
5G 核心网网管操作手册

版本：7.0

目录

目录	2
1 关于本手册	5
1.1 硬件环境	6
1.2 软件环境	7
1.3 软件安装	7
1.4 软件卸载	7
2 系统功能介绍	8
2.1 系统核心网总体架构	8
2.2 功能简介	8
3 操作指南	10
3.1 登录网管	10
3.2 系统状态	10
3.2.1 网元状态	10
3.3 监控	11
3.3.1 活动告警	13
3.3.2 历史告警	14
3.3.3 设置	15
3.4 配置	16
3.4.1 网元管理	16
3.4.2 参数配置	20
3.4.3 备份管理	32
3.4.4 软件管理	34
3.4.5 许可证管理	37
3.5 性能	38
3.5.1 任务管理	38
3.5.2 性能数据	40
3.5.3 性能门限	40

3.5.4	黄金指标.....	41
3.6	跟踪	42
3.6.1	跟踪任务.....	42
3.6.2	信令分析.....	44
3.6.3	信令抓包.....	45
3.7	终端	46
3.7.1	UDM 鉴权用户	47
3.7.2	UDM 签约用户	48
3.7.3	IMS 在线用户	50
3.7.4	UE 在线信息	51
3.7.5	基站信息.....	51
3.7.6	N3IWF 在线用户	52
3.7.7	用户策略控制信息	52
3.8	MML	53
3.8.1	网元操作.....	53
3.8.2	UDM 操作.....	54
3.8.3	OMC 操作.....	56
3.9	日志	58
3.9.1	操作日志.....	58
3.9.2	MML 日志.....	59
3.9.3	安全日志.....	59
3.9.4	告警日志.....	60
3.9.5	告警前转日志	61
3.9.6	网元日志文件	61
3.10	安全	62
3.10.1	用户管理.....	62
3.10.2	在线用户	64
3.10.3	角色管理.....	65

3. 10. 4	部门管理.....	66
3. 10. 5	岗位管理.....	67
3. 11	系统	67
3. 11. 1	调度任务.....	68
3. 11. 2	系统信息.....	74
3. 11. 3	菜单管理.....	76
3. 11. 4	字典管理.....	77
3. 11. 5	参数设置.....	79
3. 11. 6	系统设置.....	80
4	如何获得帮助.....	82
5	本软件系统售后服务的做法与原则	83
6	常见问题解答.....	83
7	版权声明	83

1 关于本手册

本手册是 5G 核心网网管操作手册，主要描述的是系统的软硬件环境，系统功能简介、操作指南和常见问题及解答，手册可提供网管在管理维护、监测状态、网元配置、异常告警、统计报表等相关操作指导。

缩略语和术语表：

缩略语	英文解释	中文解释
OMC	Operations & Maintenance Centre	操作维护中心
NFV	Network Function Virtualization	网络功能虚拟化
VNF	Virtualised Network Function	虚拟网络功能
PNF	Physical Network Function	物理网络功能
GUI	Graphic User Interface	图形用户界面
IMS	IP Multi-media Subsystem	IP 多媒体子系统
CS	Circuit Switched	电路交换
DRA	Diameter Routing Agent	信令网路由代理
VoLTE	Voice over LTE	基于 IMS 的 LTE 语音解决方案
TCE	Trace Collection Entity	跟踪收集实体
EPC	Evolved Packet Core	演进的分组核心网
NB-IOT	Narrow Band Internet of Things	窄带物联网
SMSC	Short Message Service Center	短信中心
MMSC	Multimedia Messaging Service Center	多媒体消息业务中心（彩信中心）
IP-SM-GW	IP-Short Message-Gateway	IP 短信网关
ISMG	Internet Short Message Gateway	互联网短信网关
SCP	Service Control Point	业务控制点
MRFC	Multimedia Resource Function Controller	多媒体资源功能控制器
MRFP	Multimedia Resource Function Processor	多媒体资源功能处理器
AMF	Access and Mobility Management Function	接入和移动管理功能
SMF	Session Management Function	会话管理功能
UPF	User Plane Function	用户面功能
UDM	Unified Data Management	统一数据管理
AUSF	Authentication Server Function	鉴权服务器功能
PCF	Policy Control Function	策略控制功能
NRF	Network Repository Function	网络存储功能
NSSF	Network Slice Selection Function	网络切片选择功能
IWF	Interworking Function	互操作功能
NSSMF	Network Slice Subnet Management Function	网络切片子网管理功能
5GMC	5G Message Center	5G 消息中心

1.1 硬件环境

5GC 及网管支持实体机、本地虚拟化或云化部署，下面为一个基本功能 5GC 核心网（支持多个基站）的硬件规格配置推荐：

网元	内存(G)	硬盘(G)	Vcpu	备注
AMF	4	100	4	
SMF	4	100	4	
AUSF	4	100	4	
UDM	4	100	4	
UPF	8	100	8	
PCF	4	100	4	
NSSF	4	100	4	
NRF	4	100	4	
OMC	8	100	4	

推荐 Dell PowerEdge R640 服务器，配置要求如下：

配置	规格	数量
CPU	24 CPUs x Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz	>=20
内存	2666MT/s RDIMMs	64G
硬盘	10K RPM SAS 12Gbps 512n 2.5 英寸热插拔硬盘	2TB*2
网卡	英特尔以太网 I350 QP 1Gb 网络子卡	1
网口	前置：视频，1×USB2.0 接口，可用的 USB3.0，专用 iDRAC Direct USB 后置：视频，串口，2×USB3.0，专用网络端口	1

1.2 软件环境

系统运行的操作系统软件环境是 VMWare ESXi+Linux 虚拟机。

1.3 软件安装

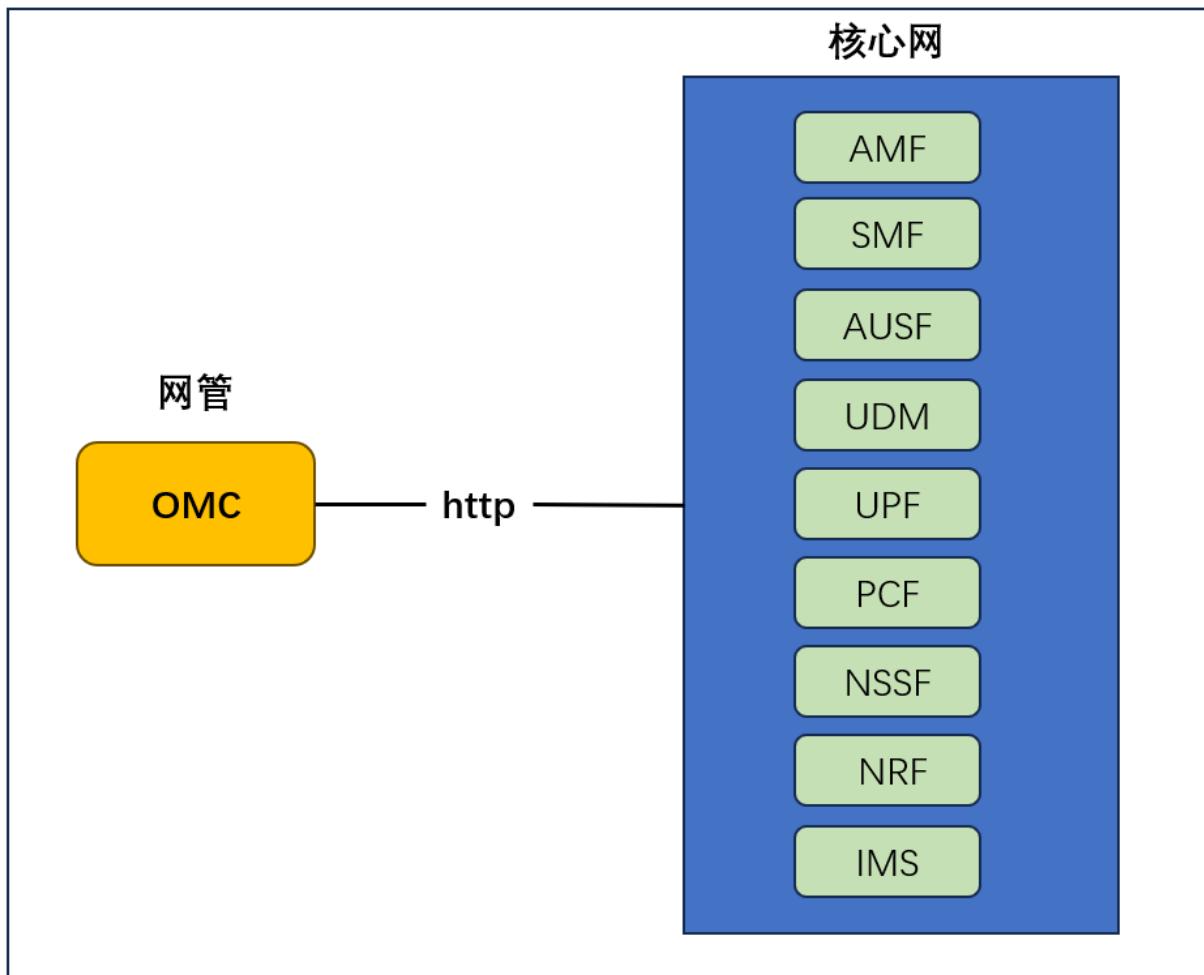
软件是随硬件一起发货的，在出厂前已经安装调试好，因此这里不再详细介绍。

1.4 软件卸载

本系统软硬件是一体的，因此无法单独进行软件卸载操作。

2 系统功能介绍

2.1 系统核心网总体架构



网管与 5GC 网元之间主要通过 http 协议来做信息交互。

2.2 功能简介

1. OMC 网管功能

管理维护、监测状态、网元配置、异常告警、统计报表等

2. AMF 网元功能

完成移动性管理，NAS MM 信令处理、NAS SM 信令路由、安全上下文管理等。

3. AUSF 网元功能

完成用户接入的认证功能。

4. UDM 网元功能

管理和存储签约数据、鉴权数据。

5. SMF 网元功能

完成会话管理、UE IP 地址分配和管理、UPF 选择和控制等。

6. UPF 网元功能

完成不同用户面的处理。

7. PCF 网元功能

支持制定统一的策略框架，提供策略规则。

8. NRF 网元功能

支持服务发现功能，从 NF 实例接收 NF 发现请求，并将发现的 NF 实例(被发现)的信息提供给另一个 NF 实例供策略规则。

9. NSSF 网元功能

支持网络切片选择功能。

10. IMS 网元功能

支持多媒体业务需求。

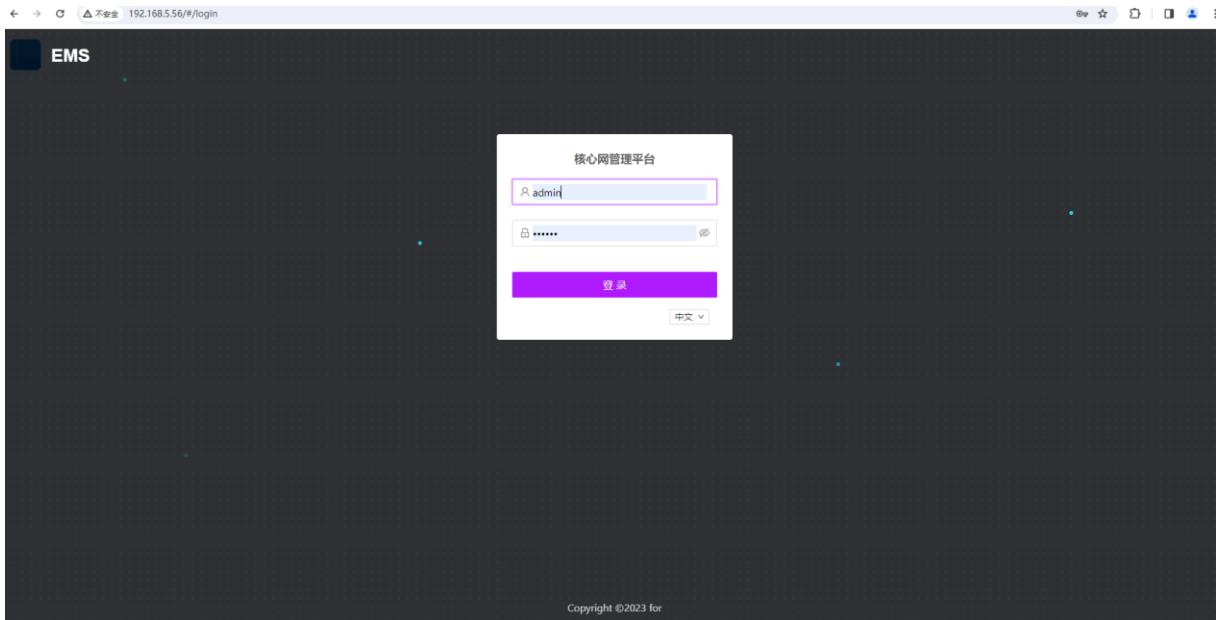
11. MME 网元功能

它是 EPC 控制面中的网元，主要负责信令处理部分。

3 操作指南

3.1 登录网管

在浏览器地址栏输入 `http://<OMC 网管 IP>`, 进入 web 管理界面, 登录界面如下图所示:



- 推荐使用谷歌，火狐浏览器或者 Microsoft Edge

3.2 系统状态

3.2.1 网元状态

- 登陆界面后会自动显示所有网元的系统状态，包含网元名称和 ID，运行状态，更新时间，版本号以及 IP 地址：

对象	网元状态	刷新时间	软件版本	IP地址
OMC_001	正常	2023-12-29 14:42:58	2.2312.9	172.16.14.100
MME_001	正常	2023-12-29 14:42:58	1.2312.10	172.16.14.200
AMF_001	正常	2023-12-29 14:42:58	2.2312.8	172.16.14.120
AUSF_001	正常	2023-12-29 14:42:58	2.2311.7	172.16.14.130
UDM_001	正常	2023-12-29 14:42:58	2.2312.9	172.16.14.140
SMF_001	正常	2023-12-29 14:42:58	2.2312.10	172.16.14.150
PCF_001	正常	2023-12-29 14:42:58	2.2312.9	172.16.14.160
UPF_001	正常	2023-12-29 14:42:58	2.2312.8	172.16.14.190
NRF_001	正常	2023-12-29 14:42:58	2.2312.8	172.16.14.180
IMS_001	正常	2023-12-29 14:42:58	2.2312.8	172.16.14.170
NSSF_001	正常	2023-12-29 14:42:58	2.2312.8	172.16.14.110

- 点击网元状态下的网元的心跳状态后，窗口右边可查看网元的详细信息，如 CPU 和内存使用率，license 序列号和有效期、操作系统、数据库，IP，端口，用户容量等)：

网元状态显示，网元状态会每 10s 进行刷新：

对象	网元状态	刷新时间	版本	IP地址
OMC_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.100
IMS_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.110
AMF_001	正常	2023-11-09 08:57:57	1.6.2	172.16.14.120
AUSF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.130
UDM_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.140
SMF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.150
PCF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.160
UPF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.190
NRF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.180
NSSF_001	正常	2023-11-09 08:57:57	2.2311.7	172.16.14.170

3.3 监控

当系统或网元出现故障时，OMC 会立即检测并上报告警，并根据故障的严重程度产生相应级别的告警，并使用不同的颜色(可定制)和声音进行提醒。故障消除后，相应的告警也会在历史告警中自动清除。

告警管理使运维人员能够对系统或网元上报的告警或事件进行监控和管理。告警管理提供各种监控和处理规则，及时通知运维人员故障。这样可以有效地监控、快速定位和处理网络故障，保证业务正常运行。

告警级别表示故障的严重程度、重要性和紧迫性。能够帮助运维人员快速识别告警的重要性，并采取相应的处理策略，根据需要调整告警的级别。

告警级别：

告警级别	默认颜色	描述	处理策略
严重告警	严重告警	影响业务的告警。必须立即采取纠正措施。	必须立即排除故障。否则可能导致业务中断或系统崩溃。
主要告警	主要告警	影响业务的告警。如果不及时排除故障，可能会造成严重的后果。	重要告警需要及时处理。否则会影响重要业务。
次要告警	次要告警	对业务影响不大。需要采取纠正措施以防止严重故障的发生。	检查告警产生的原因，排除故障。
警告告警	事件告警	检测到潜在的或即将发生的影响业务的故障，但对业务没有影响。	根据网络和网元的运行状态对告警进行处理。

告警状态：

状态名称	告警状态	描述
确认状态	已确认和未确认	初始确认状态为“未确认”。当用户查看到未确认告警并计划处理该告警时，可以确认该告警。确认告警后，告警状态变为“已确认”。当告警暂时不需要处理，但需要引起注意或其他用户处理时，可以取消确认告警。当告警被反确认时，告警状态恢复为“未确认”。用户还可以配置自动确认规则，自动确认告警。
清除状态	已清除和未清除	初始清除状态为“未清除”。故障修复后，告警自动上报到“告警管理”中，清除状态变为“已清除”。部分告警无法自动上报清除通知。当相应的故障排除后，需要手动清除这些告警。已清除的告警背景颜色为绿色。

事件告警：

事件	描述
通信告警	通信系统的故障，如网线断开、网络设备故障等。
设备告警	设备上的故障导致的告警
处理错误	处理过程中出现的错误或异常，如数据库异常、网元异常退出等
环境告警	机房环境故障，如电源故障、CPU 温度过高等。

服务质量

通常是指对核心网的业务质量进行监控和管理时出现的异常情况的告警。

3.3.1 活动告警

活动告警包括未清除未确认的告警、已确认未清除的告警和已确认已清除的告警。通过监控当前告警，可以及时发现故障，进行相应的处理，并及时通知运维人员。

用户可以执行告警搜索、过滤、自动确认、导出和查看告警详细信息等功能。

当前活动告警列表：

告警唯一标识	告警网元标识	告警网元名称	告警设备类型	告警级别	告警编号	告警名称	告警产生时间	告警类型	虚拟化标识	告警清除用户	操作
HXEMSPM10201	4400HX1UDM001	UDM_001	UDM	Minor	10201	Performance data report timed out	2023-11-07 03:14:08	设备告警	PNF		① ②
HXEMSPM10201	4400HX1AMF002	AMF_002	AMF	Minor	10201	Performance data report timed out	2023-11-06 01:48:16	设备告警	PNF		① ②
300011699172170347	4400HX1SMF001	SMF_001	SMF	Critical	30001	N4 Broken	2023-11-05 08:16:10	通信告警	PNF		① ②
300071698991026224	4400HX1SMF001	SMF_001	SMF	Major	30007	DSTNF-DISCONNECTED	2023-11-03 14:32:36	通信告警	PNF		① ②
300011698991025752	4400HX1SMF001	SMF_001	SMF	Critical	30001	N4 Broken	2023-11-03 13:57:05	通信告警	PNF		① ②

窗口右上角同步显示当前活动告警数量；每个告警右侧有详细告警信息，及相关告警的帮助文档：

The screenshot displays two windows of the core network management system:

- Left Window (告警历史 - History Alert):** Shows a detailed alert record for '告警唯一标识: HXEMSPM10201' (告警唯一标识: HXEMSPM10201). It includes fields like告警设备类型: 告警告警设备类型, 告警网元名称: 4400HX1UDM001, 告警产生时间: 2023-11-07 05:14:08, and告警级别: 严重告警.
- Right Window (告警活动 - Alert Activity):** Shows a list of active alerts. One specific alert for '设备告警' (Device Alert) is highlighted with a red box. The alert details are: 告警唯一标识: HXEMSPM10201, 告警网元名称: 4400HX1UDM001, 告警产生时间: 2023-11-07 05:14:08, and告警级别: 严重告警.

3.3.2 历史告警

已确认已清除告警和未确认已清除告警均为历史告警。通过分析历史告警，可以优化系统性能。如果设置了当前告警的生命周期，已确认已清除的告警会在“当前告警”页面中显示一段时间。生命周期结束后，确认清除的告警将被移至历史告警列表中。

告警唯一标识	告警网元名称	告警设备类型	告警级别	告警编号	告警名称	告警产生时间	告警类型	虚拟化标识	告警清除用户	告警清除类型	操作
HXEMSSM10000 4400HX1NRF001	NRF_001	NRF	Major	10000	The system state is abnormal	2023-11-08 02:31:29	设备告警	PNF		自动清除	
HXEMSSM10000 4400HX1NSSF001	NSSF_001	NSSF	Major	10000	The system state is abnormal	2023-11-08 02:31:39	设备告警	PNF		自动清除	
HXEMSSM10000 4400HX1IMS001	IMS_001	IMS	Major	10000	The system state is abnormal	2023-11-08 09:41:15	设备告警	PNF		自动清除	
HXEMSSM10000 4400HX1AMF001	AMF_001	AMF	Major	10000	The system state is abnormal	2023-11-08 09:41:15	设备告警	PNF		自动清除	
HXEMSSM10000 4400HX1AUSF001	AUSF_001	AUSF	Major	10000	The system state is abnormal	2023-11-08 09:41:15	设备告警	PNF		自动清除	
HXFMSSM10000 4400HX1UDM001	UDM_001	UDM	Major	10000	The system state	2023-11-08	设备告警	PNF		自动清除	

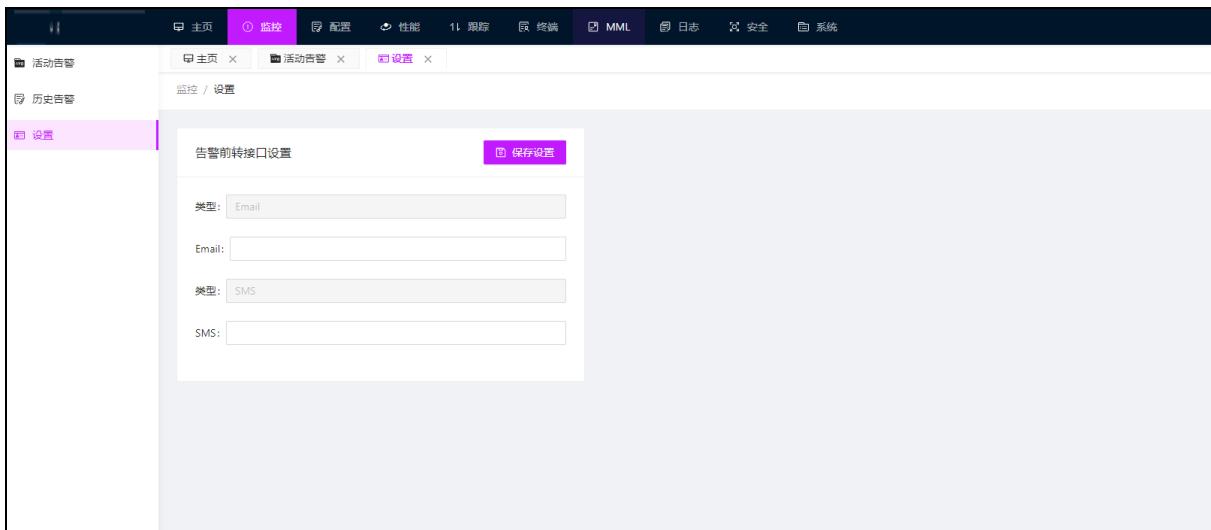
3.3.3 设置

告警转发是一种对核心网进行监控和管理的技术和机制。核心网络设备和系统需要始终保持正常运行，提供稳定、高效的服务。但是，由于各种原因，如设备故障、网络拥塞、配置错误等，核心网可能会出现异常或故障。

核心网告警转发的目的是为了及时发现并处理核心网中的故障或异常，保证网络的可靠性和业务的连续性。当核心网中的设备或系统出现故障或异常时，设备或系统会产生告警。通过对告警系统的监控和检测，可以自动将告警信息转发给网络操作员或具有网络维护职责的技术人员，以便他们及时采取措施排除故障。

核心网告警转发是一项关键技术。通过将告警信息及时转发到核心网，可以提高故障检测和处理效率，保证核心网的稳定运行和服务质量。它对于网络运营商的正常运营和用户的良好体验至关重要。

操作员可以配置告警转发接口设置，在设置告警之前重定向到目标邮件。如图所示，填写告警转发邮箱地址。



3.4 配置

这部分介绍了常用的配置操作，以及如何查看网元的配置信息。包括网元管理、参数管理、备份管理、软件管理和 License 管理。

3.4.1 网元管理

网元管理（Network Element Management）是核心网网管操作系统的关键组成部分。它致力于监控和操作网络中的各个网元，如 AMF、SMF、UDM、PCF、AUSF、UPF、IMS、MME、NRF、NSMF 等。通过网元管理系统，操作员可以确保网络的持续、可靠运行。网元管理包含了网元的生命周期全部阶段，包括配置、监控、维护和优化。

- **新增、删除和修改网元：**网管系统提供了一个直观的用户界面，让操作员能够添加新的网元，以适应网络扩展的要求，或者在必要时移除旧网元。用户可以在图形界面上通过拖放组件来架构网络，或使用自动化脚本来处理网元的批量操作。
- **停止、启动和重启操作：**OSS 提供了停止、启动和重启网络设备的控制。这些操作通常用于执行常规维护或应用新配置。网管系统通常包含安全协议和流程，以确保操作的顺利进行，避免产生不必要的网络中断。
- **导入和导出网元配置：**网络管理员可以在需要时导出关键配置文件进行备份，以便在丢失数据或出现故障时迅速恢复。同样，新的配置文件可以被导入到网元中，以快速更新和部署新的网络设定。导入导出操作通常支持标准化格式，比如 XML 或 JSON，方便跨平台的配置管理。

-
- **修改网元细节：**从内部标识、资源标识到厂商和位置信息，网管系统使得修改和更新这些细节信息变得很简单。更改网元的方位、IP、端口等可以直接通过 UI 来完成，或者通过 API 进行自动化。更深入地，还可以涉及到参数的调整，以优化网络的性能和容量。

管理员也需要留心如网元名称、物理地址和网络标识等信息的更改，以确保网络地图保持最新。同时可以为网元设置服务省份等逻辑分类，从而实现更细致的网络管理。

此外，随着网络功能虚拟化（NFV）的发展，管理系统可以区分物理网络功能（PNF）和虚拟网络功能（VNF），并分别进行管理。这为网络操作提供了额外的灵活性，因为 VNF 可以快速部署和伸缩，以适应不断变化的流量需求。

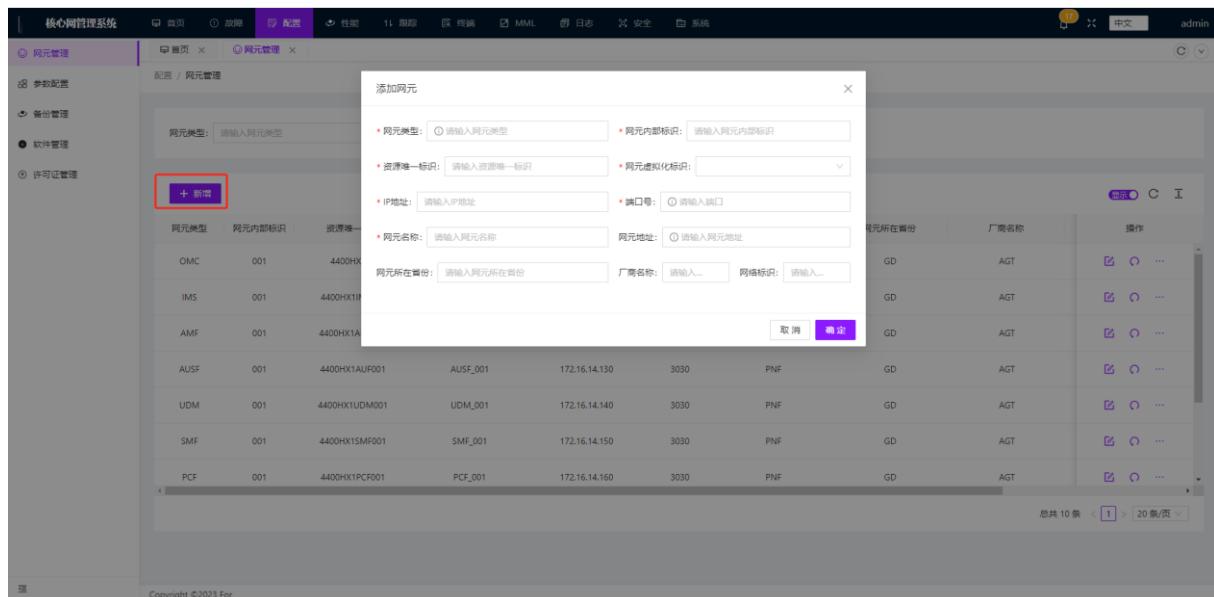
总之，网元管理是 5G 核心网网管 OS 配置管理不可或缺的一部分，它确保了网络设施能够按照预定的性能和效率运行。

操作部分如下：

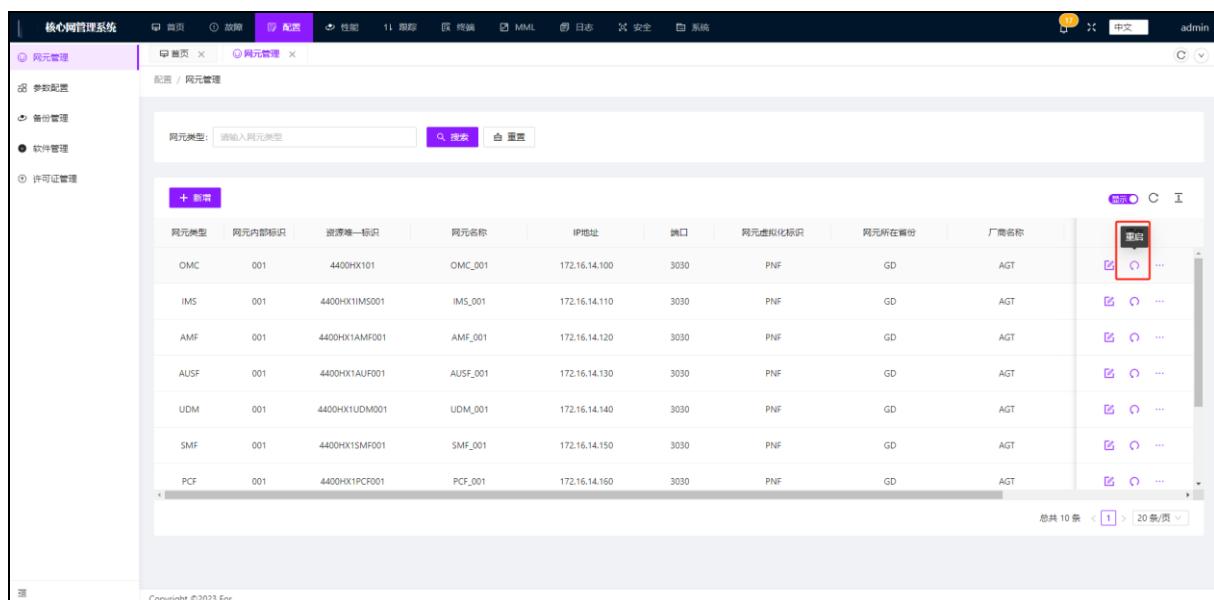
单击  **+ Add** 添加网元网元参数(以下参数需与网元配置一致)：

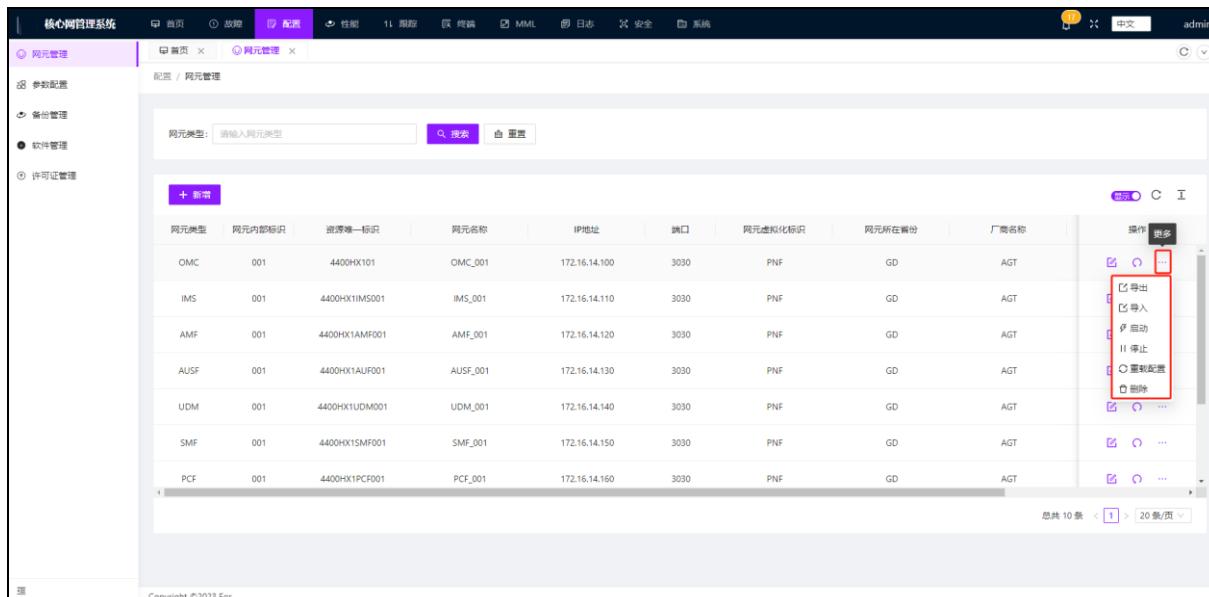
- 网元类型
- 网元内部标识
- 资源唯一标识
- 网元虚拟化标识（PNF）
- 端口号（一般设置为 3030）
- IP 地址
- 网元名称

新增网元时上述为必填项



网元管理每个网元右侧配置有网元重启、启动、停止、重载配置、删除功能，以及对网元配置的导入导出功能

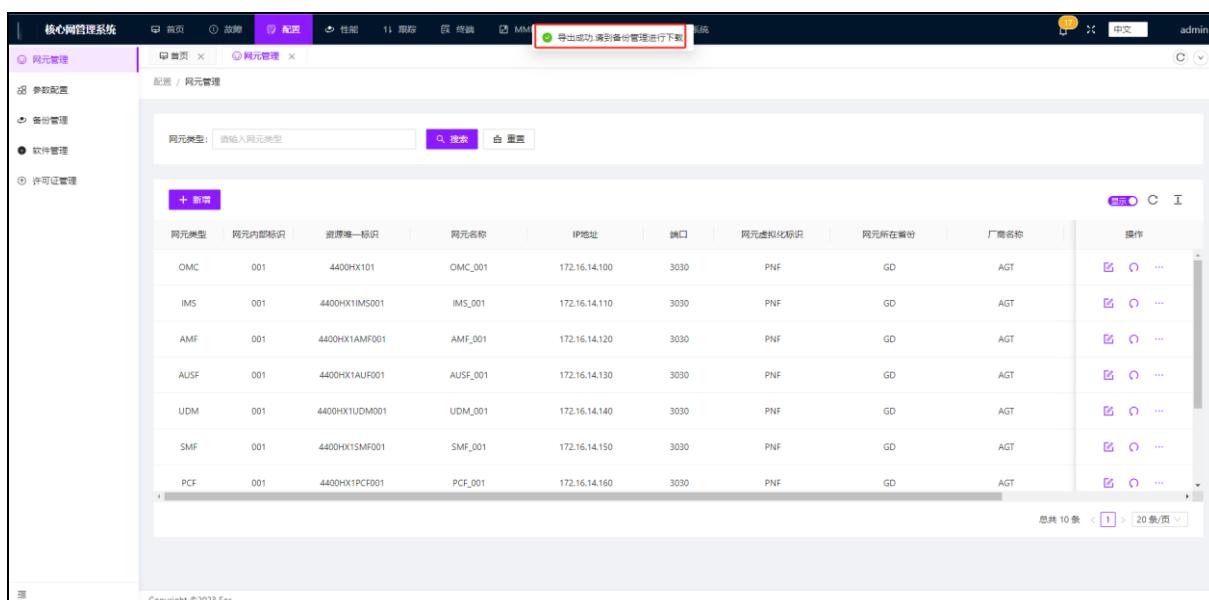




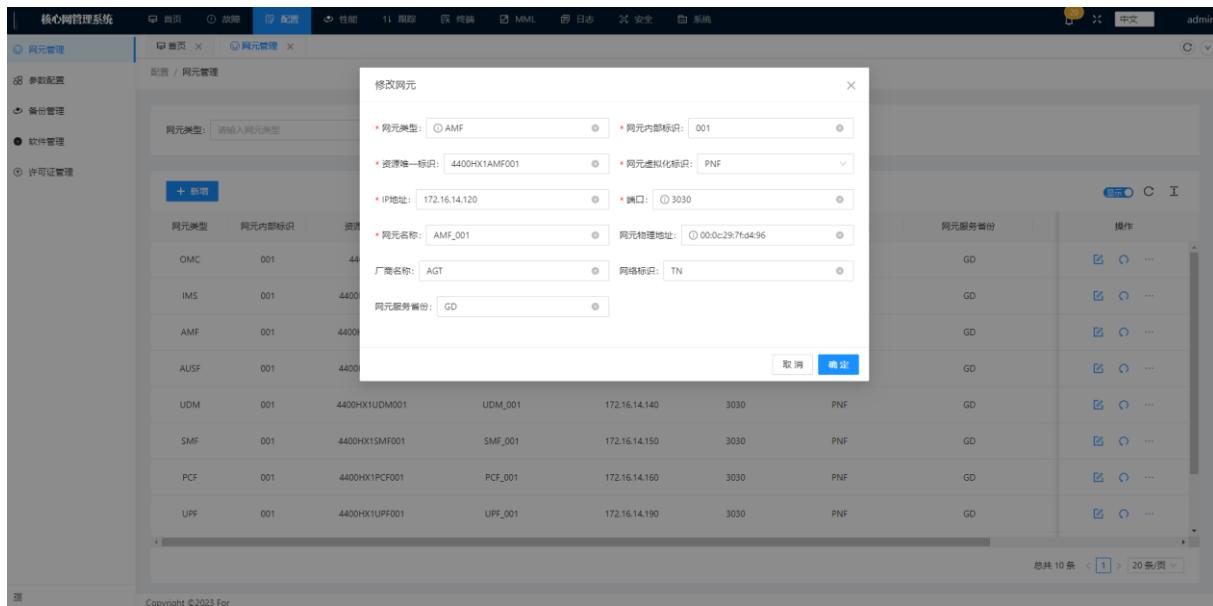
导出：网元配置导出后会，可以在备份管理中查询到

导入：单击“导入”，导入网元配置。文件来源选择“服务器文件”，可以将之前的备份文件导入服务器。选择“本地文件”可以导入本地配置文件。

操作人员可以点击 more 中的“开始”按钮开始运行网元，点击“停止”按钮停止运行网元，点击“重新加载”按钮重置网元参数，点击“删除”按钮删除网元。



网元右侧可点击修改标识对网元进行修改



3.4.2 参数配置

参数配置是调优 5G 核心网性能和服务的关键环节

- 功能概述:** 参数配置允许网络管理员细致调节核心网各个网元的运行参数。它涉及到网络的方方面面，从数据传输速率到信号处理策略，从安全协议到接入控制列表（ACLs）。参数配置的灵活性和原子性是衡量 5G 网管操作系统成熟度的关键指标。
- 新增、删除、修改网元参数:** 在网络运营中，有时需要引入新的参数以支持新技术或服务策略；有时需要删除旧参数，以优化网络性能或是符合新的规范；有时则需要修改现有参数，以适应网络质量或客户需求的变化。这些操作在 5G 核心网的网管系统中可以通过图形用户界面（GUI）手动完成，也可以通过命令行界面（CLI）或 API 实现自动化。参数的变动常因实时监测到的网络状态而触发，这要求网管系统有高度的实时性和灵敏度。
- 配置快速生效:** 在传统的网络系统中，参数变更往往需要重启网元，才能使配置生效。这在 5G 环境下不再是必需的。现代网管系统能够实现热更改，让参数配置的更改能够在无需重启的情况下立即生效。这种即时生效的功能对于保持网络的最高时效性至关重要，并能保证服务不会因为配置更改而中断。
- 参数配置的挑战与自动化:** 在高度复杂的 5G 核心网中，手动进行参数调整可能不再现实，因此更多依赖于智能化工具和自动化策略。预定义的策略和机器学习模型可以根据实时数据流和网络性能指标实现自动调优。自动化的参数配置不仅提高了效率，还提

高了准确性，减少了由于配置失误可能导致的网络故障。同时，自动化策略必须包括相应的安全机制，以防止误配置和网络攻击。

5、参数审计和合规性：为了确保网络遵守规定的政策和标准，参数配置的一个重要方面是审计和合规性检查。网管系统通常包括审计日志和合规性报告的功能，确保所有配置更改都被记录并且可以追溯。这些记录在解决网络问题或执行安全审计时至关重要。

参数配置该功能对应每个网元的配置参数，该工作决定了 5G 核心网的运转质量和效率，是网络健康和功能完善的关键。

下面是常见的网元配置修改示例，当需要修改时，将鼠标放在出现修改标记的修改值上，点击即可修改，或者某些地方右侧会出现修改标记，点击即可修改。

选择相应网元获取配置信息或修改

3.4.2.1 AMF

1、System Config: 在 AMF 的 System Config 中，主要是修改连接 AUSF、UDM 和 SMF 的 AUSF URI 和 UDM URI 以及 SMF URI，修改接入 AMF 的默认 DNN，还修改了一些定时器，如 3512。

The screenshot shows the EMS (Network Management System) interface. The top navigation bar includes tabs for '主页' (Home), '监控' (Monitoring), '配置' (Configuration), '性能' (Performance), '跟踪' (Tracing), '终端' (Terminals), 'MML' (MML), '日志' (Logs), '安全' (Security), and '系统' (System). The current view is under the '配置' tab, specifically in the '参数配置' (Parameter Configuration) section. On the left, there's a sidebar with options like '网元管理' (Equipment Management), '参数配置' (Parameter Configuration, which is selected and highlighted in purple), '备份管理' (Backup Management), '软件管理' (Software Management), and '许可证管理' (License Management). The main content area has a '配置导航' (Configuration Navigation) panel on the left showing sections like 'AMF / AMF_001', 'System Config', 'TNL Association List', 'GUAMI List', 'TAI List', and 'Slice List'. The right side displays the 'System Config' table with various parameters. Two specific rows are highlighted with red boxes: 'AUSF URI' (Value: http://172.16.14.130:8080) and 'Default DNN' (Value: cmnet). Other visible parameters include 'AMF Name' (AMF), 'Ciphering Algorithm' (NEAO), 'DNN Correction Enabled' (false), 'Integrity Algorithm' (NIA2), 'LMF URI' (http://172.16.14.200:8080), 'NEF URI' (http://172.16.14.210:8080), 'NRF Enabled' (false), 'NRF URI' (http://172.16.14.180:8080), 'PCF URI' (http://172.16.14.160:8080), and 'Relative Capacity' (255).

EMS

配置 / 参数配置

AMF / AMF_001

System Config

SBI Server IP	172.16.14.120
SBI Server Port	8080
SMF URI	http://172.16.14.150:8080
T3502	720
T3512	3300
T3513	2
T3522	2
T3550	2
T3555	2
T3560	2
T3565	2
T3570	2
UDM URI	http://172.16.14.140:8080

2、TNL Association List: 在 TNL Association List, 可以修改与 Gnb 对接的 N2 IP 和 NGAP SCTP 端口。

配置 / 参数配置

AMF / AMF_001

TNL Association List

Index	NGAP IP	NGAP SCTP Port	Weight	操作
0	192.168.14.70	38412	255	<input checked="" type="checkbox"/> <input type="button"/>

3、GUAMI List: 可以对 GUAMI List 进行修改、添加、删除。当用户设备尝试接入或进行移动性管理时，网络会根据 GUAMI 列表中的 AMF ID 来确定所需的 AMF，并将相关控制指令路由到相应的 AMF。

Index	PLMN ID	Region ID	Set ID	Pointer	操作
0	46000	1	1	1	

4、TAI List: 在 TAI List, 以修改、增加和删除 PLMN 对应的 TAC, PLMN 和 TAC 对应基站。如果填充错误, 可能会导致 AMF 与基站的连接中断。

Index	PLMN ID	TAC	操作
0	46000	4388	
1	46000	1	

5、Slice List: 在 Slice List, 可以修改 PLMN 对应的切片信息, 即 AMF 允许访问的切片

Index	PLMN ID	SST	SD	操作
0	46000	1	000001	
1	45402	1	000001	

3.4.2.2 AUSF

1、System: 在这个配置中可以修改与 AUSF 相关联的 UDM URI:

配置 / 参数配置

System	
Key	Value
Group ID	ausfGroup001
NRF URI	http://172.16.14.180:8080
Scheme	HTTP
Service IP	172.16.14.130
Service Port	8080
UDM URI	http://172.16.14.140:8080

3.4.2.3 UDM

1、**System**: 此配置中主要修改与 UDM 相关联的 AUSF IP。

配置 / 参数配置

System	
Key	Value
AUSF IP	172.16.14.130
Capacity	4096
FQDN	udm.agt.com
GPSI Ranges	msisdn-69072000~msisdn-69072099
Group ID	0
NRF URI	http://172.16.14.180:8080
Priority	1

2、**Subs SMF Selection**: 此配置中主要是修改会话管理中切片信息对应的 DNN。

Index	Name	SNSSAI	DNN List	操作
1	def_snsai	1-000001	展开 (cmnet,ims)	

Index	DNN	Default DNN Indicator	LBO Roaming Algo	操作
1	cmnet	true	false	
2	ims	true	false	

3、DNN Conf: 用户可以对终端接入的 DNN 进行添加、删除、修改等操作。用户可以根据需要添加不同的 DNN，修改不同 DNN 的参数配置，如“Default SSC Mode”、“Subscribed Session AMBR Uplink”等

Name	Default PDU Session Type	Allowed PDU Session Types	5QI	Priority Level	Default	操作
cmnet	IPv4	IPv4 & IPv4v6	9	90	SSC Mode	
ims	IPv4	IPv4 & IPv4v6	5	10	SSC Mode	

4、Application Server: 此处操作员主要是添加或修改与 IMS 数据对应的 mmTel_as 数据，修改服务器名称中的 sip IP 地址和 Diameter address。

AS Name	Default Handling	Server Name	Diameter Address	Rep Data Size Limit	操作
mmtel_as	Session Continued	sip:192.168.14.74:7060	mmtel.ims.mnc000.mcc460.3gppnetwork.org	0	
sms_as	Session Continued	sip:10.10.1.123:5060	sms.ims.mnc000.mcc460.3gppnetwork.org	0	

5、SCSCF Set: 这里主要是修改与 IMS 的 sip 数据对应的 scscf 的参数。

Index	Name	Priority	Server Name	操作
1	def_scscf	1	sip:scscf.ims.mnc000.mcc460.3gpnetwork.org:6060	

6、S6a Server: 此处主要修改与 MME 对接的 S6a 接口的参数，包括开关，host、Link Type，及 Realm。

Key	Value
Address	172.16.14.140:3868
Enable	true
Host	hss.ims.mnc000.mcc460.3gppnetwork.org
Link Type	SCTP
Realm	ims.mnc000.mcc460.3gppnetwork.org

7、Cx Server: 操作人员主要打开 IMS 对应的 Cx 端口，修改对应的 host。

Key	Value
Address	172.16.14.140:3868
Enable	true
Host	hss ims.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	ims.mnc000.mcc460.3gppnetwork.org

3.4.3.4 SMF

1、SMF System: 此处配置主要修改与 SMF 对应的 AMF URI 及 UDM URI。

Key	Value
AMF URI	172.16.14.120:8080
N4 IPv4	172.16.14.150
N4 IPv6	
N4U IPv4	

配置 / 参数配置

配置导航

SMF / SMF_001

SMF System

Primary DNS IPv4	114.114.114.114
Primary DNS IPv6	
Primary PCSCF IPv4	172.16.14.110
Primary PCSCF IPv6	
SBI IP	172.16.14.150
SBI Port	8080
SBI Scheme	http
Secondary DNS IPv4	223.5.5.5
Secondary DNS IPv6	
Secondary PCSCF IPv4	
Secondary PCSCF IPv6	
UDM URI	172.16.14.140:8080
UE MTU	1400

2、UPF Config: 用户可以在“**UPF Config**”中配置 SMF 对应的 UPF IP、配置给终端分配的 IP 地址池、配置静态 IP 地址。

配置 / 参数配置

配置导航

SMF / SMF_001

UPF Config

UPF ID	Address	IPv4 Pools	IPv6 Pools	Static IPv4 Enable	Static IPv4 Start	操作
upf-1	172.16.14.190:8805	10.10.31.0/24		false	10.2.1.200	

3、DNN Select UPF: 此处可以根据 DNN 配置不同的 UPF.

配置 / 参数配置

配置导航

SMF / SMF_001

DNN Select UPF

Index	DNN	UPF ID	操作
0	cmnnet	upf-1	
1	ims	upf-1	

3.4.4.5 PCF

1、Session Rules: 操作者可以配置不同的会话规则，修改相应规则的 5QI 和 AMBR 下行链路参数。

The screenshot shows the 'Session Rules' configuration page. On the left, a navigation pane lists various PCF components: System, Service Area Restriction, PCC Rules, Session Rules (which is selected), Gx Server, Rx Server, Flow Template, QoS Template, Usage Monitoring Template, Traffic Control Template, and Header Enrich Template. The main panel displays a table titled 'Session Rules' with two entries:

Rule ID	Activate	5QI	5QI Priority Level	Flow Usage	操作
internet	true	9	0	General	
ims_sig	true	5	0	IMS-Signalling	

2、Gx Server: 操作员可以配置 Gx 服务器参数，包括 Gx 开关、host 等

The screenshot shows the 'Gx Server' configuration page. The left navigation pane includes 'Gx Server' under the 'PCF / PCF_001' section. The main panel displays a table with the following parameters:

Key	Value
Address	172.16.14.160:3868
Enable	true
Host	pcrf.epc.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	epc.mnc000.mcc460.3gppnetwork.org

3、Rx Server: 操作者可以配置 Rx Server 相关的参数，包括开关、host 等。

The screenshot shows the 'Rx Server' configuration page. The left navigation pane includes 'Rx Server' under the 'PCF / PCF_001' section. The main panel displays a table with the following parameters:

Key	Value
Address	172.16.14.160:3867
Enable	true
Host	pcrf.epc.mnc000.mcc460.3gppnetwork.org
Link Type	TCP
Realm	epc.mnc000.mcc460.3gppnetwork.org

3.4.4.6 UPF

1、**OMC**: 操作者可以配置与 OMC 相关的参数，包括 OMC 的 IP、端口等。

The screenshot shows the 'OMC' configuration page. On the left, there is a navigation tree under 'UPF / UPF_001' with the 'OMC' option selected. The main area displays a table of OMC parameters:

Key	Value
Enabled	true
HTTP Scheme	http
IP Type	ipv4
KPI Statistic Interval	1
Local IPv4	172.16.14.190
Local IPv6	
Local Server Port	3030
NE Id	upf1
NE Name	upf1
Object Name	upf1
OMC IPv4	172.16.14.100
OMC IPv6	

2、**Data Interface List**: 操作者可以配置 N3/N6/N9/N19 的参数,包括 IP, Driver Type, MAC Address, Interface PCI, Gateway IPv4 等。

The screenshot shows the 'Data Interface List' configuration page. On the left, there is a navigation tree under 'UPF / UPF_001' with the 'Data Interface List' option selected. The main area displays a table of data interface configurations:

Interface Type	Interface ID	Driver Type	IP Type	IPv4 Address List	操作
N3	1	vmxnet3	ipv4	[展开]	[编辑] [删除]
+ 新增 IPv4 Address List [列设置]					
Index	IPv4	IPv4 Mask	操作		
1	192.168.14.72	255.255.240.0	[编辑] [删除]		
N6	1	vmxnet3	ipv4	[展开]	[编辑] [删除]
N9	1		ipv4	[展开]	[编辑] [删除]
N19	1		ipv4	[展开]	[编辑] [删除]

3.4.4.7 MME

1、**System Config**: 此处操作者主要可以配置对应 S10, S11, S1, SGs 的 IP 及端口, 同时可

以配置 VoLTE 开关。

The screenshot shows the 'Parameter Configuration' section under 'MME / MME'. On the left, there is a navigation tree with 'System Config' selected. The main area displays a table of system configuration parameters:

Key	Value
CSFB Enabled	false
S10 MME IP	172.16.14.201
S10 MME Port	2123
S11 MME IP	172.16.14.200
S11 MME Port	2123
S1 MME IP	192.168.14.75
S1 MME Port	36412
SGs MME IP	172.16.14.200
SGs MME Port	29118
VoLTE Enabled	true

2、Gummei List: 此处主要配置 GUMMEI List 的参数，包括 PLMN 和 Group ID.

The screenshot shows the 'Parameter Configuration' section under 'MME / MME'. On the left, 'Gummei List' is selected in the navigation tree. The main area displays a table of GUMMEI List entries:

Index	PLMN ID	Group ID	Code	操作
0	46000	4	1	

3、TAI List: 此处操作者主要配置与接入核心网相关的 TAC 及 PLMN 的参数。

The screenshot shows the 'Parameter Configuration' section under 'MME / MME'. On the left, 'TAI List' is selected in the navigation tree. The main area displays a table of TAI List entries:

Index	PLMN ID	TAC	操作
0	46000	4388	

4、HSS List: 此处主要配置与 MME 相匹配的 HSS 的 Hostname 及端口。

Index	IMSI Prefix	HSS Hostname	Protocol	HSS Port	操作
0	46000	hssims.mnc000.mcc460.3g ppnetwork.org	SCTP	3868	

5、SGW List: 此处主要配置与 MME 相关的 SGW 的配置，包括 SGW 的 IP、TAC、PLMN 等。

Index	PLMN ID	TAC	SGW IP	操作
0	55201	300	172.16.14.150	
1	46000	4388	172.16.14.150	

6、AMF List: 这里操作者主要是配置与 MME 互操作的 AMF 信息，包括 AMF PLMN、TAC 等。

Index	PLMN ID	TAC	Region ID	Set ID	操作
0	46000	4388	1	1	

3. 4. 3 备份管理

备份管理是任何 IT 基础设施管理的核心组件，特别是在核心网中，它尤其重要因为它保证了在数据丢失、故障或其他灾难性事件发生时，服务可以快速恢复。以下是备份管理的细节介绍：

1、备份策略的重要性

一个有效的备份策略需要综合考虑数据的价值、恢复时间目标（RTO）、数据恢复点目标（RPO）和业务连续性要求。策略制定时，也需要权衡备份频率和成本。例如，更频繁的备份可以减少数据丢失，但同时也会增加存储和资源的花费。

2、完整备份与增量备份

完整备份意味着复制所有选定的数据集，虽然这会消耗较多时间和存储资源，但恢复起来较为简单。而增量备份只复制上一次备份以后有变化的数据。这节省了存储空间和备份时间，但恢复过程可能更复杂且耗时，因为需要所有之前的增量备份协同工作。

3、自动备份

现代的 5G 网管系统可以自动化执行备份任务，以减少人为错误并确保定期备份。这可能包括每日或每周的任务安排，以及根据特定事件或条件触发的备份，例如在进行大规模更新之前。现在设定为每日 0:30 分对所有网元进行配置备份。

4、容错能力

一个好的备份管理系统应该具有容错能力，以确保即使在备份过程中出现部分失败，系统也能恢复并尽可能完成备份任务。它可以通过校验和或其它完整性检查来验证备份文件的准确性。

5、备份存储

备份数据的存储同样重要。备份应存储在安全可靠的位置，且最好与生产环境地理位置分离，以保护数据不受物理灾害的影响。通常会使用本地存储、网络存储或云存储解决方案，有时甚至会将它们结合使用以提供额外的安全性。

6、恢复过程

准备好的备份策略还需要能够指导高效的数据恢复过程。这意味着出现故障时，必须能够迅速定位到恰当的备份集，并按照预定程序恢复系统运行。此外，定期的恢复演练是非常有价值的，因为它可以验证备份的有效性并确保团队熟悉恢复流程。

备份管理确保 5G 网络服务的可靠性和数据的安全性，是提供连续业务服务的关键策略。

目前网元的备份管理通常包括系统自动备份和手动备份：

手动备份: 手动备份主要是在网元管理中对网元导出操作后得到的备份文件。导出的配置文件将显示在备份管理中。

自动备份: 在自动备份中，系统实现对网元备份的自动备份和调度管理。可以在系统配置的调度任务下配置备份任务。目前，每个网元的配置文件每天 00:30 备份一次。

The top screenshot shows the 'Backup Management' page of the network management system. It lists 225 backup files across various network elements (AMF, UPF, NRF, AMF, NSSF, PCF) with their respective file names, creation times, and operation icons. The bottom screenshot shows the 'Scheduling Tasks' page, where a task named 'Network Element Configuration Automatic Backup' is listed with a cron expression of '0 30 * * ?'. This task is highlighted with a red border.

3.4.4 软件管理

软件管理是指管理和升级网络中各个网元的软件，并确保网络的稳定性和功能升级的顺利进行。在网络中，网元升级是非常重要的，可以带来新的功能和性能改进，同时也可修复已知的问题和漏洞。

软件版本管理: 对各网元的软件版本进行管理。这包括记录和管理每个网元上运行的当前软件版本，以及新版本的发布和升级计划。

软件升级计划:根据提供的软件更新和升级，制定合理的升级计划。您可以先将需要升级的网元上传到服务器，然后根据需要进行升级。

回退和降级管理:当软件升级过程中出现问题或意外情况时，需要设置回退和降级策略，保证对应的网元可以回退。

软件升级流程:

- **上传软件:** 将新版本的网元软件上传到核心网管理系统的软件库中。
- **下发软件:** 在管理系统中对目标网元选择升级操作，这通常通过点击一个“下发”按钮来开始。
- **激活软件:** 软件下发后，若要完成升级过程，往往需要激活软件。这可以通过点击“激活”来实现，这一步骤通常会触发网元重启来使用新的软件版本。

软件回退流程:

如果升级后的软件有问题或者不满足需求，可以通过以下步骤回退到之前版本的软件：

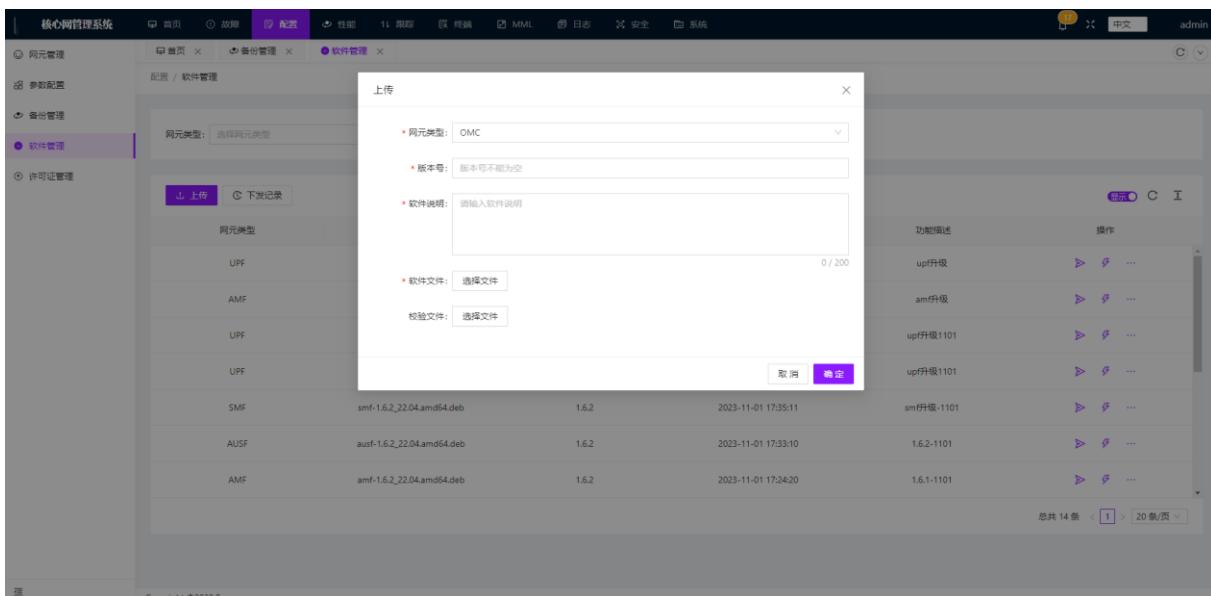
- **点击回退:** 选择需要回退软件的网元，执行回退操作。网络运维人员可以通过管理系统界面上的“回退”按钮来操作。

在这整个过程中，管理员可以通过管理系统来监控和记录每次的软件升级或回退操作：

- **下发记录:** 软件升级或回退的操作记录通常会被系统记录下来，以便在必要时进行审计和复查。管理员可以在“下发记录”部分查看到所有已经执行的操作记录，包括时间、操作人员及结果等详细信息。

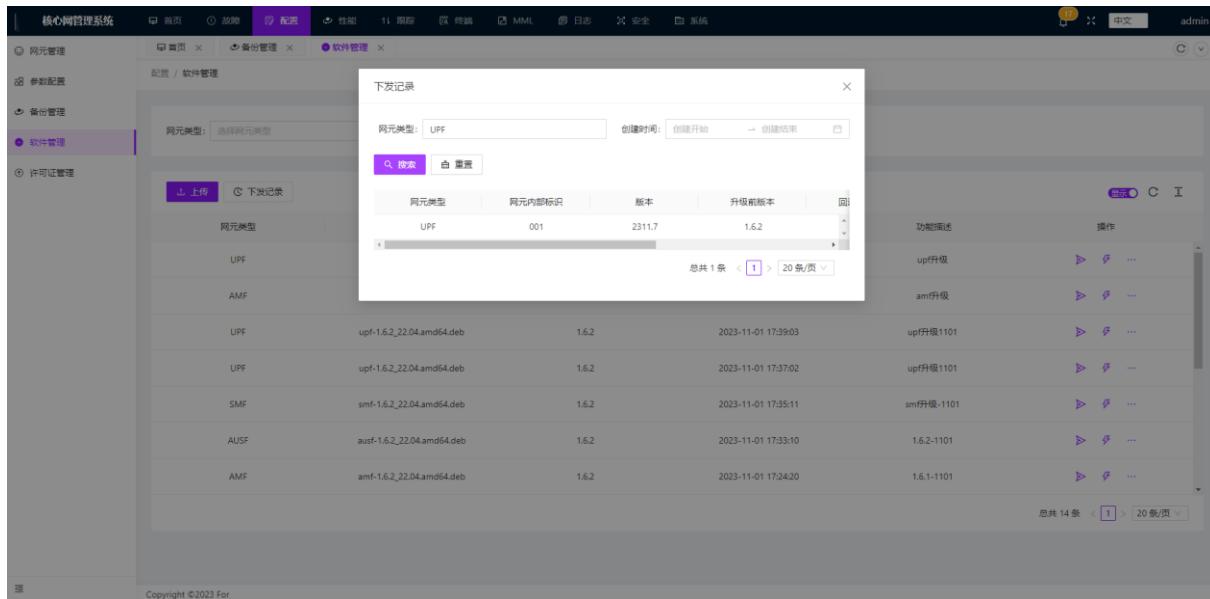
这种软件管理流程是核心网运维中保证网元软件为最新版本和最佳状态运行的重要环节。通过软件管理界面，运维团队可以轻松对网元软件进行升级和维护，确保网络的稳定与安全

操作：上传->下发->激活/回退



配置 / 软件管理					
网元类型	文件名	版本号	上传时间	功能描述	操作
UPF	upf-r2.2311.7_u22.deb	2311.7	2023-11-08 08:49:48	upf升级	...
AMF	amf-r2.2311.7_u22.deb	1.6.2	2023-11-08 08:47:53	am升级	...
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:39:03	upf升级1101	...
UPF	upf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:37:02	upf升级1101	...
SMF	smf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:35:11	smf升级-1101	...
AUSF	ausf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:33:10	1.6.2-1101	...
AMF	amf-1.6.2_22.04.amd64.deb	1.6.2	2023-11-01 17:24:20	1.6.1-1101	...

可查看每个网元下发记录



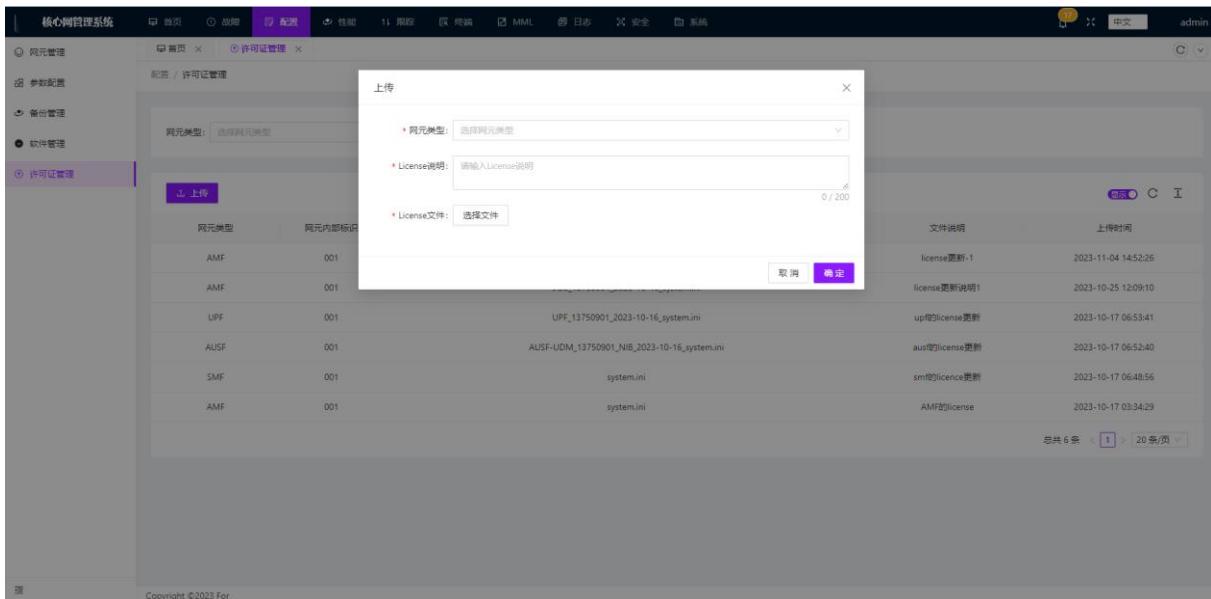
3.4.5 许可证管理

网元 License 管理是指管理和更新网络中各个网元的许可证（License），以确保网络运营商的合规性和资源管理的有效性。在网络中，网元的 License 是网络功能的许可凭证，决定了网元的功能和服务能力。

许可证管理可以记录和管理每个网元的许可证信息，包括许可证类型、有效期限、授权功能等。这对于准确掌握每个网元的许可证情况以及合理规划和管理网络资源非常重要。

通过有效的网元 License 管理，网络运营商可以确保网络设备和功能的合规性和合法性，合理管理网络资源，提高网络的稳定性和性能。这对于提供高质量的网络服务、优化网络资源利用效率非常重要。

操作方法：单击“上传”，输入“网元类型”和“License 说明”，单击“选择文件”，选择要上传的更新后的 License 文件，单击“确定”，完成更新。



3.5 性能

性能管理是指对核心网络的性能进行管理和监测，以确保网络的高效运行和可靠性。核心网性能管理具备定期收集和分析性能数据，确保网络地质标准化，及时发现问题及其根源。主要包括任务管理、性能数据、性能门限和黄金指标四个方面。

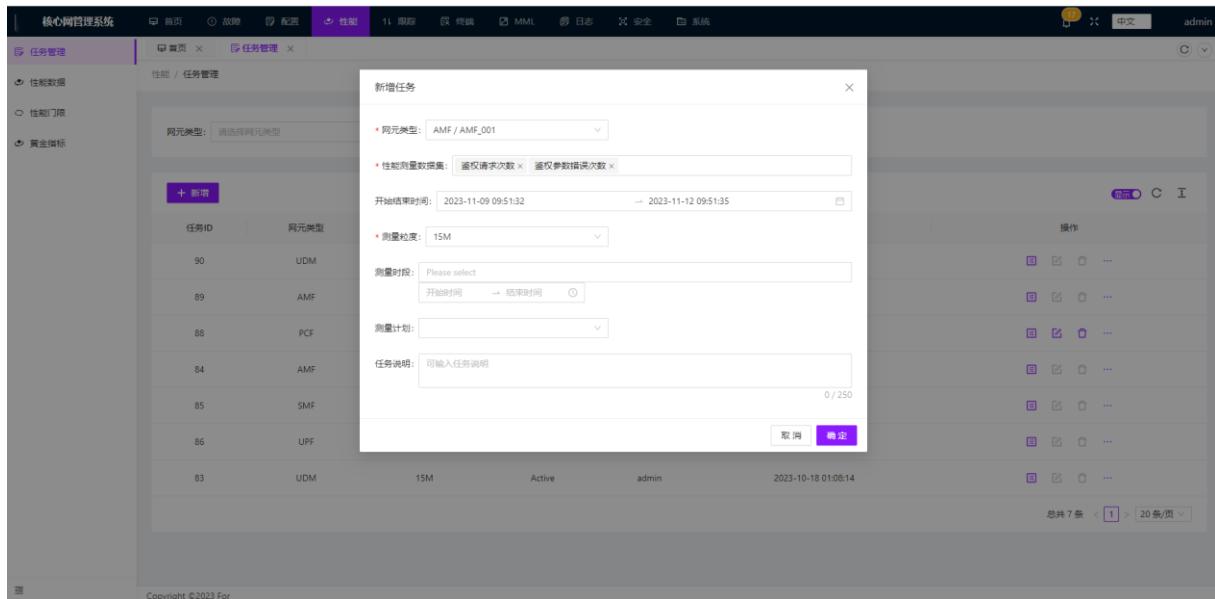
通过有效的核心网性能管理，可以准确掌握网络的性能状况，发现并解决性能问题，提高网络的效率和用户体验。同时，核心网性能管理还可以优化网络资源组合、调整网络容量规划、优化服务提供等相关内容，提高运营和管理效益。

3.5.1 任务管理

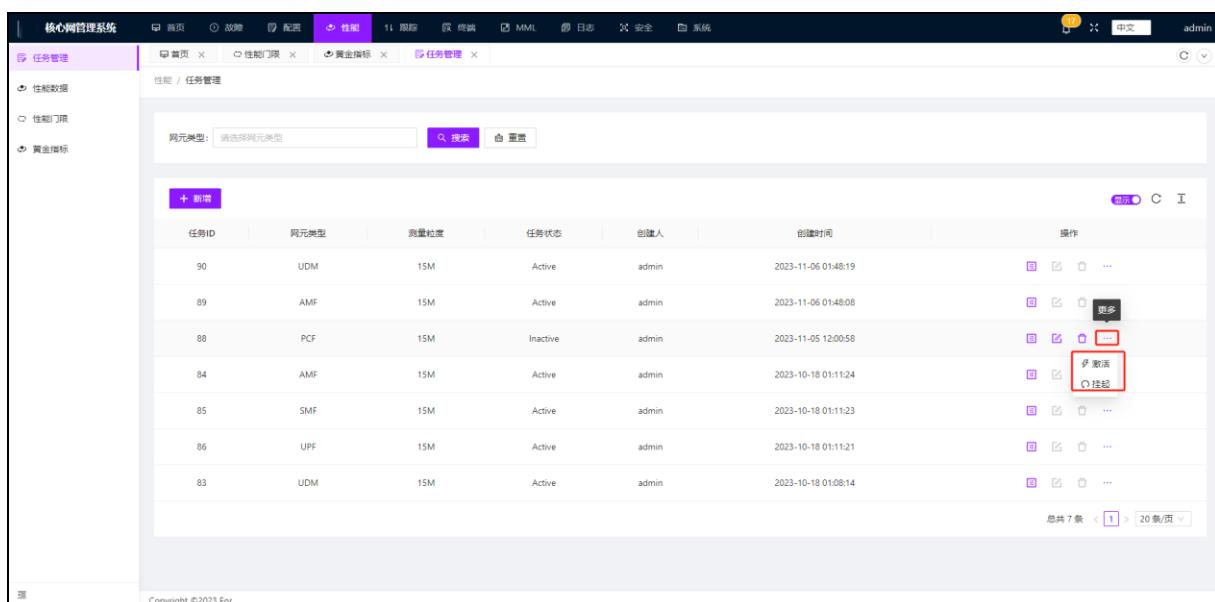
性能任务是通过监测各核心网元的性能指标，进行性能评估和分析，保证网络的地质可靠性。性能任务针对不同的网元，可以创建不同的性能指标任务。您可以设置任务的开始和结束时间。统计粒度分为 15 分钟、30 分钟、1 小时和 24 小时四种。

如创建 AMF 任务时，需要根据网元 AMF 的测量参数、测量粒度、测量周期等配置相应的测量任务。创建任务后，点击右侧的“激活”。当需要中断任务时，可以单击“停止任务”。创建任务后，可以查看每个任务右侧的详细信息，以提供正在创建的任务的具体信息。

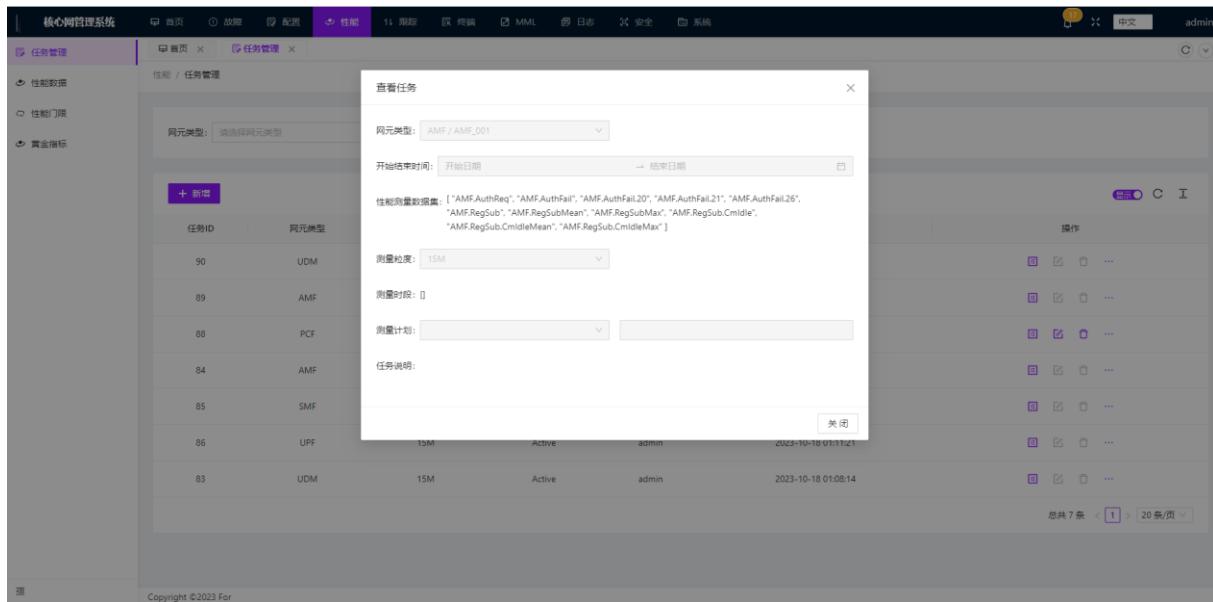
如创建 AMF 任务，配置以网元 AMF，测量参数，测量颗粒度、测量时段等为相应的测量任务：



创建任务后再右侧点击激活，如任务中断可以进行挂起操作



创建任务后可以每个任务右侧详情可查看创建任务的具体信息：



3.5.2 性能数据

性能数据是指对核心网元在不同时间段的各项性能指标进行采集和记录，然后将数据进行分析和展示。性能数据显示在性能任务中创建的性能任务中测量的指标。

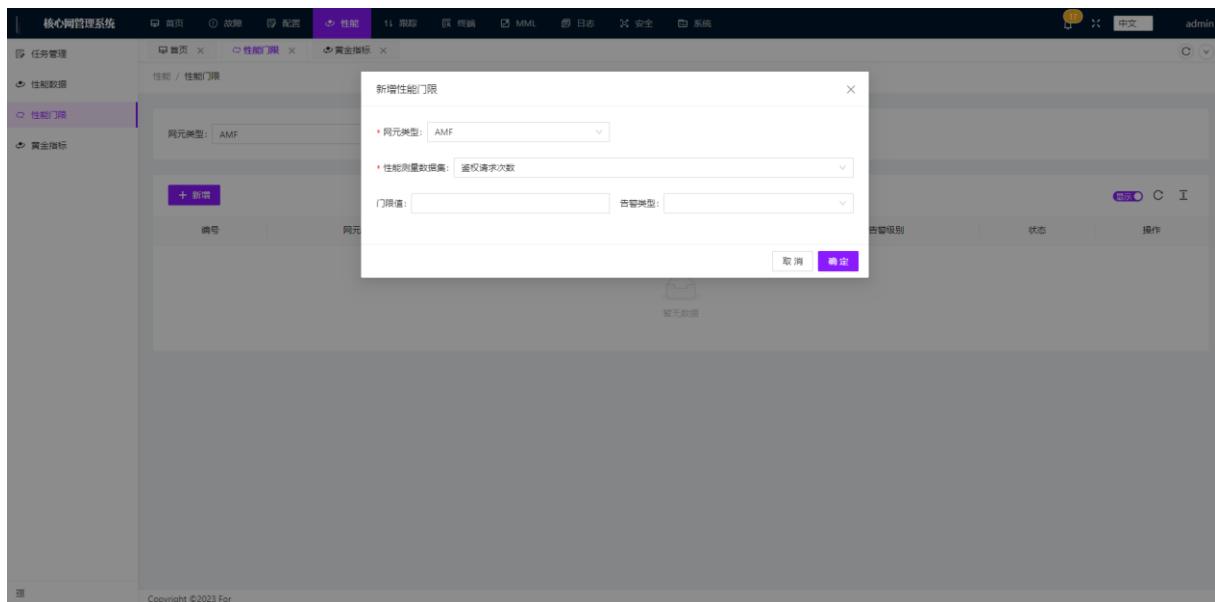
可以根据测量任务制定的网元测量任务，根据网元类型及任务 ID 查看相应统计指标项值：

任务 ID	网元类型	网元名称	颗粒度	统计指标项	值	开始时间	结束时间
90	UDM	UDM_001	15M	UDM.AmfUeCmRegReq	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegSucc	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDM.SdmGetReq	0	2023-11-07 02:49:04	2023-11-07 03:04:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegReq	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegSucc	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDM.SdmGetReq	0	2023-11-07 02:34:04	2023-11-07 02:49:04
90	UDM	UDM_001	15M	UDM.SdmGetReq	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegReq	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegSucc	0	2023-11-07 02:19:04	2023-11-07 02:34:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegReq	0	2023-11-07 02:04:04	2023-11-07 02:19:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegSucc	0	2023-11-07 02:04:04	2023-11-07 02:19:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegReq	0	2023-11-07 02:04:04	2023-11-07 02:19:04
90	UDM	UDM_001	15M	UDM.AmfUeCmRegSucc	0	2023-11-07 02:04:04	2023-11-07 02:19:04

3.5.3 性能门限

性能门限是指将性能数据设定一个正常区间以及预警与警告区间，以便及时发现异常情况。性能门限的设定需要依据当前网络的负载、拓扑结构、运营商要求和设备性能等因素进行综合考虑。

这里可以根据需要定义性能门限，即是对性能测量项（性能测量数据）设定阈值及告警级别。OMC 对性能门限定义的性能测量项进行监测，在性能测量数据超过阈值的情况下产生业务质量告警，提醒业务异常。



3.5.4 黄金指标

核心网元的黄金指标，直接影响网络稳定性和用户体验。通过对重要性能指标的监控，可以及时发现性能问题，并采取相应的措施，保证网络的高效运行和用户的满意度。

黄金指标部分可以表格及图表两种方法展示。在图表展示区，点击右侧 KPI 指标即可选中需要以折线图图表展示的指标

The figure consists of two screenshots of a network management interface. Both screenshots have a dark header bar with various menu items like '主页' (Home), '监控' (Monitoring), '配器' (Config), '性能' (Performance), '问题' (Issues), '报告' (Reports), 'MML' (MML), '日志' (Logs), '安全' (Security), and '系统' (System). The user is logged in as 'admin'. The left sidebar has sections for '任务管理' (Task Management), '性能数据' (Performance Data), '性能门限' (Performance Thresholds), and '黄金指标' (Golden Metrics), with '黄金指标' currently selected.

Screenshot 1 (Top): KPI Statistical Table

This screenshot shows a table titled 'KPI统计图表' (KPI Statistical Chart) with the following columns: 网元名称 (Equipment Name), AMF注册态用户数 (AMF Registered User Count), AMF初始注册请求次数 (AMF Initial Registration Request Count), AMF初始注册成功次数 (AMF Initial Registration Success Count), AMF初始注册失败次数_非法用户 (AMF Initial Registration Failure Count_Invalid User), AMF初始注册失败次数_PDN不允许 (AMF Initial Registration Failure Count_PDN Not Allowed), AMF初始注册失败次数_非法设备 (AMF Initial Registration Failure Count_Invalid Equipment), and 时间 (Time). The data shows 8 rows for 'AMF_001' from 2023-12-29 00:00 to 2023-12-29 02:00, all with 0 values.

Screenshot 2 (Bottom): KPI Statistical Chart

This screenshot shows a line chart titled 'KPI统计图表' (KPI Statistical Chart) with a legend titled '完整统计数据' (Full Statistical Data). The legend lists 10 data series, each represented by a colored circle: AMF注册态用户数 (blue), AMF初始注册请求次数 (green), AMF初始注册成功次数 (yellow), AMF初始注册失败次数_非法用户 (light blue), AMF初始注册失败次数_PDN不允许 (orange), AMF初始注册失败次数_非法设备 (red), AMF初始注册失败次数_5G服务不支持 (purple), AMF初始注册失败次数_弱小区内无合法小区 (pink), and AMF初始注册失败次数_N1模式不匹配 (brown). The x-axis shows time from 2023-12-29 00:00 to 2023-12-29 14:00. The y-axis ranges from 0.3 to 1.2. The chart shows several data series fluctuating over time, with some series having higher peaks than others.

3.6 跟踪

核心网跟踪管理是指对核心网络中的关键业务流程和信令进行监控和分析的管理办法。它通过建立跟踪任务、进行信令分析和信令抓捕等方式，实现对核心网的实时监测和故障排查。在跟踪管理中，目前可以建立与用户数据管理（UDM）相关的跟踪任务，包括接口跟踪、设备跟踪和用户跟踪。

3.6.1 跟踪任务

跟踪任务是核心网跟踪管理的基础，用于监控和分析特定的核心网业务流程。在与用户数据管理（UDM）相关的跟踪管理中，跟踪任务可包括接口跟踪、设备跟踪和用户跟踪三种类型。

- 这里可以配置三种类型跟踪任务：

The screenshot shows the CNMS tracking tasks interface. At the top, there are tabs for '跟踪任务' (Tracking Tasks), '告警' (Alerts), '配置' (Configuration), '性能' (Performance), '日志' (Logs), '安全' (Security), and '系统' (System). The '跟踪任务' tab is selected. On the left, there is a sidebar with '命令分析' (Command Analysis) and '命令抓包' (Command Sniffing). The main area has a search bar with fields for '网元类型' (Element Type), '开始时间' (Start Time), '结束时间' (End Time), and a '搜索' (Search) button. Below the search bar is a table with columns: 编号 (ID), 网元类型 (Element Type), 网元内部标识 (Element Internal Identifier), 跟踪类型 (Tracking Type), 创建人 (Creator), 开始时间 (Start Time), 结束时间 (End Time), and 操作 (Operations). The table contains 13 rows of data, each with a set of three icons for edit, delete, and details.

接口跟踪：

The screenshot shows the CNMS tracking tasks interface with a modal window titled '添加任务' (Add Task) overlaid. The modal contains fields for '跟踪类型' (Tracking Type) set to '接口跟踪' (Interface Tracking), '网元类型' (Element Type) set to 'UDM / UDM_001', '源IP地址' (Source IP Address) set to '172.16.14.140', '目标IP地址' (Target IP Address) set to '172.16.14.120', '命令端口' (Command Port) set to '8080', and '开始结束时间' (Start End Time) set to '2023-11-09 10:12:03' to '2023-11-12 10:12:05'. There is also a '任务说明' (Task Description) field with placeholder text '请输入任务说明' (Please enter task description). The background shows the same tracking tasks table as the previous screenshot.

设备跟踪：

用户跟踪:

3.6.2 信令分析

信令分析是实时监测和解析核心网传输的信令数据，并从中提取有价值的信息和指标。通过对信令数据进行深入分析，可以及时发现网络性能问题、故障和异常现象，并为故障诊断和性能优化提供参考。

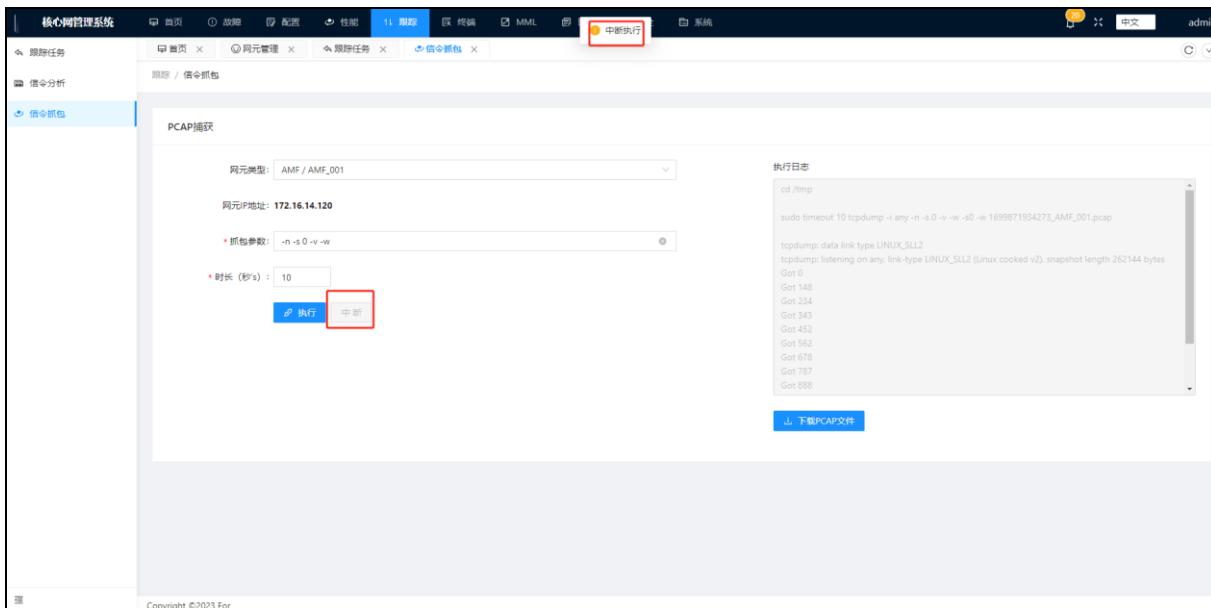
Tracking task tag	IMSI	MSISDN	Source IP address	Destination IP address	Signaling type	Message type	Message direct	Record time	Operate
83	46000010000001		172.25.97.132	172.25.97.133	2	1	1	1982-05-06 02:38:57	
83	46000010000002		172.25.97.132	172.25.97.133	4	1	1	1982-05-06 02:38:57	
83	460000100001002		172.25.97.132	172.25.97.133	8	1	1	1982-05-06 02:38:57	
83	460000100001001		172.25.97.132	172.25.97.133	8	1	0	1982-05-06 02:38:57	
83	46000010000001		172.25.97.132	172.25.97.133	4	1	1	1982-05-06 02:38:57	
83	46000010000001		172.25.97.132	172.25.97.133	8	1	0	1982-05-06 02:38:57	
83	46000010000002		172.25.97.132	172.25.97.133	8	1	1	1982-05-06 02:38:57	
83	46000010000001		172.25.97.132	172.25.97.133	2	1	1	1982-05-06 02:38:57	
83	46000010000001		172.25.97.132	172.25.97.133	4	1	1	1982-05-06 02:38:57	
83	46000010000001		172.25.97.132	172.25.97.133	8	1	0	1982-05-06 02:38:57	

3.6.3 信令抓包

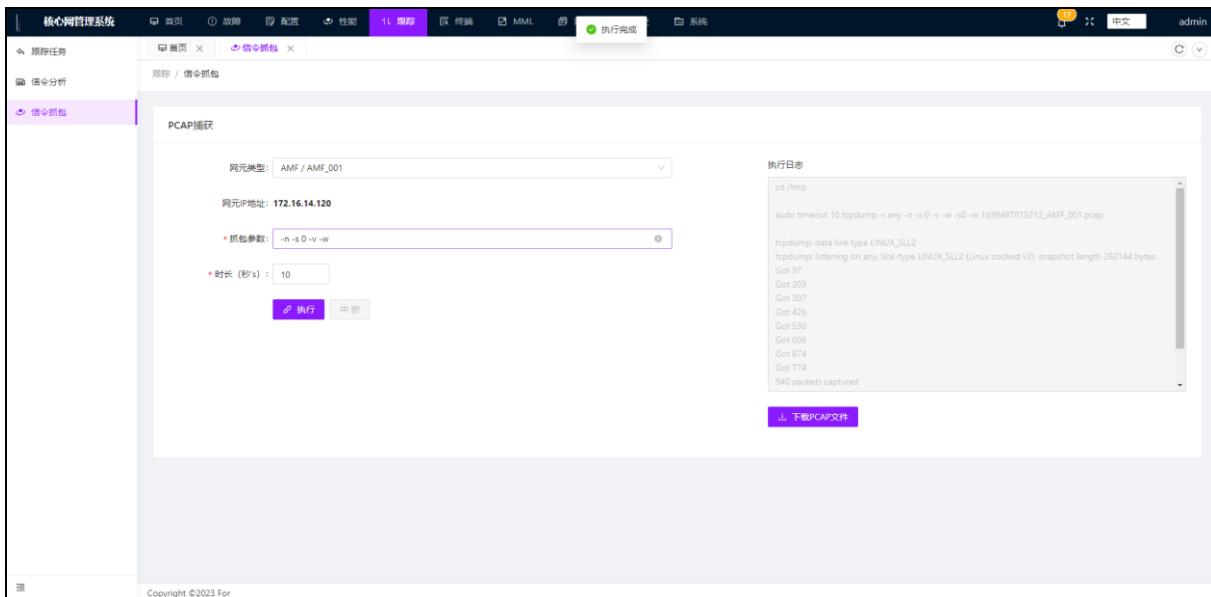
信令抓包是指在核心网中捕获和记录特定的信令流量，以便后续分析和调试。通过信令抓包，运营商可以在出现问题时对相关的信令进行详细的检查和分析，帮助定位故障原因，并制定针对性的解决方案。

在抓信令界面，选择需要抓信令的网元，输入抓包参数和持续时间，单击“执行”。捕获完成后，您可以在右侧下载捕获结果。

执行过程中点击“中断”可中途停止抓包。



抓包完成后右侧可查看抓包结果，抓包名称及抓的包数，执行完成后点击右下角的“下载 PCAP 文件”按钮可对文件进行下载。



3.7 终端

核心网终端管理是指对 5G 核心网络中终端设备的管理和控制，以确保网络的安全性和运行的顺畅性。核心网终端管理包括对用户数据管理（UDM）中的鉴权数据、签约

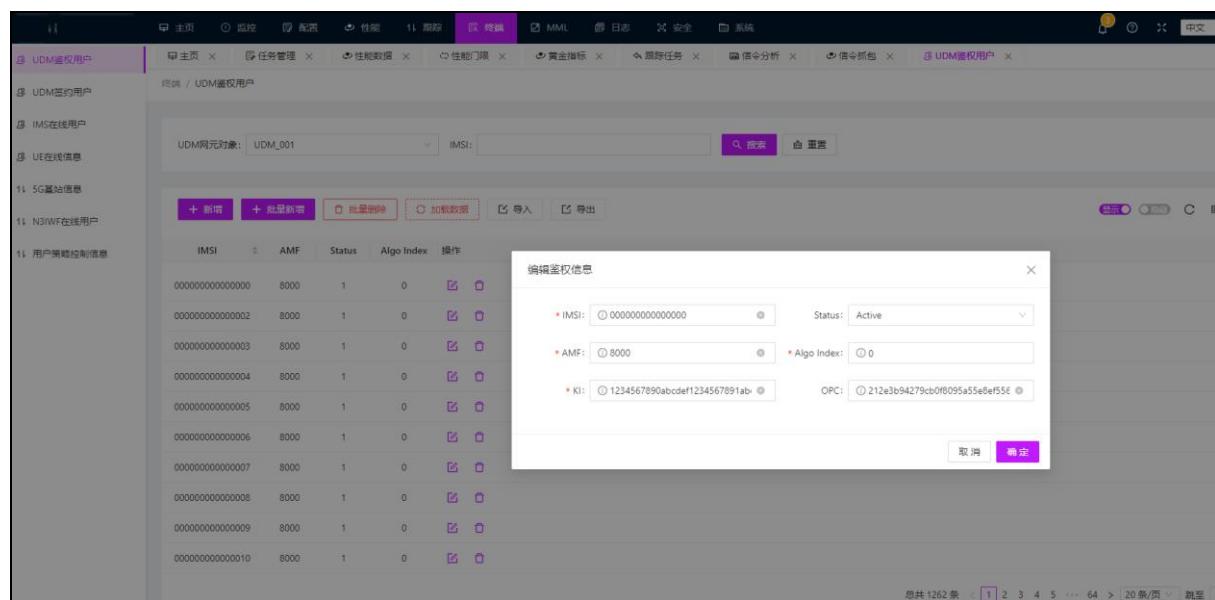
用户数据，以及对 IMS 在线用户、终端在线信息和基站信息的管理。

通过有效的核心网终端管理，网络运营商可以保障终端设备的安全性和可靠性，提高网络的稳定性和性能，为用户提供高质量的服务和良好的用户体验。同时，终端管理还可以帮助运营商优化网络资源的利用，提高网络的运营效率和成本控制。

3.7.1 UDM 鉴权用户

UDM 鉴权数据是存储在用户数据管理（UDM）中的终端设备的鉴权信息。这些数据包括终端的标识信息、密钥信息等，用于在终端与核心网之间进行安全的认证和鉴权。核心网终端管理可以通过添加、修改和删除鉴权数据，单个或批量操作，以确保鉴权信息的准确性和及时性。

这里点击  可以查看 UDM 鉴权用户信息，可以查看 imsi 的 opc 及 ki 等



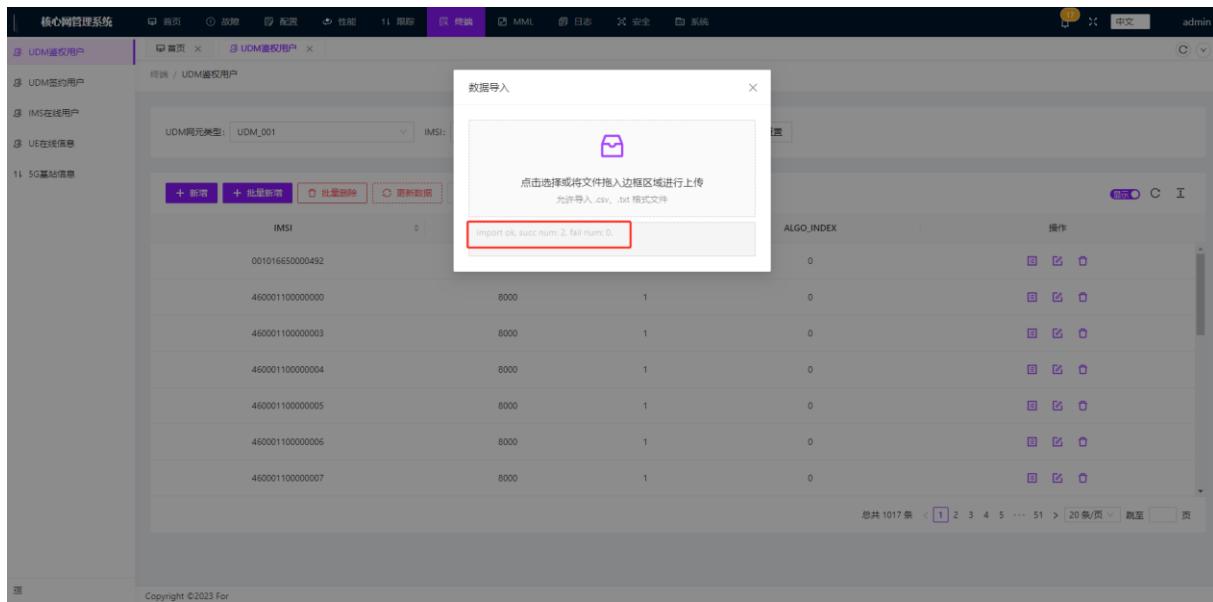
The screenshot shows the UDM鉴权用户 management interface. On the left is a sidebar with navigation links: UDM鉴权用户, UDM签约用户, IMS在线用户, UE在线信息, 5G基站信息, N3IWF在线用户, and 用户策略控制信息. The main area has tabs: 1. 主页, 2. 监控, 3. 配置, 4. 性能, 5. 安全, 6. 期限, 7. 编辑 (highlighted in purple), 8. MML, 9. 日志, 10. 安全. Below these tabs is a breadcrumb trail: 资源 / UDM鉴权用户. A search bar at the top right contains 'UDM网元对象: UDM_001' and 'IMSI:'. Buttons below the search bar include '+ 新增', '+ 批量新增', '批量删除', '加载数据', '导入', and '导出'. The main table lists 10 rows of user data with columns: IMSI, AMF, Status, Algo Index, and 操作 (with icons for edit, delete, and more). A modal window titled '编辑鉴权信息' is open, showing fields for IMSI (0000000000000000), Status (Active), AMF (8000), Algo Index (0), KI (1234567890abcdef1234567891ab...), and OPC (212e3b94279cb0f6095a55e8ef556). Buttons at the bottom of the modal are '取消' and '确定'.

可以对 UDM 鉴权用户进行单个添加，批量新增，单个删除及批量删除，带*号为必填项，填完后点击确定即可。

操作员可以使用 txt 文件导入或导出单个或批量数据。

导入：点击“导入”，点击弹出的窗口，选择要导入的文件。确认后，下面将出现一个提示，指示导入是否成功。

导出：点击“导出”，系统将导出文件并自动下载。



3.7.2 UDM 签约用户

UDM 签约用户是存储在 UDM 中的终端设备的用户信息。这些数据包括用户的 IMSI、MSISDN、SM-DATA、4G 静态 IP、4G 上下文列表等，用于核心网的用户识别和业务管理。核心网终端管理可以对签约用户数据进行单个或批量的添加、修改和删除，确保用户信息的完整性和更新性。

单击右侧的修改按钮，可以查看更详细的用户数据并进行修改，例如修改静态 IP 数据。这里可以查看 UDM 签约用户数据，包括 imsi、msisdn、sm-date、Eps flag 等数据

This screenshot shows the 'UDM签约用户' (UDM签约用户) interface. At the top, there are tabs for '主页', '监控', '配置', '性能', '规则', '策略', 'MML', '日志', '安全', and '系统'. Below the tabs, there's a search bar with fields for 'UDM网元类型' (UDM_001), 'IMSI' (70001546), 'MSISDN' (1-000001&cmnet&ims), and buttons for '搜索' (Search) and '重置' (Reset). A toolbar below the search bar includes buttons for '+ 新增' (Add New), '+ 批量新增' (Batch Add New), '批量删除' (Batch Delete), '加载数据' (Load Data), '导入' (Import), and '导出' (Export). The main area displays a table titled '1l 用户策略控制信息' (User Policy Control Information) with columns: IMSI, MSISDN, Subscribed AMBR, Subscribed SNSSAI, RAT, Forbidden Areas, Service Area Restrict, CN Type, EPS, and Subscribed Data. The table lists 12 entries, each with edit and delete icons. At the bottom right, there's a page navigation bar showing '共 1268 条' (Total 1268 items) and a dropdown for '20条/页' (20 items per page).

This screenshot shows the '编辑签约信息' (Edit Subscription Information) dialog box. It has two input fields at the top: 'IMSI' (001016650001546) and 'MSISDN' (70001546). The main area contains several configuration sections: 'SG Subscribed UE AMBR Template' (def_ambr), 'SG Subscribed SNSSAI Template' (def_nssai), 'SG Subscribed SMF Selection Data Template' (def_nssai), 'SG Forbidden Areas Template' (def_arfb), 'SG Service Area Restriction Template' (def_sar), 'SG RFSP Index' (1), 'SG MICO Mode' (开启 - Enabled), '签约的 MICO 业务标识位' (Subscription MICO Service Identifier), 'SG UE Usage Type' (1), and 'Subscribed SM Data' (1-000001&cmnet&ims). At the bottom right of the dialog are '取消' (Cancel) and '确定' (Confirm) buttons.

可对 UDM 签约用户进行导入导出

导入：点击“导入”，点击弹出的窗口，选择要导入的文件。确认后，下面将出现一个提示，指示导入是否成功。

导出：点击“导出”，系统将导出文件并自动下载。

3.7.3 IMS 在线用户

IMS 在线用户是指基于 ip 的 IMS (multimedia subsystem) 核心网中的在线终端用户。核心网终端管理对 IMS 在线用户进行监控和管理，包括在线用户数、用户 IMSI、MSISDN、注册状态、激活时间等，保证网络资源的合理分配和性能的优化。

IMSI	MSISDN	IMPU	Barring	RegState	Active Time
46000123000002	12307551232	sip:12307551232@ims.mnc000.mcc460.3gpnetwork.org	0	1	2023-11-09 11:36:27
460000100000064	12307550064	sip:12307550064@ims.mnc000.mcc460.3gpnetwork.org	0	1	2023-11-09 11:39:27
46000123000001	12307551231	sip:12307551231@ims.mnc000.mcc460.3gpnetwork.org	0	1	2023-11-09 11:37:19

3.7.4 UE 在线信息

UE 在线信息是指核心网中终端设备的在线状态和连接状态。核心网终端管理可以实时监控终端的在线状态。在 SMF 中注册的用户可以查看终端的 IMSI、MSISDN、RAT 类型、DNN 列表等信息

IMSI	MSISDN	RatType	DnnList	操作
460001100000000	12346000000	NR	cmnet	

3.7.5 基站信息

基站信息是指核心网中基站设备的相关信息，包括 4G 和 5G 基站的 IP、ID、名称、接入基站的 UE 号等。OMC 可以对接入 AMF 的基站信息进行管理，使运营商能够更好地了解接入 AMF 的基站数量和信息。

The screenshot shows the OMC (Open Mobile Orchestrator) web interface. The top navigation bar includes links for Home, Monitoring, Configuration, Performance, Monitoring, Metrics, MML, Log, Security, and System. The current page is '5G Base Station Information' under the 'Metrics' section. A search bar at the top allows filtering by 'AMF Node Type' (set to 'AMF_001') and 'GNB ID'. The main content area displays a table with one row of data:

GNB_ID	ADDRESS	GNB_NAME	UE_NUM
76	192.168.14.47:38412	gNodeB-1-1-0	1

At the bottom right, there is a note indicating 'Total 1 item' and a page navigation bar.

3.7.6 N3IWF 在线用户

N3IWF 在线用户可以实时监控 N3IWF 的在线用户，查看在线用的 IMSI、Active Time、Registration State 及 Network Access Identity。

The screenshot shows the OMC interface with the 'N3IWF Online User' section selected. The top navigation bar and search bar are identical to the previous screenshot. The main content area displays a table with columns: IMSI, Active Time, Registration State, and Network Access Identity. The 'Network Access Identity' column contains a small icon and the text '暂无数据' (No data available).

3.7.7 用户策略控制信息

用户策略控制信息是可以为不同的用户设置不同 PCC Rules 和 SESS Rules 等。

IMSI	MSISDN	SAR	RFSP	QoS Video	QoS Audio	PCC Rules	SESS Rules	HDR Enrich	UE Policy	操作
460001100000000	12346000000	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>
460111111111111	22444	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>
460001100000001	12346000001	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>
460441100000000	11111	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>
460001100000002	12346000002	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>
460111111111112	22445	0				internet ims_sig	internet ims_sig			<input checked="" type="checkbox"/> <input type="checkbox"/>

3.8 MML

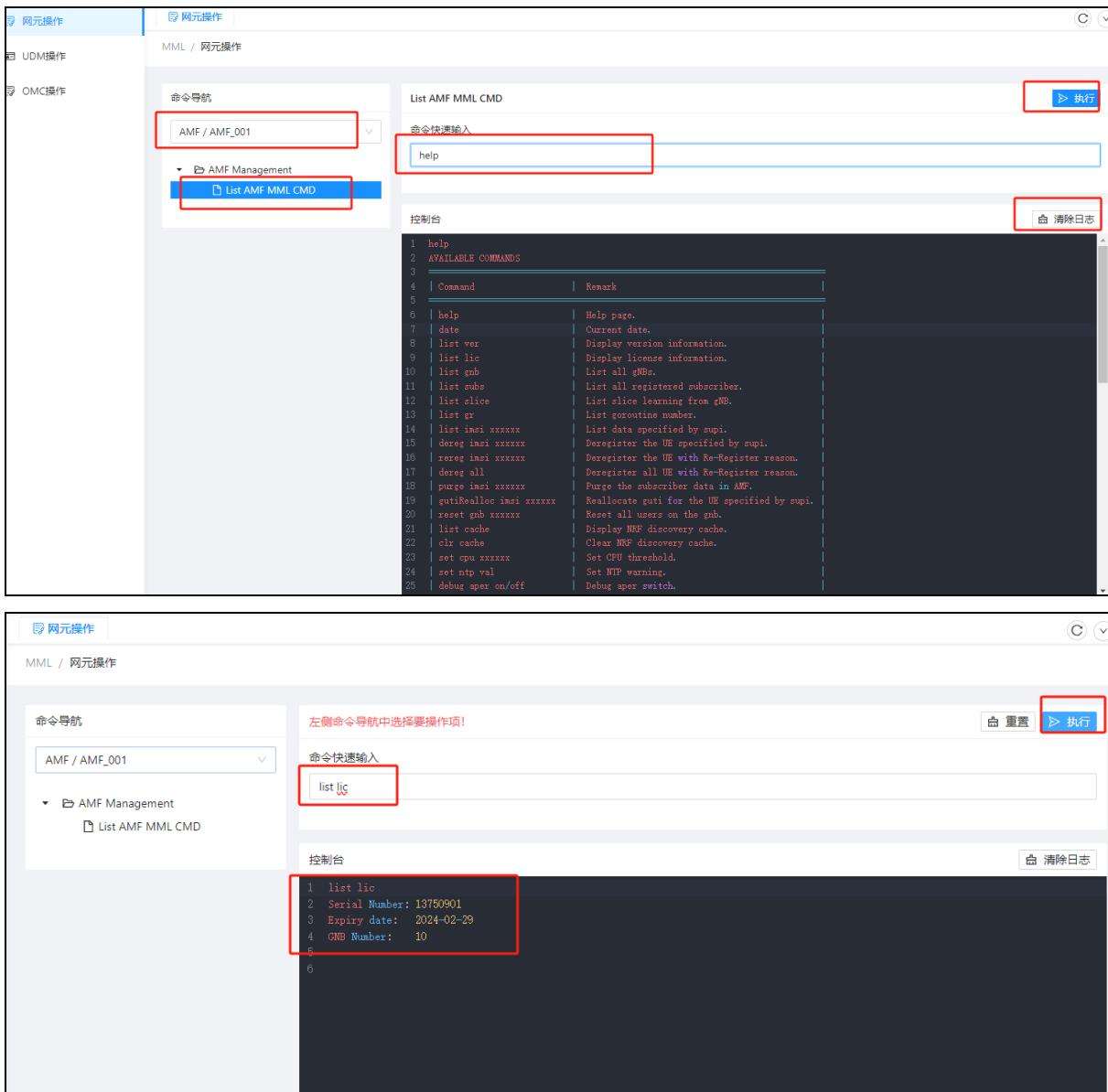
MML(人机语言)管理是指使用特定的命令语言对核心网的各个部分进行管理和配置的方法。MML 管理包括网元操作、UDM 操作和 OMC 操作。

通过 MML 管理，运营商可以对核心网进行管理和配置，保证核心网的稳定运行和高性能。MML 命令具有灵活性和可扩展性，可以根据具体的网络需求和运营商要求进行定制和配置。同时，MML 管理还要求操作人员具备相应的技术和知识，以保证管理操作的准确性和安全性。

3.8.1 网元操作

网元操作通过 MML 命令对核心网元进行管理和配置。网元操作可以查询和配置各个网元的数据信息，如查询网元的 license 信息，版本信息，在 AMF 中查询接入基站的信息，在 UDM 中批量添加删除用户数据等。通过 MML 命令，运营商可以灵活、准确地配置整个核心网的网元，以满足网络性能的要求。

操作步骤：在网元操作界面中选择需要操作的网元，点击下面的“List XXX MML CMD”，然后点击右侧的“执行”，会在下面弹出控制台，控制台中会显示该网元可操作的命令及命令解释。点击“清除日志”可以清空控制台。如果需要输入命令则在“命令快速输入”下面的框框中输入命令，如输入“list lic”，然后点击“执行”，相应结果会出现在控制台中。



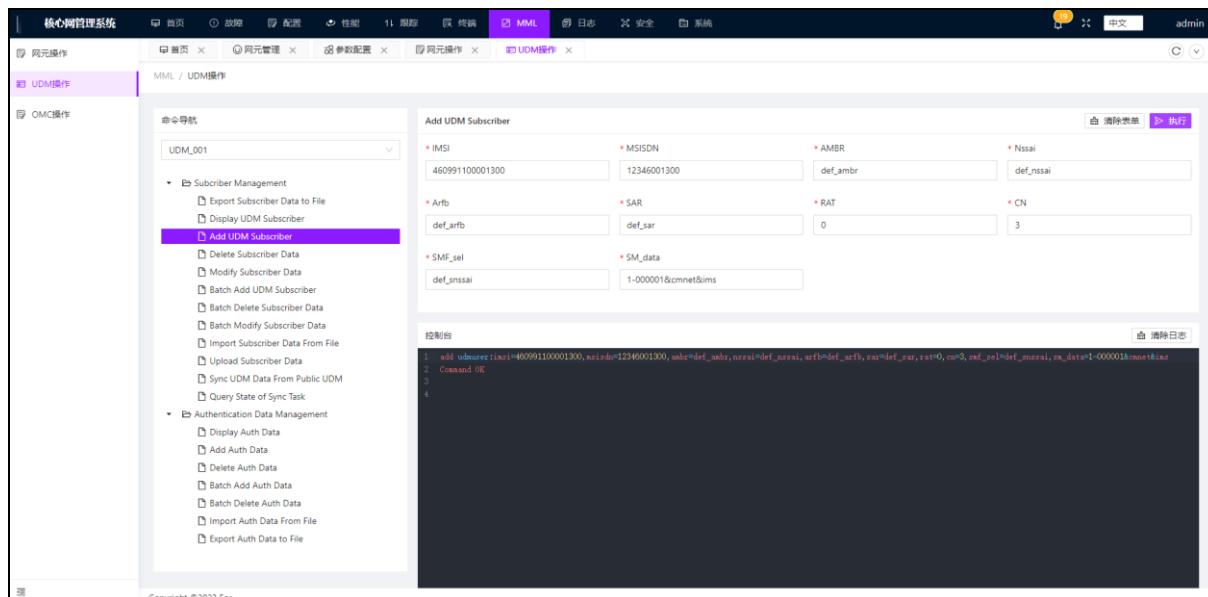
3.8.2 UDM 操作

UDM 操作主要是针对用户数据管理 (UDM) 部分进行配置。这包括对 UDM 鉴权信息的配置，包括终端设备的标识信息和密钥信息的设置，以确保安全认证的正确进行。同时，UDM 操作也包括对 UDM 签约用户数据的配置，包括用户的身份信息、订阅信息和服务配置等。

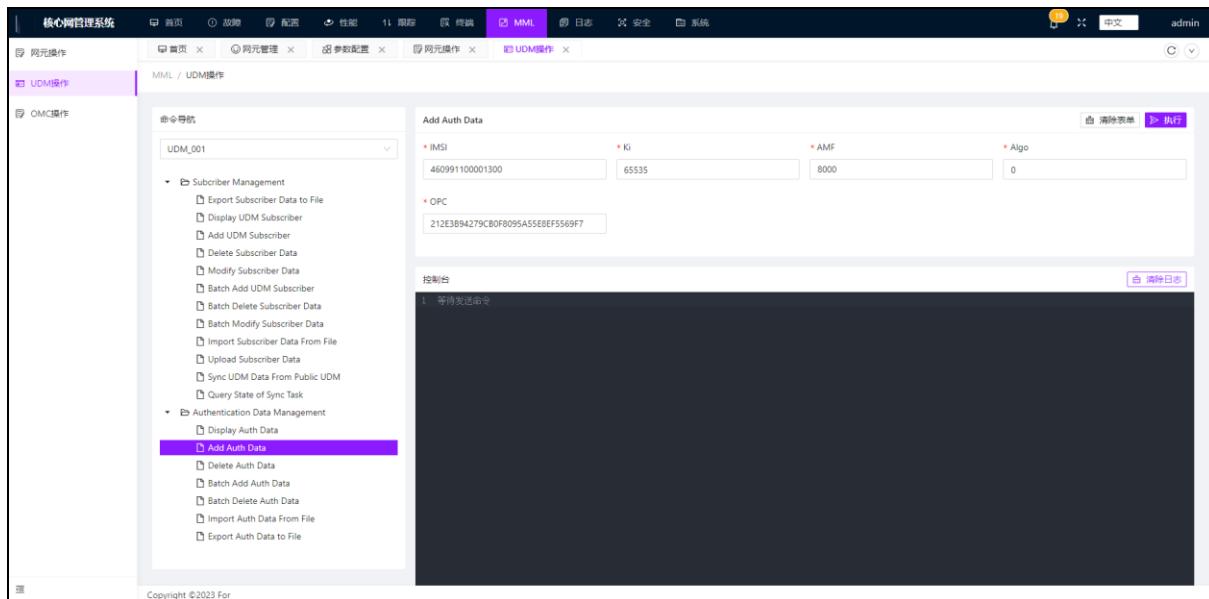
这里可以对 UDM 的签约数据及鉴权数据进行操作，包括添加、删除、批量添加、批量删除用户数据及鉴权数据等，各条命令作用如下，点击命令后带红色*号为必填项，填完之后点击右上角“执行”，结果呈现在下面黑色窗口中。

MML 命令	作用
Export Subscriber Data to File	导出签约用户数据到文件
Display UDM Subscriber	查询签约用户数据
Add UDM Subscriber	添加签约用户数据
Delete Subscriber Data	删除签约用户数据
Modify Subscriber Data	修改签约用户数据
Batch Add UDM Subscriber	批量添加签约用户数据
Batch Delete Subscriber Data	批量删除签约用户数据
Batch Modify Subscriber Data	批量修改签约用户数据
Import Subscriber Data From File	从文件中导入签约用户数据
Upload Subscriber Data	从文件中导入签约用户数据
Sync UDM Data From Public UDM	从大网 UDM 同步 UDM 数据
Query State of Sync Task	查询同步任务状态
Display Auth Data	查询鉴权用户数据
Add Auth Data	添加鉴权用户数据
Delete Auth Data	删除鉴权用户数据
Batch Add Auth Data	批量添加鉴权用户数据
Batch Delete Auth Data	批量删除鉴权用户数据
Import Auth Data From File	从文件中导入鉴权用户数据
Export Auth Data to File	导出鉴权用户数据到文件

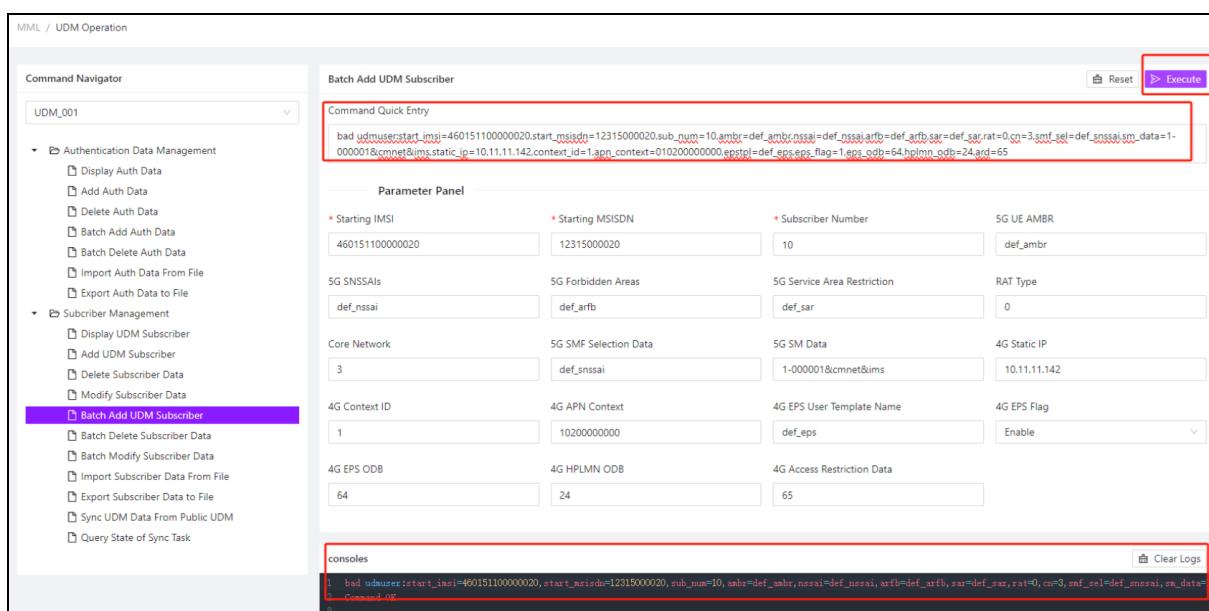
如下，添加 UDM 用户数据



添加用户鉴权数据：



操作员也可以在“命令快速输入”下方的框中输入 MML 命令，点击执行：



3.8.3 OMC 操作

OMC 运营和管理核心网的管理部分。包括对网元的管理，如增加、删除、修改网元信息等。管理网元配置参数，如查询网元配置参数。进行故障管理操作，如查询 AMF 等网元的告警。性能管理操作，如性能数据的收集和分析；系统管理操作，如查询 AMF 等网元的系统信息。

网元管理：

OMC操作

MML / OMC操作

命令导航

- OMC_001
- Network Element Management
 - List NE Information
 - List Managed Element Map
 - Add Network Element
 - Modify Network Element
 - Delete Network Element
- NE Config Parameter Management
 - Display NE Config Parameter
- Fault Management
 - Display Alarm Information
- Linux System Command
 - Run Shell Command
- NBI Resource Management
 - Display NBI Resource Management
- NE Version Management
 - Upgrade NE Software Version

List NE Information

命令快速输入: `lst neinfo;netype=AMF`

参数面板

NE type	NE ID	Resource management UID	NE name	PV flag	IP address	Port	St
AMF							

控制台

```

1 lst neinfo;netype=AMF
2 RetCode = 0 operation succeeded
3
4 Network element information
5
6 NE type NE ID Resource management UID NE name PV flag IP address Port St
7
8 AMF 001 4400HXIAMI001 AMF_001 PNF 172.16.14.120 3030 on
9 AMF 002 4400HXIAMI002 AMF_002 PNF 192.168.14.12 3030 on
10
  
```

故障管理:

OMC操作

MML / OMC操作

命令导航

- OMC_001
- Network Element Management
 - List NE Information
 - List Managed Element Map
 - Add Network Element
 - Modify Network Element
 - Delete Network Element
- NE Config Parameter Management
 - Display NE Config Parameter
- Fault Management
 - Display Alarm Information
- Linux System Command
 - Run Shell Command
- NBI Resource Management
 - Display NBI Resource Management
- NE Version Management
 - Upgrade NE Software Version
- Performance Measure Task Management
 - List Performance Measure Task
 - Add Performance Measure Task
 - Modify Performance Measure Task
 - Delete Performance Measure Task
 - Active Performance Measure Task

Display Alarm Information

命令快速输入: `dsp alarm;netype=AMF`

参数面板

NE type	NE UID	NE name	Alarm code
AMF			

Original severity PV flag Alarm event start time Alarm event end time

--	--	--	--

Alarm type Alarm status

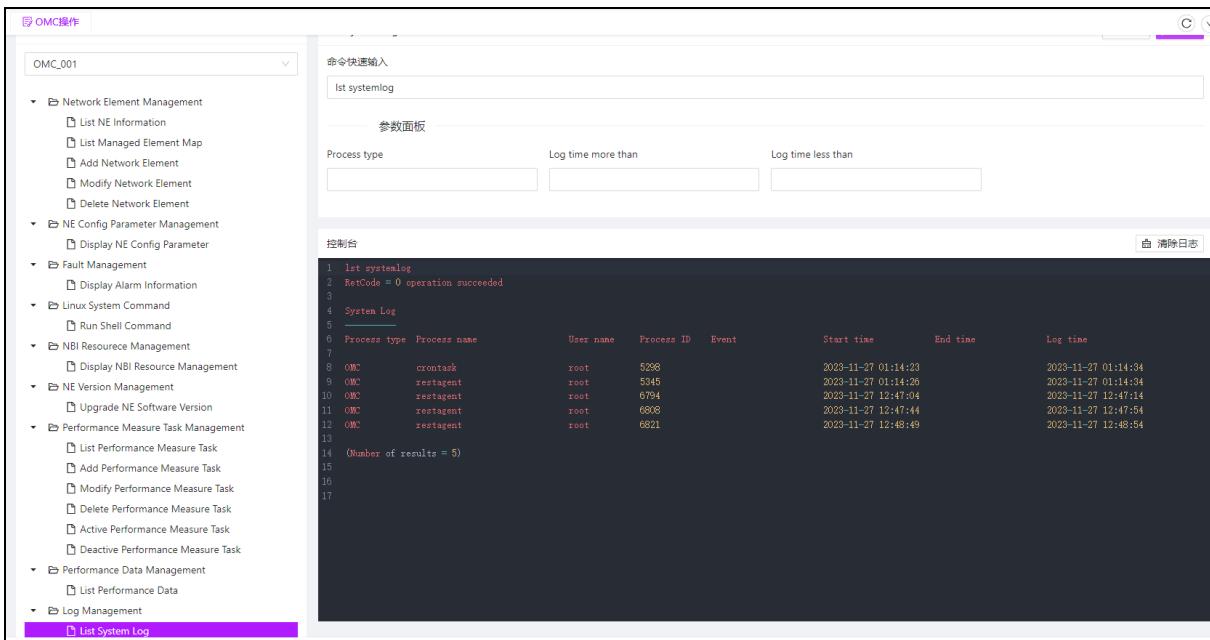
--	--

控制台

```

1 dsp alarm;netype=AMF
2 RetCode = 0 operation succeeded
3
4 Alarm Information
5
6 NE type NE UID NE name Alarm sequence Alarm title Original severity PV flag Event time
7
8 AMF 4400HXIAMI001 AMF_001 256 Performance data report timed out Critical PNF 2023-10-22 00
9 AMF 4400HXIAMI001 AMF_001 257 Performance data report timed out Critical PNF 2023-10-22 00
10 AMF 4400HXIAMI001 AMF_001 258 Performance data report timed out Critical PNF 2023-10-22 00
11 AMF 4400HXIAMI001 AMF_001 259 Performance data report timed out Critical PNF 2023-10-22 00
  
```

日志管理:



3.9 日志

核心网日志管理是网络正常运行时间维护的重要组成部分，管理员可以通过日志跟踪核心网各部分的状态，记录潜在问题，并进行故障排除和性能分析。日志管理包括操作日志、MML 日志、安全日志、告警日志和告警转发日志。

日志管理是高效、准确运维的重要支撑，在保障核心网稳定运行、保障网络安全、优化网络性能方面发挥着非常重要的作用。在实践中，日志管理一般需要结合相应的日志分析工具，通过对各种日志的综合分析，才能发挥出最大的价值。

3.9.1 操作日志

操作日志是记录网络设备管理、软件升级、业务修改等操作过程的关键信息。它们记录了操作的具体细节，包括操作者、操作时间、操作对象和操作结果等。通过操作日志可以快速追溯和审计操作行为，发现潜在问题，确保操作的合规性和责任追溯的可行性。

用户可以查看网管相关的操作记录，并在右侧的详细信息中查看具体的操作信息。

日志编号	模块名称	业务类型	操作人员	请求方式	请求主机	操作状态	操作日期	消耗时间	操作
134	Parameter Configuration	修改	admin	PUT	192.168.0.11	成功	2023-11-09 15:25:06	5 ms	[详细]
133	Parameter Configuration	修改	admin	PUT	192.168.0.11	成功	2023-11-09 15:25:03	29 ms	[详细]
132	UDM Contracted User	修改	admin	PUT	192.168.0.11	成功	2023-11-09 15:12:04	405 ms	[详细]
131	UDM Contracted User	修改	admin	PUT	192.168.0.11	成功	2023-11-09 15:11:37	449 ms	[详细]
130	UDM Contracted User	新增	admin	POST	192.168.0.11	成功	2023-11-09 15:10:28	410 ms	[详细]
129	UDM Contracted User	新增	admin	POST	192.168.0.11	成功	2023-11-09 15:09:15	404 ms	[详细]
128	UDM Contracted User	新增	admin	POST	192.168.0.11	成功	2023-11-09 15:08:22	43 ms	[详细]
127	UDM Contracted User	删除	admin	DELETE	192.168.0.11	成功	2023-11-09 15:08:16	405 ms	[详细]
126	UDM Contracted User	删除	admin	DELETE	192.168.0.11	成功	2023-11-09 15:08:01	405 ms	[详细]
125	UDM Contracted User	删除	admin	DELETE	192.168.0.11	成功	2023-11-09 15:06:38	405 ms	[详细]
124	UDM Authentication User	新增	admin	POST	192.168.0.11	成功	2023-11-09 15:01:54	35 ms	[详细]

3.9.2 MML 日志

MML 日志是记录 MML (Man-Machine Language) 操作命令的执行过程和结果的日志。MML 是一种用于管理和配置网络设备的命令语言，它可以执行配置修改、状态查询和性能统计等操作。MML 日志详细记录了命令的执行情况，包括输入参数、输出结果和执行时间等。通过对 MML 日志的管理和分析，可以追踪命令的执行过程，发现异常情况，定位问题源头，并及时采取相应的修复措施。

编号	登录账号	IP地址	网元类型	网元唯一标识	MML	记录时间
164	admin	192.168.0.11	OMC	001	dsp licenseInforntytype=AMF.neid=001	2023-11-09 08:14:22
163	admin	192.168.0.11	UDM	001	add authdatimsi=460991100001300.ki=65535.amf=8000.algo=0.opc=212E3B94279CB0F8095A55E8EF5569F7	2023-11-09 08:13:19
162	admin	192.168.0.11	UDM	001	add udmsuserimsi=460991100001300.msisdn=12346001300.ambr=def_ambr.nssai=def_nssai.arfb=def_arfb.sar=def_sar.rat=0.cn=3.smt_set=def_snssai.sm_data=1-000001&cmnet&ims	2023-11-09 08:09:12
161	admin	192.168.0.11	UDM	001	add udmsuserimsi=460991100001200.msisdn=12346001200.ambr=def_ambr.nssai=def_nssai.arfb=def_arfb.sar=def_sar.rat=0.cn=3.smt_set=def_snssai.sm_data=1-000001&cmnet&ims	2023-11-09 08:09:03
160	supervisor	192.168.2.114	UDM	001	dsp udmuserimsi=46000011100249	2023-11-07 06:42:35
153	admin	192.168.0.11	UDM	001	dsp udmuserimsi=46099665000505.msisdn=62357000505.ambr=def_ambr.nssai=def_nssai.arfb=def_arfb.sar=def_sar.rat=0.cn=3.smt_set=def_snssai.sm_data=1-000001&cmnet&ims	2023-11-05 14:05:50
152	admin	192.168.0.11	UDM	001	add udmsuserimsi=46099665000504.msisdn=62357000504.ambr=def_ambr.nssai=def_nssai.arfb=def_arfb.sar=def_sar.rat=0.cn=3.smt_set=def_snssai.sm_data=1-000001&cmnet&ims	2023-11-05 14:05:41
151	admin	192.168.0.11	UDM	001	add udmsuserimsi=46099665000504.msisdn=62357000504.ambr=def_ambr.nssai=def_nssai.arfb=def_arfb.sar=def_sar.rat=0.cn=3.smt_set=def_snssai.sm_data=1-000001&cmnet&ims	2023-11-05 13:59:36

3.9.3 安全日志

安全日志主要记录用户登录的信息，包括登录账号、登录 IP 地址、操作系统、登录时间以及登录状态等。通过安全日志可以追踪用户的登录行为，检测异常登录，分析登录模式和行为模式，进一步加强系统的安全性。例如，通过对安全日志的分析，可以发现登录尝试次数过多、非常规的登录时间和地点等异常情况，从而及时采取防护措施，保护系统免受未经授权的访问和攻击。

日志编号	登录账号	登录地址	登录地点	操作系统	浏览器	登录状态	登录信息	登录时间
12	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	Login Successful	2023-11-09 16:17:34
11	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	Login Successful	2023-11-09 14:58:35
10	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	Login Successful	2023-11-09 14:13:18
9	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-09 09:49:58
8	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	退出成功	2023-11-09 09:49:08
7	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-09 08:45:54
6	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	退出成功	2023-11-09 08:45:46
5	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-09 08:45:38
4	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-08 17:43:49
3	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-08 14:44:45
2	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-08 09:47:57
1	admin	192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	成功	登录成功	2023-11-08 09:17:16

3.9.4 告警日志

告警日志是记录网络系统发生异常情况的重要来源之一。它包括 CPU、内存、磁盘、网络等各方面的异常情况，以及服务异常、流量异常、链路异常等告警信息，包括历史告警，活动告警等。告警日志的管理对于及时发现和解决系统故障、提高系统稳定性至关重要。通过对告警日志的分析，可以帮助管理人员快速响应和处理网络故障，减少系统的不可用时间，并进行合理的故障预测和预防。

编号	网元类型	告警网元标识	告警唯一标识	告警流水号	告警编号	原始告警级别	告警产生时间	记录时间
198327	IMS	4400HX1IMS001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198328	AMF	4400HX1AMF001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198331	SMF	4400HX1SMF001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198332	PCF	4400HX1PCF001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198333	UPF	4400HX1UPF001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198329	AUSF	4400HX1AUF001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198330	UDIM	4400HX1UDM001	HXEMSSM10000	10000	历史报警	2023-11-09 06:11:22	2023-11-09 06:11:22	
198322	AUSF	4400HX1AUF001	HXEMSSM10000	10000	活动报警	2023-11-09 06:11:12	2023-11-09 06:11:12	
198325	PCF	4400HX1PCF001	HXEMSSM10000	10000	活动报警	2023-11-09 06:11:12	2023-11-09 06:11:12	
198324	SMF	4400HX1SMF001	HXEMSSM10000	10000	活动报警	2023-11-09 06:11:12	2023-11-09 06:11:12	

3.9.5 告警前转日志

告警前转日志用于记录告警信息的转发过程。它包括告警的产生时间、告警内容、告警级别等。通过告警前转日志，管理人员可以了解告警产生的原因、处理过程和结果。这有助于改进告警处理流程，提高系统故障处理的效率和准确性。同时，告警前转日志还能提供数据支持，用于分析告警等级和频率，进而优化监控策略，减少误报和冗余告警。

编号	网元类型	告警网元标识	告警唯一标识	告警流水号	告警前转对象	告警标题	告警内容	告警产生时间	记录时间
396439	IMS	4400HX1IMS001	HXEMSSM10000	1	simonzhangzz@outlook.com;om.shuzone@126.com	The system state is abnormal	Failed to DialAndSend:dial tcp: lookup smtpp:xxxx.com on 127.0.0.53:53: server misbehaving	2023-11-09 06:11:22	2023-11-09 06:11:22
396440	IMS	4400HX1IMS001	HXEMSSM10000	1	11111112312	The system state is abnormal	Failed to send request: Get "http://smss.co.com? Action=SendSms&PhoneNum bers=11111112312&SignName =%XX+SMSG&TemplateCode= 1000&TemplateParam=%7B%2 2message%22%3A%22alarm% 22%7D": dial tcp: lookup smss.co.com on 127.0.0.53:53: server misbehaving	2023-11-09 06:11:22	2023-11-09 06:11:22

3.9.6 网元日志文件

网元日志文件不分用于下载各个网元的 log，根据点击时间，实时刷新获取网元 log，选择网元后，下面会呈现与该网元相关的所有实时 log，点击右侧可进行下载，点击右上角的刷新标识可实时刷新获取 log。

文件权限	所属用户	所属组	文件大小	修改时间	文件名称	操作
-rw-r--r--	root	root	15M	2023-12-29 14:35:58	amf.log	↓ 下载
-rw-r--r--	agtuser	agtuser	129M	2023-12-28 09:19:39	amf.log.1	↓ 下载
-rw-----	root	root	0	2023-12-22 09:34:12	amfsikey.log	↓ 下载
-rw-r--r--	agtuser	agtuser	129M	2023-12-07 00:52:54	amf.log.2	↓ 下载

3.10 安全

核心网安全管理是指对核心网的用户进行管理和权限控制，以保证网络安全，保护系统免受非法访问或恶意攻击。核心网络安全管理包括用户管理、在线用户管理、角色管理、部门管理和岗位管理。

3.10.1 用户管理

用户管理是核心网安全管理中最基本的实践之一，主要负责管理登录用户的账户。它包括创建新用户、修改用户信息、删除用户和管理用户登录权限等。核心网通常有预定义的默认用户，其中包括 supervisor、admin、manager 和 monitor 这四类用户，每个用户的权限和角色权限都是不同的。具体到权限层面，supervisor 拥有最高权限，可以执行所有配置和管理任务；admin 通常具备管理员权限，能够进行大多数的管理任务和一些高级配置；manager 主要针对运营和维护人员，拥有对核心网进行维护和监控的权限；monitor 则主要担任监控角色，负责监督网络状态，但他们通常不能进行配置更改。

操作员可以查看用户的相关信息，并对用户信息进行添加、删除、修改等操作（“admin”和“supervisor”为超级管理用户）。请注意，只有高权限用户可以删除低权限用户。

核心网管理系统

安全 / 用户管理

用户编号	登录账号	用户名	用户权限	部门名称	登录地址	登录时间	用户状态	操作
1	supervisor	supervisor	Supervisor		192.168.2.114	2023-11-02 18:26:55	正常	编辑 删除 禁用 启用
2	admin	admin	Supervisor, Administrator		192.168.0.11	2023-11-09 16:17:34	正常	编辑 删除 禁用 启用
103	manager	manager	Operator		192.168.2.114	2023-10-30 18:26:36	正常	编辑 删除 禁用 启用
104	monitor	monitor	Monitor				正常	编辑 删除 禁用 启用

总共 4 条 < 1 > 20 条/页

点击新增，可添加登录用户，可根据需要设置不同的用户岗位，添加不同的用户权限，具体权限可参考角色管理：

核心网管理系统

安全 / 用户管理

新增用户信息

登录账号:	username2	账户密码:	*****
用户名:	username2	用户性别:	男
手机号码:		电子邮箱:	
所属部门:	运维部		
用户岗位:	管理人员	用户权限:	manager
用户说明:			

0 / 450

取消 确定

可对用户进行导入导出操作，可下载导入模板添加用户数据后进行导入，右侧可查看用户的具体详细信息，同时可以修改用户密码：

User Information Dialog (Top Screenshot):

字段	值
用户编号	2
登录账号	supervisor
用户名	admin
手机号码	
所属部门	
用户岗位	请选择用户岗位
用户权限	Administrator
用户说明	

Reset Password Dialog (Bottom Screenshot):

字段	值
登录账号	admin
登录密码	岳

3. 10. 2 在线用户

在线用户管理是实时控制和监控当前登录系统用户的重要环节。管理人员可以实时看到哪些用户处于登录状态，以及他们登录的具体时间、使用的主机 IP 地址、所使用的操作系统等信息。此外，为了保证系统的安全，管理员通过在线用户管理还能执行必要的控制操作，如对异常登录或未经授权的用户执行强制登出（强退）操作。

序号	会话编号	登录账号	所属部门	登录主机	登录地点	操作系统	浏览器	登录时间	操作
1	vk9iwa07exgkp3pf	admin		192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	2023-11-09 14:58:35	
2	w2xt0jvq95pr832i	admin		192.168.0.11	内网IP	Windows 10	Chrome 118.0.0.0	2023-11-09 16:17:34	

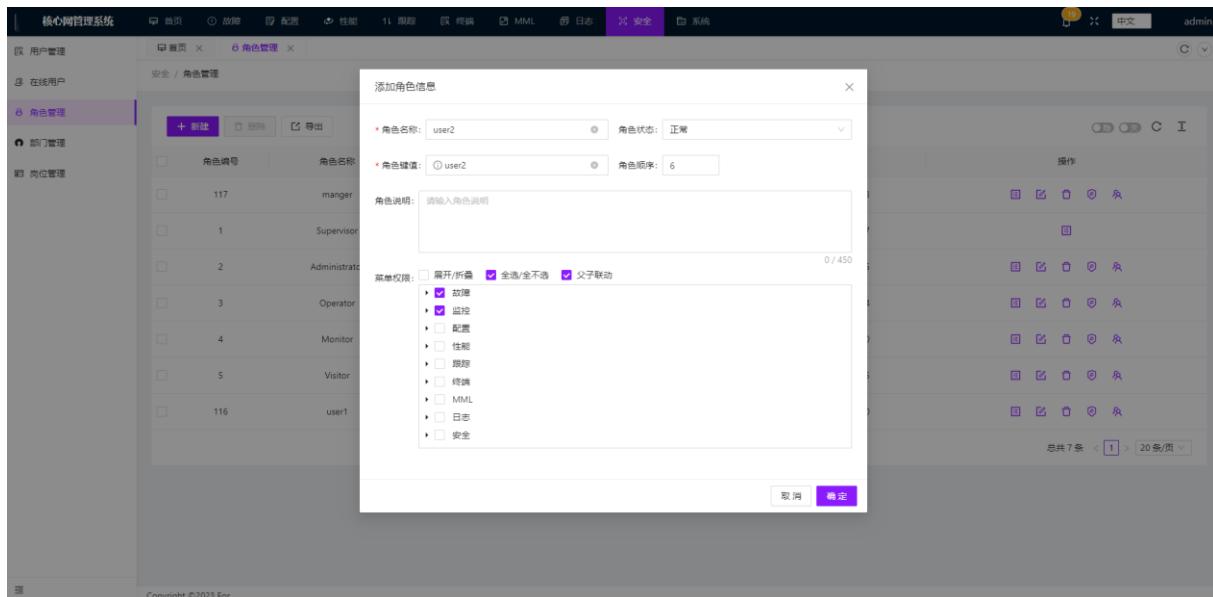
3. 10. 3 角色管理

心网的角色管理允许定义不同的用户角色，并基于角色分配权限。这个过程通常涉及到定义角色名称、分配权限以及将这些角色与具体用户关联。通过角色管理，管理员能够对系统访问进行精细化控制，确保用户只能访问对应于他们工作职责的资源和数据，这样不仅提高了工作效率也大大降低了信息泄露的风险。

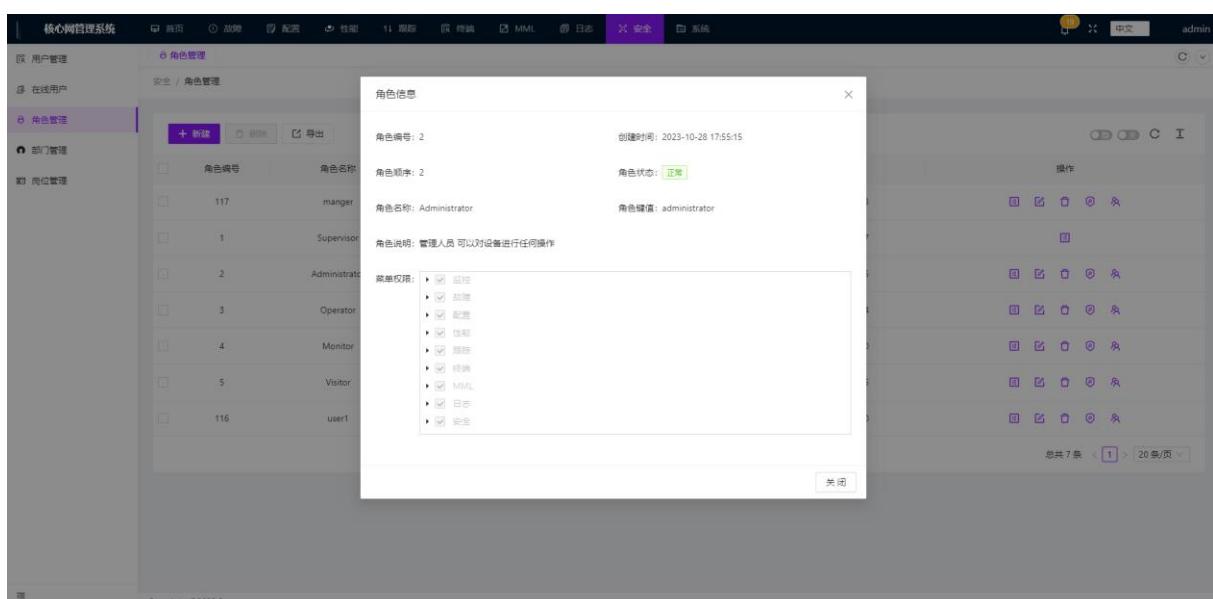
- 这里可以查看角色相关信息并操作增删修改，可以添加角色权限集：

角色编号	角色名称	角色值	角色顺序	角色状态	创建时间	操作
117	manager	manager	0		2023-11-05 16:41:23	
1	Supervisor	supervisor	1		2023-10-12 14:17:17	
2	Administrator	administrator	2		2023-10-28 17:55:15	
3	Operator	operator	3		2023-10-28 17:55:34	
4	Monitor	monitor	4		2023-10-28 17:55:50	
5	Visitor	vistor	5		2023-10-28 17:56:15	
116	user1	user1	6		2023-11-05 00:39:20	

添加角色信息，可根据需要添加不同角色，给与角色不同的菜单权限：



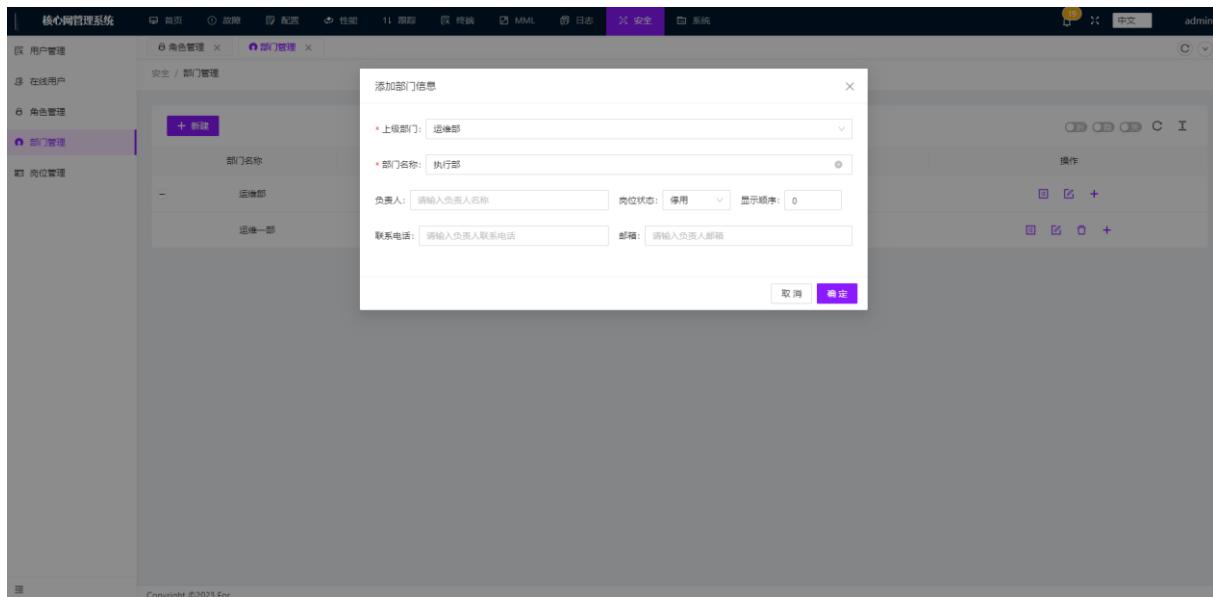
角色名称右侧可查看每个角色的具体菜单权限，并可进行修改删除操作等



3. 10. 4 部门管理

部门管理涉及到组织内不同部门的权限和资源分配。通过定义部门结构和层级，核心网能够精确地将资源和数据访问分配到不同的业务单元。每个部门或团队都有自己特定的权限等级，确保数据的适当访问，同时防止跨部门的未授权访问。

- 这里可以看到部门类别，可根据需要新建不同部门，并给不同用户分配不同的部门：



3.10.5 岗位管理

岗位管理与职位和个人工作职责密切相关。通过为不同的岗位配置特定权限，可以更加精确地管理网络访问。这也有助于创建明确的责任链，并确保关键任务和职责分配给具备相关技能和授权的员工。

- 这里可以看到不同岗位名称，并新增删除修改岗位：

岗位编号	岗位编码	岗位名称	岗位排序	岗位状态	创建时间	操作
1	Administrator	管理人员	1	正常	2023-10-12 19:28:26	
2	Operator	运维人员	2	正常	2023-10-12 19:28:26	
3	Monitor	监控人员	3	正常	2023-10-12 19:28:26	
4	Visitor	普通用户	4	正常	2023-10-12 19:28:26	

3.11 系统

核心网系统管理是指对核心网系统的功能和配置进行管理和维护。主要包括调度任

务、系统信息、菜单管理、字典管理、参数设置、系统设置等功能。

通过核心网系统管理，管理员可以对核心网系统进行灵活的配置和管理，以满足业务需求，提高系统的可用性和安全性。管理员可以根据实际情况定制配置，以保证系统的稳定运行和高效维护。

3.11.1 调度任务

调度任务管理是核心网系统管理中的一个重要方面，它允许网络管理员自动化执行重复性任务，确保系统正常运行同时减少了人为的干预。一个高效的调度系统可以定时执行多种任务，保证资源的合理利用和网络的持续稳定性。

在初始设置中，可以建立以下五个调度任务：

- 1、**监控-系统资源**：这个任务负责实时监控和记录系统资源的使用情况，包括CPU占用率、内存利用率、存储空间使用情况以及网络带宽的使用。有效监控这些参数对于预防系统过载和性能瓶颈是必要的，也可以帮助管理员针对特定的资源使用趋势进行规划和调整
- 2、**删除过期网元备份文件**：该任务自动删除历史的网元备份文件，特别是那些已经过了保留期限的备份。自动化这一过程确保了存储空间的最优利用，防止不必要的数据积聚，并减低手动清理的负担。
- 3、**删除过期历史告警记录**：历史告警记录是系统运行中出现的问题的记录。这项任务的目标是清除旧的和不再相关的告警日志，以免数据库不断膨胀而影响系统性能。同时也有助于安保人员集中注意力于最近和最相关的安全问题。
- 4、**删除过期黄金指标记录**：黄金指标是网络性能管理中至关重要的性能指标。这些记录随着时间的推移可能会变得不再相关，任务是删除这些过期记录以保持数据库的准确性和有效性。
- 5、**网元配置自动备份任务**：定时自动备份网络设备配置是防止因配置错误或其他问题造成严重影响的重要措施。这项任务确保所有的配置变更都有备份，以便于在必要情况下迅速恢复正常的工作。

调度任务管理还需要一个用户友好的界面，让管理员能轻松创建、配置、监控和管理这些任务。它应该提供日志记录功能，以便审核每个任务的历史运行情况。此外，对任务执行结果的通知也是必不可少的，保证管理员能及时了解任务执行状态和必要时进行干预。

The screenshot shows the 'Task Scheduling' module of the CNMS. The main table lists seven scheduled tasks:

任务编号	任务名称	任务组名	调用目标	cron表达式	状态	记录日志	操作
1	监控-系统资源	系统	monitor_sys_resource	0 0/5 * * ?	正常	记录	
4	删除过期元备份文件	系统	delExpiredNBackup	0 20 0 * * ?	正常	记录	
5	删除过期历史告警记录	系统	deleteExpiredRecord	0 10 0 * * ?	正常	记录	
6	删除过期黄金指标记录	系统	deleteExpiredRecord	0 15 0 * * ?	正常	记录	
7	网元配置自动备份任务	系统	backupEtcFromNE	0 30 0 * * ?	正常	记录	

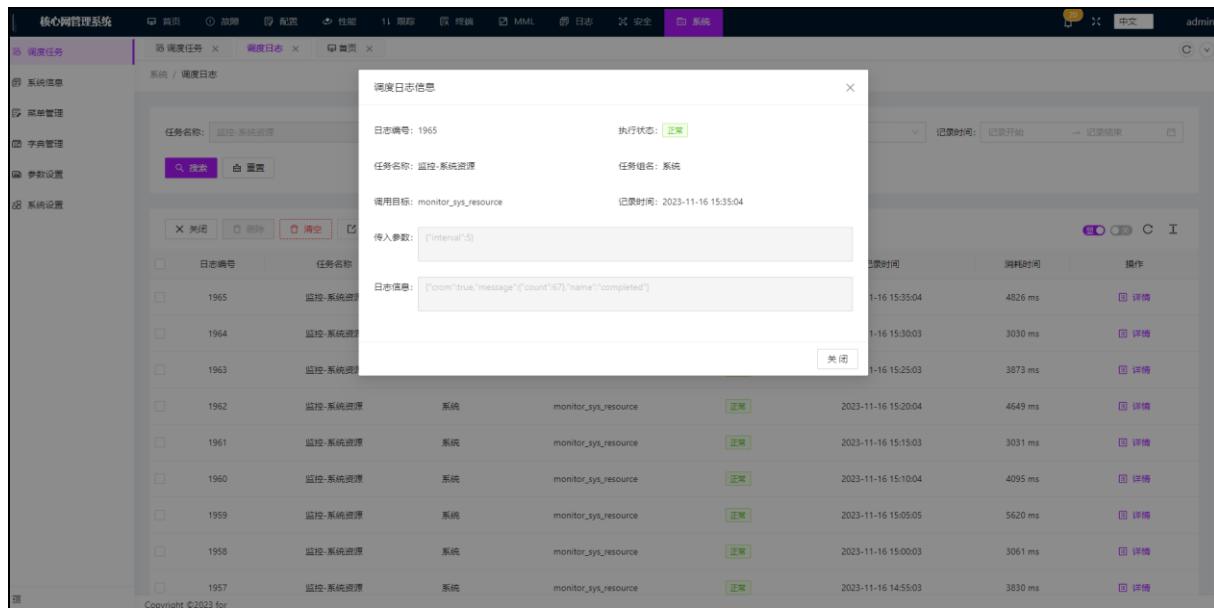
Total 5 items < 1 > 20 items/page

- 监控-系统资源：此项为统资源CPU/IO/Network收集可查看及修改系统平均interval5分钟资源情况，任务右侧的日志点击后，可查看系统资源每次具体的刷新时间。

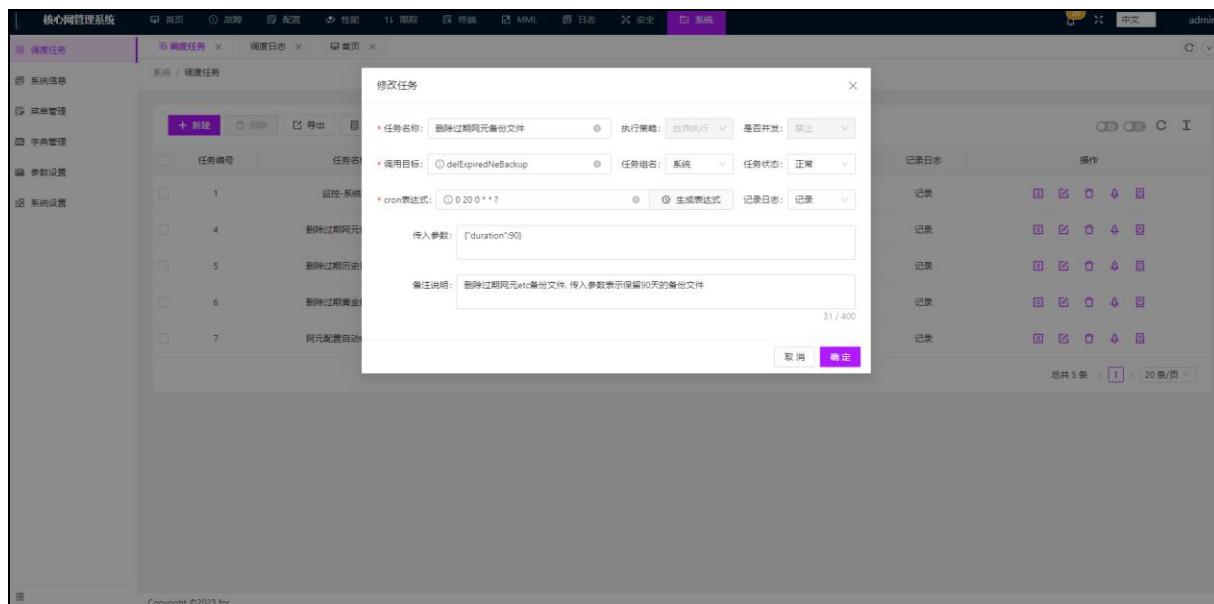
The screenshot shows the 'Edit Task' dialog box for the task '监控-系统资源'. The dialog contains the following fields:

- 任务名称: 监控-系统资源
- 执行策略: 放弃执行
- 是否并发: 禁止
- 调用目标: monitor_sys_resource
- 任务组名: 系统
- 任务状态: 正常
- cron表达式: 0 0/5 * * ?
- 生成表达式
- 记录日志: 记录
- 传入参数: ["interval":5]
- 备注说明: 系统资源CPU/IO/Network收集, interval单位分钟, 0 0/5 * * ? 表示平均interval5分钟资源情况

Buttons: 取消, 确定



- **删除过期网元备份文件:** 此项可查看及修改过期网元 etc 备份文件的时间，达到时间后进行记录删除，传入参数表示保留 90 天的备份文件，删除时间为 0:20。点击右侧日志，可查看之前删除过期网元备份文件的历史记录



The screenshot shows the 'Audit Log' (调度日志) page of the CNMS. The table lists the following data:

日志编号	任务名称	任务组名	调用目标	执行状态	记录时间	消耗时间	操作
1878	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-16 08:20:00	86 ms	
1586	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-15 08:20:00	101 ms	
1294	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-14 08:20:00	114 ms	
749	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-10 08:20:00	84 ms	
458	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-09 08:20:00	80 ms	
167	删除过期网元备份文件	系统	delExpiredNetBackup	正常	2023-11-08 08:20:00	120 ms	

- **删除过期历史告警记录:** 此项可查看及修改过期历史告警记录的时间，达到时间后进行记录删除，传入参数 duration:34 表示保留 34 天的历史告警记录，删除时间为 0:10。点击右侧日志，可查看之前删除过期历史告警记录的历史记录

The screenshot shows the 'Modify Task' (修改任务) dialog box. The task configuration is as follows:

- 任务名称: 剔除过期历史告警记录
- 执行策略: 放开执行
- 是否并发: 禁止
- 任务编号: 1
- 任务名: 清理_系统
- 调用目标: deleteExpiredRecord
- 任务组名: 系统
- 任务状态: 正常
- cron表达式: 0 10 0 * *?
- 生成表达式: 记录日志: 记录
- 传入参数: [{"duration":34,"tableName":"alarm","colName":"event_time","extras":{"alarm_status":0}}]
- 备注说明: 剔除过期历史告警记录，传入参数表示保留34天的历史告警记录。

日志编号	任务名称	任务组名	调用目标	执行状态	记录时间	消耗时间	操作
1874	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-16 08:10:00	77 ms	
1582	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-15 08:10:00	10 ms	
1290	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-14 08:10:00	10 ms	
745	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-10 08:10:00	11 ms	
454	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-09 08:10:00	11 ms	
163	删除过期历史告警记录	系统	deleteExpiredRecord	正常	2023-11-08 08:10:00	15 ms	

- **删除过期黄金指标记录：**此项可查看及修改过期黄金指标记录的时间，达到时间后进行记录删除，duration:39 表示黄金指标记录保留 39 天，删除时间为 39 天后的 0:15。点击右侧日志，可查看之前删除黄金指标记录的历史记录

修改任务

记录日志	操作
记录	

日志编号	任务名称	任务组名	调用目标	执行状态	记录时间	消耗时间	操作
1877	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-16 08:15:20	28255 ms	
1585	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-15 08:15:19	19700 ms	
1293	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-14 08:15:17	17258 ms	
748	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-10 08:15:30	30368 ms	
457	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-09 08:15:21	21362 ms	
166	删除过期黄金指标记录	系统	deleteExpiredRecord	正常	2023-11-08 08:15:08	8719 ms	

- 网元配置自动备份任务：可查看及修改网元自动备份时间，图中的 cron 表达式中“0 30 0 * * ?”表示每天 0:30 分进行备份。调度日志中可以查看备份历史记录

The screenshot shows the 'Modify Task' dialog box overlaid on the main task list. The dialog contains the following information:

- 任务名称:** 网元配置自动备份任务
- 执行策略:** 异步执行
- 是否并发:** 禁止
- 任务编号:** 1
- 任务名称:** 监控-系统
- 调用目标:** backupEtcFromNE
- 任务组名:** 系统
- 任务状态:** 正常
- cron表达式:** 0 30 0 * * ? (highlighted with a red box)
- 输入参数:** 调用目标传入参数，仅支持json字符串
- 备注说明:** 自动备份网元etc目录下的配置文件

3.11.2 系统信息

系统信息管理是核心网系统管理的另一个关键组成部分。通过系统信息管理，管理员可以轻松访问系统的关键性能指标和硬件状态。下面是在核心网管理中可能涉及的系统信息：

- 1、**系统信息：**这部分信息包括操作系统类型、版本、系统启动时间、当前在线用户数量以及系统整体的健康状况等基础数据。它为管理员提供了系统的高层概览，帮助进行日常的运维决策。
- 2、**CPU 信息：**处理器的性能直接影响着核心网系统的效率。系统信息管理需要展示 CPU 的型号、核心数、使用率和温度等数据。通过实时监控 CPU 使用情况，管理员可以及时发现和解决可能影响系统性能的瓶颈问题。
- 3、**内存信息：**内存信息管理包括总体的内存容量、当前使用量、缓存和缓冲区占用量，以及内存交换情况等。内存泄漏或资源紧张的情况可以通过这些信息得以发现，确保系统不会因内存不足而出现性能下降。
- 4、**时间信息：**准确的系统时间对于日志记录、任务调度以及多设备协同工作至关重要。系统信息管理会显示当前的系统时间，时间同步状态，以及与时间服务器的连接状况等。

5、网络信息：管理系统网络性能和连接状态的信息，包括网卡的状态、IP地址、数据包传输速率、网络延迟以及各种网络协议的使用状况。这有助于确保网络连接稳定可靠，以及及时发现并处理网络相关的问题。

6、磁盘信息：存储状况对核心网系统同样重要。系统信息管理需要包含磁盘使用情况、文件系统类型、读写速率及可用空间等。合理的磁盘管理可以避免存储空间不足导致的系统问题

系统信息管理通常通过一个集中的仪表板或控制台展示，该仪表板可对上述每个部分进行实时监测，并提供直观的图表和警告机制，以便管理员可以轻松识别并解决潜在问题。此外，对历史性能数据的长期跟踪和分析有助于规划未来的资源需求和系统升级。

The figure consists of two vertically stacked screenshots of a network management system's 'System Information' page. Both screenshots have a dark header bar with tabs for 首页 (Home), 故障 (Faults), 配置 (Config), 性能 (Performance), 11 期数 (Issue 11), 恢复 (Recovery), MML, 日志 (Logs), 安全 (Security), and 系统 (System). The user is logged in as 'admin'. The top screenshot shows the 'System Information' section with details like Platform (ubuntu), Architecture (x86_64), and CPU usage. The bottom screenshot shows the same section but includes a 'Disk Usage' table at the bottom.

System Information (Top Screenshot)

运行平台	ubuntu	平台版本	22.04
系统平台	linux	系统架构	x86_64
主机名称	omc	运行时长	4天 2小时 15分钟 1秒

CPU信息

型号	Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz
速率(Hz)	2394MHz
核心数	4
使用率(%)	31.71 / 31.95 / 31.88 / 31.76

内存信息

总内存	3.82GB	剩余内存	2.65GB
使用率(%)	23.41	进程总内存	70.85MB
堆的总大小	62.22MB	堆已分配	42.37MB
链接库占用	8.63MB		

System Information (Bottom Screenshot)

使用率(%)	23.41	进程总内存	70.85MB
堆的总大小	62.22MB	堆已分配	42.37MB
链接库占用	8.63MB		

Time Information

时间	2023-11-09 09:54:28	时区	+0000 UTC	时区名称	UTC
----	---------------------	----	-----------	------	-----

Network Information

ens16	IPv4 172.16.14.100 / IPv4 192.168.5.56 / IPv6 fe80::20c:9fffe22:44d0
-------	--

Disk Usage (Bottom Screenshot)

路径/设备	总大小	剩余大小	已使用大小	空间使用率(%)
/dev/dm-0	23.45GB	2.05GB	20.18GB	90.8%
/dev/loop2	47.00MB	0B	47.00MB	100.0%
/dev/loop0	62.00MB	0B	62.00MB	100.0%
/dev/loop1	80.00MB	0B	80.00MB	100.0%
/dev/sda2	1.90GB	1.66GB	128.75MB	7.0%

3.11.3 菜单管理

菜单管理在核心网络系统管理中作为一个中心功能，它允许管理员定制和优化用户界面（UI）导航，以满足特定用户和权限组的需求。管理系统的菜单项通常来说是多级的，它们提供了访问系统各个部分的路径和选项。良好的菜单管理能够增强用户体验，并简化系统操作流程。

下面是菜单管理的功能：

- 1、增加菜单项：允许管理员向系统菜单中添加新的选项或功能。例如，如果引入了一个新的分析工具或报告功能，管理员可以在适当的菜单类别下添加该工具的入口，以便用户可以访问。
- 2、删除菜单项：当某个功能过时或不再需要时，管理员可以从菜单中移除相关的选项，这有助于避免界面上的混乱，并确保用户界面保持相关性和精简性。
- 3、修改菜单项：为保证菜单的逻辑性和用户友好性，不时需要对菜单项进行重命名、重新排序或更改其在菜单结构中的位置。菜单管理应该能够让管理员轻松做出这些调整。
- 4、菜单项权限管理：依据用户的角色和权限授予用户访问特定菜单项的能力。这意味着某些用户可能只能看到对其工作必要的菜单选项，而不是整个系统的所有选项。这有助于减少错误操作的风险，以及保护敏感数据。
- 5、菜单样式自定义：允许更改菜单的外观，如颜色、字体和图标等，以保持与公司品牌标识一致或简化用户界面

为了高效管理菜单，一个可视化的拖放界面工具是非常有用的，它允许非技术背景的管理员也能便捷地管理和组织菜单结构。还要提供菜单配置文件的备份和恢复功能，以防在修改过程中发生错误需要回退到之前的版本。还必须确保菜单管理功能的自适应性，即菜单应该能够在不同的设备和屏幕尺寸上保持清晰和易用性，尤其是在移动设备上。

菜单名称	菜单编号	菜单排序	菜单图标	权限标识	组件路径	显示状态	菜单状态	创建时间	操作
+ 监控	2	2	💻			隐藏	禁用	2023-09-13 18:09:59	编辑 可见 禁用 +
故障	2097	2	⌚			显示	正常	2023-09-25 16:33:58	编辑 可见 正常 +
活动告警	2088	1	💻	faultManage/active-alarm/index	faultManage/active-alarm/index	显示	正常	2023-09-25 18:51:26	编辑 可见 正常 +
历史告警	2097	2	🕒	faultManage/history-alarm/index	faultManage/history-alarm/index	显示	正常	2023-10-07 16:01:36	编辑 可见 正常 +
故障通用设置	2098	3	💻	faultManage/fault-setting/index	faultManage/fault-setting/index	显示	正常	2023-10-07 16:50:01	编辑 可见 正常 +
+ 配置	4	3	🔧			显示	正常	2023-09-13 18:09:59	编辑 可见 正常 +
+ 性能	2099	5	⌚			显示	正常	2023-10-10 15:30:32	编辑 可见 正常 +
+ 报警	2083	6	⚠️			显示	正常	2023-09-22 18:46:48	编辑 可见 正常 +
+ 编辑	5	7	📝			显示	正常	2023-08-26 14:37:27	编辑 可见 正常 +
+ MML	2107	8	💻			显示	正常	2023-10-10 15:57:14	编辑 可见 正常 +
+ 日志	2089	9	🕒			显示	正常	2023-09-26 10:59:06	编辑 可见 正常 +

3.11.4 字典管理

字典管理功能是指系统管理员用于维护系统中各类预定义数据字典的工具。数据字典包含一组特定的标准值，它们在系统操作中起到标准化和规范化的作用，比如定义用户性别、菜单状态和任务状态等。这个功能是系统配置的关键部分，因为很多系统逻辑和用户接口都依赖于这些字典数据。

目前列出的 20 个字典提供了系统运行所需的基础数据结构，如下：

- **用户性别：** 包括了性别选项，比如男、女、不透露等。
- **菜单状态：** 确定菜单项是否可见、禁用等。
- **系统开关：** 包含系统功能的开启或关闭状态。
- **任务状态：** 任务执行的不同阶段，如待执行、执行中、已完成。
- **任务分组：** 用于将任务按组织或类别分类。
- **系统是否：** 一个通用的二选字典，通常有是和否两个选项。
- **操作类型：** 描述用户或系统可执行的操作类型。
- **系统状态：** 反映系统当前的运行状态。
- **跟踪类型：** 定义可能跟踪的活动或变更类型。
- **操作日志类型：** 用于分类不同的操作日志。

-
- **告警日志类型**: 归类告警日志条目。
 - **安全日志类型**: 定义有关安全事件的日志类型。
 - **网元软件版本状态**: 描述网络元素软件版本的状态。
 - **多语言-英文**: 管理系统支持的英文翻译字典。
 - **多语言-中文**: 管理系统支持的中文翻译字典。
 - **系统角色数据范围**: 确定角色在系统中数据访问的范围。
 - **活动告警类型**: 分类活动告警信息。
 - **告警清除类型**: 包括由谁、如何清除告警的类型。
 - **告警确认类型**: 似乎重复，请确认是否为其他类型，如“告警确认类型”。
 - **严重程度**: 定义问题的严重性等级。

同时，管理员应该能够对字典中的数据进行以下管理操作：

- **查看**: 显示字典内容。
- **导入**: 批量添加字典条目。
- **导出**: 备份字典数据。
- **搜索/过滤**: 快速找到特定的字典条目。
- **排序**: 根据需要调整字典项的顺序。
- **首页状态**: 可根据需要修改首页正常与异常网元的饼状图颜色

维护字典数据的完整性对于系统的稳定性和数据的一致性非常重要。此外，管理员往往需要确保对字典的修改有审计跟踪，以保持操作的透明性和可追溯性。

操作	创建时间	状态	类型	名称	编号
	2023-09-05 18:01:19		sys_user_sex	用户性别	1
	2023-09-05 18:01:19		sys_show_hide	菜单状态	2
	2023-09-05 18:01:19		sys_normal_disable	系统开关	3
	2023-09-05 18:01:19		sys_job_status	任务状态	4
	2023-09-05 18:01:19		sys_job_group	任务分组	5
	2023-09-05 18:01:19		sys_yes_no	系统是否	6
	2023-09-05 18:01:19		sys_notice_type	通知类型	7
	2023-09-05 18:01:19		sys_notice_status	通知状态	8
	2023-09-05 18:01:19		sys_oper_type	操作类型	9
	2023-09-05 18:01:19		sys_common_status	系统状态	10
	2023-09-06 10:35:58		trace_type	跟踪类型	100

3.11.5 参数设置

参数设置功能是任何核心网络系统管理的关键组成部分，此功能允许管理员配置和维护系统运行所依赖的各项参数。它的灵活性对于能够调整系统以适应组织的具体需求至关重要。参数可以分为几个主要类别：用户管理、系统设置和监控。

1、用户管理：

- 账号初始密码：** 定义用户创建账户时分配的默认密码。
- 密码最大错误次数：** 设置用户输入密码错误的最大尝试次数。
- 密码锁定时间：** 密码输入错误超过限制后，账号被锁定的时长。
- 账号自助-验证码开关：** 开启或关闭验证码功能，以增加登录安全性。
- 账号自助-是否开启用户注册功能：** 是否允许用户自行注册账号。

2、系统设置

- 官网链接：** 设置指向组织官方网站的链接。
- 系统使用文档：** 指定系统使用说明文档的存放位置或链接。
- LOGO 类型：** 选择系统 LOGO 的类型（例如 icon 或 brand）。
- LOGO 文件 icon：** 上传和管理用作系统图标的 LOGO 文件。
- LOGO 文件 brand：** 上传和管理用作品牌标识的 LOGO 文件。

- **登录界面背景:** 设置登录界面的背景图像或颜色。
- **系统名称:** 配置显示在界面上的系统名称。
- **版权声明:** 输入系统版权信息和声明文本。

3、监控

- **系统资源-数据保留时长:** 设定系统监控数据的保留时长。

对于这些参数，管理员通常需要以下功能：

- **修改和保存:** 更改参数值并保存更新。
- **权限管理:** 确保只有有相应权限的用户才能修改关键参数。
- **历史记录和跟踪:** 跟踪参数变更历史，对修改操作进行审计。
- **导入导出配置:** 允许管理员备份参数配置或从配置文件快速恢复参数设定。

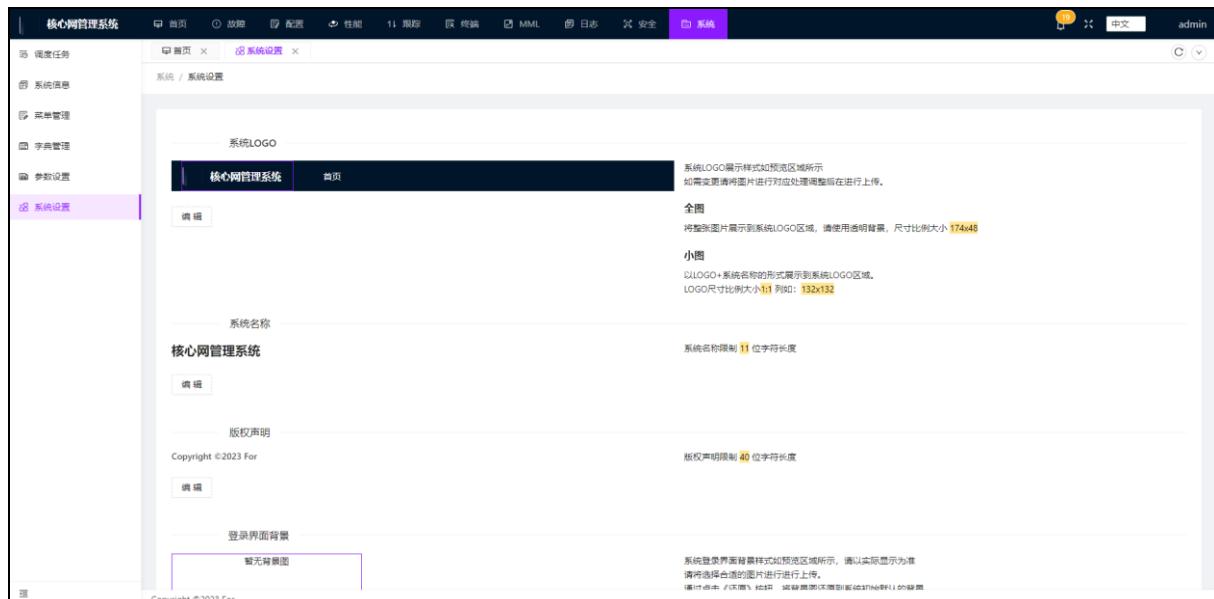
参数编号	参数名称	参数键名	参数键值	系统内置	创建时间	操作
1	用户管理-账号初始密码	sys.user.initPassword	Abcd@1234..	是	2023-09-05 18:01:19	
2	账号自助-验证码开关	sys.account.captchaEnabled	false	是	2023-09-05 18:01:19	
3	账号自助-是否开启用户注册功能	sys.account.registerUser	false	是	2023-09-05 18:01:19	
4	用户管理-密码最大错误次数	sys.user.maxRetryCount	5	是	2023-09-05 18:01:19	
5	用户管理-密码锁定时间	sys.user.lockTime	10	是	2023-09-05 18:59:01	
6	用户管理-授权有效时间	sys.user.expiresIn	120	是	2023-09-05 18:59:01	
7	用户管理-多端用户授权登录	sys.user.multi_login	true	是	2023-09-05 18:59:01	
10	监控-系统资源-数据保留时长	monitor.sysResource.storeDays	30	是	2023-10-28 16:56:10	
102	系统设置-LOGO类型	sys.logo.type	icon	是	2023-10-24 09:59:03	
103	系统设置-LOGO文件图标	sys.logo.filePathIcon	/upload/default/2023/11/左上角/logo_vbosqb.jpg	是	2023-10-24 10:02:15	
104	系统设置-系统名称	sys.title	核心网管理系统	是	2023-10-24 10:03:55	

3.11.6 系统设置

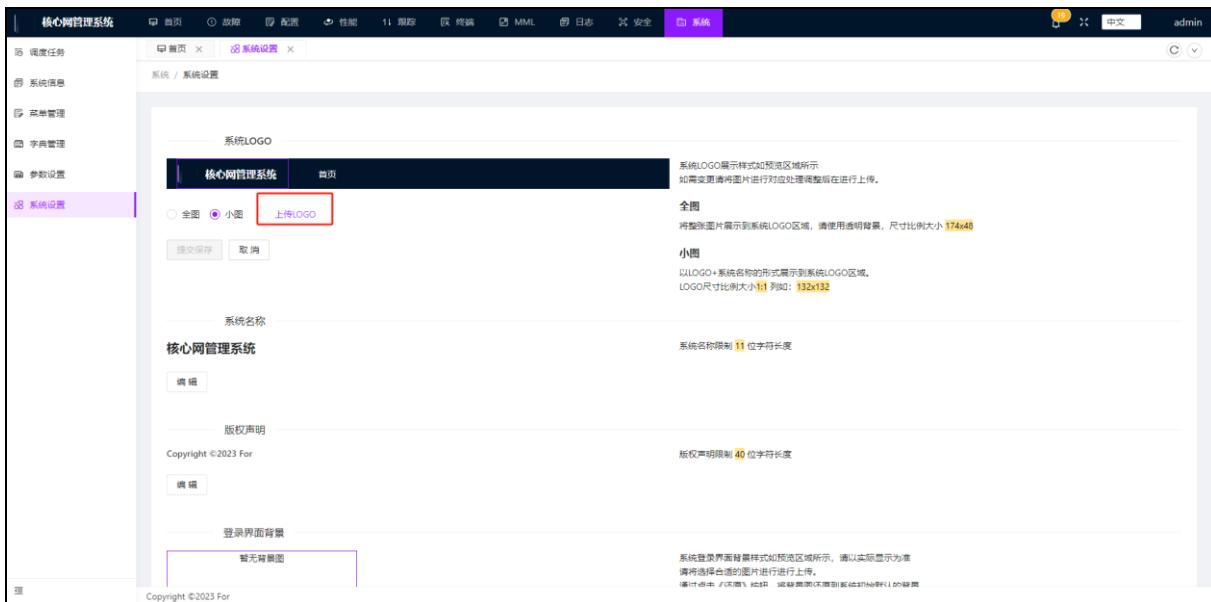
在网管操作系统中，“系统设置”是一个关键模块，它提供了一系列的配置选项，允许管理员对系统进行个性化调整，以适应特定需求和偏好。这些设置会影响到系统的外观、行为、访问权限和用户体验。管理员通常是唯一可以访问此部分的用户，以确保系统的稳定和安全。系统设置的目标是提供足够的灵活性，以便管理员可以在不影响总体性能和用户体验的前提下，调整和维护系统。

系统设置可以设置修改系统 LOGO，修改系统名称，版权声明，登录界面，系统使用文档及官网链接。

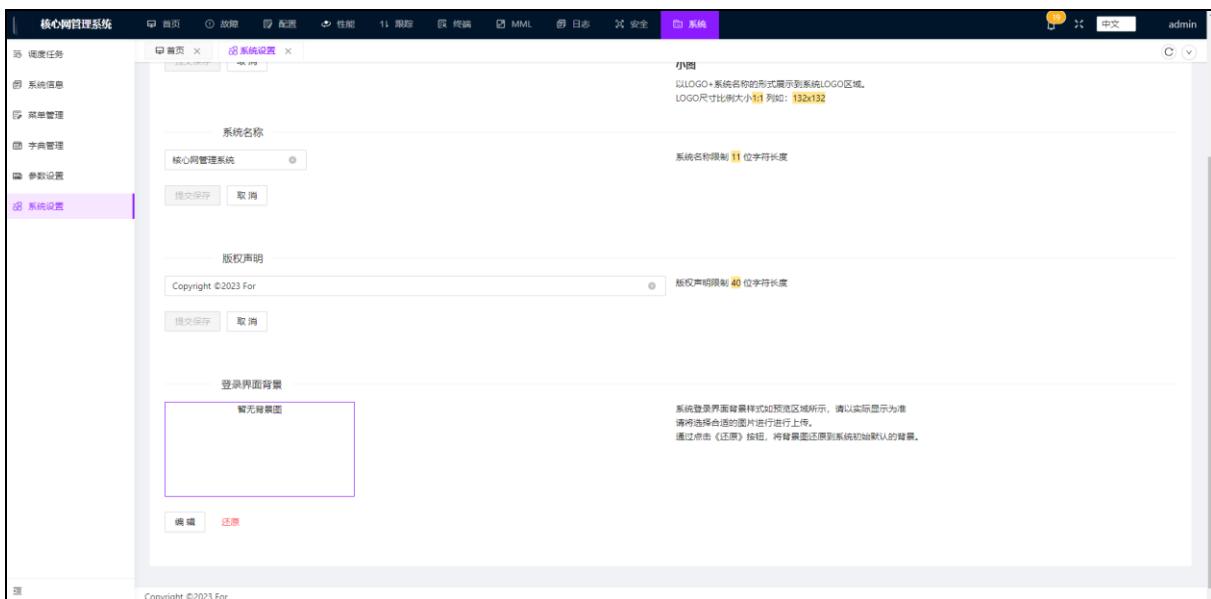
- **修改系统 LOGO:** 这个功能允许管理员上传一个新的 LOGO 图片，用来替换系统界面上现有的 LOGO。该功能通常会支持常用的图片格式（如. jpg, . png 等），并可能有图片尺寸和分辨率的要求，以确保新 LOGO 在不同设备和分辨率下的兼容性和视觉效果。
- **修改系统名称:** 这个选项允许管理员修改系统的显示名称，这个名称将会出现在浏览器的标题栏、登录界面、系统界面的顶部以及可能的系统通知邮件等地方。通过该设置，管理员可以将系统名称定制化以符合机构或企业的品牌。
- **版权声明:** 在这里，管理员可以编辑和更新系统底部的版权信息，以确保系统的版权声明是最新和准确的。它通常包含版权符号、年份和拥有版权的公司或个人的名称。
- **登录界面:** 系统设置可能会提供一些选项让管理员自定义登录界面的外观，例如更改背景图片或颜色、调整布局或添加额外的提示信息等。
- **系统使用文档及官网链接:** 管理员可以在这里设置系统使用手册文档的链接，以便用户能够直接通过系统访问。此外，如果有官方网站或支持社区，相关的链接也可以在该部分进行设置，方便用户访问。
- **国际化切换:** 管理员可以在这里设置国际化语言切换，设置是否显示国际化切换。



更改系统 logo：点击“上传”选择 logo 图片，然后点击“提交保存”即可更换 logo



修改系统名称，修改版权声明，修改登录界面背景：点击“编辑”修改后，再点击“提交保存”即可：



4 如何获得帮助

千通公司的技术支持及售后服务热线：15017928635

5 本软件系统售后服务的做法与原则

软件移交到用户后，我公司将依据合同条约进行支持和跟踪售后服务，未有约定的将依据国家相关产品的条例进行售后服务。

6 常见问题解答

序号	问题	解答
1	部分浏览器操作和显示异常	建议采用谷歌浏览器或者 Microsoft Edge (chromium 内核) 版本 清除浏览器缓存
2	网元无法添加成功	查看网元侧 oam 配置开关是否打开
3	核心网功能配置操作	见 5GC 维护手册

7 版权声明

本手册是我公司的知识版权，受法律保护，任何个人和公司不得进行非法盗版。手册所述核心网软件产品是我公司的知识版权，受法律保护，任何个人和公司不得进行非法盗版使用。