置阈值的高低反映出来。

背景信息

系统提供多种预定义服务供用户选择，在预定义服务不满足用户需求情况下，用户可新建服务。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > SLA 管理”。
- 步骤 2** 在导航树中选择“SLA 服务管理”，单击“创建”。
- 步骤 3** 用户输入“名称”、“描述”、“符合度阈值”，选择对应的“星级”。
- 步骤 4** 在页面下方的表格中勾选对应的“测试例”，输入对应的“阈值”和“权重”。



说明

测试例名称被选中将采集该测试例下所有指标数据；指标设置阈值将参与符合度计算，反之则不参与符合度计算。

系统根据用户选择的星级，提供默认的阈值和权重。

步骤 5 单击“确定”，即完成服务的创建。

----结束

后续处理

完成服务的创建后，即可在“SLA 服务管理”页面查看该条服务。

9.4.3.2 新建任务

SLA 任务是为监控具体的网络链路及其上承载的业务质量的测试任务实例。

背景信息

用户已创建 SLA 服务。

操作步骤

步骤 1 在主菜单中选择“网络应用 > SLA 管理”。

步骤 2 在导航树中选择“SLA 任务管理”，单击“创建”。

步骤 3 设置任务基本参数：

1. 填写“任务名称”、“任务描述”。
2. 在“服务名称”中，选择用户所需的服务，如不存在用户所需的服务，在“SLA 服务管理”中创建。
3. 在“源设备”中选择对应的源设备，在“目的 IP”中选择对应的目的设备和接口。



说明
目的 IP 最多支持五个，且支持用户手工输入。

步骤 4 设置任务执行策略：

1. 选择任务执行的“起止日期”，或直接手工输入。



说明
创建任务会在下一个周期的整数倍时刻开始执行。例如：当前时间为 9:28，任务周期为 5 分钟，则任务会在 9:30 开始执行，每 5 分钟执行一次。

2. 选择“执行周期”和“执行工作日”。

步骤 5 设置告警策略：

1. 选择是否“触发符合度告警”，如选择是，则符合度低于用户设置的阈值时，触发告警。
2. 选择是否“触发指标告警”，如选择是，则指标的采集值低于用户设置的阈值时，触发告警。



说明
因系统支持的指标多达几十种，如网络情况差且用户设置了大量的阈值，则告警数量会繁多，请用户谨慎选择。

步骤 6 设置测试例参数：

测试例的数量由用户在“任务基本参数”中选择的“服务名称”以及源设备所支持的测试例决定。

步骤 7（可选）单击“测试”，可以检测新建的 SLA 任务是否能正常运行。

步骤 8 单击“确定”，即可完成任务的创建。

----结束

9.4.3.3 快速诊断

快速诊断功能用来临时发起源宿设备间的链路及其之上的业务的诊断。

背景信息

用户已创建 SLA 服务。

操作步骤

步骤 1 在主菜单中选择“网络应用 > SLA 管理”。

步骤 2 在导航树中选择“快速诊断”。

步骤 3 设置任务基本参数：

1. 在“服务名称”中，选择用户所需的服务，如不存在用户所需的服务，在“SLA 服务管理”中创建。
2. 在“源设备”中选择对应的源设备，在“目的 IP”中选择对应的目的设备和端口。

步骤 4 设置测试例参数：

测试例参数的数量由用户在“任务基本设置”中选择的“服务名称”以及源设备所支持的测试例决定。

测试例参数的具体含义详见对应设备所提供资料的“特性描述手册”。

步骤 5 单击“诊断”，弹出诊断界面，显示“执行状态”和“连通性状态”和其他诊断参数值。

----结束

9.4.4 监控 SLA 任务

介绍监控 SLA 任务的操作方法。

9.4.4.1 查看 SLA 任务管理界面

用户浏览系统中存在的 SLA 任务的总体信息。该 SLA 任务管理界面可作为用户长期监控 SLA 的界面。

操作步骤

步骤 1 在主菜单中选择“网络应用 > SLA 管理”。

步骤 2 在左侧导航树中选择“SLA 管理 > SLA 任务管理”，即进入 SLA 任务的管理界面。

- 步骤 3** 界面上方为条件过滤区，用户可按照“任务名称”、“服务名称”、“源设备”、“当日符合度”进行过滤查询。
- 步骤 4** 界面表格上方为工具栏，系统提供“创建”、“删除”、“启动”、“停止”四种操作。
除“创建”外，其他三种操作都支持批量下发。
- 步骤 5** 界面中心为表格区，展示了各条任务的主要信息。其中的动态信息“状态”、“当日符合度”、“告警数量”会根据任务的运行情况动态刷新。
- 步骤 6** 表格操作区提供“查看历史数据”、“复制创建”、“诊断”三种功能。
- “查看历史数据”详见 [9.4.4.2 查看 SLA 单任务历史数据统计界面](#)。
 - “复制创建”：和创建功能相似，但会复制选中的该条记录的所有信息，仅任务名称不同。
 - “诊断”：判断该条任务的通断，和导航栏“快速诊断”功能相同。

----结束

9.4.4.2 查看 SLA 单任务历史数据统计界面

SLA 单任务历史数据统计界面可展示出该条 SLA 任务下发到设备后，测试例返回的指标值在某时间范围内的曲线图。

操作步骤

- 步骤 1** 在主菜单中选择“网络应用 > SLA 管理”。
- 步骤 2** 在左侧导航树中选择“SLA 管理 > SLA 任务管理”，即进入 SLA 任务的管理界面。
- 步骤 3** 在界面右侧的表格操作区，单击某条任务后的“历史数据”图标，即展开该条任务的指标统计图形化界面。
- 用户可在最上方的过滤区选择要查看数据的时间跨度。
 - 最上方的可折叠区域为“符合度”区域，用户可直观查看到某时间跨度内符合度的折线图及与用户所设置的阈值的对比，蓝色线条代表实际的 SLA 符合度，红色线条代表用户所设置的阈值。
 - 下方的可折叠区域为测试例指标展示区域，系统根据任务中服务所对应的测试例个数不同，会展示多个区域，用户可在折叠区域的右侧进行指标的切换。其中蓝色线条代表实际的指标取值，红色线条代表该任务中用户设置的服务星级对应的阈值。
 - 所有的可折叠区域内的 SLA 数据，都支持“导出数据”。

 说明

汇聚数据保存策略：

- 原始数据：原始数据保存一个月。
- 小时：小时数据保存一年。
- 天：天数据保存一年。
- 周：周数据保存三年。
- 月：月数据保存没有限制。

----结束

9.4.5 SLA 配置举例

介绍 SLA 的两个典型应用。

9.4.5.1 示例：创建系统预定义视频监测任务

通过学习本示例，您可参照示例中的步骤，独立完成系统预定义任务的创建。

前提条件

- 具有“操作员”及以上的网管用户权限。
- 网管与网元间已建立通信，且能对网元进行管理和维护。
- 设备支持内置 NQA 探针。

场景介绍

由于业务的增长，深圳 A 公司 B 大楼新增了一台设备，这台设备在网络中已完成安装和调测，并加入到网管中进行管理，管理员小王现需要测试这台设备和其他设备之间承载的视频业务质量，以便尽快发现和解决问题。

操作步骤

步骤 1 在主菜单中选择“网络应用 > SLA 管理”。

步骤 2 在导航树中选择“SLA 任务管理”，单击“创建”。

步骤 3 设置任务基本参数：

1. 填写“任务名称”为“B 大楼视频测试”、“任务描述”为“B 大楼视频测试专用”。
2. 在“服务名称”中，选择“视频”。
3. 在“源设备”中选择该新设备，在“目的 IP”中选择临近设备的 IP 和接口。

步骤 4 设置任务执行策略和告警策略可按照系统默认提供的方式，无需更改。单击“确定”即完成任务的创建。

----结束

9.4.5.2 示例：创建用户自定义监测任务

通过学习本示例，您可参照示例中的步骤独立完成自定义任务的创建。

前提条件

- 具有“操作员”及以上的网管用户权限。
- 网管与网元间已建立通信，且能对网元进行管理和维护。
- 设备支持内置 NQA 探针。

场景介绍

A 公司 B 大楼内，员工投诉经常出现即时通讯业务中断，严重影响工作效率，管理员小王现需要测试 B 大楼的出口设备和公司出口设备之间承载的即时通讯业务质量，以便尽快定位和解决问题，提高客户的满意度。

操作步骤

步骤 1 在主菜单中选择“网络应用 > SLA 管理”。

步骤 2 创建 SLA 服务：

1. 在导航树中选择“SLA 服务管理”，单击“创建”。
2. 填写“服务名称”为“即时通讯业务”、“服务描述”为“测试即时通讯业务质量”、“符合度阈值”填写为“80”、选择“星级”为“五星级”。
3. 勾选表格区“ICMP Echo”和“UDP Echo”，设置其阈值和权重。
4. 单击“确定”，即完成服务的创建。

步骤 3 创建 SLA 任务，设置任务基本参数：

1. 在导航树中选择“SLA 任务管理”，单击“创建”。
2. 填写“任务名称”为“B 楼即时通讯业务”、“任务描述”为“测试 B 楼即时通讯业务质量”。
3. 在“服务名称”中，选择刚刚新建的“即时通讯业务”。
4. 在“源设备”中选择 B 楼出口设备，在“目的 IP”中选择公司出口设备和对应的接口。

步骤 4 设置任务执行策略：

1. 选择任务执行的“起止日期”，或直接手工输入。
2. 选择“执行周期”为“5 分钟”，“执行工作日”为周一到周五。

步骤 5 设置告警策略：

1. 选择“触发符合度告警”为“是”。
2. 选择“触发指标告警”为“否”。

步骤 6 设置测试例参数：

1. 填写“ICMP Echo”所对应的测试例参数。
2. 填写“UDP Echo”所对应的测试例参数。

步骤 7 单击“确定”，即完成该任务的创建。

系统同时提供“测试”的功能，可以检测一下，新建的 SLA 任务是否能正常运行。

----结束

10 智能配置工具

关于本章

介绍智能配置工具提供的主要功能及配置方法。

10.1 智能配置工具全景图

通过智能配置工具全景图可以了解智能配置工具的所有操作，并根据实际情况，选择操作方式。

10.2 智能配置工具功能

在搭建网络环境的过程中，对大量网元的配置操作是必不可少的。用户根据网络规划表手工制作脚本时，不仅耗时长，且容易出错。智能配置工具可以通过配置模板和规划表一键式将同一配置多个参数批量下发到网元，大大提升配置网元的效率。

10.3 智能配置工具流程介绍

介绍智能配置工具“按模板下发”和“按规划表下发”两大主要功能的主要流程。

10.4 智能配置工具配置任务

介绍使用智能配置工具的配置流程，包括模板管理与下发和规划表管理与下发。

10.5 智能配置工具配置示例

为了能够帮助网络管理员更好的了解智能配置工具，这里介绍了两种常见的典型应用。

10.1 智能配置工具全景图

通过智能配置工具全景图可以了解智能配置工具的所有操作，并根据实际情况，选择操作方式。

智能配置工具全景图，如图 10-1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

智能配置工具全景图

图 10-1 智能配置工具全景图



智能配置工具操作的简要说明如表 10-1 所示。

表 10-1 操作简要说明

操作	说明	操作入口
按模板下发	模板下发主要功能为将常用的或用户自定义的命令行集，由用户输入所需参数，下发到多个设备上。	“操作维护 > 智能配置工具 > 模板下发”
按规划表下发	按规划表下发的主要功能为，将同一模板设置不同的参数，下发到网络规划表中不同的网络设备上。	“操作维护 > 智能配置工具 > 规划表下发”
下发记录管理	介绍了下发记录的数据来源及界面操作。	“操作维护 > 智能配置工具 > 下发记录”
新建模板	智能配置工具提供系统预定义模板、用户自定义模板两种方式。	“操作维护 > 智能配置工具 > 模板下发”
部署模板	部署模板即是网管中存在的模板，下发到对应网元。	“操作维护 > 智能配置工具 > 模板下发”

操作	说明	操作入口
导出规划表	即将校验过的模板按固定格式导出，待用户修改后，用于用户在“规划表下发”功能中导入，实现将同一模板设置不同的参数，下发到不同的网络设备上。	“操作维护 > 智能配置工具 > 模板下发”
规划表管理与下发	通过规划表管理，用户可以将同一模板的不同参数，下发到不同网元上。	“操作维护 > 智能配置工具 > 下发记录”
示例：按模板下发场景	智能配置工具可以将某个配置片段部署到一台或者多台设备上。	“操作维护 > 智能配置工具 > 模板下发”
示例：按规划表下发场景	通过导入规划数据，智能配置工具可以自动生成每个网元的配置脚本并下发到设备。	“操作维护 > 智能配置工具 > 规划表下发”

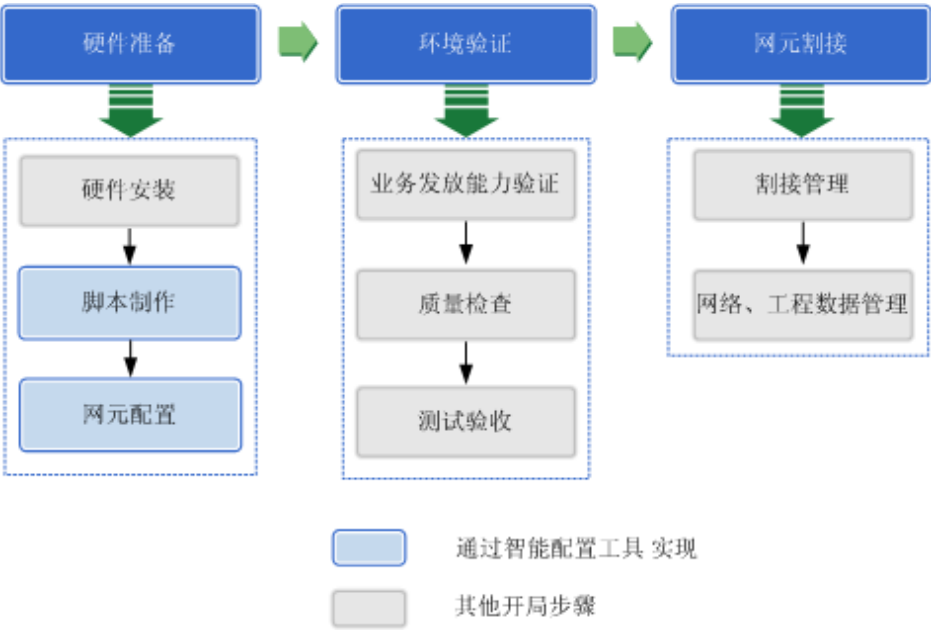
10.2 智能配置工具功能

在搭建网络环境的过程中，对大量网元的配置操作是必不可少的。用户根据网络规划表手工制作脚本时，不仅耗时长，且容易出错。智能配置工具可以通过配置模板和规划表一键式将同一配置多个参数批量下发到网元，大大提升配置网元的效率。

- 智能配置工具提供了模板管理的功能，可以快速生成配置脚本，用来对多个网元进行同一条命令行批量配置。
- 智能配置工具还提供了规划表下发的功能，可以根据网络规划表，用来对多个网元进行同一条命令行不同参数的批量下发。

智能配置工具的使用场景如图 10-2 所示。

图 10-2 智能配置工具使用场景



智能配置工具应用于开局流程中的脚本制作过程和设备配置过程，实现了命令行的图形化下发。目前只支持华为设备。

10.3 智能配置工具流程介绍

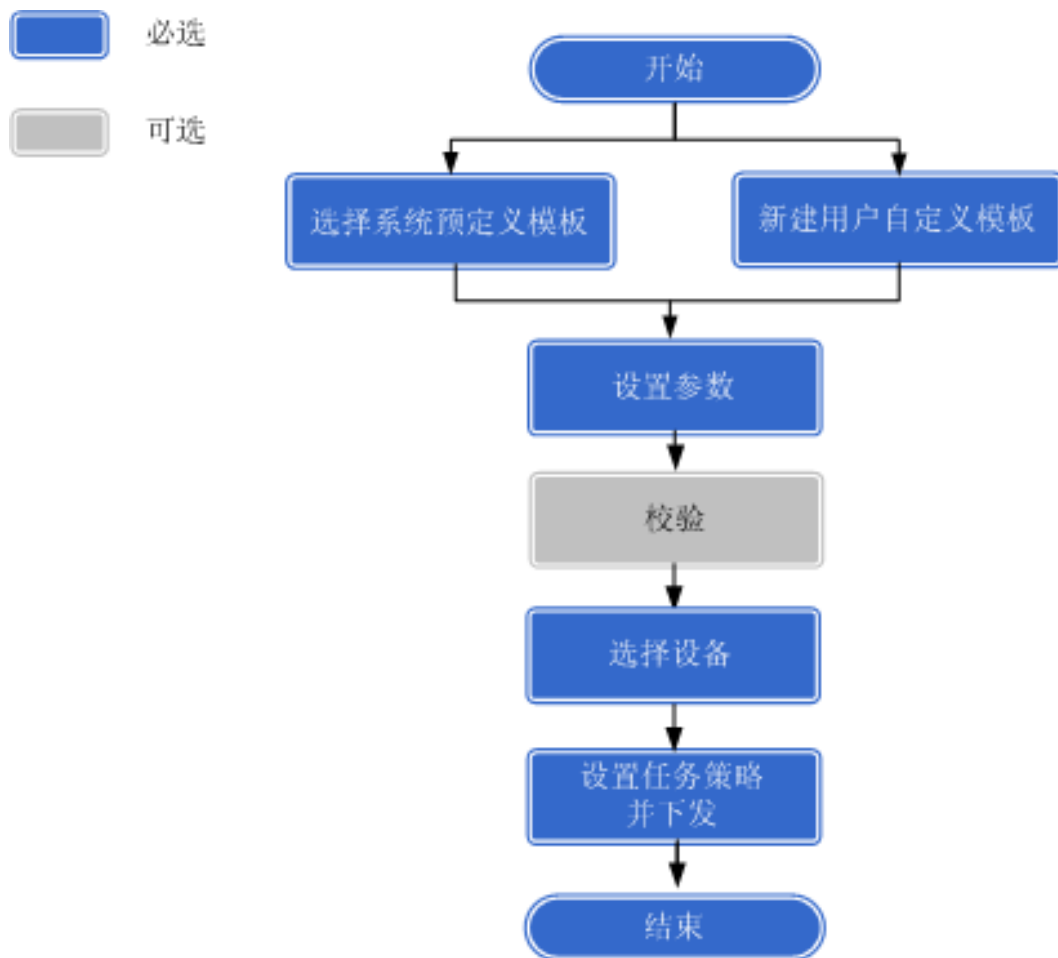
介绍智能配置工具“按模板下发”和“按规划表下发”两大主要功能的主要流程。

10.3.1 按模板下发

主要功能为将常用的或用户自定义的命令行集，由用户输入所需参数，下发到多个设备上。

流程说明

图 10-3 按模板下发流程图



功能说明

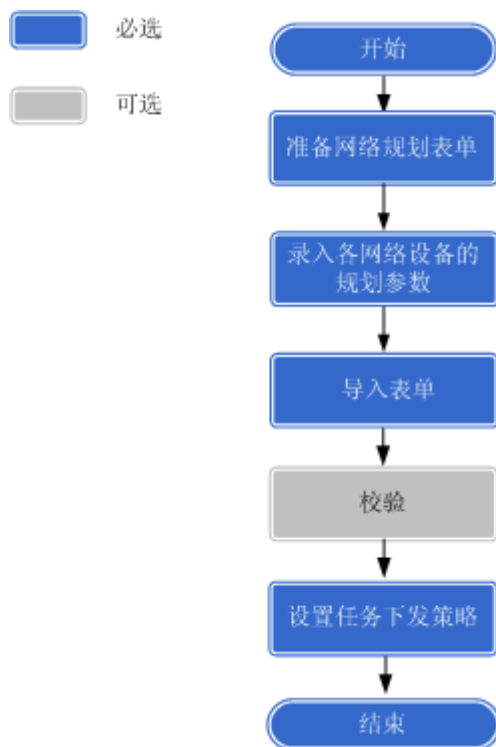
1. 模板库
 - 系统预定义模板：显示系统预定义的各种常用模板。
 - 用户自定义模板：在用户自定义文件夹中显示用户自定义的模板，提供新建、复制创建、移动、修改和删除功能，也可以创建文件夹将模板分类，便于查找和管理。
2. 模板下发
 - “部署”即是把模板库中已有的模板，待用户填写所需参数后，下发到多个设备上。
 - 需要经过模板选择，参数配置、设备选择，任务设置三个步骤

10.3.2 按规划表下发

主要功能为将同一模板设置不同的参数，下发到网络规划表中不同的网络设备上。

流程说明

图 10-4 按规划表下发流程图



主要功能说明

1. 导入表单

- 规划表单：该规划表可以通过“模板下发”导航树中的“导出规划表单”来生成，也可以用户在本地手工创建。
- 根据用户在网络规划表中输入网络设备的名称、ip 地址及各网络设备对应的参数，即可生成对应的脚本。
- 规划表单只支持 Office2003 的 Excel 格式，暂不支持 Office2007 及以上版本格式。

2. 校验

- 校验即为将网管服务器存放的设备的命令集和当前用户输入的参数进行匹配。
- 若网管服务器不存在设备的命令集，系统将实时去设备上获取。

10.3.3 下发记录管理

介绍了下发记录的数据来源及界面操作。

功能说明

通过下发记录，可查看所有任务的执行状态和详细执行结果。

1. 在下发记录表格中，系统显示所有任务的“任务名称”、“任务类型”、“任务状态”、“任务结果”、“任务描述”、“创建时间”、“执行时间”。
2. 单击表格最后一列“操作”，可以查看任务的详细信息，包含该任务所下发的“设备名称”、“IP 地址”、“设备类型”、单击“配置命令”可以看到用户下发的配置命令，单击“下发结果”，可以看到该配置命令在命令行执行的详细结果。
3. 单击“导出结果”，即将单任务下，所下发的所有设备执行信息保存到本地。
4. 系统支持对任务记录的批量删除。
5. 智能配置工具的操作日志记录在日志中，路径为：“eSight 安装路径\gcli\deploy\log\SctOperation-YEAR.MON.DAY-HOUR.MIN.SEC.log”。

10.4 智能配置工具配置任务

介绍使用智能配置工具的配置流程，包括模板管理与下发和规划表管理与下发。

10.4.1 模板管理与下发

模板下发主要功能为将常用的或用户自定义的命令行集，由用户输入所需参数，下发到多个设备上。

10.4.1.1 新建模板

智能配置工具提供系统预定义模板、用户自定义模板两种方式。

背景信息

系统提供多种预定义模板供用户选择，在预定义模板不满足用户需求情况下，用户可新建模板。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 智能配置工具”。
- 步骤 2** 在导航树中选择“模板下发”。
- 步骤 3** 单击“新建模板”，系统即切换到新建模板的页面。
- 步骤 4** 用户选择“所在目录”、输入“模板名称”和“描述”，在“配置内容”区域键入所需下发的命令。



注意

拷贝命令时文字不能带有格式，比如不能从网页中拷贝命令，这样会带有隐藏的特殊字符。



说明

配置内容一栏，一般需要在开头输入命令 system-view，用于进入系统视图。而退出命令 quit 则可以输入，在生成模板时，系统会根据命令行匹配自动追加。

- 步骤 5** 单击“确定”，即新建模板成功，用户可以在模板库表格的“用户模板”文件夹中查看到新建的模板。



说明

用户若单击“生成模板”，则需要选择一个设备，进行校验，校验成功后，生成表格模板。两者的区别即为是否需要校验。

----结束

10.4.1.2 部署模板

将网管中存在的模板，下发到对应网元。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 智能配置工具”。
- 步骤 2** 在导航树中选择“模板下发”，在模板库表格中查找用户所需下发的模板。
- 步骤 3** 单击“部署”，即进入模板下发的导航页面。
- 步骤 4** 模板下发第一步“配置参数”：在命令表格中设置对应的参数，单击“下一步”。
- 步骤 5** 模板下发第二步“选择设备”：单击“增加”，在弹出的“选择设备”对话框内选择所需下发的网元集合，单击“确定”即关闭对话框，单击“下一步”。
- 步骤 6** 模板下发第三步“任务设置”：用户输入“任务名称”、“任务描述”（可选）、选择“计划执行时间”和“配置恢复策略”（可选），单击“下发/确定”。在“确认”对话框中单击“是”。

----结束

后续处理

1. 选择“下发记录”页签。
2. 即可在任务列表中查看到各个任务执行的进度和下发到各个设备的详细内容。

10.4.1.3 导出规划表

将校验过的模板按固定格式导出，待用户填写配置信息后，用于用户在“规划表下发”功能中导入，实现将同一模板设置不同的参数，下发到不同的网络设备上。

前提条件

模板通过了校验。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 智能配置工具”。
- 步骤 2** 在导航树中选择“模板下发”，在模板库表格中查找所需模板。
- 步骤 3** 选中该模板后单击“导出规划表单”，系统即弹出“导出规划表单”的对话框。
- 步骤 4 可选：**用户输入“前预置列”和“后预置列”。

规划表导出后为 excel 格式，用户在导出表格头尾增加前后预置列，方便标识如设备地理位置、备注等信息，利于维护。

步骤 5 选择欲导出的设备。

步骤 6 单击“确定”，即弹出“文件下载”对话框，单击“保存”，选择存储路径后存储到本地。

步骤 7 关闭对话框，即完成导出规划表。

----结束

10.4.2 规划表管理与下发

通过规划表管理，用户可以将同一模板的不同参数，下发到不同网元上。

前提条件

- 用户已准备好网络数据规划表，该规划表可以通过“模板下发”导航树中的“导出规划表单”来生成，也可以用户在本地手工创建。



说明

规划表单中如果单元格的内容是表示时间的，如“00:00”，需要将该单元格格式设为“文本”。

- 导出的规划表必须填写完整，且对应的“设备名称”都要真实在网管上存在的，否则无法成功导入。

操作步骤

步骤 1 在主菜单中选择“操作维护 > 智能配置工具”。

步骤 2 在导航树中选择“规划表下发”，页面展现按规划表下发的向导。

步骤 3 单击“导入”，弹出“导入规划表”对话框，选择要加载的文件。

步骤 4 单击“确定”，页面中即显示规划表中的“设备名称”、“IP 地址”、“设备类型”。

步骤 5 可选: 单击“校验”，页面表格上即显示对应的“校验结果”。

步骤 6 可选: 用户可单击“删除”，删除校验失败的设备。

步骤 7 单击“下一步”，即展现“任务设置”页面。

步骤 8 输入“任务名称”、“任务描述”、选择“计划执行时间”和“配置恢复策略”，单击“下发”。

步骤 9 用户可在当前页面看到该任务执行的进度和下发到各个设备的详细内容。也可在“下发记录”页签，查看该任务执行的详细信息。

----结束

10.5 智能配置工具配置示例

为了能够帮助网络管理员更好的了解智能配置工具，这里介绍了两种常见的典型应用。

10.5.1 示例：按模板下发场景

背景信息

用户需要将某个配置片段统一部署到一台或者多台设备上。

如：下发“批量创建 VLAN”配置片段到 IP 地址为 10.138.35.43 和 10.38.35.60 的两个设备上，该配置片段有两个参数：vlan 起始编号和 vlan 终止编号，并希望按照指定的部署顺序立即执行部署任务。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 智能配置工具”。
- 步骤 2** 在导航树中选择“模板下发”，在模板库表格中选择“批量创建 vlan”。
- 步骤 3** 选中该模板后单击“部署”，系统即显示模板下发的配置向导。
- 步骤 4** 模板下发第一步“配置参数”：用户可根据需要修改起始和终止 vlan 编号。单击“下一步”。

说明

- 对于带星号的参数，都要设置其参数值。系统如果未填写参数值，生成的脚本不会包含该命令。
- 系统提供默认参数，供用户修改。

- 步骤 5** 模板下发第二步“选择设备”：单击“选择设备”，系统弹出“选择设备”对话框，显示网管中已加载的设备列表。选择 IP 地址为 10.38.35.43 和 10.138.35.60 的两个设备，单击“确定”关闭设备列表，回到原页面，单击“下一步”。

说明

- 在选择设备操作之后，用户可选择对命令行进行校验，校验时间可能较长，并且不可中断，请谨慎进行校验操作。
- 验证脚本可以在离线的情况下实现，根据命令集验证脚本语法的正确性。

- 步骤 6** 模板下发第三步“任务设置”：用户输入“任务名称”、“任务描述”（可选）、选择“计划执行时间”和“配置恢复策略”，单击“下发”。

----结束

后续处理

1. 选择“下发记录”页签。
2. 即可在任务列表中查看到各个任务执行的进度和下发到各个设备的详细内容。

10.5.2 示例：按规划表下发场景

通过导入规划数据，智能配置工具可以自动生成每个网元的配置脚本并下发到设备。

前提条件

- 请提前准备好网络数据规划表，该规划表可以通过“模板下发”导航树中的“导出规划表单”来生成，也可以用户在本地图工创建。

- 导出的规划表必须填写完整，且对应的“设备名称”、“设备 ip”等都要真实在网管上存在的，否则无法成功导入。

背景信息

对于用户自定义模板可以直接进行导出规划表操作，自定义模板需要经过校验生成模板后，才支持导出规划表。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 智能配置工具”。
- 步骤 2** 在导航树中选择“规划表下发”，页面展现按规划表下发的向导。
- 步骤 3** 单击“导入”，弹出“导入规划表”对话框的，选择要加载的文件。
- 步骤 4** 单击“确定”，页面中即显示规划表中的“设备名称”、“IP 地址”、“设备类型”。
- 步骤 5** 单击“校验”，页面表格上即显示对应的“校验结果”。
- 步骤 6** 单击“下一步”，即展现“任务设置”页面。
- 步骤 7** 输入“任务名称”、“任务描述”、选择“计划执行时间”，单击“下发”。

----结束

后续处理

1. 选择“下发记录”页签。
2. 即可在任务列表中查看到各个任务执行的进度和下发到各个设备的详细内容。

11 设备配置文件管理

关于本章

设备上的配置文件随着设备上各种业务不断的变更或扩展，设备配置文件的内容会发生变化，为了保证设备配置文件的安全性，网管需要提供备份设备配置文件、恢复设备配置文件的功能。

11.1 设备配置文件管理全景图

通过设备配置文件管理全景图可以了解设备配置文件管理的所有操作，并根据实际情况，选择操作方式。

11.2 设置 FTP 参数

在对设备配置文件进行备份、恢复操作前，需确认文件传输服务 FTP 参数配置正确，以确保网元与网管之间文件传输服务正常运行。

11.3 备份网元配置数据

因网元维护或升/降级需要，将网元数据备份到网管服务器上，以防止升/降级或意外原因导致网元数据损坏或丢失。

11.4 管理网元配置数据

介绍管理网元配置数据的常用操作。

11.5 恢复网元配置数据

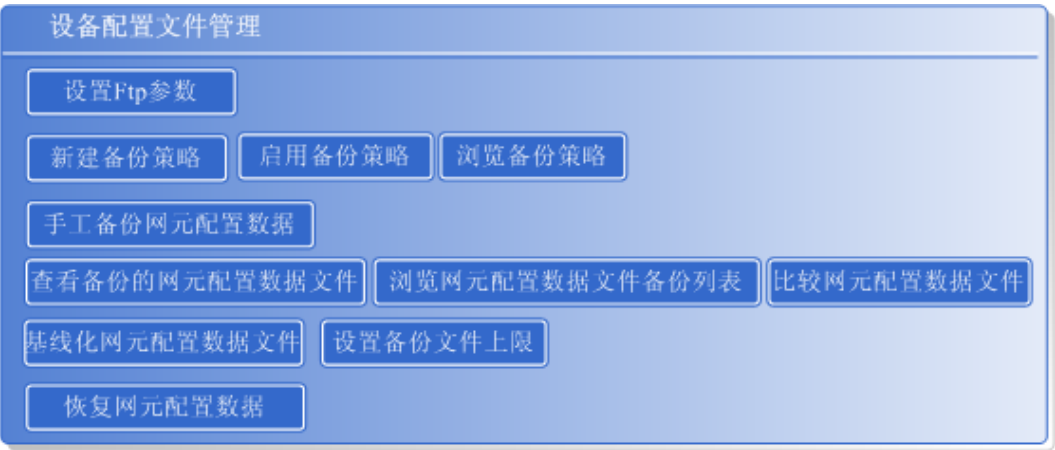
当设备系统遇到故障时，可通过将配置文件恢复上传到设备上，恢复网元配置数据。

11.1 设备配置文件管理全景图

通过设备配置文件管理全景图可以了解设备配置文件管理的所有操作，并根据实际情况，选择操作方式。

设备配置文件操作全景图，如图 11-1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 11-1 设备配置文件操作全景图



设备配置文件操作的简要说明如表 11-1 所示。

表 11-1 操作简要说明

操作	说明	操作入口
设置 Ftp 参数	在对设备配置文件进行备份、恢复操作前，需确认文件传输服务 FTP 参数配置正确，以确保网元与网管之间文件传输服务正常运行。	“操作维护>配置文件管理”
新建备份策略	当需要对指定类型的网元单独进行策略管理时，可以新建任务。	“操作维护>配置文件管理”
启用备份策略	当配置文件的备份任务处于禁用状态时，需要及时启动备份任务，备份任务才可正常运行。	“操作维护>配置文件管理”
浏览备份策略	通过浏览备份任务，便于对备份任务的管理。	“操作维护>配置文件管理”

操作	说明	操作入口
手工备份网元配置数据	需要对网元的配置文件进行即时备份时，可以使用手工备份网元配置数据的方法，即时执行备份操作。	“操作维护>配置文件管理”
查看备份的网元配置数据文件	介绍查看备份的网元配置文件和正在运行的配置文件的方法。	“操作维护>配置文件管理”
浏览网元配置数据文件备份列表	用户备份了配置文件之后，需要浏览一下该网元备份的所有配置文件的备份情况，以确保成功备份了相关配置文件。	“操作维护>配置文件管理”
比较网元配置数据文件	通过比较网元配置文件，可以了解不同配置文件之间的差异。	“操作维护>配置文件管理”
基线化网元配置数据文件	设备的运行配置文件备份到网管上后，对配置文件进行基线化标识，以方便基线化文件恢复操作。	“操作维护>配置文件管理”
设置备份文件上限	对于配置文件的备份个数需要进行限制，不允许备份个数持续的增加，以避免备份文件所占用的存储空间持续增长。	“操作维护>配置文件管理”
恢复网元配置数据	当设备系统遇到故障时，可通过将配置文件恢复上传到设备上，恢复网元配置数据。	“操作维护>配置文件管理”

11.2 设置 FTP 参数

在对设备配置文件进行备份、恢复操作前，需确认文件传输服务 FTP 参数配置正确，以确保网元与网管之间文件传输服务正常运行。

背景信息



说明

FTP 使用的端口必须为 21。

为了确保备份恢复操作功能正常，网管服务器上只能启动网管自带的 FTP 服务。

FTP 默认用户名：admin，密码：Changeme123。

FTP 默认文件传输路径：“esight 安装目录/AppBase/var/runtime.center/data/ftp”。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树上选择“系统参数设置 > FTP 参数”。
- 步骤 3** 设置 FTP 的配置参数，单击“应用”。

----结束

11.3 备份网元配置数据

因网元维护或升/降级需要，将网元数据备份到网管服务器上，以防止升/降级或意外原因导致网元数据损坏或丢失。

11.3.1 使用备份任务备份网元配置数据

通过使用备份任务，网管可以按照备份任务自动实现网元配置数据的周期备份。

11.3.1.1 新建备份任务

当需要对指定类型的网元单独进行策略管理时，可以新建任务。

前提条件

网管与网元通信正常。

已配置并启动 FTP 服务，配置 FTP 操作请参考 [11.2 设置 FTP 参数](#)。

对于自定义设备，需配置网管侧和网元侧的 Telnet 参数为相同值。

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 备份任务”。
- 步骤 3** 单击“创建”，配置备份任务的相关参数。
- 步骤 4** 在“应用到设备”后单击“增加”，选择相关设备，单击“确定”，将备份任务应用到这些设备上。
- 步骤 5** **可选：**根据需要，可在“应用到设备”窗格中选中相应设备，单击“删除设备”，取消将备份应用到该设备上。
- 步骤 6** 单击“确定”。

----结束

11.3.1.2 启用备份任务

当配置文件的备份任务处于禁用状态时，需要及时启动备份任务，备份任务才可正常运行。

前提条件

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 备份任务”。
- 步骤 3** 设置“状态”为“禁用”的过滤条件，单击“搜索”。
- 步骤 4** 选择相应的备份策略，单击“启用”。

----结束

11.3.1.3 维护备份任务

通过浏览备份任务，便于对备份任务的管理。

前提条件

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 备份任务”。
- 步骤 3** 在窗口上方设置过滤参数，单击“搜索”。
- 步骤 4** **可选：**若“最新备份结果”为“失败”或“部分成功”，可单击“失败”或“部分成功”，查看详细的记录信息。排除故障后，选中相应设备，重新备份。
- 步骤 5** **可选：**根据需要，可执行如下操作。
 - 在相应的备份策略中单击，修改其相关参数。
 - 在相应的备份策略中单击，立即执行备份操作。
 - 选中相应的备份策略，单击“禁用”，禁用该备份策略。
 - 选中相应的备份策略，单击“删除”，删除该备份策略。

----结束

11.3.2 手工备份网元配置数据

需要对网元的配置文件进行即时备份时，可以使用手工备份网元配置数据的方法，即时执行备份操作。

前提条件

网管与网元通信正常。

已配置并启动 FTP 服务，配置 FTP 操作请参考 [11.2 设置 FTP 参数](#)。

配置网管侧和网元侧的 Telnet 参数为相同值。

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树上选择“设备配置管理 > 配置文件”。
- 步骤 3** 如果选中一个或多个设备，选择“备份 > 备份选中”，备份选中设备的相关信息；如果需要备份全部可以直接单击“备份 > 备份所有”，若设置了搜索条件，只能备份该搜索条件下的所有设备的相关信息。

----结束

操作结果

当设备上正在运行的配置文件与已备份的配置文件相同时，网管默认保留原有的配置文件，丢弃刚备份的配置文件。

当设备上正在运行的配置文件与已备份的配置文件不同，且备份的文件已达到上限时，则网管默认丢弃最早的非基线配置文件。

11.4 管理网元配置数据

介绍管理网元配置数据的常用操作。

11.4.1 查看网元配置数据文件

介绍查看备份的网元配置文件和正在运行的配置文件的方法。

前提条件

备份文件的格式为*.cfg。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 配置文件”。
- 步骤 3** 查看设备当前运行的配置文件。在相应的设备后，单击.
- 步骤 4** 单击相应设备的“文件名称”，查看已备份的最新配置文件。
- 步骤 5** 查看备份的设备配置文件。
 - 1. 在相应的设备中单击，进入文件管理界面。
 - 2. 在相应的配置文件后单击，查看该配置文件。

----结束

11.4.2 浏览网元配置数据文件备份列表

用户备份了配置文件之后，需要浏览一下该网元备份的所有配置文件的备份情况，以确保成功备份了相关配置文件。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 配置文件”。
- 步骤 3** 在相应的设备中单击，在文件管理列表中查看备份了网元配置数据文件。

----结束

11.4.3 比较网元配置数据文件

通过比较网元配置文件，可以了解不同配置文件之间的差异。

前提条件

网管上已备份 2 个或以上的网元配置文件。

已配置 SNMP 写权限。

操作步骤

- 步骤 1** 在主菜单中选择“操作维护 > 配置文件管理”。
- 步骤 2** 在左侧导航树选择“设备配置管理 > 配置文件”。
- 步骤 3** 在相应的设备中单击，进入网元的配置文件管理界面。
- 步骤 4** 选择待比较的两个配置文件，单击“比较”，查看两个配置文件之间的比较结果。
- 可通过选择“显示所有内容”和“显示差异内容”对显示比较结果进行定制。
 - 在界面下方，查看“相同的行”、“修改的行”、“添加的行”和“删除的行”，整体掌握配置文件的差异点。
 - 可单击“上一个不同”或“下一个不同”高亮显示差异点。

----结束

11.4.4 基线化网元配置数据文件

设备的运行配置文件备份到网管上后，对配置文件进行基线化标识，以方便基线化文件恢复操作。

前提条件

配置文件被成功备份到网管。

背景信息

第一次备份下来的配置文件默认为基线化文件，同一个设备上只允许一个配置文件被基线化。

操作步骤

步骤 1 在主菜单中选择“操作维护 > 配置文件管理”。

步骤 2 在左侧导航树选择“设备配置管理 > 配置文件”。

步骤 3 基线化单个设备上的配置文件。

1. 在相应的设备中单击，进入网元的配置文件管理界面。
2. 在待基线化的配置文件后单击，该配置文件的“文件类型”变更为“基线”，表示基线化成功。



说明

为确保设备数据正常，不允许删除基线化配置文件。

步骤 4 可选：批量基线化多设备上备份的最新配置文件。

1. 同时选中多个待基线化的设备，单击“基线化”。
2. 若基线化失败或部分成功，在弹出的“提示”窗口中单击“详细信息”，查看操作失败的原因。
3. 在弹出的“提示”窗口中单击“确定”。

----结束

11.4.5 设置备份文件上限

对于配置文件的备份个数需要进行限制，不允许备份个数持续的增加，以避免备份文件所占用的存储空间的持续增长。

背景信息



注意

当设置的文件上限值小于当前已有的备份文件值时，则网管会自动删除时间最早的多余备份文件，请谨慎操作！

当备份文件个数超出备份上限时，网管默认删除备份时间最早的备份文件。

操作步骤

步骤 1 在主菜单中选择“操作维护 > 配置文件管理”。

步骤 2 在左侧的导航树中选择“系统参数设置 > 文件上限”。

步骤 3 设置“备份上限设置”的值。

步骤 4 选择“变更触发备份设置”模式。



说明

1. “变更触发备份设置”为使能时：当网管监听到设备发出配置变更告警后，配置文件模块自动进行配置文件备份。
2. “变更触发备份设置”为去使能时：当网管监听到设备发出配置变更告警后，配置文件模块不会进行配置文件备份。

步骤 5 单击“应用”。

----结束

11.5 恢复网元配置数据

当设备系统遇到故障时，可通过将配置文件恢复上传到设备上，恢复网元配置数据。

前提条件

已配置 SNMP 写权限。

背景信息



警告

执行恢复网元配置数据，可能导致业务的中断，请谨慎！

操作步骤

步骤 1 在主菜单中选择“操作维护 > 配置文件管理”。

步骤 2 在左侧导航树选择“设备配置管理 > 配置文件”。

步骤 3 恢复单个设备上的配置文件。

1. 在相应的设备配置文件中单击，进入设备文件管理界面。
2. 选择待恢复的配置文件，单击，执行恢复网元配置数据。

步骤 4 可选：批量恢复多个设备的上的基线配置文件。

1. 同时选中多个设备，单击“恢复成基线”。
2. 弹出“确认”对话框，单击“是”。
3. 待恢复操作完成，在弹出的“操作结果”对话框中查看操作结果信息，单击“确定”。

----结束

12 自定义设备管理

关于本章

在多厂商设备共存的网络环境下，eSight 支持对设备类型为 Huawei Device、H3C Device、Cisco Device 和 Unknown 的设备进行定制，从而实现同一网络、统一网管、统一监控，降低运维成本。

12.1 自定义设备管理全景图

通过自定义设备操作全景图可以了解自定义设备管理的所有操作，并根据实际情况，选择操作方式。

12.2 自定义设备功能介绍

eSight 提供统一的管理平台，可以将现网所有支持 SNMP 协议的设备添加到网管，对于预集成设备，eSight 提供完善的管理能力，对于自定义设备（设备类型为 Huawei Device/H3C Device/Cisco Device/Unknown）提供定制功能，客户根据需要对其定制，从而实现 eSight 对现网多厂商设备的统一管理和统一监控。

12.3 自定义设备配置流程

客户在判定需要对自定义设备进行定制时，可以按如下流程方式进行快速、有序、准确定制。

12.4 发现自定义设备

eSight 支持通过三种方式将自定义设备添加到网管上，进行管理。

12.5 自定义厂商和设备类型

对于自定义设备，eSight 无法识别其厂商信息和设备类型，用户可以根据实际情况对其进行定制。

12.6 设备管理能力定制

12.7 检测自定义设备网络状态

定期检测自定义设备的网络状态，实时了解网管和自定义设备之间的通信状态。

12.8 调用自定义设备的 Web 网管

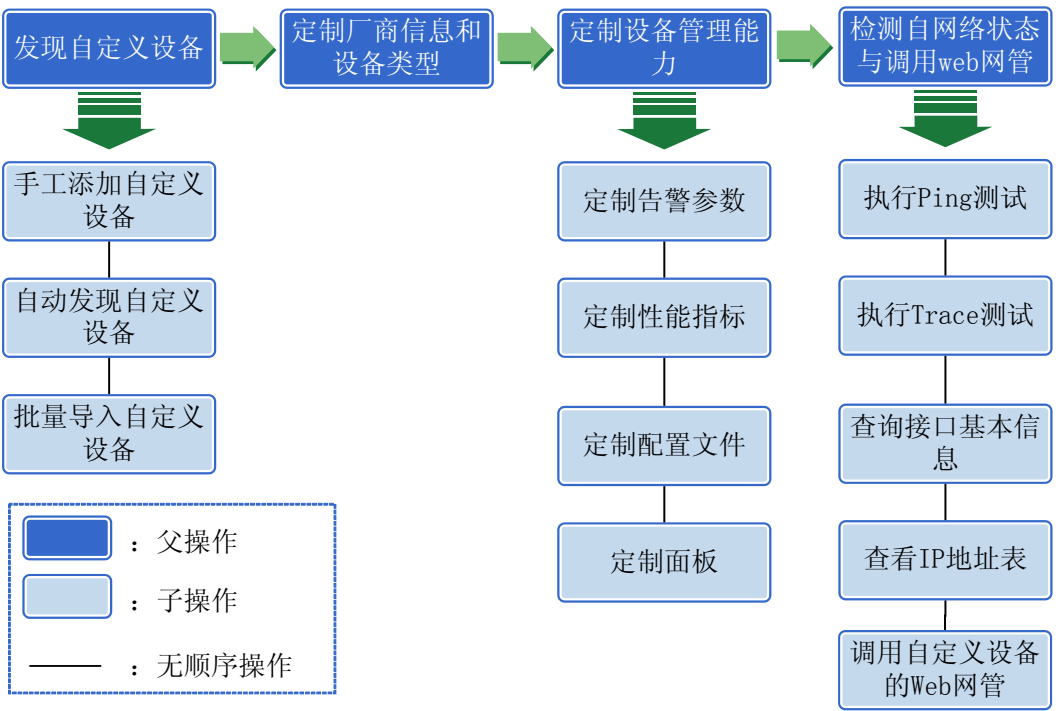
eSight 提供调用自定义设备的 Web 网管功能，通过自定义设备的 web 网管对其进行相关业务配置。

12.1 自定义设备管理全景图

通过自定义设备操作全景图可以了解自定义设备管理的所有操作，并根据实际情况，选择操作方式。

自定义设备管理全景图，如图 12-1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 12-1 系统操作全景图



自定义设备管理的简要说明如表 12-1 所示。

表 12-1 操作简要说明

操作	说明	操作入口
手工添加自定义设备	当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。	“资源 > 资源管理”
自动发现自定义设备	通过网元自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。当指定网段中的所有网元都需要增加到 eSight 时，该功能可以实现批量操作，节省时间。	“资源 > 资源管理”

操作	说明	操作入口
批量导入自定义设备	当开局或设备扩容时，被管设备较多，以创建单个网元方式增加网元比较繁琐，可以选择手工批量导入网元方式批量增加网元。	“资源 > 资源管理”
自定义厂商和设备类型	对于自定义设备，eSight 无法识别其厂商信息和设备类型，用户可以根据实际情况对其进行定制。	“系统 > 自定义设备管理”
自定义告警参数	对于非华为设备私有的 SNMP 告警，可以通过网管定制方式将其上报到网管上进行管理。	“系统 > 自定义设备管理”
自定义性能指标	本节以定制设备温度、接口错包率和 CPU 利用率为例，介绍自定制性能指标的过程。	“系统 > 自定义设备管理”
自定义设备配置文件	不同厂家的设备的备份、恢复和重启的命令各不相同，需要根据设备的实际情况，对其进行定制。	“系统 > 自定义设备管理”
自定义设备面板	对于自定义设备的面板图，可以通过实物拍照上传照片定制，也可以通过手绘图方式进行定制。	“系统 > 自定义设备管理”
执行 Ping 测试	在自定义设备的网元管理器中对其进行 ping 测试，检查网管与自定义设备之间的通信状态。	“资源 > 资源管理”
执行 Trace 测试	在自定义设备的网元管理器中对其进行 Trace 测试，检查网管与自定义设备之间的通信状态，并根据测试结果定位故障原因。	“资源 > 资源管理”
查询接口参数	网管支持对接口的索引、接口描述、接口 IP 地址、接口类型、接口状态、接口速率、接口别名等信息查询。	“资源 > 资源管理”
查询 IP 地址	在进行业务配置及网络规划时，需要查询网元及其接口的 IP 地址，eSight 支持对网元的 IP 地址以及接口的 IP 地址进行查询。	“资源 > 资源管理”
调用自定义设备的 Web 网管	eSight 提供调用自定义设备的 Web 网管功能，通过自定义设备的 web 网管对其进行相关业务配置。	“资源 > 资源管理”

12.2 自定义设备功能介绍

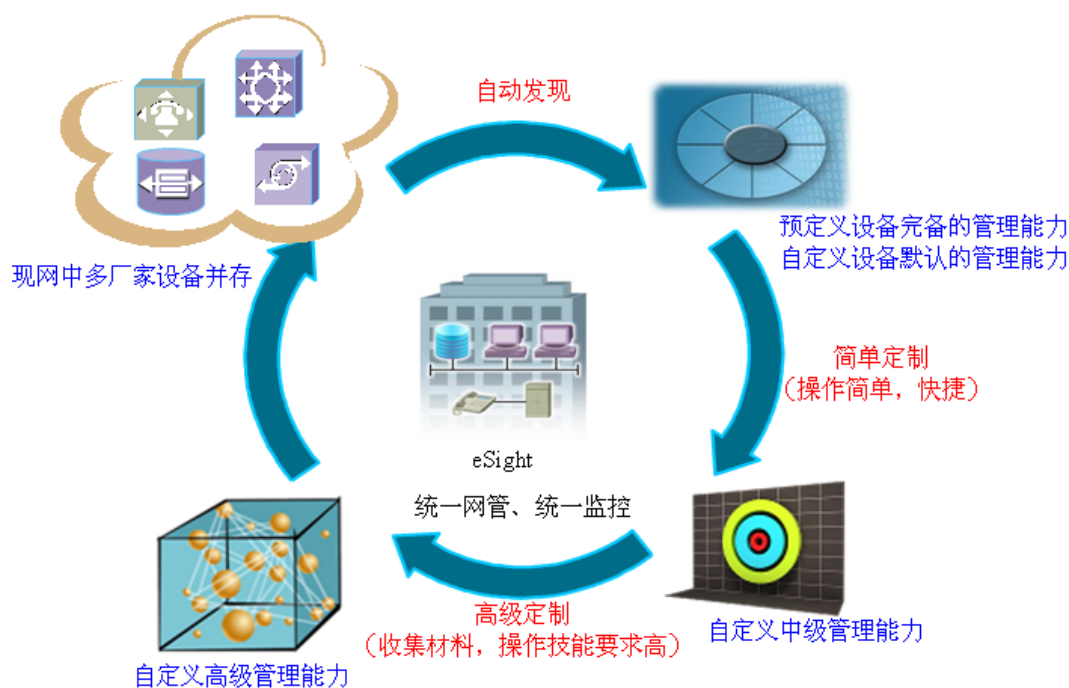
eSight 提供统一的管理平台，可以将现网所有支持 SNMP 协议的设备添加到网管，对于预集成设备，eSight 提供完善的管理能力，对于自定义设备（设备类型为 Huawei Device/H3C Device/Cisco Device/Unknow）提供定制功能，客户根据需要对其进行定制，从而实现 eSight 对现网多厂商设备的统一管理和统一监控。

自定义设备的应用场景

自定义设备的应用场景简要描述如下：

1. 客户统一将现网中的所有设备发现到 eSight 中。
2. 客户对 eSight 中的设备进行统一管理，对于自定义设备（设备类型为 Huawei Device/H3C Device/Cisco Device/Unknow）根据网管提供的默认功能，判断是否需要定制。
3. 通过简单的定制（厂商和设备类型定制），使 eSight 对自定义设备达到中级管理能力。
4. 通过收集相关材料，根据需要完成高级功能的定制，使 eSight 对自定义设备达到高级管理能力。

客户通过灵活定制，以满足对不同厂商不同管理能力需求，最终实现在 eSight 上对所有厂商设备的统一管理。



缺省与定制功能

设备	添加网元后网管默认提供功能项	定制后新增的功能项
Huawei Device/H3C Device/ Cisco Device	● 基本信息 ● 默认面板 ● SNMP 参数 ● 公有告警（故障菜单和网元管理器） ● IP 地址管理 ● 接口管理 ● Telnet 参数管理 ● 性能指标 ● 备份恢复配置文件	● 私有告警 ● 性能指标 ● 面板 ● 拓扑图标
Unknown	● 基本信息 ● 默认面板 ● SNMP 参数	● IP 地址管理 ● 接口管理 ● Telnet 参数管理 ● 告警 ● 性能指标 ● 拓扑图标 ● 备份恢复配置文件 定制后可以执行备份和恢复配置文件的操作，但需要重启网元才能生效。

根据场景对自定义设备进行定制

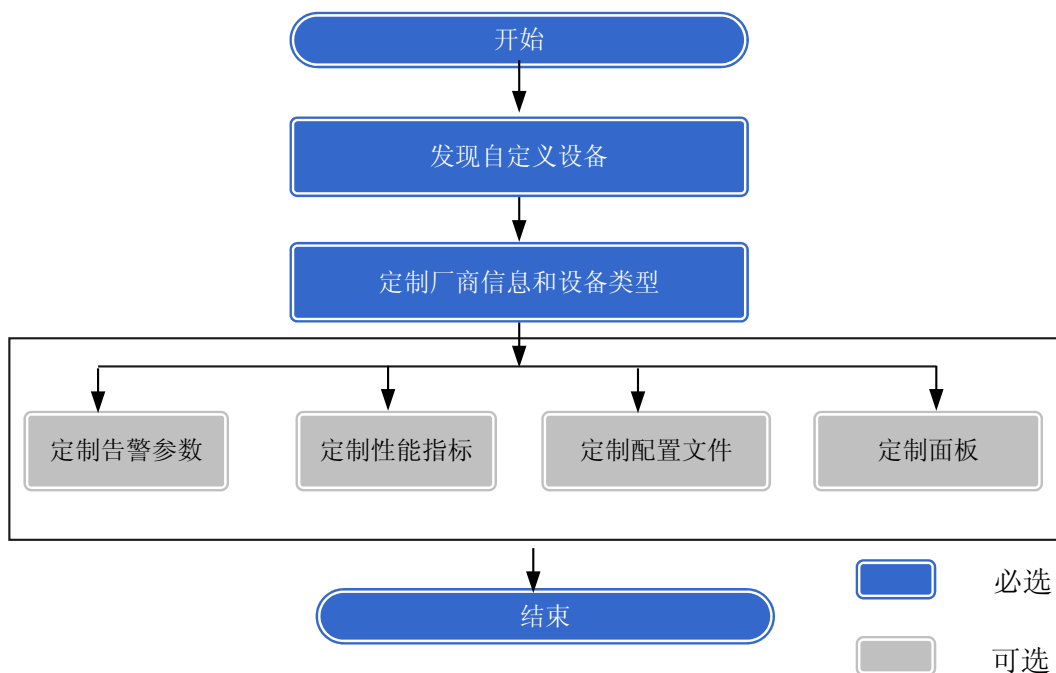
场景	定制项	定制准备材料	适用范围
中级管理能力			
IP 地址管理	定制厂商及设备类型。 定制工时：0.2 人/天 具体步骤，请参见 12.5 自定义厂商和设备类型 。	● 厂商名称（Unknown） ● 网元类型名称 ● 网元类别	Unknown
接口管理			Unknown
Telnet 参数管理			Unknown
拓扑图标			Huawei Device/H3C Device/Cisco Device/Unknown
高级管理能力			

场景	定制项	定制准备材料	适用范围
告警	定制告警，对其进行监控管理。 定制工时：1 时/条 具体步骤，请参见 12.6.1 自定义告警参数 。	● 要定制告警的 trapOID ● VB（mib 节点信息） 说明 以上材料需向厂家获取。	HuaweiDevice/H3C Device/Cisco Device/Unknown
性能指标	Huawei Device/H3C Device/Cisco Device 默认支持的性能指标同各自预定义设备一致。 Unknown 设备默认不支持性能指标，需要定制其性能指标。 定制工时：2 时/条 具体步骤，请参见 12.6.2 自定义性能指标 。	● 性能指标的 OID ● 计算公式 ● 测量对象索引 说明 以上材料需向厂家获取。	● Huawei Device/H3C Device/Cisco Device: 支持定制功能，若无特殊要求，不需要定制。 ● Unknown: 需定制。
配置文件	仅 Unknown 设备需要进行定制，定制后可以执行备份和恢复配置文件的操作，但是有些执行结果提示可能与实际不符。 定制工时：0.2 人/天 具体步骤，请参见 12.6.3 自定义设备配置文件 。	● 备份命令 ● 恢复命令 ● 重启命令 说明 以上材料需向厂家获取。	Unknown
定制面板	对于 Huawei、H3C、Cisco，支持面板展示，但是面板和实际情况可能不完全一致。 定制工时：1 人/天 具体步骤，请参见 12.6.4 自定义设备面板 。	● 真实外观 ● 各实体的层次关系 ● 各实体的 vendortype（实体的唯一标识） ● 起始索引	Huawei Device H3C Device Cisco Device

12.3 自定义设备配置流程

客户在判定需要对自定义设备进行定制时，可以按如下流程方式进行快速、有序、准确定制。

定制流程



12.4 发现自定义设备

eSight 支持通过三种方式将自定义设备添加到网管上，进行管理。

12.4.1 手工添加自定义设备

当需要添加到 eSight 的网元数量较少、网元所属类型较多时，可以通过手工创建单个网元的方式将网元添加到 eSight 中。

前提条件

已具备“资源接入”的操作权限。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”。
- 步骤 2** 在“资源管理”窗口的导航树中，选择新增网元的父对象，在右侧页面单击“单个创建”。
- 步骤 3** 在“选择类型”页面的“物理设备类”中，选择待创建网元的类型。

步骤 4 在“配置参数”页面中，设置待创建网元的基本信息和 SNMP 协议参数。



说明

对于需要配置 SNMP 协议参数的网元，可配置完 SNMP 协议参数后单击“保存协议模板”，作为 SNMP 协议参数的配置模板。当再次需要配置 SNMP 协议参数时可直接单击“选择协议模板”，应用已保存的协议模板。

步骤 5 单击“确定”。



说明

单击“应用”，可继续创建网元。

- 如果网元创建成功，在管理对象列表中可查看到新增网元。
- 如果网元创建失败，则会弹出“错误”提示框，说明网元添加失败的原因。单击“确定”，重新配置参数。

---结束

后续处理

通过手工单个创建网元功能增加网元到 eSight 后，在“资源管理”窗口中可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 1. 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 1. 在“搜索类型”下拉框中选择搜索类型。 2. 在“搜索条件”文本框中输入搜索条件。 2. 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的 2. 在修改网元信息页面修改网元的名称。 3. 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 1. 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的 ● 批量删除：选择需要删除的网元，单击“批量删除”。 2. 在“确认”对话框中，单击“是”。

维护网元	操作方法
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理窗口。 1. 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的 . 2. 在弹出的网元管理器窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监报告警和 6.4.3 查看网元性能概况。

12.4.2 自动发现自定义设备

通过网元自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。当指定网段中的所有网元都需要增加到 eSight 时，该功能可以实现批量操作，节省时间。

前提条件

- 已具备“资源接入”的操作权限。
- 网元支持 eSight 指定的 SNMP 协议。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口右侧页面中，单击“自动发现”。

步骤 3 在自动发现页面中，单击“网段发现”。

步骤 4 在“网段发现”页面中，设置网段发现参数和 SNMP 协议参数。

为了操作快捷，可以通过单击“选择协议模板”使用已保存的 SNMP 协议模板来设置 SNMP 协议参数。详情请参见[手工创建单个网元](#)页面中的[保存协议模板](#)。

步骤 5 可选：选中“发现的对象自动添加到本网管系统中”。

 说明

- 如果选择了“发现的对象自动添加到本网管系统中”，发现的网元将自动进行添加操作，不需要执行[步骤 7](#)。
- 如果不选择“发现的对象自动添加到本网管系统中”，需要您执行[步骤 7](#)，增加发现的网元。

步骤 6 单击“开始发现”。

发现结果列表中显示自动发现的网元信息以及增加结果。

 说明

发现过程中，可单击“停止发现”，暂停发现操作。

步骤 7 在列表中选择网元，单击“创建”。

如果选择了“发现的对象自动添加到本网管系统中”，此步骤省略。

- 如果网元添加成功，“添加结果”列显示“添加成功”。
- 如果网元添加失败，“添加结果”列显示失败原因。

步骤 8 单击“完成”。

返回“资源管理”窗口，右侧管理对象列表中可查看到添加的网元信息。

----结束

后续处理

通过自动发现网元功能增加网元到 eSight 后，在“资源管理”窗口中可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 - 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 - 在“搜索类型”下拉框中选择搜索类型。 - 在“搜索条件”文本框中输入搜索条件。 - 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在修改网元信息页面修改网元的名称。 - 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 - 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的. ● 批量删除：选择需要删除的网元，单击“批量删除”。 - 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理窗口。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在弹出的网元管理器窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

12.4.3 批量导入自定义设备

当开局或设备扩容时，被管设备较多，以创建单个网元方式增加网元比较繁琐，可以选择手工批量导入网元方式批量增加网元。

前提条件

已具备“资源接入”的操作权限。

背景信息

手工批量导入网元是通过导入 Excel 模板资源文件增加网元。

表 12-2 对 Excel 模板中的各个字段进行了说明。

表 12-2 Excel 模板信息

字段名称	设置说明
IP	例如 10.123.124.115。
名称（可选）	1 - 128 位字符，不能包含#%&+/,<=>? \特殊字符。
协议类型	设置为“SNMP”。
协议版本	需与设备的 SNMP 协议版本一致。取值为“V1”或“V2c”。
端口	需与设备的 SNMP 协议的端口号一致，如“161”。
读团体字	需与设备的 SNMP 协议的读团体字一致，如“public”。
写团体字	需与设备的 SNMP 协议的写团体字一致，如“private”。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在“资源管理”窗口右侧页面中，单击“批量导入”。

步骤 3 在“选择批量导入类型”页面中，选择“导入主机及网络类设备”。

步骤 4 在“导入主机及网络类设备”中，单击“模板下载”后的  模板.xls，下载 Excel 模板到本地。

步骤 5 打开模板，填入网元信息，保存文件。

步骤 6 在批量导入页面单击“待导入的模版资源文件”后的 ，选择所保存的 Excel 文件。

如果需要导入其他文件，可以单击  清除已选择的文件。

步骤 7 单击 ，上传文件。

“待导入的资源列表”中显示文件中各网元的信息以及校验结果。“结果”列为空白，表示网元校验通过。

步骤 8 在待导入资源列表中选择网元，单击“创建”，

eSight 开始导入网元。

- 如果网元创建成功，“结果”列显示“创建成功”。
- 如果网元创建失败，“结果”列显示失败原因。请根据失败原因提示解决问题，尝试重新导入。如果不能解决，请联系技术支持人员。

----结束

后续处理

通过手工批量导入网元功能增加网元到 eSight 后，在“资源管理”窗口可以执行如下操作。

维护网元	操作方法
查看网元信息	在 eSight 中可以方便的查看网元信息，包括网元的基本信息和协议信息等。 - 在“资源管理”窗口右侧的管理对象页面中，设置搜索条件，单击“搜索”。 - 在“搜索类型”下拉框中选择搜索类型。 - 在“搜索条件”文本框中输入搜索条件。 - 单击目标网元的网元名称，eSight 显示此网元的所有信息。
修改网元信息	在 eSight 中可以方便的修改网元的属性，例如网元名称等。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在修改网元信息页面修改网元的名称。 - 单击“确定”。
删除网元	当网络结构调整，不再需要 eSight 管理某些网元，可以删除。 - 在“资源管理”窗口右侧的管理对象列表中，删除网元。 ● 单个删除：单击目标网元所在“操作”列中的. ● 批量删除：选择需要删除的网元，单击“批量删除”。 - 在“确认”对话框中，单击“是”。
管理网元	在 eSight 中可以在资源管理窗口进入到网元管理页面。 - 在“资源管理”窗口右侧的管理对象列表中，单击目标网元所在“操作”列中的. - 在弹出的网元管理窗口可以对网元进行相应的管理操作。详情请参见 5.4.4 通过网元管理器监控告警和 6.4.3 查看网元性能概况。

12.5 自定义厂商和设备类型

对于自定义设备，eSight 无法识别其厂商信息和设备类型，用户可以根据实际情况对其进行定制。

操作步骤

- 步骤 1 进入“厂商基本信息定制”界面。
1. 在主菜单中选择“资源 > 资源管理”，查看网元列表。

2. 在网元列表中单击网元操作列的“管理”，进入网元管理器。

3. 在“基本信息”页签下，在“产品型号”后单击“定制设备类型”，进入厂商基本信息定制界面。

步骤 2 单击“创建”，在弹出的窗口中定制厂商信息。

步骤 3 单击“确定”，返回“厂商基本信息定制”界面。

步骤 4 默认选择刚创建的厂商名称“ZZZ”，单击“下一步”。

步骤 5 设置“设备类型”、“设备类别”和“当前设备图标”，单击“完成”。

步骤 6 弹出对话框提示操作成功，单击“确认”，即完成配置。

----结束

后续处理

1. 在主菜单中选择“资源 > 资源管理”，查看网元列表。
2. 在网元列表中单击自定义设备对应的网元名称，进入该网元基本配置信息界面。
3. 单击“管理”，进入网元管理器查看该设备的设备类型已定制成功。

12.6 设备管理能力定制

12.6.1 自定义告警参数

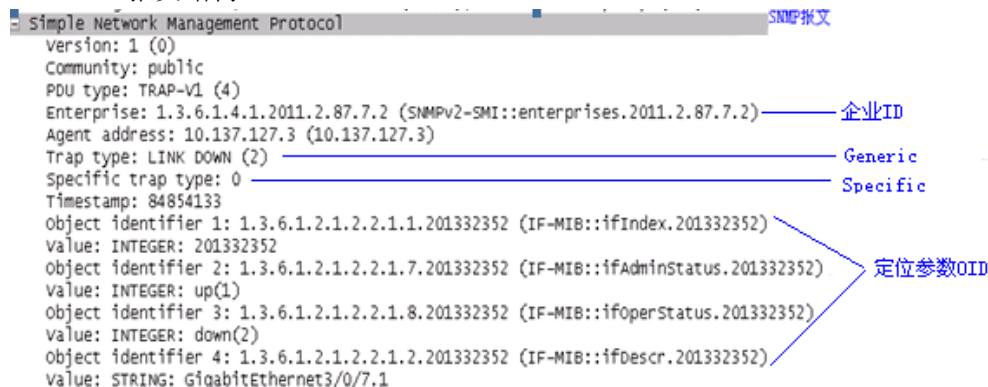
对于非华为设备私有的 SNMP 告警，可以通过网管定制方式将其上报到网管上进行管理。

背景信息

定制告警的 Trap ID 以及定位告警参数的 MIB 节点信息，需要向厂家获取。

可通过工具（如：Mib Browser）获取告警 Trap 报文，根据报文结构，获取告警定制相关参数。

SNMPV1 报文结构：



Simple Network Management Protocol

Version: 1 (0)
Community: public
PDU type: TRAP-V1 (4)
Enterprise: 1.3.6.1.4.1.2011.2.87.7.2 (SNMPv2-SMI::enterprises.2011.2.87.7.2) ———— 企业ID
Agent address: 10.137.127.3 (10.137.127.3)
Trap type: LINK DOWN (2) ———— Generic
Specific trap type: 0 ———— Specific
Timestamp: 84854133
Object identifier 1: 1.3.6.1.2.1.2.2.1.1.201332352 (IF-MIB::ifIndex.201332352)
Value: INTEGER: 201332352
Object identifier 2: 1.3.6.1.2.1.2.2.1.7.201332352 (IF-MIB::ifAdminStatus.201332352)
Value: INTEGER: up(1)
Object identifier 3: 1.3.6.1.2.1.2.2.1.8.201332352 (IF-MIB::ifOperStatus.201332352)
Value: INTEGER: down(2)
Object identifier 4: 1.3.6.1.2.1.2.2.1.2.201332352 (IF-MIB::ifDescr.201332352)
Value: STRING: GigabitEthernet3/0/7.1

定位参数OID

SNMPV2 报文结构：

Simple Network Management ProtocolSNMP报文

```
Version: 2C (1)
Community: public
PDU type: TRAP-v2 (7)
Request id: 0x69aadf54
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
Value: Timeticks: (20118615) 2 days, 7:53:06.15
Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)
Value: OID: IF-MIB::linkDown告警OID
Object identifier 3: 1.3.6.1.2.1.2.2.1.1.84609 (IF-MIB::ifIndex.84609)
Value: INTEGER: 84609
Object identifier 4: 1.3.6.1.2.1.2.2.1.7.84609 (IF-MIB::ifAdminStatus.84609)
Value: INTEGER: down(2)
Object identifier 5: 1.3.6.1.2.1.2.2.1.8.84609 (IF-MIB::ifOperStatus.84609)
Value: INTEGER: down(2)
Object identifier 6: 1.3.6.1.2.1.2.2.1.2.84609 (IF-MIB::ifDescr.84609)
Value: STRING: GigabitEthernet2/0/1
Object identifier 7: 1.3.6.1.2.1.2.2.1.8.84609 (IF-MIB::ifOperStatus.84609)
Value: INTEGER: down(2)
```

定位参数OID

操作步骤

- 步骤 1 在主菜单中选择“系统 > 自定义设备管理”。
- 步骤 2 在左侧的导航树中选择“设备管理能力定制 > 告警参数定制”。
- 步骤 3 定制告警。

1. 在“告警参数定制”界面，单击“创建”，进入“创建告警参数”页签。

2. 在“创建告警参数”页签下配置自定义告警的相关参数，单击“确定”。

参数名称		说明
SNMP 版本		当前支持 SNMPv1、SNMPv2c、SNMPv3 三个版本 ● 对于 SNMP v2c/v3 设备，需要配置告警 OID。 ● 对于 SNMP v1 设备，需要配置“Generic”、“Specific”和“企业 ID”。
Generic		“Generic” + “Specific” + “企业 ID” 组合值，唯一标识一条 SNMP V1 告警。
Specific		
企业 ID		
告警 OID		即 SNMP V2c 版本的 Trap OID，用于唯一标识该告警。
新增参数项目	定位参数名称	告警的定位信息参数项的名称。 如接口索引，用于定位具体某端口上报告警。
	定位参数 OID	告警的定位信息参数项的取值 MIB 节点。

步骤 4 定制恢复告警。

1. 在“告警参数定制”界面，单击“创建”，进入“创建告警参数”页签。
2. 在“创建告警参数”页签下配置“厂商名称”为对应告警的厂商；“通知类型”为“恢复告警”。
3. 单击“选择”，选择相应的告警，单击“确定”。
4. 设置“告警 OID”，单击“确定”。

---结束

后续处理

告警定制成功后，当设备出现该定制告警对应的故障时，可在“故障 > 当前告警”界面下查看对应的告警信息。

12.6.2 自定义性能指标

本节以定制设备温度、接口错包率和 CPU 利用率为例，介绍自定制性能指标的过程。

背景信息

- 用户自定义设备指标组：针对设备级，设备仅有这一个指标，监视对象为设备，例如：设备的温度。
- 用户自定义接口指标组：监视对象为接口，例如接口流量。
- 未指定对象指标组：不同厂家的设备上自有的私有指标，该性能指标定制以后，由用户自己指定监视对象。

说明

定制性能的指标 MIB 节点信息，需要向厂家获取。

- 指标公式说明：指标公式是用户要监视的 MIB 节点及其运算的一个表达式。
- 表达式支持：MIB OID、“\$”、“+”、“-”、“*”、“/”、“=”、“period”（小写）、“()”、“(”、“)”字符。当选择“用户自定义设备指标组”进行指标定制时，MIB OID 后需要加上“.0”。其中：“\$”是索引节点(MIB OID)的前后缀字符，所有的索引节点都需要用这个字符括起来，“()”紧随 OID 后，表示索引节点上一次轮询的值，主要用于差值计算，“period”表示轮询周期，“=”用于判断使用。

操作步骤

步骤 1 在主菜单中选择“系统 > 自定义设备管理”。

步骤 2 在左侧的导航树选择“设备管理能力定制 > 性能指标定制”。

步骤 3 分别创建自定义设备、自定义接口和未指定对象指标。

1. 创建自定义设备指标。单击“创建”，在“创建性能指标”页签下配置设备性能指标参数，单击“确定”。

说明

对于设备性能指标，设置“指标公式”为性能指标的 MIB ID+.0。

2. 创建自定义接口指标。单击“创建”，在“创建性能指标”页签下配置接口性能指标参数，单击“确定”。
3. 创建未指定对象指标。单击“创建”，在“创建性能指标”页签下配置未指定对象性能指标参数，单击“确定”。

步骤 4 创建性能监控实例。

1. 在主菜单中选择“性能 > 性能监视设置”，单击“创建”。
2. 单击“选择管理对象”，弹出“选择管理对象”窗口。在左侧拓扑树中选择一个子网，右侧管理对象列表中选择自定义的设备。
3. 单击“选择指标”，选择定制的设备性能指标，单击“确定”。
4. 分别单击“未指定对象指标组”和“用户自定义接口指标组”后的，设置测量对象，单击“确定”。

说明

对于未指定对象指标组，需要手工设置具体的监视对象。

5. 单击“确定”，在“操作结果列表”提示操作成功，单击“完成”。

----结束

后续处理

在主菜单中选择“性能 > 性能监视设置”，单击网元列表中的网元名称，打开网元管理器，再单击“性能状态”，即可查看自定义的性能状态。

12.6.3 自定义设备配置文件

不同厂家的设备的备份、恢复和重启的命令各不相同，需要根据设备的实际情况，对其进行定制。

操作步骤

步骤 1 在主菜单中选择“系统 > 自定义设备管理”。

步骤 2 在左侧的导航树选择“设备管理能力定制 > 配置文件定制”。

步骤 3 单击“创建”，在“设备类型”后单击“选择”，选择需定制配置文件的设备。

步骤 4 分别配置“备份命令”、“恢复命令”和“重启命令”，单击“确定”。

步骤 5 创建配置文件的备份任务。

1. 在主菜单中选择“操作维护 > 配置文件管理”。
2. 在主菜单中选择“设备配置管理 > 备份任务”。
3. 单击“创建”，配置备份任务的相关参数。
4. 在“应用到设备”后单击“增加”，选择自定义设备，单击“确定”，将备份任务应用到这些设备上。

说明

- 配置非华为设备备份恢复功能需要设置 telnet 参数。
- 当前网管可以直接定制的厂商设备为华为、CISCO 和 H3C。对于其他厂商的设备，可能会出现备份恢复任务执行失败的现象。

----结束

12.6.4 自定义设备面板

对于自定义设备的面板图，可以通过实物拍照上传照片定制，也可以通过手绘图方式进行定制。

背景信息

- 通过网元管理器中进行定制面板，不需要收集实体的 vendortype（实体唯一标识）和实体的起始索引，网管会自动适配。
- Unknown 设备网管提供默认的面板，不支持定制。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击管理进入网元管理器。

步骤 2 在左侧导航树选择“查看 > 设备面板”，在右侧窗口中显示的是网管默认为非华为设备提供的面板图。

步骤 3 定制机框。

1. 右键单击机框，选择“创建新样式”。
2. 设置机框大小。在窗口的菜单栏中选择槽位图标，将其拖入编辑器，根据机框图片大小设置槽位的大小。
3. 选择机框图标，将其拖入步骤步骤 3.2 创建的槽位中。
4. （可选）单击上传本地机框图片，在“扩展属性”下选择上传的机框图片。
5. 根据设备的实际情况，设置机框上的槽位，一块单板对应一个槽位。将菜单栏中槽位图标拖入机框，设置槽位的大小和“索引标识”。
6. 单击保存模板设置机框模板的名称，单击“保存”。
7. 在右上角单击“完成”。

步骤 4 定制单板。

1. 在网元管理器下的设备面板页签下，右键单击单板，选择“创建新样式”。
2. 设置单板大小。在菜单栏中选择槽位图标，将其拖入编辑器，根据单板图片大小设置槽位的大小。
3. 选择单板图标，将单板拖入步骤步骤 4.2 创建的槽位中。
4. （可选）单击上传本地单板图片，在“扩展属性”下选择刚上传的图片，设置端口的个数。

若需要端口和设备的端口排列完全一致，槽位图标拖入单板中，设置槽位的大小和“索引标识”，将槽位按照单板上端口的实际排列情况进行布局。

5. 单击保存模板设置单板模板的名称，单击“保存”。
6. 在右上角单击“完成”。

步骤 5 定制端口模板。

1. 在网元管理器下的设备面板页签下，右键单击端口，选择“创建新样式”。

 说明

鼠标放在端口上，tip 会显示“端口型号”，不同端口型号需要创建不同的端口模板。

2. 设置端口大小。在菜单栏中选择槽位，将其拖入编辑器，根据端口图片大小设置槽位的大小。
3. 选择端口图标，将端口拖入步骤步骤 5.2 创建的槽位中。

4. （可选）单击  上传本地端口图片，在“扩展属性”下选择刚上传的图片。
5. 单击  保存模板设置端口模板的名称，单击“保存”。
6. 在右上角单击“完成”。

----结束

后续处理

验证定制的设备面板，在左侧导航树选择“查看 > 设备面板”，查看自定义的设备面板。

12.7 检测自定义设备网络状态

定期检测自定义设备的网络状态，实时了解网管和自定义设备之间的通信状态。

12.7.1 执行 Ping 测试

在自定义设备的网元管理器中对其进行 ping 测试，检查网管与自定义设备之间的通信状态。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧的窗口中单击“查看 > 基本信息”，在右侧的窗口中单击“Ping”。
- 步骤 3** 在弹出的“Ping”窗口中，设置 Ping 测试参数，单击“Ping”。
- 步骤 4** 在“Ping”窗口中查看 Ping 测试结果，单击“关闭”。

----结束

12.7.2 执行 Trace 测试

在自定义设备的网元管理器中对其进行 Trace 测试，检查网管与自定义设备之间的通信状态，并根据测试结果定位故障原因。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧的窗口中单击“查看 > 基本信息”，在右侧的窗口中单击“Trace”。
- 步骤 3** 在弹出的“Trace”窗口中，查看 Trace 测试的结果。
- 步骤 4** 单击“关闭”。

----结束

12.7.3 查询接口基本信息

网管支持接口信息查询。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧导航树单击“设备配置 > 接口管理”。
- 步骤 3** 在窗口上方设置过滤参数，单击“搜索”。
- 步骤 4** 在下方的窗格中查看接口相关参数。

----结束

12.7.4 查看 IP 地址表

在进行业务配置及网络规划时，需要查询网元及其接口的 IP 地址，eSight 支持对网元的 IP 地址以及接口的 IP 地址进行查询。

操作步骤

- 步骤 1** 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。
- 步骤 2** 在左侧导航树单击“设备配置 > IP 地址管理”。
- 步骤 3** 单击“同步”，待同步结束，在“同步进度”窗口中查看详细信息，单击“确定”，将设备上的 IP 地址参数同步到网管上。
- 步骤 4** 在窗口上方设置过滤参数，单击“搜索”。在下方的窗格中查看 IP 地址的相关参数。

----结束

12.8 调用自定义设备的 Web 网管

eSight 提供调用自定义设备的 Web 网管功能，通过自定义设备的 web 网管对其进行相关业务配置。

前提条件

已定制设备类型。

自定义设备支持 web 网管，且已在定制设备类型时配置其 web 网管。

背景信息

 说明

对于华为框式交换机和路由器设备，不支持设备 Web 网管，支持使用智能工具进行相关业务配置。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”，在网元列表中单击相应网元的“名称”，单击“管理”进入网元管理器。

步骤 2 在左侧的窗口中单击“配置 > Web 网管”。

----结束

13 系统管理

关于本章

13.1 系统操作全景图

通过系统操作全景图可以了解系统管理的所有操作，并根据实际情况，选择操作方式。

13.2 设置 eSight 数据溢出转储

为了避免数据库表空间不足而影响业务运行，eSight 提供了数据溢出转储功能。数据溢出转储包括日志溢出转储、告警溢出转储、性能溢出转储和 SLA 溢出转储。请在安装 eSight 之后根据实际情况进行设置。

13.3 查询日志

日志记录网管操作的信息以及 eSight 中发生的重要事件。通过查询日志信息可以了解 eSight 的运行情况和网管的具体操作情况。

13.4 下级网管

eSight 可以管理下级网管，通过分级管理，建立其区域化、层次化的管理体制，并且分散了大规模网络的管理压力，突破了单网管站点的资源管理能力和性能压力。

13.5 管理 License

需获取 License 后才能使用 eSight 的各项功能。License 用于对 eSight 资源和功能进行控制。

13.6 备份/恢复数据库

为了保障网管数据库的安全，需及时对网管数据库进行备份/恢复操作。

13.7 网元包组件管理

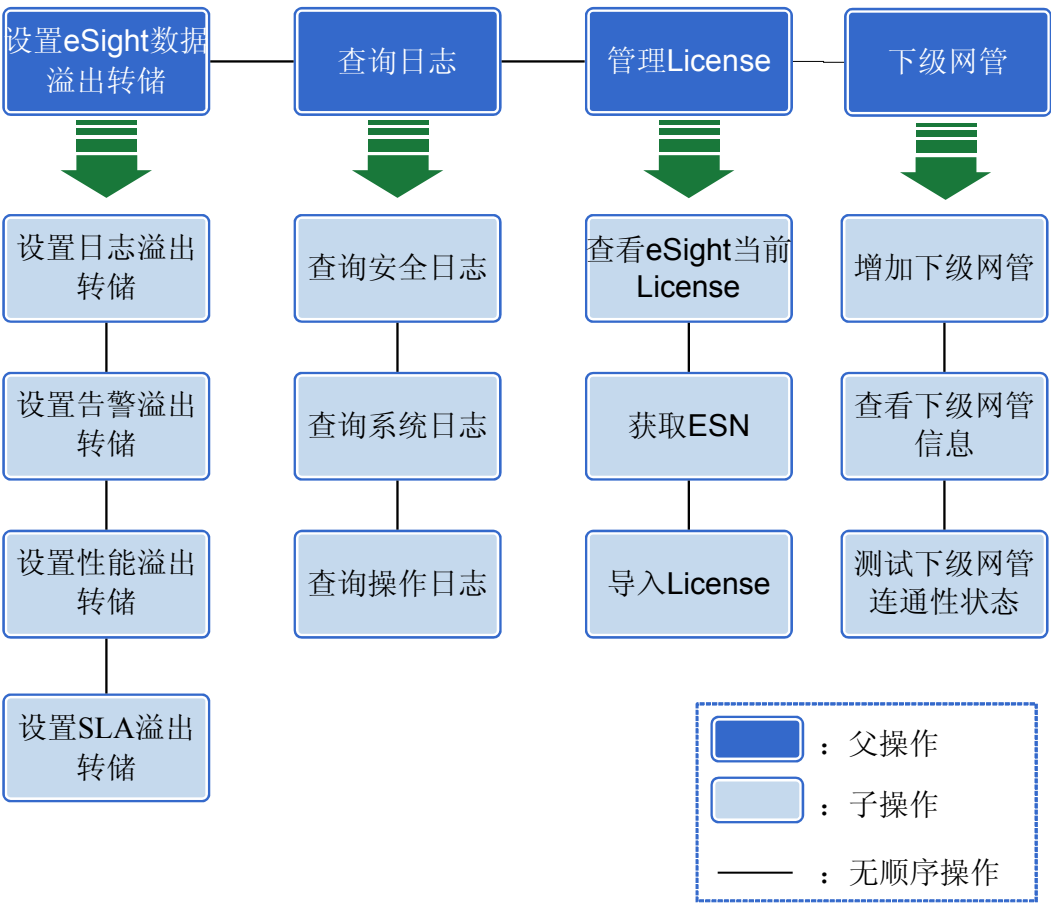
通过网元包组件管理可以查看网元包版本、厂商、网元类型、网元包特性等信息，完成网元包的安装和升级操作。

13.1 系统操作全景图

通过系统操作全景图可以了解系统管理的所有操作，并根据实际情况，选择操作方式。

系统操作全景图，如图 13-1 所示。若需要了解更多操作详情，可以单击全景图中的内容进入相关页面。

图 13-1 系统操作全景图



系统操作的简要说明如表 13-1 所示。

表 13-1 操作简要说明

操作	说明	操作入口
13.2.1 设置日志数据库溢出转储	为了避免数据库安全管理表空间不足，eSight 提供了日志溢出转储功能。eSight 可以按照配置条件每日检测日志数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。	“系统 > 系统配置 > 数据库溢出转储 > 日志数据库溢出转储”
13.2.2 设置告警数据库溢出转储	为了避免告警管理表空间不足，eSight 提供了告警溢出转储功能。eSight 可以按照配置条件每日检测告警数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。	“系统 > 系统配置 > 数据库溢出转储 > 告警数据库溢出转储”
13.2.3 设置性能数据库溢出转储	为了避免数据库性能管理表空间不足，eSight 提供了性能溢出转储功能。eSight 可以按照配置条件每日检测审计性能数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定路径下进行保存。	“系统 > 系统配置 > 数据库溢出转储 > 性能数据库溢出转储”
13.2.4 设置 SLA 数据库溢出转储	为了避免 SLA 管理表空间不足，eSight 提供了 SLA 数据库溢出转储功能。eSight 可以按照配置条件每日检测 SLA 数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。	“系统 > 系统配置 > 数据库溢出转储 > SLA 数据库溢出转储”
13.3.2 查询安全日志	可以通过查询安全日志了解涉及 eSight 安全操作的相关信息。	“系统 > 日志管理 > 日志查询 > 安全日志”
13.3.3 查询系统日志	可以通过查询系统日志了解涉及 eSight 系统操作的相关信息。	“系统 > 日志管理 > 日志查询 > 系统日志”
13.3.4 查询操作日志	可以通过查询操作日志了解涉及用户执行操作的相关信息。	“系统 > 日志管理 > 日志查询 > 操作日志”
13.5.1 查看 eSight 当前 License	eSight 支持查看当前使用的 License 的所有信息。	“系统 > License 管理”

操作	说明	操作入口
13.5.2 获取 ESN	当 License 即将过期时，需要获取本机的 ESN 号，用于申请 License。	“系统 > License 管理”
13.5.3 导入 License	当 eSight 当前 License 即将过期时，需要及时导入新的 License。	“系统 > License 管理”
13.4.2.1 增加下级网管	可以通过增加下级网管操作，实现上级网管管理下级网管。	“系统 > 下级网管”
13.4.2.2 查看下级网管信息	定期查看下级网管的状态，及时对其状态进行跟踪管理。	“系统 > 下级网管”
13.4.2.3 测试下级网管连通性状态	定期测试下级网管的连通性状态，便于对下级网管的连通性状态进行跟踪。	“系统 > 下级网管”

13.2 设置 eSight 数据溢出转储

为了避免数据库表空间不足而影响业务运行，eSight 提供了数据溢出转储功能。数据溢出转储包括日志溢出转储、告警溢出转储、性能溢出转储和 SLA 溢出转储。请在安装 eSight 之后根据实际情况进行设置。

13.2.1 设置日志数据库溢出转储

为了避免数据库安全管理表空间不足，eSight 提供了日志溢出转储功能。eSight 可以按照配置条件每日检测日志数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。

前提条件

已具备“系统配置”的操作权限。

背景信息

当数据库安全管理表空间使用率超出设置的数据库空间阈值时，数据溢出。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 系统配置”。
- 步骤 2** 在“系统配置”窗口的导航区中，选择“数据库溢出转储 > 日志数据库溢出转储”。
- 步骤 3** 在“日志数据库溢出转储”页面中，设置日志转储参数。

数据库中日志管理表空间最大值根据 eSight 版本及数据库类型不同有所区别，具体参见 [表 13-2](#)。

表 13-2 日志管理表空间最大值列表

版本	MySQL 数据库	SQL Server 数据库	Oracle 数据库
体验版	2G	-	-
精简版	2G	-	-
标准版	2G	1G	-
专业版（Windows）	2G	1G	-
专业版（SUSE Linux）	-	-	2G

 说明

“数据库空间阈值（%）”表示日志管理表空间最大值的百分比。

“保存文件路径”支持输入相对路径和绝对路径。当输入相对路径时，则该相对路径是相对 eSight 安装路径 “%eSight_ROOT/var/runtime.center/data/dump”（以 Linux 操作系统为例）而言。例如输入 AAA，则表示文件将保存到 “%eSight_ROOT/var/runtime.center/data/dump/AAA” 下。

步骤 4 单击“应用”。

----结束

13.2.2 设置告警数据库溢出转储

为了避免告警管理表空间不足，eSight 提供了告警溢出转储功能。eSight 可以按照配置条件每日检测告警数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。

前提条件

已具备“系统配置”的操作权限。

背景信息

当告警管理表空间使用率超出设置的数据库空间阈值时，数据溢出。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 系统配置”。
- 步骤 2** 在“系统配置”窗口的导航区中，选择“数据库溢出转储 > 告警数据库溢出转储”。
- 步骤 3** 在“告警数据库溢出转储”页面中，设置告警转储参数。
- 数据库中告警管理表空间最大值根据 eSight 版本及数据库类型不同有所区别，具体参见 [表 13-3](#)。

表 13-3 告警管理表空间最大值列表

版本	MySQL 数据库	SQL Server 数据库	Oracle 数据库
体验版	8G	-	-
精简版	8G	-	-
标准版	8G	2G	-
专业版（Windows）	8G	2G	-
专业版（SUSE Linux）	-	-	4G

 说明

“数据库空间阈值（%）”表示告警管理表空间最大值的百分比。

“保存文件路径”支持输入相对路径和绝对路径。当输入相对路径时，则该相对路径是相对 eSight 安装路径 “%eSight_ROOT/var/runtime.center/data/dump”（以 Linux 操作系统为例）而言。例如输入 AAA，则表示文件将保存到 “%eSight_ROOT/var/runtime.center/data/dump/AAA” 下。

步骤 4 单击“应用”。

----结束

13.2.3 设置性能数据库溢出转储

为了避免数据库性能管理表空间不足，eSight 提供了性能溢出转储功能。eSight 可以按照配置条件每日检测审计性能数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定路径下进行保存。

前提条件

已具备“系统配置”的操作权限。

背景信息

当性能管理表空间使用率超出设置的数据库空间阈值时，数据溢出。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 系统配置”。
- 步骤 2** 在“系统配置”窗口的导航区中，选择“数据库溢出转储 > 性能数据库溢出转储”。
- 步骤 3** 在“性能数据库溢出转储”页面中，设置性能转储参数。
- 数据库中性能管理表空间最大值根据 eSight 版本及数据库类型不同有所区别，具体参见 [表 13-4](#)。

表 13-4 性能管理表空间最大值列表

版本	MySQL 数据库	SQL Server 数据库	Oracle 数据库
体验版	8G	-	-
精简版	8G	-	-
标准版	8G	4G	-
专业版（Windows）	8G	8G	-
专业版（SUSE Linux）	-	-	30G

 **说明**

“数据库空间阈值（%）”表示性能管理表空间最大值的百分比。

“保存文件路径”支持输入相对路径和绝对路径。当输入相对路径时，则该相对路径是相对 eSight 安装路径 “%eSight_ROOT/var/runtime.center/data/dump”（以 Linux 操作系统为例）而言。例如输入 AAA，则表示文件将保存到 “%eSight_ROOT/var/runtime.center/data/dump/AAA” 下。

步骤 4 单击“应用”。

----结束

13.2.4 设置 SLA 数据库溢出转储

为了避免 SLA 管理表空间不足，eSight 提供了 SLA 数据库溢出转储功能。eSight 可以按照配置条件每日检测 SLA 数据是否溢出，如果溢出，则 eSight 自动将最早的数据转储到指定的路径下进行保存。

前提条件

已具备“系统配置”的操作权限。

背景信息

当数据库 SLA 管理表空间使用率超出设置的数据库空间阈值时，数据溢出。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 系统配置”。
- 步骤 2** 在“系统配置”窗口的导航区中，选择“数据库溢出转储 > SLA 数据库溢出转储”。
- 步骤 3** 在“SLA 数据库溢出转储”页面中，设置 SLA 转储参数。
- 数据库中 SLA 管理表空间最大值根据 eSight 版本及数据库类型不同有所区别，具体参见[表 13-5](#)。

表 13-5 SLA 管理表空间最大值列表

版本	MySQL 数据库	SQL Server 数据库	Oracle 数据库
体验版	-	-	-
精简版	-	-	-
标准版	20G	20G	-
专业版（Windows）	20G	20G	-
专业版（SUSE Linux）	-	-	20G

 说明

“数据库空间阈值（%）”表示 SLA 管理表空间最大值的百分比。

“保存文件路径”支持输入相对路径和绝对路径。当输入相对路径时，则该相对路径是相对 eSight 安装路径 “%eSight_ROOT/var/runtime.center/data/dump”（以 Linux 操作系统为例）而言。例如输入 AAA，则表示文件将保存到 “%eSight_ROOT/var/runtime.center/data/dump/AAA” 下。

步骤 4 单击“应用”。

----结束

13.3 查询日志

日志记录网管操作的信息以及 eSight 中发生的重要事件。通过查询日志信息可以了解 eSight 的运行情况和网管的具体操作情况。

13.3.1 日志类型

eSight 的日志包括安全日志、系统日志和操作日志。

安全日志

安全日志记录涉及 eSight 安全操作的信息，如登录服务器、修改密码、创建用户和退出服务器等。

系统日志

系统日志记录 eSight 发生的事件，如 eSight 运行异常、网络故障、eSight 受到攻击等，有利于分析 eSight 运行状态，排除故障。

操作日志

操作日志记录用户在 eSight 上的操作的信息，如新增监视图、修改资源管理等。

13.3.2 查询安全日志

可以通过查询安全日志了解涉及 eSight 安全操作的相关信息。

前提条件

已具备“日志管理”的操作权限。

背景信息

- 如果没有设置任何查询条件，则表示查询所有的安全日志。
- 查询结果基于数据库中的现有数据。如果数据未产生，则无数据显示。

操作步骤

步骤 1 在主菜单中选择“系统 > 日志管理”。

步骤 2 在“日志管理”窗口的导航区中，选择“日志查询 > 安全日志”。

步骤 3 直接查看日志信息，或设置搜索条件后查看指定的日志信息。

单击目标日志所在“详细信息”列中的值，在“安全日志详情”对话框中，可以查看详细的日志信息。

----结束

13.3.3 查询系统日志

可以通过查询系统日志了解涉及 eSight 系统操作的相关信息。

前提条件

已具备“日志管理”的操作权限。

背景信息

- 如果没有设置任何查询条件，则表示查询所有的系统日志。
- 查询结果基于数据库中的现有数据。如果数据未产生，则无数据显示。

操作步骤

步骤 1 在主菜单中选择“系统 > 日志管理”。

步骤 2 在“日志管理”窗口的导航区中，选择“日志查询 > 系统日志”。

步骤 3 直接查看日志信息，或设置搜索条件后查看指定的日志信息。

单击目标日志所在“详细信息”列中的值，在“系统日志详情”对话框中，可以查看详细的日志信息。

----结束

13.3.4 查询操作日志

可以通过查询操作日志了解涉及用户执行操作的相关信息。

前提条件

已具备“日志管理”的操作权限。

背景信息

- 如果没有设置任何查询条件，则表示查询所有的操作日志。
- 查询结果基于数据库中的现有数据。如果数据未产生，则无数据显示。

操作步骤

步骤 1 在主菜单中选择“系统 > 日志管理”。

步骤 2 在“日志管理”窗口的导航区中，选择“日志查询 > 操作日志”。

步骤 3 直接查看日志信息，或设置搜索条件后查看指定的日志信息。

- 查看单个操作的日志详细信息。
单击目标日志所在“详细信息”列中的值，在“操作日志详情”对话框中可以查看详细的日志信息。
- 查看批量操作的日志详细信息。
 - 单击目标日志所在“详细信息”列中的值。
 - 在“操作日志详情”对话框中单击“查看具体操作日志信息”，查看该操作对应的所有操作结果信息。

----结束

13.4 下级网管

eSight 可以管理下级网管，通过分级管理，建立其区域化、层次化的管理体制，并且分散了大规模网络的管理压力，突破了单网管站点的资源管理能力和性能压力。

13.4.1 了解下级网管

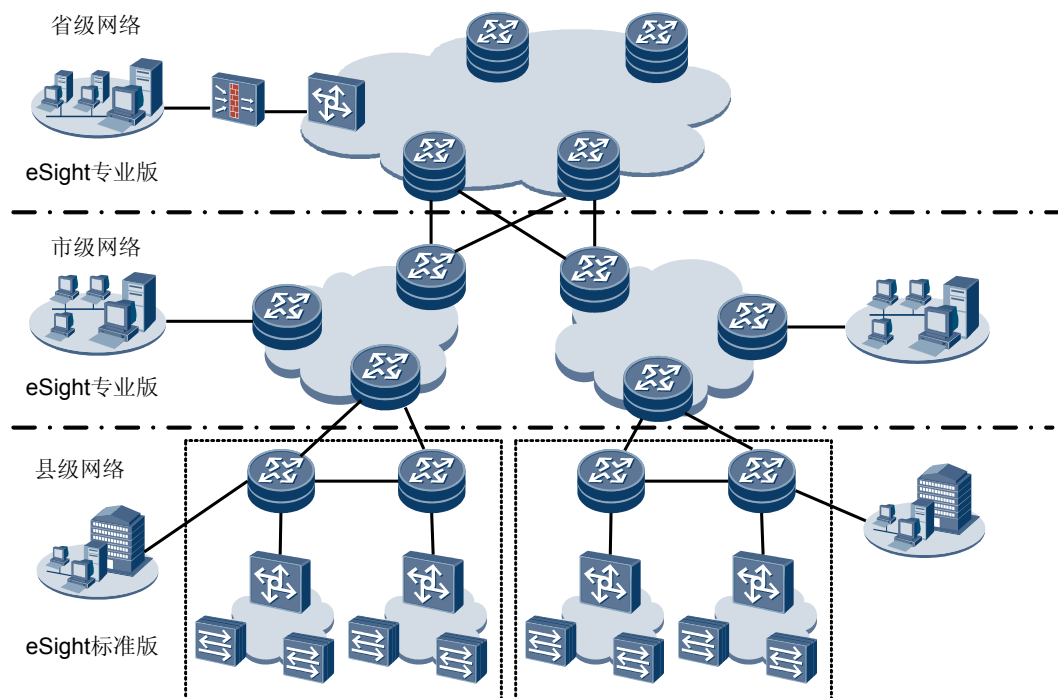
eSight 网管需要建立分级的层次化关系，用户能够按照地域、组织结构等层次关系，划分管理区域，建立起层次化的管理体系，上级网管的权限大于下级网管的权限，上级网管能够管理下级网管，下级网管没有管理上级的权限。

13.4.1.1 下级网管的应用

分级网管，可以对网管权限进行划分，同时分散了管理压力，将一套网管管理的能力分散到多套网管中。

如 [图 13-2](#) 所示，对于不同管理区域，分别有下级网管进行管理，上级网管可以登录到下级网管中，实现对区域设备的管理。

图 13-2 下级网管的应用



13.4.1.2 下级网管相关功能

本节介绍分级网管的基本功能。

用户能够在上级网管界面上打开下级网管的界面，从而查看下级网管的告警、拓扑、性能和报表等功能。所有下级网管的功能，都在下级网管的界面中展现，上级网管只监控下级网管的连通状态，并作单点登录。

为实现上级网管对下级网元的监控，eSight 实现如下功能：

- 增加下级网管
增加下级网管，上级网管才可以对其进行监控。
- 打开下级网管
在上级网管，可以直接打开下级网管，对下级网管的告警、拓扑、性能和报表进行监控。
- 查看下级网管列表
可以查看下级列表的相关信息。
- 删除下级网管
不需要对该下级网管进行监控管理时，可删除该下级网管。

13.4.2 管理下级网管

介绍管理下级网管的操作任务。

13.4.2.1 增加下级网管

可以通过增加下级网管操作，实现上级网管管理下级网管。

前提条件

- 下级网管运行正常。
- 具备增加下级网管的权限。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 下级网管”。
 - 步骤 2** 单击“创建”，在弹出的窗口中，设置“网管名称”、“IP 地址”、“端口号”、“备注”。
 - 步骤 3** 单击“确定”。
- 结束

13.4.2.2 查看下级网管信息

定期查看下级网管的状态，及时对其状态进行跟踪管理。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 下级网管”。
 - 步骤 2 可选:** 在窗口上方设置过滤参数，单击“搜索”。
 - 步骤 3** 查看相关下级网管的状态。
 - 步骤 4 可选:** 单击，修改下级网管的备注信息。单击“确定”。
 - 步骤 5 可选:** 单击相应下级网管的“网管名称”，弹出下级网管的登录页面。输入下级网管的“用户名”和“密码”，进入下级网管，对下级网管进行管理。
- 结束

13.4.2.3 测试下级网管连通性状态

定期测试下级网管的连通性状态，便于对下级网管的连通性状态进行跟踪。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 下级网管”。
 - 步骤 2** 单击“状态检测”，网管将检测下级网管的连通性状态。
-  说明
- 如果没有选择下级网管，网管默认检测所有下级网管的连通性状态。
- 结束

13.5 管理 License

需获取 License 后才能使用 eSight 的各项功能。License 用于对 eSight 资源和功能进行控制。

13.5.1 查看 eSight 当前 License

eSight 支持查看当前使用的 License 的所有信息。

前提条件

已导入 License。

背景信息

License 信息详细说明如[表 13-6](#) 所示。

表 13-6 License 信息

类别	属性	说明	举例
基本信息	有效截止日期	在此日期前 License 有效	2011-04-14
	失效前提醒时间（天）	提示您 License 在此时间后失效并产生告警，您需导入新的 License	15
资源控制	资源名称	License 管理的资源的名称	客户端数
	License 使用状态	License 管理的资源的使用情况	30/2000 表示 License 能够管理的此类资源为 2000，当前已使用 30
	重要告警阈值	当资源使用率超过设定的告警阈值时，系统产生告警	80%
功能控制	功能名称	eSight 提供的功能	故障管理
	是否支持	License 是否支持用户使用此功能	支持

操作步骤

- 步骤 1

在主菜单中选择“系统 > License 管理”。
- 在“License 管理”窗口中，可以查看 License 基本信息、License 资源控制信息、License 功能控制信息。
- 如果当前 License 将要过期，请及时导入新的有效 License。如何导入 License 请参见[13.5.3 导入 License](#)。
- 结束

13.5.2 获取 ESN

当 License 即将过期时，需要获取本机的 ESN 号，用于申请 License。

前提条件

当前用户知道 eSight 服务器的网卡号或 MAC 地址。

背景信息

可以通过选择网卡生成 ESN，也可以通过输入 MAC 地址生成 ESN。

操作步骤

步骤 1 在主菜单中选择“系统 > License 管理”。

步骤 2 在“License 管理”窗口中单击“获取 ESN”。

步骤 3 在“获取 ESN”页面获取 ESN。

- 通过选择网卡生成 ESN
 1. 设置生成 ESN 的网卡。
 2. 单击网卡文本框后的“生成 ESN”。
- 通过输入 MAC 地址生成 ESN
 1. 输入本机 MAC 地址。
 2. 单击 MAC 地址文本框后的“生成 ESN”。

生成的 ESN 会显示在页面最下方的“生成的 ESN”栏中。

----结束

13.5.3 导入 License

当 eSight 当前 License 即将过期时，需要及时导入新的 License。

前提条件

- 已具备“更新 License”的操作权限。
- 已获取新的 License。

操作步骤

步骤 1 在主菜单中选择“系统 > License 管理”。

系统显示当前 License 的所有信息。

步骤 2 在“License 管理”窗口中，单击“导入 License”。

步骤 3 在“导入 License”页面，单击“License 文件”文本框后的 ，选择 License 文件。

步骤 4 单击“导入”。

界面显示新导入的 License 的所有信息。

步骤 5 单击“应用”。

----结束

13.6 备份/恢复数据库

为了保障网管数据库的安全，需及时对网管数据库进行备份/恢复操作。

操作步骤

步骤 1 在网管服务器端启动维护工具。

- Windows 操作系统：单击“开始 > 所有程序 > eSight > 启动维护工具”。
- Linux 操作系统：在安装路径“eSight\mttools\bin”下，执行 run.sh 文件。

步骤 2 在客户端的浏览器中输入登录备份/恢复的 url 地址，登录维护工具。

登录 url 地址示例：http://10.135.23.61:8889。

 说明

- 端口号固定为“8889”。
- 默认的用户名为“admin”，密码为“Changeme123”。

步骤 3 单击“设置备份路径”，设置存储备份文件的路径，单击“确定”。

 说明

网管提供的备份路径为“backupdata”，与安装目录（如 eSight）同级。

步骤 4 单击“备份”，设置“描述信息”，单击“备份”。

步骤 5 可选：根据需要，停止网管服务器，单击  恢复数据库。

步骤 6 可选：根据需要，选中备份任务，单击“删除”，删除备份任务及对应的备份文件。

----结束

13.7 网元包组件管理

通过网元包组件管理可以查看网元包版本、厂商、网元类型、网元包特性等信息，完成网元包的安装和升级操作。

前提条件

已具备“超级管理员”操作权限。

已准备好待安装或待升级的网元包。

已在网管服务器端启动网元包组件管理工具。

- Windows 操作系统：在安装路径“eSight\mttools\bin\runtime.maintenance\bin\”下，执行 startup.bat。
- Linux 操作系统：在安装路径“eSight\mttools\bin\runtime.maintenance\bin\”下，执行 startup.sh。

背景信息

网元包组件管理只支持网元包安装和升级，不支持网元包组件的卸载和降级。

网元包组件管理默认的用户名和密码与 eSight 一致，可在 eSight 中修改用户名和密码。

网元包组件管理使用过程中不允许停止维护工具或数据库，如果出现异常停止导致网元包管理工具不能使用，需要重启维护工具，重新安装/升级网元包。

在用网元包管理工具对网元包进行管理时，在操作前或操作过程中都不允许篡改网元包的数据。

操作步骤

步骤 1 在客户端的浏览器地址栏中输入 **http://eSight服务器的IP地址:8889/**，按“Enter”。

步骤 2 在主菜单中选择“组件 > 网元包组件管理”。

步骤 3 单击“上传网元包”。

步骤 4 在“上传网元包”界面，单击 ，选择准备安装或升级的网元包。

步骤 5 单击 。

步骤 6 上传成功后，单击“返回”。

步骤 7 可选：可通过单击“全部收缩”和“全部展开”查看网元包的详细信息。

 说明

用户可以通过“查询”快速定位到需要查看的网元包，查询的方式支持模糊匹配。

步骤 8 在“操作”中单击  或 ，完成安装或升级。

步骤 9 在“提示”窗口中，单击“是”。

步骤 10 在“任务列表”中可以查看当前任务的状态。

 说明

如果操作结果失败，在“备注”信息中会给出失败的原因。为了便于再次安装或升级网元包，

“操作”下的图标将变为原来的图标  或 。

----结束

14 例行维护

关于本章

介绍日维护操作、周维护操作、月维护操作、季度维护操作，以及如何获取技术支持。通过例行维护，可以及时发现并消除网管运行过程中可能存在的隐患，使系统能够长时间安全、稳定、可靠运行。

14.1 维护项目列表

根据维护的周期不同，例行维护可分为每日维护、每周维护、每月维护和每季度维护。在此按维护周期给出了维护项目列表，在进行网管系统维护时可以参考此表。

14.2 如何获取技术支持

介绍用户在日常维护过程中遇到问题时，获取技术支持的方法。

14.3 每日维护操作

通过日维护操作，可以实时掌握网管的运行情况，了解网管的运行趋势，提高对突发事件的处理效率。

14.4 每周维护操作

通过周维护操作，可以及时发现网管在运行过程中的功能失效、性能下降等缺陷，并采取适当的措施及时予以处理，以消除隐患，预防事故的发生。

14.5 每月维护操作

通过月维护操作，可以使网管系统的健康水平长期处于良好状态，确保系统安全、稳定、可靠的运行。

14.6 每季度维护操作

通过季度维护操作，可以使网管机房环境长期处于良好状态，确保供电及相关硬件的可靠性。

14.1 维护项目列表

根据维护的周期不同，例行维护可分为每日维护、每周维护、每月维护和每季度维护。在此按维护周期给出了维护项目列表，在进行网管系统维护时可以参考此表。

表 14-1 维护项目列表

维护周期	例行维护任务
每日	14.3.1 浏览当前网管告警
	14.3.2 查询安全日志
	14.3.3 备份/恢复数据库
每周	14.4.1 检查服务器磁盘状态
	14.4.2 检查服务器磁盘空间
	14.4.3 检查 Oracle 数据库日志
	14.4.4 检查防病毒软件运行状态
	14.4.5 检查操作系统日志
	14.4.6 检查 MySQL 数据库日志
每月	14.5.1 修改 eSight 当前用户密码
	14.5.2 检查 eSight 服务器时间
	14.5.3 清理 eSight 服务器磁盘空间
每季度	14.6.1 检查机房环境
	14.6.2 检查服务器供电情况
	14.6.3 检查服务器硬件和外设

14.2 如何获取技术支持

介绍用户在日常维护过程中遇到问题时，获取技术支持的方法。

如果在网管系统的日常维护过程中遇到难以确定或难以解决的问题，或者通过本手册的指导仍然不能解决问题，请联系华为技术有限公司客户服务中心，或发邮件至客户服务邮箱 support@huawei.com，也可以从华为技术有限公司的技术支持网页上直接获取最新的技术资料，网址是 <http://support.huawei.com>。

在获取技术支持之前请收集相关信息。

14.3 每日维护操作

通过日维护操作，可以实时掌握网管的运行情况，了解网管的运行趋势，提高对突发事件的处理效率。

14.3.1 浏览当前网管告警

通过在当前告警中设置过滤条件和搜索告警，查看当前需要关注和处理的告警。

前提条件

已具备“当前告警管理”的操作权限。

背景信息

- 当前告警列表是告警归并后的展示。对于新上报的告警，只要当前告警列表中存在符合归并规则的告警记录，都将新上报的告警归并到原有的告警记录中，归并后告警次数加一；若当前告警列表中不存在符合归并规则的告警记录，新上报的告警以一条新记录显示在当前告警列表中。
告警归并规则：当告警源、定位信息和告警标识相同时会归并成一条告警记录。
- 当修改了当前设置的过滤条件时，系统即按照新的过滤条件进行搜索。

操作步骤

- 步骤 1** 在主菜单中选择“故障 > 当前告警”。
- 步骤 2** 在“当前告警”窗口的“过滤条件”下拉菜单中，选择条件进行查询。若当前的过滤条件不满足需求可以自定义过滤条件，请参见 [5.3.3 设置告警自定义过滤条件](#)。
- 步骤 3** 在“当前告警”窗口中可以执行如下操作。

管理告警	操作方法	说明
锁定告警	在窗口中单击“锁定”，当前列表中的告警处于锁定状态。 此时“锁定”按钮自动更新为“解锁”按钮。	当告警处于锁定状态时需要注意： ● 新上报的告警不会更新到当前列表中，解锁后才会更新到当前列表中。 ● 当告警处于可选状态时，可以进行确认、清除和查看详细信息等操作。处于不可选状态的告警，不可以做任何操作。 ● 在锁定状态下确认、清除告警，该告警不会列入到历史告警列表，解锁后才会更新到历史列表中。

管理告警	操作方法	说明
解锁告警	在窗口中单击“解锁”，系统会自动上报告警到当前列表中。 此时“解锁”按钮自动更新为“锁定”按钮。	当告警处于解锁状态时，不能选择条件范围进行搜索，锁定后才能进行搜索。
搜索告警	在窗口中支持如下搜索方式： ● 不设置任何条件直接单击“搜索”，在当前列表中显示所有告警。 ● 当告警处于锁定状态时，在下拉框中选择搜索范围，在文本框中输入搜索的值，单击“搜索”，在当前列表中显示搜索的告警。	-
确认告警	在窗口中选中一条或多条告警，单击“确认”。	● 已确认告警：在“确认用户”列中显示确认用户。 ● 未确认告警：在“确认用户”列中显示👤。
反确认告警	在窗口中选中一条或多条告警，选择“更多 > 反确认”。	通过反确认后，告警由确认状态变成未确认状态。
清除告警	在窗口中选中一条或多条未清除的告警，单击“清除”。	● 已清除告警：告警背景颜色为绿色。 ● 未清除告警：告警背景颜色为白色。
屏蔽告警	1. 在窗口中单击目标告警所在“操作”列中的⚙️，选择“屏蔽规则”。 2. 在“屏蔽规则”对话框中设置规则名称和日期，单击“确定”。	● 新增的告警屏蔽规则默认为启用状态。 ● 屏蔽规则只对屏蔽规则启用且处于生效期间上报的告警生效。屏蔽规则对屏蔽规则设置前上报的告警不生效。 ● 性能告警和已清除的告警不可以设置屏蔽规则。
定制告警列表显示列	单击⚙️，在打开的页面中设置告警列表显示列，单击“确定”。	-
定位拓扑	在窗口中单击目标告警所在“操作”列中的📍。	eSight 将该告警记录定位到拓扑视图中产生告警的对象。
查看告警详情	在窗口中单击需要查看详细信息的“告警名称”。	在“告警详情”对话框中显示了所选告警的名称、告警可能原因和修复建议等信息。
查看告警日志信息	在窗口中单击需要查看日志信息的“告警次数”。	在“告警日志信息”对话框中显示了与该条记录相关的告警日志。

管理告警	操作方法	说明
导出告警信息	在窗口中选择一条或多条告警，选择“导出>导出选中”，导出选择告警的相关信息。 如果需要导出全部可以直接选择“导出>导出全部”。	-

----结束

14.3.2 查询安全日志

可以通过查询安全日志了解涉及 eSight 安全操作的相关信息。

前提条件

已具备“日志管理”的操作权限。

背景信息

- 如果没有设置任何查询条件，则表示查询所有的安全日志。
- 查询结果基于数据库中的现有数据。如果数据未产生，则无数据显示。

操作步骤

步骤 1 在主菜单中选择“系统>日志管理”。

步骤 2 在“日志管理”窗口的导航区中，选择“日志查询>安全日志”。

步骤 3 直接查看日志信息，或设置搜索条件后查看指定的日志信息。

单击目标日志所在“详细信息”列中的值，在“安全日志详情”对话框中，可以查看详细的日志信息。

----结束

14.3.3 备份/恢复数据库

为了保障网管数据库的安全，需及时对网管数据库进行备份/恢复操作。

操作步骤

步骤 1 在网管服务器端启动维护工具。

- Windows 操作系统：单击“开始>所有程序>eSight>启动维护工具”。
- Linux 操作系统：在安装路径“eSight\mttools\bin”下，执行 run.sh 文件。

步骤 2 在客户端的浏览器中输入登录备份/恢复的 url 地址，登录维护工具。

登录 url 地址示例：http://10.135.23.61:8889。

 说明

- 端口号固定为“8889”。
- 默认的用户名为“admin”，密码为“Changeme123”。

步骤 3 单击“设置备份路径”，设置存储备份文件的路径，单击“确定”。



说明

网管提供的备份路径为“backupdata”，与安装目录（如 eSight）同级。

步骤 4 单击“备份”，设置“描述信息”，单击“备份”。

步骤 5 可选：根据需要，停止网管服务器，单击恢复数据库。

步骤 6 可选：根据需要，选中备份任务，单击“删除”，删除备份任务及对应的备份文件。

----结束

14.4 每周维护操作

通过周维护操作，可以及时发现网管在运行过程中的功能失效、性能下降等缺陷，并采取适当的措施及时予以处理，以消除隐患，预防事故的发生。

14.4.1 检查服务器磁盘状态

磁盘状态异常会造成数据丢失，网管无法正常使用。建议定期检查磁盘状态，当发现磁盘故障时及时修复或更换硬盘。

操作步骤

- 对于单机系统（Windows）：
 1. 在“我的电脑”窗口中，选中某个磁盘，单击右键，选择“属性”。
 2. 在弹出的对话框中选择“工具”页签。
 3. 在“查错”区域框中单击“开始检查”。
 4. 在弹出的对话框中，勾选相应的检查选项，单击“开始”，根据系统提示，检查硬盘状态。
- 对于单机系统（Linux）
 1. 打开一个终端窗口，执行以下命令切换到 root 用户：

```
$ su
```

```
Password: <root 用户密码>
```
 2. 执行以下命令查看当前服务器硬盘的物理状态：

```
# smartctl -H /dev/sda
```

----结束

参考标准

如果符合以下标准则证明磁盘状态正常：

1. 在 Windows 单机环境，执行磁盘查错后，提示设备或者磁盘没有问题。
2. 在 Linux 单机系统环境，执行 **smartctl -H /dev/sda** 后，硬盘的“SMART overall-health self-assessment test result”为“PASSED”，表示硬盘的物理状态正常。

异常处理

若磁盘发生了故障，应及时与设备供应商联系修复或更换磁盘。

14.4.2 检查服务器磁盘空间

如果磁盘空间占用率超过 80%，可能会影响网管系统的运行效率或导致服务器无法启动。建议定期检查并及时清理磁盘空间。

操作步骤

- 对于 Windows 系统：
在“计算机管理”中，选择“存储>磁盘管理”，查看服务器磁盘空间。主要查看操作系统和网管程序所在磁盘的空间占用情况。
- 对于 SUSE Linux 系统：
可以通过命令行的方法查看服务器磁盘空间。下面介绍通过命令查看磁盘空间的方法。
 1. 以 root 用户登录操作系统。
 2. 执行以下命令在服务器上查看磁盘使用情况：
df -k

----结束

参考标准

通常情况下，各磁盘空间占用率应低于 80%。

14.4.3 检查 Oracle 数据库日志

介绍如何检查 Oracle 数据库运行的日志信息。

背景信息

eSight 使用 Oracle 数据库。

操作步骤

检查 Oracle 数据库日志文件 \$ORACLE_BASE/diag/rdbms/esight/\$ORACLE_SID/trace/alert_\$ORACLE_SID.log。

 说明

其中环境变量“ORACLE_BASE”和“ORACLE_SID”根据 Oracle 的具体安装情况确定。

参考标准

日志文件中没有影响运行的错误信息。

异常处理

根据日志文件中的错误信息进行修复，如果不能处理，请联系 Oracle 公司技术支持人员。

14.4.4 检查防病毒软件运行状态

及时安装操作系统补丁，升级防病毒软件，查杀病毒，避免服务器和计算机感染网络病毒，保证网管系统安全运行。

操作步骤

及时安装操作系统补丁，升级防病毒软件，定期查杀病毒。

参考标准

没有检查出病毒。

异常处理

检查出病毒后请立即进行杀毒。如果不能解决，请尝试重新安装操作系统。

14.4.5 检查操作系统日志

介绍通过检查操作系统日志的方法检查操作系统运行情况。

操作步骤

- 对于 Windows:
 1. 选择“开始 > 控制面板 > 管理工具 > 事件查看器”。
 2. 在弹出的窗口中查看事件日志信息，检查是否有影响系统运行的异常信息。

 说明
事件查看器的使用方法请参考操作系统自带的联机帮助或用户手册。
- SUSE Linux:
 1. 以 **root** 用户登录操作系统。
 2. 执行以下命令进入日志文件所在目录：
 - SUSE Linux: # **cd /var/log**
 3. 执行以下命令，可以快速查找到是否存在 **error** 信息。
grep error messages*
如果不存在 **error** 信息，执行命令后不显示任何信息。
如果存在 **error** 信息，执行命令后将显示文件中包含的所有 **error** 信息。

----结束

参考标准

- 对于 Windows:
“事件查看器”中没有“错误”信息。
 - 对于 SUSE Linux:
操作系统日志文件中没有“error”信息。
-  窍门
执行以下命令查看所有操作系统日志文件，即 **messages** 开头的文件（包括 **error** 和非 **error**）：
more messages*

异常处理

根据日志文件中的错误信息进行修复，如果不能处理，请联系华为技术有限公司技术支持人员。

14.4.6 检查 MySQL 数据库日志

介绍如何检查 MySQL 数据库运行的日志信息。

背景信息

eSight 使用 MySQL 数据库。

操作步骤

检查 MySQL 安装目录\$eSight_ROOT\MySQL\data 目录下的“.err”日志文件。

参考标准

日志文件中没有影响运行的错误信息。

异常处理

根据日志文件中的错误信息进行修复，如果不能处理，请联系华为技术有限公司技术支持人员。

14.5 每月维护操作

通过月维护操作，可以使网管系统的健康水平长期处于良好状态，确保系统安全、稳定、可靠的运行。

14.5.1 修改 eSight 当前用户密码

介绍用户修改自身密码的操作。建议定期修改密码提高帐户密码的安全性。

前提条件

所设置的密码必须符合密码策略的要求。

操作步骤

- 步骤 1** 在主菜单中选择“系统 > 用户设置”。
 - 步骤 2** 在左侧导航树选择“基本设置 > 修改密码”。
 - 步骤 3** 设置相关参数，单击“应用”。
- 结束

14.5.2 检查 eSight 服务器时间

介绍如何检查服务器的时间是否准确。

操作步骤

- 对于 Windows:
 1. 打开“控制面板”窗口，双击“日期和时间”图标。
 2. 在弹出的对话框中单击“时间和日期”页签，检查系统时间。
- 对于 SUSE Linux:
 1. 以 **root** 用户登录操作系统。
 2. 执行以下命令查看当前服务器时间：
date

----结束

参考标准

服务器时间正确。



注意

- 在告警信息中，如果时间不准确，将无法判断告警发生的先后、告警持续的实际时间、告警之间的关联。
 - 在性能数据记录和统计过程中，如果时间不准确，将直接影响统计的精确度。
-

14.5.3 清理 eSight 服务器磁盘空间

介绍如何清理磁盘空间。定期清理磁盘空间，节省资源。

前提条件



注意

请首先确认所要删除的文件为无用的文件，建议不要删除三天之内生成的文件。

操作步骤

- 对于 Windows:
 1. 使用具有管理员权限的用户登录到 Windows 操作系统。
 2. 删除过时无用的自动转储文件（缺省路径为：“\$eSight_ROOT/AppBase/var/runtime.center/data/dump/”）。
 3. 删除过时无用的运行日志文件（缺省路径为：“\$eSight_ROOT/AppBase/var/runtime.center/log/”）。
 4. 删除其他过时无用的文件，如：旧版本程序安装文件、旧版本补丁安装文件等。
- 对于 SUSE Linux:
 1. 以 **root** 用户登录操作系统。

2. 删除过时无用的自动转储文件（缺省路径为：“\$eSight_ROOT/AppBase/var/runtime.center/data/dump/”）。
3. 删除过时无用的运行日志文件（缺省路径为：“\$eSight_ROOT/AppBase/var/runtime.center/log/”）。
4. 删除其他过时无用的文件，如：旧版本程序安装文件、旧版本补丁安装文件等。

----结束

14.6 每季度维护操作

通过季度维护操作，可以使网管机房环境长期处于良好状态，确保供电及相关硬件的可靠性。

14.6.1 检查机房环境

介绍如何检查网管机房环境是否符合要求。

操作步骤

步骤 1 检查机房环境的温度、湿度和清洁度。

步骤 2 检查机房的供电系统、防尘网、火警装置和防雷击装置。

----结束

参考标准

项目	指标
温度	范围：15° C ~ 35° C。
湿度	范围：40%~ 65%。
清洁度	干净，无明显灰尘。
供电系统	供电正常，保证机房设备的正常运行。
防尘网	防尘网清洁，机柜进风、排风通畅。
火警装置	正常工作，能有效感应火灾的发生。
防雷击装置	正常工作，有效地预防雷击发生。

异常处理

1. 适当调整机房的温度、湿度，改善门、窗的密封效果，以及定期清洁等。
2. 将防尘网从机柜中拆卸下来，用吸尘器将防尘网上面的灰尘吸干净后，再将防尘网安装到机柜中。
3. 维修供电系统、火警装置或防雷击装置，保证机房设备安全、正常地工作。

14.6.2 检查服务器供电情况

检查网管服务器电源是否正常。

前提条件

网管服务器处于通电状态。

操作步骤

步骤 1 查看服务器和显示器电源指示灯是否正常。

步骤 2 对于 SUSE Linux 系统，执行以下命令，查看系统最近几天内日志信息所记录的电源故障信息。

```
# more /var/log/messages|grep PSU
```

```
# more /var/log/warn|grep PSU
```

显示类似如下信息：

```
Jun 23 16:53:40 Server rmclomv: [ID 632913 kern.error] Input power unavailable for PSU @ PS1.
```

如果显示有 error 或 WARN，表示电源有故障。

步骤 3 检查系统外部电源故障。

步骤 4 确认服务器电源正常。

----结束

参考标准

正常情况下，服务器外设所有电源指示灯都是绿色的，所有故障指示灯都是一直熄灭的。

异常处理

如果是系统外部电源故障，则系统不会记录电源故障信息，需通过其他方法检测外部供电电源和线路，请参见服务器随机手册查找故障。复杂问题请联系生产厂家进行维修或更换。

14.6.3 检查服务器硬件和外设

介绍如何检查网管服务器的硬件和外设状态。

前提条件

网管系统处于通电状态。

操作步骤

步骤 1 根据服务器的具体型号，参见服务器的随机手册，检查硬件设备。

步骤 2 如果使用了磁盘阵列，查看其型号参见对应的磁盘阵列的相关手册，检查硬件设备。

步骤 3 检查 CD/DVD-ROM 是否可以正常运行。

----结束

参考标准

正常情况下，服务器和外设运行正常，各指示灯显示正常。

异常处理

根据服务器和外设的具体型号，参见随机手册，查找故障。复杂问题请联系生产厂家进行维修或更换。

15 命令参考

关于本章

介绍维护 eSight 的常用命令。

[15.1 eSight 命令参考](#)

介绍 eSight 的命令及功能。

[15.2 Oracle 命令参考](#)

介绍常见的 Oracle 数据库命令的使用参考，包括各命令的功能说明和应用实例。

15.1 eSight 命令参考

介绍 eSight 的命令及功能。

15.1.1 启动 eSight 进程和帮助进程

在此给出了启动 eSight 进程和帮助进程的命令参考。

前提条件

数据库已启动。

背景信息

成功启动进程并退出命令行窗口后，eSight 仍正常运行。

操作步骤

可在如下操作系统中启动 eSight 进程和帮助进程：

- [Windows 操作系统](#)
- [Linux 操作系统](#)

Windows 操作系统

- 命令格式：run.bat
- 输入示例

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

```
cd /d eSight_ROOT\AppBase\bin
```

 说明

“eSight_ROOT” 为 eSight 的安装目录。

3. 执行如下命令启动 eSight 进程和帮助进程。

```
run.bat
```

 说明

执行此命令后，会打开一个新的命令行窗口。

- 输出示例

执行成功后，输出结果如下所示：

```
[10:50:44] Help System: started
[10:51:35] Loading kernel
[10:51:35] com.huawei.oms.bootstage: started
[10:51:38] org.eclipse.virgo.kernel.userregion.springdm: started
[10:51:41] org.eclipse.virgo.web: started
[10:51:50] com.huawei.oms.base: started
[10:52:29] com.huawei.oms.web.portal: started
[10:52:29] Loading PKG
[10:52:32] com.huawei.oms.app.audit: started
[10:52:35] com.huawei.oms.app.autodiscovery: started
[10:52:38] com.huawei.oms.app.dump: started
[10:52:41] com.huawei.oms.app.email: started
[10:52:53] com.huawei.oms.app.license.monitor: started
```

```
[10:52:56] com.huawei.oms.app.license: started
[10:52:59] com.huawei.oms.app.nbi: started
[10:53:02] com.huawei.oms.app.panel: started
[10:53:14] com.huawei.oms.app.pm: started
[10:53:26] com.huawei.oms.framework.core: started
[10:53:26] com.huawei.oms.app.sm: started
[10:53:26] com.huawei.oms.app.topo: started
[10:53:32] com.huawei.oms.framework.eam: started
[10:53:32] com.huawei.oms.framework.med.center: started
[10:53:32] com.huawei.oms.framework.med.node: started
[10:53:35] com.huawei.oms.framework.nem: started
[10:53:35] com.huawei.oms.sdk.audit: started
[10:53:35] com.huawei.oms.sdk.eam: started
[10:53:35] com.huawei.oms.app.integrated: started
[10:53:36] com.huawei.oms.sdk.fm: started
[10:53:39] com.huawei.oms.app.fm: started
[10:53:45] com.huawei.oms.sdk.med: started
[10:53:45] com.huawei.oms.sdk.momgr: started
[10:53:45] com.huawei.oms.sdk.topo: started
[10:53:45] com.huawei.oms.sdk.sm: started
[10:53:54] com.huawei.oms.test: started
[10:53:54] Activating system
[10:53:54] MORE service: actived
[10:53:54] PM SnmpByTable: actived
[10:53:54] LICENSE: actived
[10:53:54] PM SnmpByIndex: actived
[10:53:54] MOPKG: actived
[10:53:54] PM: actived
[10:53:54] EAM AS: actived
[10:53:54] TOPO: actived
[10:53:57] FM probe: actived
[10:53:57] FM: actived
[10:54:00] EAM DS: actived
[10:54:00] SM: actived
[10:54:00] EAM IconMgr: actived
[10:54:00] System start completely
Finished
```

Linux 操作系统

- 命令格式: **run.sh**
- 输入示例

1. 以 root 用户登录服务器。
2. 执行如下命令切换目录。
cd eSight_ROOT/AppBase/bin
3. 执行如下命令启动 eSight 进程和帮助进程。

./run.sh



说明
执行此命令后, 会打开一个新的命令行窗口。

- 输出示例

执行成功后, 输出结果如下所示:

```
[11:00:35] Help System: started
[11:00:42] Loading kernel
[11:00:42] com.huawei.oms.bootstage: started
[11:00:45] org.eclipse.virgo.kernel.userregion.springdm: started
[11:00:48] org.eclipse.virgo.web: started
[11:00:51] com.huawei.oms.base: started
[11:01:12] com.huawei.oms.web.portal: started
[11:01:12] Loading PKG
[11:01:12] com.huawei.oms.sdk.sm: started
[11:01:15] com.huawei.oms.sdk.med: started
[11:01:15] com.huawei.oms.framework.med.center: started
```

```
[11:01:15] com.huawei.oms.app.audit: started
[11:01:18] com.huawei.oms.app.license.monitor: started
[11:01:18] com.huawei.oms.app.panel: started
[11:01:21] com.huawei.oms.app.license: started
[11:01:21] com.huawei.oms.app.sm: started
[11:01:21] com.huawei.oms.app.nbi: started
[11:01:21] com.huawei.oms.sdk.audit: started
[11:01:21] com.huawei.oms.sdk.fm: started
[11:01:21] com.huawei.oms.sdk.mongr: started
[11:01:21] com.huawei.oms.app.autodiscovery: started
[11:01:24] com.huawei.oms.app.dump: started
[11:01:24] com.huawei.oms.framework.nem: started
[11:01:27] com.huawei.oms.test: started
[11:01:27] com.huawei.oms.sdk.topo: started
[11:01:27] com.huawei.oms.sdk.eam: started
[11:01:27] com.huawei.oms.framework.core: started
[11:01:27] com.huawei.oms.framework.eam: started
[11:01:27] com.huawei.oms.app.integrated: started
[11:01:27] com.huawei.oms.framework.med.node: started
[11:01:30] com.huawei.oms.app.fm: started
[11:01:33] com.huawei.oms.app.email: started
[11:01:36] com.huawei.oms.app.topo: started
[11:01:39] com.huawei.oms.app.pm: started
[11:01:39] Activating system
[11:01:39] MORE service: actived
[11:01:39] LICENSE: actived
[11:01:39] MOPKG: actived
[11:01:39] PM SnmpByTable: actived
[11:01:39] PM SnmpByIndex: actived
[11:01:39] PM: actived
[11:01:39] EAM AS: actived
[11:01:39] TOPO: actived
[11:01:42] FM probe: actived
[11:01:42] FM: actived
[11:01:42] EAM IconMgr: actived
[11:01:42] EAM DS: actived
[11:01:42] SM: actived
[11:01:42] System start completely
Finished
```

15.1.2 停止 eSight 进程和帮助进程

在此给出了停止 eSight 进程和帮助进程的命令参考。

可在如下操作系统中停止 eSight 进程和帮助进程：

- [Windows 操作系统](#)
- [Linux 操作系统](#)

Windows 操作系统

- 命令格式：stop.bat
- 输入示例

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

```
cd /d eSight_ROOT\AppBase\bin
```

 说明

“eSight_ROOT” 为 eSight 的安装目录。

3. 执行如下命令停止 eSight 进程和帮助进程。

```
stop.bat
```



说明

执行此命令后，会打开一个新的命令行窗口。

- **输出示例**

执行成功后，输出结果如下所示：

```
[11:00:18] Base Module: stopped
[11:00:18] Kernel Module: stopped
[11:00:19] Help System: stopped
Finished
```

Linux 操作系统

- **命令格式：stop.sh**

- **输入示例**

1. 以 root 用户登录服务器。
2. 执行如下命令切换目录。
cd eSight_ROOT/AppBase/bin
3. 执行如下命令停止 eSight 进程和帮助进程。

./stop.sh



说明

执行此命令后，会打开一个新的命令行窗口。

- **输出示例**

执行成功后，输出结果如下所示：

```
[11:03:40] Base Module: stopped
[11:03:40] Kernel Module: stopped
[11:03:44] Help System: stopped
Finished
```

15.1.3 查看日志级别

在此给出了查看日志级别的命令参考。

前提条件

数据库已启动。

操作步骤

可在如下操作系统中查看日志级别：

- **Windows 操作系统**
- **Linux 操作系统**

Windows 操作系统

- **命令格式：omscli.bat log <[all | logname]>**
- **输入示例**

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

cd /d eSight_ROOT\AppBase\bin\runtime.center\bin



说明

“eSight_ROOT”为 eSight 的安装目录。

3. 执行如下命令启动 eSight 进程。

startup.bat

4. 执行如下命令查看日志级别。

- 查看所有日志级别。

omscli.bat log all

- 查看单个模块日志的日志级别。

例如，查看“bme”日志的日志级别。

omscli.bat log bme

● 输出示例

- 执行成功后，所有日志的日志级别如下所示：

No	Name	Level	
	File		
1	apache	WARN	D:\OMS\var\runtime.center\log\oms\core\apache.log
2	asutil	DEBUG	D:\OMS\var\runtime.center\log\oms\asutil\asutil.log
3	base	DEBUG	D:\OMS\var\runtime.center\log\oms\core\base.log
4	bme	DEBUG	D:\OMS\var\runtime.center\log\bme\bme.log
5	cache	DEBUG	D:\OMS\var\runtime.center\log\oms\core\cache.log
6	configure	DEBUG	D:\OMS\var\runtime.center\log\oms\core\configure.log
7	dbvtutil	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\dbvtutil.log
8	dis_frame	DEBUG	D:\OMS\var\runtime.center\log\oms\autodis\dis_frame.log
9	dis_lldp	DEBUG	D:\OMS\var\runtime.center\log\oms\autodis\dis_lldp.log
10	dis_snmp	DEBUG	D:\OMS\var\runtime.center\log\oms\autodis\dis_snmp.log
11	dump_ds	DEBUG	D:\OMS\var\runtime.center\log\oms\dump\dump_ds.log
12	dump_support	DEBUG	D:\OMS\var\runtime.center\log\oms\dump\dump_support.log
13	dump_ui	DEBUG	D:\OMS\var\runtime.center\log\oms\dump\dump_ui.log
14	eam_as	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\eam_as.log
15	eam_ds	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\eam_ds.log
16	eam_sdk	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\eam_sdk.log
17	eam_test	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\eam_test.log
18	eam_ui	DEBUG	D:\OMS\var\runtime.center\log\oms\eam\eam_ui.log
19	email	DEBUG	D:\OMS\var\runtime.center\log\oms\email\email.log
20	email.server.support	DEBUG	D:\OMS\var\runtime.center\log\oms\email\email.server.support.log
21	event	DEBUG	D:\OMS\var\runtime.center\log\oms\core\event.log
22	fm	DEBUG	D:\OMS\var\runtime.center\log\oms\fm\fm.log
23	fmbackup	DEBUG	D:\OMS\var\runtime.center\log\oms\fm\fmbackup.log
24	fmcolor	DEBUG	D:\OMS\var\runtime.center\log\oms\fm\fmcolor.log

25 fmconnect \fmconnect.log	DEBUG D:\OMS\var\runtime.center\log\oms\fm
26 fmprobe \fmprobe.log	DEBUG D:\OMS\var\runtime.center\log\oms\fm
27 fmtest \fmtest.log	DEBUG D:\OMS\var\runtime.center\log\oms\fm
28 fmui \fmui.log	DEBUG D:\OMS\var\runtime.center\log\oms\fm
29 framework.portal.ds \framework.portal.ds.log	DEBUG D:\OMS\var\runtime.center\log\oms\core
30 fsm \fsm.log	DEBUG D:\OMS\var\runtime.center\log\oms\core
31 ftp.client \ftp.client.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
32 ftp.med \ftp.med.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
33 ftp.server \ftp.server.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
34 iconmgr \iconmgr.log	DEBUG D:\OMS\var\runtime.center\log\oms\eam
35 ip.validate \ip.validate.log	DEBUG D:\OMS\var\runtime.center\log\oms\core
36 log.mgmt \log.mgmt.log	DEBUG D:\OMS\var\runtime.center\log\oms\core
37 mapping \mapping.log	DEBUG D:\OMS\var\runtime.center\log\oms\topo
38 med \med.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
39 med.enter \med.enter.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
40 med.node \med.node.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
41 med.util \med.util.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
42 mim \mim.log	DEBUG D:\OMS\var\runtime.center\log\oms\eam
43 mimcache \mimcache.log	DEBUG D:\OMS\var\runtime.center\log\oms\eam
44 mml.client \mml.client.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
45 mml.med \mml.med.log	DEBUG D:\OMS\var\runtime.center\log\oms\med
46 moTypeUpdate \moTypeUpdate.log	DEBUG D:\OMS\var\runtime.center\log\demo
47 moconfig \moconfig.log	DEBUG D:\OMS\var\runtime.center\log\oms\momgr
48 monitor \monitor.log	DEBUG D:\OMS\var\runtime.center\log\oms\license
49 mopkg \mopkg.log	DEBUG D:\OMS\var\runtime.center\log\oms\core
50 more \more.log	DEBUG D:\OMS\var\runtime.center\log\oms\momgr
51 moservice \moservice.log	DEBUG D:\OMS\var\runtime.center\log\demo
52 moui \moui.log	DEBUG D:\OMS\var\runtime.center\log\oms\momgr
53 nbi \nbi.log	DEBUG D:\OMS\var\runtime.center\log\oms\nbi
54 nePermitGate \nePermitGate.log	DEBUG D:\OMS\var\runtime.center\log\oms\sm
55 oms.license.as \oms.license.as.log	DEBUG D:\OMS\var\runtime.center\log\oms\license
56 oms.license.ui \oms.license.ui.log	DEBUG D:\OMS\var\runtime.center\log\oms\license
57 oms_audit \oms_audit.log	DEBUG D:\OMS\var\runtime.center\log\oms\audit
58 oms_audit_as \oms_audit_as.log	DEBUG D:\OMS\var\runtime.center\log\oms\audit
59 panel_ds	DEBUG D:\OMS\var\runtime.center\log\oms\panel

```
\panel_ds.log
60 panel_gapi          DEBUG D:\OMS\var\runtime.center\log\oms\panel
\panel_gapi.log
61 panel_ui            DEBUG D:\OMS\var\runtime.center\log\oms\panel
\panel_ui.log
62 persistence         DEBUG D:\OMS\var\runtime.center\log\oms\core
\persistence.log
63 pm                  DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pm.log
64 pmdata              DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmdata.log
65 pmds                DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmds.log
66 pmmeastype          DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmmeastype.log
67 pmprobe             DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmprobe.log
68 pmtest              DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmtest.log
69 pmthreshold         DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmthreshold.log
70 pmui                DEBUG D:\OMS\var\runtime.center\log\oms\pm
\pmui.log
71 portal.client       DEBUG D:\OMS\var\runtime.center\log\oms\core
\portal.client.log
72 portal.server       DEBUG D:\OMS\var\runtime.center\log\oms\core
\portal.server.log
73 root                DEBUG D:\OMS\var\runtime.center\log
\root.log
74 sbus                DEBUG D:\OMS\var\runtime.center\log\oms\core
\sbus.log
75 sbus.client         DEBUG D:\OMS\var\runtime.center\log\oms\core
\sbus.client.log
76 sbus.heartbeat      DEBUG D:\OMS\var\runtime.center\log\oms\core
\sbus.heartbeat.log
77 sbus.server         DEBUG D:\OMS\var\runtime.center\log\oms\core
\sbus.server.log
78 sm                  DEBUG D:\OMS\var\runtime.center\log\oms\sm
\sm.log
79 snmp4j              DEBUG D:\OMS\var\runtime.center\log\oms\med
\snmp4j.log
80 ssh.client          DEBUG D:\OMS\var\runtime.center\log\oms\med
\ssh.client.log
81 ssh.med             DEBUG D:\OMS\var\runtime.center\log\oms\med
\ssh.med.log
82 task                DEBUG D:\OMS\var\runtime.center\log\oms\core
\task.log
83 telnet.client       DEBUG D:\OMS\var\runtime.center\log\oms\med
\telnet.client.log
84 telnet.med          DEBUG D:\OMS\var\runtime.center\log\oms\med
\telnet.med.log
85 topo_ds             DEBUG D:\OMS\var\runtime.center\log\oms\topo
\topo_ds.log
86 topo_sdk            DEBUG D:\OMS\var\runtime.center\log\oms\topo
\topo_sdk.log
87 topo_ui             DEBUG D:\OMS\var\runtime.center\log\oms\topo
\topo_ui.log
88 topomgr             DEBUG D:\OMS\var\runtime.center\log\oms\topo
\topomgr.log
```

- 执行成功后，“bme”日志的日志级别如下所示：

```
No  Name  Level  File
1   bme   DEBUG  D:\OMS\var\runtime.center\log\bme\bme.log
```

Linux 操作系统

- 命令格式：**omscli.sh log <[all | logname]>**
- 输入示例

1. 以 root 用户登录服务器。
2. 执行如下命令切换目录。
cd eSight_ROOT/AppBase/bin/runtime.center/bin
3. 执行如下命令启动 eSight 进程。
./startup.sh
4. 执行如下命令查看日志级别。
 - 查看所有日志级别。
./omscli.sh log all
 - 查看单个模块日志的日志级别。
例如，查看“bme”日志的日志级别。
./omscli.sh log bme

● 输出示例

- 执行成功后，所有日志的日志级别如下所示：

No	Name	Level	File
1	apache	WARN	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/core/apache.log
2	asutil	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/asutil/asutil.log
3	base	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/core/base.log
4	bme	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/bme.log
5	cache	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/core/cache.log
6	configure	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/core/configure.log
7	dbevtutil	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/dbevtutil.log
8	dis_frame	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/autodis/dis_frame.log
9	dis_lldp	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/autodis/dis_lldp.log
10	dis_snmp	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/autodis/dis_snmp.log
11	dump_ds	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/dump/dump_ds.log
12	dump_support	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/dump/dump_support.log
13	dump_ui	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/dump/dump_ui.log
14	eam_as	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/eam_as.log
15	eam_ds	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/eam_ds.log
16	eam_sdk	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/eam_sdk.log
17	eam_test	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/eam_test.log
18	eam_ui	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/eam_ui.log
19	email	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/email/email.log
20	email.server.support	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/email/email.server.support.log
21	event	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/core/event.log
22	fm	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/fm.log
23	fmbackup	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/fmbackup.log

24	fmcolor	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/
	fmcolor.log		
25	fmconnect	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/
	fmconnect.log		
26	fmprobe	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/
	fmprobe.log		
27	fmtest	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/
	fmtest.log		
28	fmui	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/fm/
	fmui.log		
29	framework.portal.ds	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	core/framework.portal.ds.log		
30	fsm	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	core/fsm.log		
31	ftp.client	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	ftp.client.log		
32	ftp.med	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	ftp.med.log		
33	ftp.server	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	ftp.server.log		
34	iconmgr	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/
	iconmgr.log		
35	ip.validate	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	core/ip.validate.log		
36	log.mgmt	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	core/log.mgmt.log		
37	mapping	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	topo/mapping.log		
38	med	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	med.log		
39	med.enter	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	med.enter.log		
40	med.node	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	med.node.log		
41	med.util	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	med.util.log		
42	mim	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/
	mim.log		
43	mimcache	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/eam/
	mimcache.log		
44	mml.client	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	mml.client.log		
45	mml.med	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
	mml.med.log		
46	moTypeUpdate	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/demo/
	moTypeUpdate.log		
47	moconfig	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	momgr/moconfig.log		
48	monitor	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	license/monitor.log		
49	mopkg	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	core/mopkg.log		
50	more	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	momgr/more.log		
51	moservice	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/demo/
	moservice.log		
52	moui	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	momgr/moui.log		
53	nbi	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/nbi/
	nbi.log		
54	nePermitGate	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/sm/
	nePermitGate.log		
55	oms.license.as	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	license/oms.license.as.log		
56	oms.license.ui	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	license/oms.license.ui.log		
57	oms_audit	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
	audit/oms_audit.log		
58	oms_audit_as	DEBUG	/opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/

audit/oms_audit_as.log	
59 panel_ds	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
panel/panel_ds.log	
60 panel_gapi	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
panel/panel_gapi.log	
61 panel_ui	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
panel/panel_ui.log	
62 persistence	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/persistence.log	
63 pm	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pm.log	
64 pmdata	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmdata.log	
65 pmds	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmds.log	
66 pmmeastype	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmmeastype.log	
67 pmprobe	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmprobe.log	
68 pmtest	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmtest.log	
69 pmthreshold	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmthreshold.log	
70 pmui	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/pm/
pmui.log	
71 portal.client	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/portal.client.log	
72 portal.server	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/portal.server.log	
73 root	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/
root.log	
74 sbus	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/sbus.log	
75 sbus.client	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/sbus.client.log	
76 sbus.heartbeat	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/sbus.heartbeat.log	
77 sbus.server	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/sbus.server.log	
78 sm	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/sm/
sm.log	
79 snmp4j	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
snmp4j.log	
80 ssh.client	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
ssh.client.log	
81 ssh.med	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
ssh.med.log	
82 task	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
core/task.log	
83 telnet.client	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
telnet.client.log	
84 telnet.med	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/med/
telnet.med.log	
85 topo_ds	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
topo/topo_ds.log	
86 topo_sdk	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
topo/topo_sdk.log	
87 topo_ui	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
topo/topo_ui.log	
88 topomgr	DEBUG /opt/OMS/OMS_run/17_12_sub/var/runtime.center/log/oms/
topo/topomgr.log	
- 执行成功后，“bme”日志的日志级别如下所示：	
No	Name Level File
1	bme DEBUG /opt/OMS/SUBtr51201/../../var/runtime.center/log/bme/bme.log

15.1.4 修改日志级别

在此给出了修改日志级别的命令参考。

前提条件

数据库已启动。

操作步骤

可在如下操作系统中修改日志级别：

- **Windows 操作系统**
- **Linux 操作系统**

Windows 操作系统

- **命令格式：**`omscli.bat log <[ all | logname ]> <[ level | default ]>`
- **输入示例**

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

```
cd /d eSight_ROOT\AppBase\bin\runtime.center\bin
```



“eSight_ROOT” 为 eSight 的安装目录。

3. 执行如下命令启动 eSight 进程。

```
startup.bat
```

4. 执行如下命令修改日志级别。

- 修改所有日志的日志级别。

例如，将所有日志的日志级别修改为 “error”。

```
omscli.bat log all error
```

- 修改单个模块日志的日志级别。

例如，将 “bme” 日志的日志级别修改为 “debug”。

```
omscli.bat log bme debug
```

- **输出示例**

- 执行成功后，所有日志级别被修改为 “error”。输出结果如下所示：

```
Change log level of apache           from WARN  to ERROR
Change log level of asutil           from DEBUG to ERROR
Change log level of base             from DEBUG to ERROR
Change log level of bme              from DEBUG to ERROR
Change log level of cache            from DEBUG to ERROR
Change log level of configure        from DEBUG to ERROR
Change log level of dbvtutil         from DEBUG to ERROR
Change log level of dis_frame        from DEBUG to ERROR
Change log level of dis_lldp         from DEBUG to ERROR
Change log level of dis_snmp         from DEBUG to ERROR
Change log level of dump_ds          from DEBUG to ERROR
Change log level of dump_support     from DEBUG to ERROR
Change log level of dump_ui          from DEBUG to ERROR
Change log level of eam_as           from DEBUG to ERROR
Change log level of eam_ds           from DEBUG to ERROR
Change log level of eam_sdk          from DEBUG to ERROR
Change log level of eam_test         from DEBUG to ERROR
Change log level of eam_ui           from DEBUG to ERROR
Change log level of email            from DEBUG to ERROR
Change log level of email.server.support from DEBUG to ERROR
Change log level of event            from DEBUG to ERROR
Change log level of fm               from DEBUG to ERROR
Change log level of fmbackup         from DEBUG to ERROR
Change log level of fmcolor          from DEBUG to ERROR
```

```
Change log level of fmconnect          from DEBUG to ERROR
Change log level of fmprobe            from DEBUG to ERROR
Change log level of fmtest             from DEBUG to ERROR
Change log level of fmui               from DEBUG to ERROR
Change log level of framework.portal.ds from DEBUG to ERROR
Change log level of fsm                from DEBUG to ERROR
Change log level of ftp.client         from DEBUG to ERROR
Change log level of ftp.med            from DEBUG to ERROR
Change log level of ftp.server         from DEBUG to ERROR
Change log level of iconmgr            from DEBUG to ERROR
Change log level of ip.validate        from DEBUG to ERROR
Change log level of log.mgmt           from DEBUG to ERROR
Change log level of mapping            from DEBUG to ERROR
Change log level of med                from DEBUG to ERROR
Change log level of med.enter          from DEBUG to ERROR
Change log level of med.node           from DEBUG to ERROR
Change log level of med.util           from DEBUG to ERROR
Change log level of mim                from DEBUG to ERROR
Change log level of mimcache           from DEBUG to ERROR
Change log level of mml.client         from DEBUG to ERROR
Change log level of mml.med            from DEBUG to ERROR
Change log level of moTypeUpdate       from DEBUG to ERROR
Change log level of moconfig           from DEBUG to ERROR
Change log level of monitor            from DEBUG to ERROR
Change log level of mopkg              from DEBUG to ERROR
Change log level of more               from DEBUG to ERROR
Change log level of moservice          from DEBUG to ERROR
Change log level of moui               from DEBUG to ERROR
Change log level of nbi                from DEBUG to ERROR
Change log level of nePermitGate       from DEBUG to ERROR
Change log level of oms.license.as     from DEBUG to ERROR
Change log level of oms.license.ui     from DEBUG to ERROR
Change log level of oms_audit          from DEBUG to ERROR
Change log level of oms_audit_as       from DEBUG to ERROR
Change log level of panel_ds           from DEBUG to ERROR
Change log level of panel_gapi         from DEBUG to ERROR
Change log level of panel_ui           from DEBUG to ERROR
Change log level of persistence        from DEBUG to ERROR
Change log level of pm                 from DEBUG to ERROR
Change log level of pmdata             from DEBUG to ERROR
Change log level of pmds               from DEBUG to ERROR
Change log level of pmmeastype         from DEBUG to ERROR
Change log level of pmprobe            from DEBUG to ERROR
Change log level of pmtest             from DEBUG to ERROR
Change log level of pmthreshold        from DEBUG to ERROR
Change log level of pmui               from DEBUG to ERROR
Change log level of portal.client      from DEBUG to ERROR
Change log level of portal.server      from DEBUG to ERROR
Change log level of root               from DEBUG to ERROR
Change log level of sbus               from DEBUG to ERROR
Change log level of sbus.client         from DEBUG to ERROR
Change log level of sbus.heartbeat     from DEBUG to ERROR
Change log level of sbus.server        from DEBUG to ERROR
Change log level of sm                 from DEBUG to ERROR
Change log level of snmp4j             from DEBUG to ERROR
Change log level of ssh.client         from DEBUG to ERROR
Change log level of ssh.med            from DEBUG to ERROR
Change log level of task               from DEBUG to ERROR
Change log level of telnet.client       from DEBUG to ERROR
Change log level of telnet.med         from DEBUG to ERROR
Change log level of topo_ds            from DEBUG to ERROR
Change log level of topo_sdk           from DEBUG to ERROR
Change log level of topo_ui            from DEBUG to ERROR
Change log level of topomgr            from DEBUG to ERROR
```

- 执行成功后，“bme”日志级别被修改为“debug”。输出结果如下所示：

```
Change log level of bme                from ERROR to DEBUG
```

Linux 操作系统

- 命令格式: **omscli.sh log** <[all | logname]> <[level | default]>

- 输入示例

1. 以 root 用户登录服务器。

2. 执行如下命令切换目录。

cd eSight_ROOT/AppBase/bin/runtime.center/bin

3. 执行如下命令启动 eSight 进程。

./startup.sh

4. 执行如下命令修改日志级别。

- 修改所有日志的日志级别。

例如，将所有日志的日志级别修改为 “error”。

./omscli.sh log all error

- 修改单个模块日志的日志级别。

例如，将 “bme” 日志的日志级别修改为 “error”。

./omscli.sh log bme error

- 输出示例

- 执行成功后，所有日志的日志级别被修改为 “error”。输出的结果如下所示：

```
Change log level of apache           from WARN  to ERROR
Change log level of asutil           from DEBUG to ERROR
Change log level of base              from DEBUG to ERROR
Change log level of bme              from DEBUG to ERROR
Change log level of cache             from DEBUG to ERROR
Change log level of configure         from DEBUG to ERROR
Change log level of dbvtutil         from DEBUG to ERROR
Change log level of dis_frame         from DEBUG to ERROR
Change log level of dis_lldp         from DEBUG to ERROR
Change log level of dis_snmp         from DEBUG to ERROR
Change log level of dump_ds          from DEBUG to ERROR
Change log level of dump_support     from DEBUG to ERROR
Change log level of dump_ui          from DEBUG to ERROR
Change log level of eam_as           from DEBUG to ERROR
Change log level of eam_ds           from DEBUG to ERROR
Change log level of eam_sdk          from DEBUG to ERROR
Change log level of eam_test         from DEBUG to ERROR
Change log level of eam_ui           from DEBUG to ERROR
Change log level of email            from DEBUG to ERROR
Change log level of email.server.support from DEBUG to ERROR
Change log level of event            from DEBUG to ERROR
Change log level of fm              from DEBUG to ERROR
Change log level of fmbackup         from DEBUG to ERROR
Change log level of fmcolor         from DEBUG to ERROR
Change log level of fmconnect        from DEBUG to ERROR
Change log level of fmprobe         from DEBUG to ERROR
Change log level of fmtest          from DEBUG to ERROR
Change log level of fmui            from DEBUG to ERROR
Change log level of framework.portal.ds from DEBUG to ERROR
Change log level of fsm             from DEBUG to ERROR
Change log level of ftp.client       from DEBUG to ERROR
Change log level of ftp.med         from DEBUG to ERROR
Change log level of ftp.server      from DEBUG to ERROR
Change log level of iconmgr         from DEBUG to ERROR
Change log level of ip.validate     from DEBUG to ERROR
Change log level of log.mgmt        from DEBUG to ERROR
Change log level of mapping         from DEBUG to ERROR
Change log level of med             from DEBUG to ERROR
Change log level of med.enter       from DEBUG to ERROR
Change log level of med.node        from DEBUG to ERROR
Change log level of med.util        from DEBUG to ERROR
Change log level of mim             from DEBUG to ERROR
```

```
Change log level of mimcache           from DEBUG to ERROR
Change log level of mml.client          from DEBUG to ERROR
Change log level of mml.med             from DEBUG to ERROR
Change log level of moTypeUpdate        from DEBUG to ERROR
Change log level of moconfig            from DEBUG to ERROR
Change log level of monitor             from DEBUG to ERROR
Change log level of mopkg               from DEBUG to ERROR
Change log level of more                 from DEBUG to ERROR
Change log level of moservice            from DEBUG to ERROR
Change log level of moui                from DEBUG to ERROR
Change log level of nbi                  from DEBUG to ERROR
Change log level of nePermitGate         from DEBUG to ERROR
Change log level of oms.license.as      from DEBUG to ERROR
Change log level of oms.license.ui      from DEBUG to ERROR
Change log level of oms_audit           from DEBUG to ERROR
Change log level of oms_audit_as        from DEBUG to ERROR
Change log level of panel_ds            from DEBUG to ERROR
Change log level of panel_gapi          from DEBUG to ERROR
Change log level of panel_ui            from DEBUG to ERROR
Change log level of persistence         from DEBUG to ERROR
Change log level of pm                  from DEBUG to ERROR
Change log level of pmdata              from DEBUG to ERROR
Change log level of pmds                from DEBUG to ERROR
Change log level of pmmeastype          from DEBUG to ERROR
Change log level of pmprobe             from DEBUG to ERROR
Change log level of pmtest              from DEBUG to ERROR
Change log level of pmthreshold         from DEBUG to ERROR
Change log level of pmui                from DEBUG to ERROR
Change log level of portal.client       from DEBUG to ERROR
Change log level of portal.server       from DEBUG to ERROR
Change log level of root                from DEBUG to ERROR
Change log level of sbus                from DEBUG to ERROR
Change log level of sbus.client          from DEBUG to ERROR
Change log level of sbus.heartbeat      from DEBUG to ERROR
Change log level of sbus.server         from DEBUG to ERROR
Change log level of sm                  from DEBUG to ERROR
Change log level of snmp4j              from DEBUG to ERROR
Change log level of ssh.client          from DEBUG to ERROR
Change log level of ssh.med             from DEBUG to ERROR
Change log level of task                from DEBUG to ERROR
Change log level of telnet.client        from DEBUG to ERROR
Change log level of telnet.med          from DEBUG to ERROR
Change log level of topo_ds             from DEBUG to ERROR
Change log level of topo_sdk            from DEBUG to ERROR
Change log level of topo_ui             from DEBUG to ERROR
Change log level of topomgr             from DEBUG to ERROR
```

- 执行成功后，“bme”日志的日志级别被修改为“error”。输出的结果如下所示：

```
Change log level of bme           from DEBUG to ERROR
```

15.1.5 查看 eSight 启动状态

在此给出了查看 eSight 启动状态的命令参考。

可在如下操作系统中查看 eSight 启动状态：

- [Windows 操作系统](#)
- [Linux 操作系统](#)

Windows 操作系统

- 命令格式：**omscli.bat checkstate startup**
- 输入示例

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

```
cd /d eSight_ROOT\AppBase\bin\runtime.center\bin
```



说明
“eSight_ROOT” 为 eSight 的安装目录。

3. 执行如下命令查看 eSight 的启动状态。

```
omscli.bat checkstate startup
```

- 输出示例

执行成功后，输出结果如下所示：
System already loaded bundle.

Linux 操作系统

- 命令格式：omscli.sh checkstate startup
- 输入示例

1. 以 root 用户登录服务器。
2. 执行如下命令切换目录。

```
cd eSight_ROOT/AppBase/bin/runtime.center/bin
```

3. 执行如下命令查看 eSight 启动状态。

```
./omscli.sh checkstate startup
```

- 输出示例

执行成功后，输出结果如下所示：
System already loaded bundle.

15.1.6 查看 eSight 进程状态

在此给出了查看 eSight 进程状态的命令参考。

可在如下操作系统中查看 eSight 进程状态：

- [Windows 操作系统](#)
- [Linux 操作系统](#)

Windows 操作系统

- 命令格式：omscli.bat checkstate process
- 输入示例

1. 以 Administrator 用户登录服务器。
2. 执行如下命令切换目录。

```
cd /d eSight_ROOT\AppBase\bin\runtime.center\bin
```



说明
“eSight_ROOT” 为 eSight 的安装目录。

3. 执行如下命令查看 eSight 进程状态。

```
omscli.bat checkstate process
```

- 输出示例

执行成功后，输出结果如下所示：

System process already started.

Linux 操作系统

- 命令格式: **omscli.sh checkstate process**
- 输入示例
 1. 以 root 用户登录服务器。
 2. 执行如下命令切换目录。
cd eSight_ROOT/AppBase/bin/runtime.center/bin
 3. 执行如下命令查看 eSight 进程状态。
./omscli.sh checkstate process
- 输出示例
执行成功后，输出结果如下所示：
System process already started.

15.1.7 查看 SBus 服务信息

在此给出了查看 SBus（Service Bus）服务信息的命令参考。

可在如下操作系统中查看 SBus 服务信息：

- [Windows 操作系统](#)
- [Linux 操作系统](#)

Windows 操作系统

- 命令格式: **omscli.bat service <[all | ip | self]>**
- 输入示例
 1. 以 Administrator 用户登录服务器。
 2. 执行如下命令切换目录。
cd /d eSight_ROOT\AppBase\bin\runtime.center\bin
 说明
“eSight_ROOT” 为 eSight 的安装目录。
 3. 执行如下命令查看 SBus 服务信息。
 - 查看 eSight 使用 SBus 发布的所有服务信息。
omscli.bat service all
 - 查看某个远程环境使用 SBus 发布的所有服务信息。例如，查看本机 IP 地址为 “12.62.34.228” 的环境的所有服务信息。
omscli.bat service 12.62.34.228
 - 查看当前环境使用 SBus 发布的所有服务信息。
omscli.bat service self
- 输出示例
 - 执行成功后，eSight 使用 SBus 发布的所有服务信息如下所示：

No	Host	Type	Date	Interface
1	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audit.api.OperationDetailManager
2	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audit.api.OperationLogManager

3	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audit.api.SecurityLogManager
4	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audit.api.SystemLogManager
5	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:11	com.huawei.oms.app.dump.api.DumpConfigManager
6	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:44	com.huawei.oms.app.pm.StatusChangedOperation
7	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:42	com.huawei.oms.app.pm.TemplateManager
8	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:38	com.huawei.oms.app.pm.alarm.AlarmManager
9	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:46	com.huawei.oms.app.pm.momgr.PMMoreManager
11	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:51	com.huawei.oms.app.sm.api.as.SecurityManager
13	12.66.90.215:31902	JSON	2012-02-28 11:08:51	com.huawei.oms.app.sm.api.as.SecurityManager
14	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.api.OperationLogManager
15	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.api.SecurityLogManager
16	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.api.SystemLogManager
17	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:22	com.huawei.oms.eam.access.AccessManager
18	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:59	com.huawei.oms.eam.mim.MITManager
19	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:13	com.huawei.oms.email.api.emailserver.EmailServerManager
20	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.EventService
21	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.EventServiceExt
22	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:23	com.huawei.oms.fm.api.FaultManager
23	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.api.probe.ProbeCenter
24	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.customfault.CustomFaultManager
25	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.probe.dao.HandlerReaderDao
26	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:06	com.huawei.oms.fm.uiapi.InternalFaultManager
27	12.66.90.215:31902	JSON	2012-02-28 11:08:55	com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28	12.66.90.215:31902	JSON	2012-02-28 11:07:38	com.huawei.oms.homepage.ext.HomepageExtension
29	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license.api.as.LicenseControl
30	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license.api.as.LicenseManager
31	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:26	com.huawei.oms.log.mgmt.LogMgmtService
32	12.66.90.215:31902	JSON	2012-02-28 11:07:26	com.huawei.oms.log.mgmt.LogMgmtService
33	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:02	com.huawei.oms.med.Mediation
34	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:00	com.huawei.oms.momgr.eam.MOLifeCycleManager
35	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.momgr.eam.MOLifeCycleManager
36	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.momgr.pm.PMProbeCenter
37	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:30	com.huawei.oms.nbi.api.

ds.bus.INBIJsonEventService						
38	12.66.90.215:31902	JSON	2012-02-28	11:08:30	com.huawei.oms.nbi.api.	
ds.bus.INBIJsonEventService						
39	12.66.90.215:31903	HESSIAN	2012-02-28	11:09:22	com.huawei.oms.nem.more	
.server.MoreService						
40	12.66.90.215:31903	HESSIAN	2012-02-28	11:09:14	com.huawei.oms.net.ftp.	
server.FtpService						
41	12.66.90.215:31903	HESSIAN	2012-02-28	11:09:14	com.huawei.oms.net.ftp.	
server.FtpsService						
42	12.66.90.215:31903	HESSIAN	2012-02-28	11:09:15	com.huawei.oms.net.ftp.	
server.SftpService						
43	12.66.90.215:31903	HESSIAN	2012-02-28	11:08:45	com.huawei.oms.pm.DataC	
enter						
44	12.66.90.215:31903	HESSIAN	2012-02-28	11:08:43	com.huawei.oms.pm.monit	
oring.MonitoringManager						
45	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.ValidateService						
46	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.callback.CallbackService						
47	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.ext.SbusHeartbeatService						
48	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.ext.SbusInfoService						
49	12.66.90.215:31902	JSON	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.ext.SbusInfoService						
50	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:25	com.huawei.oms.sbus.api	
.sync.SyncService						
51	12.66.90.215:31903	HESSIAN	2012-02-28	11:08:51	com.huawei.oms.sm.as.ap	
i.Administration						
52	12.66.90.215:31903	HESSIAN	2012-02-28	11:07:26	com.huawei.oms.task.Tas	
kManager						
53	12.66.90.215:31903	HESSIAN	2012-02-28	11:09:06	com.huawei.oms.topo.map	
ping.MappingManager						
54	12.66.90.215:31903	HESSIAN	2012-02-28	11:08:56	com.huawei.oms.topo.top	
omgr.TopoManager						

- 执行成功后，本机 IP 地址为“12.62.34.228”的环境的所有服务信息如下所示：

No	Host	Type	Date	Interface
1	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi
t.api.OperationDetailManager				
2	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi
t.api.OperationLogManager				
3	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi
t.api.SecurityLogManager				
4	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi
t.api.SystemLogManager				
5	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:11	com.huawei.oms.app.dump
.api.DumpConfigManager				
6	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:44	com.huawei.oms.app.pm.S
tatusChangedOperation				
7	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:42	com.huawei.oms.app.pm.T
emplateManager				
8	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:38	com.huawei.oms.app.pm.a
larm.AlarmManager				
9	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.app.pm.m
omgr.InternalPMPProbeCenter				
10	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:46	com.huawei.oms.app.pm.m
omgr.PMMoreManager				
11	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.app.pm.m
onitoring.InternalMonitoringManager				
12	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:51	com.huawei.oms.app.sm.a
pi.as.SecurityManager				
13	12.62.34.228:31902	JSON	2012-02-28 11:08:51	com.huawei.oms.app.sm.a
pi.as.SecurityManager				
14	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as
.api.OperationLogManager				
15	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as
.api.SecurityLogManager				
16	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as

.api.SystemLogManager					
17 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:22	com.huawei.oms.eam.am.A		
ccessManager					
18 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:59	com.huawei.oms.eam.mim.		
MITManager					
19 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:13	com.huawei.oms.email.ap		
i.emailserver.EmailServerManager					
20 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.Ev		
entService					
21 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.Ev		
entServiceExt					
22 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:23	com.huawei.oms.fm.api.F		
aultManager					
23 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.api.p		
robe.ProbeCenter					
24 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.custo		
mfault.CustomFaultManager					
25 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.probe		
dao.HandlerReaderDao					
26 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:06	com.huawei.oms.fm.uiapi		
.InternalFaultManager					
27 12.62.34.228:31902	JSON	2012-02-28 11:08:55	com.huawei.oms.gapi.cor		
e.mopkg.ChangeInfoMgr					
28 12.62.34.228:31902	JSON	2012-02-28 11:07:38	com.huawei.oms.homepage		
.ext.HomepageExtension					
29 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license.		
as.api.LicenseControl					
30 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license.		
as.api.LicenseManager					
31 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:26	com.huawei.oms.log.mgmt		
.LogMgmtService					
32 12.62.34.228:31902	JSON	2012-02-28 11:07:26	com.huawei.oms.log.mgmt		
.LogMgmtService					
33 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:02	com.huawei.oms.med.Medi		
ation					
34 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:00	com.huawei.oms.momgr.ea		
m.MOLifeCycleManager					
35 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.momgr.ea		
m.MOLifeCycleManager					
36 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.momgr.pm		
.PMProbeCenter					
37 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:30	com.huawei.oms.nbi.api.		
ds.bus.INBIJsonEventService					
38 12.62.34.228:31902	JSON	2012-02-28 11:08:30	com.huawei.oms.nbi.api.		
ds.bus.INBIJsonEventService					
39 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:22	com.huawei.oms.nem.more		
.server.MoreService					
40 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:14	com.huawei.oms.net.ftp.		
server.FtpService					
41 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:14	com.huawei.oms.net.ftp.		
server.FtpsService					
42 12.62.34.228:31903	HESSIAN	2012-02-28 11:09:15	com.huawei.oms.net.ftp.		
server.SftpService					
43 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:45	com.huawei.oms.pm.DataC		
enter					
44 12.62.34.228:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.pm.monit		
oring.MonitoringManager					
45 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.ValidateService					
46 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.callback.CallbackService					
47 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.ext.SbusHeartbeatService					
48 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.ext.SbusInfoService					
49 12.62.34.228:31902	JSON	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.ext.SbusInfoService					
50 12.62.34.228:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api		
.sync.SyncService					

51	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:51	com.huawei.oms.sm.as.ap i.Administration
52	12.62.34.228:31903	HESSIAN	2012-02-28 11:07:26	com.huawei.oms.task.Tas kManager
53	12.62.34.228:31903	HESSIAN	2012-02-28 11:09:06	com.huawei.oms.topo.map ping.MappingManager
54	12.62.34.228:31903	HESSIAN	2012-02-28 11:08:56	com.huawei.oms.topo.top omgr.TopoManager

- 执行成功后，当前环境使用 SBus 发布的所有服务信息如下所示：

No	Host	Type	Date	Interface
1	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi t.api.OperationDetailManager
2	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi t.api.OperationLogManager
3	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi t.api.SecurityLogManager
4	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.app.audi t.api.SystemLogManager
5	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:11	com.huawei.oms.app.dump .api.DumpConfigManager
6	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:44	com.huawei.oms.app.pm.S tatusChangedOperation
7	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:42	com.huawei.oms.app.pm.T emplateManager
8	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:38	com.huawei.oms.app.pm.a larm.AlarmManager
9	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.app.pm.m omgr.InternalPMProbeCenter
10	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:46	com.huawei.oms.app.pm.m omgr.PMMoreManager
11	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.app.pm.m onitoring.InternalMonitoringManager
12	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:51	com.huawei.oms.app.sm.a pi.as.SecurityManager
13	12.66.90.215:31902	JSON	2012-02-28 11:08:51	com.huawei.oms.app.sm.a pi.as.SecurityManager
14	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as .api.OperationLogManager
15	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as .api.SecurityLogManager
16	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:04	com.huawei.oms.audit.as .api.SystemLogManager
17	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:22	com.huawei.oms.eam.am.A ccessManager
18	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:59	com.huawei.oms.eam.mim. MITManager
19	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:13	com.huawei.oms.email.ap i.emailserver.EmailServerManager
20	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.Ev entService
21	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.event.Ev entServiceExt
22	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:23	com.huawei.oms.fm.api.F aultManager
23	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.api.p robe.ProbeCenter
24	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.custo mFault.CustomFaultManager
25	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:20	com.huawei.oms.fm.probe dao.HandlerReaderDao
26	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:06	com.huawei.oms.fm.uiapi .InternalFaultManager
27	12.66.90.215:31902	JSON	2012-02-28 11:08:55	com.huawei.oms.gapi.cor e.mopkg.ChangeInfoMgr
28	12.66.90.215:31902	JSON	2012-02-28 11:07:38	com.huawei.oms.homepage .ext.HomepageExtension
29	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license. as.api.LicenseControl

30	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:29	com.huawei.oms.license.as.api.LicenseManager
31	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:26	com.huawei.oms.log.mgmt.LogMgmtService
32	12.66.90.215:31902	JSON	2012-02-28 11:07:26	com.huawei.oms.log.mgmt.LogMgmtService
33	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:02	com.huawei.oms.med.Mediation
34	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:00	com.huawei.oms.momgr.eam.MOLifeCycleManager
35	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.momgr.eam.MOLifeCycleManager
36	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:40	com.huawei.oms.momgr.pm.PMProbeCenter
37	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:30	com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38	12.66.90.215:31902	JSON	2012-02-28 11:08:30	com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:22	com.huawei.oms.nem.more.server.MoreService
40	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:14	com.huawei.oms.net.ftp.server.FtpService
41	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:14	com.huawei.oms.net.ftp.server.FtpsService
42	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:15	com.huawei.oms.net.ftp.server.SftpService
43	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:45	com.huawei.oms.pm.DataCenter
44	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:43	com.huawei.oms.pm.monitoring.MonitoringManager
45	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api.ValidateService
46	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api.callback.CallbackService
47	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api.ext.SbusInfoService
49	12.66.90.215:31902	JSON	2012-02-28 11:07:25	com.huawei.oms.sbus.api.ext.SbusInfoService
50	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:25	com.huawei.oms.sbus.api.sync.SyncService
51	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:51	com.huawei.oms.sm.as.api.Administration
52	12.66.90.215:31903	HESSIAN	2012-02-28 11:07:26	com.huawei.oms.task.TaskManager
53	12.66.90.215:31903	HESSIAN	2012-02-28 11:09:06	com.huawei.oms.topo.mapping.MappingManager
54	12.66.90.215:31903	HESSIAN	2012-02-28 11:08:56	com.huawei.oms.topo.topomgr.TopoManager

Linux 操作系统

- 命令格式: **omscli.sh service** <[*all* | *ip* | *self*]>

- 输入示例

1. 以 root 用户登录服务器。
2. 执行如下命令切换目录。

cd eSight_ROOT/AppBase/bin/runtime.center/bin

3. 执行如下命令查看 SBus 服务信息。

- 查看 eSight 使用 SBus 发布的所有服务信息。

./omscli.sh service all

- 查看某个远程环境使用 SBus 发布的所有服务信息。例如，查看 IP 地址为“12.62.34.228”的环境的所有服务信息。

```
./omscli.sh service 12.62.34.228
```

- 查看当前环境使用 SBus 发布的所有服务信息。

```
./omscli.sh service self
```

- 输出示例

- 执行成功后，eSight 使用 SBus 发布的所有服务信息如下所示：

```
o Host                                Type      Date
Interface

1  12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager
2  12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager

3  12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SecurityLogManager
4  12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager
5  12.67.176.108:31903  HESSIAN  2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager
6  12.67.176.108:31903  HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation
7  12.67.176.108:31903  HESSIAN  2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager
8  12.67.176.108:31903  HESSIAN  2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager
9  12.67.176.108:31903  HESSIAN  2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager
11 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
13 12.67.176.108:31902  JSON     2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
14 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager
15 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager
16 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SystemLogManager
17 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager
18 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager
19 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager
20 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventService
21 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt
22 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26 12.67.176.108:31903  HESSIAN  2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27 12.67.176.108:31902  JSON     2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28 12.67.176.108:31902  JSON     2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
29 12.67.176.108:31903  HESSIAN  2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
```

```
30 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32 12.67.176.108:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38 12.67.176.108:31902 JSON 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.pm.DataCenter
44 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49 12.67.176.108:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
51 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager
```

- 执行成功后，IP 地址为“12.62.34.228”的环境的所有服务信息如下所示：

No	Host	Type	Date
Interface			
1	12.62.34.228:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager			
2	12.62.34.228:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager			
3	12.62.34.228:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SecurityLogManager			
4	12.62.34.228:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager			
5	12.62.34.228:31903	HESSIAN	2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager			
6	12.62.34.228:31903	HESSIAN	2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation			
7	12.62.34.228:31903	HESSIAN	2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager			
8	12.62.34.228:31903	HESSIAN	2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager			

```

9 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter
10 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager
11 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager
12 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
13 12.62.34.228:31902 JSON 2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager
14 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager
15 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager
16 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SystemLogManager
17 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager
18 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager
19 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager
20 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.event.EventService
21 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt
22 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27 12.62.34.228:31902 JSON 2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28 12.62.34.228:31902 JSON 2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
29 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
30 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32 12.62.34.228:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38 12.62.34.228:31902 JSON 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:17

```

```
com.huawei.oms.pm.DataCenter
44 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49 12.62.34.228:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
51 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52 12.62.34.228:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54 12.62.34.228:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager
```

- 执行成功后，当前环境使用 SBus 发布的所有服务信息如下所示：

No	Host	Type	Date
Interface			
1	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationDetailManager			
2	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.OperationLogManager			
3	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SecurityLogManager			
4	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.app.audit.api.SystemLogManager			
5	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:02
com.huawei.oms.app.dump.api.DumpConfigManager			
6	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:16
com.huawei.oms.app.pm.StatusChangedOperation			
7	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:15
com.huawei.oms.app.pm.TemplateManager			
8	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:13
com.huawei.oms.app.pm.alarm.AlarmManager			
9	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:14
com.huawei.oms.app.pm.momgr.InternalPMProbeCenter			
10	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:17
com.huawei.oms.app.pm.momgr.PMMoreManager			
11	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:16
com.huawei.oms.app.pm.monitoring.InternalMonitoringManager			
12	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager			
13	12.67.176.108:31902	JSON	2012-02-28 11:06:58
com.huawei.oms.app.sm.api.as.SecurityManager			
14	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.audit.as.api.OperationLogManager			
15	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SecurityLogManager			
16	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:56
com.huawei.oms.audit.as.api.SystemLogManager			
17	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:17
com.huawei.oms.eam.am.AccessManager			
18	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:06
com.huawei.oms.eam.mim.MITManager			
19	12.67.176.108:31903	HESSIAN	2012-02-28 11:07:10
com.huawei.oms.email.api.emailserver.EmailServerManager			
20	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:32
com.huawei.oms.event.EventService			
21	12.67.176.108:31903	HESSIAN	2012-02-28 11:06:32
com.huawei.oms.event.EventServiceExt			

```

22 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:18
com.huawei.oms.fm.api.FaultManager
23 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.api.probe.ProbeCenter
24 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.customfault.CustomFaultManager
25 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:07
com.huawei.oms.fm.probedao.HandlerReaderDao
26 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:10
com.huawei.oms.fm.uiapi.InternalFaultManager
27 12.67.176.108:31902 JSON 2012-02-28 11:07:05
com.huawei.oms.gapi.core.mopkg.ChangeInfoMgr
28 12.67.176.108:31902 JSON 2012-02-28 11:06:39
com.huawei.oms.homepage.ext.HomepageExtension
29 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseControl
30 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.license.as.api.LicenseManager
31 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
32 12.67.176.108:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.log.mgmt.LogMgmtService
33 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.med.Mediation
34 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:04
com.huawei.oms.momgr.eam.MOLifeCycleManager
35 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.momgr.eam.MOLifeCycleManager
36 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:14
com.huawei.oms.momgr.pm.PMProbeCenter
37 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
38 12.67.176.108:31902 JSON 2012-02-28 11:06:59
com.huawei.oms.nbi.api.ds.bus.INBIJsonEventService
39 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.nem.more.server.MoreService
40 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpService
41 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.FtpsService
42 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:55
com.huawei.oms.net.ftp.server.SftpService
43 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:17
com.huawei.oms.pm.DataCenter
44 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:16
com.huawei.oms.pm.monitoring.MonitoringManager
45 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ValidateService
46 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.callback.CallbackService
47 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusHeartbeatService
48 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
49 12.67.176.108:31902 JSON 2012-02-28 11:06:32
com.huawei.oms.sbus.api.ext.SbusInfoService
50 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.sbus.api.sync.SyncService
51 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:58
com.huawei.oms.sm.as.api.Administration
52 12.67.176.108:31903 HESSIAN 2012-02-28 11:06:32
com.huawei.oms.task.TaskManager
53 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.mapping.MappingManager
54 12.67.176.108:31903 HESSIAN 2012-02-28 11:07:11
com.huawei.oms.topo.topomgr.TopoManager

```

15.2 Oracle 命令参考

介绍常见的 Oracle 数据库命令的使用参考，包括各命令的功能说明和应用实例。

更多的命令参考，请参考 Oracle 命令参考手册。

15.2.1 sqlplus 命令

命令 **sqlplus** 可以用于访问 Oracle 数据库。

命令功能

命令 **sqlplus** 可以用于连接 Oracle 数据库，然后可在 **sql** 命令行中执行 sql 语句或对 Oracle 数据库进行配置。

命令格式

sqlplus 参数

参数说明

sqlplus 命令的参数说明如表 15-1 所示。

表 15-1 参数说明

参数	说明
/ as sysdba	“/ as sysdba”表示以 sysdba 角色连接 Oracle 数据库。sysdba 角色包含启动和停止 Oracle 数据库的权限，此连接方式只能使用 Oracle 用户执行。
dbuser/ password	“dbuser/password”表示以数据库用户连接 Oracle 数据库，其中 password 是数据库用户的密码。此方式下可执行的操作由数据库用户的权限决定。

说明

此处只对访问 Oracle 数据库的参数进行说明，包括 “/ as sysdba” 和 “dbuser/password” 两种形式。更多参数的使用方法请参见 Oracle 公司提供的相关文档。

使用实例

本例中假设以 root 用户登录 SUSE Linux 操作系统，Oracle 数据库的操作系统用户名为 “oracle”。

在命令行中执行如下命令连接 Oracle 数据库：

- 方法一：执行如下命令切换为 oracle 用户。

su - oracle

执行如下命令以 sysdba 角色连接 Oracle 数据库。

sqlplus / as sysdba



说明

若远程登录，则需要提供帐号和密码。假设用 system 用户连接 Oracle 数据库，密码为 testpwd。

sqlplus system/testpwd as sysdba

屏幕显示如下信息，表示已正常连接到 Oracle 数据库。否则请根据提示信息排查出错原因。

SQL>

- 方法二：执行如下命令切换为 oracle 用户。

su - oracle

执行如下命令以 system 角连接 Oracle 数据库，假设 system 用户的密码为 testpwd。

sqlplus system/testpwd

屏幕显示如下信息，表示已正常连接到 Oracle 数据库。否则请根据提示信息排查出错原因。

SQL>

15.2.2 startup 命令

命令 startup 可以用于启动 Oracle 数据库。

命令功能

命令 startup 可以用于在 sql 命令行中启动 Oracle 数据库。

命令格式

startup 参数

参数说明

startup 命令的参数说明如表 15-2 所示。

表 15-2 参数说明

参数	说明
空	正常启动。执行 startup 后，将依次执行启动实例、装载数据库和打开数据库的操作。
force	强制重启数据库。当不能关闭数据库时，可以用 startup force 来完成数据库的关闭并正常启动。
nomount	仅启动实例。
mount	启动实例后装载数据库。

使用实例

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 oracle）。

在命令行中执行如下命令连接 Oracle 数据库。

sqlplus / as sysdba

 说明

- 若远程登录，则需要提供帐号和密码。假设用 system 用户连接 Oracle 数据库，密码为 testpwd。
\$ **sqlplus system/testpwd as sysdba**
- **sqlplus** 命令的使用方法请参见 [15.2.1 sqlplus 命令](#)。

使用 **startup** 命令启动 Oracle 数据库。

startup

输出结果如下所示：

```
ORACLE instance started.  
Total System Global Area 1610612736 bytes  
Fixed Size 2046264 bytes  
Variable Size 385877704 bytes  
Database Buffers 1207959552 bytes  
Redo Buffers 14729216 bytes  
Database mounted.  
Database opened.
```

其中 ORACLE instance started，Database mounted 和 Database opened 表明 Oracle 数据库已正常启动。

15.2.3 shutdown 命令

命令 shutdown 可以用于关闭 Oracle 数据库。

命令功能

命令 shutdown 用于在 sql 命令行中关闭 Oracle 数据库。

命令格式

shutdown 参数

参数说明

shutdown 命令的参数说明如[表 15-3](#)所示。

表 15-3 参数说明

参数	说明
normal	等待所有用户断开连接时，关闭数据库、卸载数据库和关闭实例。
immediate（推荐使用）	回滚所有用户事务，关闭数据库、卸载数据库和关闭实例。
transactional	当所有用户事务结束时，关闭数据库、卸载数据库和关闭实例。

参数	说明
abort	立即终止实例。对用户未提交事务，下次启动数据时恢复。 说明 在无法正常关闭的情况才使用 abort 参数，可能导致数据丢失。

使用实例

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 oracle）。
在命令行中执行如下命令连接 Oracle 数据库。

sqlplus / as sysdba

 说明

- 若远程登录，则需要提供帐号和密码。假设用 system 用户连接 Oracle 数据库，密码为 testpwd。
\$ **sqlplus system/testpwd as sysdba**
- **sqlplus** 命令的使用方法请参见 [15.2.1 sqlplus 命令](#)。

使用 **shutdown** 命令关闭 Oracle 数据库。

shutdown immediate

输出结果如下所示：

```
Database closed.  
Database dismounted.  
ORACLE instance shut down.
```

其中 Database closed，Database dismounted，ORACLE instance shut down 分别表示关闭 Oracle 数据库成功、卸载数据库成功和关闭数实例成功。

15.2.4 show 命令

命令 show 可以用于查看 Oracle 数据库的运行参数。

命令功能

命令 show 用于在 sql 命令行中查看 Oracle 数据库的运行参数。

命令格式

show parameter 参数

参数说明

show 命令的参数说明如[表 15-4](#) 所示。

表 15-4 参数说明

参数	说明
空	列出 Oracle 数据库所有的运行参数。内容为 NAME（参数名称）、TYPE（参数类型）和 VALUE（参数值）。
参数	显示指定“参数”的参数值。

使用实例一

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 oracle）。

查看所有的 Oracle 数据库的运行参数。

在命令行中执行如下命令连接 Oracle 数据库。

sqlplus / as sysdba

 说明

- 若远程登录，则需要提供帐号和密码。假设用 system 用户连接 Oracle 数据库，密码为 testpwd。
\$ **sqlplus system/testpwd as sysdba**
- **sqlplus** 命令的使用方法请参见 [15.2.1 sqlplus 命令](#)。

使用 **show** 命令查看 Oracle 数据库的运行参数：

show parameter

下面列出显示信息的部分内容。

```
NAME TYPE VALUE
-----
undo_management string AUTO
undo_retention integer 900
undo_tablespace string UNDOTBS1
use_indirect_data_buffers boolean FALSE
user_dump_dest string /opt/oracle/oradb/home/admin/i
mapdb/udump
utl_file_dir string
workarea_size_policy string AUTO
```

使用实例二

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 oracle）。

查看指定参数 processes 的参数值。

在命令行中执行如下命令连接 Oracle 数据库。

sqlplus / as sysdba

使用 **show** 命令查看 Oracle 数据库的运行参数：

show parameter process

屏幕显示所有包含“processes”字符的参数信息。

```
NAME TYPE VALUE
-----
```

```
aq_tm_processes integer 0
db_writer_processes integer 1
gcs_server_processes integer 0
job_queue_processes integer 10
log_archive_max_processes integer 2
processes integer 150
```

15.2.5 alter 命令

命令 alter 可以用于修改 Oracle 数据库的运行参数。

命令功能

命令 alter 用于在 sql 命令行中修改 Oracle 数据库的运行参数。

命令格式

```
alter 选项 1 参数 1 选项 2 参数 2……
```

参数说明

alter 命令的参数说明如表 15-5 所示。

表 15-5 参数说明

参数	说明
user	对 Oracle 数据库用户进行设置（例如设置用户的密码）。 说明 在本节示例中只介绍如何修改 Oracle 用户的密码，更多参数设置请参见 Oracle 公司提供的相关文档。
system set	对 Oracle 数据库的系统参数进行设置。 说明 在本节示例中只介绍如何修改 Oracle 数据库系统参数的方法，具体参数的取值请根据实际应用选取。本节提供的示例仅供参考，更多参数设置方法请参见 Oracle 公司提供的相关文档。

使用实例一

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 oracle）。

在命令行中执行如下命令连接 Oracle 数据库：

```
sqlplus / as sysdba
```

 说明

- 若远程登录，则需要提供帐号和密码。假设用 system 用户连接 Oracle 数据库，密码为 testpwd。
\$ sqlplus system/testpwd as sysdba
- sqlplus 命令的使用方法请参见 15.2.1 sqlplus 命令。

执行如下命令修改数据库用户 system 的密码：

```
alter user system identified by "testpwd"
```

其中 `system` 是要修改的数据库用户名称，`testpwd` 是自定义的 `system` 用户的密码。
屏幕显示 `User altered` 表示修改成功，否则请根据提示信息排查出错原因。

使用实例二

假设当前登录 SUSE Linux 的用户为管理 Oracle 数据库的用户（名称为 `oracle`）。

初始化运行参数 `processes`：设置能同时链接 Oracle 数据库实例的进程数为 1024。

在命令行中执行如下命令连接 Oracle 数据库：

```
sqlplus / as sysdba
```

执行如下命令修改 Oracle 数据库的运行参数。

```
alter system set processes=1024 scope=spfile
```

其中 `processes` 是要修改的运行参数名称，`scope=spfile` 表示 `processes` 是数据库初始化参数。可参见 [15.2.4 show 命令](#) 查看 `processes` 的当前参数值。

屏幕显示 `System altered` 表示修改成功，否则请根据提示信息排查出错原因。

16 FAQ

关于本章

介绍常见问题和参考信息，让您在问题出现时能采取合适的应对处理策略。

[16.1 如何解决通过 IE8 操作 eSight 时系统提示未选中告警声音复选框的问题](#)

[16.2 如何解决登录 eSight 时发生安全证书错误的问题](#)

[16.3 如何解决登录 eSight 时发生的安全警告问题](#)

[16.4 如何解决使用中文版本的 Firefox 浏览器访问 eSight 英文界面时，个别英文字段无法完全显示的问题](#)

[16.5 如何解决在 IE 浏览器中安装 eSight 提供的 Adobe Flash Player 时安装失败问题](#)

[16.6 如何解决使用 Firefox 浏览器访问 eSight 的 Flash 页面时，提示 Flash 插件已崩溃问题](#)

[16.7 如何解决复制某些阿拉伯字符显示为乱码的问题](#)

[16.8 如何根据网管所需端口情况，自定义端口连接规则](#)

[16.9 如何解决因数据库异常停止使网元出现垃圾数据而导致网管无法管理该网元的问题](#)

[16.10 如何解决 eSight 界面无法正常显示，注销时出现整页程序代码的问题](#)

[16.11 如何配置服务器 SNMP 参数](#)

[16.12 如何解决因修改 eSight 服务器系统时间对 eSight 产生的影响](#)

16.1 如何解决通过 IE8 操作 eSight 时系统提示未选中告警声音复选框的问题

现象描述

通过 IE8 浏览器操作 eSight 时，对复选框进行操作，系统提示没有选中任何记录。

图 16-1 系统错误提示



可能原因

该问题是用户使用的 IE8 浏览器的兼容性视图导致，需要去除兼容性视图设置。

处理步骤

- 步骤 1** 打开 IE8 浏览器。
- 步骤 2** 在主菜单中选择“工具 > 开发人员工具”，打开“开发人员工具”界面。
- 步骤 3** 在“开发人员工具”界面中，设置“浏览器模式”为 IE8，同时设置“文本模式”为 IE8 标准。
- 步骤 4** 关闭“开发人员工具”界面，重新登录 esight。

----结束

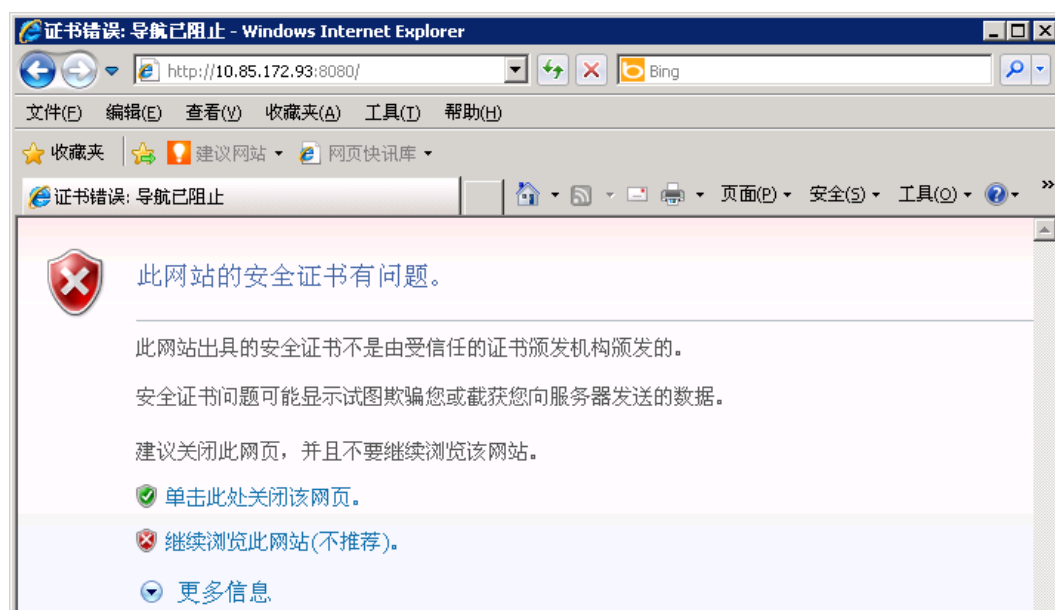
16.2 如何解决登录 eSight 时发生安全证书错误的问题

现象描述

登录 eSight 时，Web 浏览器提示安全证书错误。

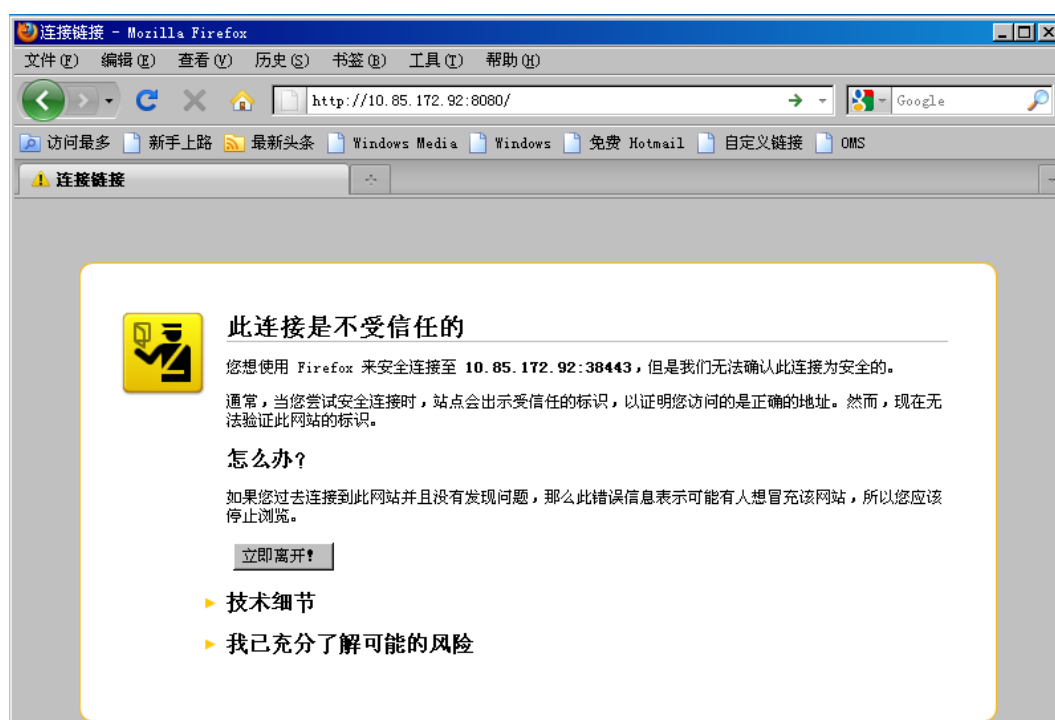
- IE 浏览器提示安全证书错误。

图 16-2 安全证书错误提示(IE)



- Firefox 浏览器提示安全证书错误。

图 16-3 安全证书错误提示 (Firefox)



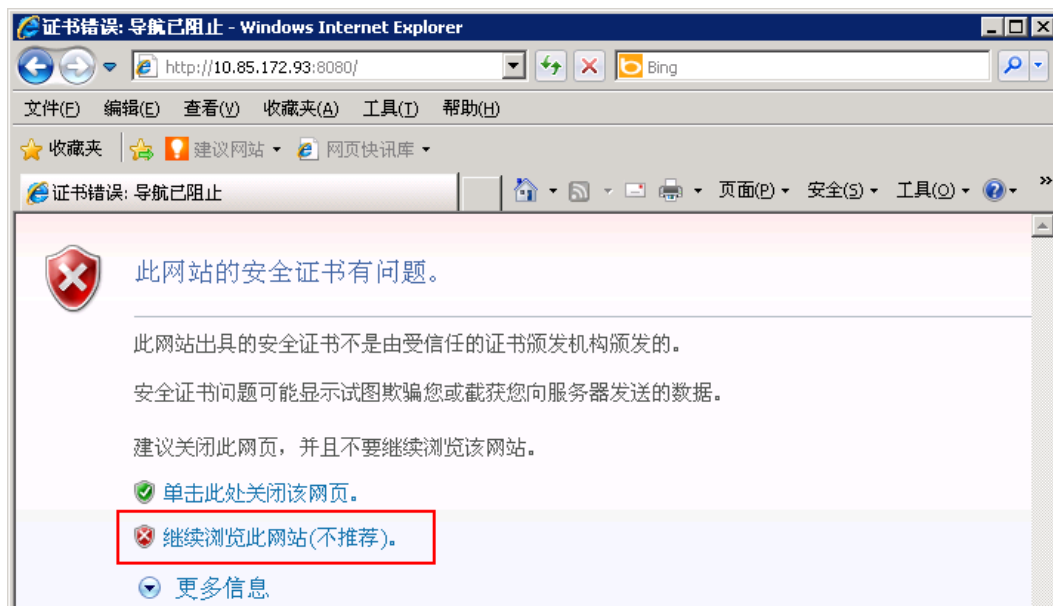
可能原因

安全证书错误, 需要安装相应的安全证书。

处理步骤

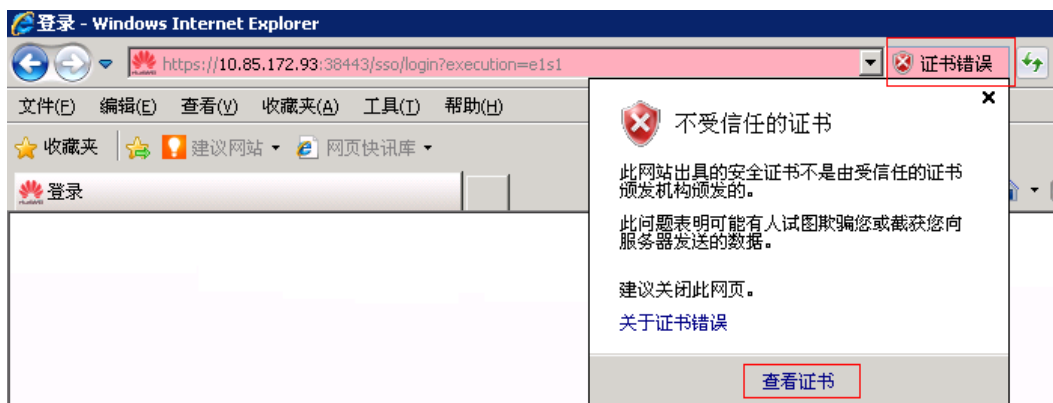
- 在 IE 浏览器中安装安全证书
 1. 在安全证书错误提示页面中，单击“继续浏览此网站（不推荐）”。

图 16-4 证书错误提示



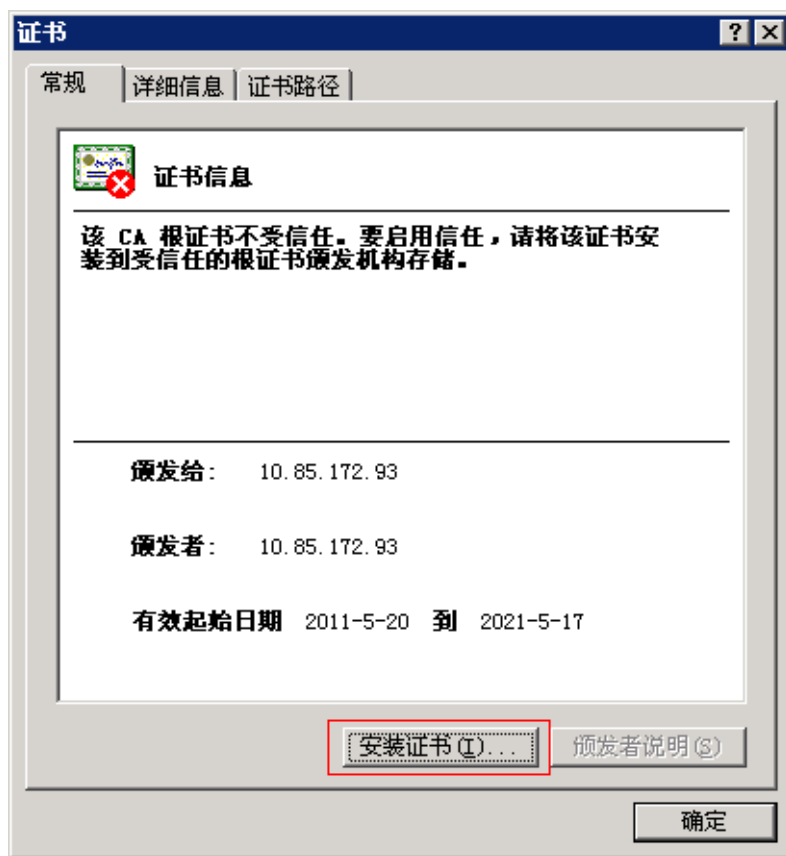
2. 单击“证书错误”，在“不受信任的证书”提示框中，单击“查看证书”。

图 16-5 不受信任的证书



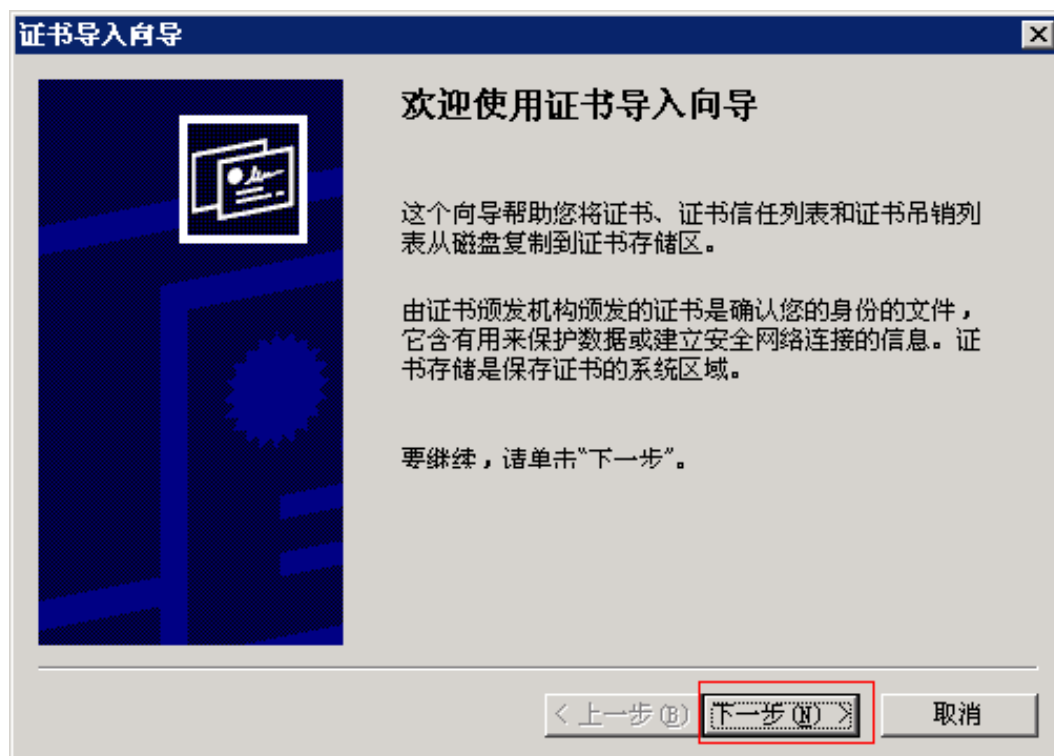
3. 在“常规”页签中，单击“安装证书”。

图 16-6 证书信息



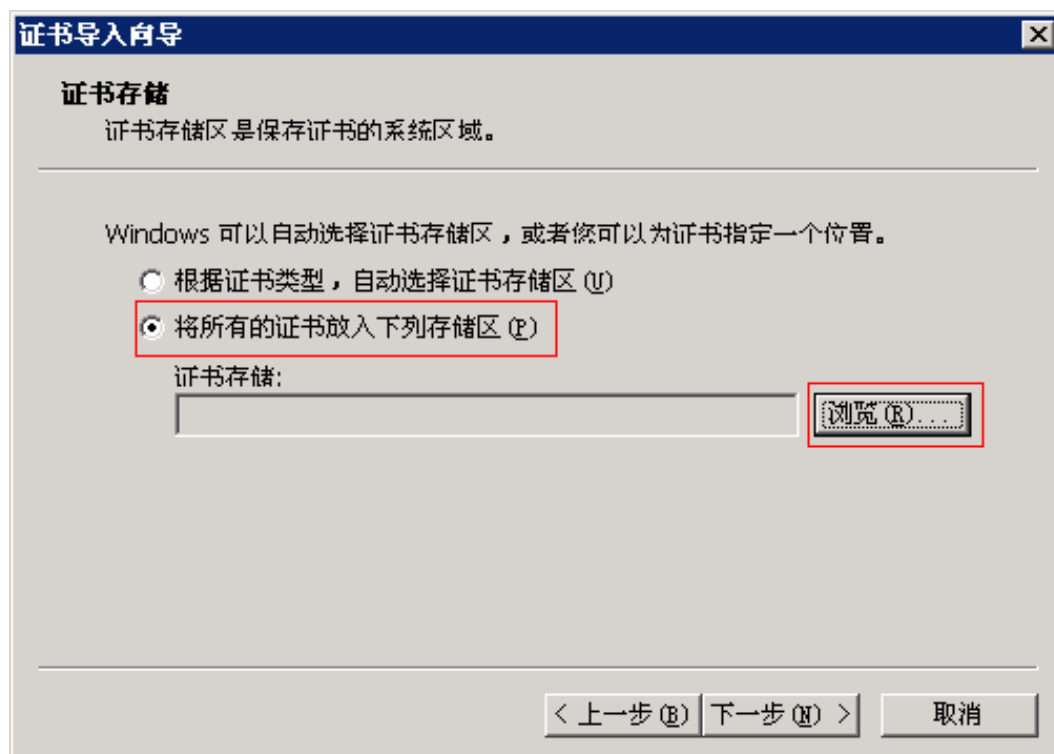
4. 在“证书导入向导”对话框中，单击“下一步”。

图 16-7 证书导入向导



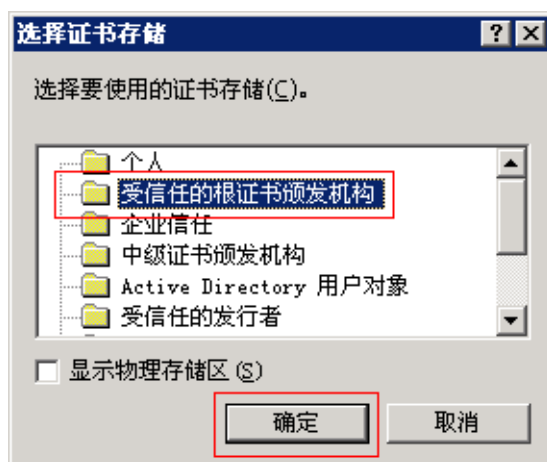
5. 选中“将所有的证书放入下列存储区 (P)”单选按钮，单击“浏览”。

图 16-8 导入证书



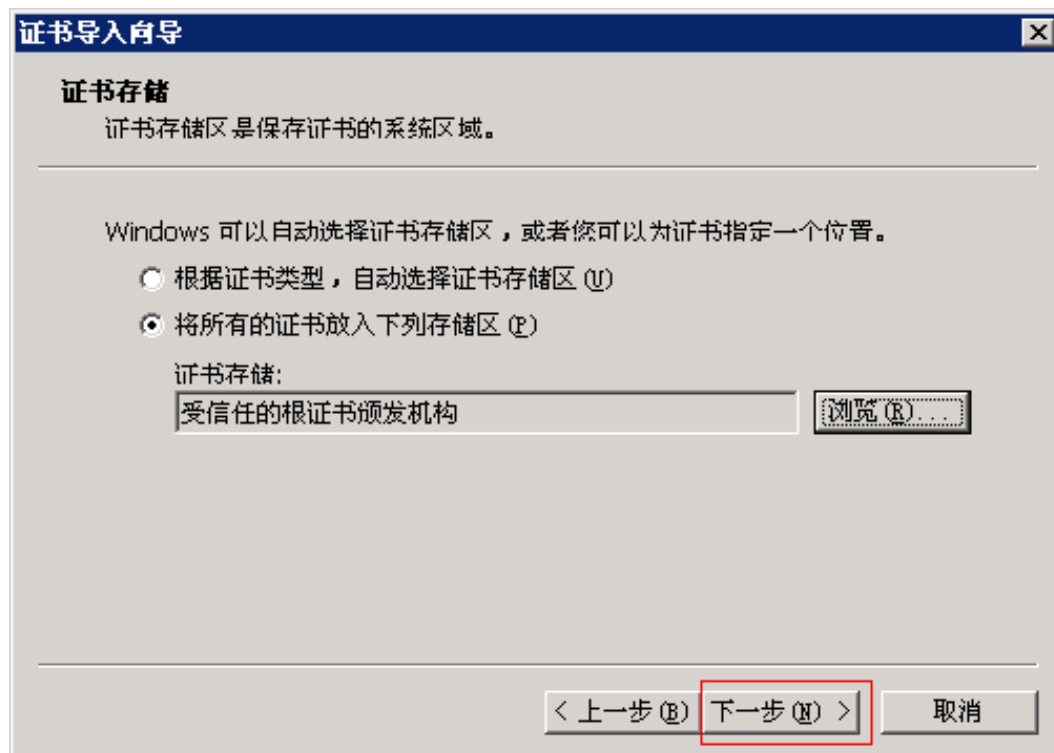
6. 在“选择证书存储”对话框中，选择“受信任的根证书颁发机构”，单击“确定”。

图 16-9 选择证书存储



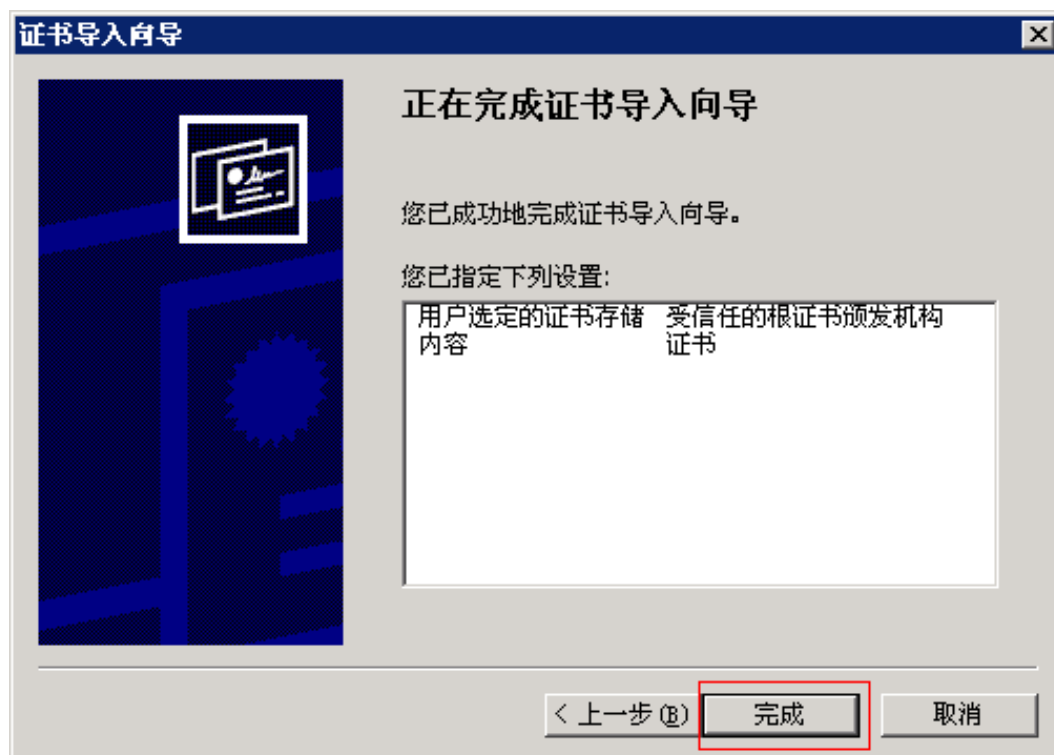
7. 单击“下一步”。

图 16-10 证书存储



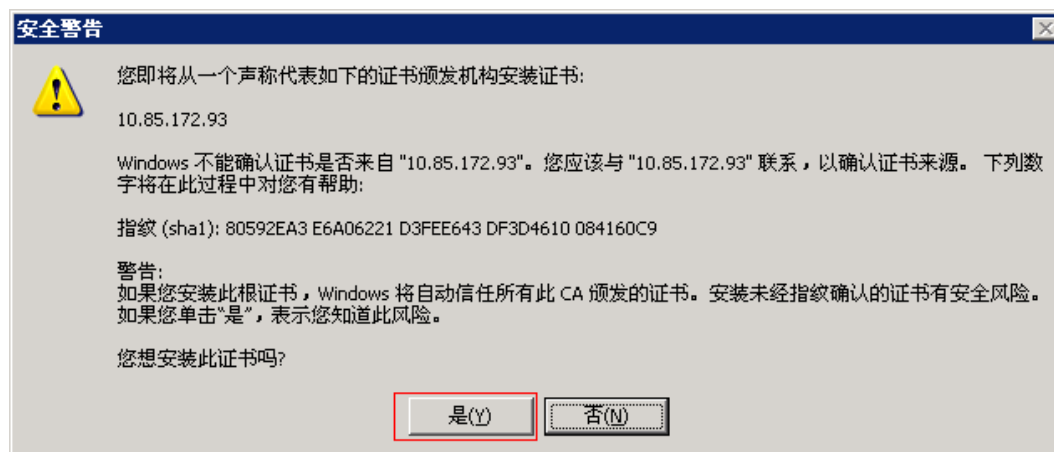
8. 在“证书导入向导”对话框中，单击“完成”。

图 16-11 完成证书导入向导



9. 在“安全警告”对话框中，单击“是”。

图 16-12 安装证书



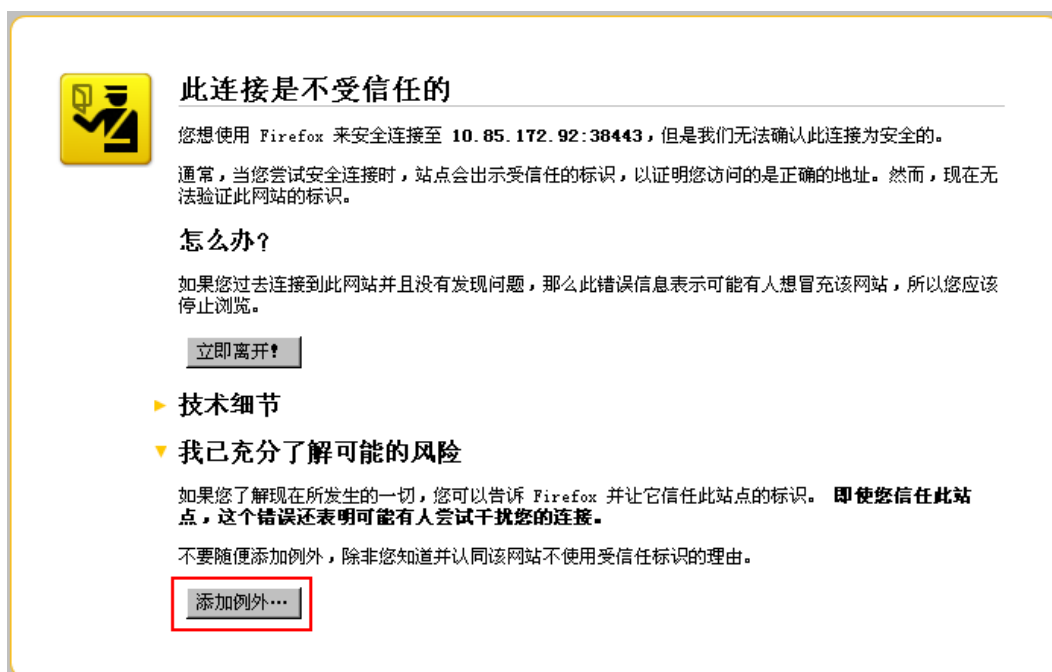
10. 在“证书导入向导”提示框中，单击“确定”。

图 16-13 证书导入成功



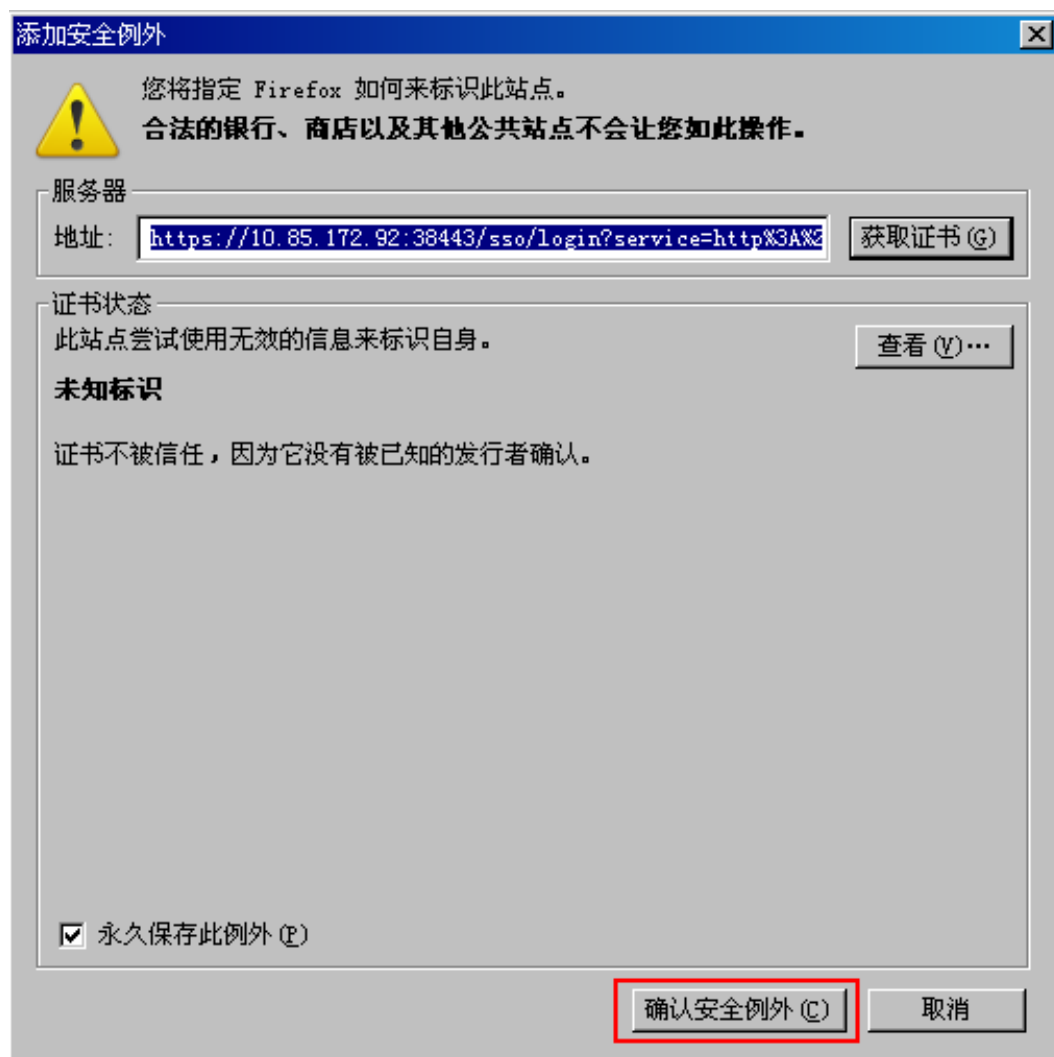
11. 关闭 IE 浏览器，然后重新打开 IE 浏览器，登录 eSight。
- 在 Mozilla Firefox 中安装安全证书
 1. 在安全证书错误提示页面中，展开“我已充分了解可能的风险”，单击“添加例外”。

图 16-14 添加例外



2. 在“添加安全例外”对话框中，单击“确认安全例外”。

图 16-15 确认安全例外



3. 关闭 Firefox 浏览器，然后重新打开 Firefox 浏览器，登录 eSight。

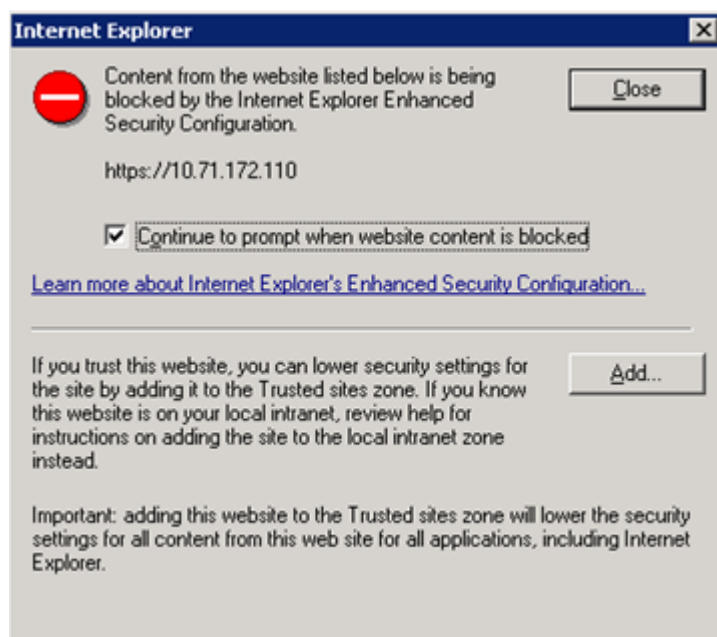
---结束

16.3 如何解决登录 eSight 时发生的安全警告问题

现象描述

登录 eSight 时，Web 浏览器提示安全警告。

图 16-16 Security Alert



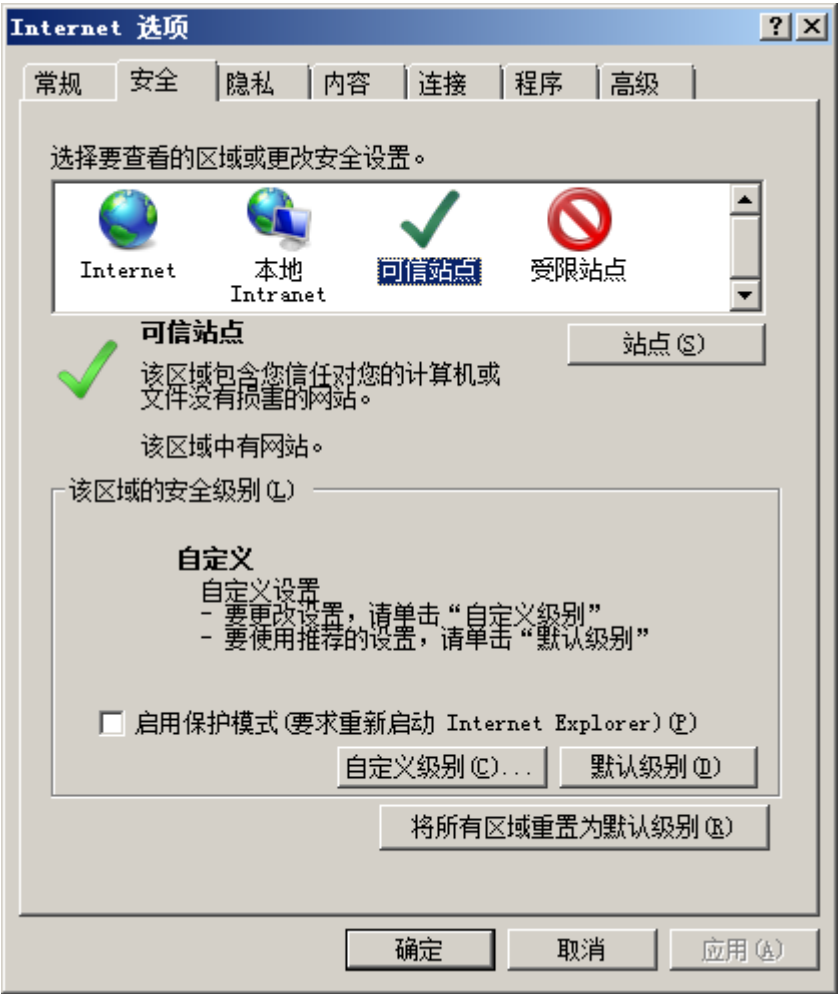
可能原因

浏览器的安全级别过高，可以通过添加 eSight 的网址为信任网站或者设置浏览器的安全级别解决该问题。

处理步骤

- 方法一：添加信任网站
 1. 在如图 16-16 所示的提示框中单击“Add”。
 2. 在“安全”页签下选择“可信站点”图标，单击“站点”。

图 16-17 Internet 选项

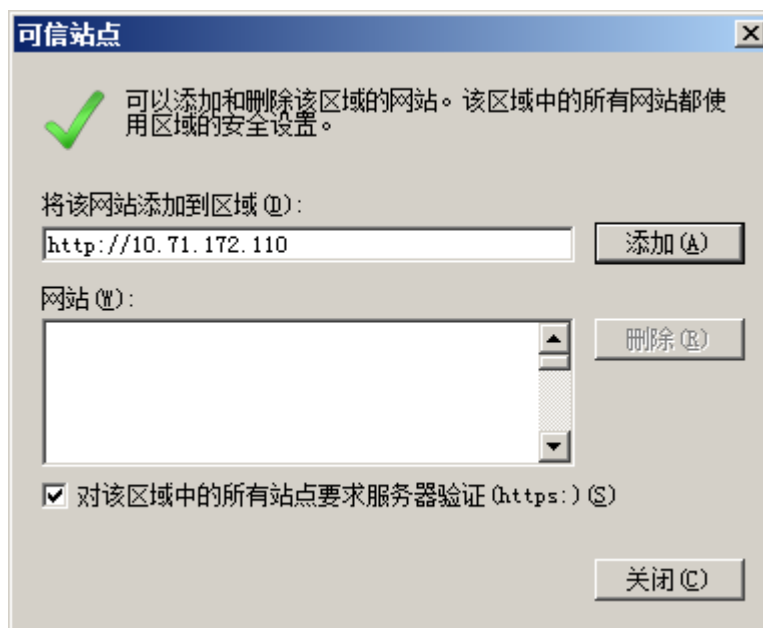


3. 在“将该网站添加到区域”文本框中输入访问 eSight 的网址，单击“添加”，将其添加为可信站点。

说明

通过 http 协议和 https 协议访问 eSight 的网址都需添加为可信站点。

图 16-18 可信站点



4. 单击“关闭”。
- 方法二：设置安全级别
 1. 选择浏览器菜单栏中的“工具 > Internet 选项”。
 2. 在“Internet 选项”窗口中选择“安全”页签，单击“自定义级别”。

图 16-19 Internet 选项



3. 在“安全设置-受信任的站点区域”窗口中选中“提交非加密表单数据”下的“启用”和“活动脚本”下的“启用”，单击“确定”。

图 16-20 安全设置-受信任的站点区域

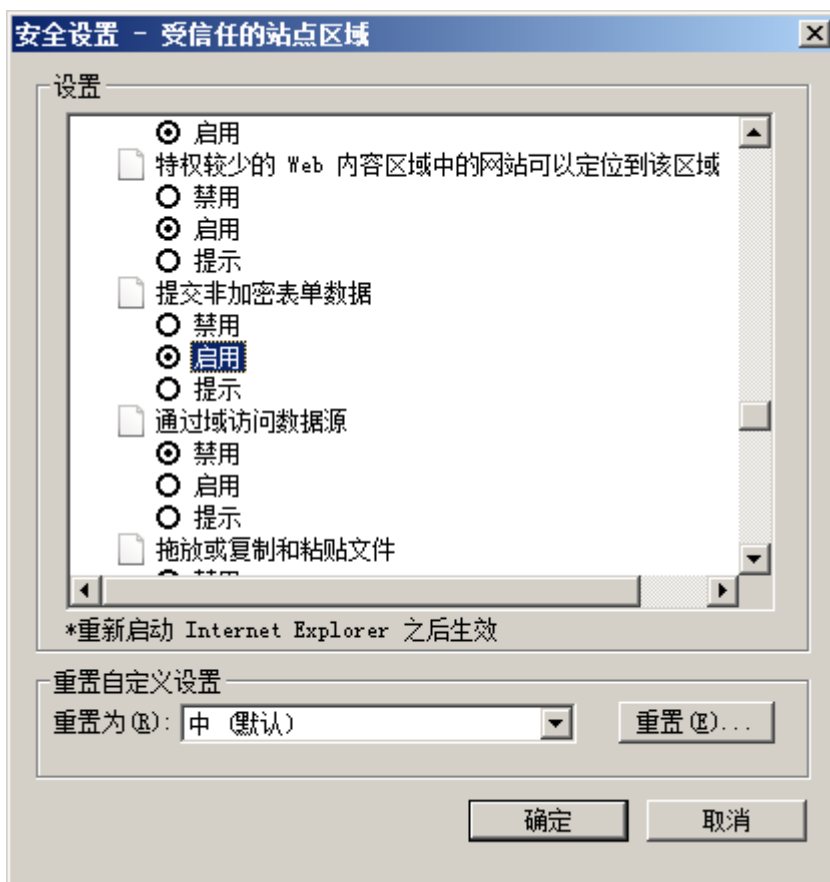


图 16-21 字段无法完全显示

Security Management > Rights Assignment > User > **Create User** Help ?

Basic Info Roles Access Control Polici...

* User name:

* Password:

* Confirm password:

Account status: ☒ Enabled ☐ Disabled

Description:

The password must meet the following rules:

- 1, The password is different from the user name.
- 2, The length ranges from 6 to 32 characters.
- 3, The number of occurrences of a character in a password cannot exceed 3.
- 4, The password contains uppercase and lowercase letters and digits.

- 场景二：在创建角色的英文界面中，出现如图 16-22 所示字段无法完全显示的问题。

图 16-22 字段无法完全显示

Security Management > Rights Assignment > Role > Create Role Help ?

Basic InfoSelect Managed Obj...Select OperationsSummary

* Role name:

Description:

Select users:

User name:

Search

	User Name	Description
☐	admin	超级管理员
☐	Test05	

Total records: 2

Selected Users:

User Name	Operation
No record.	

Next

Cancel

可能原因

中文版本的 Firefox 浏览器设置的默认字体不正确，导致访问 eSight 英文页面时，个别较长英文字段无法完全显示。

定位思路

更改中文版本的 Firefox 浏览器的默认字体后，再查看 eSight 英文界面中的英文字段显示效果时，发现个别较长英文字段可以完全显示。

处理步骤

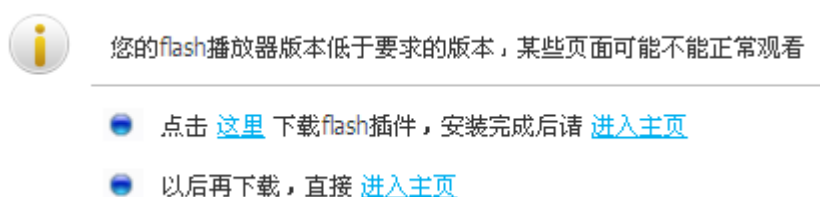
- 步骤 1 在中文版本的 Firefox 浏览器菜单栏中，选择“Tools > Options”。
- 步骤 2 在“Options”对话框中，单击“Content”页签。
- 步骤 3 在“Fonts & colors”区域框的“Default Font”下拉框中，选择“Arial”。
- 步骤 4 单击“OK”。
- 设置完成后，请重新进入界面查看显示效果。
- 结束

16.5 如何解决在 IE 浏览器中安装 eSight 提供的 Adobe Flash Player 时安装失败问题

现象描述

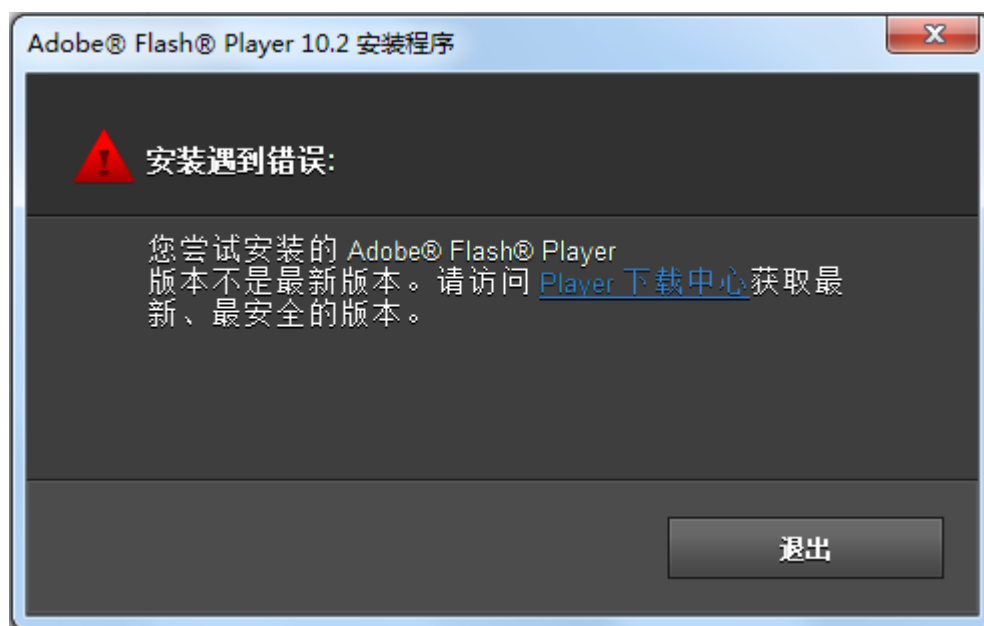
使用 IE 浏览器访问 eSight 时，正常登录后遇到如图 16-23 所示的提示。

图 16-23 flash 播放器版本低的提示



按照提示步骤下载安装了 eSight 提供的适用于 IE 浏览器的 Adobe Flash Player 后，遇到如图 16-24 所示的错误提示，安装失败。

图 16-24 错误提示



可能原因

因 eSight 提供的适用于 IE 浏览器的 Adobe Flash Player 版本低于客户端机注册表中有过安装记录的 Adobe Flash Player 版本，导致安装失败。

定位思路

卸载了原有的 Adobe Flash Player 程序之后，预备分别安装不同高低版本的 Adobe Flash Player 程序。

- 安装高于客户端机原有 Adobe Flash Player 版本的程序时，无错误提示，安装顺利完成。
- 安装低于客户端机原有 Adobe Flash Player 版本的程序时，出现相同的错误提示，安装失败。

处理步骤

- 步骤 1** 在错误提示框中，单击“Player 下载中心”。
- 访问 Adobe Flash Player 下载中心获取最新版本的 Adobe Flash Player 程序。
- 步骤 2** 安装最新版本的 Adobe Flash Player 程序，以便正常使用 eSight。
- 结束

16.6 如何解决使用 Firefox 浏览器访问 eSight 的 Flash 页面时，提示 Flash 插件已崩溃问题

现象描述

使用 Firefox 浏览器访问 eSight 的 Flash 页面，如首页告警柱状图、拓扑页面、性能监控页面等，出现如图 16-25 所示的提示。

图 16-25 Flash 插件已崩溃



可能原因

- Flash 插件运行过程中，与 Firefox 浏览器之间读写内存出现冲突。为保证浏览器正常运行，浏览器自动终止插件管理进程，从而导致 Flash 插件崩溃。
- Firefox 浏览器运行时所在的操作系统的内存与 CPU 不足，Firefox 自动终止插件管理进程，从而导致 Flash 插件崩溃。

处理步骤

- 步骤 1** 单击提示信息中“重新加载页面”的链接。
- 页面自动刷新，跳转回 eSight 首页，Flash 页面即可正常显示。
- 结束

16.7 如何解决复制某些阿拉伯字符显示为乱码的问题

现象描述

- 场景一：在复制某些阿拉伯字符，粘贴到 Flex 界面的文本框或可编辑区域（如粘贴到“拓扑管理”窗口的“搜索”文本框）中，文字显示为乱码。
- 场景二：在资源管理中创建网元时，复制某些含阿拉伯字符的字符串到“名称”文本框中，字符串显示正常。但该网元的名称在“拓扑管理”窗口中显示为乱码。

可能原因

Flex 不支持复制粘贴某些阿拉伯字符。

 说明

阿拉伯字符在 unicode 的码点范围有两个：

- 0x0600-06ff 之间，主要用于输入处理。Flex 支持复制粘贴。
- 0xfe70-0xfeff 之间，主要用于显示。Flex 不支持复制粘贴。

处理步骤

步骤 1 当出现复制阿拉伯字符显示为乱码的情况，使用输入法手工输入可以规避该问题。

----结束

16.8 如何根据网管所需端口情况，自定义端口连接规则

问题

如何根据网管所需端口情况，自定义端口连接规则？

 说明

本文适用于 Windows 7 和 Windows Server 2008。

回答

步骤 1 单击“开始”，在“搜索程序和文件”中，输入“firewall.cpl”。

弹出“Windows 防火墙”。

步骤 2 在左侧单击“打开或关闭 Windows 防火墙”，用户根据自己所处的网络位置在“家庭或工作（专用）网络位置设置”或者“公用网络位置设置”中，选择“启用 Windows 防火墙”，单击“确认”。

返回“Windows 防火墙”。

步骤 3 在左侧单击“高级设置”。

弹出“高级安全 Windows 防火墙”。

步骤 4 在左侧单击“入站规则”。

在右侧弹出“操作”。

步骤 5 单击“新建规则”。

弹出“新建入站规则向导”。

步骤 6 在左侧选择“规则类型”，右侧选择“端口”，单击“下一步”。

步骤 7 在“该规则应用于 TCP 还是 UDP？”中，选择“TCP”或者“UDP”，在“此规则适用于所有本地端口还是特性端口”中，选择“特定本地端口”，并在“特定本地端口”中设置网管所需端口。

单击“下一步”。

步骤 8 选择“允许连接”，单击“下一步”。

步骤 9 单击“下一步”。

步骤 10 单击“下一步”，输入“名称”和“描述”。

单击“完成”，完成自定义端口连接规则设置。

----结束

16.9 如何解决因数据库异常停止使网元出现垃圾数据而导致网管无法管理该网元的问题

现象描述

网元资源管理数据、物理资源数据、物理拓扑不一致，导致网管无法管理网元。

可能原因

在网元增加或者删除过程当中，如果数据库因异常停止，网元可能出现垃圾数据，进而使网元资源管理数据、物理资源数据、物理拓扑不一致，导致网管无法管理网元。

处理步骤

步骤 1 停止 eSight 服务。

- Windows 系统：
 1. 单击“开始 > 所有程序 > eSight > 停止 eSight”。
- SUSE Linux 系统：
 1. **cd /opt/eSight/AppBase/bin**
 2. **./stop.sh**

步骤 2 连接数据库后，可通过下列语句删除垃圾数据。

- **oracle 数据库：**

```
delete from nemgr.tbl_ne_extinfo where not exists (select * from omsmodel.tbl_mobasicattr m
where m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from omsmodel.tbl_mobasicattr m where
m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from omsmodel.tbl_mobasicattr m where
m.dn = nedn);
delete FROM omsmodel.tbl_moextendattr where dn in (select destNode from
```

```
omsmodel.tbl_morelation where srcnode in ((select m.dn from omsmodel.tbl_mobasicattr m where
not exists(select * from nemgr.tbl_ne_info n where m.dn = n.nedn) and m.DN != '/NE=OMS' and
m.DN like '%NE=%')) and type = 'Dependency');
delete from omsmodel.tbl_moextendattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_mobasicattr where dn in (select destNode from omsmodel.tbl_MORElation
where not exists(select * from nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and
DN like '%NE=%')) and type = 'Dependency';
delete from omsmodel.tbl_mobasicattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_tobasicattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
commit;
```

- **mysql 数据库:**

```
delete from nemgr.tbl_ne_extinfo where not exists (select * from omsmodel.tbl_mobasicattr m
where m.dn = nedn);
delete from nemgr.tbl_ne_info where not exists (select * from omsmodel.tbl_mobasicattr m where
m.dn = nedn);
delete FROM omsmodel.tbl_moextendattr where dn in (select destNode from
omsmodel.tbl_morelation where srcnode in ((select m.dn from omsmodel.tbl_mobasicattr m where
not exists(select * from nemgr.tbl_ne_info n where m.dn = n.nedn) and m.DN != '/NE=OMS' and
m.DN like '%NE=%')) and type = 'Dependency');
delete from omsmodel.tbl_moextendattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_mobasicattr where dn in (select destNode from omsmodel.tbl_MORElation
where not exists(select * from nemgr.tbl_ne_info n where dn = n.nedn) and DN != '/NE=OMS' and
DN like '%NE=%')) and type = 'Dependency';
delete from omsmodel.tbl_mobasicattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
delete from omsmodel.tbl_tobasicattr where not exists(select * from nemgr.tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%';
commit;
```

- **sqlserver 数据库:**

```
delete from nemgr..tbl_ne_extinfo where not exists (select * from omsmodel..tbl_mobasicattr m
where m.dn = nedn)
go
delete from nemgr..tbl_ne_info where not exists (select * from omsmodel..tbl_mobasicattr m
where m.dn = nedn)
go
delete FROM omsmodel..tbl_moextendattr where dn in (select destNode from
omsmodel..tbl_morelation where srcnode in ((select m.dn from omsmodel..tbl_mobasicattr m where
not exists(select * from nemgr..tbl_ne_info n where m.dn = n.nedn) and m.DN != '/NE=OMS' and
m.DN like '%NE=%')) and type = 'Dependency')
go
delete from omsmodel..tbl_moextendattr where not exists(select * from nemgr..tbl_ne_info n
where dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
delete from omsmodel..tbl_mobasicattr where dn in (select destNode from
omsmodel..tbl_MORElation where not exists(select * from nemgr..tbl_ne_info n where dn = n.nedn)
and DN != '/NE=OMS' and DN like '%NE=%') and type = 'Dependency'
go
delete from omsmodel..tbl_mobasicattr where not exists(select * from nemgr..tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
delete from omsmodel..tbl_tobasicattr where not exists(select * from nemgr..tbl_ne_info n where
dn = n.nedn) and DN != '/NE=OMS' and DN like '%NE=%'
go
```

步骤 3 启动 eSight 服务。

- **Windows 系统:**

1. 单击“开始 > 所有程序 > eSight > 启动 eSight”。

- **SUSE Linux 系统:**

1. **cd /opt/eSight/AppBase/bin**

2. `./run.sh`

----结束

16.10 如何解决 eSight 界面无法正常显示，注销时出现整页程序代码的问题

现象描述

登录 eSight，界面显示不全，单击“注销”后，界面出现整页的程序代码。

可能原因

eSight 服务器磁盘空间被占满，造成 WEB 服务器编译页面时生成的临时文件没有空间存放。

处理步骤

- 清理 eSight 服务器所在的磁盘空间。eSight 服务器正常运行所需要的磁盘空间大小根据您购买版本的不同有所差异，在 20G~320G 之间，具体版本的配置要求请参见《Huawei eSight V200R002C00 版本说明书》。

----结束

16.11 如何配置服务器 SNMP 参数

问题

如何配置服务器的 SNMP 参数？

回答

- 在 Windows Server 2008 环境下：
 1. 在 Windows 开始菜单中，选择“管理工具 > 服务器管理器”。
 2. 在“服务器管理器”界面，左侧导航树中选择“功能”。
 3. 在“功能”界面，单击“添加功能”。
弹出“添加功能向导”对话框。
 4. 在“添加功能向导”界面，选中“SNMP 服务”复选框，单击“下一步”。
 5. 单击“安装”，系统开始安装 SNMP 服务。
 6. 单击“关闭”。
 7. 在 Windows 开始菜单中，选择“管理工具 > 服务”。
 8. 在“服务”界面中，右键单击“SNMP Service”，在右键菜单中选择“属性”。
弹出“SNMP Service 的属性”对话框。
 9. 在“SNMP 的属性”对话框，单击“安全”页签。
 10. 单击“添加”。

弹出“SNMP 服务配置”对话框。

11. 设置“团体权限”为“只读”，输入“社区名称”为“public”，单击“添加”。
12. 单击“添加”。

弹出“SNMP 服务配置”对话框。

13. 设置“团体权限”为“读写”，输入“社区名称”为“private”，单击“添加”。
14. 选中“接受来自任何主机的 SNMP 数据包”前面的复选框，单击“确定”。

● 在 Linux 环境：

1. 将 suse 安装盘放入光驱中。
2. 选择“计算机 > 安装软件”，进入“YaST2”界面。
3. 单击“搜索”页签，在查询条件中输入SNMP，单击“搜索”。
4. 选择安装的 SNMP 组件，单击“接受”。
5. 组件安装成功后，运行如下命令对 SNMP 配置文件进行编辑。

```
# vi /etc/snmp/snmpd.conf
```

6. 查找“rocommunity”和“rocommunity”，具体设置如下。

```
# on setting up groups and limiting MIBS.
```

```
rocommunity public
```

```
rwcommunity private
```

7. 输入：**wq**，按“Enter”，退出文件编辑界面。
8. 进入“init.d”文件夹，执行如下命令重新启动 SNMP 代理服务。

```
# ./snmpd restart
```

当出现如下信息时，即完成 SNMP 参数配置。

```
Shutting down snmpd:  
done  
Starting snmpd
```

----结束

16.12 如何解决因修改 eSight 服务器系统时间对 eSight 产生的影响

现象描述

修改 eSight 服务器系统时间后会导致 eSight 无法正常使用，如会导致拓扑不刷新等情况。

处理步骤

步骤 1 停止 eSight 服务。

步骤 2 重新启动 eSight 服务。

----结束

A 术语

A

AAA	见 Authentication, Authorization and Accounting ; 认证、授权和计费。
ABR	见 Available Bit Rate ; 可用比特率。
AC	见 Access Controller ; 无线控制器。
ACL	见 Access Control List ; 访问控制列表。
AH	见 Authentication Header ; 报文认证头协议。
AIS	Alarm Indication Signal; 告警指示信号
ANCP	见 Access Node Control Protocol ; 接入节点控制协议。
AP	Access Preamble; 接入前缀
APS	Automatic Protection Switching; 自动保护倒换
ARP	见 Address Resolution Protocol ; 地址解析协议。
ARQ	见 Automatic Repeat reQuest ; 自动重传请求。
AS	Access Server; 接入服务器
ASIC	见 Application-Specific Integrated Circuit ; 专用集成电路。
ATAE	见 Advanced Telecommunications Application Environment ; 高级电信应用平台。
ATM	Asynchronous Transfer Mode; 异步传输模式
Access Control List (ACL); 访问控制列表	被授权访问某一资源的实体及其访问权限的列表。
Access Controller (AC); 无线控制器	对无线局域网中的所有接入点（AP）进行控制和管理，并通过与认证服务器交互信息，为无线局域网用户提供认证服务。
Access Node Control Protocol (ANCP); 接入节点控制协议	一种以 IP 为基础的协议，通过数字用户线接入和汇聚网运行在接入节点和网络接入服务器之间。
Address Resolution Protocol (ARP); 地址解析协议	将 IP 地址映射为 MAC 地址的互联网协议，允许主机和路由器通过 ARP 请求和 ARP 回应确定链路层地址。

Advanced Telecommunications Application Environment (ATAE); 高级电信应用平台	华为公司为了满足用户对业务应用专业化和高集成的需求而推出的一款电信级高性能处理平台。
Application-Specific Integrated Circuit (ASIC); 专用集成电路	一种特殊类型的芯片，开始时作为一个逻辑门非特定集合，后在制造过程中，为实现特定功能，一层被添加以便连接逻辑门。通过改变连接的模式，制造商可以制造适应多种需要的芯片。
Authentication Header (AH); 报文认证头协议	一种协议，为 IP 数据提供无连接完整性与数据源认证，并提供保护以避免重播情况。
Authentication, Authorization and Accounting (AAA); 认证、授权和计费	一个用于配置认证、授权和计费的机制。认证是指对用户的身份与可使用的网络服务进行确认；授权（Authorization）是指依据认证结果开放网络服务给用户；计费是指记录用户对各种网络服务的用量并提供给计费系统。
Automatic Repeat reQuest (ARQ); 自动重传请求	数据传输中的一种差错控制方法。接收方检测到数据包存在错误时，会自动请求发送方重新发送数据。如果接收方收到的下个数据包是正确的，那么接收方不再进行请求。
Available Bit Rate (ABR); 可用比特率	ATM 论坛定义的一种业务分类。ABR 只提供尽力转发服务，不能对信元丢失、延时方面提供保证。适用于对实时性没有要求的业务连接。
B	
BAS	见 Broadband Access Server; 宽带接入服务器 。
BFD	见 Bidirectional Forwarding Detection; 双向转发检测 。
BGP	Border Gateway Protocol; 边界网关协议
BIP	见 Bit Interleaved Parity; 比特间插奇偶校验 。
BITS	见 Building Integrated Timing Supply; 通信楼定时供给系统 。
BPDU	见 Bridge Protocol Data Unit; 桥接协议数据单元 。
BRAS	见 Broadband Remote Access Server; 宽带远程接入服务器 。
Bidirectional Forwarding Detection (BFD); 双向转发检测	简单的“Hello”协议，与路由协议的邻居检测部分相似。一对系统在它们之间的通道上周期性的发送 BFD 检测报文，如果某个系统在足够长的时间内没有收到对端发来的检测报文，则认为在这条到相邻系统的双向通道的某个部分发生了故障。在某些条件下，为了减少负荷，系统之间的发送和接收速率需要协商。
Bit Interleaved Parity (BIP); 比特间插奇偶校验	用来检测误码的一种方法。发端设备在信号的特定区间产生偶校验的 X-bit 码：码中的第一位为此信号区间的 X-bit 序列的第一位提供偶校验，码中的第二位为此信号区间的 X-bit 序列的第二位提供偶校验。通过设置 BIP-X 位产生偶校验进而保证被检测信号区间总有偶数个 1。被检测区间包括覆盖信号区段中 X-bit 序列处在同一字节位的比特。覆盖的区段包括 BIP-X。
Bridge Protocol Data Unit (BPDU); 桥接协议数据单元	使用生成树协议（STP）拓扑结构的扩展的局域网内的交换机之间用于交流的一组数据消息。BPDU 单元包含端口，地址，优先级，以及开销等信息，从而保证数据能到达它想去的地方。BPDU 消息在网桥之间进行交换来检测网络拓扑结构中是否有环存在。通过关闭特定的网桥端口和把多余的交换机端口设置为备份或者阻止的状态，BPDU 能去除环。

Broadband Access Server (BAS); 宽带接入服务器	该服务器提供用户接入、连接管理、地址分配、认证授权、用户计费等接入等特性。同时又具有路由器的路由管理功能强、转发性能高、业务丰富等特点。
Broadband Remote Access Server (BRAS); 宽带远程接入服务器	一种面向宽带网络应用的新型接入网关。它是宽带接入网和骨干网之间的桥梁，提供基本的接入手段和宽带接入网的管理功能。它位于网络的边缘，提供宽带接入服务、实现多种业务的汇聚与转发，能满足不同用户对传输容量和带宽利用率的要求。BRAS 是宽带用户接入的核心设备。
Building Integrated Timing Supply (BITS); 通信楼定时供给系统	在同步节点或通信设备较多的情况下，以及通信网的重要枢纽上，单独设置时钟系统，承上启下，沟通整个同步网，对所在的通信楼的设备提供满意的同步基准信号。这种设备称为“通信楼综合定时供给系统”。
C	
CAC	见 Connection Admission Control; 连接允许控制 。
CCM	Central Control Module; 中心控制模块
CDR	见 Call Detail Record; 呼叫详细记录 。
CE	见 Customer Edge; 用户边缘设备 。
CES	见 Circuit Emulation Service; 电路仿真功能 。
CF	见 Call Forwarding; 呼叫前转 。
CG	见 Charging Gateway; 计费网关 。
CHAP	见 Challenge Handshake Authentication Protocol; 质询握手验证协议 。
CRC	见 Cyclic Redundancy Check; 循环冗余校验 。
CRL	见 Certificate Revocation List; 证书撤销列表 。
CSPF	Constraint Shortest Path First; 约束最短路径优先
Call Detail Record (CDR); 呼叫详细记录	用于产生计费记录的数据库记录。CDR 包括呼叫方、被叫方、发起交换机、终止交换机、通话长度，以及时间。
Call Forwarding (CF); 呼叫前转	电话网络的特性之一，当被叫用户在无法接听来电时，该呼叫将被前转到其他指定号码。
Certificate Revocation List (CRL); 证书撤销列表	被撤销的数字证书列表。一个由认证中心废除的所有认证的时间戳组成的列表。CRL 是由认证中心签署并且使之对需要依赖认证授权的实体有效。
Challenge Handshake Authentication Protocol (CHAP); 质询握手验证协议	采用 3 次握手对对端的身份进行周期性验证的方法。链路建立连接的过程中，验证方给对端发送一个“challenge”消息，对端则回应一个通过“单向哈希”函数计算出的数值。验证方根据自行计算出的预期哈希值对返回值进行校验；如果两值相符，验证通过。盘问握手验证协议可以防止重放攻击。
Charging Gateway (CG); 计费网关	该网关提供基于业务的计费采集、批价、扣费和业务控制等功能，在网络中是以一种计费功能部件形式存在。对于业务而言，它是一种隐式服务，在网络中存在形态类似一个路由设备，不对外提供 Proxy、GW 形式的服务。
Circuit Emulation Service (CES); 电路仿真功能	一种功能，利用 ATM 网络传输 E1/T1 时隙数据，时隙数据在发端被打包成 ATM 信元，然后通过 ATM 网络传输到收端，收端将 ATM 信元中的数据重新分配到 E1/T1 时隙中，整个打包、传输和分配过程必须保证收端能够恢复出原有顺序结构的 E1/T1 时隙数据。

Connection Admission Control (CAC); 连接允许控制	在呼叫建立阶段（或者呼叫重协商阶段）网络执行的一系列活动，以判断是否接受或拒绝某个连接请求。
Coordinated Universal Time (UTC); 通用协调时间	一个全球通用的科学计时标准。它是通过精心维护原时钟，确保全球保持统一（精确到微秒）。
Customer Edge (CE); 用户边缘设备	BGP/MPLS IP VPN 模型的一部分，用于提供接口直接与服务提供商（SP）网络相连。CE 可以是路由器或交换机，也可以是一台主机。
Cyclic Redundancy Check (CRC); 循环冗余校验	一种检测数据传输中的错误的过程。CRC 检验根据传输的数据通过复杂的计算产生一个数。发送设备在发送数据前进行这个计算，然后将结果发送给接收设备。接收设备在接收后，重复同样的运算，如果两个设备的运算结果相同，就认为传输无误，这个过程被称为冗余检验是因为每次传输不仅包含数据而且包含额外（冗余）的差错检验值。
D	
DAS	见 Data Access Service; 数据访问服务 。
DHCP	见 Dynamic Host Configuration Protocol; 动态主机配置协议 。
DIMM	见 Dual In-line Memory Module; 双列直插内存模块 。
DNS	Domain Name Server; 域名服务器
DPI	Deep Packet Inspection; 深度报文检测
DR	见 Disaster Recovery; 容灾 。
DSLAM	见 Digital Subscriber Line Access Multiplexer; 数字用户线接入复接器 。
DSP	见 Digital Signal Processor; 数字信号处理器 。
Data Access Service (DAS); 数据访问服务	商业管理点的组成部分之一，实现应用对数据的透明访问，屏蔽了数据的存储类型、存储格式、存储位置的差异。
Digital Signal Processor (DSP); 数字信号处理器	专门用来实时处理数字信号的微处理器。
Digital Subscriber Line Access Multiplexer (DSLAM); 数字用户线接入复接器	一部网络设备，通常在电话公司总局，从多个用户数字用户线路（DSL）连接接受信号，并用复用技术把信号承载在一条高速骨干线路上。
Disaster Recovery (DR); 容灾	对生产中心的重要设备数据和应用软件进行远程备份，当生产中心机器发生灾难或故障时，使用远程备份机器和数据，代替故障机器对业务进行处理。
Dual In-line Memory Module (DIMM); 双列直插内存模块	挂载了 RAM 内存芯片的电路板。DIMM 指可装一组内存芯片的小型电路板。DIMM 可支持 64 位数据传输而 SIMM 仅支持 32 位数据传输。奔腾处理器需要 64 位内存数据通道，因此进行内存条安装时，需要同时安装两个 SIMM 内存，而安装 DIMM 内存时仅需要一根。
Dynamic Host Configuration Protocol (DHCP); 动态主机配置协议	客户端—服务器网络协议。DHCP 服务器针对 DHCP 客户端的请求提供对应的配置参量，这些参量通常是客户端主机连接因特网时需要的信息。DHCP 同时提供为主机分配 IP 地址的机制。

E

ECM	Entitlement Control Message; 授权控制信息
EEPROM	见 Electrically Erasable Programmable Read-Only Memory ; 电可擦可编程只读存储器。
EFM	Ethernet in the First Mile; 最后一公里以太网
EPLD	见 Erasable Programmable Logic Device ; 可擦除可编程逻辑器件。
EPON	见 Ethernet Passive Optical Network ; 以太网无源光网络。
ESN	见 Equipment Serial Number ; 设备序列号。
ESP	见 Encapsulating Security Payload ; 封装安全载荷协议。
Electrically Erasable Programmable Read-Only Memory (EEPROM); 电可擦可编程只读存储器	一种可以用电信号擦除的可擦可编程只读存储器。它用于长时间没有电源供应而需要维持稳定的存储信息，同时又需要能重编程的场合。与 RAM 相比，EEPROM 存储容量小，重编程花的时间长，而且只能重编程很有限的几次。
Encapsulating Security Payload (ESP); 封装安全载荷协议	该协议在传输模式和隧道模式下使用，它采用加密和验证机制，为 IP 数据包提供数据源验证、数据完整性、反重放和机密安全服务。
Equipment Serial Number (ESN); 设备序列号	唯一标识设备的字符串，用以保证将 License 授权给指定设备的关键，又称“设备指纹”。
Erasable Programmable Logic Device (EPLD); 可擦除可编程逻辑器件	一种可擦除、可编程逻辑阵列，用户只要对它编程就可实现所需要的功能。而且用户可以反复修改、反复编程，直到程序完全满足要求。
Ethernet Passive Optical Network (EPON); 以太网无源光网络	基于以太网方式的无源光网络，它是新一代的宽带接入技术，采用点到多点结构、无源光纤传输方式。目前可支持 1.25Gbit/s 上下行对称速率，实现最远 20km 的接入能力。下行采用针对不同用户加密广播传输的方式共享带宽，上行利用时分复用 TDM 共享带宽，充分满足接入网客户的带宽需求。
二层组播	当链路层应用以太网技术时，二层组播使用组播 MAC 地址。同时必须存在一种技术将 IP 组播地址映射为组播 MAC 地址。

F

FDI	见 Forward Defect Indication ; 前向缺陷通告。
FE	见 Fast Ethernet ; 快速以太网。
FEC	见 Forward Error Correction ; 前向纠错。
FIB	见 Forward Information Base ; 转发信息库。
FPGA	见 Field Programmable Gate Array ; 现场可编程门阵列。
FR	见 Frame Relay ; 帧中继。
FRR	见 Fast ReRoute ; 快速重路由。
FTP	File Transfer Protocol; 文件传输协议

Fast Ethernet (FE); 快速以太网	任何支持 100Mbit/s 的 Ethernet 规范的网络。快速以太网的速率比 10BaseT 以太网快 10 倍，并保留了帧格式、MAC 寻址机制、MTU 等特性。快速以太网是基于 IEEE 802.3 标准的扩展，可以使用以下三种传输介质：100BASE-T4（4 对电话双绞线）、100BASE-TX（2 对数据级双绞线）、100BASE-FX（2 芯光纤）。
Fast ReRoute (FRR); 快速重路由	MPLS TE 中实现网络局部保护的技术，只有速率在 100Mbps 以上的接口才支持 FRR。FRR 的切换速度可以达到 50 毫秒，能够最大程度减少网络故障时数据的丢失。
Field Programmable Gate Array (FPGA); 现场可编程门阵列	专用集成电路（ASIC）领域中的一种半定制电路。它是在 PAL、GAL、EPLD 等可编程器件的基础上进一步发展的产物，既解决了定制电路的不足，又克服了原有可编程器件门电路数有限的缺点。
Forward Defect Indication (FDI); 前向缺陷通告	该报文由第一个检测到缺陷的节点产生并向下游发送，报文中会携带缺陷的类型和位置。其主要目的是抑制受影响的客户 LSP 层产生告警。
Forward Error Correction (FEC); 前向纠错	一种误码纠错方式，它通过在发送端为净荷附加纠错信息，在接收端利用纠错信息来纠正净荷在传输时产生的误码。
Forward Information Base (FIB); 转发信息库	在数据通信中，是一种为网络硬件（网桥、交换机或路由器）提供将数据包传送至其他网络所需方向的信息表。路由表中包含的信息根据其是否被网桥或路由器使用而有所不同。网桥根据源（起源）地址和目标地址来确定将数据包发送至何处与如何转发数据包。
Frame Relay (FR); 帧中继	一种在广域网中应用的分组交换协议。帧中继通过事先确定的通道，即 PVC，以高达 2Mbit/s 的速率传输可变长度的数据包。是 X.25 的变体，但为了高速传输而舍弃了 X.25 中的错误检测机制。
防火墙	设置在不同网络或网络安全域之间的一系列部件的组合。它通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现对网络的安全保护。
G	
GE	见 Gigabit Ethernet; 千兆以太网 。
GGSN	见 Gateway GPRS Support Node; 网关 GPRS 支持节点 。
Gateway GPRS Support Node (GGSN); 网关 GPRS 支持节点	为提供分组数据业务功能而引入的一个的网元功能实体，提供数据包在 GPRS（General Packet Radio Service）/UMTS（Universal Mobile Telecommunications System）网和外部数据网之间的路由和封装。
Gigabit Ethernet (GE); 千兆以太网	以每秒千兆的速度传输以太网帧的技术，遵守 IEEE 802.3z 标准，兼容 10M 及 100M 以太网。运行速度达到 1000M。千兆以太网都使用完全专用的介质，不支持共享的同轴电缆或其他电缆。千兆以太网支持以共享带宽方式使用信道，但当千兆以太网以网桥（交换机）或路由器为中心，部署成专用带宽系统时，能够达到最佳的性能和最大的带宽。千兆以太网的基本结构形式是采用全双工的、专用的链路。这使得链路长度足以支持建筑物内部和园区主干的应用。
广播域	一组网络局点，这些局点接收在组内任何设备发送的广播报文。也指设备上负责转发组播帧、广播帧和未知目的帧的所有接口的集合。
H	
HA	见 High Availability; 高可用性 。

HTTP	Hypertext Transfer Protocol; 超文本传输协议
High Availability (HA); 高可用性	通常指采用主、备两个相同的模块以热备份的方式完成指定功能，以提高可靠性的方式。在主用模块故障时，备用模块会自动接替主用模块执行系统功能。
黑白名单	系统根据预定义的主、被叫所属组之间的限呼关系来决定是否允许该呼叫。
黑名单	根据报文的源 IP 地址进行过滤的一种方式。同 ACL 相比，由于进行匹配的域非常简单，可以以很高的速度实现报文的过滤，从而有效地将特定 IP 地址发送来的报文屏蔽。
I	
IAB	见 Internet Architecture Board ; 因特网体系委员会。
ICMP	见 Internet Control Message Protocol ; 因特网控制报文协议。
IETF	见 Internet Engineering Task Force ; Internet 工程任务组。
IGMP	见 Internet Group Management Protocol ; 因特网组管理协议。
IGP	见 Interior Gateway Protocol ; 内部网关协议。
IKE	见 Internet Key Exchange ; 因特网密钥交换协议。
IPSec	见 Internet Protocol Security ; 因特网协议安全协议。
IP 地址	一种 32 位（四字节）的二进制数码，它唯一标识一台连入因特网的主机（计算机），与因特网上其他主机相区分，其目的在于以包传送的形式进行通信。IP 地址以“点分”的形式表示以四个字节的十进制数字组成，以句点分隔（例如，127.0.0.1）。IP 地址的第一个字节、第二个字节或第三个字节标明主机连入的网络；剩余的位表明主机本身。
IPv4	见 Internet Protocol version 4 ; 第四版互联网协议。
IPv6	见 Internet Protocol version 6 ; 第六版因特网协议。
IS-IS	见 Intermediate System to Intermediate System ; 中间系统到中间系统。
ISAKMP	见 Internet Security Association and Key Management Protocol ; Internet 安全联盟和密钥管理协议。
ISSU	见 In-Service Software Upgrade ; 不断业务升级。
In-Service Software Upgrade (ISSU); 不断业务升级	一种升级模式，激活时分别复位主用和备用主控单板，业务不中断。系统会自动对网元状态、基本业务、路由关系等信息进行检测。
Interior Gateway Protocol (IGP); 内部网关协议	运行于自治系统内部的路由协议，运行于小型或中等网络中。目前常用的有 RIP、IGRP、EIGRP、OSPF 等。
Intermediate System to Intermediate System (IS-IS); 中间系统到中间系统	网络设备（路由器）使用的一种协议。这种协议在以信息包为基础的网络上确立传送数据报文或信息包的最佳路径，即所谓的路由选择。
Internet Architecture Board (IAB); 因特网体系委员会	为 TCP/IP 和国际互联网制定政策和发展方向的组织，经选举产生，负责上诉仲裁、起草体系文件。

Internet Control Message Protocol (ICMP); 因特网控制报文协议	一种网络层（ISO/OSI level 3）因特网协议，提供与 IP 报文处理相关的错误纠正和其他信息。例如，ICMP 使得一台机器上的 IP 软件能够告知另外一台机器某个目的地址不可达。
Internet Engineering Task Force (IETF); Internet 工程任务组	由来自全球对组网和因特网感兴趣的个人组成的组织，由 IESG（互联网工程指导小组）管理。IETF 是负责研究面向互联网的技术问题并负责向互联网架构委员会（IAB）提供解决方案。IETF 的工作由其下的各种工作组完成，集中于特定的议题，例如路由和安全。IETF 的是 TCP/IP 协议标准的出版商。
Internet Group Management Protocol (IGMP); 因特网组管理协议	TCP/IP 协议族中负责 IP 组播成员管理的协议。它用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。
Internet Key Exchange (IKE); 因特网密钥交换协议	一种混合协议，在 ISAKMP 框架内实现了 Oakley 密钥交换和 SKEME 密钥交换。Oakley 和 SKEME 都定义了一种交换密钥的方法，这包括了有效负载的结构、传输的信息有效负载、密钥的处理步骤以及如何使用密钥。
Internet Protocol Security (IPSec); 因特网协议安全协议	IETF 制定的一系列协议，通过对数据流中的每个 IP 包进行鉴权和加密，为 IP 数据报提供了高质量的、可互操作的、基于密码技术的安全性。
Internet Protocol version 4 (IPv4); 第四版互联网协议	互联网协议（IP）的当前版本。IPv4 使用 32 字节用作主机地址，每个地址属于 A、B、C、D、E 五类中的一类。地址为 32 位编码，通常用 4 个点分十进制数表示。每个地址由一个网络码、（可选）子网码、主机码组成。网络码和（可选）子网码用于路由，主机码用于在网络或子网内部寻址到一台具体主机。
Internet Protocol version 6 (IPv6); 第六版因特网协议	Internet 工程任务组（IETF）设计的一套规范，是 IPv4 的升级版。它是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation）。IPv6 和 IPv4 之间最显著的区别就是 IP 地址的长度从 32 位升为 128 位。
Internet Security Association and Key Management Protocol (ISAKMP); Internet 安全联盟和密钥管理协议	允许消息接收方获得公共密钥并使用数字认证鉴别发送方身份的一种协议。

J

加密	一种变换数据的功能，目的是掩藏信息内容从而防止未经授权的使用。
介质	用于存储计算机信息的物理媒介。可以用于复制数据并将该数据保持一定时间的设备或记录装置。通过该装置，仍可以获取原始数据。

K

KPI	Key Performance Indicator; 关键性能指标

L

L2TP Network Server (LNS); L2TP 网络服务器	L2TP 隧道的一个端点，同时也是 LAC 的对端。LNS 是一个与远端系统连接的 PPP 会话的逻辑终结点。
L2VPN	Layer 2 Virtual Private Network; 二层虚拟专用网

L3VPN	Layer 3 Virtual Private Network; 三层虚拟专用网
LAG	见 Link Aggregation Group ; 链路聚合组。
LCP	Link Control Protocol; 链路控制协议
LDAP	见 Lightweight Directory Access Protocol ; 轻型目录访问协议。
LDP	Label Distribution Protocol; 标签分发协议
LLDP	见 Link Layer Discovery Protocol ; 链路层发现协议。
LNS	见 L2TP Network Server ; L2TP 网络服务器。
LOS	见 Loss Of Signal ; 信号丢失。
LPU	Line interface Processing Unit; 线路接口处理单元
LSP	见 Label Switched Path ; 标签交换路径。
LSR	见 Label Switching Router ; 标签交换路由器。
Label Switched Path (LSP); 标签交换路径	信息包通过标记交换机制传送中的一系列跳转站（从 RO 到 Rn）所形成的传输通道。一个标记交换路径可以按照常规路由机制或配置来灵活选用。
Label Switching Router (LSR); 标签交换路由器	MPLS 网络中的基本元素，所有 LSR 都支持 MPLS 协议。LSR 由两部分组成：控制单元和转发单元。控制单元负责标签的分配、路由的选择、标签转发表的建立、标签交换路径的建立、拆除等工作；转发单元则依据标签转发表对收到的分组进行转发。
Lightweight Directory Access Protocol (LDAP); 轻型目录访问协议	基于 TCP/IP 的网络协议，允许对目录系统代理的访问，X.500 目录访问协议的简化形式。
Link Aggregation Group (LAG); 链路聚合组	允许一条或多条连接到同一设备的以太网链路聚合在一起形成链路聚合组，以便 MAC 客户将链路聚合组看作是一条链路。
Link Layer Discovery Protocol (LLDP); 链路层发现协议	链路层发现协议是 IEEE 802.1ab 中定义的第二层发现协议。通过采用 LLDP 技术，在网络规模迅速扩大时，网管系统可以快速掌握二层网络拓扑信息、拓扑变化信息。
Loss Of Signal (LOS); 信号丢失	接收的信号无法转换。
路由表	储存和更新网络设备地址信息的表。路由器之间要共享路由表信息以保证信息的及时性。路由器根据目标地址和路由表中的信息进行转发，其中路由表以中继断或许多跳转给出路由器自身、中转路由器和目标方的可能路径选择。当有新的或更新的信息时，路由表就进行更新。
路由器	网络层设备。使用路由器可以在因特网中进行路由选择，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。可用于连接本地网和本地网、广域网和广域网、或本地网和互联网。

M

MAC 地址认证	一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法。通过手工维护一组允许访问的 MAC 地址列表，实现对客户端物理地址过滤，但这种方法的效率会随着终端数目的增加而降低，因此 MAC 地址认证适用安全需求不太高的场合，如家庭、小型办公室等环境。
MD	见 Maintenance Domain ; 维护域。
MD5	见 Message Digest algorithm 5 ; 消息摘要算法第五版。
ME	见 Mobile Equipment ; 移动设备。
MEG	见 Maintenance Entity Group ; 维护实体组。
MEP	Maintenance association End Point; 维护联盟边缘节点
MIB	见 Management Information Base ; 管理信息库。
MLD	见 Multicast Listener Discovery ; 组播监听者发现协议。
MPLS	见 MultiProtocol Label Switching ; 多协议标记交换。
MPLS TE	MultiProtocol Label Switching Traffic Engineering; 多协议标记交换流量工程
MPLS TP	见 Multiprotocol Label Switching Traffic Policing ; 多协议标签交换流量监控。
MPLS VPN	见 MultiProtocol Label Switching Virtual Private Network ; MPLS 虚拟专用网。
MPU	Main Processing Unit; 中央交换框主控板
MSDP	见 Multicast Source Discovery Protocol ; 组播源发现协议。
MSTP	见 Multiple Spanning Tree Protocol ; 多生成树协议。
MTU	见 Maximum Transmission Unit ; 最大传输单元。
Maintenance Domain (MD); 维护域	对其实施以太网 CFM 管理的一个网络或一个网络的一部分，一个 MD 由一个统一的 ISP（Internet Service Provider）进行管理。
Maintenance Entity Group (MEG); 维护实体组	维护实体组（MEG）是满足下列条件的 ME： ● MEG 中的 ME 存在于相同的管理边界之内 ● MEG 中的 ME 具有相同的 MEG 层次 ● MEG 中的 ME 属于相同的点到点连接或者点到多点连接
Management Information Base (MIB); 管理信息库	一种存放在网络代理的配置管理数据库。它用于网络管理站或本地用户接口设备的访问。
Maximum Transmission Unit (MTU); 最大传输单元	在网络中能够传输的最大数据报文。大小根据网络可变，如在 X.25 网络中是 576 字节，以太网中是 1500 字节，16Mbit/s 令牌环中是 17914 字节。MTU 大小取决于网络的链路层。当报文在网络上传输时，路径 MTU，即 PMTU 确定了相关网络中最小报文尺寸，即所有网络能够不分段传输的报文大小。
Message Digest algorithm 5 (MD5); 消息摘要算法第五版	计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护。MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由四个 32 位分组组成，将这四个 32 位分组级联后将生成一个 128 位散列值。
Mobile Equipment (ME); 移动设备	移动台的一个组成部分。当移动设备放入 SIM 卡后，它们就组成一个移动台，然后在 GSM 网络上注册。

MultiProtocol Label Switching (MPLS); 多协议标记交换	在 IP 路由和控制协议的基础上，向网络层提供面向连接的交换的技术。它采用短而定长的标记封装各种链路层分组。该技术可以提高网络的性能/价格比，改善网络的可扩展性，并为路由服务。
MultiProtocol Label Switching Virtual Private Network (MPLS VPN); MPLS 虚拟专用网	一种基于 MPLS 技术的 IP VPN，它是在网络路由和交换设备上应用 MPLS 技术、简化核心路由器路由选择方式并结合传统路由技术和标记交换实现的 IP 虚拟专用网络，可用于构造宽带 Intranet、Extranet，满足多种业务需求。
Multicast Listener Discovery (MLD); 组播监听者发现协议	用于 IPv6 路由器发现其直连网段上组播监听者（Multicast Listener）、建立、维护组成员关系的协议。在 IPv6 网络中，通过在接收者主机和与其直连的组播路由器上配置 MLD，可以实现主机动态加入和组播路由器对本地网络组成员信息的管理。
Multicast Source Discovery Protocol (MSDP); 组播源发现协议	只适用于 PIM-SM 域，仅对 ASM（Any-Source Multicast）模型有意义的协议。通过在不同 PIM-SM 域的 RP 之间建立 MSDP 对等体关系，在域间共享组播源信息，实现跨域组播。通过在同一 PIM-SM 域的多个 RP 之间建立 MSDP 对等体关系，在域内共享组播源信息，实现 Anycast RP。
Multiple Spanning Tree Protocol (MSTP); 多生成树协议	可应用于环路网络的协议。该协议通过一定算法阻断冗余路径，将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。MSTP 提出了 VLAN 与多个生成树之间的映射的概念，解决了 STP、RSTP 中由于只有一棵生成树对应所有 VLAN 导致 VLAN 内数据不能正常转发的缺陷。
Multiprotocol Label Switching Traffic Policing (MPLS TP); 多协议标签交换流量监控	一套管理进入通信设备的 mpls 流量的方案。通过对进入网络的流量速度制定策略，惩罚超过阈值的流量，因此把进入网络的流量限制在合理的范围，以保护网络资源和运营商的利益。
O	
OAM	见 Operation, Administration and Maintenance ; 操作、管理和维护。
OMC	见 Operation and Maintenance Center ; 操作维护中心。
ONT	见 Optical Network Terminal ; 光网络终端。
ONU	见 Optical Network Unit ; 光网络单元。
OSI	见 Open Systems Interconnection ; 开放系统互连。
OSPF	见 Open Shortest Path First ; 开放式最短路径优先。
Open Shortest Path First (OSPF); 开放式最短路径优先	显示链路状态，用于网络路由的一种分级内部网关协议。Dijkstra 运算法则用来计算最短路径树。它将成本作为选择路由的衡量因素。一个链路状态数据库是由跟该域内所有路由器相同的网络拓扑构建的。
Open Systems Interconnection (OSI); 开放系统互连	ISO 标准的一种框架结构，用于由不同供应商制造的系统之间的通信，通信过程由 7 个不同的基于与用户的关系的分层排列的层组成。每一层将使用下一层所提供的环境并为上一层提供服务。第 7 层到第 4 层处理消息源和消息目的地之间的端到端通信，第 3 层到第 1 层处理网络功能。
Operation and Maintenance Center (OMC); 操作维护中心	网络管理系统的实体，负责一个或一组网元的操作维护。例如，OMC-radio 可负责无线子系统的管理，OMC-switch 可负责交换网元的管理。此外，网络管理中心（NMC）控制整个网络，OMC 在 NMC 控制之下。

Operation, Administration and Maintenance (OAM); 操作、管理和维护	一组监控和逐段维护的网络功能，可进行网络故障监测、故障申告、故障定位，以及误码控制等，使每段网络都处于正常工作状态，为用户提供满足需要的业务承载网络。
Optical Network Terminal (ONT); 光网络终端	为光接入网络提供直接或者远程的用户侧接口设备，与局端设备相连。
Optical Network Unit (ONU); 光网络单元	接入节点的一种形式，利用光缆将发送的光信号转换成电信号，然后通过同轴电缆或是双绞铜缆传送给每个客户。
P	
P2P	见 Point-To-Point service; 点到点业务 。
PAP	见 Password Authentication Protocol; 密码验证协议 。
PCI	见 Peripheral Component Interconnect; 外围部件互连标准 。
PD	Product Daemon; 产品服务器程序
PDSN	见 Packet Data Serving Node; 分组数据服务节点 。
PIC	Parallel Interference Cancellation; 并行干扰抵消
PIM	Protocol Independent Multicast; 协议无关组播
PLL	见 Phase-Locked Loop; 锁相环 。
POS	见 Packet Over SDH/SONET; 基于 SDH/SONET 的封装 。
PPP	Point-to-Point Protocol; 点对点协议
PPPoE	Point-to-Point Protocol over Ethernet; 以太网承载 PPP 协议
PSN	见 Packet Switched Network; 分组交换网络 。
PTP	见 Point To Point; 点对点 。
PVC	见 Permanent Virtual Circuit; 永久虚电路 。
PW	见 Pseudo Wire; 伪线 。
PWE3	见 Pseudo Wire Emulation Edge-to-Edge; 端到端伪线仿真 。
Packet Data Serving Node (PDSN); 分组数据服务节点	连接移动网络和 IP 骨干网络的网关设备，为移动用户提供分组数据接入服务。
Packet Over SDH/SONET (POS); 基于 SDH/SONET 的封装	一种城域网及广域网技术，提供点到点的数据连接。POS 接口以 SDH/SONET 为物理层协议，支持在城域网及广域网中传送分组数据（如 IP 分组）。
Packet Switched Network (PSN); 分组交换网络	一种按报文交换方式运行的电信网络。
Password Authentication Protocol (PAP); 密码验证协议	验证企图登录到点对点协议（PPP）服务系统的用户身份的一种方法。如果一种更严格的方法（如查询信号交换认证协议）无法起作用，或者用户提交给 PAP 的用户名和口令必须不加密地送给其他程序时，则应使用口令认证协议。

Peripheral Component Interconnect (PCI); 外围部件互连标准	一种连接计算机主板和外部设备的总线标准。1992 年由 Intel 公司发布 PCI1.0 标准, 从 1993 年开始由 PCI-SIG 发布 PCI 相关标准。外设部件互连传送输入/输出函数给电脑, 包括服务器、工作站、个人电脑、便携机以及移动设备。
Permanent Virtual Circuit (PVC); 永久虚电路	分组交换网络上两个节点之间的一种永久性逻辑连接。PVC 就像节点间的专用连接, 但数据可以在公共载体上传输。
Phase-Locked Loop (PLL); 锁相环	这是由鉴相器 (PD)、环路滤波器 (LPF)、压控振荡器 (VCO) 和分频器 (/N) 等组成的一个相位负回授的环路。它比较压控振荡器和输入载频信号或参考频率发生器的频率。鉴相器的输出经过环路滤波器后反馈到压控振荡器, 使得此输出和输入载频信号或参考频率在同一相位。
Ping	利用 ICMP Echo 消息及其应答来测试 IP 网络中某个网络设备是否可达的方法。
Point To Point (PTP); 点对点	一种服务类型。数据从一个单一网络发出, 在另一个网络终止。
Point-To-Point service (P2P); 点到点业务	指在两个终点之间操作的业务。发送方和接收方都是最终用户。
Pseudo Wire (PW); 伪线	两个 PE 间的虚拟连接, 在两个 PE 之间传输帧。建立和维护 PW 的工作由 PE 利用信令完成, 并由 PW 的两个端点 PE 维护 PW 的状态信息。
Pseudo Wire Emulation Edge-to-Edge (PWE3); 端到端伪线仿真	将传统通信网络与现有分组网络结合而提出的解决方案之一。PWE3 是指在 PSN 网络中尽可能真实地模仿 ATM、帧中继、以太网、低速 TDM 电路和 SONET/SDH 等业务的基本行为和特征的一种二层业务承载技术。
配置文件	包含硬件或软件的机器可读的运行规范, 或者包含另外一个文件的信息或者某个特定用户的信息 (例如该用户的登录 ID) 的文件。
Q	
QoS	见 Quality of Service; 服务质量 。
Quality of Service (QoS); 服务质量	通信系统或信道的常用性能指标之一。不同的系统及业务中其定义不尽相同, 可能包括抖动、时延、丢包率、误码率、信噪比等。用来衡量一个传输系统的传输质量和服务有效性, 评估服务商满足客户需求的能力。
确认告警	已经处理的告警。通过确认告警, 能了解到未被处理的告警从而及时的处理。
R	
RADIUS	见 Remote Authentication Dial-In User Service; 拨号用户远程认证服务 。
RADIUS 计费	一种计费模式。BRAS 设备将计费报文送往 RADIUS 服务器, 由 RADIUS 服务器完成对用户的计费。
RADIUS 认证	一种认证模式。BRAS 将用户名和密码通过 RADIUS 协议传送给 RADIUS 服务器, RADIUS 服务器完成对用户的认证并将认证结果反馈给 BRAS。
RDI	Remote Defect Indication; 远端缺陷指示
RDS	见 Replicated Data Set; 复制数据集 。
RP	Routing Performer; 路由执行器
RPT	COPS 协议的一个操作码, 用于 PEP 向 PDP 报告执行决策时是成功还是失败, 或报告一次状态变化。

RRPP	见 Rapid Ring Protection Protocol ; 快速环网保护协议。
RSVP-TE	见 Resource ReserVation Protocol-Traffic Engineering ; 针对流量工程扩展的资源预留协议。
Rapid Ring Protection Protocol (RRPP); 快速环网保护协议	专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。
Remote Authentication Dial-In User Service (RADIUS); 拨号用户远程认证服务	一种鉴别和授权拨号用户的安全服务，并且是一种集中式访问的控制机制。RADIUS 使用 UDP 作为传输协议来确保良好的实时性，通过支持重传机制和多服务器机制来确保良好的可靠性。
Replicated Data Set (RDS); 复制数据集合	主节点主机上的复制卷组（RVG）和辅助节点主机上相对应的复制卷组构成了复制数据集（RDS）。RDS 不是一个 Volume Manager 对象，而是在 VVR 中使用的概念。RDS 允许对主节点上的 RVG 和辅助节点上相对应的 RVG 进行分组。
Resource ReserVation Protocol-Traffic Engineering (RSVP-TE); 针对流量工程扩展的资源预留协议	在已有的 RSVP 协议基础上加入了几个新的消息对象，用于在 MPLS 网络中发起标签请求和分发标签绑定来建立和维护 LSP，并提供重路由 LSP 和增加已建立的 LSP 的带宽的能力。
S	
SA	见 Source Active ; Source Active 消息。
SD	见 Signal Degrade ; 信号劣化。
SDH	见 Synchronous Digital Hierarchy ; 同步数字体系。
SFTP	见 Secure File Transfer Protocol ; 安全文件传输协议。
SFU	Signal Filtering Unit; 信号接口处理单元
SIG	见 Security Immunity Gateway ; 安全免疫网关。
SLA	见 Service Level Agreement ; 服务水平协议。
SMTP	见 Simple Mail Transfer Protocol ; 简单邮件传输协议。
SNMP	见 Simple Network Management Protocol ; 简单网络管理协议。
SPI	见 Security Parameter Index ; 安全参数索引。
SPS	见 Security Policy Server ; 安全策略服务器。
SPU	Service Process Unit; 业务处理单元
SQ	见 Subscriber Queue ; 用户队列。
SRAM	见 Static Random Access Memory ; 静态随机存取存储器。
SSH	见 Secure SHell ; 安全外壳。
SSL	见 Secure Sockets Layer ; 安全套接层。
SSM	见 Synchronization Status Message ; 同步状态信息。
STP	Signaling Transfer Point; 信令转接点
SVC	见 Switched Virtual Circuit ; 交换虚电路。

Secure File Transfer Protocol (SFTP); 安全文件传输协议	一个基于 SSH（Secure Shell）提供安全文件传输的网络协议。
Secure SHell (SSH); 安全外壳	一套标准和网络协议，允许在本地计算机和远程计算机之间建立安全渠道。用户通过一个不能保证安全的网络环境远程登录时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护网络不受诸如 IP 地址欺诈、明文密码截取等攻击。
Secure Sockets Layer (SSL); 安全套接层	工作于套接字层的安全协议。该层位于 TCP 层和应用层之间，用于数据的加解密以及相关实体的认证。
Security Immunity Gateway (SIG); 安全免疫网关	从网络蠕虫病毒的最大源头--终端用户计算机入手，检测用户计算机的安全状态的网关。对不安全的计算机，提示其进行系统加固或杀毒操作。对于已经感染蠕虫病毒的计算机，根据安全接入策略，从网络接入层暂时隔离或限制，从而解决网络上蠕虫病毒泛滥的问题。
Security Parameter Index (SPI); 安全参数索引	一个引用保护传输数据所用的会话密钥和算法的指针。安全参数索引在安全联盟（SA）间定义并在封装安全载荷（ESP）中或鉴权报头（AH）至 IP 报头的扩展中描述。
Security Policy Server (SPS); 安全策略服务器	方案中的用户管理与策略控制中心，实现用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能，是 EAD 解决方案的核心部件。
Service Level Agreement (SLA); 服务水平协议	用户和服务商之间的服务约定，规定了用户应当得到的转发服务水平。这里的用户可以是一个组织（源域）或 DS 域（上行域）。SLA 可以全部或部分为流量控制规则。
Signal Degrade (SD); 信号劣化	在出现劣化缺陷的情况下，指示相关数据劣化的信号。
Simple Mail Transfer Protocol (SMTP); 简单邮件传输协议	用于发送 e-mail 的 TCP/IP 协议，该协议规定两个系统如何相互作用以及用于控制发送的消息的格式。
Simple Network Management Protocol (SNMP); 简单网络管理协议	TCP/IP 协议簇中的网络管理协议。可使某网元的管理信息由逻辑上的远程用户察看和修改。目标是保证管理信息在任意两点间传送。采用轮询机制，提供最基本的功能集。在简单网络管理协议 SNMP 中，软硬件代理均能监视网上多种设备的活动并将这些信息向网络控制台工作站报告。关于每个设备的控制信息用一种结构（称为管理信息结构块）来维护。
Source Active (SA); Source Active 消息	MSDP 消息类型。SA 消息中包含多组（S，G）信息，或封装一个 Register 消息。MSDP 对等体之间通过交互 SA 消息，共享组播源信息。
Static Random Access Memory (SRAM); 静态随机存取存储器	随机存取存储器的一种类型，只要电源持续供电，就可以保留其内容。它不像动态随机存取存储器，不需要不断刷新。
Subscriber Queue (SQ); 用户队列	一种虚拟队列。每个 SQ 固定对应 8 种 FQ 业务优先级，可配置 1～8 个 FQ。空闲 FQ 不能被其它 SQ 利用，即这 1～8 个 FQ 共享该 SQ 的带宽。
Switched Virtual Circuit (SVC); 交换虚电路	在包交换网络中的两个节点之间的一种逻辑连接，仅在数据将要传输时创建。
Synchronization Status Message (SSM); 同步状态信息	该信息用于在同步定时链路中传递定时信号的质量等级，使得 SDH 网和同步网中的节点时钟通过对 SSM 的读解获取上游时钟的信息，对本节点的时钟进行相应操作（例如跟踪、倒换或转入保持），并将该节点同步信息传递给下游。

Synchronous Digital Hierarchy (SDH); 同步数字体系	一种传输体制，遵循 ITU-T G.707, G.708 和 G.709 建议，定义了数字信号传输的帧结构、复用方式、传输速率等级、接口码型等特性。SDH 是构成 ISDN 和 B-ISDN 的重要组成部分。SDH 通过将低速信号通过字节间插方式复接进高速信号中，仅对信号进行扰码的线路编码方式，采用同步复用方式和灵活的映射结构，使得 SDH 体制特别适合于高速大容量的光纤通信系统。
T	
TCP	见 Transmission Control Protocol ; 传输控制协议。
TE	见 Traffic Engineering ; 流量工程。
TFTP	见 Trivial File Transfer Protocol ; 简单文件传输协议。
TLV	见 Type-Length-Value ; 类型长度值。
TM	见 Terminal Multiplexer ; 终端复用器。
TTL	见 Time To Live ; 生存时间。
Terminal Multiplexer (TM); 终端复用器	在网络的终端把多路低速信号复用成一路高速信号，或反过来把一路高速信号分接成多路低速信号的设备。
Time To Live (TTL); 生存时间	尽力而为传输机制采用的一种技术，用于避免报文无限环回。发送方将 TTL 值设置为报文在网络中允许生存的最长时间。网络中的每台路由器在收到报文时，将 TTL 值减一；如果 TTL 值为零，将丢弃报文。
Traffic Engineering (TE); 流量工程	通过动态监控网络的流量和网元的负载，实时调整流量管理参数、路由参数和资源约束参数等，优化网络资源的使用，避免负载不均导致的拥塞。
Transmission Control Protocol (TCP); 传输控制协议	TCP/IP 中的协议，用于将数据信息分解成信息包，使之经过 IP 协议发送；并对由 IP 接收来的信息包进行校验并将其重新装配成完整的信息。TCP 是面向连接的可靠协议，能够确保信息的无误发送，它与 ISO/OSI 基准模型中的传输层相对应。
Trivial File Transfer Protocol (TFTP); 简单文件传输协议	文件传输协议 FTP 的另一种小型简单协议形式。TFTP 协议用于客户端和服务端之间不需要复杂交互的应用上，它把业务限制在简单的文件传输上，不需要进行验证。TFTP 协议很小，可以存储在 ROM 上，用于引导没有硬盘的设备。
Type-Length-Value (TLV); 类型长度值	一种高效率，扩展性好的协议报文编码方式。也称为 CLV 编码（code-length-value）。 ● T-Type: 采用不同的值定义不同类型 ● L-Length: Value 域的整体长度 ● V-Value: 本 TLV 的实际内容，最重要的部分 TLV 编码的优点：可扩展性好，如果想增加对于新特性的支持，只需增加新的 TLV 类型，它采取这样一种形式更加灵活的方式来描述报文中需要加载的信息。
拓扑对象	网管系统拓扑视图中的基本元素，包括子图、节点和链接（连接）等。
拓扑发现	一种精确确定网络布局的技术，使用几个网络结构假设和简单工具实现。
拓扑视图	人机交互界面的一个基本组成部分。拓扑视图直观地显示网络的组网情况和网络中各网元、子网的告警、通讯状态，反映网络运行的基本情况。
跳数	最简单的路由度量值，每条链路的花费值为 1。该功能可以计算出报文转发的额定次数。

traceroute	一个能够显示到达目的地路径的程序。Traceroute 发出 TTL 值为 1、2、……的数据报序列，并根据返回的 ICMP 超时消息来判断路径上的路由器的状态。
U	
UNI	见 User Network Interface ; 用户网络接口。
URI	见 Uniform Resource Identifier ; 统一资源标识。
URPF	见 Unicast Reverse Path Forwarding ; 单播反向路由转发。
USAU	见 Universal Signaling Access Unit ; 通用信令接入单元。
USB	见 Universal Serial Bus ; 通用串行总线。
UTC	见 Coordinated Universal Time ; 通用协调时间。
Unicast Reverse Path Forwarding (URPF); 单播反向路由转发	该功能用于防止基于源地址欺骗的网络攻击行为。
Uniform Resource Identifier (URI); 统一资源标识	标识一个抽象资源或物理资源的字符串。
Universal Serial Bus (USB); 通用串行总线	带接口设备的串行总线的标准。这标准原本是专为计算机而设计，如：个人电脑，苹果的 Macintosh 电脑等。但随着它的普及，此标准被广泛应用于计算机游戏和个人数字助理的业务。
Universal Signaling Access Unit (USAU); 通用信令接入单元	作为通信设备的信令接入单元，完成各通信设备间的信令协议转换，支持基于 TDM 的窄带 No.7 信令网和基于 IP 的宽带 SIGTRAN 信令网。
User Network Interface (UNI); 用户网络接口	用户设备与私网或公网设备（例如 ATM 交换机）之间的接口。
V	
VC	见 Virtual Channel ; 虚拟信道。
VLAN	Virtual Local Area Network; 虚拟局域网
VP	见 Virtual Path ; 虚拟通路。
VPLS	见 Virtual Private LAN Service ; 虚拟专用局域网业务。
VPN	Virtual Private Network; 虚拟专用网
VPN Routing and Forwarding (VRF); 虚拟专用网路由转发	应用于计算机网络的一项技术。该技术允许一个路由器的路由表中同时存在多个的实例。由于这些实例彼此之间是独立的，它们可以使用重叠或重复的 IP 地址，不会产生冲突。
VPN-Target	也称为 Route Target，是 BGP/MPLS IP VPN 中用来控制 VPN 路由信息的发布 BGP 扩展团体属性。VPN-Target 属性定义了一条 VPN-IPv4 路由可以为哪些 Site 所接收，以及 PE 可以接收哪些 Site 发送来的路由。
VPN 实例	PE 为直接相连的 site 建立并维护的一个专门实体，每个 site 在 PE 上都有自己的 VPN 实例。VPN 实例也称为 VPN 路由转发表 VRF（VPN Routing and Forwarding table）。PE 上存在多个转发表，包括一个公网路由转发表，以及一个或多个 VRF。

VRF	见 VPN Routing and Forwarding ; 虚拟专用网路由转发。
VRRP	见 Virtual Router Redundancy Protocol ; 虚拟路由冗余协议。
VSI	Virtual Switch Interface; 虚拟交换机接口
Virtual Channel (VC); 虚拟信道	异步传输网络中的逻辑连接。虚拟信道是指由虚拟信道标识符标识的特定异步传输网络中交换机的基本单元。是传送用于虚拟信道连接的交换机发送的异步传输信元的信道。
Virtual Path (VP); 虚拟通路	虚拟通路是用于描述单向传送 ATM 信元的概念，这些 ATM 信元由一个共同的且唯一的标识（VPI）联系在一起。
Virtual Private LAN Service (VPLS); 虚拟专用局域网业务	公用网络中提供的一种点到多点的 L2VPN 业务，使地域上隔离的用户站点能通过 MAN/WAN 相连，并且使各个站点间的连接效果像在一个 LAN 中一样。
Virtual Router Redundancy Protocol (VRRP); 虚拟路由冗余协议	为具有多播或广播能力的局域网（如以太网）设计的协议。VRRP 将局域网的一组路由器（包括一个 MASTER 和若干个 BACKUP）组织成一个虚拟的路由器，称之为一个备份组。这个虚拟的路由器拥有自己的 IP 地址，网络内的主机就通过这个虚拟的路由器来与其他网络进行通信。如果备份组内的 MASTER 路由器损坏时，备份组内的其它 BACKUP 路由器将会接替成为新的 MASTER，继续向网络内的主机提供路由服务。
VoIP	见 Voice over IP ; IP 承载语音。
Voice over IP (VoIP); IP 承载语音	IP 电话术语，用于描述对 Internet 上的语音信息发送进行管理的一套设施。VoIP 涉及以数字形式发送语音信息。这种发送是通过不连续的数据包，而不是通过 PSTN 传统的面向电路的协议。
W	
WAN	见 Wide Area Network ; 广域网。
WLAN	见 Wireless Local Area Network ; 无线局域网。
WTR	见 Wait To Restore ; 等待恢复。
Wait To Restore (WTR); 等待恢复	路径/连接故障清除后，业务倒换回正常工作线路所需等待的时间。
Wide Area Network (WAN); 广域网	由许多在空间上相隔很远的计算机通过特定的协议和物理方式连接而成的一种网络，通常跨越很大的地域，例如包含一个省、州或国家。
Wireless Local Area Network (WLAN); 无线局域网	计算机网络与无线通信技术相结合的产物，它以无线多址信道作为传输媒介，利用电磁波完成数据交互，实现传统有线局域网的功能。
物理链路	两个物理网元之间存在的物理链接，在创建网元或者刷新设备状态时，系统根据对设备的拓扑结构信息分析而自动创建，物理链路可以修改备注信息，不能被删除。
X	
信道	一个网络中两个或者多个位置之间的具有指定容量或者指定速度的电信通路，可以是通过线缆、无线（微波）、光纤或者以上三者的结合建立的通路。信道中每秒钟所传输的信息量称为信息传输速率。信息传输速率的单位是 b/s、kb/s、Mb/s、Gb/s、Tb/s 等。

虚电路	在分组交换散列网络上的两个或多个端点站点间的链路。虚电路分为永久虚电路（PVC）和交换虚电路（SVC）。
虚连接	在一个 OSPF 路由域中的两台 ABR 之间，通过一个非骨干区域建立的一条逻辑上的连接通道。用于使那些物理上分割的区域仍可保持逻辑上的连通性，它的两端必须是 ABR，而且必须在两端同时配置方可生效。虚连接由对端路由器的 ID 号来标识。
虚拟链路	网管系统拓扑图中表示拓扑对象之间逻辑连接关系的连接。
虚拟网元	虚拟网元在视图上的显示与实际网元一样是采用图标显示，但它只是一个根据实际情况模拟的网元，不代表一个实际网元，所以不能查询该网元的实际状态，和通过颜色等来显示其告警状态。通常在对网管不能管理的网元或子网使用路径管理功能，或与其他厂商网元对接配置业务的情况下，提供端到端配置业务的方法及路径管理能力。
Y	
邮件服务器	报表系统中，可以将报表转发到用户的外部 E-mail 邮箱。邮件服务器就是提供接收和发送邮件功能的服务器。
远程登录	TCP/IP 协议堆栈中的标准终端仿真协议。远程登录应用于远程终端连接，通过它用户能像使用本地系统一样登录远程系统、使用资源。RFC 854 对远程登录做了规范。
Z	
主备倒换	一种故障处理技术，当主用设备发生故障时，系统自动将业务、控制等功能切换到备用设备上，以保证系统的正常运行。
子网	可以按照某种原则（如按地域划分）将一个比较大的网络结构分解为几个相对较小的网络结构，以方便操作员对网络的管理。在拓扑视图中，把这种相对较小的网络结构称为子网。