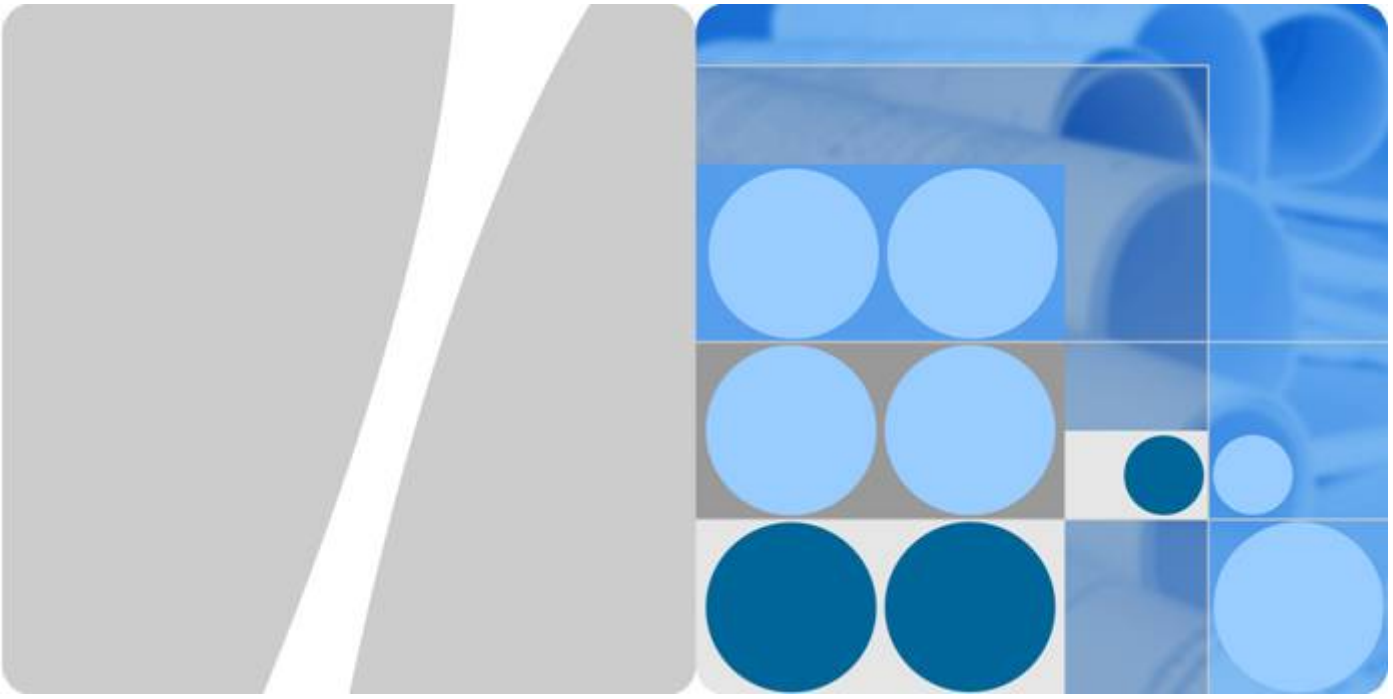


Huawei eSight 应用平台

V200R001C00

操作指南

文档版本　02

发布日期　2011-09-30

华为技术有限公司

商标声明


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

前 言

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
eSight 应用平台	V200R001C00

读者对象

本文档介绍了*《Huawei eSight 操作指南》*中公共功能操作。

本文档主要适用于以下工程师：

- 网络监控工程师
- 数据配置工程师
- 网管管理员
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。

符号	说明
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。

图形界面元素引用约定

在本文中可能出现下列图形界面元素，它们所代表的含义如下。

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

修改记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

产品版本(V200R001C00)-文档版本 02 (2011-09-30)

V200R001C00 版本第二次正式发布。

在上一版本基础上修正错误。

产品版本(V200R001C00)-文档版本 01 (2011-08-31)

第一次正式发布。

目 录

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。

可以通过增加下级网管操作，实现上级网管管理下级网管。

1.1 了解 eSight 的功能

指导您快速了解企业网网管的功能特点。

表 1-1 eSight 的基本功能

功能	简要描述
安全管理	安全管理能基于角色模型，从用户可管理设备以及用户可进行操作两个方面对用户的权限进行控制。 ● 支持实时监视登录网管系统的用户，并支持强制用户下线操作。 ● 支持设定服务器的访问限制，从而对用户登录网管服务器进行策略控制。 ● 支持设置帐户的安全策略，对帐户、密码的设置进行强制约束，提升系统帐户密码的安全性。
日志管理	日志信息记录了用户进行的一些重要操作，用户可以查看、过滤日志列表，还可以详细查看某条系统日志的内容。 eSight 支持管理操作日志、安全日志和系统日志，提供 warning（提示）、minor（一般）、risk（危险）三种级别的信息。 ● 操作日志：记录针对网管的各种操作。 ● 安全日志：与系统安全相关活动的日志。 ● 系统日志：记录在网管运行、任务执行过程中的各种关键信息。
告警管理	告警管理是对网络中的异常运行情况进行实时监视，通过告警监控板、实时告警浏览、历史告警浏览、事件列表查看功能，对网络故障进行监控。 用户可以根据需要设定告警的远程通知规则，设定告警屏蔽规则，设定告警的声音。丰富网络管理员优化网络管理方法。
性能管理	eSight 可以对网络的关键性指标进行监控，并对采集到性能数据进行统计。 通过可视化的操作界面，方便用户对网络性能进行管理。
报表管理	eSight 提供丰富的预定义报表，同时提供强大易用的报表设计功能，用户可根据行业特点和自身运维要求进行客户报表定制。

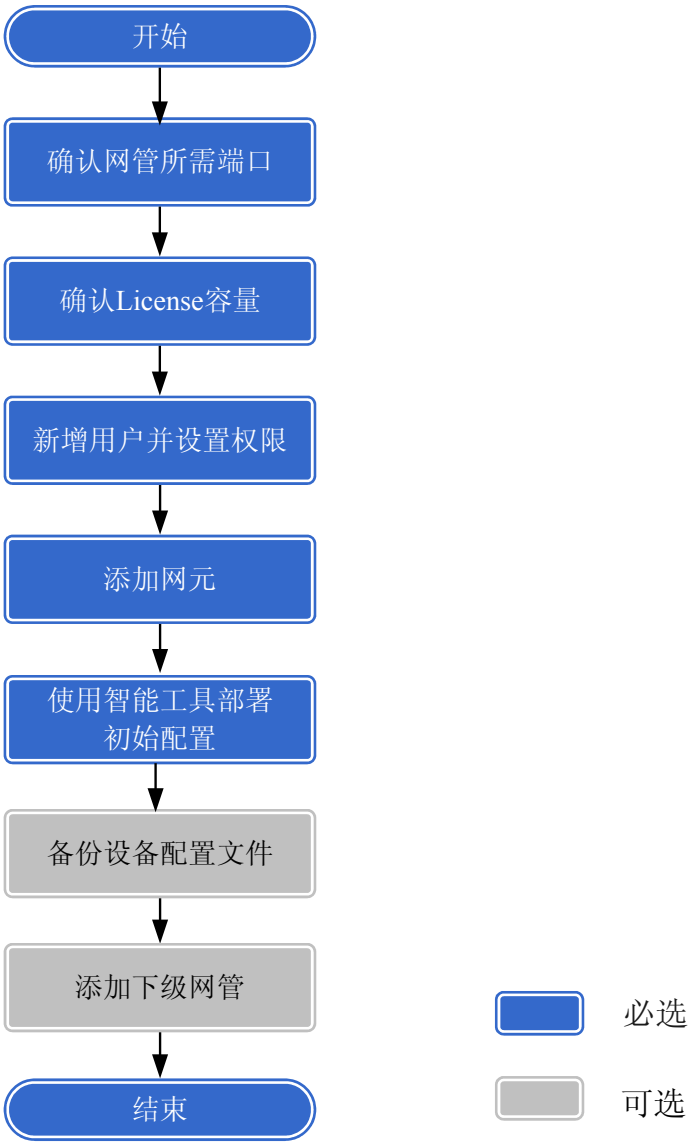
功能	简要描述
配置文件管理	提供设备配置文件自动备份、恢复、比较功能，从而实时记录设备的配置数据，保障保证设备配置数据的安全性。
分级网管	eSight 网管支持在上级网管维护下级网管列表，通过链接可以直接打开下级网管的界面，实现下级网管的单点（SSO）登录，从而实现查看下级网管告警、拓扑、性能和报表等功能。
资源管理	支持资源模型管理、存取、移动；支持资源的添加、删除、属性修改、属性查询；支持资源的审计与权限控制、版本升级管理、增删的 license 控制能力及二次开发能力。
拓扑管理	eSight 以左树右图的方式组织整个视图，其中左导航树以树型直观的体现出网络结构的层次关系；右视图在背景图上将指定网络层次的对象显示在不同的坐标上，可直观了解对象部署。
网元管理	eSight 支持管理华为路由器、交换机、AR、安全设备，同时通过系统预集成实现了对基于标准 MIB 的第三方设备管理。 eSight 对华为设备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。
业务管理	eSight 支持对 IPSec VPN、WLAN 业务的管理监测。

1.2 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、**1.3.1 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、**1.3.2 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。
3、**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、**1.8.2 手工添加网元**	将网元添加到网管，并进行管理。

操作	备注
5、1.9 使用智能工具部署初始配置	通过智能配置工具，将网元配置脚本下发到网元，完成对网元的初始配置。
7、(可选)1.10 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。
8、(可选)1.11 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。

1.3 调测准备

在进行基础调测前，您需要首先检查网管所需端口是否打开以及 License 是否满足需求。

1.3.1 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。

网管所用的端口列表如表 1-2 所示。

表 1-2 网管端口列表

端口号	端口说明	独立部署网管场景	需和上层网管对接场景	目的设备侧防火墙是否要打开此端口
8888	图形化命令行 http 访问端口。	是	是	是
8899	故障采集工具和报表服务器提供给客户端下载报表的共用访问端口。	是	是	是
8443	用于登录界面	是	是	是
38080	用于联机帮助	是	是	是
8030	Web 服务端口	是	是	是
8080	Web 服务端口	是	是	是
8009	tomcat 的 AJP 协议使用的标准端口	是	是	是

端口号	端口说明	独立部署网管场景	需和上层网管对接场景	目的设备侧防火墙是否要打开此端口
38988	备份工具 Virgo 的 debug 端口	是	是	否
9975	备份工具 Virgo 的 JMX 管理端口	是	是	否
8533	用于数据库备份工具登录界面	是	是	是
8130	数据库备份工具 Web 服务端口	是	是	是
38005	OM Web 服务停止端口	是	是	否
38085	Hedex web 服务停止端口	是	是	否
31004	JSON 总线端口	是	是	否
31005	Hessian 总线端口	是	是	否
31002	Virgo 的 OSGI 管理端口	是	是	否
39875	Virgo 的 JMX 管理端口	是	是	否
38788	Virgo 的 debug 端口	是	是	否
32403	OMS 状态监控端口	是	是	否
30999	Virgo 的 shell 端口	是	是	否
31003	SSO Server 访问安全管理	是	是	否
31006	Med Node 和 Center 连接	是	是	否
33306	MySql 数据库连接的端口	是	是	是
8097	eSight 安装盘的调试端口	是	是	否

端口号	端口说明	独立部署网管场景	需和上层网管对接场景	目的设备侧防火墙是否要打开此端口
31021	FTP 服务器用于传输文件	是	是	是
162	接收被管理设备 trap	是	是	是
10162	接收被管理设备 trap	是	是	否
39008	Mediation 的 soap 协议适配器	是	是	否
23	Telnet 端口	是	是	是
161	设备接收 SNMP 请求的端口	是	是	是
随机端口	向北向发送 trap 源端口	否	是	是
4700	网管接受北向命令	否	是	是
7890	CMPP2.0/2.1 协议端口	使用到对应的短信网关时打开	使用到对应的短信网关时打开	是
7891	CMPP3.0 协议端口	使用到对应的短信网关时打开	使用到对应的短信网关时打开	是
5018	SMPP3.3/3.4 协议端口	使用到对应的短信网关时打开	使用到对应的短信网关时打开	是
8801	SGIP1.2 协议端口	使用到对应的短信网关时打开	使用到对应的短信网关时打开	是
5090	SMPP3.3/3.4 协议端口	使用到对应的短信网关时打开	使用到对应的短信网关时打开	是
25	SMTP 协议端口	使用 SMTP Email 服务器时打开	使用 SMTP Email 服务器时打开	是

说明

对于随机端口，防火墙根据 Session 临时打开监听端口（根据请求的 port/ip，允许接收对应的响应消息），当会话结束后会关闭，因此不需要在防火墙上打开某动态端口。

1.3.2 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 1-3 所示。

表 1-3 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

1.4 运行环境要求

为了更好的在客户端中浏览并操作 eSight 系统，需要满足一定的运行环境要求。

客户端运行环境要求，如表 1-4 所示。

表 1-4 客户端运行环境要求

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、Windwos 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 > 兼容器视图设置”。 2. 在“兼容器视图设置”对话框中，去勾选“在兼容性视图中显示 Intranet 站点”和“在兼容性视图中显示所有站点”。 ● 由于 Windows 2008 操作系统默认具有较高的安全策略，因此若客户端是 Windows 2008 操作系统，则无法使用 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

1.5 登录和退出 eSight 系统

eSight 采用浏览器/服务器工作模式。您使用浏览器登录到 eSight 之后，可以执行各种网管任务。

前提条件

- 确保当前客户端和 eSight 服务器之间的网络连接正常，并且 eSight 服务器工作正常。
- 登录的用户帐号已经创建。

背景信息

- 系统安装完后，提供了一个初始用户和初始密码（admin/admin）。此用户拥有 eSight 网管系统的所有操作权限。
- admin 用户登录 eSight 网管系统后，需要添加新的用户、角色等。
- 登录 eSight 网管系统后，选择“系统 > 用户设置”，可对屏幕锁定时长和密码进行设置。

注意

首次登录 eSight 系统后，请根据界面上的密码设置策略修改初始用户 admin 的初始密码，以确保系统的安全性。

操作过程中如果需要回退，请您直接使用 eSight 界面中的返回功能，不要使用浏览器自带的返回功能。后者会导致不可预知的问题。

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://10.10.10.1:8080/），按“Enter”键。

系统显示 eSight 登录页面。

步骤 2 输入登录用户名和密码。

步骤 3 单击“登录”。

- 如果输入的用户名或密码错误，系统提示错误信息。例如：登录失败，用户名或密码错误！
- 当密码将要超过有效期时，系统会提示您需在有效期内修改密码。

----结束

退出 eSight

步骤 1 单击 eSight 系统右上角的  。

退出 eSight。

----结束

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

1.7 添加用户并设置权限

设置用户密码复杂度、更新周期的策略，合理设置可提高 eSight 系统访问安全性。密码策略将应用于所有用户，由安全管理员设置。

前提条件

拥有设置密码策略权限的用户登录，系统提供默认配置，维护期间可以适当调整。

背景信息

- 密码策略调整后将对 eSight 所有用户立即生效。例如：当调整用户密码长度的最小值，在线用户修改密码时，密码的最小长度需要符合密码策略的要求。
- 新的密码策略对已经设置的密码无影响。
- 密码策略规定了密码的复杂度、更新周期、字符限制。使用密码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。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“安全策略 > 密码策略”。

步骤 3 根据策略计划设置密码策略。

在创建用户和角色时，必须按照密码策略进行设置密码。

步骤 4 单击“应用”。

----结束

1.8 添加网元

将网元添加到网管进行管理。

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 设置网元侧 SNMPv3 参数。

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

1.8.2 手工添加网元

当需要接入到 eSight 的网元个数较少，网元所属类型较多时，您需要以手工创建单个网元的方式将网元一一接入到 eSight 中。

操作步骤

步骤 1 选择“资源 > 资源管理”。

“资源管理”页面右侧列举出已接入的所有对象。

步骤 2 在左侧导航树中选择新增网元的父对象，在右侧单击“单个创建”。

步骤 3 在“选择类型”页面选择“Snmp 网络设备”。

系统显示“配置参数”页面。

步骤 4 配置网元参数。

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“确认”，重新配置参数。

----结束

1.8.3 设置网管侧 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

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 > 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。

- 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。
- 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。

步骤 4 单击“确定”。

----结束

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

1.9 使用智能工具部署初始配置

通过下发脚本可以实现网元的批量配置。

前提条件

已经有经过验证的脚本，“验证脚本”的方法请参见 9.4.5 验证脚本。

背景信息

下发脚本可以批量进行，即可以选中多个网元下的多个脚本同时进行下发操作。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树上，选择要配置的网元或者要下发的脚本，单击右键，选择“下发脚本”。

步骤 4 在“下发脚本”对话框中，在左侧“脚本选择”区域框中，选择要下发的脚本，在右侧可以查看该脚本的详细信息。

如果有需要修改的命令行或者参数，可以进行修改。

可以同时选择多个网元下面的多个脚本进行下发。

步骤 5 单击“下发”。

步骤 6 在弹出的提示框中，单击“确定”。

步骤 7 在“下发窗口”中显示脚本的执行过程。

如果某个脚本执行异常，可进行以下操作：

- 重试：系统将执行异常的命令重新执行。
- 忽略：系统将忽略执行异常的命令，继续进行下一条命令的执行。
- 终止：系统将终止脚本的执行。

步骤 8 单击“保存配置”，手动将配置结果保存到网元上。

步骤 9 单击“关闭”，完成下发。

----结束

1.10 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 **10.2 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 在左侧导航树上选择“设备配置管理 > 配置文件”。

步骤 3 选中相应的设备，单击“备份”。

----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时，且备份的文件已达到上限，则网管默认丢弃最早的非基线配置文件。

1.11 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”、“用户名”、“密码”。

步骤 3 单击“确定”。

----结束

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 的数据安全性。

2.1 了解安全管理
安全管理包括对用户权限、系统安全策略等的管理。通过了解安全管理的相关功能，可以有效的设置用户、角色和访问控制等信息。

2.2 安全策略设置
安全策略是为管理用户而制定的“帐户策略”和“密码策略”。在初始安装时应进行必要的安全策略规划和配置，配置后可根据管理需要进行调整。

2.3 角色管理
当 eSight 提供的默认角色不能满足用户授权需求时，可以根据角色的管理特性创建自定义角色，以便为用户集中分配设备的管理权限。自定义角色由 Administrators 根据需要创建。

2.4 用户管理
为网络设备的维护人员在 eSight 上创建 eSight 用户帐号，设置用户的基本信息和操作权限。eSight 用户由安全管理员来创建和设置。

2.5 用户访问控制
设置访问控制列表，使用户只能从特定 IP 地址和时间段登录服务器。用户访问控制列表由安全管理员设置。

2.6 安全监控
介绍拥有超级管理员角色权限的用户监控 eSight 用户会话、操作、强制 eSight 用户退出和解锁 eSight 用户的操作。

2.7 示例：创建网管用户并分配权限
介绍分权分域场景下如何创建网管用户并分配权限。

2.1 了解安全管理

安全管理包括对用户权限、系统安全策略等的管理。通过了解安全管理的相关功能，可以有效的设置用户、角色和访问控制等信息。

2.1.1 安全管理概述

用户管理是 eSight 安全策略的重要组成部分，安全机制主要从用户授权、访问控制和安全监控等方面实现。

用户授权

具有合法身份的用户只有经过授权，才能对 eSight 内的资源进行相关的访问或操作。

用户授权就是为用户分配 eSight 操作权限。在授权前规划好角色、对象集和操作集可提高授权效率。帐号管理员需要通过新建角色来给新用户授权。

访问控制

防止用户对网络资源进行未授权的访问，例如采用“登录时间控制”或“登录 IP 地址控制”进行控制。

安全监控

监控用户的访问行为，确保用户行为安全、合法。

2.1.2 安全基本概念

在进行安全管理操作时，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和准确地进行安全管理的操作。

表 2-1 安全基本概念

概念	说明
用户	用户及其密码唯一确定了相应的操作管理权限。 “admin”是系统缺省提供的超级管理员，能管理所有的设备和具有所有的操作权限。
角色	角色是用户的集合，对用户进行授权。 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”是系统缺省提供的超级管理员角色。
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。

概念	说明
系统访问控制	用于限制用户只能在特定时间或特定 IP 地址登录 eSight 系统。 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，从而提高了的安全性。

2.1.3 用户角色缺省的操作权限列表

介绍 eSight 各角色在缺省情况下拥有的操作权限。

名称	说明
超级管理员	具有所有的操作权限。
安全管理员	具有角色、用户创建和维护的权限，具有在线用户管理的权限。
操作员	具有各特性配置和查询的权限，不具有安全管理员的权限。
监视员	只具有各特性查询的权限。

2.2 安全策略设置

安全策略是为管理用户而制定的“帐户策略”和“密码策略”。在初始安装时应进行必要的安全策略规划和配置，配置后可根据管理需要进行调整。

2.2.1 设置帐号策略

设置用户名的长度和用户登录相关的策略，合理设置可提高 eSight 访问安全性。帐号策略将应用于所有用户，所以应由安全管理员设置。

前提条件

拥有设置帐号策略权限的用户登录，系统提供默认配置，维护期间可以适当调整。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“安全策略 > 帐号策略”。

步骤 3 根据策略计划设置帐号策略。

在创建用户或角色时，必须按照帐号策略设置用户名或角色名。

步骤 4 单击“应用”。

----结束

2.2.2 设置密码策略

设置用户密码复杂度、更新周期的策略，合理设置可提高 eSight 系统访问安全性。密码策略将应用于所有用户，由安全管理员设置。

前提条件

拥有设置密码策略权限的用户登录，系统提供默认配置，维护期间可以适当调整。

背景信息

- 密码策略调整后将对 eSight 所有用户立即生效。例如：当调整用户密码长度的最小值，在线用户修改密码时，密码的最小长度需要符合密码策略的要求。
- 新的密码策略对已经设置的密码无影响。
- 密码策略规定了密码的复杂度、更新周期、字符限制。使用密码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。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“安全策略 > 密码策略”。

步骤 3 根据策略计划设置密码策略。

在创建用户和角色时，必须按照密码策略进行设置密码。

步骤 4 单击“应用”。

----结束

2.3 角色管理

当 eSight 提供的默认角色不能满足用户授权需求时，可以根据角色的管理特性创建自定义角色，以便为用户集中分配设备的管理权限。自定义角色由 Administrators 根据需要创建。

2.3.1 创建角色

当 eSight 提供的默认角色不能满足用户授权需求时，您可以根据角色的管理特性创建自定义角色，以便为用户集中分配设备的管理权限。

前提条件

- 拥有创建角色权限的用户登录。
- 清楚维护人员职责分工、eSight 默认角色权限。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“权限分配 > 角色”。

您可以查看角色相关信息。

步骤 3 单击“创建角色”。

步骤 4 设置参数，单击“下一步”。

选择角色成员的时候，可以在列表中选择角色成员，也可以输入角色名进行搜索选择角色成员，在已选择成员列表中可以删除已选成员。

步骤 5 单击“增加”，设置管理对象，单击“确定”。

您可以设置一个或多个管理域下的管理对象。

1. 在“管理域列表”中选择管理域。

   管理域右上方显示红星号，表示属于该管理域的一个或多个管理对象被选中。
2. 在右侧区域框中选中一个或多个管理对象。

   已经选择过的管理对象将不会出现在列表中。

步骤 6 单击“下一步”。

步骤 7 单击“增加”，设置操作对象，单击“确定”。

您可以设置一个或多个操作组下的操作对象。

1. 在“操作组列表”中选择操作对象。

   操作组右上方显示红星号，表示属于该操作组的一个或多个操作对象被选中。
2. 在右侧区域框中选中操作对象。

   已经选择过的操作对象将不会出现在列表中。

步骤 8 单击“下一步”。

步骤 9 核对设置的信息，单击“完成”。

----结束

2.3.2 维护角色

角色创建后，超级管理员角色可以查看角色信息，根据实际情景进行修改角色信息。

前提条件

拥有维护角色权限的用户登录

背景信息

角色创建后，需要对角色信息通过下面操作进行维护。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“权限分配 > 角色”。

步骤 3 在“角色”窗口中，可以进行下面操作。

操作名称	操作方法
查看	1. 选择需要查看的角色，单击角色名。 2. 查看用户列表、管理对象和操作权限信息。
修改	1. 选择需要修改信息的角色，单击“  ”。 2. 修改用户列表、管理对象和操作权限相关信息。 3. 单击“确认”。
删除	1. 选择需要删除的角色，单击“  ”。 2. 确认系统提示。 **说明** 不可以删除系统缺省角色。

----结束

2.3.3 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，角色可以管理指定的自定义管理域中的对象。

背景信息

在创建和维护角色时，可以从管理域列表中选择用户自定义管理域。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“高级 > 自定义管理域”。

步骤 3 在“自定义管理域”窗口可以进行以下操作。

操作名称	操作方法
创建自定义管理域	1. 单击“创建”。 2. 设置参数。 选择管理域成员：单击“增加”，选择一个或者多个管理对象，单击“确定”。 3. 单击“确定”。

操作名称	操作方法
修改自定义管理域	1. 选择管理域，单击“  ”。 2. 修改相关信息。 选择自定义管理域中的成员： ● 单击“增加”，在“选择管理域”窗口中选择一个或者多个管理对象，单击“确定”。 ● 选中一个或者多个管理对象，单击“删除”。 3. 单击“确定”。
删除自定义管理域	1. 选择管理域，单击“  ”。 2. 确认系统提示。

----结束

2.4 用户管理

为网络设备的维护人员在 eSight 上创建 eSight 用户帐号，设置用户的基本信息和操作权限。eSight 用户由安全管理员来创建和设置。

2.4.1 创建用户

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。

前提条件

- 拥有创建用户权限的用户登录系统。
- 已了解用户帐户策略和密码策略，即帐号和密码的设置要求、合法条件。
  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 在左边导航树上选择“权限分配 > 用户”。

步骤 3 单击“创建”。

步骤 4 设置用户基本信息属性，单击“下一步”。

步骤 5 设置用户所属角色，单击“下一步”。

步骤 6 设置访问控制属性。

设置访问控制	操作
设置登录时间控制	1. 单击“创建”。 2. 在“创建登录时间控制”窗口中设置登录时间范围。 3. 单击“确定”。 如果设置多个时间策略，您只能选择 1 个。
设置登录 IP 地址控制	1. 单击“创建”。 2. 在“创建登录 IP 地址控制”窗口中设置 IP 地址区间。 3. 选中可登录的 IP 地址区间，单击“确定”。 如果设置多个 IP 地址区间，您可以选中 1 个或多个。

步骤 7 单击“完成”。

----结束

2.4.2 维护用户

用户创建后，安全管理员可以查看和修改用户信息。

前提条件

拥有维护用户权限的用户登录系统。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“权限分配 > 用户”。

步骤 3 在“用户”窗口中，可以进行下面操作。

操作名称	操作方法
查看	1. 选择需要查看的用户，单击用户名。 2. 查看相关信息。
修改	1. 选择需要修改信息的用户，单击“  ”。 2. 修改相关信息。 3. 单击“确认”。

操作名称	操作方法
重置密码	1. 选择需要修改密码的用户，单击“  ”。 2. 修改密码。 3. 单击“确认”。 **说明** 不可以修改系统缺省管理员的密码。
删除	1. 选择需要删除的用户，单击“ ”。 2. 确认系统提示。 **说明** 不可以删除系统缺省管理员和当前用户。
启用/停用	1. 选择需要启用/停用的用户，单击“  /  ”。 2. 在使用状态栏，显示当前用户使用状态。

----结束

2.5 用户访问控制

设置访问控制列表，使用户只能从特定 IP 地址和时间段登录服务器。用户访问控制列表由安全管理员设置。

2.5.1 登录时间控制

设置登录时间控制策略，使用户只能在设定的时间段登录服务器。登录时间控制策略由超级用户管理员设置。

前提条件

拥有登录时间控制权限的用户登录。

背景信息

默认策略不限制任何时间登录。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“访问控制 > 登录时间控制”。

步骤 3 在“登录时间控制”区域框中查看时间策略信息或执行如下操作。

设置登录时间控制信息	操作
创建登录时间控制策略	1. 单击“创建”。 2. 设置登录时间策略信息。 3. 单击“确定”。
修改登录时间控制策略	1. 在时间策略表格中，单击  。 2. 修改登录时间策略信息。 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	1. 在时间策略表格中，单击  。 2. 确认系统提示。 **说明** 默认策略不可以删除。

----结束

2.5.2 登录 IP 地址控制

通过设置登录 IP 地址，限制用户登录服务器。登录 IP 地址控制设置后将对所有用户生效，由“Administrators”的用户设置。

前提条件

拥有登录 IP 地址控制权限的用户登录。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“访问控制 > 登录 IP 地址控制”。

步骤 3 在“登录 IP 地址控制”区域框中查看系统访问信息或执行如下操作。

设置系统访问信息	操作
创建登录 IP 地址控制	1. 单击“创建”。 2. 设置参数。 3. 单击“确定”。

设置系统访问信息	操作
修改登录 IP 地址控制	1. 在登录 IP 地址控制列表中，单击  。 2. 修改登录 IP 地址控制信息。 3. 单击“确定”。
删除登录 IP 地址控制	1. 在登录 IP 地址控制列表中，单击。 2. 确认系统提示。

----结束

2.6 安全监控

介绍拥有超级管理员角色权限的用户监控 eSight 用户会话、操作、强制 eSight 用户退出和解锁 eSight 用户的操作。

2.6.1 监控用户会话

安全管理员通过监视用户会话，能了解当前系统中登录用户信息。

前提条件

- 会话是客户端和服务器端建立的连接。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 在左边导航树上选择“安全监控 > 监控用户会话”。

步骤 3 单击“刷新”。

步骤 4 查看在线的用户会话信息。

----结束

2.6.2 强制用户注销

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

前提条件

- 安全管理员可以执行强制注销操作。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。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“安全监控 > 监控用户会话”。

步骤 3 在需要其注销的用户一栏单击“强制注销”。

步骤 4 确认系统提示。

----结束

2.7 示例：创建网管用户并分配权限

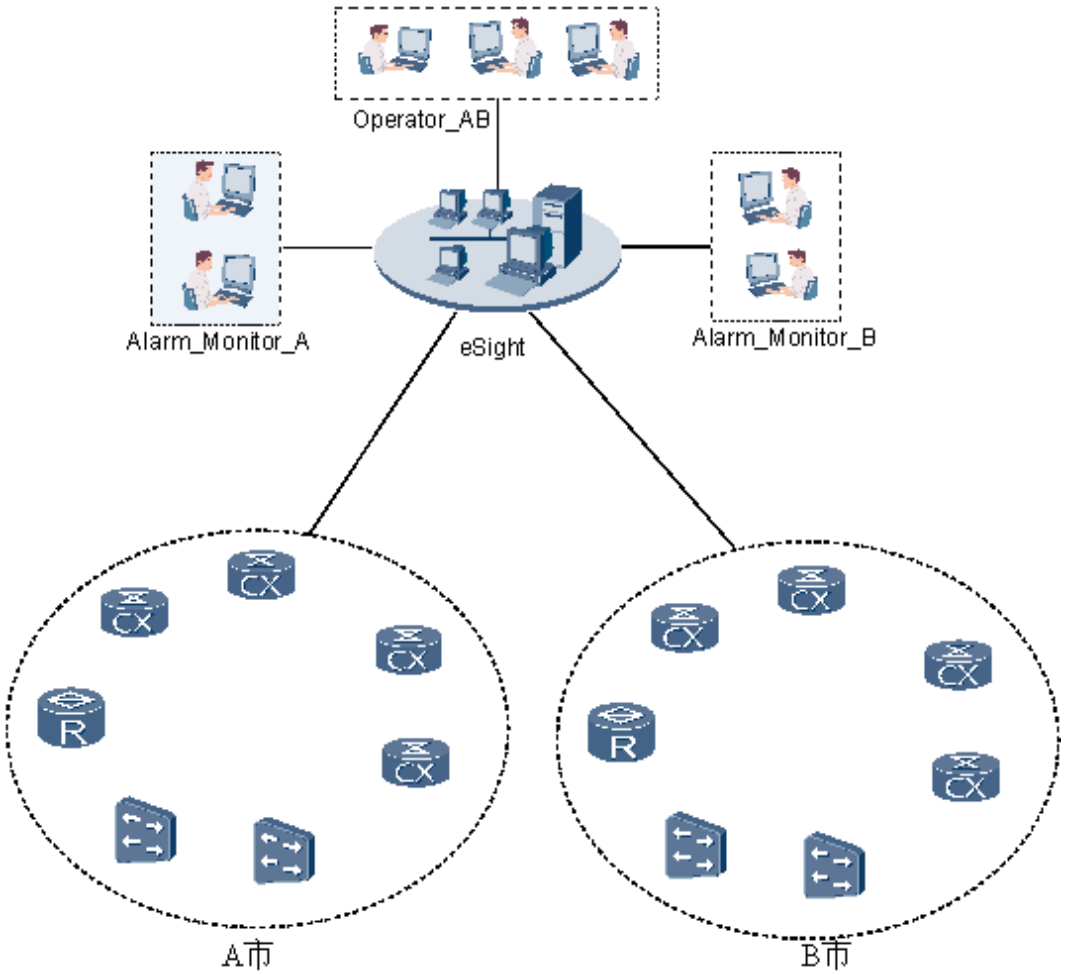
介绍分权分域场景下如何创建网管用户并分配权限。

场景介绍

某局点的网元通过 eSight 进行集中监控管理。该局点所管理的网元按照地域分属于 A 市和 B 市两个子网，分别有不同的人员负责对这些网元进行监控/维护。为了使不同的人员能够通过 eSight 对网元进行监控/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 2-1 所示。

图 2-1 分权分域组网图



数据规划

根据地域划分，规划 A 市/B 市两个子网。

根据角色职责的划分，规划以下 3 个角色：

表 2-2 角色规划

角色名称	职责说明	管理域	操作权限
Operator	负责 A 和 B 市网元的操作维护。	A 和 B 市网元	eSight 操作护员默认操作权限
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

角色名称	职责说明	管理域	操作权限
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 2-3 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。	操作员
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

在 eSight 上创建用户并分配相应权限的过程如下：

1. 新建 A 市子网和 B 市子网。
   (1) 在主菜单中选择“资源 > 资源管理”，在左侧导航树中选择子网父对象“Root”。
   (2) 单击“单个创建”，在“子网与解决方案类”下单击“子网”。
   (3) 设置“子网名”为“A 市”，单击“应用”。
   (4) 参考 **1.1** 至 **1.3** 创建 B 市子网。
2. 分别将 A/B 市网元添加到 A/B 市子网中。
   (1) 在左侧导航树中单击  ，弹出“移动树节点”窗口。
   (2) 在左侧的“要移动的节点”下，选择 A 市网元，在右侧的“目标容器节点”下选择“A 市”子网。
   (3) 单击“确定”，将 A 市的网元添加到 A 市子网中。
   (4) 参考 **2.1** 至 **2.3**，将 B 市的网元添加到 B 市子网中。
3. 分别创建 A 和 B 两市告警监视员角色，并分配角色的管理域、操作权限。
   (1) 在主菜单中选择“系统 > 安全管理”，在左侧导航树选择“权限分配 > 角色”。
   (2) 单击“创建”，设置“角色名”为“A 市告警监视员”，单击“下一步”。
   (3) 单击“增加”，在弹出的窗口中选择 A 市网元，单击“确定”。
   (4) 选择所有 A 市网元，单击“下一步”。
   (5) 单击“增加”，参考**表 2-2** 给出的操作权限，在弹出的窗口中选择相应的操作权限，单击“确定”。
   (6) 选择相应的操作权限，单击“下一步”。

(7) 单击“完成”，角色创建成功。

(8) 参考 3.1 至 3.7 创建 B 市告警监视员角色。

说明

操作员角色是 eSight 默认的角色，管理域默认是全网网元，操作权限也已默认提供，故不需要单独创建。

4. 分别创建用户 Operator_AB、Alarm_Monitor_A、Alarm_Monitor_B，设置用户所属的角色，这样各用户就可以具有角色的管理域和操作权限。

(1) 在左侧导航树选择“权限分配 > 用户”。

(2) 单击“创建”，设置“用户名”为“Operator_AB”，同时设置该用户的“密码”和“确认密码”。

(3) 所属角色设置为“Operator”，单击“下一步”

(4) 为了保证 eSight 的安全，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。

(5) 单击“完成”。

(6) 参考 4.1 至 4.5，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。

admin 用户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。

3 资源管理

关于本章

eSight 为用户提供针对网络中的资源进行统一查询和统计功能，支撑客户的业务规划和扩容计划。

3.1 资源管理
资源管理用于将资源接入 eSight 并对这些资源进行管理。

3.2 拓扑管理
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。通过拓扑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。

3.3 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。

3.4 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。

3.5 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。

3.1 资源管理

资源管理用于将资源接入 eSight 并对这些资源进行管理。

3.1.1 接入被管资源

当一个或多个资源需要在 eSight 上进行管理或监控时，请根据实际情况选择接入资源的类型和方式。

3.1.1.1 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，以使网络便于管理。在资源管理中，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。

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  将网元移动到新增子网中。
- 子网的层次不能超过 10 层。
- 每个子网中的网元数量不要超过 500 个。

操作步骤

步骤 1 选择“资源 > 资源管理”。

步骤 2 在左侧导航树中选择新增子网的父对象，在右侧单击“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。

系统显示“配置参数”页面。

步骤 4 配置子网参数。

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，则系统提示子网创建失败的原因。单击“确认”，重新配置参数。

----结束

3.1.1.2 创建网元

网元是 eSight 管理的各类设备的统称。通过创建网元，建立设备与 eSight 间的通信，从而实现对网元的管理。系统以不同的图标代表各种类型的网元。本章节中的网元都为实网元，即实际存在的设备。

?.1. 手工创建单个网元

当需要接入到 eSight 的网元个数较少，网元所属类型较多时，您需要以手工创建单个网元的方式将网元一一接入到 eSight 中。

操作步骤

步骤 1 选择“资源 > 资源管理”。

“资源管理”页面右侧列举出已接入的所有对象。

步骤 2 在左侧导航树中选择新增网元的父对象，在右侧单击“单个创建”。

步骤 3 在“选择类型”页面选择“Snmp 网络设备”。

系统显示“配置参数”页面。

步骤 4 配置网元参数。

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“确认”，重新配置参数。

----结束

?.2. 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接入网元比较繁琐，您可以选择手工批量导入网元方式批量添加网元。

操作步骤

步骤 1 选择“资源 > 资源管理”。

步骤 2 单击“批量导入”。

步骤 3 单击“导入主机及网络类设备”。

步骤 4 单击“模板下载”后的，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，选择所填写的 Excel 文件。

步骤 7 单击，上传文件。

“待导入的资源列表”中会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勾选网元，单击“创建”，系统开始导入网元。

- 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。

----结束

?.3. 自动发现网元

通过网元自动发现功能，eSight 可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索网元，并把发现的网元加入到 eSight 中。当指定网段中的所有网元都需要接入 eSight 时，该功能可以帮助您实现批量操作、节省时间。

操作步骤

步骤 1 选择“资源 > 资源管理”。

步骤 2 单击“自动发现”。

步骤 3 选择“网段发现”。

步骤 4 设置网段发现参数和 SNMP 协议参数。

为了操作快捷，可以使用已保存的 SNMP 协议模板来设置 SNMP 协议参数。

步骤 5 （可选）勾选“发现的对象自动添加到本网管系统中”前的多选框。

说明

- 如果勾选了“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。
- 如果不勾选“发现的对象自动添加到本网管系统中”，需要您执行步骤 7，添加发现的网元。

步骤 6 单击“开始发现”。

发现结果表格中显示自动发现的网元信息以及添加结果。

说明

发现过程中，可单击“停止发现”，终止发现操作。

步骤 7 在表格中勾选网元，单击“创建”。

如果勾选了“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”页面，管理对象表中可查看到添加的网元信息。

----结束

3.1.2 管理资源信息

管理资源信息是对接入系统的资源的信息进行查看、修改等操作。当不需要某个网元或子网时，可删除。

3.1.2.1 查看资源信息

资源的信息，包括资源的基本信息、协议信息等。

操作步骤

步骤 1 选择“资源 > 资源管理”。

“资源管理”页面右侧管理对象列表中显示已接入的所有对象。

步骤 2 **可选:** 在“搜索类型”下拉框中选择搜索类型，在“搜索条件”文本框中设置搜索条件，单击“搜索”，可过滤出符合条件的资源。

步骤 3 单击目标资源的资源名称，系统显示此资源的资源信息。

----结束

3.1.2.2 修改资源信息

您可以根据需要修改资源的属性，例如资源名称。

操作步骤

步骤 1 选择“资源 > 资源管理”。

“资源管理”页面右侧的管理对象列表中显示已接入的所有对象。

步骤 2 单击目标资源所在行对应的 。

步骤 3 修改资源的配置参数。

步骤 4 单击“确定”。

----结束

3.1.2.3 调整网元所属子网

通过移动网元所属子网，调整网元网络结构。

操作步骤

步骤 1 选择“资源 > 资源管理”。

步骤 2 在左侧的管理对象列表区域，单击 ，在“移动树节点”窗口中，进行调整网络结构。

步骤 3 在左侧区域框中选择需要移动的设备，在右侧选中目标容器节点。单击“确定”。

----结束

3.1.2.4 删除网元

当网络结构调整时，不再需要某些网元，可以将此删除。

操作步骤

步骤 1 选择“资源 > 资源管理”。

“资源管理”页面右侧的管理对象列表中显示已接入的所有对象。

步骤 2 在管理对象列表中删除目标网元。

- 单个删除：单击目标网元所在行对应的。
- 批量删除：勾选需要删除的目标网元，单击“批量删除”。

步骤 3 在弹出的“确认”对话框中单击“是”。

网元从管理对象列表中被删除。

----结束

3.1.2.5 删除子网

您可以根据实际情况对不需要 eSight 管理的子网进行删除操作。

操作步骤

步骤 1 选择“资源 > 资源管理”。

步骤 2 在管理对象列表中删除目标子网。

- 单个删除：单击目标子网所在行对应的。
- 批量删除：勾选需要删除的目标子网，单击“批量删除”。

步骤 3 在弹出的“确认”对话框中单击“是”。

子网从管理对象列表中删除。

----结束

3.2 拓扑管理

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。通过拓扑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。

3.2.1 了解拓扑管理

了解拓扑的基础知识将有助于您更好的进行拓扑管理的相关操作。

3.2.1.1 拓扑管理功能

了解 eSight 拓扑管理所提供的功能，将有助于您进行拓扑管理的规划和快速选择您所需的操作。

拓扑管理支持以下功能：

- 支持展示拓扑视图。用户可以根据实际需要来创建和组织拓扑视图。
- 支持以不同的图标标识不同的拓扑对象类型，并以小图标的形式标识拓扑对象的状态，如连接状态。
- 支持对拓扑视图中虚拟网元和链路的增加、删除等功能。
- 支持对拓扑视图中网元和子网的坐标位置的调整但不支持对链路的调整。
- 支持显示各个被管理对象的状态，如是否有故障、网元的连接状态等。
- 支持通过拓扑视图查询或浏览网元的告警信息。

- 支持根据用户权限过滤显示拓扑对象。
- 支持拓扑导航树对象展开、收缩、展开全部和收缩全部。
- 支持背景图的设置。通过拓扑图标在背景图中的位置，可以了解网元节点的大致位置信息。
- 支持拓扑放大、缩小、局部放大、恢复原始大小和调整到适合窗口功能，方便于查看网络拓扑结构。
- 支持全局和局部拓扑对象查找功能，便于定位拓扑对象。
- 支持鸟瞰、打印、导出等辅助功能，便于更好完成拓扑管理工作。

3.2.1.2 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。

子网

在网管系统中，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，以便于网络管理。这种相对较小的网络结构在 eSight 中称为子网。

网元

网元用于标识具体的实体设备，网元分为实网元和虚拟网元。

- 实网元：可以通过 eSight 进行管理，如路由器、交换机、AR 系列设备等。
- 虚拟网元：eSight 当前版本不支持管理的网元，可以创建为虚拟网元，用于网络拓扑图的构造，使您更清楚地了解整个通信网。

链路

链路是网元之间的连接在拓扑中的映射，链路分为实链路和虚链路。

- 实链路：实链路是指两个实网元之间存在的通信，用户可以在 eSight 上创建网元后，将实链路发现到网管上。
- 虚链路：虚拟链路是指两个网元（包括实网元和虚拟网元）之间存在逻辑通信，需要用户在 eSight 中手工创建。

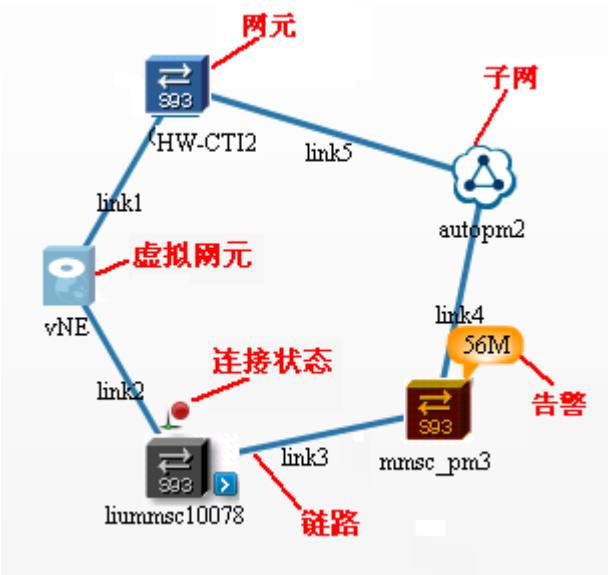
3.2.1.3 拓扑图例

eSight 使用不同的图标来表示子网、网元、链路以及他们的状态。在此给出一个拓扑图示例。

拓扑图

了解拓扑图中各对象及状态。

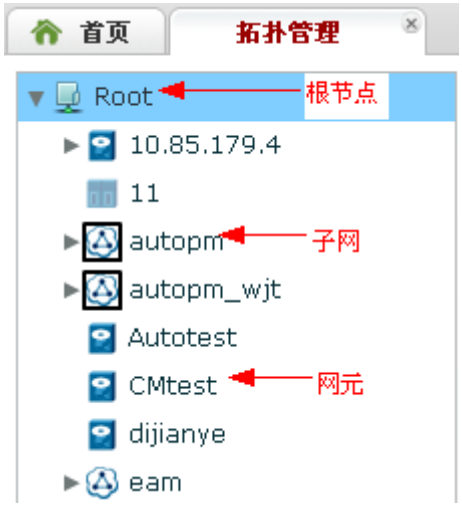
图 3-1 拓扑图



拓扑树图例

拓扑树中包含子网和网元，链路不在拓扑导航树中显示。

图 3-2 拓扑树图例



3.2.2 构建拓扑

拓扑图直观的反映了各个拓扑对象直接的关系。拓扑图中的网元、子网统称为拓扑对象。

3.2.2.1 创建虚拟网元

虚拟网元是指整个网络中不能通过 eSight 进行管理的设备的映射。通过将虚拟网元添加到拓扑视图中，您可以更清楚地了解整个网络的情况。

背景信息

虚拟网元无任何管理功能。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 单击拓扑工具栏中的  图标，选择待创建的虚拟网元在拓扑视图中的位置后单击。

说明

再次单击  图标，可取消创建。

步骤 3 在弹出的“创建虚拟网元”对话框中设置参数。

步骤 4 单击“确认”。
所创建的虚拟网元呈现在拓扑图中。

----结束

3.2.2.2 创建链路

链路用来标识拓扑对象之间的物理或者逻辑连接。您可以根据需要在拓扑图中的任意两个拓扑对象之间创建链路，更好的体现拓扑对象之间的关系。

背景信息

- 链路不在拓扑导航树中显示，只在拓扑图中显示。
- 两个拓扑对象间支持多条链路。
- 只能在网元或子网之间创建链路，链路的两端不能为链路。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 单击工具栏中的  图标。

说明

再次单击  图标或单击拓扑图空白处，可取消创建。

步骤 3 在拓扑视图中选择链路的起始网元和目标网元。
新建链路的两个拓扑对象之间会出现连接线。

步骤 4 在弹出的“输入添加链路名称”对话框中输入链路名称。

步骤 5 单击“确认”。

链路创建成功。

----结束

3.2.2.3 调整网元位置

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

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 在拓朴图中调整网元位置。

- 单个移动网元：在拓扑图中单击某个网元，按住鼠标并将网元拖动至指定位置。
- 批量移动网元：按住“Ctrl”在拓扑图中选中多个网元，按住鼠标并将网元拖动至指定位置。

步骤 3 在拓扑工具条上单击  ，保存调整后的网元位置。

----结束

3.2.2.4 调整子网

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

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 在拓扑图中单击某个子网，按住鼠标并将子网拖动至指定位置。

步骤 3 在拓扑工具条上单击  ，保存调整后的子网位置。

----结束

3.2.3 管理拓扑对象

在构建好拓扑视图后，您可以根据实际需要对拓扑对象进行管理。

3.2.3.1 删除链路

当网络结构调整时，不再需要某些链路，可以将其从拓扑视图中删除。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 在拓扑视图中选中目标虚拟链路，单击，选择“删除虚拟链路”。
目标虚拟链路从拓扑图中删除。

----结束

3.2.3.2 删除虚拟网元

当网络结构调整时，不再需要某些虚拟网元，可以将其从拓扑视图中删除。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 在拓扑视图中选中目标虚拟网元，单击，选择“删除虚拟网元”。
目标虚拟网元从拓扑图中删除。

----结束

3.2.3.3 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 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 在前设置搜索条件。

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。
系统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 选择某个拓扑对象，在拓扑图中快速定位到此对象。

----结束

3.2.3.4 设置拓扑背景图

您可以根据设备的布局设置合适的背景图。通过背景图和设备位置的恰当设置，可以帮助您直观地了解设备所在的位置。

背景信息

导入拓扑背景图时图片的文件格式需为以下格式的一种：

- *.jpg

- *.jpeg
- *.gif
- *.png
- *.JPG
- *.JPEG
- *.GIF
- *.PNG

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 在拓扑工具条中单击  。

步骤 3 在“设置背景图”对话框中，选中“显示背景图”，单击  ，选择目标图片导入系统中。

说明

如果设置的背景图不需要展示在拓扑图中，请勾选“不显示背景图”。

步骤 4 单击“确认”。

拓扑背景图显示为设置后的图片。

----结束

3.2.3.5 缩放拓扑视图

您可以根据需要缩小、放大和实际大小显示。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 选择以下方式缩放拓扑视图。

- 单击拓扑工具条上的  ，放大拓扑视图。
- 单击拓扑工具条上的  ，缩小拓扑视图。
- 单击拓扑工具条上的  ，还原拓扑视图。

----结束

3.2.3.6 保存拓扑图

当拓扑图中拓扑对象位置发生改变后，您可以根据需要对改变后的拓扑图进行保存。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 修改拓扑图中网元位置。

步骤 3 单击工具栏中的  ，保存拓扑图。

----结束

3.2.3.7 布局拓扑对象

当拓扑视图中的子网或者网元的展示布局混乱时，您可以通过拓扑布局功对拓扑对象进行重新布局。

背景信息

- 选中部分拓扑对象，则只针对选中的拓扑对象进行布局。
- 没有选中任何拓扑对象，则对拓扑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：将拓朴对象排列成环形。
  - 对称：将拓朴对象排列成对称。
  - 上下树形：将拓朴对象排列成上下树形。
  - 下上树形：将拓朴对象排列成下上树形。
  - 左右树形：将拓朴对象排列成左右树形。
  - 右左树形：将拓朴对象排列成右左树形。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。

系统显示“拓扑管理”界面。

步骤 2 在拓扑视图中选择需要布局的拓扑对象，单击拓扑工具条中的  ，选择拓扑对象布局方式。

拓扑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  ，保存布局后各节点新的坐标位置。

----结束

3.2.3.8 全屏/鸟瞰查看拓扑图

您可以通过鸟瞰图浏览拓扑视图的全貌，并定位拓扑窗口所显示的区域，也可以全屏显示拓扑视图。

背景信息

分辨率的大小按照您当前使用机器的屏幕实际设置而定，并不总是 1024*768 像素。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 单击拓扑视图右下角的  。
系统显示鸟瞰图，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 单击  ，关闭鸟瞰图。

步骤 5 单击拓扑工具条上的  ，全屏显示拓扑视图。

说明

- 单击该按钮后，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

3.2.3.9 显示拓扑图例

通过拓扑图例可了解拓扑视图中拓扑对象颜色或状态的含义。

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 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 选择“  > 显示图例”。

通过图例的颜色可以查看到拓扑视图中各个对象或状态的含义。

----结束

3.2.3.10 设置设备标签

您可以通过设置设备标签，显示设备的名称和 IP 地址等。

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 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 选择“  > 设备标签”。

步骤 3 在“设置设备标签”窗口中，选择设备标签的内容。

步骤 4 单击“确定”，在设备上显示所选择设备标签的内容。
当设备标签内容未配置时，系统缺省显示设备的名称。

----结束

3.2.3.11 打印拓扑视图

打印拓扑视图功能可以将拓扑视图打印到纸件或文件中。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 单击工具栏中的  。

步骤 3 设置打印参数。

步骤 4 单击“确定”。

----结束

3.2.3.12 导出拓扑视图

您可以根据需要将拓扑视图导出到本地。

操作步骤

步骤 1 选择“资源 > 拓扑管理”。
系统显示“拓扑管理”界面。

步骤 2 单击工具栏中的  。

步骤 3 选择拓扑视图的保存路径和文件格式。

步骤 4 单击“保存”。
拓扑视图以文件形式保存到指定位置。

----结束

3.3 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 3-1。

表 3-1 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。

3.4 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“完成”。

表 3-2 发现 LLDP 链路命令

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 3-2 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 3-2 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。

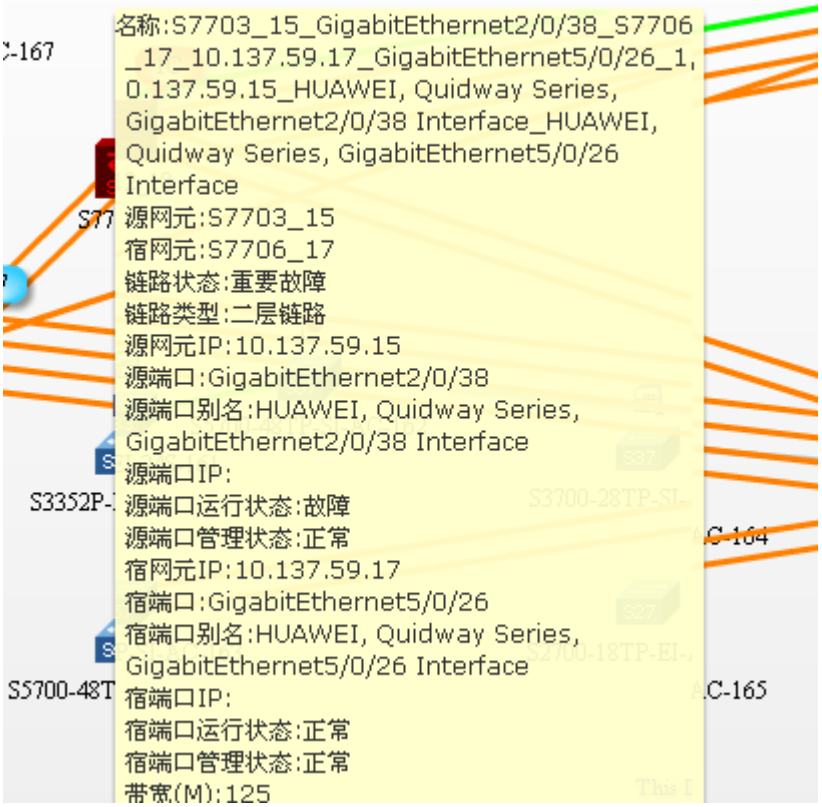
步骤 4 **可选:** 单击“显示规则”，设置链路的显示规则。

1. 在“名称规则”下设置链路名称的显示字段。
   设置完名称规则后，可在“链路管理”界面下的“名称”进行验证。

2. 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。



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”。

步骤 6 **可选:** 根据需要，选择待删除的链路，单击“删除”,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。

----结束

3.5 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。

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

4 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，提供了监控网络告警、查询告警/事件和设置告警通知等管理功能。

说明

网管要管理设备的告警，必须先配置设备上报的 Trap 报文的目的 IP 地址为网管服务器的 IP 地址。

4.1 了解故障管理
了解故障管理功能以及相关的概念，如“告警级别”、“告警状态”、“告警”和“事件”的定义等，有助于您进行故障管理的相关操作。

4.2 监控网络告警
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。

4.3 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、定位告警和清除告警等。

4.4 管理告警数据
为了避免数据库空间不足，可以通过溢出转储及时清理数据库中的告警数据。

4.5 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。

4.6 设置告警屏蔽
对于网元上报到 eSight 不需要关注的告警，可以通过在 eSight 中设置屏蔽规则列入到被屏蔽告警列表中。

4.7 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。

4.1 了解故障管理

了解故障管理功能以及相关的概念，如“告警级别”、“告警状态”、“告警”和“事件”的定义等，有助于您进行故障管理的相关操作。

4.1.1 故障管理功能

故障管理功能主要包括显示和统计告警、清除告警和确认告警等。

显示和统计告警

eSight 实时接收被管理网元产生的告警，并提供多种方式显示和统计告警。

表 4-1 显示和统计告警的方式

显示和统计告警的方式	说明
告警板	告警板分级别显示当前告警列表中的告警数量，提供整个网络的故障状况。告警板可作为监视面板。
告警柱状图	告警柱状图是 eSight 提供的一个告警展示窗口。告警柱状图以图形和数字方式显示出被管理对象的不同级别和状态的告警，提供整个网络的简要故障状况。告警柱状图可作为监视面板。
查询告警	eSight 支持浏览当前告警、查询历史告警和查询事件等，在当前告警列表中显示当前需要关注和处理的告警。

清除告警

对一些无法自动清除的告警或者确认已不存在的告警，在 eSight 上可以手工清除。

确认告警

确认告警以标识某条告警已经被用户处理，可以不必过多关注。如果要重新关注该告警，可以对该告警进行反确认操作并采取相应的处理措施。

屏蔽告警

可以设置屏蔽规则，屏蔽符合屏蔽规则的告警。被 eSight 屏蔽的告警可以在被屏蔽的告警列表中查看该告警的信息。

告警远程通知

当符合条件的告警发生时，自动通过邮件或短消息通知给设定的维护人员，以便维护人员及时了解告警信息并采取相应措施。

4.1.2 告警级别

根据告警的严重性，告警级别分为紧急、重要、次要和提示。根据不同的告警级别您可以采取对应的处理策略。

表 4-2 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，以防止更为严重的故障的发生。
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。

4.1.3 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。

表 4-3 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

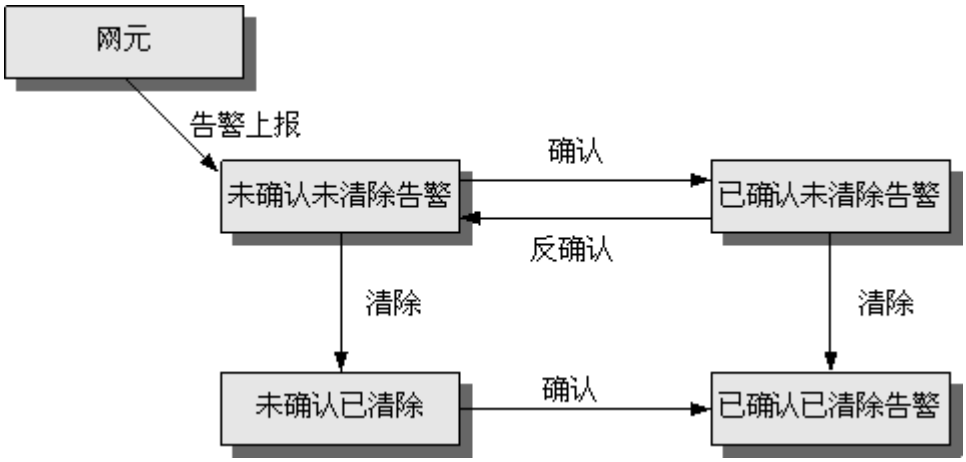
表 4-4 告警状态转换分类

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，网元或 eSight 服务器恢复正常，此时网元或 eSight 服务器将上报对应的清除告警，告警由**未清除**状态变成**清除**状态。

告警状态转换类别	说明
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下图所示。

图 4-1 告警状态转换关系模型



4.1.4 告警和事件

介绍告警和事件在 eSight 中的相同点和区别。

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

告警是指系统检测到故障而产生的通知。

事件是指被管对象发生的任何情况的统称。

两者的区别在于：

- 告警是事件的特例。eSight 产生了异常或故障，否则会导致由于 eSight 或设备的功能异常而引起业务的异常。用户必须要处理发生的告警。
- 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。

4.2 监控网络告警

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。

4.2.1 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。

背景信息

在拓扑视图中，网元的图标上会显示与产生告警级别相对应的颜色。如果该网元同时产生多个告警，网元图标上将显示其中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 Tips 信息和网元位置。

- 通过 Tips 信息了解到告警的清除状态、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。

----结束

4.2.2 通过资源管理器监控告警

通过监控网元状态查看 eSight 所管理的网元的名称、类型、告警级别和连接状态，可以了解网元当前运行状况，以便及早发现并解决异常。

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”窗口中选中一条告警，在操作栏中单击  。

说明

在“拓扑管理”窗口中，显示了 eSight 管理的网元的信息。

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

在“当前告警”窗口中查看到该网元告警信息。

----结束

后续处理

在告警管理中查看当前告警、历史告警和被屏蔽告警。“当前告警”窗口中显示该网元产生的所有告警，并且可以进行确认清除等操作。

4.2.3 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。

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紧急告警、重要告警、次要告警、提示告警、清除告警和所有告警信息。

说明

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

4.2.4 查询告警

在 eSight 可以通过浏览当前告警、查询被屏蔽告警和查询历史告警等方式进行查询告警。

4.2.4.1 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。

背景信息

- 对于新上报的告警，只要告警列表中存在符合归并规则的告警记录，都将该告警归并到告警列表中，归并后告警次数加一，当前告警列表是告警归并后的展示。

  默认的告警归并规则：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。
- 在“当前告警”窗口中可以查看每条告警的信息。
- 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。
- 在浏览当前告警时，通过单击  定制显示列。

操作步骤

步骤 1 在主菜单中选择“故障 > 当前告警”。

步骤 2 在“过滤条件”下拉菜单中，选择条件进行查询，如果不满足需求可以自定义过滤条件，请参见 4.2.4.5 设置告警自定义过滤条件。

步骤 3 在“当前告警”窗口中，可进行如下操作。

表 4-5 “当前告警”窗口操作

操作名称	操作方法	说明
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。 ● 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。 状态： ● 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	在窗口中支持如下搜索方式： ● 不设置任何条件直接点击“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”。	● 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”。	通过反确认后，告警由确认状态变成未确认状态。
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”。	● 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。

操作名称	操作方法	说明
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。
拓扑定位	在窗口中选择一条告警，在操作栏中单击 。	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

4.2.4.2 查询历史告警

通过设置历史告警查询条件，您可以快速找到您所关注的历史告警。

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。

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 在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”对话框中进行选择需要查询的子网或网元。

说明

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”：输入查询的历史告警名称。
- “时间范围”：输入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”：勾选需要查询历史告警的级别。

步骤 3 在搜索结果窗口中，可以进行如下操作。

操作名称	操作方法
告警详细信息	在窗口中选中需要查看的告警，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。
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”，导出选择月份中的告警的相关信息。 **说明** 如果需要导出全部可以直接单击“导出 > 导出全部”。 只能导出所选择月份的历史告警，非所有的历史告警。

----结束

4.2.4.3 查询事件

通过查询事件信息，可以查看到设备侧向 eSight 发送的具体通知消息。

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 在搜索栏中设置搜索信息，单击“搜索”。

步骤 3 在搜索结果窗口中，可以查看事件信息。

----结束

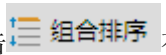
4.2.4.4 查询被屏蔽告警

通过下面操作，可以查询被屏蔽的告警信息。

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  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。

  说明

  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”：输入查询的被屏蔽告警名称。
- “首次发生时间”：输入该告警第一次被屏蔽的时间。
- “告警级别”：勾选需要查询被屏蔽告警的级别。

步骤 3 在搜索结果窗口中选中需要查看的告警，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。

----结束

4.2.4.5 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。

背景信息

系统默认有以下过滤条件：

- 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

系统默认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“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”窗口中，可以进行如下操作。

操作名称	操作方法
创建	1. 单击“创建”，在右边区域框中设置名称、告警级别、清除状态、事件类型和首次发生时间。 2. 单击“保存”。 在右边窗口中，提示添加成功。
删除	1. 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”。 2. 在“确认”对话框中单击“是”
修改	1. 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、清除状态、事件类型和首次发生时间。 2. 单击“保存”。 在右边窗口中，提示修改成功。
复制	1. 在左边过滤条件列表中选中过滤条件，单击“复制”，在右边窗口中设置名称、告警级别、清除状态、事件类型和首次发生时间。 2. 单击“保存”。 在右边窗口中，提示添加成功。

----结束

4.3 处理告警

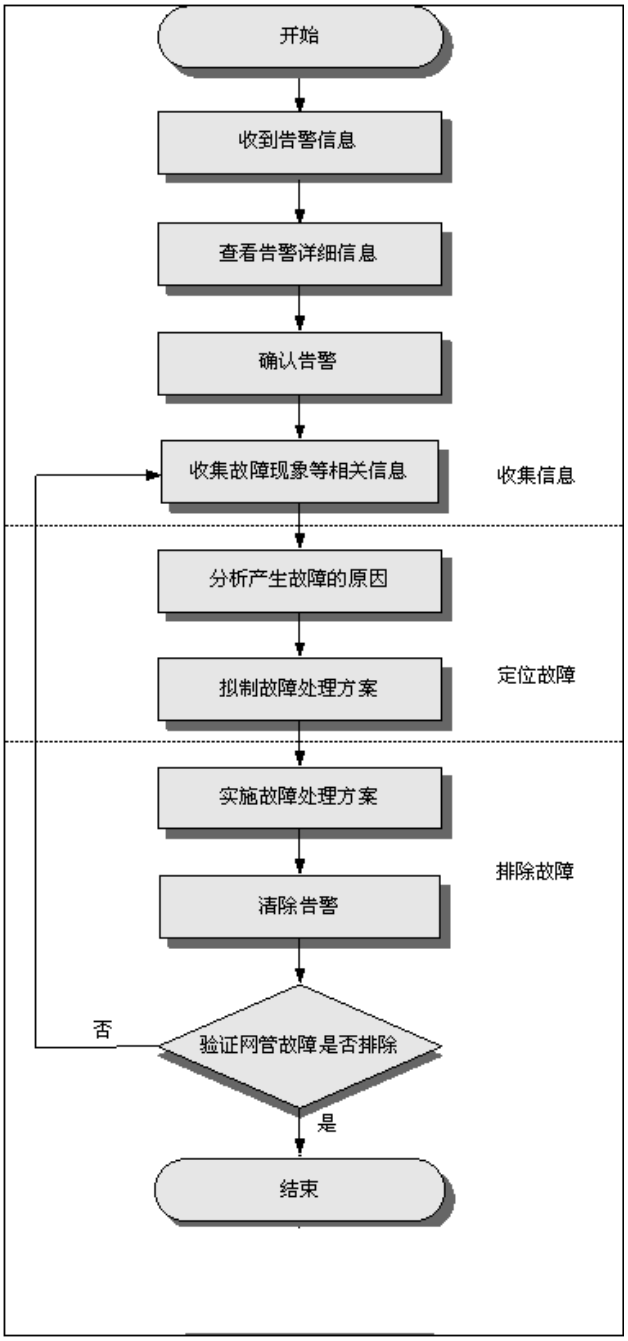
在发现告警信息后，需要按照流程来处理告警以排除故障。处理告警的操作包括查看告警详细信息、确认告警、定位告警和清除告警等。

4.3.1 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 4-2 告警处理流程



流程说明

表 4-6 告警处理流程说明

步骤	操作	说明
1	收到告警信息	管理员收到告警信息后，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。
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信息。
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，分析出产生故障的现象。
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 eSight 故障是否排除	故障排除后，需要验证故障处理效果。

4.3.2 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 4-7 告警详情参数

参数	说明
告警名称	告警对象的故障现象的简要描述。
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。

参数	说明
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	清除告警的网管的用户标识符。当网元自动清除告警时，该参数值不存在；当网管主动清除告警时，该参数值为发出清除操作的网管的用户标识。
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。
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。

参数	说明
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。

4.3.3 确认告警

标识某条告警已经被用户处理，不必过多关注。

背景信息

- 已确认告警：在“确认用户”栏中显示确认用户 ID。
- 未确认告警：在“确认用户”栏中显示  。

操作步骤

步骤 1 在主菜单中选择“故障 > 当前告警”。

步骤 2 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：**4.2.4.5 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”栏显示确认用户 ID。

----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。

4.3.4 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。

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 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：**4.2.4.5 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”。

该告警背景颜色为绿色。

----结束

4.3.5 示例：告警处理

本主题通过一个对磁盘占用率过高告警处理的示例，展示了告警处理的流程和方法。通过本示例，可以了解告警处理的基本流程和操作。

背景介绍

管理员小王发现 eSight 有新的告警提示。

操作指导

小王根据告警处理流程对该告警进行了以下处理（告警处理流程请参见 **4.3.1 告警处理流程**）：

1. 收到告警通知

   选择“故障 > 当前告警”，在“当前告警”窗口中发现有“未清除的磁盘占用率过高告警”。
2. 查看告警详细信息

   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。
3. 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。
4. 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。
5. 排除告警故障

   将非 eSight 自带的冗余文件删除，将导出文件备份到其它磁盘上，并将原磁盘上的导出文件删除。查看 eSight 服务器的磁盘空间，已经获得了较大的可用磁盘空间。
6. 验证处理结果

   选择“故障 > 历史告警”，可以查看到原来的“未清除的磁盘占用率过高告警”。

4.4 管理告警数据

为了避免数据库空间不足，可以通过溢出转储及时清理数据库中的告警数据。

4.4.1 设置告警溢出转储

为了避免数据库表空间不足，eSight 系统提供了告警溢出设置功能。系统可以按照条件每日检测告警数据是否溢出，如果溢出，则系统自动将数据转储到您指定路径下进行保存。

背景信息

数据库表空间使用率超出设置的数据库空间阈值，说明数据溢出。

eSight 每日在设置的时刻检测数据库中告警管理表空间的使用率，如果使用率超过阈值，系统按告警上报月份的先后顺序将最早月份上报的告警数据（包括历史告警、已清除的被屏蔽告警和事件列表数据）转储到设置的保存文件路径下，并将这些数据从数据库中删除，直到使用率低于阈值。转储后系统会检测转储目录中文件的总大小和保存时间，如果文件的总大小或者文件保存的时间超过设置的值，系统将删除最早的转储文件，直到满足设置的值。

操作步骤

步骤 1 选择“系统 > 系统配置”。

步骤 2 在左侧导航树中选择“数据库溢出转储 > 告警数据库溢出转储”。

步骤 3 设置告警转储参数。

说明

“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网管安装路径“%ENT_ROOT%/run/dump”（以 LWindows 操作系统为例）而言，例如输入 AAA，则表示文件将保存到“%ENT_ROOT%/run/dump/AAA”下。

步骤 4 单击“应用”。

----结束

4.5 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。

4.5.1 设置邮箱服务器

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

背景信息

在设置邮箱服务器时，需要知道 SMTP 服务器 IP 地址和发件箱地址。

- “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”：选中需要检查权限后，检查是否当前用户是否可以进行发送邮件。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“远程通知 > 邮箱服务器”。

步骤 3 设置参数。

步骤 4 单击“应用”。

您可以单击“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。

----结束

4.5.2 设置短消息服务器

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

背景信息

在设置短消息服务器时，需要知道主机名、端口、编码协议和主叫号码信息。

- 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：短信中心的编码协议。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“远程通知 > 短消息服务器”。

步骤 3 在“短消息服务器设置”窗口中设置主机名、端口和短消息通知主叫号码等信息。

如果需要支持长短信和状态恢复。可以单击“高级设置”选中是否支持。

选择不同协议支持的短信长度不一样。

表 4-8 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。

协议类型	是否支持长短信
CMPP2_x/ CMPP3_x	● 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。
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”。

您可以单击“测试”，检测与该短信服务器是否连通，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。

----结束

4.5.3 设置内容模板

您可以定制上报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。

背景信息

eSight 会按照定制的信息内容模板发送用户需要关注的信息。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“远程通知 > 通知内容模板”。

步骤 3 在“通知内容模板设置”窗口中可以设置告警内容模板和事件内容模板，单击“应用”。

单击  ，选择设置告警内容模板或事件内容模板。

- 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。

说明

- 在右侧“已选择的告警字段”区域中，对不同的“字段名”可输入不同的字段前缀信息，即成为告警转短信时各个字段的前缀，它会加到告警信息各字段的最前处然后转短信。
- 在右侧“已选择的事件字段”区域中，对不同的“字段名”可输入不同的字段前缀信息，即成为事件转短信时各个字段的前缀，它会加到事件信息各字段的最前处然后转短信。

----结束

4.5.4 设置用户组

在告警远程通知设置时，需要设置远程通知的用户组。

背景信息

在用户组的设置中，可以对用户组进行新增、查看、修改和删除。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“远程通知 > 通知用户组”。

步骤 3 在“通知用户组”窗口中，可以进行如下操作。

操作名称	操作方法
新增用户组及组内成员	在窗口中单击“创建”，设置用户组信息，单击“保存”。 ● 添加成员需要通过单击“创建”进行添加新的成员，需要设置用户名、手机号码和邮箱地址。 ● 可以对新添加的用户组，在“创建用户组”窗口中，进行修改和删除信息。
查看用户组及组内成员	选中一条用户组信息，在用户组名栏中单击“用户组名”，在“查看用户组”窗口中，查看到用户组的详细信息。
修改用户组及组内成员	选中一条用户组信息，在操作栏中单击“”，可以对用户名、描述和成员进行修改。 修改成员，包括对成员进行增、删、改操作。
删除用户组	选中一条用户组信息，在操作栏中单击“”，并确认系统提示。

----结束

4.5.5 设置远程通知规则

通过设置告警远程通知规则，系统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。

背景信息

系统支持“按告警级别设置”和“按具体告警设置”两种方式来新增通知规则。

- 按告警级别设置：当指定级别的告警产生或清除时，系统向指定的用户组发送远程通知。
- 按具体告警设置：当指定设备的指定告警产生或清除时，系统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 在左边导航树上选择“远程通知 > 远程通知规则”。

步骤 3 在“远程通知规则”窗口中，可以进行下面的操作。

操作名称	操作方法
新增	在窗口中单击“创建”，可以通过“按告警级别”和“按具体告警”方式来新增通知规则。 ● 选择按告警级别： 在“按告警级别”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，可以点击 通知多个用户组。 ● 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：**4.5.4 设置用户组**。 ● 选择按具体告警： 请参见：**4.5.6 按具体告警设置远程通知规则**
启用	在窗口中，选中一条或者多条通知规则单击“启用”，启用该规则进行远程通知。
停用	在窗口中，选中一条或者多条通知规则单击“停用”，停用该规则进行远程通知。
修改	在窗口中，选中一条规则单击“ ”，修改选择选中的规则信息。请参见新增操作设置。
删除	在窗口中，删除通知规则信息。 选中一条通知规则信息，在操作栏中单击“ ”，确认系统提示。

----结束

4.5.6 按具体告警设置远程通知规则

通过选择具体的告警源、告警和通知用户组来设置通知规则。

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 在左边导航树上选择“远程通知 > 远程通知规则”。

步骤 3 单击“创建”选择“按具体告警”。

步骤 4 设置“规则名称”，然后单击“添加告警源”。

步骤 5 在子网列表中选择告警源，单击“确定”。

1. 在“子网列表”区域框中，选择子网。
   - 选择“Root”节点，在“告警源”区域框中，显示所有的告警源。
   - 选择具体子网，在“告警源”区域框中，显示该子网下所有的告警源。
   - 在子网中选择具体的网元后，在子网右上方会显示红星号，标示在该子网下选择了告警源。
2. 在“告警源”区域框中，选择具体的告警源。
   - 单击“全选/清空”，将选中/清空选中“告警源”区域框中的所有告警源。
   - 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”区域框中。

步骤 6 单击“下一步”。

步骤 7 单击“添加告警和事件”。

步骤 8 选择告警和事件，单击“确定”。

1. 在“设备类型”区域框中，选择设备类型。
   - 选择具体设备类型，在“告警列表”区域框中，显示该子网下所有设备类型。
   - 在“设备类型”的右上方会显示红星号，标示在该“设备类型”下选择了告警/事件。
2. 在“告警列表”或“事件列表”区域框中，选择具体的告警/事件。
   - 单击“全选/清空”，将选中/清空选中“告警源”区域框中的所有告警源。
   - 根据需要可以选择多个子网下的多个告警/事件，已经选择过的告警/事件将不会出现在子网中。
   - 在“告警列表”区域框中，设置告警级别列出告警，选择需要关注的告警。
   - 在“事件列表”区域框中，选择需要关注的事件。

步骤 9 单击“下一步”。

步骤 10 设置通知用户组，单击“完成”。

----结束

4.6 设置告警屏蔽

对于网元上报到 eSight 不需要关注的告警，可以通过在 eSight 中设置屏蔽规则列入到被屏蔽告警列表中。

背景信息

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。时段分为“全时段”和“分时段”如下：

- “全时段”：指定日期内所有的时间内有效。
- “分时段”：指定日期内指定的时间范围内有效。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“基础设置 > 屏蔽规则”。

步骤 3 在“屏蔽规则”窗口中，可以进行如下操作。

操作名称	操作方法
新增	单击“创建”新增一条屏蔽规则，请参见：4.6.1 新增告警屏蔽规则。 **说明** 在当前告警窗口中，对已上报的告警新增屏蔽规则。该屏蔽规则对后续上报的告警生效。
启用	选中一条规则，单击“启用”。 在启动状态栏中显示“已启动”，表示该规则已启用，后续上报的告警会按照此规则进行屏蔽。
停用	选中一条规则，单击“停用”。 在启动状态栏中显示“未启用”，表示该规则处于停用状态。
删除	选择一条规则，在操作栏中单击“  ”并确认系统提示。
修改	选中一条规则，在操作栏中单击“  ”并设置相关参数。

----结束

4.6.1 新增告警屏蔽规则

通过新增告警屏蔽规则并启用该规则，将该屏蔽规则生效后接收到的告警，将符合告警屏蔽规则的告警列入被屏蔽告警列表中。

背景信息

时间分为“全时段”和“分时段”如下：

- “全时段”：指定日期内所有的时间内有效。
- “分时段”：指定日期内指定的时间范围内有效，可以添加多个分时段。

操作步骤

步骤 1 在主菜单中选择“故障 > 告警设置”。

步骤 2 在左边导航树上选择“基础设置 > 屏蔽规则”。

步骤 3 单击“创建”。

步骤 4 设置“规则名称”、“日期”和“时间”，单击“下一步”。

步骤 5 单击“添加告警源”，设置告警源，单击“确定”。

1. 在“子网列表”区域框中，选择子网。
   - 选择“Root”节点，在“告警源”区域框中，显示所有的告警源。
   - 选择具体子网，在“告警源”区域框中，显示该子网下所有的告警源。
   - 在子网中选择具体的网元后，在子网右上方会显示红星号，标示在该子网下选择了告警源。
2. 在“告警源”区域框中，选择具体的告警源。
   - 单击“全选/清空”，将选中/清空选中所有告警源。
   - 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”区域框中。

步骤 6 单击“下一步”。

步骤 7 单击“添加告警”，设置告警，单击“确定”。

1. 在“设备类型”区域框中，选择设备类型。
   - 选择具体设备类型，在“告警列表”区域框中，显示该子网下所有设备类型。
   - 在“设备类型”的右上方会显示红星号，标示在该“设备类型”下选择了告警。
2. 在右侧区域框中，选择具体的告警。
   - 单击“全选/清空”，将选中/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。

步骤 8 单击“完成”。

----结束

4.7 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。

背景信息

- 系统默认告警声音为“启动状态”。
- 系统分别为不同级别的告警声音值默认设置为：
  - “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“故障管理 > 告警设置”。

步骤 2 在左边导航树上选择“基础设置 > 告警声音”。

步骤 3 在“告警声音”窗口中，可以进行如下操作。

- 选择“告警级别”前面的复选框，单击“停用”，对选中的“告警级别”停止使用告警声音。
- 选择“告警级别”前面的复选框，单击“启用”，对选中的“告警级别”启用使用告警声音。
- 单击“试听”，试听告警声音。
- 在操作栏中单击“告警声音设置”，在“告警声音设置”窗口中，选择“告警声音”和“告警次数”，单击“保存”。

说明

单击“恢复默认设置”可以将告警声音恢复为默认设置。

----结束

5 性能管理

关于本章

性能管理能为网络管理、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。

5.1 了解性能管理

介绍在进行具体的性能监视操作前用户需要掌握的相关基本概念。

5.1.1 性能事件与性能指标

网络在正常运行的过程中，因为内部与外部的原因，可能会影响传输质量，造成传输损伤。这些损伤的体现就是各种类型的性能事件。

性能事件

性能与告警不同，上报性能事件时业务并没有发生中断，但此时传输的质量相比正常情况下已经劣化，只是由于设备自身的纠错机制，暂时弥补了这些劣化。但是这些因素逐步的积累，最终将会导致性能越限，进而产生阈值告警。

通过性能管理可以提前发现这种劣化的趋势，并在故障发生前解决掉这些隐患。

性能指标

性能指标与资源相关。CPU、内存是资源，而指标是监视资源的性能数据，例如 CPU 占用率、内存占用率等。性能监视时会采集监视资源的性能数据并进行计算。可通过修改性能指标的阈值来控制是否上报告警以及上报的告警级别。

5.1.2 性能门限

通过设置性能门限可以屏蔽在正常区间内变化的性能事件，使用户集中精力关注严重劣化的性能事件。

性能门限即满足网络正常工作的设备性能阈值。引入性能门限的目的是判断设备是否工作正常。当某一性能指标测量值超出预期的性能门限，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。而当测量值降低到性能门限允许的范围内时，产生的 Qos 告警会被清除。

正常情况下，设置性能门限时需要预留一定的余量，以保证可以提前发现问题。

5.1.3 最近性能和历史性能

网络运维人员通过查询最近性能和历史性能的统计数据，能够对网络或业务历史运行情况进行统计分析。

最近性能

最近性能是指在性能管理中能实时监视到的性能数据，并且能够通过性能监视视图进行浏览。最近性能在性能监视视图中是动态变化，实时更新的。在性能监视视图中浏览最近性能时，支持在一个监视视图中选择多个网元或指标进行监视，可以是对多个网元同类指标的对比监视，也可以是对一个网元多个相关指标的集中监视。

历史性能

历史性能是指过去一段时间内从网元检测到的性能数据，查询条件有对象类型、对象实例、测量单元、测量对象、时间段等，历史性能统计数据支持数据列表展示和数据趋势曲线图展示。

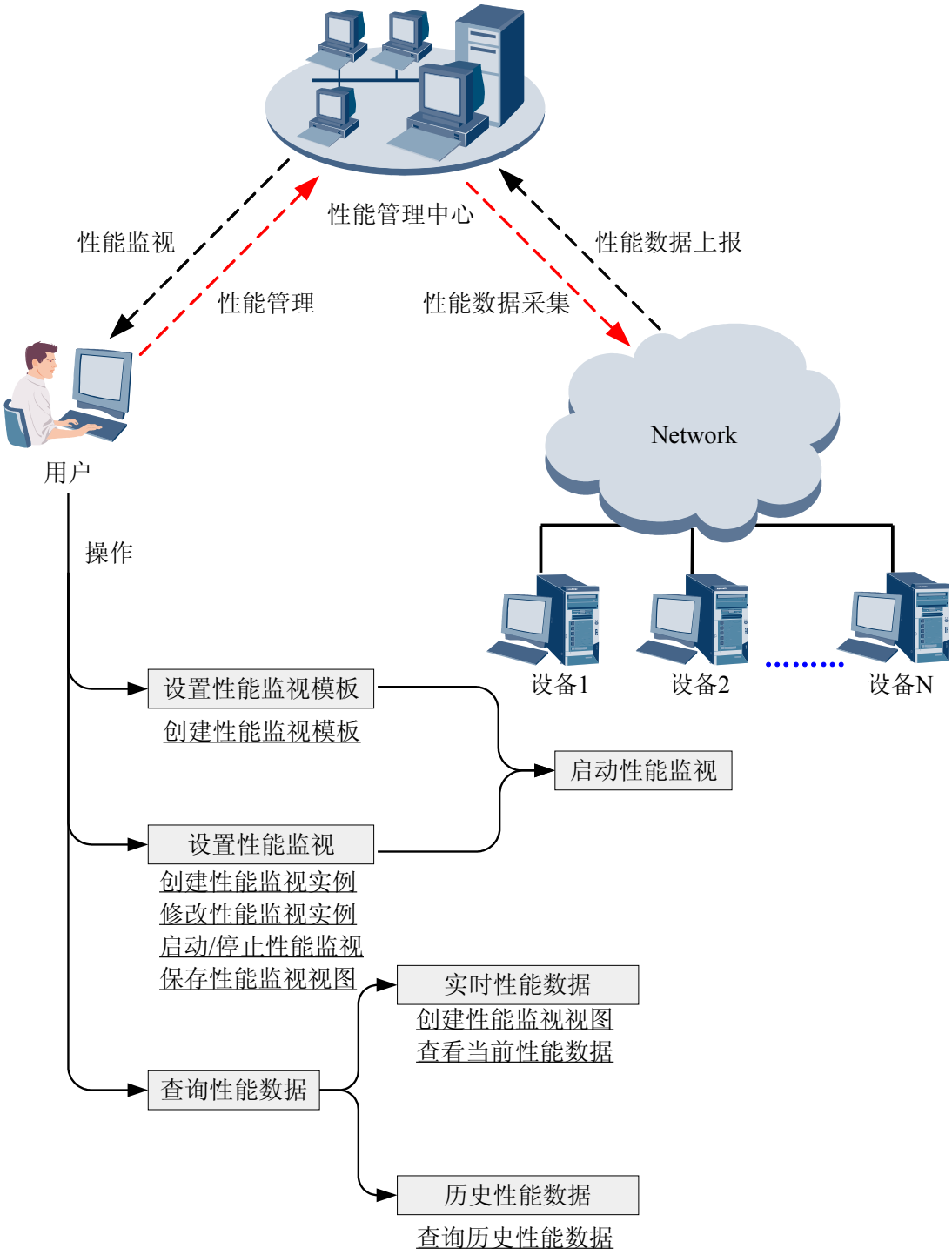
5.2 性能监视流程

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 5-1 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并查看性能监视数据，网元侧将从设备上采集到的性能数据上报到网管。

图 5-1 性能监视上报流程



用户侧性能监视的流程

1. 设置性能监视模板：由于同类型网元具有相同的设置属性，可以在一个模板中提前预制性能监视参数，网管会自动将性能模板下发到可管理的网元上，为网元提供默

认的监视和告警能力，网元能够根据模板自动产生采集任务，提供性能数据的采集并上报产生的告警。

2. 设置性能监视：在需要进行性能监视的对象上创建一个性能监视实例，通过启/停性能监视实例实现对性能指标数据的采集。支持对已监视对象的性能指标、属性进行修改，实现了对所有性能监视实例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，有最近性能和历史性能二种数据查询方式。最近性能统计数据能够通过性能监视视图进行实时监视，历史性能支持按照指定时间段查询统计数据，查询结果分为表格展示（默认）和曲线图展示（高级展示）。可参考查询最近性能和查询历史性能。

网络侧设备上报性能数据的流程

网络侧设备收到从网管下发的性能采集任务，任务可能是来自性能监视模板，也可能来自用户创建的性能监视实例，然后启动性能指标的采集并将采集到的数据以及产生的相关告警定期上报到网管。网管上的预统计模块会根据需要在出报表及向上级网管提供性能数据的时候对这些原始测量数据进行统计处理，并将预处理后的性能数据入库保存在性能数据库中。

5.3 设置性能监视

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。

5.3.1 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，网元创建后能够根据设置的模板自动产生采集任务、采集数据和产生告警。

背景信息

由于同类型网元具有相同的设置属性，将这些设置属性创建为一个性能监视模板后，当有新网元接入时，会自动继承模板中的设置属性，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 在左侧树型列表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”窗口中设置告警产生的条件。单击“确定”。

说明

当“重复次数”设置为 3 时，表示在设备连续 3 个性能采集周期中，只有当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，选中“缺省监视”。

步骤 6 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

设置了“缺省监视”的性能指标，当该网元类型的网元创建时，系统会自动在“性能监视设置”窗口中增加该性能指标的监视实例。

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。

5.3.2 创建性能监视任务

用户创建性能监视任务后，就能够启动采集任务对性能指标进行监视与数据采集。

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 单击“创建”，新增一个性能采集任务。

步骤 3 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联动显示该子网下所有可管理对象。

步骤 4 单击 ，展开管理对象，选中复选框，单击“确定”。

步骤 5 单击“选择指标”，弹出“选择指标”窗口。在左侧拓扑树中选择一个对象类型，右侧指标列表中联动显示该对象类型所有可选择的指标。

步骤 6 单击 ，展开指标列表，选中复选框，单击“确定”。

步骤 7 **可选:** 如果需要自定义性能监视的采集间隔、阈值条件，单击“修改属性”。

1. 将指标对应的“是否启用模板”属性复选框设置为禁用。

   说明

   - 如果启用模板设置，监视实例的属性会使用对应模板中设置的值，且全部灰化不能修改，只有去掉启用模块设置才能手动修改。
   - 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。

2. 调整性能指标采集周期，单击 ，修改告警上报的阈值条件。单击“确认”。

   说明

   当“重复次数”设置为 3 时，表示只有当设备连续 3 个性能采集周期中都产生了这个告警，设备才会上报该告警。

3. 单击“确定”。

步骤 8 在已选指标“测量对象”栏中，单击“ ”,在“选择测量对象”窗口中，输入或选择测量对象。单击“确定”。

说明

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。

步骤 9 单击“确定”，完成性能监视参数设置并创建实例，在“操作结果列表”中分别查看对应指标上的性能监视创建结果。

步骤 10 单击“完成”，返回到性能监视设置主界面。

----结束

5.3.3 设置性能监视任务

在成功创建性能指标监视任务后，可以修改、删除、启动、停止、查看性能监视任务。

前提条件

已创建性能监视任务。

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 根据需要设置过滤条件，单击“搜索”，界面显示出符合特定查询条件的性能监视任务。

步骤 3 在性能监视列表中同时选中多个监视对象，单击“修改”，可批量修改多个监视任务。

步骤 4 在弹出的“修改属性”窗口中选中要修改的指标，设置是否启用模板，调整性能采集周期并修改告警上报的阈值条件，单击“确定”。

步骤 5 在性能监视列表中同时选中多个监视对象，单击“启动”，同时启动多个性能采集任务。

说明

- 只有当“采集状态”为“停止”，才能启动采集任务。如果“采集状态”为“异常”，需要先停止采集，然后检查设备通信状态是否正常，再启动采集。
- 性能监视任务的停止和删除也都支持批量操作。

----结束

5.3.4 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

- 至少存在 1 个以上性能监视实例。
- 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

步骤 1 **可选:** 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. 单击“增加监视视图”，弹出“增加监视视图”窗口。

3. 设置视图名称，在左边列表中选择管理对象，右边联动显示该对象对应的指标实例。
4. 选择需要添加到性能监视视图的指标，单击“确定”。

步骤 2 **可选:** 在性能监视列表中直接保存性能监视视图。

1. 在主菜单中选择“性能 > 性能监视设置”。
2. 根据需要设置过滤条件，单击“搜索”，界面显示出符合特定查询条件的性能监视任务。
3. 在性能监视列表中同时选中多个监视对象，单击“保存为监视视图”。
4. 在弹出的“增加监视视图”窗口中设置视图名称，单击“确定”。

----结束

后续处理

在主菜单中选择“性能 > 性能监视视图”，选择相应监视视图，单击  ，弹出“修改监视视图”窗口，可修改视图名称，并对视图中监视的指标实例进行增删。

5.4 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。

5.4.1 查询最近性能数据

性能监视视图中能够查询到最近一周内监视到的性能指标数据，并图形化展示指标数据的变化情况。

前提条件

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

5.4.2 查询历史性能监视数据

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。

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 单击“选择管理对象”，在弹出的“选择管理对象”对话框中选择查询的对象类型。单击“确定”，下方的管理对象列表联动显示该类型下的所有管理对象。

步骤 3 批量选择需要查询的管理对象，单击“确定”。左侧“管理对象”联动显示与对象类型关联的管理对象。

步骤 4 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，测量对象下拉框使能，否则灰化。

步骤 5 单击“数据曲线图”页签，选择测量指标。

步骤 6 单击“选择实例”，在弹出窗口中选择多个与指标相关的对象实例，单击“确定”，下方显示测量指标的数据曲线图。

说明

在曲线图中不同实例的测量指标也会以不同颜色的曲线表示。

----结束

后续处理

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。

5.4.3 查看网元性能概况

在资源管理器中支持对关键 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

查看的网元支持性能管理。

操作步骤

步骤 1 在主菜单中选择“资源 > 资源管理”。

步骤 2 在左侧设备导航树中选择一个网元，在右侧列表的“名称”属性列中单击网元名称。

步骤 3 单击，查看网元基本信息和性能 KPI 信息。

步骤 4 **可选:** 单击“设置”，在“设置”窗口中选中需要在“性能 KPI”中图形化显示的性能指标，单击“确定”。

窍门

- 单击，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，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。

----结束

6 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。

6.1 了解报表功能
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。

6.2 配置流程
介绍配置报表系统的配置流程。

6.3 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。

6.4 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。

6.5 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。

6.6 维护报表系统
根据需要，定期对报表系统进行维护。

6.1 了解报表功能

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：

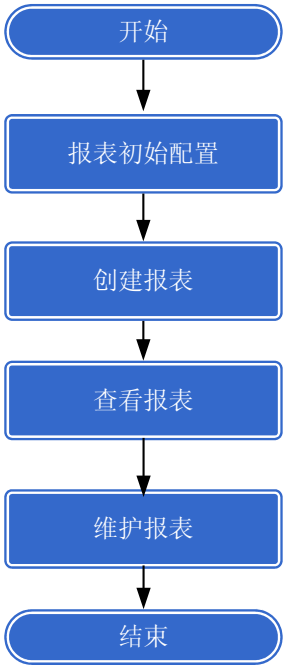
- 将报表保存到报表存储区中。
- 周期报表保存到报表存储区的报表文件夹中，手工报表不保存。
- 设置设置存储区的空间大小。
- 在报表系统中打印报表存储区的报表。

6.2 配置流程

介绍配置报表系统的配置流程。

配置报表系统的流程请参见图 6-1。

图 6-1 配置报表系统流程图



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。
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。

6.3 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。

6.3.1 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

6.3.2 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”按钮，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”。

6.4 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。

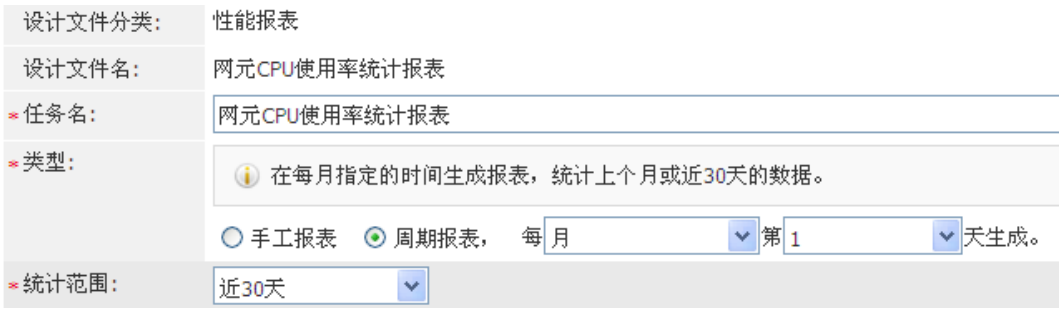
窍门

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。



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。
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

6.5 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。

1. 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。
2. 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。

网元CPU使用率统计报表

生成时间： 2011-08-04 19:59:13

统计范围： 2011-08-01 19:01:28 - 2011-08-05 19:01:30

设备名称	设备区域	设备类型	设备IP	实例名称
cisco_10.137.134.192	ROOT	Catalyst4507RE	10.137.134.192	CPU:1
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:0
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:2
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:3
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:5
h3c_10.112.57.135	ROOT	S8505-EI	10.112.57.135	Slot:6

----结束

6.6 维护报表系统

根据需要，定期对报表系统进行维护。

6.6.1 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“过滤”，过滤出相应的报表任务。

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

6.6.2 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

6.6.3 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“过滤”，过滤出相应的报表任务。

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

7 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。

7.1 了解网元管理器功能

介绍网元管理器的基本功能。

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。
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，实现网管和网元的之间的通信正常。

7.2 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。

7.2.1 查看基本信息

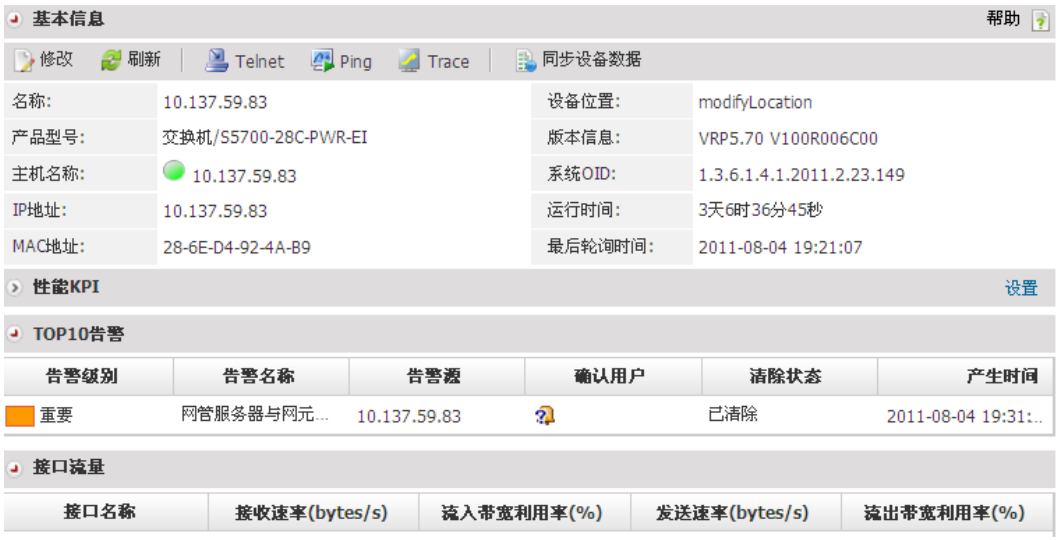
通过查看网元基本信息，了解网元的基本情况。

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 在左侧的导航树上单击“查看 > 基本信息”。

步骤 3 在右侧的“基本信息”窗格中查看网元的基本信息。



在基本信息里可执行如下操作：

- 单击“修改”，在弹出的窗口修改网元的基本信息，单击“确认”。
- 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 **7.3.2.1 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可以查看同步设备的数据详细情况。

步骤 4 单击“性能 KPI”，查看网元当前的关键性能信息。

步骤 5 单击“TOP10 告警”，查看网元当前的 TOP10 告警信息。

步骤 6 单击“接口流量”，查看网元的接口流量信息。

----结束

7.2.2 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 将鼠标放在对于的单板、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。

----结束

7.2.3 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点击“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”。

操作名称	操作方法
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。
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。 **说明** 如果需要导出全部可以直接单击“导出 > 导出全部”。

----结束

7.2.4 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

7.2.5 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”窗口中单击“查看详情”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

7.3 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。

7.3.1 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

7.3.2 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。

7.3.2.1 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

7.3.2.2 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。

- 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。
- 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。

步骤 4 单击“测试”，测试成功后，单击“应用”。

----结束

7.3.3 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。

7.3.3.1 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。

7.3.3.2 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”按钮，弹出“同步进度”对话框，待同步任务完成后，单击“确定”。

步骤 4 单击  配置接口相关参数。

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

7.3.3.3 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。

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

7.3.4 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“配置 > 配置文件”。

步骤 3 在“操作”下执行恢复操作。

----结束

后续处理

备份配置文件请参见 **10.4.2 手工备份网元配置数据**。

8 业务管理

关于本章

eSight 提供对 WLAN 和 IPSec VPN 业务管理。

8.1 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）。

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

8.1 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）。

8.1.1 了解 IPSec VPN

IPSec VPN 是 IETF 制定的为保证在 Internet 上传送数据的安全保密性能的三层隧道加密协议。 IPSec VPN 在 IP 层对 IP 报文提供安全服务。IPSec 协议本身定义了如何在 IP 数据包中增加字段来保证 IP 包的完整性、私有性和真实性，以及如何加密数据包。IPsec VPN 提供了两个主机之间、两个安全网关之间或主机和安全网关之间的保护。

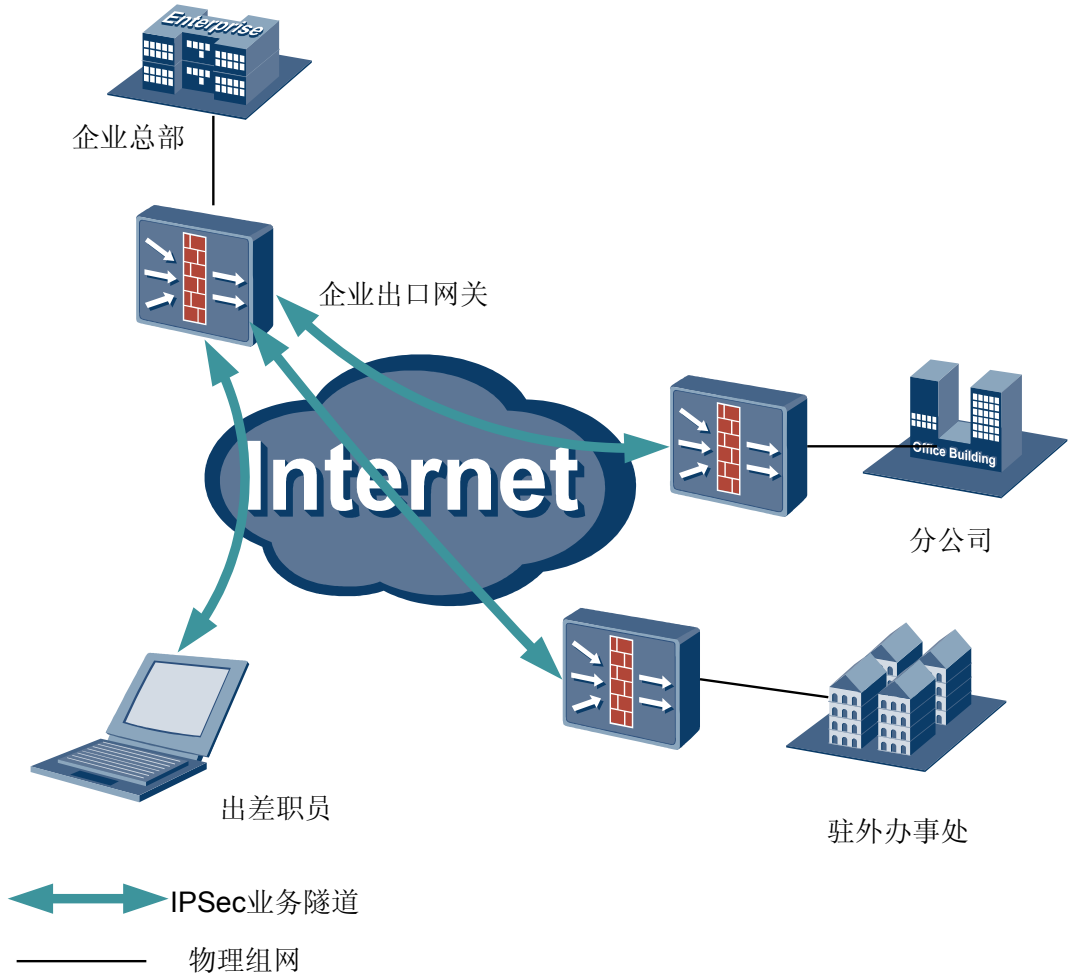
8.1.1.1 IPSec VPN 应用

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 8-1 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 8-1 IPSec VPN 典型应用场景



8.1.1.2 IPSec VPN 相关概念

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

8.1.2 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

8.1.3 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,便于网管对隧道的联通性进行监控。

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

8.1.4 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

8.1.5 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

8.2 WLAN 业务管理

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

8.2.1 WLAN 简介

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。

8.2.2 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。

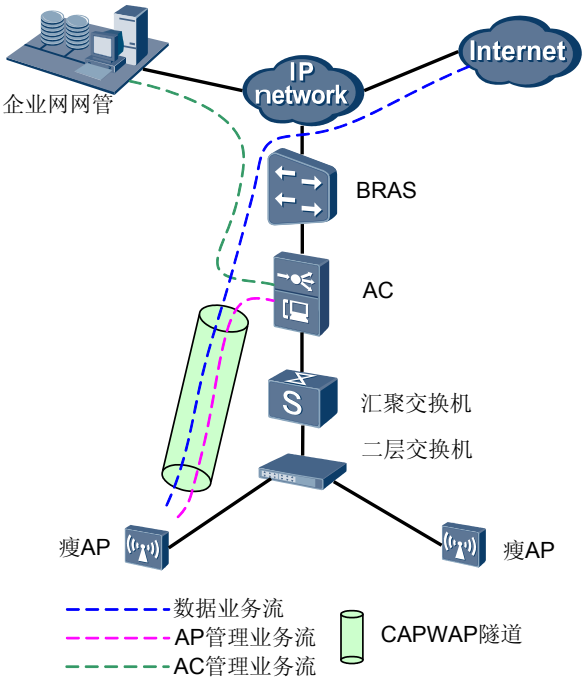
直连式组网方案中，AP 和 AC 建立 CAPWAP 隧道，管理流必须封装在 CAPWAP 隧道中，数据业务流可以选择是否封装在 CAPWAP 隧道中。

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 8-2 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 8-2 数据业务流封装在 CAPWAP 隧道

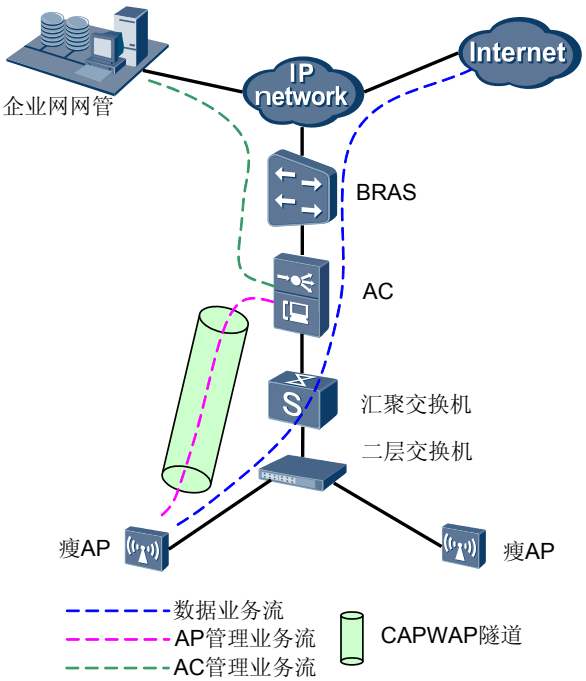
  

  在这种方式下，只需预先在交换机配置管理 VLAN，无需配置数据 VLAN。AP 管理 VLAN 用于 AP 与 AC 间的对接。

- 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 8-3 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 8-3 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

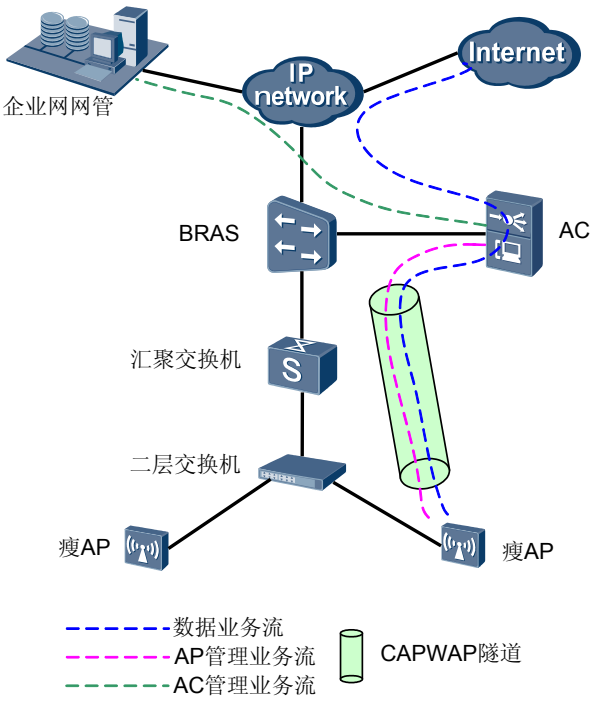
旁挂式组网是指 AC 旁挂在 BRAS 旁边，实现对 AP 的 WLAN 业务管理。在旁挂式组网模式下，BRAS 设备管辖范围内部署的 AP 都由 BRAS 旁挂的 AC 管理，AC 部署相对集中，适合于 AP 比较分散的全城热点部署的组网应用。

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 8-4 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 8-4 数据业务流封装在 CAPWAP 隧道

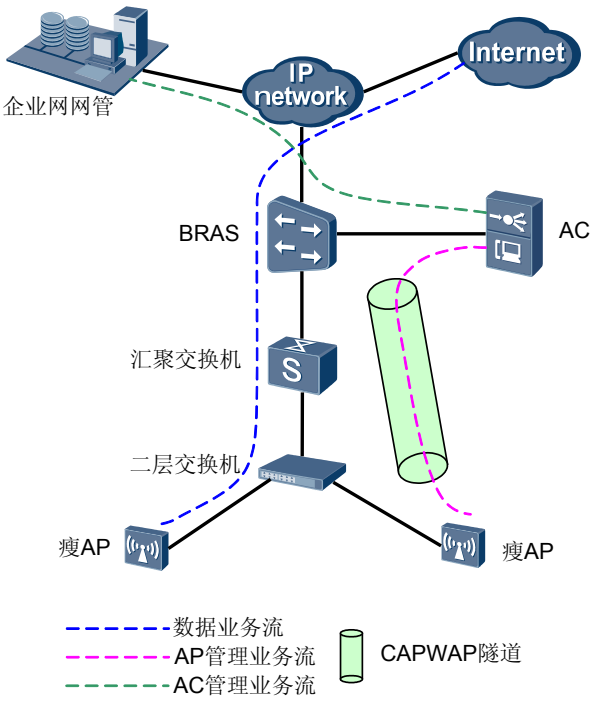


在这种方式下，只需预先在交换机配置管理 VLAN，无需配置数据 VLAN。AP 管理 VLAN 用于 AP 与 AC 间的对接。

- 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 8-5** 所示。

图 8-5 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 8-1 所示。

表 8-1 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。

8.2.3 WLAN 操作任务

介绍完成 WLAN 业务管理的操作方法。

8.2.3.1 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”。

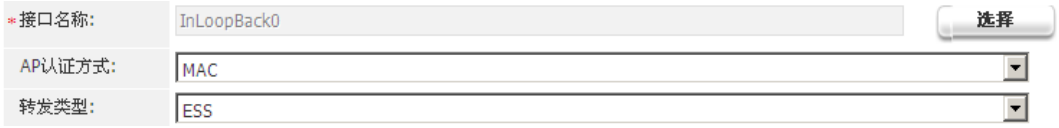
步骤 3 在右侧的窗口中，单击“创建”，在“新建 AC”窗口中单击“选择”，在弹出窗口中选择 AC 设备，单击“确定”，新建 AC 设备。

步骤 4 在“新建 AC”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”。

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用户数据。

转发类型为 AP 时，AP 以自己设置的用户数据转发模式转发用户数据。

----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。

8.2.3.2 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”，在右侧窗口中单击 AC 的“名称”。

步骤 3 离线添加 AP。

1. 在左侧导航树中选择“WLAN 管理 > AP”，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. 在左侧导航树中选择“WLAN 管理 > AP 白名单”，单击“创建”。
2. 在“新增记录”下设置 AP 的“MAC”或“SN”。

步骤 5 确认未授权 AP。

1. 在左侧导航树中选择“WLAN 管理 > 未授权 AP”，单击“同步”。

2. 在选中未授权 AP，单击“确认上线”。

----结束

8.2.3.3 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。

?.1. 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”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > AP 模板”。

步骤 4 单击“创建”，在弹出的窗口中设置 AP 模板相关参数。

步骤 5 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

?.2. 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”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > 射频模板”。

步骤 4 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输至少要间隔 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 5 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

?.3. 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 对象上，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”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > ESS 模板”。

步骤 4 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 5 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

8.2.3.4 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“业务管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“Wlan 管理 > AP 域”。

步骤 4 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 5 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，将对应的 AP 域设置为默认 AP 域。

----结束

8.2.3.5 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 AC 的“名称”。

步骤 3 在左侧的导航树中选择“Wlan 管理 > AP”。

步骤 4 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 5 在“绑定模板”界面根据需要设置 AP 绑定的模板。

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

8.2.3.6 查看 AP 信息

配置 AP 上线后，可以通过该操作查看所有网管管理的所有 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 8-2 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。
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。
信道值	

参数	说明
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

8.2.3.7 浏览 STA

用户浏览当前网络中所有无线终端的信息。

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 > 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

8.2.3.8 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

8.2.3.9 管理 Rogue AP

Rogue AP 即非法 AP，是未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。

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输至少要间隔 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 智能配置工具

关于本章

介绍智能配置工具的功能，并指导用户如何配置和下发。

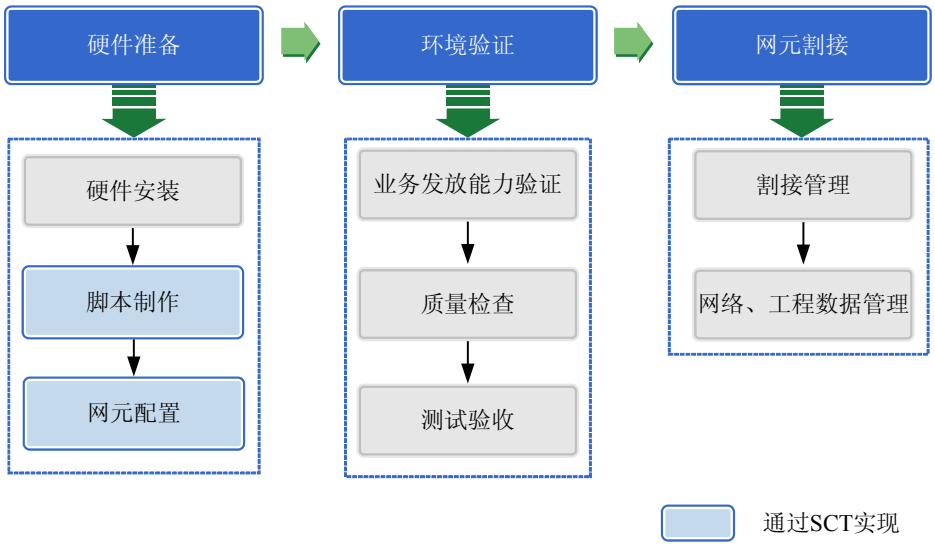
9.1 智能工具概述

介绍 eSight 智能工具的系统功能。

9.1.1 系统简介

在搭建网络环境的过程中，制作和下发脚本是必不可少的。用户根据脚本样例和网络规划表手工制作脚本时，不仅耗时长，且容易出错。智能工具可以通过配置模板和规划表一键式生成脚本，并批量下发到网元，大大提升脚本制作效率。

- 智能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。在系统中输入命令关键字可以查询相关的配置命令，用户只需要填写配置参数即可创建脚本。
- 智能工具还提供了模板管理的功能，可以快速生成配置脚本，用来对网元进行批量配置。



SCT (Smart Configuration Tool): 智能配置工具

通过智能配置工具制作脚本分为以下几种情况：

- 根据详细设计文档(LLD，Low Level Design)创建模板，导入网络数据规划表批量生成脚本。
- 通过已有脚本反向生成模板，再将模板应用于相同类型网元，即生成网元的配置脚本。
- 根据通用模板生成脚本。
- 通过手工输入命令行的方式编辑脚本。

9.1.2 系统功能

介绍智能配置工具所提供的主要功能。

离线校验脚本

在离线的情况下编写脚本，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。

快速生成模板

可直接将用户脚本一键式生成为模板，方便后续类似配置的应用。

从规划表“一键式”生成脚本

可以将多个模板批量导出生成规划表，填入参数后，再将规划表导入，工具会根据规划信息自动生成脚本。

批量配置

可针对多网元多脚本，进行快速批量配置。

通用模板

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完成脚本制作。

9.2 了解客户端界面

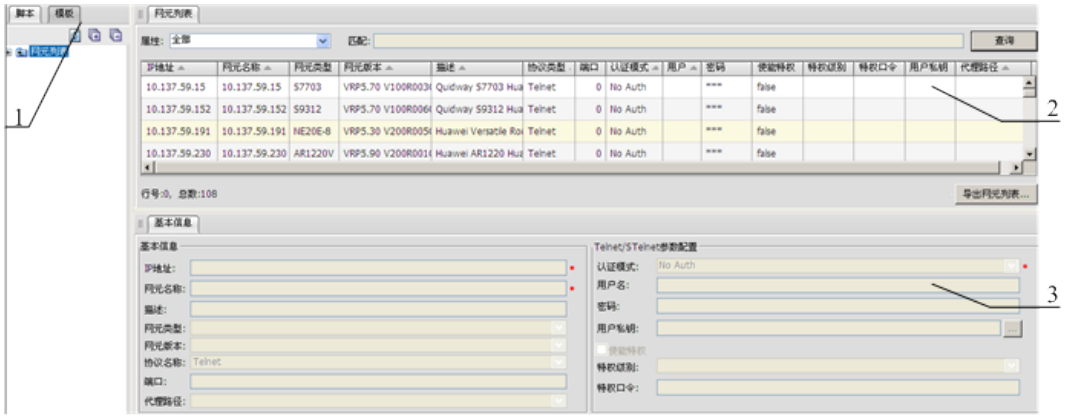
了解客户端的界面，有助于快速找到操作入口，提高操作效率。

9.2.1 主界面

介绍了智能配置工具主界面的组成，以及每个组成部分的作用。

主界面

图 9-1 主界面组成



(1).脚本/模板　　(2).配置区

(3).基本信息显示区

主界面说明

1. 脚本/模板页签
   - 脚本页签：显示网元的导航树，在每一个网元下面可以创建脚本。也可以创建文件夹将网元分类，便于查找和管理。
   - 模板页签：显示模板的导航树，其中包括通用模板和用户自定义的模板。也可以创建文件夹将模板分类，便于查找和管理。
2. 配置区
   - 选中脚本，在配置区域可以输入脚本信息，并且可以进行“保存”、“下发”、“验证脚本”和“生成模板”等操作。
   - 选中模板，在配置区域可以对模板进行编辑操作。

   说明

   当选择“网元”、“文件夹”和导航树主节点时，配置区域只有查看的功能，用于查看网元下的脚本信息，或者查看文件夹中的网元或模板信息。
3. 基本信息显示区

   当选择配置区域的一条记录时，在基本信息显示区域会显示该条记录的基本信息。

   说明

   当选择一个脚本或者模板时，没有基本信息显示区。

9.2.2 快捷图标

介绍脚本和模板配置时快捷图标的功能。

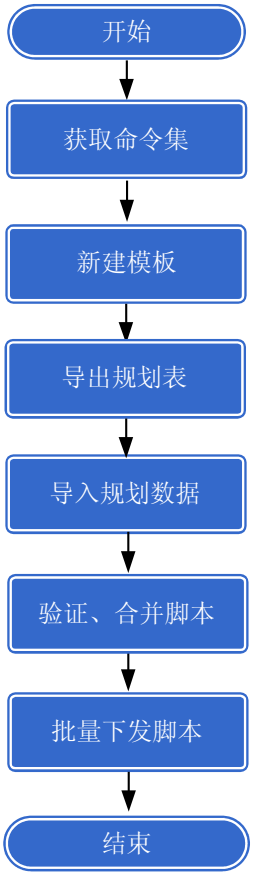
图标	名称	功能说明
脚本配置快捷图标		
	编辑	锁定该脚本，并同步脚本信息。 编辑脚本时单击此快捷图标，则只有该客户端可以编辑脚本，对其他客户端锁定，防止多客户端同时操作。
	保存	保存脚本信息。 保存之后才能进行验证、下发或生成模板，同时脚本信息会变成彩色。如果命令输入有错误，将以红色字体显示整行命令。
	查找/替换	在脚本中查找/替换与关键字相匹配的信息。
	下发	将脚本信息下发到网元上。
	验证脚本	验证脚本信息是否符合语法，同时给出校验结果。对于“失败”的命令将以红色显示出来；对于输入不完整的命令，同时将给出“模糊匹配”，提示用户输入完整的命令。
	生成模板	将脚本信息生成模板，方便后续类似配置的应用。

图标	名称	功能说明
	查询	在查询框中，输入命令关键字后，单击此快捷图标可以查看和该命令关键字相关的命令。 **说明** ● 最多显示和该命令关键字相关的前 200 条命令。 ● 查询时，只能输入命令关键字，不能携带命令参数。
模板配置快捷图标		
	编辑	锁定该模板，并同步模板信息。 编辑模板时单击此快捷图标，则只有该客户端可以编辑模板，对其他客户端锁定，防止多客户端同时操作。
	复制	复制当前模板或其他模板中选中的一条命令或一个视图。
	粘贴	将复制的命令或视图粘贴到新的位置。
	上移	将选中的命令或视图及其子节点上移。
	下移	将选中的命令或视图及其子节点下移。
	插入	在模板中插入一条命令。
	删除	删除模板中选中的一条命令。
	更新描述	更新命令的描述信息。
	编辑命令	编辑当前选中的命令。
	应用	将当前模板应用到网元生成脚本。
	保存	保存模板信息。
	另存为	另存为一个新模板。
	展开	展开所有的命令。
	收缩	收缩所有的命令。
	切换	切换“命令”和“命令描述”的显示。

9.3 智能工具配置流程

结合典型使用场景介绍智能工具配置网元的流程。

图 9-2 配置网元流程图



流程序号	流程任务	任务说明
1	获取命令集	介绍如何获取命令集。获取网元命令集之后，才能进行脚本验证、生成模板等操作。
2	新建模板	介绍如何制作脚本模板。在网络配置过程中，需要对大量网元进行配置，对同类型网元可以先创建脚本模板，再批量应用于这些网元，大大提升脚本制作效率。
3	导出规划表	根据配置模板可直接导出网络数据规划表。
4	导入规划数据	通过导入规划数据，工具可以自动生成每个网元的配置脚本。
5	验证、合并脚本	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。 可以将网元的多个脚本文件合并为一个脚本文件。
6	批量下发脚本	通过下发脚本可以实现网元的批量配置。

9.4 智能工具操作任务

通过本章可以尽快了解智能配置工具的典型使用场景，并按照操作步骤完成网元配置。

9.4.1 获取命令集

介绍如何获取命令集。获取网元命令集之后，才能进行脚本验证、生成模板等操作。

背景信息

- 在网元列表中查看网元类型和网元版本是否为空，如果不为空，无需执行“获取命令集”操作。说明智能工具已经获取了该网元的命令集。
- 如果获取命令集不成功，请检查网元的 Telnet/STelnet 参数是否设置正确。检查方法：在网元列表的“基本信息”区域，单击“测试连通性”。如果测试失败，请重新配置网元的 Telnet/STelnet 参数，直到测试成功后，再进行获取命令集操作。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树中，选择一个要获取命令集的网元，单击右键，选择“获取命令集”。

系统开始获取网元命令集，以进度条显示获取的进度。

步骤 4 **可选:** 单击“后台运行”。

步骤 5 在获取完成后，单击“关闭”。

网元的“网元版本”和“网元类型”被更新。

----结束

9.4.2 新建模板

介绍如何制作脚本模板。在网络配置过程中，需要对大量网元进行配置，对同类型网元可以先创建脚本模板，再批量应用于这些网元，大大提升脚本制作效率。

可以通过以下三种方式制作模板：

- 导入已有模板：将已提前制作好的模板导入到配置计划工具中。
- 通过已有脚本生成模板：通过 LLD 中的脚本样例或其他已有的脚本反向生成配置模板。
- 手动创建模板：若既没有 LLD 文件，也没有可以利用的脚本，还可以通过手动创建的方法创建模板。这种方式要求用户能够准确掌握网元的配置命令。

9.4.2.1 导入模板

智能工具提供了部分通用模板，如果有其他自定义的模板，可以通过此功能导入。

前提条件

已准备好需要导入的模板。

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 选择“模板”页签。

步骤 3 **可选:** 右键单击“模板列表”导航树节点，选择“创建文件夹”。

步骤 4 **可选:** 在“创建文件夹”对话框中，输入文件夹的名称，单击“确定”。

步骤 5 选中“模板列表”节点或新建的文件夹，单击右键选择“导入模板”。

步骤 6 在弹出的对话框中选择“浏览”，选择要导入的模板。

步骤 7 单击“导入”。导航树中会出现相应的模板。

----结束

9.4.2.2 通过已有脚本生成模板

介绍通过 LLD 中的脚本样例或其他已有的脚本反向生成配置模板的方法。与手工创建模板相比，通过 LLD 生成模板更加准确和高效。

前提条件

已获取可继承的脚本文件。

背景信息

已有脚本分为以下两种：

- LLD 文件中的脚本样例。
- 用户保存的使用过的旧脚本文件。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树中，选择要配置的网元，单击右键，选择“创建脚本”。

步骤 4 在“创建脚本”对话框中，输入“脚本名称”和“描述”，单击“确定”。创建的脚本将出现在对应网元的下面。

步骤 5 单击“编辑”，将 LLD 中的脚本样例或其他脚本文件拷贝到空白处，并根据实际情况进行修改。

说明

如果脚本中命令行数量较大，可以使用查找/替换功能对脚本进行修改。

步骤 6 单击“保存”。

步骤 7 单击“验证脚本”。

步骤 8 在“验证结果”对话框中，查看每个命令行的“验证结果”。

- “验证结果”为“错误”：

  单击“关闭”。在命令查询文本框中，输入出错的命令行并回车，查看该设备是否支持该命令，在“脚本配置”区域修改相应出错的命令行。

  说明

  查询时，只能输入命令关键字，不能携带命令参数。

- “验证结果”为“模糊匹配”：

  单击“关闭”。在命令查询文本框中，输入出错的命令行并回车，可以看到该命令行的参数取值范围，在“脚本配置”区域修改出错的命令行。

步骤 9 单击“生成模板”。

步骤 10 在弹出的“生成模板”对话框中，根据需要修改命令行的参数。

步骤 11 单击“确定”。

步骤 12 在弹出的界面中，输入“模板名称”、“模板描述”、“应用场景”等参数。

步骤 13 单击“确定”。弹出操作成功的提示信息。

步骤 14 单击“确定”。

----结束

9.4.2.3 手动创建模板

可以通过查询命令方式手工创建配置模板，再将模板应用于多个网元。

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 选择“模板”页签。

步骤 3 **可选:** 右键单击“模板列表”导航树节点，选择“创建文件夹”。

步骤 4 **可选:** 在“创建文件夹”对话框中，输入文件夹的名称，单击“确定”。

步骤 5 在“模板列表”导航树上，单击右键，选择“创建模板”。

步骤 6 在“创建模板”对话框中，选择模板要存放的位置，选择模板要对应的“网元类型”和“网元版本”，输入模板的基本信息，单击“确定”。

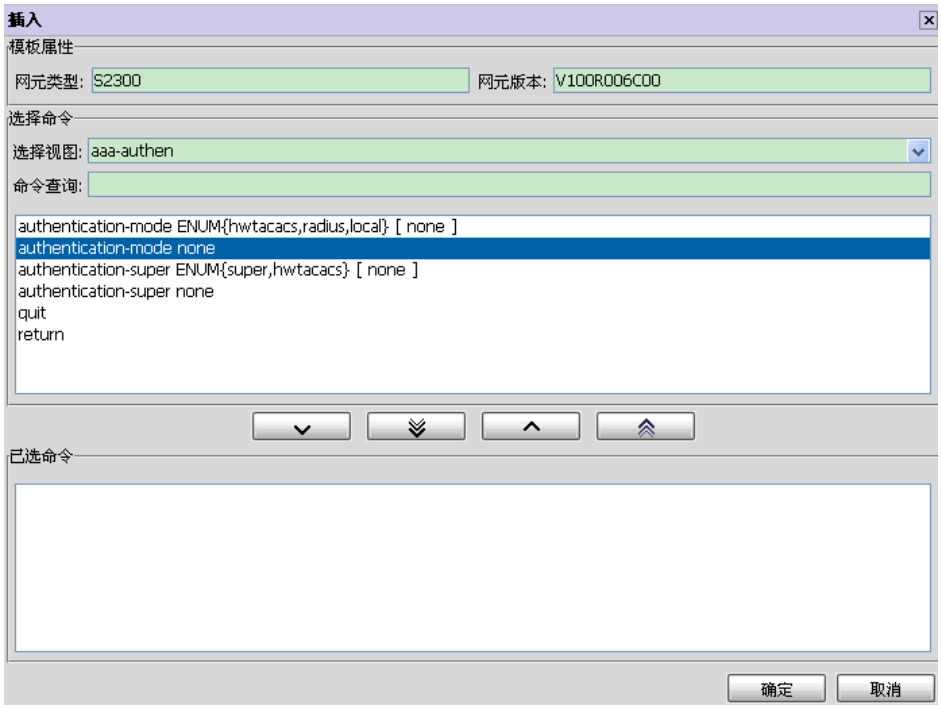
说明

如果不选择“网元类型”和“网元版本”，无法在模板中插入命令。

步骤 7 在“插入”对话框中，选择“选择视图”。

步骤 8 在“命令查询”处，输入要查找的命令的关键字。

在查询结果区域框中将显示出和该命令关键字相关的命令。



步骤 9 单击将所需命令添加到已选命令列表中。单击“确定”。

创建的模板显示在导航树中，在“模板配置”区域框中显示该模板的详细信息。

步骤 10 **可选:** 在“模板配置”区域框中，单击可以对模板进行再次编辑和修改。

- 通过双击命令或参数，可以对其描述信息进行修改。
- 双击参数值列，可输入或修改参数值。
- 通过快捷图标可以对模板进行插入命令、删除命令、更新描述和修改命令等操作。快捷图标的详细介绍请参见 **9.2.2 快捷图标**。
- 在命令行列中单击图标，在弹出的对话框中可以修改命令视图。

----结束

9.4.3 导出规划表

根据配置模板可直接导出网络数据规划表，只需按照规划表的字段填写配置信息后，再通过导入即可生成配置脚本。

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 选择“模板”页签。

步骤 3 选中“模板列表”导航树任意层级的节点，单击右键。

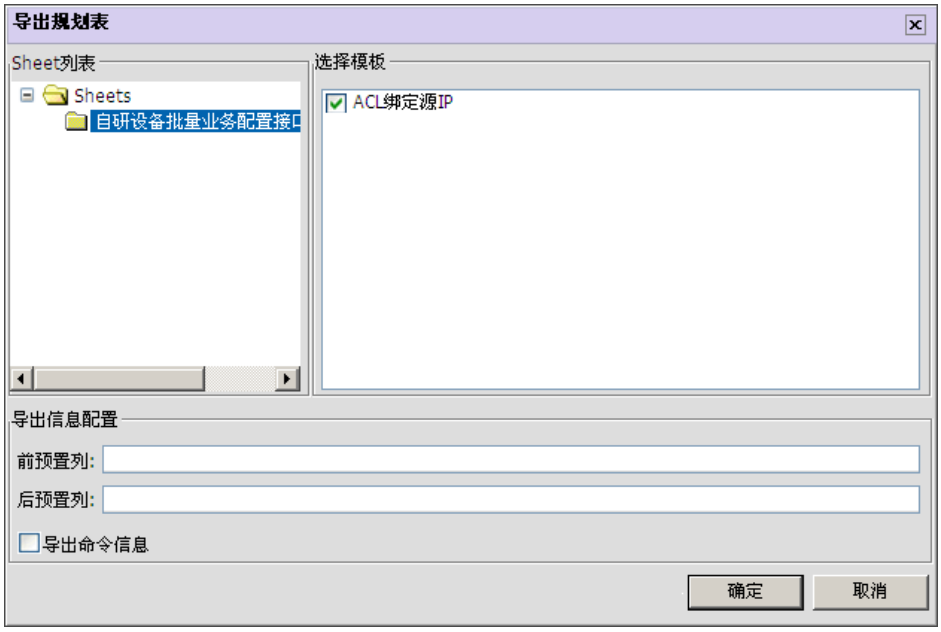
说明

若选中的是文件夹节点，则会将该文件夹下的所有模板都导出到同一个.xls 文件中。

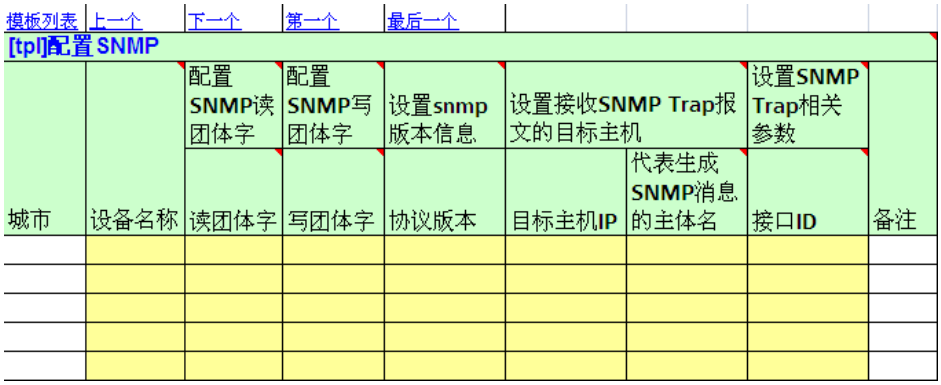
步骤 4 选择“导出规划表”。

步骤 5 在弹出的对话框中选择需要导出的模板，并填写导出信息。

- “前预置列”是指在导出的表格中最左侧(即第一列)增加自定义的列信息。也可以增加多个自定义列，每个列名之间用半角英文逗号隔开。
- “后预置列”是指在导出的表格中最右侧(即最后一列)增加自定义的列信息。也可以增加多个自定义列，每个列名之间用半角英文逗号隔开。
- 选中“导出命令信息”，导出的规划表中会显示完整的命令行。若不选中，规划表中只显示参数。



步骤 6 单击“确定”。在弹出的对话框中，单击“确定”。弹出如下图所示表格。



说明

- 表格中字体加粗的列表示该条命令是进入视图的命令。
- 填写过程中，可以添加行，但不能添加列。
- 若同一网元需要多次应用某个命令，则需要填写多行，生成脚本时就会生成多条命令。
- 填写参数时，请参考表格批注中的参数范围。
- 表格中黄色底色的表示必填参数，白色底色的表示可选参数。
- 如果不填写必选参数，生成的脚本中将不包含该参数对应的命令行。
- 单击每个表格第一行的“模板列表”、“上一个”、“下一个”、“第一个”或“最后一个”，可以跳转到相应的表格。

步骤 7 填写详细的配置信息后，选择“文件 > 另存为”将数据规划表保存到本地磁盘。

----结束

9.4.4 导入规划数据

通过导入规划数据，智能工具可以自动生成每个网元的配置脚本。

前提条件

- 已经创建或导入配置模板。
- 已经将导出的规划表填写完整。

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 选择“脚本”页签。

步骤 3 选中“网元列表”导航树节点，单击右键。

步骤 4 选择“导入规划表”。

步骤 5 在弹出的对话框中选择“浏览”，选择网络数据规划表。

若选中“覆盖同名脚本”复选框，会覆盖之前导入的同名脚本。

若不选中“覆盖同名脚本”，生成的脚本名称会在之前生成的脚本名称基础上序号递增。例如，之前已经生成脚本“接口配置(1)”，再次导入规划表生成的脚本名称为“接口配置(2)”。

步骤 6 单击“导入”。网元节点下会出现自动生成的脚本，此脚本是工具根据网络数据规划表和模板自动生成。

----结束

9.4.5 验证脚本

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。

前提条件

- 已经有创建成功的脚本，创建脚本的方法请参见 **9.5.4.1 手动新建脚本**。
- 已正确配置了网元的“网元版本”和“网元类型”。

- 工具中存在或已经导入需要验证的网元的命令集。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树中选择要验证的脚本，单击右键选择“验证脚本”。
也可以在“脚本配置”区域，单击来验证脚本。

步骤 4 在“验证结果”对话框中，查看每个命令行的“验证结果”。

- “验证结果”为“错误”：
  单击“关闭”。在命令查询文本框中，输入出错的命令行并回车，查看该设备是否支持该命令，在“脚本配置”区域修改相应出错的命令行。
  说明
  查询时，只能输入命令关键字，不能携带命令参数。
- “验证结果”为“模糊匹配”：
  单击“关闭”。在命令查询文本框中，输入出错的命令行并回车，可以看到该命令行的参数取值范围，在“脚本配置”区域修改出错的命令行。

----结束

9.4.6 合并脚本

介绍如何将网元的多个脚本文件合并为一个脚本文件。

前提条件

- 网元的所有配置脚本都已经生成。
- 网元的脚本文件都已经验证无误。

背景信息

此功能既支持合并一个网元下的多个脚本，也支持批量合并多个网元下的多个脚本。

操作步骤

- 场景一：合并单个网元下的多个脚本，操作步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。
  3. 在“网元列表”导航树中，选择一个要合并脚本的网元，右侧“脚本列表”区域显示出该网元下的所有脚本。
  4. 选中任意一个脚本文件，单击右键，选择“全选”。
  5. 在所有脚本被选中的情况下，单击右键，选择“合并脚本”。
  6. 在弹出的提示框中，查看合并脚本的进度，当进度达到 100%时，单击“关闭”。
- 场景二：合并所有网元下的多个脚本，操作步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。

3. 在“网元列表”导航树中，选择任意网元，在右侧的“属性”下拉菜单中选择“全部”。
4. 单击“查询”，页面中显示出所有网元下的所有脚本。
5. 选中任意一个脚本文件，单击右键，选择“全选”。
6. 在所有脚本被选中的情况下，单击右键，选择“合并脚本”。
7. 在弹出的提示框中，查看合并脚本的进度，当进度达到100%时，单击“关闭”。

----结束

9.4.7 下发脚本

通过下发脚本可以实现网元的批量配置。

前提条件

已经有经过验证的脚本，“验证脚本”的方法请参见 9.4.5 验证脚本。

背景信息

下发脚本可以批量进行，即可以选中多个网元下的多个脚本同时进行下发操作。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树上，选择要配置的网元或者要下发的脚本，单击右键，选择“下发脚本”。

步骤 4 在“下发脚本”对话框中，在左侧“脚本选择”区域框中，选择要下发的脚本，在右侧可以查看该脚本的详细信息。

如果有需要修改的命令行或者参数，可以进行修改。

可以同时选择多个网元下面的多个脚本进行下发。

步骤 5 单击“下发”。

步骤 6 在弹出的提示框中，单击“确定”。

步骤 7 在“下发窗口”中显示脚本的执行过程。

如果某个脚本执行异常，可进行以下操作：

- 重试：系统将执行异常的命令重新执行。
- 忽略：系统将忽略执行异常的命令，继续进行下一条命令的执行。
- 终止：系统将终止脚本的执行。

步骤 8 单击“保存配置”，手动将配置结果保存到网元上。

步骤 9 单击“关闭”，完成下发。

----结束

9.5 常用维护操作

介绍模板和脚本的一些常用操作。

9.5.1 配置单个网元

智能工具提供了配置终端的功能，可以方便地对单个网元进行配置。

背景信息

说明

在网元管理器中的左侧导航树，选择“配置 > 业务配置”，可以配置单个网元。

配置终端的功能如下：

- 支持普通的命令行输入功能，进行网元的配置。
- 在“命令查询”框中，输入命令关键字后，可以查看和该命令关键字相关的命令。
- 支持历史命令的查询功能。

  历史命令是用户本次输入过的命令行的集合，方便用户查看对网元执行过的命令信息。

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树中，选择一个要配置的网元，单击右键，选择“配置终端”。

步骤 4 可以通过以下两种方式来配置单个网元。

- 在“配置信息”页签中，输入配置命令进行下发。
  1. 在“配置信息”页签中，输入命令关键字，单击  或按回车，可以查询和该命令相关的命令。
  2. 选择要配置的命令，并输入参数值。
  3. 单击“下发”。

     在“终端窗口”中将显示配置信息的结果。
- 在“终端窗口”中输入配置信息。

  通过“终端窗口”输入配置信息和通过 Telnet 登录网元进行配置一样。

步骤 5 **可选:** 通过选择“历史命令”页签可以查看历史命令。

注意

“历史命令”不能被转储或保存，当关闭一个网元的“配置终端”时，“历史命令”也将被删除。

----结束

9.5.2 导出网元列表

工具支持将网元信息导出并保存为.xls 格式文件。

背景信息

可以根据需要选择导出全部网元列表或部分网元列表。

操作步骤

- 导出部分网元列表步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。
  3. 选中“网元列表”导航树节点。
  4. 在右侧的“网元列表”区域按 Ctrl 键选中需要导出的网元。
  5. 在选中的网元上单击右键，选择“导出网元”。
  6. 在弹出的对话框中，选择“保存文件”，单击“确定”。

     说明

     - 如果使用的是 FireFox 浏览器，导出的文件默认被保存到“C:\Documents and Settings**osuser**\My Documents\下载”。其中，**osuser** 表示登录操作系统的用户名称。保存文件的路径可以通过如下方法修改：
       1. 在 FireFox 浏览器主菜单中，选择“工具 > 选项”。
       2. 在“下载”区域框中，单击“浏览”，设置保存文件的路径。
     - 如果使用的是 IE 浏览器，会弹出“另存为”对话框，在对话框中选择保存文件的路径。
- 导出全部网元列表的步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。
  3. 选中“网元列表”导航树节点。
  4. 在右侧“网元列表”区域选择“导出全部网元列表”。
  5. 在弹出的对话框中，选择“保存文件”，单击“确定”。

     说明

     - 如果使用的是 FireFox 浏览器，导出的文件默认被保存到“C:\Documents and Settings**osuser**\My Documents\下载”。其中，**osuser** 表示登录操作系统的用户名称。保存文件的路径可以通过如下方法修改：
       1. 在 FireFox 浏览器主菜单中，选择“工具 > 选项”。
       2. 在“下载”区域框中，单击“浏览”，设置保存文件的路径。
     - 如果使用的是 IE 浏览器，会弹出“另存为”对话框，在对话框中选择保存文件的路径。

----结束

9.5.3 维护模板

介绍模板的常用操作。

9.5.3.1 编辑模板

介绍如何修改模板中的命令和参数。

背景信息

通用模板和用户自定义的模板都可以编辑。

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 选择“模板”页签。

步骤 3 选择要修改的模板，右侧会显示出该模板的所有命令以及参数值。

步骤 4 单击“编辑”。可以通过如下几种方式编辑模板。

- 选择要修改描述的命令或视图，双击进行编辑。

  说明

  - 前面带*号的行表示必填参数。
  - 同一模板中如果两个参数描述相同，导出时会被合并成一个。
  - 命令中如果包含枚举类型的参数，且枚举值不完整，可以通过修改命令来添加枚举值。例如，**authentication-mode aaa** 命令中的 **aaa** 表示验证方式为 AAA 授权验证方式，验证方式还有其他两种 **password** 和 **none**。可以通过修改命令，将 **aaa** 修改为 **ENUM {aaa,none,password}**，则设置参数时，就可以选择任意一种认证方式。
- 双击参数值列，可输入或修改参数值。
- 单击视图节点中的图标，在弹出的对话框中可以修改命令视图。
- 将模板中不含参数的命令行设置为可选执行。
  1. 选中不含参数的命令行，单击“编辑命令”，在弹出的对话框中将命令行前后加上中括号。

     说明

     前后中括号和命令之间要用空格隔开。
  2. 单击“确定”。在命令右侧会出现一个复选框，选中复选框表示执行该命令，去选中复选框表示不执行该命令。
- 拷贝并粘贴命令。
  1. 选中要拷贝的命令或视图，单击复制。

     说明

     可以拷贝当前模板中的内容，也可以拷贝其他模板中的内容。
  2. 单击将拷贝的内容粘贴到新的位置。
     - 如果选中视图或其参数，复制的内容将被粘贴在该视图的最后一个节点处。
     - 如果选中命令或其参数，复制到内容将被粘贴在该命令的后面。
     - 如果将复制的内容粘贴到一个空模板中，则要求复制的内容包含根节点。
- 调整模板中命令的先后顺序。
  1. 单击可以将选中的命令或视图及其子节点上移。
  2. 单击可以将选中的命令或视图及其子节点下移。
- 删除命令或视图。

  选中要删除的命令或视图，单击删除。

  说明

  选中视图并删除时，视图下包含的命令会一并删除。

步骤 5 单击“保存”。

----结束

9.5.3.2 应用模板

通过应用模板可以快速生成配置脚本。

前提条件

如果需要生成多个网元的配置脚本，请提前准备好网络数据规划表。

背景信息

对于用户自定义模板和通用模板都可以进行应用模板操作。

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 选择“模板”页签。

步骤 3 在“模板列表”导航树中，选择要应用的模板，单击右键选择“应用模板”。

步骤 4 在“应用模板”对话框的“选择网元”区域框中，选择要应用模板的网元。单击“下一步”。

在“应用模板”对话框的“选择模板”区域框中，也可以选择多个模板应用到网元，或选择多个网元应用同一个模板。单击“下一步”，对其进行批量操作。

步骤 5 在“参数设置”页签中，设置命令的相关参数，单击“完成”。

说明

- 对于带星号的参数，都要设置其参数值。如果未填写参数值，生成的脚本不会包含该命令。
- 如果选择了多个模板，需要选择每一个模板页签设置其参数。

----结束

后续处理

1. 选择“脚本”页签。
2. 在“网元列表”导航树中，选择已经应用模板的网元，可以查看到网元下面增加了配置脚本，脚本名称和应用的模板名称相同。

9.5.3.3 导出模板

工具支持将所有配置模板导出并备份，便于后续修改或参考。

背景信息

可以根据需要选择导出部分模板或全部模板。

操作步骤

- 导出部分模板的步骤如下。

1. 在主菜单中选择“操作维护 > 智能配置工具”。
2. 选择“模板”页签。
3. 选中“模板列表”导航树节点。右侧会显示出所有配置模板。
4. 按 Ctrl 键选中要导出的配置模板。单击右键，选择“导出模板”。
5. 在弹出的对话框中，选择“保存文件”，单击“确定”。

   说明

   - 如果使用的是 FireFox 浏览器，导出的文件默认被保存到“C:\Documents and Settings **osuser**\My Documents\下载”。其中，**osuser** 表示登录操作系统的用户名称。保存文件的路径可以通过如下方法修改:
     1. 在 FireFox 浏览器主菜单中，选择“工具 > 选项”。
     2. 在“下载”区域框中，单击“浏览”，设置保存文件的路径。
   - 如果使用的是 IE 浏览器，会弹出“另存为”对话框，在对话框中选择保存文件的路径。

----结束

9.5.3.4 导入模板

智能工具提供了部分通用模板，如果有其他自定义的模板，可以通过此功能导入。

前提条件

已准备好需要导入的模板。

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 选择“模板”页签。

步骤 3 **可选:** 右键单击“模板列表”导航树节点，选择“创建文件夹”。

步骤 4 **可选:** 在“创建文件夹”对话框中，输入文件夹的名称，单击“确定”。

步骤 5 选中“模板列表”节点或新建的文件夹，单击右键选择“导入模板”。

步骤 6 在弹出的对话框中选择“浏览”，选择要导入的模板。

步骤 7 单击“导入”。导航树中会出现相应的模板。

----结束

9.5.4 维护脚本

介绍脚本的常用操作。

9.5.4.1 手动新建脚本

脚本中包括了网元的配置信息，本节介绍如何手工新建脚本。

背景信息

创建脚本有三种方法，本节只介绍手动新建脚本的方法。

- 手动新建：通过手工输入命令的方法创建脚本。

  说明

  如果脚本命令行数量较大，建议分成多个脚本，使每个脚本的命令行数控制在 200 以内，否则会影响验证脚本和下发脚本的效率。

- 应用模板创建：通过应用模板的方法创建脚本，其中模板可以是通用模板，也可以是自定义的模板。具体操作请参见 **9.5.3.2 应用模板**。
- 导入规划表创建：已经有模板的情况下，可以从模板导出规划表，填写参数信息后，再导入规划表生成脚本。具体操作请参见 **9.4.4 导入规划数据**

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 选择“脚本”页签。

步骤 3 在“网元列表”导航树中，选择一个要创建脚本的网元，单击右键，选择“创建脚本”。

步骤 4 在“创建脚本”对话框中，输入“脚本名称”和“描述”，单击“确定”。

创建的脚本将出现在网元节点的下一级。

步骤 5 在右侧“脚本配置”区域，单击编辑脚本。

步骤 6 在空白区域输入命令行信息。

在查询框中，输入命令关键字，单击或按回车，可以查询和该关键字相关的命令。

步骤 7 输入完成后，单击保存配置。

命令行将以彩色显示，视图命令将会加粗显示。

说明

单击保存后，如果脚本的字体黑色，则说明该网元没有设置网元类型和网元版本信息，请获取命令集，详细操作请参见 **9.4.1 获取命令集**。

步骤 8 **可选:** 如果有错误的命令行，将以红色标识出来。请修改红色出错的命令行，再次单击保存配置，直到没有错误为止。

窍门

保存配置脚本后，如果有出错的命令行，请参见 **9.4.5 验证脚本**中对于出错命令行的处理方法。

----结束

9.5.4.2 编辑脚本

介绍如何修改网元的配置脚本。

前提条件

网元下已经存在脚本。

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 选择“脚本”页签。

步骤 3 展开“网元列表”节点，选择一个网元下需要修改的脚本。

步骤 4 在右侧单击编辑脚本。

步骤 5 根据需要修改脚本中的命令行。

步骤 6 单击“保存”。

----结束

9.5.4.3 导出脚本

网元配置脚本可以使用工具导出，以便于后续验证脚本或定位问题，也可以作为配置其他网元时的参考。

背景信息

可以根据需要选择导出部分脚本或全部脚本。

操作步骤

- 导出部分脚本的步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。
  3. 选中“网元列表”下的需要导出脚本的网元，右侧会列出该网元的所有配置脚本。
  4. 按 Ctrl 键选中要导出的配置脚本。单击右键，选择“导出脚本”。
  5. 在弹出的对话框中，选择“保存文件”，单击“确定”。

     说明

     - 如果使用的是 FireFox 浏览器，导出的文件默认被保存到“C:\Documents and Settings**osuser**\My Documents\下载”。其中，**osuser** 表示登录操作系统的用户名称。保存文件的路径可以通过如下方法修改：
       1. 在 FireFox 浏览器主菜单中，选择“工具 > 选项”。
       2. 在“下载”区域框中，单击“浏览”，设置保存文件的路径。
     - 如果使用的是 IE 浏览器，会弹出“另存为”对话框，在对话框中选择保存文件的路径。
- 导出所有网元的全部脚本步骤如下。
  1. 在主菜单中选择“操作维护 > 智能配置工具”。
  2. 选择“脚本”页签。
  3. 选中“网元列表”下的需要导出脚本的网元，右侧会列出该网元的所有配置脚本。
  4. **可选:** 在右侧的“属性”下拉菜单中选择“全部”。
  5. 单击“导出全部脚本”。
  6. 在弹出的对话框中，选择“保存文件”，单击“确定”。

说明

- 如果使用的是 FireFox 浏览器，导出的文件默认被保存到“C:\Documents and Settings **osuser**\My Documents\下载”。其中，**osuser** 表示登录操作系统的用户名称。保存文件的路径可以通过如下方法修改：
  1. 在 FireFox 浏览器主菜单中，选择“工具 > 选项”。
  2. 在“下载”区域框中，单击“浏览”，设置保存文件的路径。
- 如果使用的是 IE 浏览器，会弹出“另存为”对话框，在对话框中选择保存文件的路径。

----结束

9.5.4.4 导入脚本

从其他网元导出的配置脚本，可以使用工具导入到要配置的网元，如果网元之间的配置方法类似，可以大大节约制作脚本的时间。

背景信息

可以根据需要给一个网元或多个网元导入脚本。支持导入.zip 和.txt 格式的脚本文件。

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 选择“脚本”页签。

步骤 3 选中“网元列表”节点，右侧会列出所有网元。

步骤 4 在右侧列表中选择一个或多个需要导入脚本的网元，单击右键选择“导入脚本”。

步骤 5 在弹出的对话框中选择“浏览”，选择要导入的脚本。

步骤 6 单击“导入”。网元节点下会出现相应的脚本。

----结束

9.5.4.5 定时下发脚本

介绍如何创建定时任务。工具支持下发一次、按天下发、按周下发和按月下发。

前提条件

已经新建或导入网元。

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 选择“脚本”页签。

步骤 3 在“网元列表”节点上单击右键。

步骤 4 选择“定时下发”。

步骤 5 在弹出的对话框中，单击“增加”。

步骤 6 在弹出的“新建下发任务”对话框中，单击 > 或 >> 将需要定时下发脚本的设备添加到已选设备列表中。

步骤 7 单击“下一步”。

步骤 8 输入需要定时下发的脚本。单击“下一步”。

说明

脚本将会按时自动下发，请不要输入有人机交互过程的命令。

步骤 9 输入以下定时任务基本信息。

- 定时任务名称
- 日志子目录
- 厂商
- 备注
- 周期类型
- 下发日期、下发频率、启动时间

步骤 10 单击“完成”。

步骤 11 在“定时下发任务管理”对话框中，显示一条定时任务的记录。

----结束

后续处理

创建完定时下发任务，还可以根据需要进行如下操作。

- 修改定时任务
  1. 在“定时下发任务管理”对话框中，选中一项需要修改的定时任务，单击右键。
  2. 选择“修改任务”。
  3. 修改任务属性后，单击“完成”。
- 下载定时任务的日志
  1. 在“定时下发任务管理”对话框中，选中一项需要下载日志的定时任务，单击右键，选择“下载日志”。
  2. 在弹出的对话框中，选择日志的生成时间段。单击“确定”。
  3. 在弹出的对话框中，选择“保存文件”，单击“确定”。
- 清除定时任务的日志
  1. 在“定时下发任务管理”对话框中，选中一项需要清除日志的定时任务，单击右键，选择“清除日志”。
  2. 在弹出的对话框中，选择日志的生成时间段。单击“确定”。
  3. 在弹出的确认删除对话框中，单击“确定”。定时的任务的日志会从服务器中删除。

10 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。

10.1 了解网元配置数据备份与恢复

为了减少灾害带来的损失，通过配置文件备份将设备上的配置文件备份到网管,在灾害消失时通过恢复，将网管上的备份文件恢复至设备上，实现容灾。

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。

10.2 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。

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

10.3 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，单击“应用”。

----结束

10.4 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。

10.4.1 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。

10.4.1.1 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 **10.2 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

10.4.1.2 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

10.4.1.3 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

10.4.2 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 **10.2 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 在左侧导航树上选择“设备配置管理 > 配置文件”。

步骤 3 选中相应的设备，单击“备份”。

----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时，且备份的文件已达到上限，则网管默认丢弃最早的非基线配置文件。

10.5 管理网元配置数据

介绍管理网元配置数据的常用操作。

10.5.1 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

10.5.2 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

10.5.3 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

10.5.4 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

10.5.5 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

11 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。

11.1 了解自定义设备管理
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。

11.2 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

11.3 自定义设备管理流程
介绍自定义设备的管理流程。

11.4 设置自定义设备基本信息
介绍设置自定义设备的厂商信息和设备类型信息的方法。

11.5 设置自定义设备管理能力
根据需要定制自定义设备的告警参数、性能指标、配置文件和性能面板。

11.6 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。

11.7 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。

11.1 了解自定义设备管理

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。支持在面板上显示第三方设备私有 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。

11.2 自定义设备功能介绍

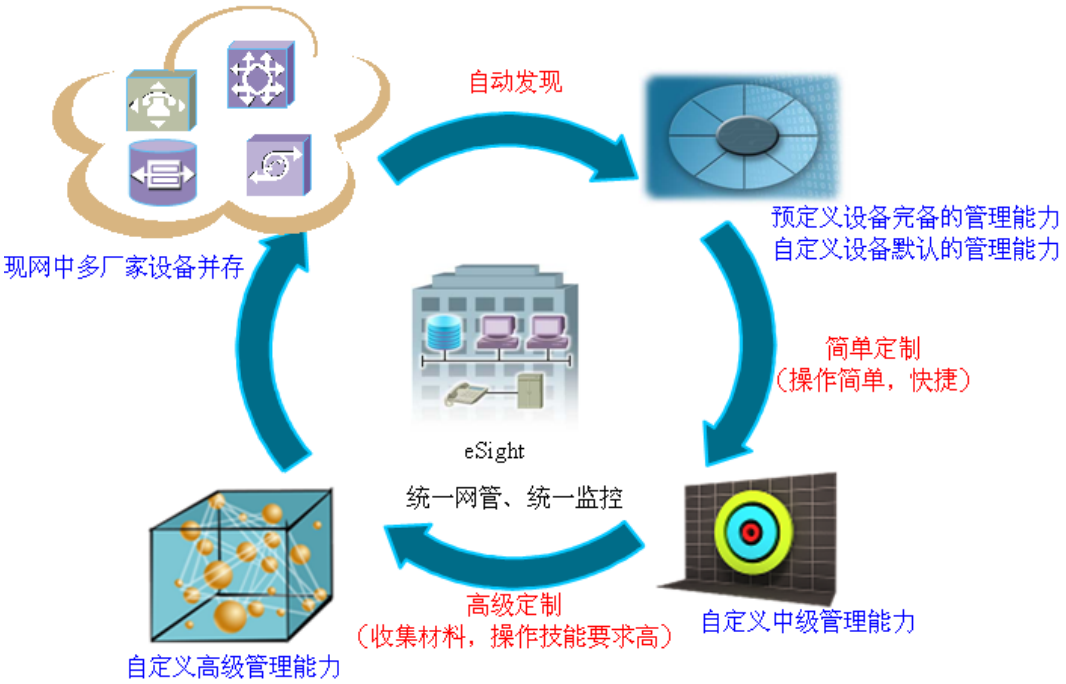
eSight 提供统一的管理平台，可以将现网所有支持 SNMP 协议的设备添加到网管，对于预集成设备，eSight 提供完善的管理能力，对于自定义设备（设备类型为 Huawei Device/ H3C Device/Cisco Device/Unknow）提供定制功能，客户根据需要对其定制，从而实现 eSight 对现网多厂商设备的统一管理和统一监控

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。



判断是否需要定制

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，但是有些执行结果提示可能与实际不符。

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			

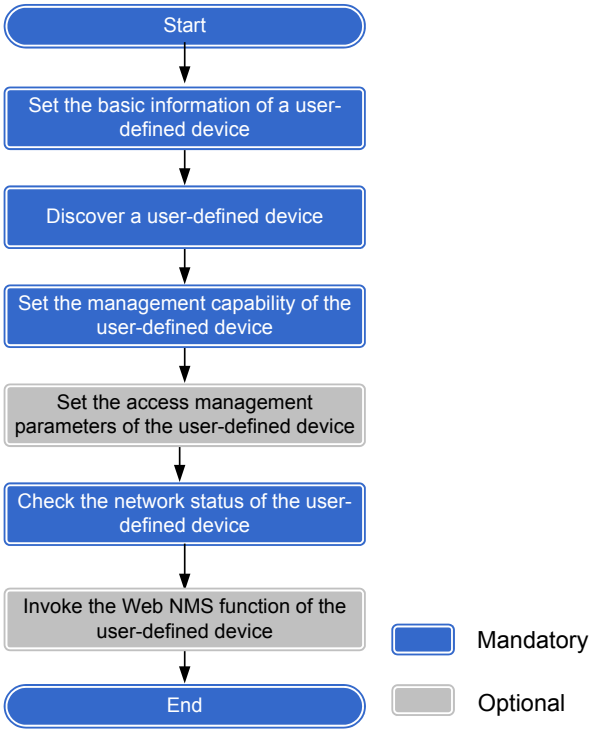
场景	定制项	定制准备材料	适用范围
告警	定制告警，对其进行监控管理。 定制工时：1 时/条 具体步骤，请参见 **11.5.1 自定义告警参数**。	● 要定制告警的 trapOID ● VB（mib 节点信息） **说明** 以上材料需向厂家获取。	HuaweiDevice/H3C Device/Cisco Device/Unknown
性能指标	Huawei Device/H3C Device/Cisco Device 默认支持的性能指标同各自预定义设备一致。 Unknown 设备默认不支持性能指标，需要定制其性能指标。 定制工时：2 时/条 具体步骤，请参见 **11.5.2 自定义性能指标**。	● 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 **11.5.3 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 **11.5.4 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

11.3 自定义设备管理流程

介绍自定义设备的管理流程。

自定义设备的管理流程如图 11-1 所示。

图 11-1 自定义设备管理流程



操作	备注
1、11.4 设置自定义设备基本信息	设置自定义设备的厂商信息和设备类型信息。
2、3.1.1.2 创建网元	将自定义设备发现到网管上，对其进行管理。
3、11.5 设置自定义设备管理能力	根据自定义设备的需要，对其告警参数、性能指标、配置文件和网元面板进行定制。
4(可选)、7.3.2 配置协议参数	若自定义设备的 SNMP 协议和 Telnet 协议参数有变化，需配置 SNMP 协议和 Telnet 协议参数保持和网元一致，以便对网元进行管理。
5、11.6 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，实时了解网管与自定义设备之间通信状态。

操作	备注
6（可选）、11.7 调用自定义设备的 Web 网管	调用自定义设备的 web 网管，对其进行相关配置操作。

11.4 设置自定义设备基本信息

介绍设置自定义设备的厂商信息和设备类型信息的方法。

11.4.1 定制厂商基本信息

设置自定义设备厂商信息，便于将自定义设备分配到自定义厂商。

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 在左侧窗口中选择“设备基本信息定制 > 厂商基本信息定制”，单击“创建”。

步骤 3 设置自定义厂商基本信息，单击“确定”。

步骤 4 **可选:** 在“厂商基本信息定制”查看自定义设备的厂商信息，根据需要单击修改其相关信息。

----结束

11.4.2 定制设备类型信息

自定义设备厂商信息后，需要对该厂商的设备类型信息进行设置。

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 在左侧窗口中选择“设备基本信息定制 > 设备类型信息定制”，单击“创建”。

步骤 3 设置设备类型的相关信息，单击“确定”。

步骤 4 **可选:** 在“设备类型信息定制”查看自定义设备的类型信息，根据需要单击修改其相关信息。

----结束

11.5 设置自定义设备管理能力

根据需要定制自定义设备的告警参数、性能指标、配置文件和性能面板。

11.5.1 自定义告警参数

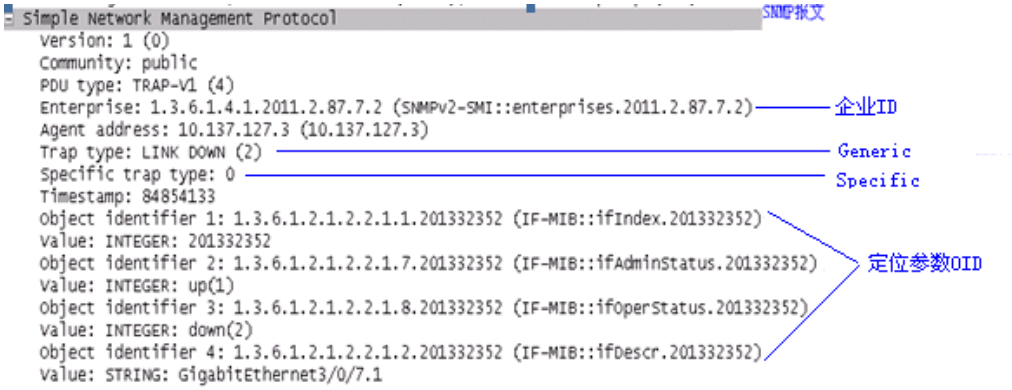
对于第三方设备私有的 SNMP 告警，可以通过网管定制方式将其上报到网管上进行管理。

背景信息

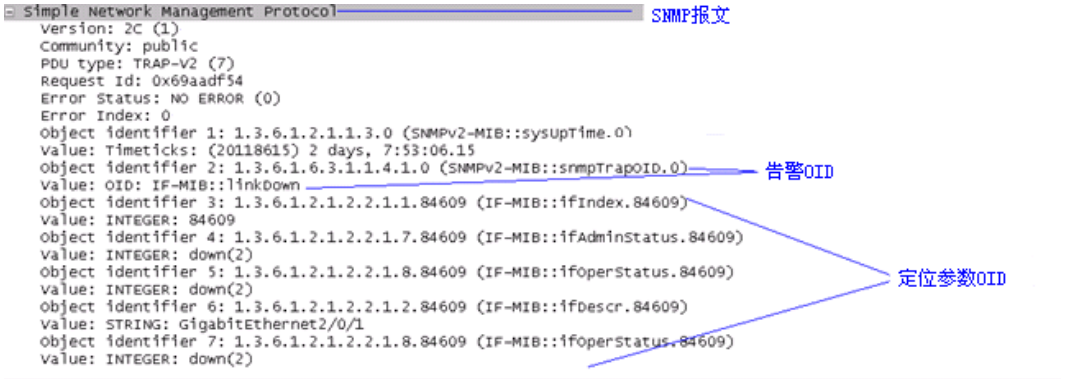
定制告警的 Trap ID 以及定位告警参数的 MIB 节点信息，需要向厂家获取。

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：



SNMPV2 报文结构：



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。单击“创建”，在“创建告警参数”页签下配置自定告警的相关参数，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. 单击“创建”，在“创建告警参数”页签下配置“通知类型”为“恢复告警”。
2. 单击“选择”，选择相应的告警，单击“确定”。

3. 对于恢复告警，仅需设置告警 OID，其它参数网管已适配，不需要配置，单击“确定”。

----结束

后续处理

在“告警定制”窗口下可以查看自定制的告警信息。

11.5.2 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。

定制性能的指标 MIB 节点信息，需要向厂家获取。

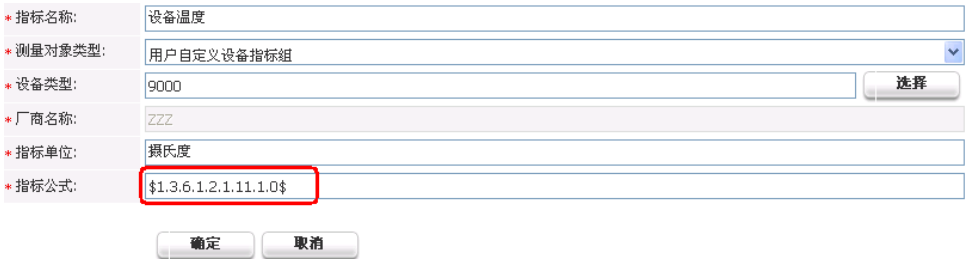
操作步骤

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。

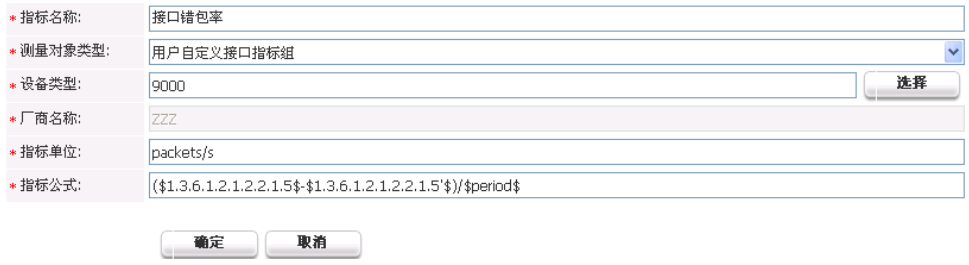
1. 创建自定义设备指标。单击“创建”，在“创建性能指标”页签下配置设备性能指标参数，单击“确定”。



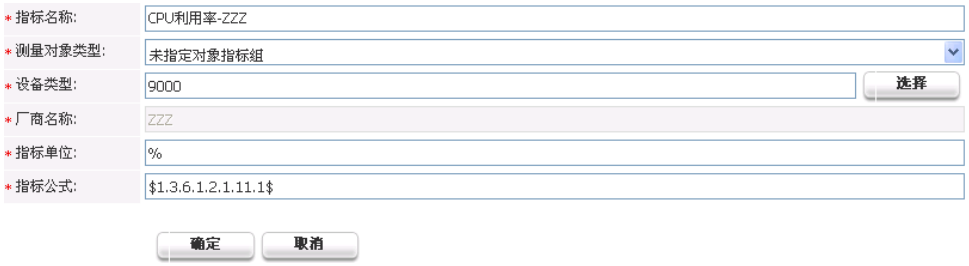
说明

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 > 性能监控设置”，单击“创建”。
2. 单击“选择管理对象”，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

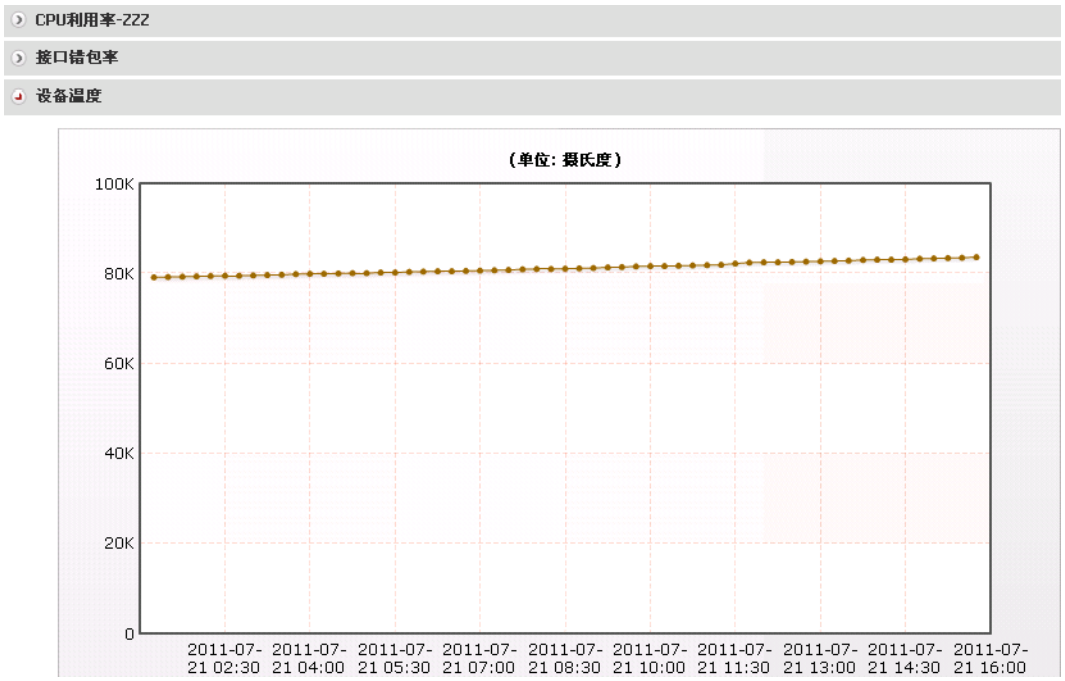
对于未指定对象指标组，需要手工设置具体的监视对象。

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

在网元管理器中的可查看自定制的性能状态。



11.5.3 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. 在左侧导航树选择“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”，选择自定制设备，单击“确定”，将备份任务应用到这些设备上。

----结束

11.5.4 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。

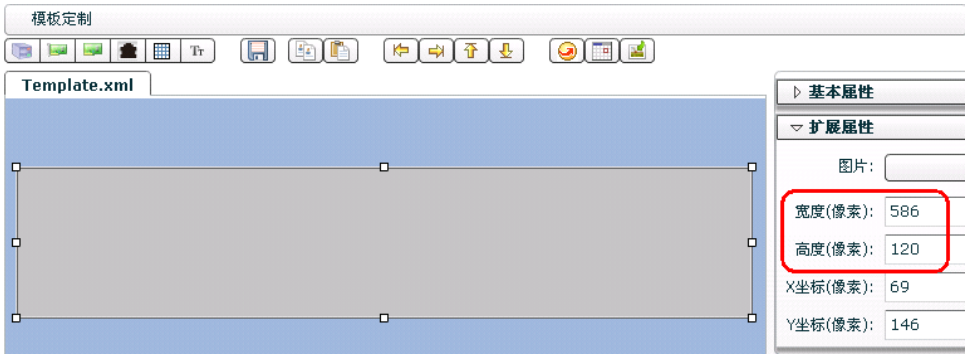
步骤 2 在左侧导航树选择“查看 > 设备面板”，在右侧窗口中显示的是网管默认为第三方设备提供的面板图。

步骤 3 定制机框。

1. 右键单击机框，选择“定制模板”。

2. 机框实体类型和实体型号网管已适配，不需要设置，单击“下一步”。

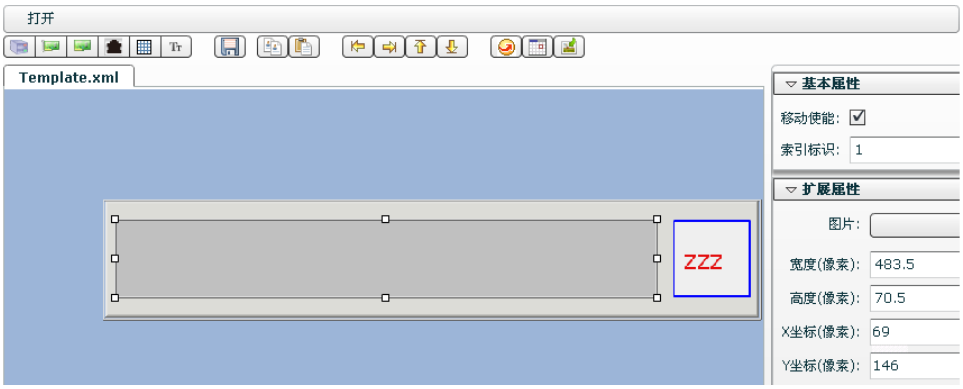
3. 设置机框大小，单击“创建模板”，在“模板定制”窗口的菜单栏中选择槽位图标，将其拖入编辑器，根据机框图片大小设置槽位的大小。



4. 选择机框图标，将其拖入步骤**步骤 3.3** 创建的槽位中。

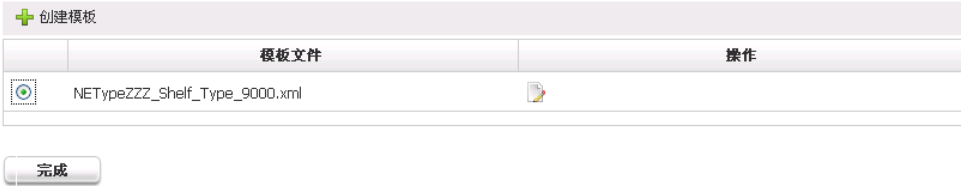
5. 单击上传本地机框图片，在“扩展属性”下选择上传的机框图片。

6. 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”。



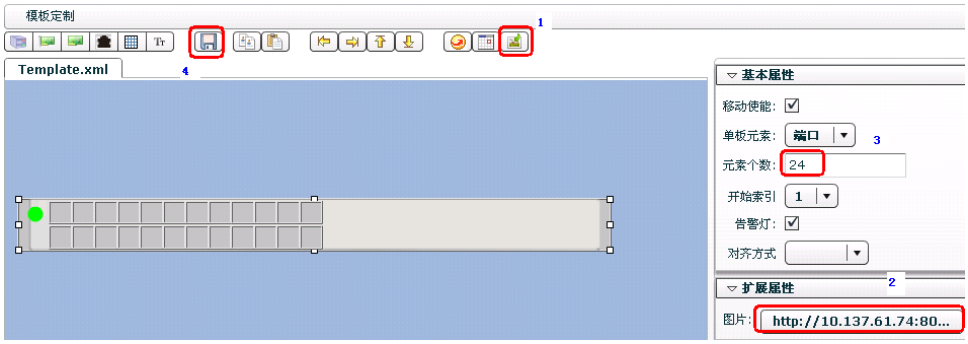
7. 单击  保存模板设置机框模板的名称，单击“保存”。

8. 在右上角单击“返回”，选择刚保存的机框模板，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“定制模板”。
2. 单板的实体类型和实体型号网管已适配，不需要设置，单击“下一步”。
3. 设置单板大小，单击“创建模板”，在“模板定制”窗口的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。
4. 选择单板图标  ，将单板拖入步骤**步骤 4.3** 创建的槽位中。
5. 单击  上传本地机框图片，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。

6. 单击保存模板设置单板模板的名称，单击“保存”。

7. 在右上角单击“返回”，选择刚保存的单板模板，单击“完成”。

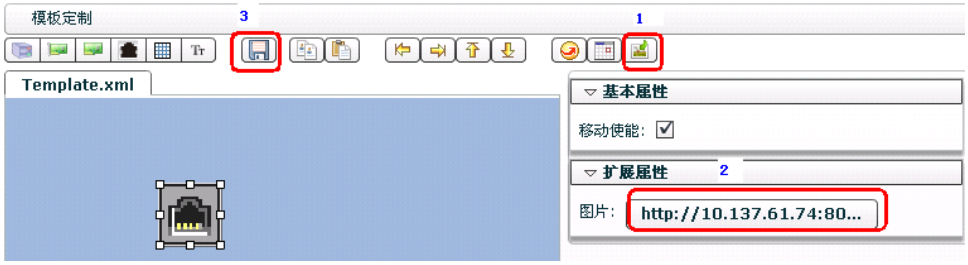
步骤 5 定制端口模板。

1. 在网元管理器下的设备面板页签下，右键单击端口，选择“定制模板”。

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. 端口的实体类型和实体型号网管已适配，不需要设置，单击“下一步”。
3. 设置端口大小，单击“创建模板”，在“模板定制”窗口的菜单栏中选择槽位，将其拖入编辑器，根据端口图片大小设置槽位的大小。
4. 选择端口图标，将端口拖入步骤**步骤 5.3** 创建的槽位中。
5. 单击上传本地端口图片，在“扩展属性”下选择刚上传的图片。



6. 单击保存模板设置端口模板的名称，单击“保存”。
7. 在右上角单击“返回”，选择刚保存的端口模板，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”，查看自定制的设备面板。

11.6 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。

11.6.1 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

11.6.2 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

11.6.3 查询接口基本信息

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。

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

11.6.4 查询 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”窗口中单击“查看详情”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

11.7 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

12 系统管理

关于本章

12.1 系统设置

网管系统在正式运行之前通常需要进行一些设置，请在安装网管系统后根据实际情况进行以下设置。

12.1.1 设置日志溢出转储

为了避免数据库表空间不足，eSight 系统提供了日志溢出转储设置功能。系统可以按照条件每日检测审计日志数据是否溢出，如果溢出，则系统自动将数据转储到您指定路径下进行保存。

背景信息

数据库表空间使用率超出设置的数据库空间阈值，说明数据溢出。

eSight 每日在设置的时刻检测数据库中安全表空间的使用率，如果使用率超过阈值，系统按日志记录月份的先后顺序将最早月份记录的审计日志数据（安全日志、操作日志和系统日志）转储到设置的保存文件路径下，并将这些数据从数据库中删除，直到使用率低于阈值。转储后系统会检测转储目录中文件的总大小和保存时间，如果文件的总大小或者文件保存的时间超过设置的值，系统将删除最早的转储文件，直到满足设置的值。

操作步骤

步骤 1 选择“系统 > 系统配置”。

步骤 2 在左侧导航树中选择“数据库溢出转储 > 日志数据库溢出转储”。

步骤 3 设置日志转储参数。

说明

“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网管安装路径“%ENT_ROOT%/run/dump”（以 LWindows 操作系统为例）而言，例如输入 AAA，则表示文件将保存到“%ENT_ROOT%/run/dump/AAA”下。

步骤 4 单击“应用”。

----结束

12.1.2 设置告警溢出转储

为了避免数据库表空间不足，eSight 系统提供了告警溢出设置功能。系统可以按照条件每日检测告警数据是否溢出，如果溢出，则系统自动将数据转储到您指定路径下进行保存。

背景信息

数据库表空间使用率超出设置的数据库空间阈值，说明数据溢出。

eSight 每日在设置的时刻检测数据库中告警管理表空间的使用率，如果使用率超过阈值，系统按告警上报月份的先后顺序将最早月份上报的告警数据（包括历史告警、已清除的被屏蔽告警和事件列表数据）转储到设置的保存文件路径下，并将这些数据从数据库中删除，直到使用率低于阈值。转储后系统会检测转储目录中文件的总大小和保存时

间，如果文件的总大小或者文件保存的时间超过设置的值，系统将删除最早的转储文件，直到满足设置的值。

操作步骤

步骤 1 选择“系统 > 系统配置”。

步骤 2 在左侧导航树中选择“数据库溢出转储 > 告警数据库溢出转储”。

步骤 3 设置告警转储参数。

说明

“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网管安装路径“%ENT_ROOT%/run/dump”（以 LWindows 操作系统为例）而言，例如输入 AAA，则表示文件将保存到“%ENT_ROOT%/run/dump/AAA”下。

步骤 4 单击“应用”。

----结束

12.1.3 设置性能溢出转储

为了避免数据库表空间不足，eSight 系统提供了性能溢出转储设置功能。系统可以按照条件每日检测性能数据是否溢出，如果溢出，则系统自动将数据转储到您指定路径下进行保存。

背景信息

数据库表空间使用率超出设置的数据库空间阈值，说明数据溢出。

eSight 每日在设置的时刻检测数据库中性能管理表空间的使用率，如果使用率超过阈值，系统按采集月份的先后顺序将最早月份采集的性能数据转储到设置的保存文件路径下，并将这些数据从数据库中删除，直到使用率低于阈值。转储后系统会检测转储目录中文件的总大小和保存时间，如果文件的总大小或者文件保存的时间超过设置的值，系统将删除最早的转储文件，直到满足设置的值。

操作步骤

步骤 1 选择“系统 > 系统配置”。

步骤 2 在左侧导航树中选择“数据库溢出转储 > 性能数据库溢出转储”。

步骤 3 设置性能转储参数。

说明

“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网管安装路径“%ENT_ROOT%/run/dump”（以 LWindows 操作系统为例）而言，例如输入 AAA，则表示文件将保存到“%ENT_ROOT%/run/dump/AAA”下。

步骤 4 单击“应用”。

----结束

12.2 日志管理

日志记录操作网管的信息以及 eSight 中发生的重要事件。通过日志管理功能，可以查询日志信息。

12.2.1 日志类型介绍

eSight 的日志包括操作日志、系统日志和安全日志。

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、修改资源管理器等。

12.2.2 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。

背景信息

- 如果您没有设置任何查询条件，则表示查询所有的安全日志。
- 查询结果都基于数据库中的现有数据。如果数据未产生，则相关信息就不会显示。

操作步骤

步骤 1 选择“系统 > 日志管理”。

步骤 2 在左侧导航树中选择“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“详细信息”，可以查看详细的日志信息。

----结束

12.2.3 查询系统日志

可以通过查询系统日志了解涉及系统操作的相关信息。

背景信息

- 如果您没有设置任何查询条件，则表示查询所有的系统日志。
- 查询结果都基于数据库中的现有数据。如果数据未产生，则相关信息就不会显示。

操作步骤

步骤 1 选择“系统 > 日志管理”。

步骤 2 在左侧导航树中选择“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“详细信息”，可以查看详细的日志信息。

----结束

12.2.4 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。

背景信息

- 如果您没有设置任何查询条件，则表示查询所有的操作日志。
- 查询结果都基于数据库中的现有数据。如果数据未产生，则相关信息就不会显示。
- 用户成功登录系统后，可以查看所有用户的操作日志。

操作步骤

步骤 1 选择“系统 > 日志管理”。

步骤 2 在左侧导航树中选择“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。

单击“详细信息”，可以查看详细的日志信息。

如果查看的是批量操作的日志详细信息，您还可以单击“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

12.3 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。

12.3.1 了解下级网管

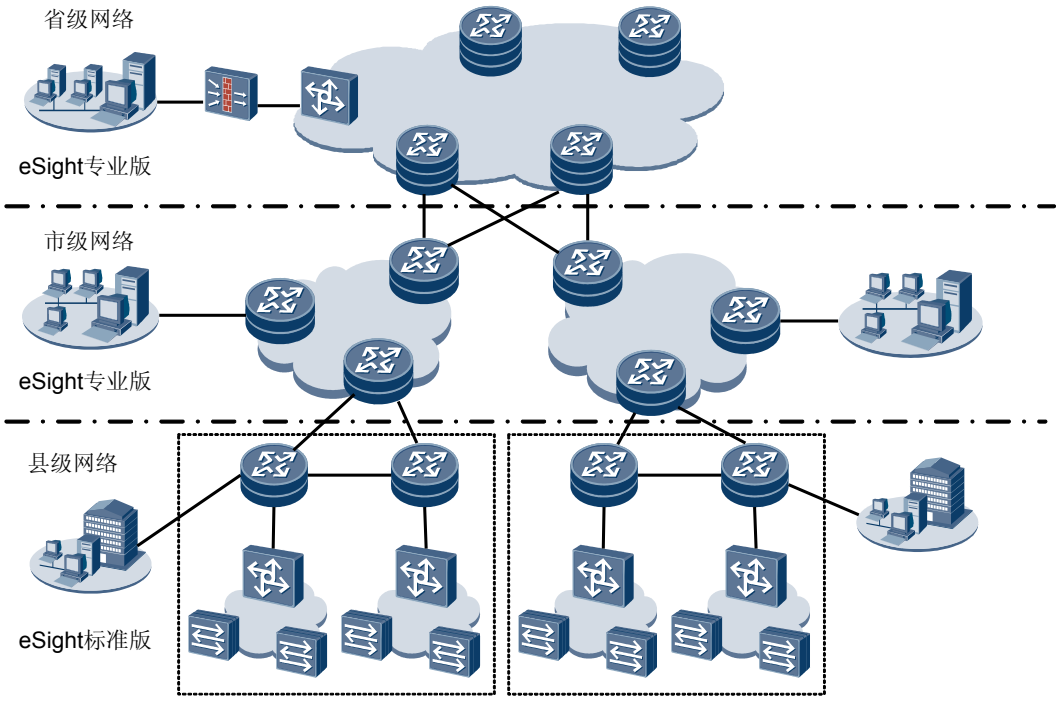
eSight 网管需要建立分级的层次化关系，用户能够按照地域、组织结构等层次关系，划分管理区域，建立起层次化的管理体系，上级网管的权限大于下级网管的权限，上级网管能够管理下级网管，下级网管没有管理上级的权限。

12.3.1.1 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，将原本一套网管管理的能力分散到多套网管中。

如图 12-1 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 12-1 下级网管的应用



12.3.1.2 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，并作单点登陆。

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。

12.3.2 管理下级网管

介绍管理下级网管的操作任务。

12.3.2.1 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”、“用户名”、“密码”。

步骤 3 单击“确定”。

----结束

12.3.2.2 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，修改下级网管的相关参数。单击“确定”。

步骤 5 **可选:** 单击相应下级网管的“网管名称”，进入下级网管，对下级网管进行管理。

----结束

12.3.2.3 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”，网管将检测所有下级网管的连通性状态。

说明

不用选择相应的下级网管，网管默认检测所有下级网管的连通性状态。

----结束

12.4 License 管理

您需要获取 License 后才具有使用 eSight 的权限。License 用于对 eSight 资源和功能进行控制。

12.4.1 查看系统当前 License

系统支持查看当前使用的 License 的所有信息。

前提条件

您已导入 License。

背景信息

License 信息详细说明如表 12-1 所示。

表 12-1 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

类别	属性	说明	举例
	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。

如果当前 License 将要过期，请及时导入新的有效 License。参见 **12.4.2 导入 License**。

----结束

12.4.2 导入 License

当 eSight 没有导入 License 或原有 License 过期时，您需要导入新的 License。

前提条件

您已向华为购买了新的 License。

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。

步骤 2 单击“导入 License”。

步骤 3 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

12.5 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数据库备份恢复工具。

- Windows 操作系统：单击“开始 > 所有程序 > eSight > tools > 启动数据库备份恢复工具”。
- Linux 操作系统：在安装路径“eSight\backuptool\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，登陆数据库备份恢复工具。

登录 url 地址示例：http://10.135.23.61:8130/backup。

说明

端口号固定为 8130。

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”。

网管提供默认的备份路径为安装目录（如 eSight）同级的目录 backupdata 中。

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 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。

13.1 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。

13.2 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。

13.3 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。

13.4 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。

13.5 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。

13.6 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。

13.1 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 13-1 维护项目列表

维护周期	例行维护任务
每日	13.3.1 浏览当前告警
	13.3.2 查询安全日志
每周	13.4.1 检查服务器磁盘状态
	13.4.2 检查服务器磁盘空间
	13.4.3 检查 Oracle 数据库日志
	13.4.4 检查防病毒软件运行状态
每月	13.5.1 维护用户
	13.5.2 修改当前用户密码
每季度	13.6.1 检查机房环境
	13.6.2 检查服务器供电情况
	13.6.3 检查服务器硬件和外设

13.2 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。

13.3 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。

13.3.1 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。

背景信息

- 对于新上报的告警，只要告警列表中存在符合归并规则的告警记录，都将该告警归并到告警列表中，归并后告警次数加一，当前告警列表是告警归并后的展示。

  默认的告警归并规则：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。
- 在“当前告警”窗口中可以查看每条告警的信息。
- 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。
- 在浏览当前告警时，通过单击  定制显示列。

操作步骤

步骤 1 在主菜单中选择“故障 > 当前告警”。

步骤 2 在“过滤条件”下拉菜单中，选择条件进行查询，如果不满足需求可以自定义过滤条件，请参见 4.2.4.5 设置告警自定义过滤条件。

步骤 3 在“当前告警”窗口中，可进行如下操作。

表 13-2 “当前告警”窗口操作

操作名称	操作方法	说明
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。 ● 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。 状态： ● 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。	-

操作名称	操作方法	说明
搜索	在窗口中支持如下搜索方式： ● 不设置任何条件直接点击“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”。	● 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”。	通过反确认后，告警由确认状态变成未确认状态。
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”。	● 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。
拓扑定位	在窗口中选择一条告警，在操作栏中单击  。	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

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。

背景信息

- 如果您没有设置任何查询条件，则表示查询所有的安全日志。
- 查询结果都基于数据库中的现有数据。如果数据未产生，则相关信息就不会显示。

操作步骤

步骤 1 选择“系统 > 日志管理”。

步骤 2 在左侧导航树中选择“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“详细信息”，可以查看详细的日志信息。

----结束

13.4 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。

13.4.1 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：

     # **iostat -E**

     屏幕显示类似如下信息：

     ```
     sd1       Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
     Vendor: HITACHI  Product: H101414SCSUN146G Revision: SA25 Serial No: 0848E3PKSA
     Size: 146.80GB <146800115712 bytes>
     ```

```
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
```

----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 **vxdisk list** 后，磁盘状态均为“online”，执行 **iostat -E** 后，硬盘的“Hard Errors”信息为“0”，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。

13.4.2 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”窗口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%。

13.4.3 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。

操作步骤

检查“$ORACLE_BASE/diag/rdbms/$ORACLE_SID/$ORACLE_SID/trace/”目录下的 *alert_$ORACLE_SID.log* 日志文件。

参考标准

日志文件中没有 ORA-*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。

13.4.4 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。

13.5 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。

13.5.1 维护用户

用户创建后，安全管理员可以查看和修改用户信息。

前提条件

拥有维护用户权限的用户登录系统。

操作步骤

步骤 1 在主菜单中选择“系统 > 安全管理”。

步骤 2 在左边导航树上选择“权限分配 > 用户”。

步骤 3 在“用户”窗口中，可以进行下面操作。

操作名称	操作方法
查看	1. 选择需要查看的用户，单击用户名。 2. 查看相关信息。

操作名称	操作方法
修改	1. 选择需要修改信息的用户，单击“  ”。 2. 修改相关信息。 3. 单击“确认”。
重置密码	1. 选择需要修改密码的用户，单击“  ”。 2. 修改密码。 3. 单击“确认”。 **说明** 不可以修改系统缺省管理员的密码。
删除	1. 选择需要删除的用户，单击“  ”。 2. 确认系统提示。 **说明** 不可以删除系统缺省管理员和当前用户。
启用/停用	1. 选择需要启用/停用的用户，单击“  /  ”。 2. 在使用状态栏，显示当前用户使用状态。

----结束

13.5.2 修改当前用户密码

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

13.6 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。

13.6.1 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。

13.6.2 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 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*

more */var/log/warn*

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。

13.6.3 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。

A 术语

A

AH	见 **Authentication Header; 报文认证头协议。**
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。

D

DHCP	见 **Dynamic Host Configuration Protocol; 动态主机配置协议。**
DNS	见 **Domain Name Service; 域名业务。**
Domain Name Service (DNS); 域名业务	一个连接到互联网或专用网络的计算机，服务，或资源的分级命名系统。该系统将各种信息与分配给每一个参加者的域名联系起来。它负责分配域名并且通过为每个域指定权威的服务器来将这些域名与其相应的 IP 地址相互映射。
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联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。

I

IETF	见 **Internet Engineering Task Force; Internet 工程任务组。**
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。**
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 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。

S

隧道	分组交换网中在 PE 之间传输业务流量的通道。VPN 应用中两个实体间建立的信息传输通道，提供足够安全性，确保 VPN 的内部信息不受外部侵扰，完成实体之间的数据透传。一般情况下为 MPLS 隧道。

T

TCP	见 **Transmission Control Protocol; 传输控制协议。**
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。

W

WLAN	见 **Wireless Local Area Network; 无线局域网。**
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。