H3C 智能管理中心

用户手册

新华三技术有限公司
http://www.h3c.com

资料版本：5W133-20250310
产品版本：iMC PLAT 7.3 (E0708)

Copyright © 2007-2025 新华三技术有限公司及其许可者 版权所有，保留一切权利。

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

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C 智能管理中心 用户手册包括六个章节，用于快速引导用户了解并使用 iMC 以及帮助用户解决使用过程中遇到的问题。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 产品配套资料
- 资料意见反馈

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。

产品配套资料

H3C 智能管理中心的配套资料包括如下部分：

大类	资料名称	内容介绍
操作系统安装	Red Hat Enterprise Linux Server 7.4 安装指导	帮助您了解Red Hat Enterprise Server Linux 7.4的安装及配置方法
	Red Hat Enterprise Linux Server 8.1 安装指导	帮助您了解Red Hat Enterprise Server Linux 8.1的安装及配置方法
数据库安装	SQL Server 2012安装配置指导书	帮助您了解SQL Server 2012的安装及配置方法
	SQL Server 2014安装配置指导书	帮助您了解SQL Server 2014的安装及配置方法
	SQL Server 2016安装配置指导书	帮助您了解SQL Server 2016的安装及配置方法
	SQL Server 2017安装配置指导书	帮助您了解SQL Server 2017的安装及配置方法
	SQL Server 2019安装配置指导书	帮助您了解SQL Server 2019的安装及配置方法
	Oracle 11g安装配置指导书	帮助您了解Oracle 11g的安装及配置方法
	Oracle 11g R2安装配置指导书	帮助您了解Oracle 11g R2的安装及配置方法
	Oracle 12c安装配置指导书	帮助您了解Oracle 12c的安装及配置方法
	Oracle 12c R2安装配置指导书	帮助您了解Oracle 12c R2的安装及配置方法
	Oracle 18c安装配置指导书	帮助您了解Oracle 18c的安装及配置方法
	Oracle 19c安装配置指导书	帮助您了解Oracle 19c的安装及配置方法
	MySQL 5.5.62安装配置指导书(Linux)	帮助您了解Linux操作系统下MySQL 5.5.62的安装及配置方法
	MySQL 5.5.62安装配置指导书(Windows)	帮助您了解Windows操作系统下MySQL 5.5.62的安装及配置方法
	MySQL 5.6.49安装配置指导书(Linux)	帮助您了解Linux操作系统下MySQL 5.6.49的安装及配置方法
	MySQL 5.6.49安装配置指导书(Windows)	帮助您了解Windows操作系统下MySQL 5.6.49的安装及配置方法
	MySQL 5.7.27安装部署指导(Linux)	帮助您了解Linux操作系统下MySQL 5.7.27的安装及配置方法
	MySQL 5.7.27安装部署指导(Windows)	帮助您了解Windows操作系统下MySQL 5.7.27的安装及配置方法
	MySQL 8.0.17安装部署指导(Linux)	帮助您了解Linux操作系统下MySQL 8.0.17的安装及配置方法
	MySQL 8.0.17安装部署指导(Windows)	帮助您了解Windows操作系统下MySQL 8.0.17的安装及配置方法

部署指导	H3C智能管理中心部署指导(集中式部署+内嵌数据库)	指导您使用内嵌数据库对iMC进行集中式部署
	H3C智能管理中心部署指导(集中式部署+本地数据库)	指导您使用本地数据库对iMC进行集中式部署
	H3C智能管理中心部署指导(集中式部署+远程数据库)	指导您使用远程数据库对iMC进行集中式部署
	H3C智能管理中心部署指导(分布式部署+本地数据库)	指导您使用本地数据库对iMC进行分布式部署
	H3C智能管理中心部署指导(分布式部署+远程数据库)	指导您使用远程数据库对iMC进行分布式部署
	H3C智能管理中心部署指导(凝思磐石+达梦数据库)	指导您使用凝思磐石+达梦数据库对iMC进行部署
	H3C智能管理中心部署指导(中标麒麟+达梦数据库)	指导您使用中标麒麟+达梦数据库对iMC进行部署
	H3C智能管理中心部署指导(CentOS 7.3+MariaDB数据库)	指导您使用CentOS 7.3+MariaDB数据库对iMC进行部署
	H3C智能管理中心部署指导(CentOS 8.3+MariaDB数据库)	指导您使用CentOS 8.3+MariaDB数据库对iMC进行部署
	H3C智能管理中心部署指导(红旗操作系统+MariaDB数据库)	指导您使用红旗操作系统+MariaDB数据库对iMC进行部署
	H3C智能管理中心部署指导(凝思磐石+MariaDB数据库)	指导您使用凝思磐石+MariaDB数据库对iMC进行部署
	H3C智能管理中心部署指导(Suse 12.2+MariaDB数据库)	指导您使用Suse 12.2+MariaDB数据库对iMC进行部署
用户手册	H3C智能管理中心用户手册	快速引导用户了解并使用iMC以及帮助用户解决使用过程中遇到的问题

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 概述 ····· 1-1
1.1 iMC 的组成 ····· 1-1
1.2 iMC 的安装和部署 ····· 1-1
2 体验 iMC ····· 2-1
2.1 访问 iMC ····· 2-1
2.2 熟悉 iMC 的管理界面 ····· 2-2
2.2.1 iMC 首页介绍 ····· 2-2
2.2.2 iMC 功能页界面 ····· 2-3
2.2.3 页签下拉菜单 ····· 2-4
2.3 首次登录后要做什么？ ····· 2-5
2.4 如何更便捷的使用 iMC？ ····· 2-7
2.4.1 iMC 帮助系统 ····· 2-7
2.4.2 收藏夹功能 ····· 2-9
2.4.3 业务操作流导航 ····· 2-10
2.5 iMC REST API ····· 2-10
2.6 内容丰富的视频案例 ····· 2-12
2.6.1 查看方法 ····· 2-12
2.6.2 案例内容介绍 ····· 2-13
3 iMC 中的资源管理 ····· 3-1
3.1 iMC 资源管理概述 ····· 3-1
3.2 使用拓扑管理网络 ····· 3-2
3.3 设备性能监控数据以及告警查询 ····· 3-4
4 iMC 中的用户管理 ····· 4-1
4.1 iMC 用户管理概述 ····· 4-1
4.2 用户管理 ····· 4-2
4.3 接入用户管理 ····· 4-2
4.4 访客管理 ····· 4-3
4.5 设备用户管理 ····· 4-4
5 iMC 对各种网络业务的管理 ····· 5-1
5.1 VLAN 管理 ····· 5-1
5.2 ACL 管理 ····· 5-1
5.3 智能配置中心 ····· 5-2

5.4 来宾接入管理 5-2
5.5 终端智能接入组件 5-3
5.6 EAD 安全策略组件 5-3
5.7 MPLS VPN 管理组件 5-4
5.8 IPsec VPN 管理组件 5-4
5.9 EPON 管理组件 5-4
5.10 网络流量分析组件 5-5
5.11 用户行为审计组件 5-5
5.12 应用管理组件 5-5
5.13 QoS 管理组件 5-5
5.14 服务健康管理组件 5-6
5.15 分支网点管理组件 5-6
5.16 VAN Fabric 管理组件 5-6
5.17 移动办公管理 5-6
5.18 业务服务管理 5-7
5.19 ITSM 服务管理组件 5-7
5.20 安全业务管理组件 5-7
5.21 无线业务管理组件 5-8
6 常见问题解答 6-1
6.1 iMC 运行时需要注意什么？ 6-1
6.2 使用浏览器访问 iMC 需要注意什么？ 6-1
6.3 在使用 iMC 过程中，界面操作出现不响应，被弹出到重新登录页面以及其他脚本错误，如何处理？ 6-2
6.4 登录操作系统时需要注意什么？ 6-2
6.5 iMC 安装完成后，如何修改 iMC 服务器的 Web 服务端口号？ 6-2
6.6 对设备进行 Telnet 操作时，弹出对话框会自动关闭，如何处理？ 6-3
6.7 如何修改超级操作员 admin 的登录密码？ 6-3
6.8 增加性能视图时，为什么没有性能管理权限的用户组还会出现在“可访问操作员分组”中呢？ 6-4
6.9 如何开启 iMC 登录验证码功能？ 6-4
6.10 如何限制管理员只能使用 HTTPS 协议访问 iMC？ 6-5
6.11 如何配置通过 HTTP 协议访问 iMC，自动跳转为 HTTPS 协议访问？ 6-5
6.12 如何为 iMC 安装证书？ 6-6
6.13 使用 Windows 操作系统时，无法在设备详细信息页面 Telnet 到设备，怎么办？ 6-8
6.14 为什么有些设备的 Web 网管界面无法打开？ 6-8
6.15 如何通过命令行停止和启动 iMC 单个进程？ 6-9

6.16 网络中的一台设备被替换后，如果新设备的 IP 地址与原设备的 IP 地址不同，网络拓扑中的拓扑计算不正确，怎么办？ ····· 6-9
6.17 为什么在数据转储功能的“转储后执行命令”中配置了某些命令，在执行时会导致 CPU 占用率长时间过高？ ····· 6-9
6.18 为什么在增加一个仅大小写不同的同名视图时，提示该视图已存在？ ····· 6-9
6.19 iMC 在使用 SQL Server 数据库运行一段时间之后，出现内存占用过高且不能恢复的现象，怎么办？ ····· 6-9
6.20 浏览 iMC 资源时，发现设备视图中没有任何设备，为什么？ ····· 6-10
6.21 在 iMC 运行过程中，能否修改操作系统时间，为什么？ ····· 6-10
6.22 在 iMC 中导入长文件名的文件时，系统没有响应怎么办? ····· 6-10
6.23 在 iMC 中输入了较长的内容后，有时会造成界面不美观，怎么办？ ····· 6-10
6.24 在表格中直接导航到最后一页，有时会出现表格下方的页数多于上方显示页数的情况，为什么？ ····· 6-11
6.25 管理员登录 iMC 时，页面提示“系统资源不足，无法完成该操作”，怎么办？ ····· 6-11
6.26 当 iMC 运行过程中出现问题，并需要技术支持解决时，如何收集 iMC 的日志？ ····· 6-12
6.27 当 iMC 服务器有多块网卡时，如何配置 iMC 使用其中一个 IP 地址监听 HTTP/HTTPS 服务？ ·· 6-13
6.28 当 iMC 采用分布式部署时，所有主从服务器重启，数据库在从服务器上的组件无法被加载，如何解决？ ····· 6-13
6.29 如何将网络中的虚拟设备加入 iMC？ ····· 6-13
6.30 在安装 iMC 时，数据库检查无法通过，提示如下，如何解决？ ····· 6-14
6.31 在 iMC 中卸载了 SOM 后，以前通过告警、iCCM、ACLM、VLANM 等模块功能创建并提交的 SOM 流程都无法执行下去了，怎么办？ ····· 6-14
6.32 iMC 在使用 Oracle 或 MySQL 数据库时，部分组件提示数据库操作异常，怎么办？ ····· 6-14
6.33 当忘记 admin 帐号的密码时，如何解决？ ····· 6-17
6.34 使用 HTTPS 访问 iMC 时，如何屏蔽 SSLv3 协议，而只启用 TLS 协议？ ····· 6-17
6.35 怎样通过域名方式访问 iMC？ ····· 6-17

1 概述

智能管理中心（简称 iMC）是 H3C 推出的一款基于 B/S 架构的综合网络管理产品。iMC 以网络管理为核心，重点关注网络中的各种资源、用户以及网络业务，目的是为网络管理员提供资源、用户和网络业务相融合的网络管理解决方案，实现对网络的端到端管理。

1.1 iMC的组成

iMC 由智能管理平台组件和业务组件组成，其中智能管理平台为必配组件，是其他业务组件的基础。网络管理员可以根据实际需要灵活选配其他业务组件以满足不同需求。iMC 产品包括以下组件：

- 智能管理平台组件
- 终端智能接入组件
- EAD 安全策略组件
- MPLS VPN 管理组件
- IPsec VPN 管理组件
- EPON 管理组件
- 网络流量分析组件
- 用户行为审计组件
- 应用管理组件
- QoS 管理组件
- 服务健康管理组件
- 分支网点管理组件
- VAN Fabric 管理组件
- 移动办公管理
- 业务服务管理
- ITSM 服务管理组件
- 安全业务管理组件
- 无线业务管理组件

1.2 iMC的安装和部署

(1) 用户在安装 iMC 前需要先准备以下资源：
   - 软件安装盘（产品包装盒内）
   - 软件授权书（产品包装盒内）

(2) 选择所采用的部署方案，iMC 支持以下几种部署方案：
   - 集中式部署+内嵌数据库
   - 集中式部署+本地数据库
   - 集中式部署+远程数据库

- 分布式部署+本地数据库
- 分布式部署+远程数据库

不同部署方案适用于不同规模的企业或组织，用户可以参考每种部署方式对应的部署指导来进行选择，文档中除了描述该方案适用的场景外，还包括了 iMC 所需服务器的硬件要求、安装步骤和注册过程等内容，这些文档可以在 H3C 网站上找到。iMC 部署指导 URL：

https://www.h3c.com/cn/Service/Document_Software/Document_Center/SDN/Catalog/IMC/IMC_V7/Installation/Installation_Manual/H3C_7.3-21299/01/?CHID=1105350

(3) 根据所选择的 iMC 部署方案准备用于安装 iMC 的服务器。

(4) 根据所选择的 iMC 部署方案安装和部署 iMC。

(5) 注册 iMC 产品。

注册 iMC 所需的 License Key 信息可以在软件授权书上找到。

2 体验 iMC

iMC 由智能管理平台组件和业务组件组成，安装了不同组件的 iMC 在访问时界面略有不同，这里仅以安装和部署了智能管理平台组件的 iMC 为例进行介绍。

2.1 访问iMC

iMC 采用 B/S 结构开发，用户访问时无需安装任何客户端，直接在 Web 浏览器的地址栏中输入 iMC 服务器的 URL 即可。

iMC 对 Web 浏览器的支持情况如表 2-1 所示。使用低版本浏览器访问 iMC，可能会出现登录异常等情况，具体情况请参考 6 常见问题解答进行处理。

表2-1 推荐的 Web 浏览器

浏览器	版本
Firefox	Firefox 50及以上版本
Chrome	Chrome 44及以上版本

浏览器配置要求如下：

- 关闭浏览器的弹出窗口阻塞设置
- 必须使能浏览器的 Cookies
- iMC 站点加入受信任站点
- 分辨率显示宽度至少为 1280

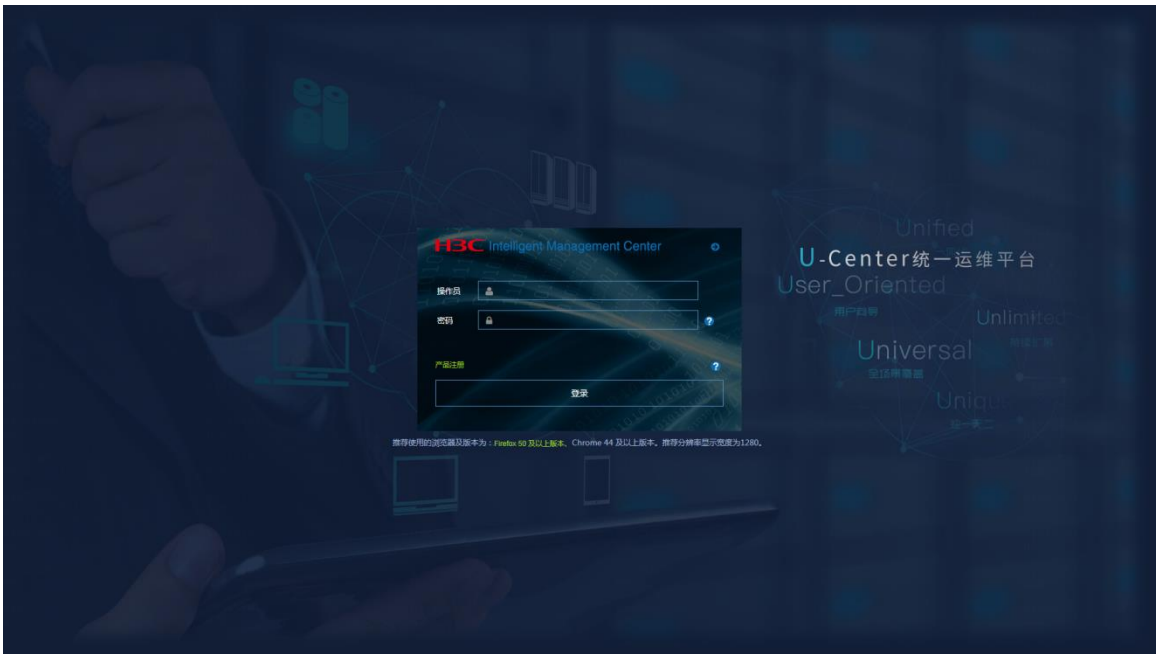
iMC 服务器的 URL 为：

- http://<*IP 地址*>:<*端口*>/imc iMC 的默认 HTTP 端口为 8080
- https://<*IP 地址*>:<*端口*>/imc iMC 的默认 HTTPS 端口为 8443

说明

HTTPS 即安全超文本传输协议，采用这种方式登录 iMC，可以更好的保证信息在交互过程中的安全性。通过 HTTPS 方式访问 iMC 时，可能会提示证书错误，请参考 6 常见问题解答进行处理。

图2-1 登录页面



在登录页面中，输入正确的操作员和密码，选择登录方式后单击<登录>按钮，即可进入系统首页。登录方式有两种：

- 经典版：继承传统 iMC 界面的风格特点，增加个性皮肤，优化视图效果，通过图形及文字的合理布局，清晰完整的展示网络运行情况，更好的帮助用户管理网络资源。
- 桌面版：以全新的 Web 桌面形式，为业务管理和解决方案管理提供更精细、更个性化的界面组织和用户体验。具有支持多业务窗口应用，可引用外界资源（如 H3C 网站）等多种功能。

说明

- 首次登录系统时，可使用默认的操作员登录。iMC 缺省的超级管理员用户名是 admin，iMC PLAT 7.3 (E0706)版本前默认密码是 admin，iMC PLAT 7.3 (E0706)及后续版本默认密码是 Pwd@12345。进入系统后请及时修改该密码。修改方法请参见 6 常见问题解答。
- 在 iMC 中可以根据需要增加不同权限的操作员。具体配置方法请参见产品附带的联机帮助。
- iMC 支持登录时输入验证码功能。管理员可通过修改配置文件开启该功能。关于如何开启验证码功能，请参见 6 常见问题解答。

2.2 熟悉iMC的管理界面

2.2.1 iMC 首页介绍

iMC 的首页界面不同于其他功能页面，用户可以在首页上定制展示元素，设定页面布局，自定义多个首页页面。用户可根据需要灵活设置，将自己关注的元素集中展示。

图2-2 iMC 首页界面

以自上而下从左到右的顺序，iMC 首页界面分为如下 5 个部分。

表2-2 首页界面

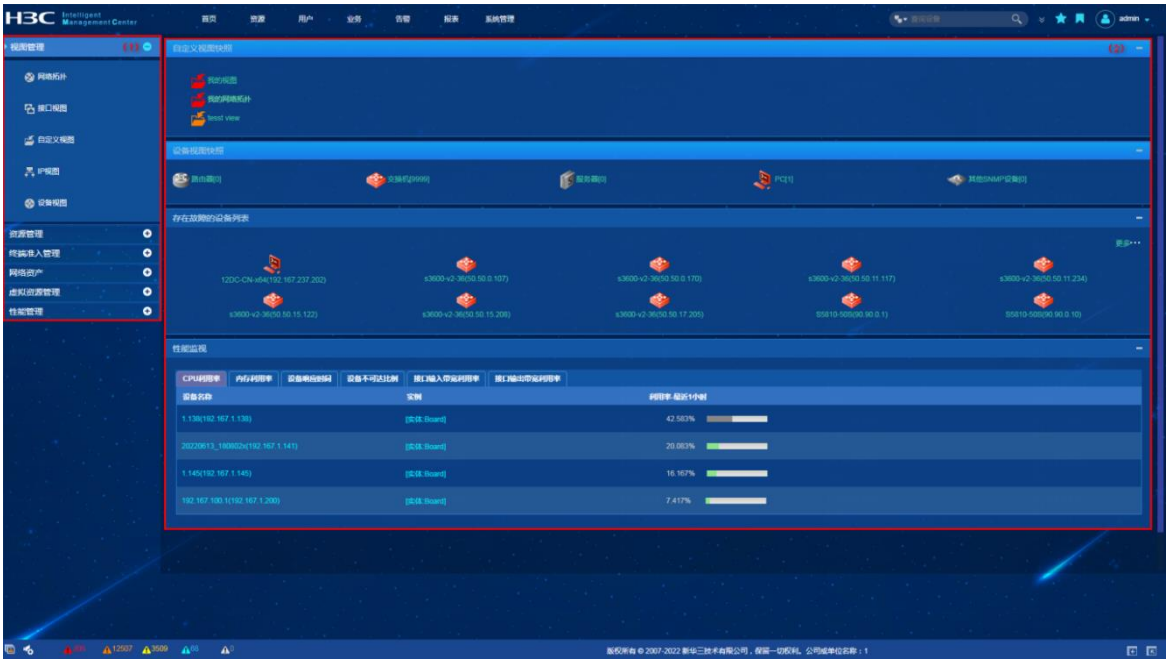
序号	名称	说明
(1)	导航条	以不同的角度提供了各类管理功能的配置入口，方便管理员根据实际需要进行切换。
(2)	搜索栏	实现了对用户、设备、接口的搜索，同时支持多条件查询的高级搜索功能。
(3)	管理链接	显示了当前登录的操作员信息以及相关的功能链接。将鼠标移动到操作员名称上可以看到当前操作员的登录时间和登录IP地址。
(4)	缺省首页	操作员登录iMC后的缺省首页（Welcome）。iMC允许操作员定制多个首页，并将其中一个指定为缺省首页。同时，iMC还提供了多种展示元素，操作员可以根据实际需要在首页上定制不同的展示元素。
(5)	告警统计控件	用于对iMC中的告警信息进行统计，并且可以根据告警的等级进行语音提示。

管理链接、导航条、搜索栏、告警统计控件会显示在所有 iMC 页面上。

2.2.2 iMC 功能页界面

iMC 功能页界面如图 2-3 所示，除首页外，其他功能页的界面相同，这里仅以资源功能页为例，管理链接、功能页签和搜索栏与首页界面相同，这里不再介绍。

图2-3 功能页界面



功能页界面不同于首页的地方，以从左到右的顺序，分为如下两个部分。

表2-3 功能页界面

序号	名称	说明
(1)	导航树	列出了当前功能页签对应的操作链接。
(2)	操作区	该区域主要用于信息展示以及相关功能的操作。

从图 2-3 中我们可以看到如下信息：

- 自定义视图、设备视图的图标颜色与视图中严重级别最高的设备图标颜色一致。
- 设备视图快照下按照类别列出了网络中各类设备的数量以及设备当前的最高告警级别。
- 存在故障的设备列表列出了处于不同告警级别的设备，并根据严重程度进行排列，仅在存在故障设备时才显示。
- 性能监控区域列出了多种用户关心的性能指标。

界面中的视图、设备类型图标均为链接，点击后在操作区中将显示其中包含的设备信息列表。

2.2.3 页签下拉菜单

iMC 的功能页签提供了方便的下拉菜单，如图 2-4 所示。

图2-4 页签下拉菜单

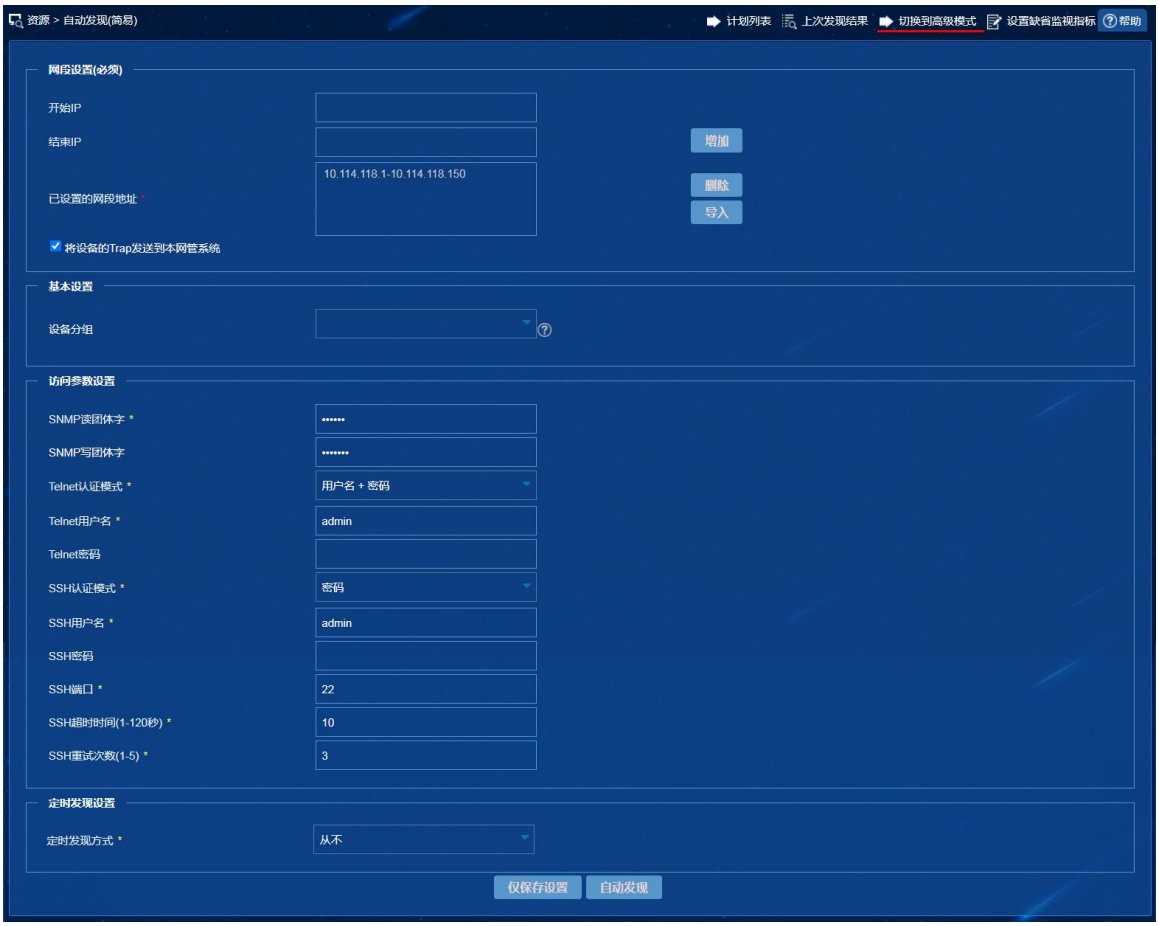
页签下拉菜单使管理员可以迅速定位到自己需要的功能，这里以业务页签为例。将鼠标指针移动至业务功能页签，页签下拉菜单会自动弹出，选择自己需要的菜单功能，单击菜单链接，即可导航至对应的功能页面。

2.3 首次登录后要做什么？

作为网络业务的承载者，网络设备是整个网络的“骨骼”，因此网络管理首先从向系统添加被管理设备开始。

操作员登录 iMC 后，在页签下拉菜单中选择“资源 > 自动发现”菜单项，进入自动发现简易模式页面，如图 2-5 所示。

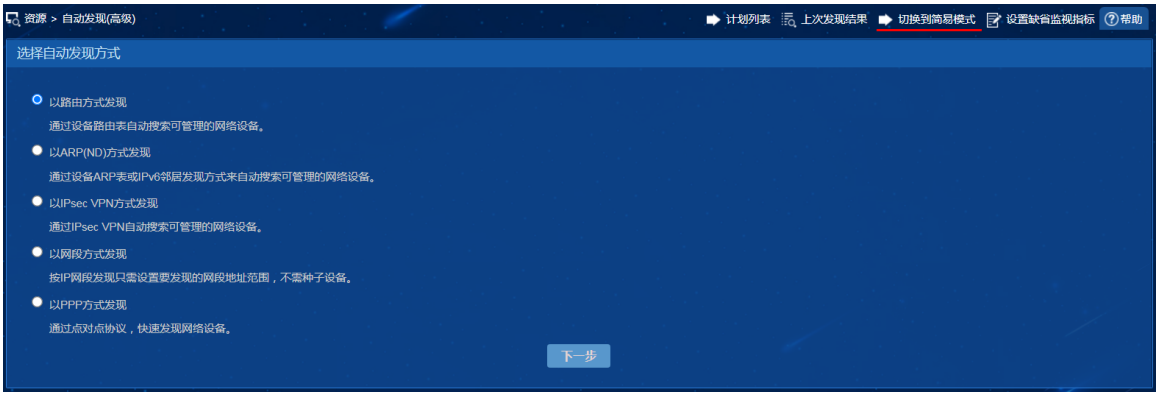
图2-5 自动发现简易模式页面



只需要输入网段起始 IP 和结束 IP（可以输入一组或多组），即可查找到该网段内的设备。

同时 iMC 还为用户提供了多种自动发现方式，点击“切换到高级模式”链接，进入自动发现高级模式页面，如图 2-6 所示。

图2-6 自动发现高级模式页面



不同的自动发现方式有其特点和适用场合，请参照表 2-4 进行选择。

表2-4 自动发现模式

模式	适用场合
以路由方式发现	如果您仅知道某个网关或路由器的IP地址，推荐采用这种方式。
以ARP(ND)方式发现	如果您想快速完成设备发现操作，推荐采用这种方式。
以IPsec VPN方式发现	如果您只需要了解与IPsec VPN业务相关的设备，推荐采用这种方式。
以网段方式发现	如果您掌握了网络中的网段规划信息，推荐采用这种方式。
以PPP方式发现	如果您的网络中三层设备互联的接口IP地址使用/30的子网掩码，推荐采用这种方式。

操作员首次登录 iMC 时，iMC 会自动引导操作员使用自动发现来向 iMC 中增加设备。除自动发现外，iMC 也提供了手动增加设备的功能，两种增加设备的方法适用于不同的情况，请参见表 2-5 进行选择。

表2-5 设备添加方式

增加方式	适用场合	操作方法
自动发现	首次使用iMC时，快速的完成网络设备的批量增加。	在页签下拉菜单中选择“资源 > 自动发现”菜单项。
手动增加	当网络中新增设备时，可以通过手工增加的方式进行单独增加。	在页签下拉菜单中选择“资源 > 增加设备”菜单项。

2.4 如何更便捷的使用iMC？

2.4.1 iMC 帮助系统

iMC 内置了内容完善、功能强大的联机帮助系统，登录 iMC 后即可随时点击配置界面中的“帮助”链接查询帮助信息。

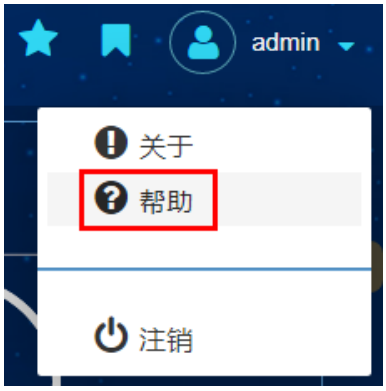
iMC 联机帮助支持以下功能：

- 全文检索：可以通过关键词的方式在全部联机帮助中检索需要的信息。
- 动态挂接：iMC 帮助内容与安装的组件一致，方便用户的查询。
- 动态页面定位：在某些配置界面中，可以通过点击其中的“帮助”链接直接访问相关功能的帮助信息。

iMC 联机帮助的操作方式：

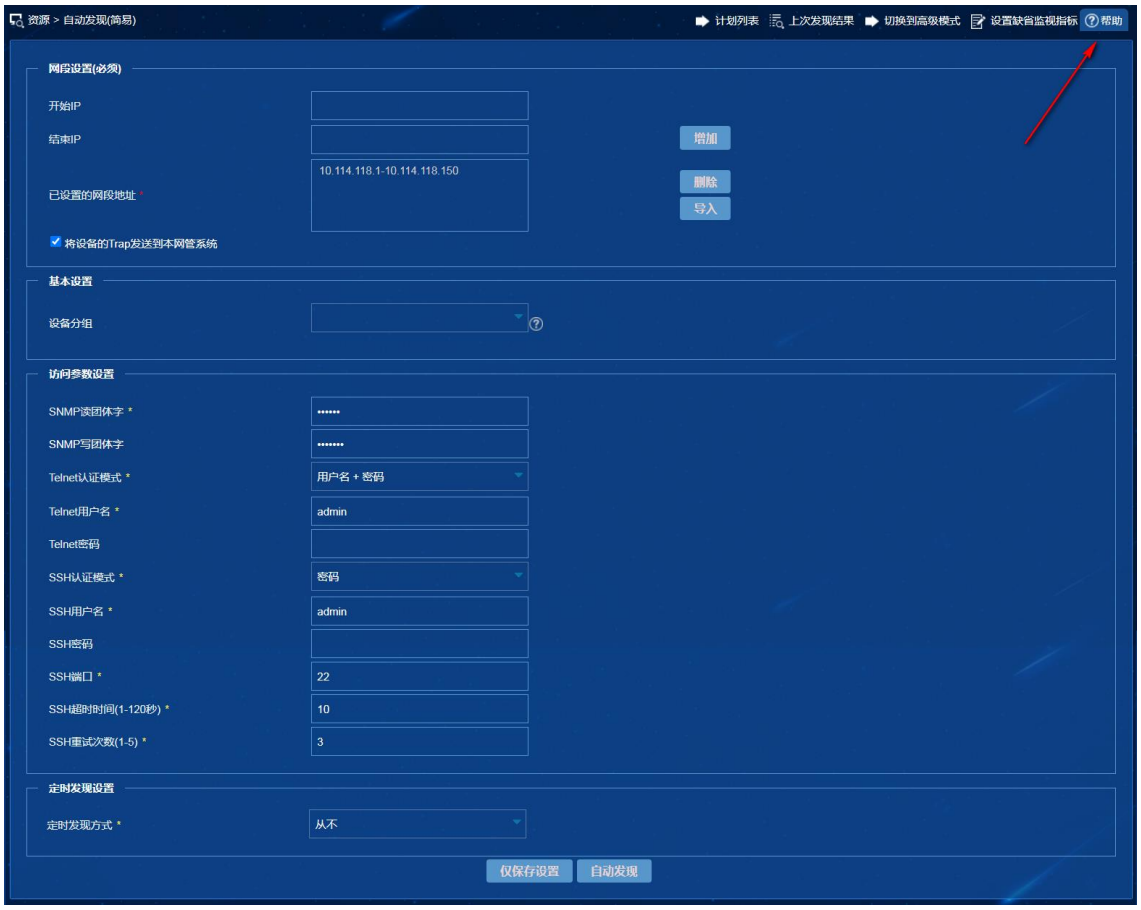
- 打开全部帮助：点击配置界面右上角的用户图标，在弹出的下拉菜单中选择“帮助”菜单项，如图 2-7 所示。

图2-7 全部帮助访问链接



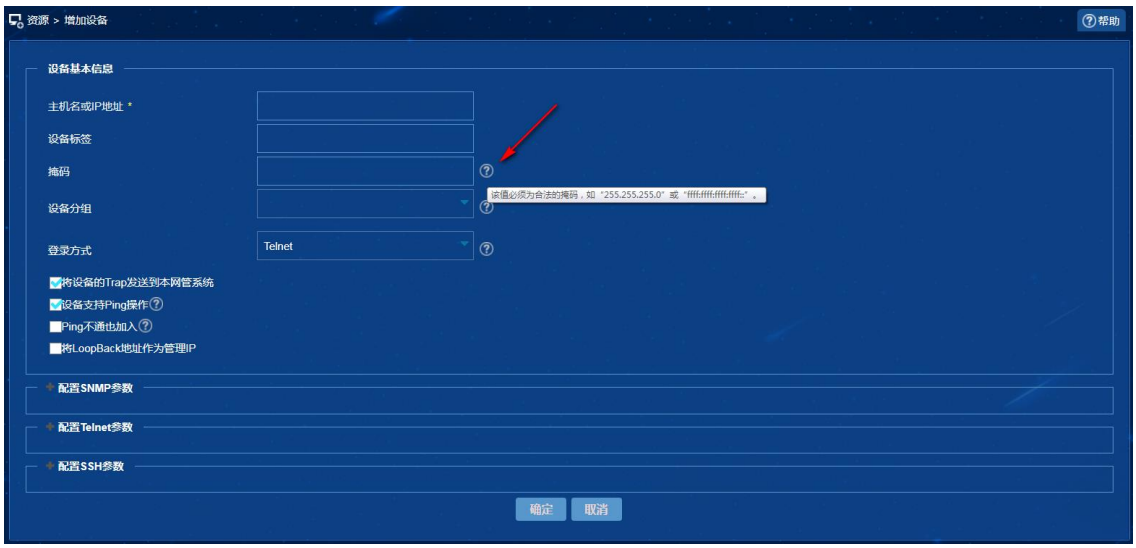
- 打开特定配置页面的帮助：点击特定操作页面右上角的“帮助”链接，如图 2-8 所示（以自动发现为例）。

图2-8 配置页面帮助链接



- 查看参数输入限制：在 iMC 任意有输入参数的配置界面中，只要将鼠标放在?之上，系统会自动弹出关于该参数输入限制的简要说明，如图 2-9 所示（以增加设备为例）。

图2-9 参数输入限制提示信息



2.4.2 收藏夹功能

操作员可以将自己经常访问的 iMC 页面加入收藏夹，然后通过收藏夹快速访问自己需要访问的页面。

1. 将页面加入收藏夹

将页面加入收藏夹的操作如图 2-10 所示，点击关注页面右上角的“加入收藏”链接，确认后将页面加入收藏夹。

图2-10 加入收藏夹

2. 访问收藏夹

如图 2-11 所示，点击界面右上方的图标，在弹出菜单中选择“我的收藏”菜单项，查看所有收藏的页面链接。

图2-11 访问收藏夹

说明

上图显示内容与所选择安装的组件有关，本手册中涉及的所有菜单、导航内容可能与实际页面略有区别，请以实际安装环境为准。

2.4.3 业务操作流导航

一些业务组件提供配置向导图，用户可以参照导航完成全套业务的部署，方便用户使用，如图 2-12 所示。

图2-12 ACL 业务配置向导图

2.5 iMC REST API

iMC 提供完善的 REST API 开发接口，使用浏览器可以直接访问这些 API。访问地址如下：

- http://<*IP 地址*>:<*端口*>/imcrs，iMC 的默认 HTTP 端口为 8080
- https://<*IP 地址*>:<*端口*>/imcrs，iMC 的默认 HTTPS 端口为 8443

系统弹出身份验证窗口，输入具有 REST API 管理权限的操作员帐号及密码。

图2-13 REST API 页面

如图 2-13 所示，在顶部下拉框中，通过选择组件及模块，进入对应的 REST API 页面。页面中列出了该组件或模块所有可用的 REST API 接口。展开后，可以在网页中直接测试这些接口功能。

图2-14 REST API 测试页面

2.6 内容丰富的视频案例

除提供在线帮助外，还可以到 H3C 网站上下载丰富的 iMC 视频案例。案例中演示了 iMC 的常用功能、典型应用及其配置方法。

2.6.1 查看方法

在浏览器地址栏中输入以下 URL：

http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Management/H3C_intelligentize/H3C_intelligentize/

或参照以下步骤查找视频资料：

(1) 登录 www.h3c.com，选择“支持 > 文档与软件 > 文档中心”。

(2) 点击“管理软件”。

(3) 点击“H3C 智能管理中心”，进入 iMC 产品资料库。

(4) 在“视频专区”中提供了“视频安装案例”和“视频配置案例”，如图 2-15 所示，点击视频案例链接进入相应页面即可在线观看。

图2-15 H3C 智能管理中心资料库

H3C智能管理中心

视频专区 安装 配置 维护 工具

视频安装案例

- iMC PLAT 7.3有声安装指导视频-5W102
- U-Center 7.3有声安装指导视频-5W101
- H3C 智能管理中心 安装视频

视频配置案例

- iMC EMO 7.3有声视频配置案例-5PW102
- iMC ITSM 7.3有声视频配置案例-5PW101
- iMC APM 7.3有声视频配置案例-5PW101
- SecCenter A2000有声视频配置案例-5PW101
- U-Center 7.3有声视频配置案例-5PW100
- iMC PLAT 7.3有声视频配置案例-5W104
- iMC WSM 7.3有声视频配置案例-5W102
- iMC EAD 7.3有声视频配置案例-5W103
- iMC EIA 7.3有声视频配置案例-5W105
- iMC IPM 7.3有声视频配置案例-5PW101
- iMC BSM 7.3有声视频配置案例-5PW100
- iMC iAR V2快速入门 演示视频-5PW100
- iMC PLAT 5.1 SP1视频配置案例(告警管理)-5PW100
- iMC PLAT 5.1 SP1 视频配置案例(性能管理)-5W100
- iMC PLAT 5.1 SP1 视频配置案例(设备管理)-5W100
- iMC L2VPN管理典型配置案例
- iMC IVM视频配置案例-5W100
- iMC使用SNMP自动发现设备-6W100
- iMC MIB管理快速入门
- iMC性能管理快速入门
- iMC EoC管理组件典型配置案例
- iMC平台快速入门视频配置案例-6W100
- iMC平台快速入门视频配置案例电子书-6W100
- iMC WSM视频配置案例-6W100
- iMC NTA视频配置案例
- iMC MPLS VPN管理视频配置案例
- iMC UAM EAD中文视频配置案例
- iMC iCC视频配置案例
- iMC平台视频配置案例

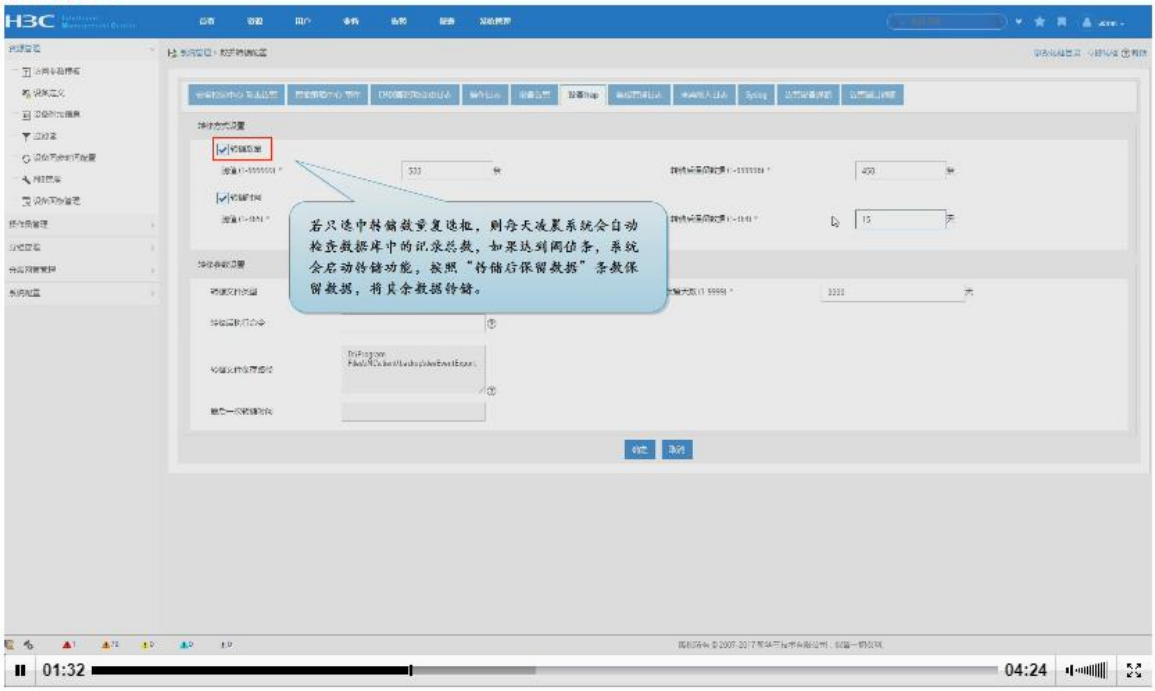
2.6.2 案例内容介绍

1. 常用功能的演示

视频案例选取了日常维护中常用的功能，进行配置演示，每个步骤均配有说明文字，方便用户理解各配置项的目的。

图2-16 常用功能演示

在线观看

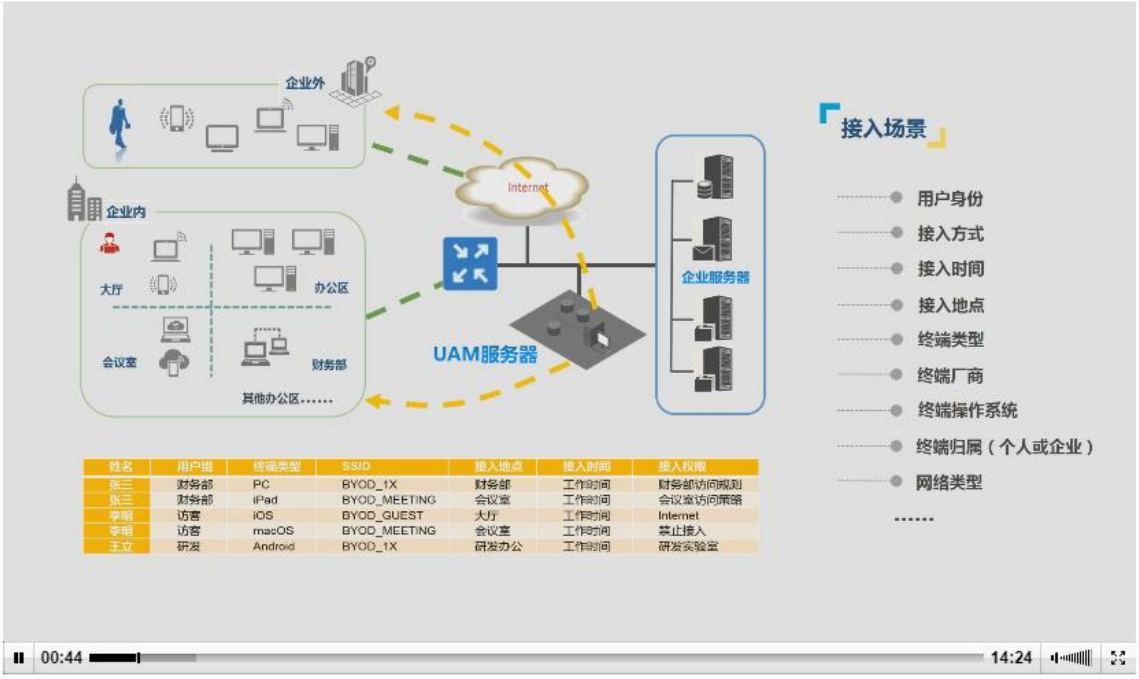


2. 典型应用配置方法演示

典型应用是针对某一应用场景，完成的较综合的配置案例。观看后可以对产品及某一方面的应用有个完整地了解。

图2-17 典型应用视频演示

在线观看



3 iMC 中的资源管理

iMC 中的资源是指网络资源，包括设备、接口、链路、虚拟网络等，网络资源的正常运行是用户和业务正常使用的前提。本章主要介绍 iMC 对网络资源的管理。

3.1 iMC资源管理概述

在导航条中点击“资源”页签，页面的左导航树如图 3-1 所示。

图3-1 资源导航树

由上图可以看出，导航树中的功能节点分为如下七类：

- 视图管理：提供了拓扑和视图的入口，操作员可以根据拓扑或视图等功能快速定位需要操作的资源。
- 资源管理：主要用来增加设备，同时还提供了批量配置设备相关参数的功能。
- 终端准入管理：用来对接入网络的终端进行统一的管理和监控。
- 网络资产：用来对网络中的各类资产，如交换机、板卡、电源模块等进行管理。
- 性能管理：提供了设备性能的全局浏览、设置等功能入口。

3.2 使用拓扑管理网络

1. 查看网络拓扑

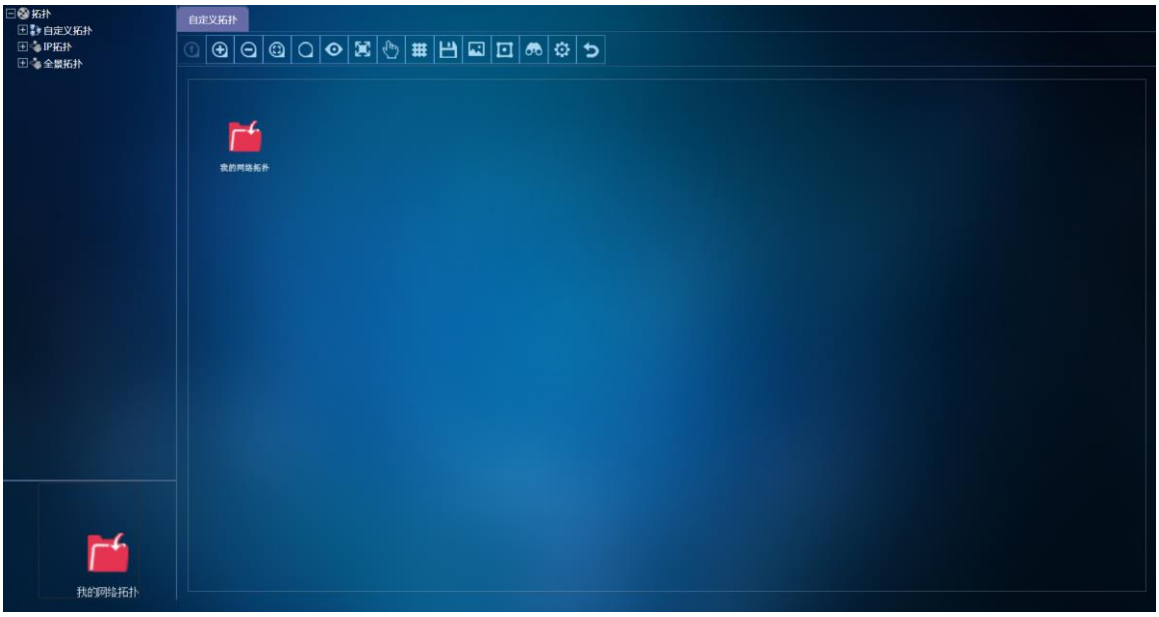
单击[网络拓扑]菜单项，如图 3-2 所示，系统将在新窗口中打开网络拓扑图。

图3-2 查看网络拓扑

2. 查看自定义拓扑

如图 3-3 所示，网络拓扑窗口默认打开自定义拓扑，用户可以双击 图标，网络拓扑窗口将在新选项卡中打开自定义视图。

图3-3 查看自定义拓扑



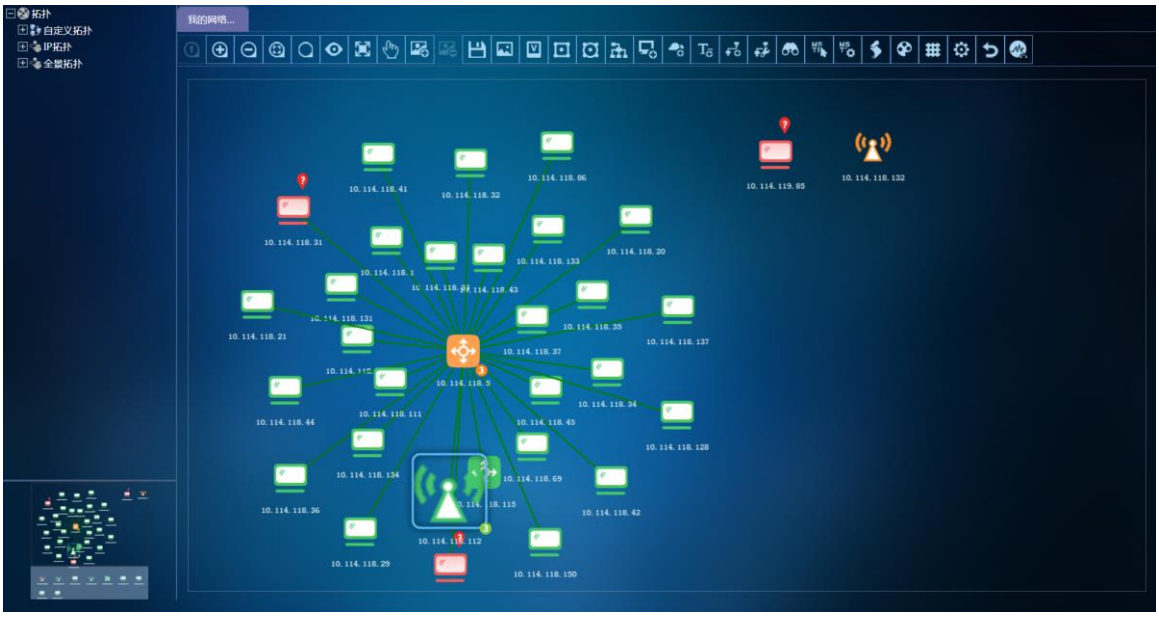
3. 在拓扑图中进行设备定位

单击导航树中的[设备视图]菜单项，打开设备视图，如图 3-4 所示。

图3-4 路由器设备视图

点击图中的“操作”链接，在弹出菜单中选择[查看拓扑]菜单项，在选择拓扑显示的视图后，系统自动定位到该设备所在的位置。如图 3-5 所示。

图3-5 设备拓扑定位



3.3 设备性能监控数据以及告警查询

点击图 3-4 中的任意一个设备标签链接，即可打开设备详细信息页面，如图 3-6 所示。

图3-6 设备详细信息

2. 设备告警信息

iMC 通过列表、图形两种形式将设备运行过程中的关键告警展示给操作员。点击上图中的柱状图，页面将自动跳转到“告警”功能，并显示该设备的相关等级的全部告警，方便操作员及时定位设备故障。

3. 性能监控信息

设备的性能监视数据，位于设备详细信息页面的最下方。操作员可以通过点击右上角的“性能数据概览”链接查看该设备的所有性能监控数据。

4. 操作菜单

设备详细信息页面右侧的操作菜单是 iMC 针对单个设备提供的配置和管理功能。操作员可以通过操作菜单完成针对该设备的各种操作，如 VLAN 管理和设备配置管理等。

4 iMC 中的用户管理

iMC 提供了多种针对用户的管理功能，这些用户可以是终端用户、访客等。智能管理平台提供了用户管理和来宾接入管理功能，为了更好的介绍 iMC 的用户管理功能，本章将结合终端智能接入（EIA）和 EAD 安全策略管理（EAD）组件来介绍 iMC 对用户的管理。

4.1 iMC用户管理概述

在导航条中点击“用户”页签，页面的左导航树如图 4-1 所示。注意，iMC 仅在部署了涉及用户管理功能的业务组件（如 EIA/EAD）时才会显示相应的功能节点。

图4-1 用户导航树

由上图可以看出，导航树中的功能节点分为如下五类：

- 用于对用户身份信息进行管理的用户管理。
- 用于对用户接入进行控制的接入用户管理、接入策略管理、用户接入日志和终端管理。
- 用于对接入用户终端安全进行管理的安全策略管理和桌面资产管理。
- 用于对来宾和访客进行管理的来宾接入管理和访客管理。
- 用于对登录设备进行管理的设备用户管理和设备用户策略管理。

说明

- 用户管理和来宾接入管理是智能管理平台提供的功能。
- 接入用户管理、接入策略管理、用户接入日志、终端管理、访客管理、设备用户管理和设备用户策略管理是终端智能接入（EIA）提供的功能。
- 安全策略管理和桌面资产管理是 EAD 安全策略管理（EAD）提供的功能。
- 如果系统安装了智能管理中心的其他业务组件，导航树中还会出现相应的功能节点。
- iMC 系统中主要有操作员和用户两类角色：操作员是指能够直接登录 iMC 系统进行相关配置和操作的网络管理人员（比如系统默认操作员 admin），常常是企业 IT 部门人员；用户指网络使用者，是 iMC 的管理对象。

4.2 用户管理

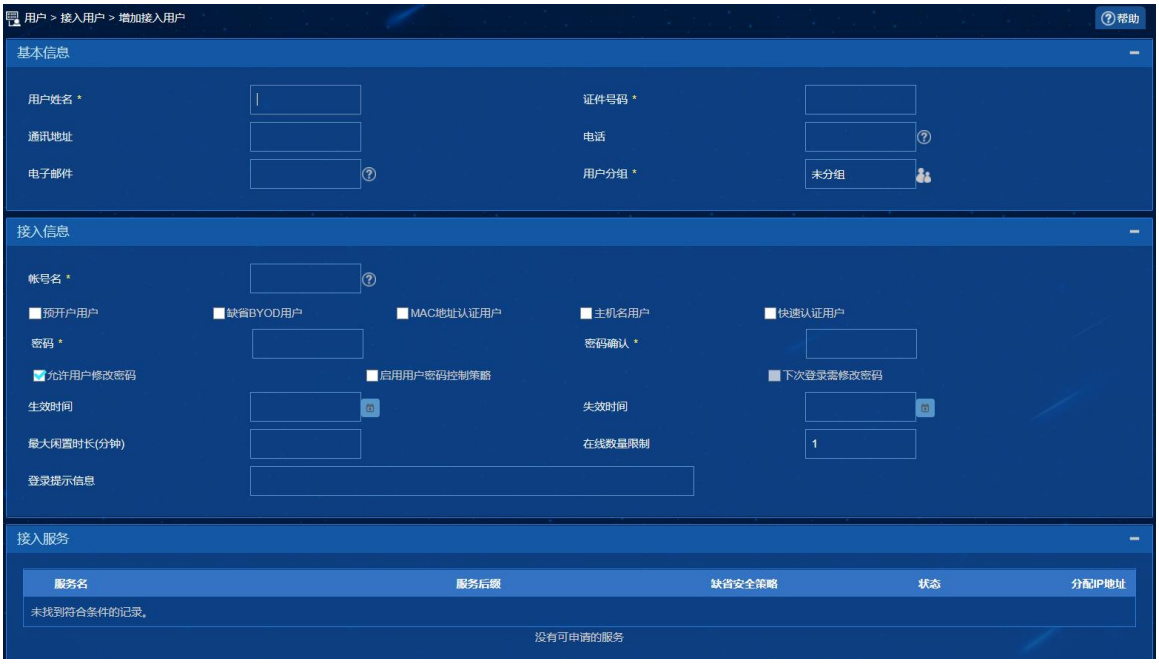
用户管理提供了对用户基本信息进行管理的功能，增加用户的界面如图 4-2 所示，必选项包括用户姓名、证件号码和用户分组，其它均为可选项。为了方便区分，这里将用户称为平台用户。

图4-2 增加用户

4.3 接入用户管理

接入用户管理提供了对用户接入进行控制的功能，一个平台用户可以有多个接入用户，每个接入用户的帐号都可以用于 AAA（认证、授权、计费）服务。增加接入用户的界面如图 4-3 所示，每个接入用户都需要关联一个平台用户。

图4-3 增加接入用户



接入用户接入网络时除了要有帐号外，还需要申请服务。服务中指定了接入用户的接入策略等信息，接入用户只有满足这些接入策略才接入网络。

如果要对接入用户的安全性进行控制，操作员还可以在服务中指定安全策略，申请了该服务的用户在接入网络时还需要满足安全性要求，从而提高整个网络的安全性。

4.4 访客管理

访客是指临时访问公司或组织网络的外部人员，这类用户访问网络的权限要受到限制，且不会长期访问公司或组织的网络。

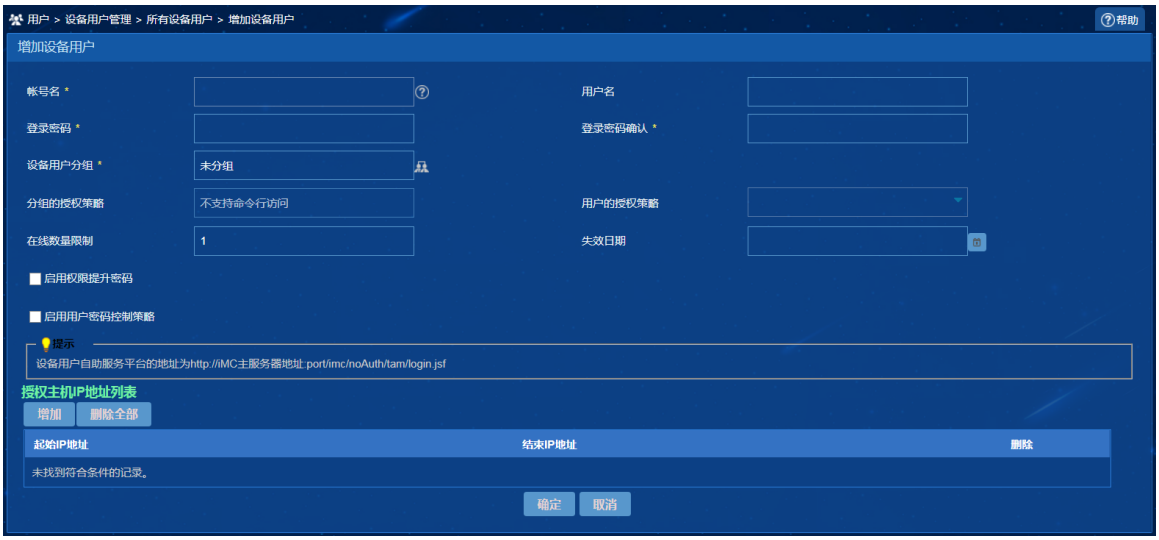
iMC 定义了访客和访客管理员两种角色来解决访客接入网络的问题。访客通过自助服务平台输入访客的身份信息和审核请求的访客管理员，如图 4-4 所示。访客管理员通过自助服务平台中对访客的访问请求进行审核。

图4-4 访客预注册

4.5 设备用户管理

设备用户管理以设备用户为主体，提供了维护设备用户信息的基本功能以及审计设备用户行为的日志监控功能。主要包括设备用户分组管理、设备用户管理、在线用户监控、黑名单用户管理、LDAP同步用户管理以及日志管理。管理员创建并维护帐号，设备用户使用该帐号登录并管理设备，增加设备用户的界面如图 4-5。

图4-5 增加设备用户



5 iMC 对各种网络业务的管理

iMC 通过按需装配的组件化结构，为管理员提供了一个具有良好可扩展性的网络管理平台，可以根据客户实际需要提供多种多样的业务组件和网络管理解决方案。

目前 iMC 平台的内置业务模块包括 VLAN 管理、ACL 管理、智能配置中心、来宾接入管理。

此外还提供多种可选组件满足用户的不同业务需求，其中包括：

- 终端智能接入组件
- EAD 安全策略组件
- MPLS VPN 管理组件
- IPsec VPN 管理组件
- EPON 管理组件
- 网络流量分析组件
- 用户行为审计组件
- 应用管理组件
- QoS 管理组件
- 服务健康管理组件
- 分支网点管理组件
- 移动办公管理
- 业务服务管理
- ITSM 服务管理组件
- 安全业务管理组件
- 无线业务管理组件

业务组件的使用方法请参考各组件对应的联机帮助。

5.1 VLAN管理

VLAN 技术在解决以太网交换机在 LAN 中无法限制广播问题上得到广泛的应用。随着网络规模的增大，对 VLAN 的配置和管理逐渐困扰起网络管理员。而 VLAN 管理（VLANM）提供了对设备的 VLAN 规划，VLAN 配置下发等功能。通过 VLAN 管理对网络的 VLAN 进行统一的规划，然后把这些配置统一下发到设备上，完成网络的 VLAN 管理。同时 VLAN 管理还提供 VLAN 拓扑功能，可以直观的查看到 VLAN 的部署情况。

VLAN 管理可以帮助操作员快速配置 VLAN，同时，针对 VLAN 资源进行统一管理的系统，实现了对设备 VLAN 信息的有效管理和灵活部署。

5.2 ACL管理

ACL 管理实现了对单设备 ACL 配置定义、应用 ACL 定义和包过滤等业务，并提供设备配置历史查看的功能；对于大量设备的批量 ACL 配置，通过友好的向导方式，利用灵活、便捷的批量部署模板，

简化管理员为多台设备配置 ACL 的步骤；提供了强大的部署处理机制和多角度的任务视图，方便管理员进行管理和任务部署，使其更加灵活。

作为网络基础资源管理的业务组件，系统安装 ACL 管理之后会将 ACL 相关资源选项融入到相关业务配置选项中，方便管理员的灵活配置。

5.3 智能配置中心

用户网络中的网络设备的种类和数量在不断增多，不同的设备类型，配置命令和软件版本会有不同；即使是同类型的设备，其配置也会因所处位置或所起作用而异，软件文件也会因网络升级的需要有不同的版本。这样配置文件和软件版本的数量就将是网络设备规模的数倍，给网络管理员管理、维护网络带来很大的难度。

智能配置中心，可以帮助管理员方便的对设备配置文件和软件文件进行集中管理；同时提供设备配置的基线化版本管理，可以对配置文件的变化进行比较跟踪；提供设备软件的升级历史记录，可以全面审计设备软件版本的变化，并可快速的恢复历史版本，极大的方便了对设备的管理，提高了网络的可维护性。

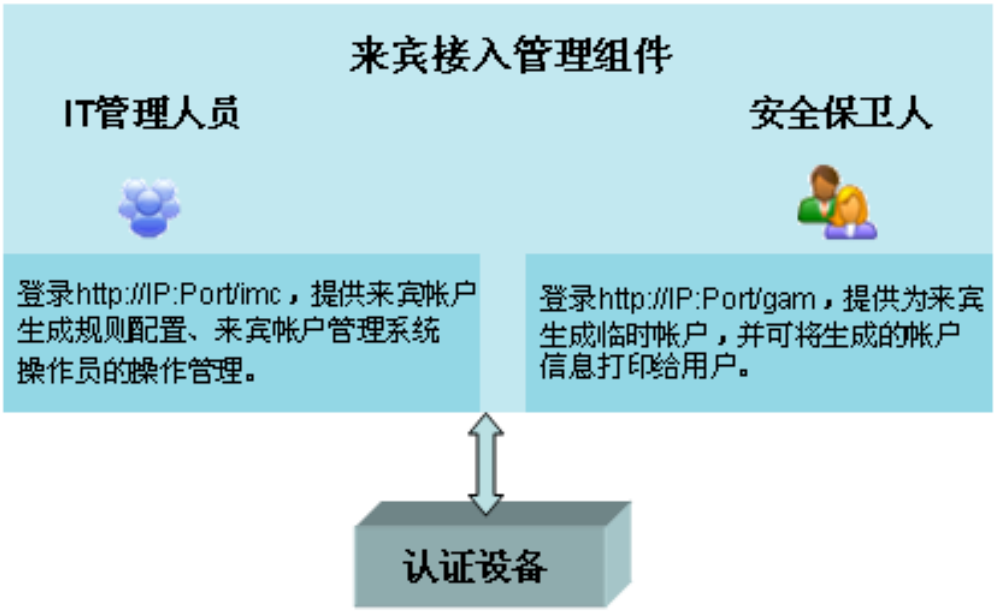
智能配置中心还从资源的角度提供配置模板库和软件文件库的管理，实现了这一类资源的重复使用和维护的方便性。

5.4 来宾接入管理

来宾接入管理提供了一种可以由非 IT 人员如安全保卫人员创建接入网络临时帐号的功能。在 IT 人员或 iMC 管理员预先配置后，非 IT 人员即成为一名来宾接入帐号管理员。

来宾接入帐号管理员不必知道如何配置和管理接入设备，就可以使用来宾接入自助系统简单而快速的创建一个来宾帐号，并将帐号信息下发到接入设备上。

图5-1 来宾接入管理结构示意图



5.5 终端智能接入组件

1. 用户接入管理

企业为确保自身网络安全、更有效的管理网络接入用户，需要部署用户接入管理产品。但是，市场上常见的用户接入管理产品往往缺乏与网络资源管理、业务管理的融合，导致管理手段单一、管理力度不足、管理操作复杂，降低了业务部署及实施、管理的方便性、同时也就降低了部署的预期效果。

终端智能接入组件的用户接入管理模块的部署可解决上述问题，它将用户接入需求细分为以下几个方面：

- 接入用户管理
- 访客管理
- 终端管理
- 用户接入日志
- 接入策略管理

通过几个方面的互相配合，用户接入管理模块可以实现对各种类型接入用户的用户信息以及接入策略的集中管理，并可以满足有线和无线网络对接入用户的的身份认证和接入控制需求。

2. 设备认证管理

终端智能接入的设备认证管理模块（以下简称 TAM）提供对管理设备（登录设备执行命令行）的维护人员进行认证、授权和审计的功能，本系统将这些维护人员统称为设备用户。

TAM 组件可以支持的主要业务特性如下：

- 支持设备的多种划分方式：设备既可以基于管理区域划分，也可以基于设备类型划分。
- 灵活的自定义授权策略：每一条策略可以按照优先级定义多套授权项，每一套授权项基于场景（设备区域、设备类型、授权时段）授权设备用户使用不同的 Shell Profile 属性和命令集。
- 支持用户分组管理：将同一类型的用户划分到一个分组中进行管理，可极大的简化操作员对用户的日常维护，同时方便操作员分权管理用户分组。
- 支持 LDAP 用户统一认证：既可以实时通过 LDAP 服务器进行认证，也可以将用户信息从 LDAP 服务器同步到本系统中进行认证。
- 统一的监控设备用户操作：统一监控设备用户的认证、授权和执行命令行操作。
- 支持与平台和其它组件的分布式部署，大大提高了系统的容量和性能。

5.6 EAD安全策略组件

EAD 安全策略组件通过对接入网络的用户终端强制实施企业安全策略，加强网络用户终端的主动防御能力，并严格控制终端用户的网络使用行为，保护网络安全。作为 EAD 解决方案的核心，EAD 安全策略组件包括以下业务模块：

- EAD 安全管理业务模块（EAD）

  EAD 通过检查接入用户的防病毒软件，操作系统补丁，注册表和网络流量等安全检查项判断接入用户的安全性，并对存在严重安全隐患的接入用户进行隔离或下线，进而达到保障网络安全的目的。除此以外 EAD 还提供了分级管理和报表等功能。
- 桌面资产管理业务模块（DAM）

DAM 将安装了 Windows 操作系统的终端（PC 或服务器）视为资产，通过 iNode 客户端收集接入用户的资产信息，并为操作员审计资产的使用情况提供依据。除此以外 DAM 还提供了软件分发和报表等功能。

5.7 MPLS VPN管理组件

MPLS VPN 技术由于可以在同一物理网络上承载不同的网络服务，并使各业务在逻辑上隔离，为不同业务提供安全可靠的专有网络，从而得到广泛的应用。但是，MPLS VPN 涉及众多专业技术，给业务运营、部署、监控等方面带来了很大的管理难度。MPLS VPN 管理组件（简称 MVM）基于 iMC 平台开发，采用业界标准的 SOA 架构，提供融合的资源管理和重整业务流程。MVM 提供了四个业务管理特性，分别为：BGP MPLS VPN 管理、L2VPN 管理、MPLS TE 管理以及 MPLS TP 管理。主要功能如下：

- BGP MPLS VPN 管理用于管理 L3VPN 网络，包括对 PE、CE 等设备资源管理，MPLS VPN 拓扑监控以及网络部署功能。
- L2VPN 管理用于管理二层 VPN 网络，包括基于 MPLS 的 VPLS 网络和 VLL 网络以及基于链路层的 PBB 网络。
- TE 特性作主要对网络中的 TE 设备提供一个集中管理的平台，可以对 TE 设备信息、设备 FRR 扫描间隔、自动带宽设置、CR－LSP 仲裁方式等进行集中展示和配置。
- MPLS TP 管理用于管理 MPLS TP 网络，定位于为城域网提供 MPLS TP 网络管理方案，提供了 VPN 设备管理、VPN 资源管理、隧道管理、E-Line 业务管理、E-Lan 业务管理、MPLS TP 拓扑展示和性能监控等功能。

5.8 IPsec VPN管理组件

IPsec VPN 管理组件（简称 IVM）是针对 IPsec VPN 网络配置进行统一管理的组件。该组件定位于管理网络域、IPsec 设备配置和 IPsec 及 IKE 安全提议模板，以实现对 IPsec VPN 网络的高效的管理和灵活部署。

IVM 提供了对 IPsec VPN、GRE over IPsec 和 DVPN 三种类型网络域的管理功能。管理员可以将 IPsec 设备加入到同一网络域中，以便统一下发和修改 IPsec 配置。网络域管理提供了批量部署、拆除 IPsec 隧道等功能，可以有效减少管理员的工作量。除此以外，IVM 还可以与分支网点管理组件联动，对使用动态 IP 地址，且位于 NAT 后的 Spoke 设备进行管理。

5.9 EPON管理组件

随着宽带业务的发展，网络接入部分(最后一公里)的带宽“瓶颈”也越来越严重。EPON 采用点到多点结构，无源光纤传输方式，由于使用这种经济而高效的结构，从而成为连接接入网最终用户的一种最有效的通信方法。10Gbps 以太主干和城域环的出现也使 EPON 成为全光网中最佳的最后一公里的解决方案。

EPON 组件用于运营商网络中对 PON 设备管理，用户通过该组件，可以方便的部署接入网中 EPON 相关配置。有效的减少用户操作。EPON 组件提供了部署，升级，拓扑等功能，将 OLT 与 ONU 之间的关系直接展现在用户目前，为用户规划网络提供有益的参考。

5.10 网络流量分析组件

网络流量分析组件简化了对于企业网络中带宽使用的监控。用户借助网络流量分析组件了解谁、何时占用了带宽，使用多长时间，网络流量来自何地、流向何处。

该组件提供易于理解的各种基于流量、应用和会话的报表，展现出网络流量的基线和趋势，以便用户快速诊断网络问题并解决带宽瓶颈。

同时作为用户进行网络优化、网络设备投资、网络带宽优化等的参考，通过故障根源分析、SLA 分析等基于规则和策略的深度分析，直观展示网络运行状态，快速定位故障源，协助优化网络结构；通过流量异常检测、网络安全事件的集中管理和基于资源管理平台的协同响应，提高风险识别的准确度、快速响应安全威胁。

5.11 用户行为审计组件

随着越来越多的企业投入资金加强 IT 信息化建设，对员工对网络使用情况的管理和监控逐渐成为重点。

用户行为审计组件对于日益增多的网络设施和复杂的业务应用环境，提供了一个简单、高效的日志审计工具，帮助操作员快速、准确地查看网络访问的相应信息，如：在邮件审计中可查询到在某一时间段内，发件人(apple@h3c.com)向哪些用户发了邮件等信息，从而帮助操作员定位问题。

用户行为审计组件采用先进的 NetStream 和探针技术，只需要很少的时间投入和带宽占用，就可以获得丰厚的收益，是一种高性能的解决方案。

该组件对海量、复杂的日志数据进行过滤处理，以表格的形式将信息展示出来，以帮助操作员掌握整个网络的运行状态、快速发现并定位网络故障、合理规划网络资源，从而为网络的稳定、高质量的运行提供有力保障。

5.12 应用管理组件

应用管理组件（简称 APM）是一款基于 iMC 平台的网络管理组件，主要用于监视网络中的各种应用。其在对应用进行持续监视的同时收集应用的各种监控指标数据，并生成应用监视报表。操作员可以通过应用监视报表找出应用的性能瓶颈，保障关键业务的可靠性，可用性和连续性。

可以监视的应用类型包含 Windows 服务器、Unix 服务器、Linux 服务器、数据库服务器、应用服务器、Web 服务器、邮件服务器、中间件/Portal、Web 服务、HTTP 服务、LDAP 服务、文件/目录、服务监视、SAP、虚拟设备和存储设备。

5.13 QoS管理组件

QoS 管理组件（简称 QoSM）以 iMC 平台为基础，通过对网络设备的 QoS 配置进行管理来实现对整个网络服务质量的控制和管理。

在 QoS 管理组件中，管理员可以配置多样的流分类、流行为和流策略，并将流策略与设备的接口或 VLAN 绑定形成 QoS 方案。

QoS 方案是 QoS 管理组件和设备交互的基本单元。QoS 管理组件既可以将 QoS 方案部署到设备上，以此改变设备上的 QoS 配置；也可以将设备上已有的 QoS 配置读取并保存为 QoS 方案，方便后续的配置升级和维护。

以上看似复杂的过程都是通过向导的方式进行，大大简化了配置的复杂性和难度。同时，QoS 管理组件屏蔽了各种设备命令行不统一、配置逻辑各不相同的现状，使用统一的配置管理界面，进一步降低了管理员的工作量，让管理员在轻松自由中更加有效、经济的规划网络资源。

5.14 服务健康管理组件

随着网络应用的不断增加，各种服务对网络的可靠性和稳定性提出了更高要求。如何为服务提供高效而可靠的网络，以确保各项应用满足用户要求，成为管理员的一大难题。

服务健康管理组件（简称 SHM）以 iMC 平台为基础，提供了服务质量可视化的管理功能。该组件融合了告警、性能、网络流量分析（NTA）和网络质量分析（NQA）等数据，通过关键质量指标（KQI）和服务等级协议（SLA），实现了对服务健康状况的监控、度量以及可视化管理。该组件提供了多种报表，可以将 SLA 的统计和评价结果通过图形和表格的形式进行直观的展示，方便管理员了解业务的整体服务水平，并及时发现潜在的问题。

5.15 分支网点管理组件

分支网点管理组件（简称 BIMS）由 BIMS 管理平台和 ACS（自动配置服务器）组成。BIMS 通过 TR-069 系列协议对广域网中的 CPE 进行远程集中管理，能够解决 CPE 设备量大、动态 IP、位于 NAT 后等管理困难，节约维护成本，提高问题解决效率。该组件主要包括 CPE 设备资源管理、CPE 设备业务配置管理、CPE 设备配置管理、告警管理、报表管理，系统管理等功能，可以满足 CPE 设备在运营商解决方案中的多种管理需求。

5.16 VAN Fabric管理组件

虚拟应用网络（Virtual Application Network，简称 VAN）是 H3C 推出的网络解决方案，主要关注虚拟化、自动化和软件定义网络三个方面。Fabric 网络是由 FCoE 交换机、服务器、存储设备组成的网络。

VAN Fabric 管理组件（简称 VFM）是基于 iMC 平台开发的数据中心网络管理组件，为广域网提供数据中心整合 LAN 网络和 SAN 网络的管理方案，可以配合 H3C 的网络设备实现对数据中心网络的管理。

VFM 通过 iMC 平台的虚拟资源管理模块来获取虚拟机的迁移信息。VFM 的主要功能包括业务概览、VAN Fabric 拓扑、DC 管理、SAN 配置管理、LAN 配置管理和统计信息。

5.17 移动办公管理

随着移动互联网的不断发展，使用移动终端的用户越来越多，移动办公的需求也变得越来越强烈。借助不断成熟的虚拟技术和云服务平台，移动办公管理（简称 EMO）具有在移动终端远程打开 Windows 应用程序和桌面的功能，在应用商店中使用本地资源实现远程办公的功能，以及管理终端安全的功能。EMO 不仅保持了用户的使用习惯，保护了用户的已有投资，还保证了用户的数据安全，极大地提高了业务的可管理性和可维护性。

5.18 业务服务管理

业务服务管理组件(简称 BSM)是一款以业务为管理对象，对企业 IT 业务的运行情况进行长期监控和维护的组件。业务运行的是否稳定通常受到网络、服务器和各种中间件的影响。BSM 通过对上述三者的实时监控，对收集的数据进行分析，最终从业务可用性、业务健康度和业务繁忙度三个角度，对业务的运行质量进行分析、实时展示和阈值告警，帮助 IT 管理者及时了解对各业务的运行情况。BSM 提供的主要功能有：

- 业务监视：用于定义一个业务，即配置一个业务涉及的网络设备、应用和主机，并对业务的可用性、健康度和繁忙度的阈值进行配置。
- 业务数据窗：提供了业务卡片，业务水晶球，基于时间轴的业务分析报表和业务拓扑等多种展示形式，向用户实时展示所有业务的运行情况。
- 业务端到端拓扑：用户可以任意输入源终端和目的终端的 IP 地址，BSM 绘制出两者之间经过的网络拓扑。通过该功能可以直观的了解到从访问业务的终端到业务服务器之间的网络拓扑。
- 维护计划：维护计划用于定义一个企业正常的对主机、业务和网络设备的维护时间计划，在维护计划之内的业务中止，不影响业务可用性、健康度的计算。

5.19 ITSM服务管理组件

ITSM 服务管理组件（简称 ITSM）是一款以 ITIL 为核心思想，实现对 IT 业务进行全生命周期管理的业务组件。ITSM 提供了一个集成、合理、有序和有效的流程集合，帮助 IT 部门将各种 IT 业务有条不紊的进行。在日常的网络和业务管理过程中，使用这种业务流程控制手段，可以实现对 IT 行为的过程和结果进行有效监管和控制，并提供事后任务审计功能。此外，ITSM 可以与 iMC 平台中常用网络配置管理操作相互配合，并结合各种基本的可配置项，为用户提供可运营维护的网络和业务配置管理环境，并最终提升管理软件的应用范围和价值。

5.20 安全业务管理组件

安全业务管理组件（简称 SSM）是 iMC 中一个负责网络安全相关业务的组件，主要用于通过对网络上的安全设备进行管理，来保障网络安全。它提供了综合的安全智能、高效实施的安全信息和事件管理解决方案，能够对全网海量的安全事件、日志进行集中收集与统一分析，兼容异构网络中各厂商的多种设备，支持海量数据的高度聚合存储及归一化处理。安全业务管理组件主要提供安全拓扑、安全事件管理、全局资源管理和防火墙业务配置的功能。

安全业务管理组件包含一个子组件，即负载均衡管理组件（简称 LBM）。负载均衡管理组件主要用于对负载均衡设备的业务管理和配置以及负载均衡性能数据展示。负载均衡管理组件通过对负载均衡设备的配置来部署实现负载均衡功能的虚服务、实服务器和实服务器组。通过配置对象和应用模板，增加业务部署的重用性。通过负载均衡设备、虚服务、实服务器以及实服务器组的性能统计，直观展示用户所关心的业务性能数据。该组件提供了资源管理、性能管理、服务管理、配置模板等功能。

5.21 无线业务管理组件

由于无线系统具有便于搭建和使用，无需考虑复杂的布线和变迁等特点已越来越多的应用到各个领域。然而，无线系统不是完全的无线系统，它的服务器和骨干网仍然安置在固定网络，只是用户可以移动。AP、AC 等设备的管理以及由此带来的网络安全问题也开始受到关注。

无线业务管理组件用于无线局域网管理，提供对无线网络中 HPE MSM 系列和 H3C 系列、Aruba 以及 Cisco 的 AC、Fat AP、Fit AP 设备以及终端用户的发现、配置和监控功能。

用户可以借助 WSM 组件对无线网络进行配置和部署，监控各无线设备的运行、使用情况，并支持按漫游域、楼层、设备类型等分组管理无线设备，同时提供直观的拓扑图来查看设备运行状态、AP 的位置和连接情况。

随着物联网的迅速发展和医院信息化服务需求的不断提高，物联网模块在医院中已经被广泛使用，对医院的物联网模块和网络资产进行统一管理和监控的需求越来越强烈，WSM 医疗物联网管理系统正是应此而生。WSM 通过物联网 AP 内置的 RFID 技术和先进的中间件技术，协助应用系统平台完成对物理实体的信息采集，为企业设施最终实现智能的物与人、物与物的控制和信息交互，提供高标准，符合标准协议和规范的网络基础平台。WSM 能够管理物联网网络设备，通过与第三方中间件系统集成，能够监控环境中的医疗标签/资产，并进行统计分析、展示，支持与有线无线设备统一管理。

6 常见问题解答

6.1 iMC运行时需要注意什么？

表6-1 iMC 运行时的注意事项

注意事项	详细说明
在安装iMC的环境中安装杀毒软件，需把iMC加入白名单。	安装杀毒软件时，若未将iMC加入白名单，杀毒软件可能会损坏iMC的后台文件，导致进程运行异常或者功能异常，请谨慎操作。
服务器如需关机，请规范操作，不要直接切断电源。	服务器异常断电，可能会造成数据库被质疑，进程启动失败，iMC相关功能无法正常运行，请谨慎操作。
请谨慎使用服务器资源动作中点击重启或者下电链接。	**1.** 误操作会导致该服务器重启或者下电。

6.2 使用浏览器访问iMC需要注意什么？

在使用浏览器访问 iMC 配置管理页面时，需要注意如下几点：

表6-2 与浏览器相关的注意事项

注意事项	详细说明
由于浏览器支持能力不同，需要避免进行如下操作，否则可能造成配置界面或系统数据异常。	1、使用浏览器的前进、后退按钮切换操作页面。 2、通过Firefox/Chrome[文件/新建窗口]的方式打开新的浏览器窗口。 3、在一台计算机上同时打开两个Firefox/Chrome窗口并访问同一个iMC服务器。 4、在输入框中输入超长数据。输入内容简捷、明确即可。 5、在加载页面的过程中出现进程条时，点击浏览器的停止按钮。此操作将导致页面无法恢复且不能进行任何操作，此时点击浏览器刷新按钮即可恢复正常。 6、在浏览器中短时间内进行频繁点击某个对象（按钮、链接、菜单项等）等异常操作。
iMC升级后，使用浏览器访问iMC时出现异常，怎么办？	这是由于浏览器缓存了旧版iMC的页面脚本，可能出现的异常现象包括： 1、浏览器提示脚本错误。 2、页面链接无法使用。 3、页面元素显示异常。 解决办法：清除浏览器的缓存，并重启浏览器。
使用Firefox访问iMC需要关注的安全性问题：	使用Firefox登录iMC后，单击浏览器的<转到上一页>按钮返回登录页面，然后再单击<转到下一页>按钮，此时浏览器页面无需再次输入用户信息即可正常登录。为了安全起见，退出系统时建议点击iMC操作页面右上角的“注销”按钮或直接关闭浏览器。
使用Firefox，如果上传文件太小（如只有几个字节），有可能出现上传文件失败。	出现这种情况时，请使用Chrome 浏览器进行操作，或换一台客户端尝试一下。

注意事项	详细说明
使用Firefox进行单设备ACL配置，有时会出现Tab错行显示的问题，这是为什么？	这是Firefox浏览器的固有缺陷造成的。这种情况下不影响功能使用，也可以使用Chrome 浏览器进行相关的配置操作。
使用Firefox新增操作员时，增加页面中的用户名和密码不为空，而是显示出登录的用户名和密码，为什么？	这是Firefox浏览器提供的自动记录登录密码功能导致的。当登录iMC时，Firefox会提示是否记录登录密码，如果选择“记住”，则会在之后的输入密码框中自动输入之前记住的信息。为了避免该情况的发生，可以选择“不记录本站点”或“暂不”。或者直接清除Firefox的密码缓存。
登录iMC后，使用浏览器记录的历史访问某个页面，可能出现越权访问、告警面板消失，拓扑无法打开等问题怎么办？	可从两方面解决此问题： **2.** 使用页面内部的导航方式进行操作，不要在网页地址栏中直接输入 URL。 **3.** 对于浏览器历史记录的问题，建议将浏览器设置为不保存历史记录。设置方法：在浏览器的工具栏中选择“工具”->“Internet 选项”->在“历史记录”中将“页面保存在历史记录中的天数”设为“0”。
浏览器弹出窗口被阻止后会报脚本错误，怎么办？	iMC的部分配置界面为弹出窗口形式，建议允许浏览器弹出窗口，以免影响正常使用。
说明： 除上述问题外，若浏览器安装了某些插件，请检查插件设置是否正确，以免影响iMC的正常使用。	

6.3 在使用iMC过程中，界面操作出现不响应，被弹出到重新登录页面以及其他脚本错误，如何处理？

请尝试如下操作：

- 将 iMC 站点加入浏览器受信任站点，检查问题是否解决。
- 换一台客户端计算机，使用浏览器访问相同页面，检查问题是否解决。

如果上述方法仍不能解决问题，请联系 H3C 公司技术支持，做进一步定位。

6.4 登录操作系统时需要注意什么？

为了保证 iMC 的正常安装和运行，建议使用管理员帐号登录操作系统。

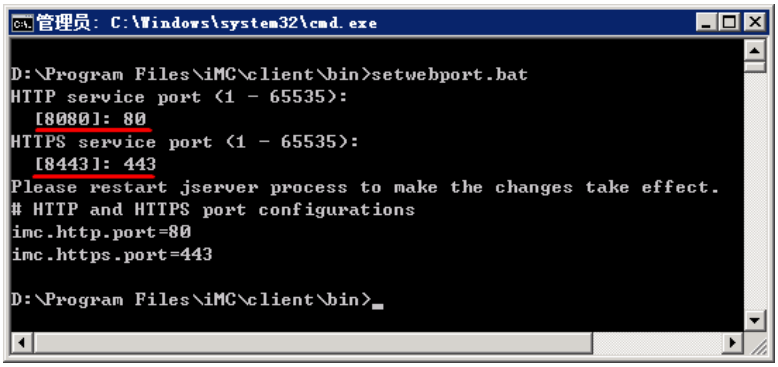
6.5 iMC安装完成后，如何修改iMC服务器的Web服务端口号？

解决方法：使用 iMC 提供的 Web 服务器端口号修改工具：

- Windows 环境：<iMC 安装目录>\client\bin\setwebport.bat
- Linux 环境：<iMC 安装目录>/client/bin/setwebport.sh

根据提示输入待设置的端口号。Windows 环境可将 iMC 服务器的 HTTP 端口号由 8080 修改为 80，HTTPS 端口号由 8443 修改为 443。Linux 环境可以参考图 6-1 进行修改。

图6-1 setwebport.bat 执行结果



修改后需要重启 jserver 进程。如果 iMC 采用分部式部署，则需要在所有 iMC 服务器上进行以上修改。

如果部署了 EIA 组件，除了需要运行工具修改 Web 端口号外，还需要在 EIA 的系统参数配置中修改 iMC 配置台端口。端口必须修改为 iMC 服务器的 HTTP 端口号，否则会造成访客管理员无法为预注册访客转正。

修改方法：

(2) 选择“用户”页签，单击[接入策略管理/业务参数配置]菜单项，进入业务参数配置页面。

(3) 点击“系统配置”链接，进入系统配置页面。

(4) 点击“系统参数配置”对应的配置图标，进入系统参数配置页面。

(5) 修改 iMC 配置台端口，修改结果如图 6-2 所示，将 iMC 配置台端口由 8080 修改为 80，单击<确定>按钮保存配置。

图6-2 修改 iMC 配置台端口

6.6 对设备进行Telnet操作时，弹出对话框会自动关闭，如何处理？

解决方法：这是由于 Telnet 命令是在本地执行的，会受到本地操作系统安全设置的影响。操作员需要把 Firefox 或 Chrome 浏览器恢复为默认设置，具体请操作方式请参见 iMC 平台联机帮助中的常见问题解答。

6.7 如何修改超级操作员admin的登录密码？

解决方法：以操作员 admin 成功登录 iMC 后，请执行如下操作：

(1) 点击“系统管理”页签。

(2) 点击左侧导航树中[操作员管理/修改密码]。

(3) 输入原密码、新密码及新密码确认后，单击<确定>按钮即可完成修改。

6.8 增加性能视图时，为什么没有性能管理权限的用户组还会出现在“可访问操作员分组”中呢？

这种情况符合 iMC 对权限管理的设计，不会影响用户的正常使用。

操作员权限包括功能权限（如导航菜单）、资源权限（如设备、用户）及数据权限（如自定义视图、性能视图、报表数据等），它们之间的关系为：功能权限优先，在具备某项功能权限的前提下，再通过资源权限和数据权限对该项操作进行过滤。

6.9 如何开启iMC登录验证码功能？

解决方法：iMC 默认不开启登录验证码功能，管理员可以通过修改 iMC 的配置文件启用该功能。

修改 iMC 配置文件，配置文件位于：

- Windows 环境：

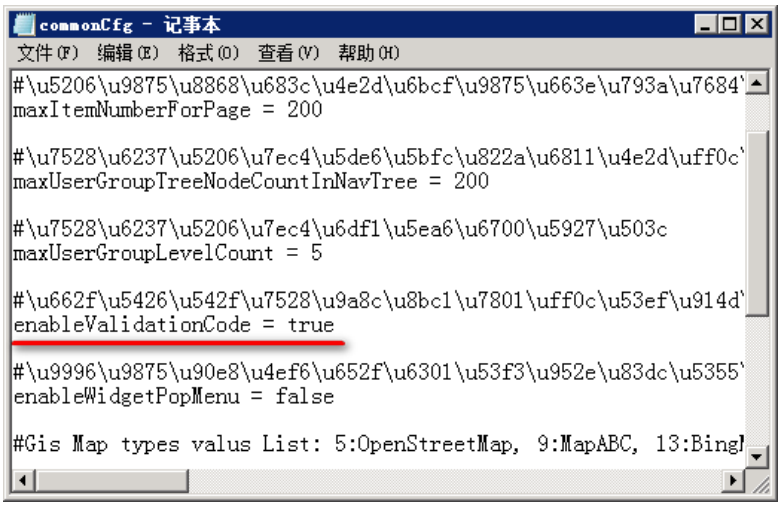
  <*iMC 安装目录*>\client\conf\commonCfg.properties

- Linux 环境：

  <*iMC 安装目录*>/client/conf/commonCfg.properties

使用文本编辑器打开配置文件，以 Windows 环境为例，将参数 enableValidationCode 的值由 false 改为 true，如图 6-3 所示。

图6-3 commonCfg.properties 配置文件



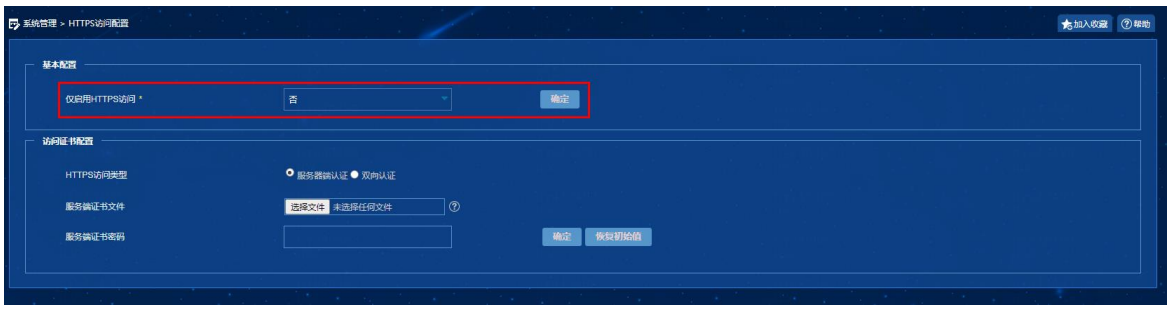
保存配置文件后，重启 iMC。登录 iMC 时，如图 6-4 所示，已启用验证码功能。

图6-4 启用登录验证码功能

6.10 如何限制管理员只能使用HTTPS协议访问iMC？

iMC 缺省提供了使用 HTTP 和 HTTPS 协议访问 iMC 的方式，如果要限制管理员只能使用 HTTPS 协议访问 iMC，可在“系统管理 > 系统配置 > HTTPS 访问配置”页面配置，如图 6-5 所示。配置完成后请重启 iMC 使配置生效。

图6-5 HTTPS 访问配置



6.11 如何配置通过HTTP协议访问iMC，自动跳转为HTTPS协议访问？

iMC 缺省提供了使用 HTTP 和 HTTPS 协议访问 iMC 的方式，如果要在管理员通过 HTTP 协议访问 iMC 时自动跳转为 HTTPS 协议访问，则需要修改 iMC 的配置文件。

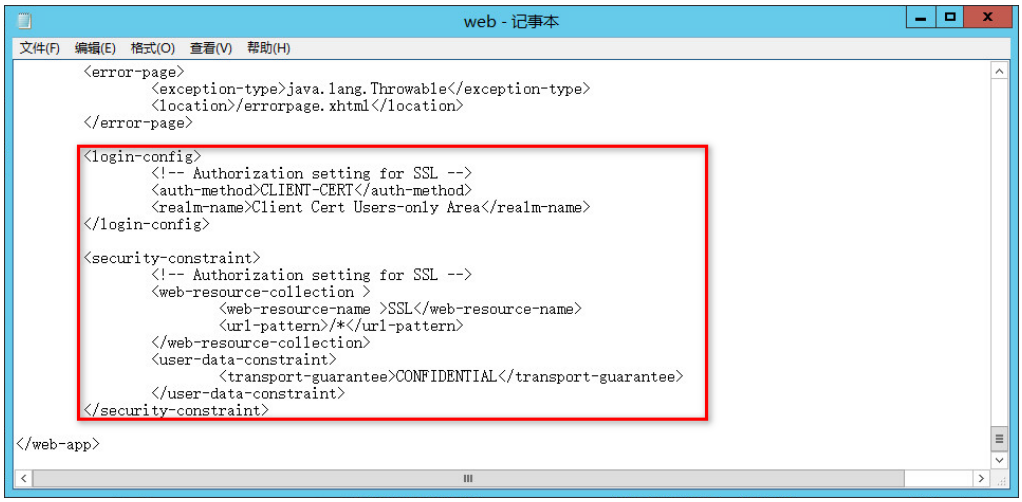
待修改的配置文件位于：

- Windows 环境：*<iMC 安装目录>*\client\web\apps\imc\WEB-INF\assembly\web.xml
- Linux 环境：*<iMC 安装目录>*/client/ /web/apps/imc/WEB-INF/assembly/web.xml

以 Windows 环境为例，使用文本编辑器打开 iMC 的配置文件*<iMC 安装目录>*\client\web\apps\imc\WEB-INF\assembly\web.xml，如图 6-6 所示，在此文件最后一行</web-app>和倒数第二行</error-page>之间增加如下配置，修改后重启 iMC 即可。

```
<login-config>
<!-- Authorization setting for SSL -->
<auth-method>CLIENT-CERT</auth-method>
<realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
<!-- Authorization setting for SSL -->
<web-resource-collection >
<web-resource-name >SSL</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

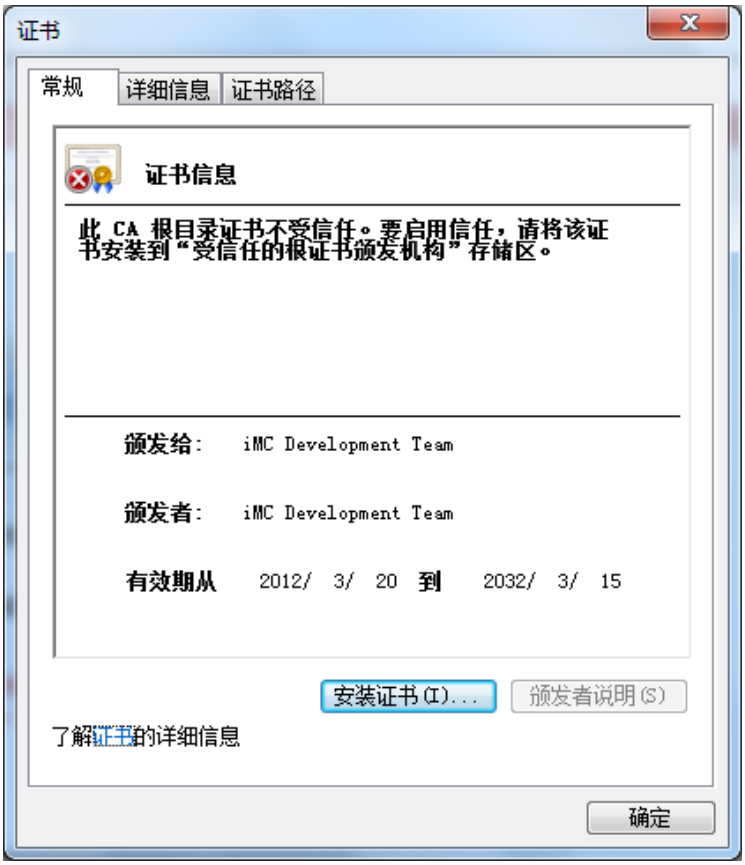
图6-6 web.xml 配置文件



6.12 如何为iMC安装证书？

iMC 缺省提供了一张由 iMC 开发团队创建的证书，如图 6-7 所示。

图6-7 iMC 缺省证书



如果用户不想使用 iMC 提供的证书，可以根据以下操作步骤在 Windows 环境中创建证书：

(2) 停止 iMC。

(3) 通过命令行进入目录<*iMC 安装目录*>\client\security\。

(4) 使用以下命令将 newks 文件重命名为 newks.bak。

```
rename newks newks.bak
```

(5) 使用以下命令创建证书：

```
<iMC 安装目录>\common\jre\bin\keytool.exe -genkey -v -alias iMC -validity 3650 -keyalg
RSA -dname "CN=192.168.1.100, OU=R&D, O=Company, L=Beijing, S=China, C=CN" -keypass
iMCV500R001 -storepass iMCV500R001 -keystore newks
```

-dname 的参数含义：

- CN：iMC 服务器的主机域名或 IP 地址。
- OU：组织单元（Organizational Unit，OU）名称。
- O：公司或组织名称。
- L：城市名称。
- S：国家名称。
- C：两位国家代码，中国为 CN。

如果 CN 的值不为 iMC 服务器的主机域名或 IP 地址，管理员在通过浏览器访问 iMC 时会提示证书地址不匹配。

(6) 使用以下命令查看创建的证书：

```
<iMC 安装目录>\common\jre\bin\keytool.exe -list -v -alias iMC -keystore <iMC 安装目录>\client\security\ newks -storepass iMCV500R001
```

(7) 修改 iMC 配置文件：

创建证书时，-keypass 和-storepass 参数分别为证书和证书库设置的密码，如果证书库密码不为 iMCV500R001 请根据下面的步骤修改 iMC 配置文件，否则跳过该步骤。

使用文本编辑器打开 iMC 的配置文件<*iMC 安装目录*>\client\conf\server.xml，如图 6-8 所示，将红线所示参数替换为新的证书库密码。

图6-8 server.xml 文件-Windows

```
<!--  HTTPS Connector  -->
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxPostSize="5242880"
  URIEncoding="UTF-8" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25"
  maxSpareThreads="75" enableLookups="false" acceptCount="100" connectionTimeout="60000"
  compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
  compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
  disableUploadTimeout="true" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
  sslProtocol="TLS" keystoreFile="security/newks" keystorePass="iMCV500R001" />
```

(8) 启动 iMC。管理员在通过浏览器访问 iMC 时还需要增加对新证书的信任。增加信任的操作步骤请参考问题 6.13 使用 Windows 操作系统时，无法在设备详细信息页面 Telnet 到设备，怎么办？。

对于 Linux 环境，管理员需将配置步骤中的“\”替换为“/”，keytool.exe 替换为 keytool，再按照步骤操作。Linux 环境下的 server.xml 文件如图 6-9 所示，将红线所示参数替换为新的证书库密码。

图6-9 server.xml 文件-Linux

```
                <!-- HTTPS Connector -->
                <Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100"
clientAuth="false" compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/
javascript,text/plain" compression="on" compressionMinSize="2048" connectionTimeout="60000"
disableUploadTimeout="true" enableLookups="false" keystoreFile="security/newks"
keystorePass="iMCV500R001" maxHttpHeaderSize="8192" maxPostSize="5242880"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" noCompressionUserAgents="gozilla,
traviata" port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLS"/>
```

6.13 使用Windows操作系统时，无法在设备详细信息页面Telnet到设备，怎么办？

问题分析：设备详细信息页面的 Telnet 功能需要依赖 Windows 操作系统的 Telnet 客户端工具。部分 Windows 操作系统缺省不提供 Telnet 客户端工具。

具体的解决办法请参考 iMC 平台联机帮助的常见问题解答。

6.14 为什么有些设备的Web网管界面无法打开？

解决办法：Web 网管功能受限于设备侧的配置，只有选择的设备支持并且启动了 Web 网管，该功能才能正常使用。

6.15 如何通过命令行停止和启动iMC单个进程？

(1) 在 iMC 运行状态下，打开命令行终端，进入“<iMC 安装路径>\deploy”路径下。

(2) 执行 procctl.bat –plist 命令（Linux 操作系统下执行./procctl.sh –plist 命令）查看进程状态以及对应 ID。

(3) 执行 procctl.bat –pstop *ID* 或 procctl.bat –pstart *ID* 命令（Linux 操作系统下执行./procctl.sh –pstop *ID* 或./procctl.sh –pstart *ID* 命令）停止或启动某个 iMC 进程。以 seplat 进程为例，该进程的 ID 为 1039，停止和启动该进程的方法如图 6-10 所示。

图6-10 停止和启动 seplat 进程

```
E:\Program Files\iMC\deploy>procctl.bat -pstop 1039
Stop process 1039 commond send  successed

E:\Program Files\iMC\deploy>procctl.bat -pstart 1039
Start
```

6.16 网络中的一台设备被替换后，如果新设备的IP地址与原设备的IP地址不同，网络拓扑中的拓扑计算不正确，怎么办？

这是由于原设备抢占了新设备在网络拓扑中的位置，iMC 无法获知原设备已被替换，解决办法：

- 可以将原设备从 iMC 中删除，然后手工同步新设备。
- 将新设备的管理地址设置为与原设备相同，然后手工同步新设备。

6.17 为什么在数据转储功能的“转储后执行命令”中配置了某些命令，在执行时会导致CPU占用率长时间过高？

解决方法：转储后执行的命令不能存在如下情况，否则可能导致执行异常：

- 有 GUI 界面的命令。
- 运行后不能自动退出的命令。

6.18 为什么在增加一个仅大小写不同的同名视图时，提示该视图已存在？

解决方法：由于 SQL Server 数据库不区分大小写，因此对于“ROUTER”和“router”这样的输入，系统将认为是同一条记录，并提示该视图已存在。在其他要求唯一性的输入框中，也请注意大小写问题，以免操作失败。

6.19 iMC在使用SQL Server数据库运行一段时间之后，出现内存占用过高且不能恢复的现象，怎么办？

解决方法：可以通过调整 SQL Server 的最大使用内存解决该问题。

使用 iMC 提供的修改 SQL Server 最大使用内存工具：

<*iMC 安装目录*>\client\bin\setsqlservermaxmem.bat -server *server* -saPwd *password* –maxMem *maxmem*

参数说明：

- **-server** *server*：SQL Server 服务器的名称或 IP 地址，可选参数，缺省值为 localhost。
- **-saPwd** *password*：数据库 sa 用户的密码，必选参数。
- **-maxMem** *maxmem*：需要调整到的最大使用内存，单位 MB，可选参数。

举例：

iMC 采用集中式部署和远程数据库时，SQL Server 服务器的 IP 地址为 192.168.100.199，sa 用户的密码为 iMC123，最大大缓冲区内存设为 1024MB。在 Windows 的命令行窗口中输入以下命令：

<*iMC 安装目录*>\client\bin\setsqlservermaxmem.bat -server 192.168.100.199 -saPwd iMC123 -maxMem 1024

注意

- 由于 SQL Server 本身要占用一定内存，因此实际使用的内存量可能比设置的数值大一些。
- SQL Server 最大使用内存调整完成后，需要重启 SQL Server 才能使配置生效。

6.20 浏览iMC资源时，发现设备视图中没有任何设备，为什么？

解决方法：发生上述情况主要原因是硬件配置不足，类似情况还有：

- iMC 进程无故自动重启。
- 系统响应缓慢，经常提示系统资源不足。
- 周期性报表无法生成。

出现上述情况后，请及时升级 iMC 服务器的内存等硬件资源。

6.21 在iMC运行过程中，能否修改操作系统时间，为什么？

解决方法：iMC 运行过程中，尽量不要手工修改操作系统的时间。因为此操作可能造成数据混乱或进程运行错误等问题。

如果修改系统时间后出现 iMC 进程运行错误，请重新启动 iMC 的相关进程（包括部署监控代理和 Intelligent Management Server 服务）。

6.22 在iMC中导入长文件名的文件时，系统没有响应怎么办?

解决办法：文件名的最大长度受不同的操作系统/浏览器的限制。请尝试缩短文件名，并重新导入。

6.23 在iMC中输入了较长的内容后，有时会造成界面不美观，怎么办？

解决办法：这是浏览器存在的固有缺陷，不会影响功能的正常使用。为了避免出现类似问题，在 iMC 相关界面输入时请补充必要的空格，浏览器会自动调整界面布局。

6.24 在表格中直接导航到最后一页，有时会出现表格下方的页数多于上方显示页数的情况，为什么？

解决办法：为了提升查询效率，表格导航控件会自动缓存上一次查询得到的总页数。如果直接导航到最后一页，表格控件将使用上次缓存的页数进行查询，在显示列表数据后重新计算总记录数并在表格下方的导航控件中显示出来。

如果两次查询过程中数据库的记录数量有增加，就会出现这种情况。此时如果要继续向后翻页，使用表格下方的导航链接即可。

6.25 管理员登录iMC时，页面提示“系统资源不足，无法完成该操作”，怎么办？

解决方法：可以通过调整 iMC 所在系统的 Java Heap 内存最大值解决该问题。

使用 iMC 提供的修改 Java Heap 内存最大值的工具：

- Windows 环境：*<iMC 安装目录>*\client\bin\setmem.bat *Maxsize*
- Linux 环境：*<iMC 安装目录>*/client/bin/setmem.sh *Maxsize*

Maxsize 为 Java Heap 内存的最大值，相应值请参考以下表格。

表6-3 32 位操作系统

节点数	采集单元	在线操作员	Java Heap 内存
0~200	0~5K	20	512M（Windows） 512M（Linux）
	5K~50K	10	
200~500	0~10K	30	1G（Windows） 1G（Linux）
	10K~100K	10	

表6-4 64 位操作系统

节点数	采集单元	在线操作员	Java Heap 内存
0~200	0~5K	20	2G（Windows） 2G（Linux）
	5K~50K	10	
200~1K	0~10K	30	2G（Windows） 4G（Linux）
	10K~100K	10	
1K~2K	0~20K	30	4G（Windows） 6G（Linux）
	20K~200K	10	
2K~5K	0~30K	40	8G（Windows） 8G（Linux）
	30K~300K	20	
5K~10K	0~40K	50	12G（Windows） 12G（Linux）
	40K~400K	20	
10K~15K	0~40K	50	16G（Windows）

节点数	采集单元	在线操作员	Java Heap 内存
	40K~400K	20	16G（Linux）

采集单元是指每 5 分钟对一个采集实例进行一次采集的过程。一个采集实例即一个性能采集指标的实例，采集实例计算的举例如表 6-5 所示，以一个设备为例。

表6-5 采集实例计算

监视对象	对象数量	性能采集指标	采集实例
设备CPU	1	CPU利用率	1
设备内存	1	内存利用率	1
设备接口	10	接收速率	10
		发送速率	10
设备整体	1	设备不可达率	1
		设备响应时间	1
总计	采集实例数：24		

如果这 24 个采集实例的采集间隔都是 5 分钟，则采集单元为 24 个。如果这 24 个采集实例的采集间隔都是 10 分钟，则采集单元为 12 个。

注意

- 调整 Java Heap 内存时，请先停止 iMC，调整完成后再启动。
- 32 位操作系统下 Java Heap 内存最大允许调整到 1G，对于需要超过 1G 的使用场景请更换为 64 位操作系统。

6.26 当iMC运行过程中出现问题，并需要技术支持解决时，如何收集iMC的日志？

使用 iMC 提供的日志收集工具：

- Windows 环境：*<iMC 安装目录>*\deploy\logfiles.bat

  收集后的日志保存在*<iMC 安装目录>*\tmp 目录下。
- Linux 环境：*<iMC 安装目录>*/deploy/logfiles.sh

  收集后的日志保存在*<iMC 安装目录>*/tmp 目录下。

注意，在 Windows 环境下运行工具时，需要在命令行窗口中使用。

直接运行日志收集工具只能收集最近 7 天的 iMC 日志，如果要收集 7 天以上的日志，则需要再指定收集日志的天数。

以 Linux 环境为例，运行工具：

<iMC 安装目录>`/deploy/logfiles.sh` *30*

日志收集工具会收集最近 30 天的 iMC 日志，并保存在*<iMC 安装目录>*/tmp 目录下的 log_YYYYMMDDhhmmss.zip 压缩文件中，YYYYMMDDhhmmss 为压缩文件生成的年、月、日、时、分、秒信息。

6.27 当iMC服务器有多块网卡时，如何配置iMC使用其中一个IP地址监听HTTP/HTTPS服务？

解决办法：iMC 缺省监听服务上所有网卡的 IP 地址，要指定使用某一个具体的 IP 地址，需要修改 iMC 的配置文件。

配置文件位于：

- Windows 环境：*<iMC 安装目录>*\client\ conf\server.xml
- Linux 环境：*<iMC 安装目录>*/client/ conf/server.xml

以 Windows 环境为例，使用文本编辑器打开 iMC 的配置文件<iMC 安装目录>\client\ conf\server.xml，如图 6-11 所示，增加红线所示参数。修改后保存文件并重启 iMC。使用该 IP 访问 iMC 可以正常访问，使用其他网卡 IP 无法访问。

图6-11 修改 server.xml 文件

```
- <Service name="Catalina">
    <!--  HTTP Connector  -->
    <Connector URIEncoding="UTF-8" acceptCount="100"
      compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
      compression="on" compressionMinSize="2048" connectionTimeout="60000"
      disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192"
      maxPostSize="5242880" maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
      noCompressionUserAgents="gozilla, traviata" port="80"
      protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443"
      address="192.168.1.163" />
    <!--  HTTPS Connector  -->
    <Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" clientAuth="false"
      compressableMimeType="text/html,text/xml,text/xhtml,text/css,text/javascript,text/plain"
      compression="on" compressionMinSize="2048" connectionTimeout="60000"
      disableUploadTimeout="true" enableLookups="false" keystoreFile="security/newks"
      keystorePass="iMCV500R001" maxHttpHeaderSize="8192" maxPostSize="5242880"
      maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
      noCompressionUserAgents="gozilla, traviata" port="443"
      protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
      sslProtocol="TLS" address="192.168.1.163" />
    <!--  AJP Connectors, disabled in default configuration  -->
```

6.28 当iMC采用分布式部署时，所有主从服务器重启，数据库在从服务器上的组件无法被加载，如何解决？

这是由于主服务器先于从服务器启动完成，造成主服务器上的 jserver 进程无法连接从服务器数据库，导致数据库在从服务器上的组件无法被加载。

解决方法：从服务器启动完成后，手工重启主服务上的 jserver 服务即可。

6.29 如何将网络中的虚拟设备加入iMC？

解决办法：可用使用自动发现添加设备，此时设备类型为“PC”，需要正确配置设备 SOAP 参数才能识别为虚拟设备。SOAP 参数配置分为以下三种情况：

- 对于虚拟机（VM）：不需要配置 VM 的 SOAP 参数。
- 对于 vCenter+ESX/ESXi 的环境：只需配置 vCenter 的 SOAP 参数即可。
- 对于独立的 ESX/ESXi 环境：需要配置每个 ESX/ESXi 的 SOAP 参数。

进入设备详细信息页面，在右侧菜单中选择“修改 SOAP 参数”，配置正确的 SOAP 参数后同步设备详细信息，即可识别为虚拟设备。

6.30 在安装iMC时，数据库检查无法通过，提示如下，如何解决？

图6-12 数据库检查提示错误

```
2010-10-25 16:24:27 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:27 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:34 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:34 [WARN ] [AWT-EventQueue-0] [com.h3c.imc.deploy.Util::getInstallInfo(614)] Can not find
instInfoFile - C:\WINDOWS\iMC-Reserved\instinfo.txt
2010-10-25 16:24:35 [INFO ] [Thread-3]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor::isSQLServer2000Installed(347)] SQL Server 2000 is
Installed
2010-10-25 16:24:35 [INFO ] [Thread-3]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor::isSQLServer2000Installed(347)] SQL Server 2000 is
Installed
2010-10-25 16:24:50 [ERROR] [SwingWorker-pool-1-thread-1]
[com.h3c.imc.deploy.dma.wizard.DatabaseSelectPanelDescriptor$DbConnectCheckingWorkingDialog::doWork(1173)] Connect
to database error
java.sql.SQLException: Unable to get information from SQL Server: 127.0.0.1.
        at net.sourceforge.jtds.jdbc.MSSqlServerInfo.<init>(MSSqlServerInfo.java:97)
        at net.sourceforge.jtds.jdbc.ConnectionJDBC2.<init>(ConnectionJDBC2.java:276)
        at net.sourceforge.jtds.jdbc.ConnectionJDBC3.<init>(ConnectionJDBC3.java:50)
        at net.sourceforge.jtds.jdbc.Driver.connect(Driver.java:184)
        at java.sql.DriverManager.getConnection(DriverManager.java:582)
        at java.sql.DriverManager.getConnection(DriverManager.java:154)
```

解决方法：在安装 SQL Server 2005 及其后版本的数据库时，如果使用了非缺省实例，必须同时启动“SQL Browser”服务，否则会造成 Java 无法连接数据库。

6.31 在iMC中卸载了SOM后，以前通过告警、iCCM、ACLM、VLANM等模块功能创建并提交的SOM流程都无法执行下去了，怎么办？

解决方法：SOM 组件卸载后，未完成的 SOM 流程都将作废，请直接删除相关流程。

6.32 iMC在使用Oracle或MySQL数据库时，部分组件提示数据库操作异常，怎么办？

解决办法：这可能是由于 Oracle 的进程数和连接数不够导致的。默认情况下，Oracle 允许的连接数为 150。iMC 各组件/模块的最大连接数如表 6-6 所示。当多个 iMC 组件/模块采用集中式部署时，建议根据实际部署情况修改 Oracle 的进程数和连接数，Oracle 的连接数需不小于 800。

表6-6 iMC 各组件/模块最大连接数

组件/模块	最大连接数
平台	14
告警	24
Syslog管理	9
性能管理	11
报表	10
访客管理	5
用户自助	5

组件/模块	最大连接数
网络资产	5
虚拟网络管理	9
设备配置管理	9
ACL管理	7
VLAN管理	11
安全控制中心	5
服务器存储自动化	6
VXLAN管理	4
VAN Fabric管理	27
资源自动化管理	16
QoS管理	5
服务健康管理	60
接入业务/计费业务	100
EAD安全管理	25
桌面资产管理	40
MPLS VPN管理	9
L2VPN管理	17
应用管理	10
分支网点管理系统	10
IPsec VPN管理	8
虚拟连接管理	5
安全业务管理	10
负载均衡管理	5
无线业务管理	50

通过以下操作查看并修改 Oracle 的进程数和连接数。

(2) 切换至 oracle 用户。

```
su - oracle
```

(3) 使用 sys 用户以 sysdba 身份登录 Oracle 数据库。

- 登录 Oracle，用 sys 密码替换*<password>*

```
sqlplus sys/<password> as sysdba
```

(4) 查看 Oracle 的进程数和连接数。

- 查看进程数

```
show parameter processes;
```

- 查看连接数

```
show parameter sessions;
```

(5) 根据组件/模块的实际使用情况修改 Oracle 的进程数和连接数。

- 修改进程数，用实际需要的进程数替换*<600>*

```
alter system set processes=<600> scope=spfile;
```

- 修改连接数，用实际需要的连接数替换*<600>*

```
alter system set sessions=<600> scope=spfile;
```

(6) 修改完成后，重启 Oracle 使修改生效。

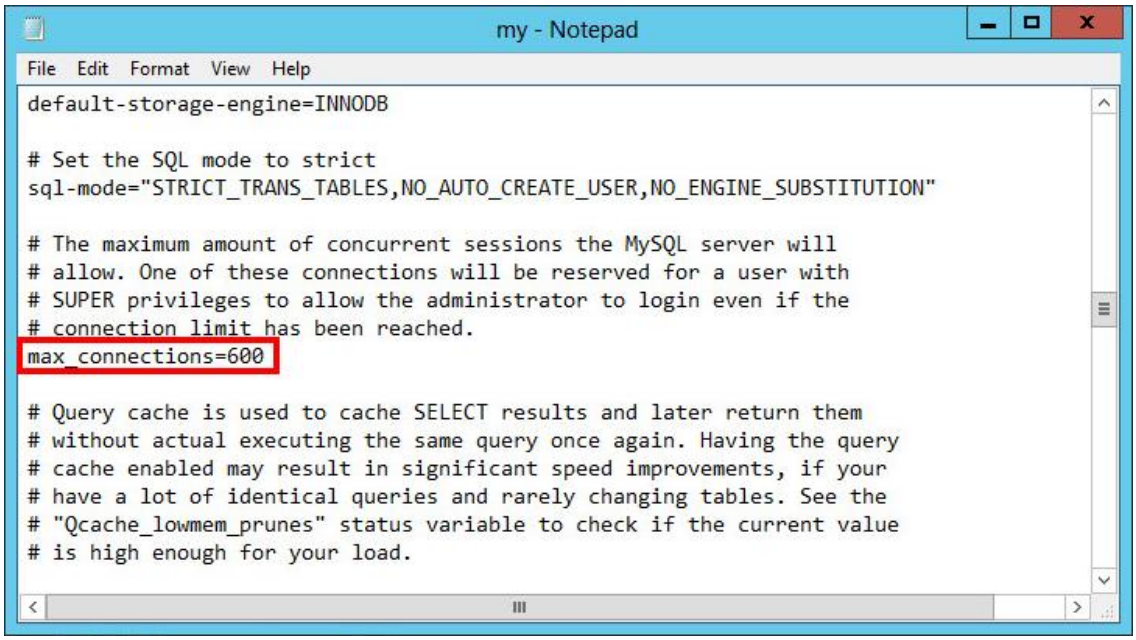
通过以下操作查看并修改 MySQL 的进程数和连接数。

Windows 环境：

(7) 打开 C:\Program Files\MySQL\MySQL Server 5.6 路径下配置文件 my.ini。

(8) 修改 max_connections 参数为 600，如图 6-13 所示。

图6-13 修改 max_connections-Windows



Linux 环境：

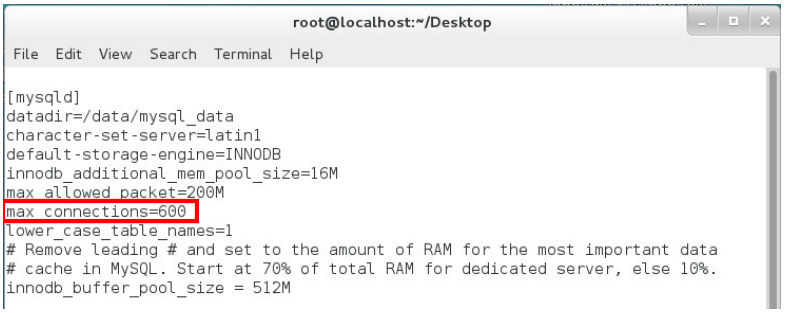
(9) 打开 my.cnf 文件。

```
vi /etc/my.cnf
```

(10) 按下 i 键进入编辑模式。

(11) 修改 max_connections 参数为 600，如图 6-14 所示。

图6-14 修改 max_connections-Linux



6.33 当忘记admin帐号的密码时，如何解决？

解决办法：Windows 环境中使用命令 resetpwd.bat（Linux 环境中使用命令 resetpwd.sh）将 admin 帐号的密码重置为默认密码。iMC PLAT 7.3 (E0706)版本前默认密码是 admin，iMC PLAT 7.3 (E0706)及后续版本默认密码是 Pwd@12345。

双击该文件后，密码会立即被重置。然后使用 admin 帐号和默认密码即可成功登录 iMC。

命令存放路径：

Windows 环境：[iMC 安装路径]client\bin\resetpwd.bat

Linux 环境：[iMC 安装路径]client\bin\resetpwd.sh

6.34 使用HTTPS访问iMC时，如何屏蔽SSLv3协议，而只启用TLS协议？

解决办法：打开“iMC 安装路径\client\conf\server.xml”文件，找到“<!-- HTTPS Connector -->”下方的“<Connector…”配置，在“sslProtocol="TLS"”属性后方增加一个新的属性“sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"”，保存后重启 jserver 进程即可。

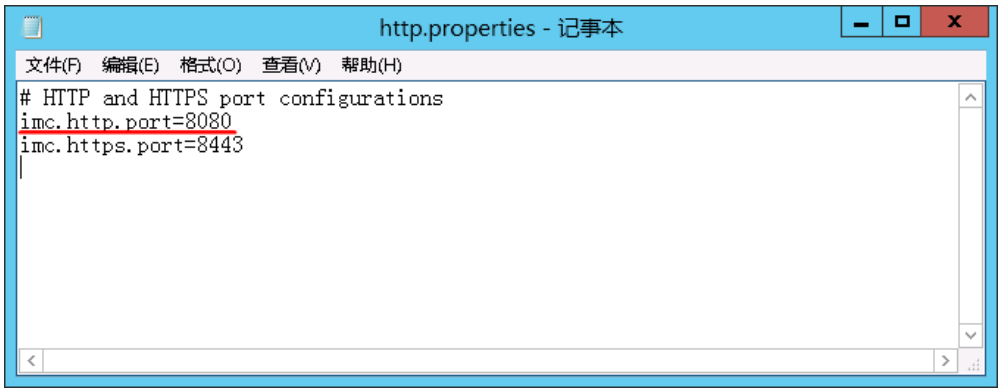
6.35 怎样通过域名方式访问iMC？

解决办法：

(1) 备份“iMC 安装路径\client\conf\http.properties”文件。

(2) 使用文本编辑器打开 iMC 的配置文件“iMC 安装路径\client\conf\http.properties”，如图 6-15 所示，将其中的 HTTP 端口号“8080”修改为“80”。

图6-15 HTTP 端口配置文件



(3) 保存配置文件，重启 jserver 进程。

(4) 在 DNS 服务器上配置域名映射。