UZ801 LTE MiFi □密狗 — ADB 自动启用（主机端）

□宜的 ~$10 Qualcomm LTE MiFi 加密狗（`05c6:90b6`, "Android"/UZ801, msm8916）以 **RNDIS** 模式启动，具有位于 `http://192.168.100.1` 的网页 UI。获取 `http://192.168.100.1/usbdebug.html` 会将它们切换到 **ADB** 模式（并且它们已经是 root 权限）。参考: https://nickvsnetworking.com/adventures-with-a-10-lte-mifi-dongle/

启用步骤必须在 **USB** 主机（Proxmox 虚拟机监控器）上运行，因为只有主机与 `192.168.100.1` 之间有 RNDIS 链接 — OmniWeb 手机代理在无特权的 LXC（CT 102）中运行，并且仅在加密狗处于 ADB 模式时才能作为 USB 设备访问。因此，这个自动化是主机端的 udev + systemd，而不是代理代码。

文件

- `mifi-adb-enable.sh` → `/usr/local/sbin/mifi-adb-enable.sh` (0755)
- `mifi-adb-enable.service` → `/etc/systemd/system/mifi-adb-enable.service`
- `99-mifi-adb-autoenable.rules` → `/etc/udev/rules.d/99-mifi-adb-autoenable.rules`

```
sudo install -m0755 mifi-adb-enable.sh /usr/local/sbin/mifi-adb-enable.sh
sudo install -m0644 mifi-adb-enable.service /etc/systemd/system/mifi-adb-enable.service
sudo install -m0644 99-mifi-adb-autoenable.rules /etc/udev/rules.d/99-mifi-adb-autoenable.rules
sudo systemctl daemon-reload && sudo udevadm control --reload
```

流程：加密狗插入（RNDIS）→ udev 触发 → `mifi-adb-enable.service` → 脚本启动 RNDIS 接口，curl `usbdebug.html` → 加密狗重启进入 ADB 模式 → 重新枚举 ADB 接口 → CT-102 udev 规则（如下）将节点交给容器 → 代理的 `adb` 看到它。在 adb 模式重新枚举时，脚本再次运行，检测到 ADB 接口（`ff/42/01`）并退出 — 无循环。

伴随的 **CT-102 USB** 直通 **udev** 更改（必需）

加密狗的 Qualcomm VID `05c6` 必须交给容器，并且组 必须是 **plugdev**（主机 **gid 100046**），而不是容器 root，否则代理的 adb（用户 `omniweb-agent`，plugdev 成员）无法打开节点。Android 手机规则也是如此：它们的 `GROUP="100000"`（容器 root），代理无法访问 — 设备仅在 adb 持有枚举时的 fd 时有效，并在每次重新枚举时丢失。修复为 `GROUP="100046"`。

在 `/etc/udev/rules.d/99-ct102-android.rules` 中，所有手机规则使用 `OWNER="100000", GROUP="100046", MODE="0660"`，加上加密狗 VID：

```
SUBSYSTEM=="tty", SUBSYSTEMS=="usb", ATTRS{idVendor}=="05c6",
OWNER="100000", GROUP="100046", MODE="0660"
SUBSYSTEM=="usb", ATTR{idVendor}=="05c6", OWNER="100000",
GROUP="100046", MODE="0660"
```

> 这些主机更改在实验室中实时应用，但应该在 OmniCore ansible（监控/主机角色）中进行编码，以□在主机重建时生效。

AMF: 接入与移动管理功能

AMF 是 5G 核心的控制平面锚点。它终止与 UE 的 **N1** 信令以及与每个 gNodeB 的 **N2** (NGAP) 关联。它处理注册和连接管理：它附加 UE，使其保持可达，并在它们空闲时进行寻呼。它拥有 **UE** 上下文（每个注册用户一个，以 SUPI 为键）和 **gNB** 关联（每个连接的无线电一个，以 SCTP 关联为键）。它为每个 PDU 会话选择 SMF，并在 UE 和 SMF 之间中继会话请求。当订阅者在网络上时，AMF 是知道他们的位置和如何联系他们的 NF。

← 5G 核心

在仪表板中

AMF 仪表板打开时显示四个标准健康卡片：**API** 健康、**NRF** 注册（AMF 是否当前已注册到 NRF）、**NF** 状态和 许可证。每个卡片按间隔轮询。在它们下面，显示 AMF 拥有的数据：

- **UE** 列���: AMF 持有的每个 UE 上下文，以 SUPI 为键，包含其注册和连接状态。这是“当前谁已连接”的视图。选择一个 UE 以打开其详细上下文。AMF 还可以按 SUPI 列出 UE 的活动 PDU 会话。
- **gNodeBs**: 连接的无线电，每个 SCTP 关联一行。该表将原始 NGAP 值解码为可读的 **gNB-ID**、**TAC**（跟踪区域）、**PLMN** 和 **SST**（切片/服务类型）。因此，操作员可以确认哪些小区处于活动状态，以及它们服务的跟踪区域和切片，而无需手动解码标识符。选择一行以通过其 SCTP 关联 ID 打开详细的 gNB。

- 统计信息：AMF 的实时计数器（注册的 UE、连接的 gNB 和信令量），用于快速了解负载和活动情况。
- 维护模式：AMF 是否处于维护状态。使用它在计划工作期间排空或保持节点。
- 配置：服务当前使用的运行时配置。

操作

仪表板提供从卡住状态恢复的操作。仪表板在运行每个操作之前会确认，因为这些操作会清除实时状态：

- 清除所有 **UE** 上下文（批量）：从 AMF 中删除每个 UE 上下文。将其作为最后的手段，以恢复持有过时或损坏上下文的节点。每个受影响的 UE 必须重新注册。
- 清除缓存（批量）：清除 AMF 的 NF 发现缓[illegible]和 UE 缓存。使用它当 AMF 在过时的对等或查找数据上操作时，例如在 NF 移动或重新注册后。
- 注销（每个 UE）：注销单个 UE 并清理其状态。使用它来删除一个订阅者的上下文，该上下文不会自行清除，而不是重置整个节点。

除了仪表板按钮，AMF 的 OAM API 还提供更细粒度的恢复控制，操作员可以通过后端代理访问：

- 强制断开 **gNB**：通过其 SCTP 关联 ID 拆除单个 gNB。使用它来清除卡住或行为不当的无线电关联，而不影响其他关联。
- 强制释放 **PDU** 会话：通过其 `supi:psi` 标识符释放一个 PDU 会话。使用它来删除在 AMF 端卡住的会话，同时 UE 保持注册状态。
- 注销或寻呼 **UE**：强制 UE 注销，或寻呼空闲 UE 以使其重新连接。使用寻呼测试可达性。使用强制注销干净地驱逐 UE。

操作

- 运行时诊断（`/api/oam/diagnostics`）：显示正在运行的服务的低级诊断信息。
- 资源使用情况（`/api/oam/resources`）：报告运行时的内存、进程和调度程序使用情况，以检查节点的健康状况。
- 对等体（`/api/oam/peers`）：列出配置和发现的 NF 对等 URI 以及当前的 SCTP 关联，以[illegible]操作员可以看到 AMF 与谁通信。
- **NRF** 发现缓存（`/api/oam/nrf_discovery`）：显示发现缓存的内容：AMF 从 NRF 学到的 NF 实例。
- 设置日志级别（`/api/oam/log_level`）：在运行时更改日志级别（`emergency`、`alert`、`critical`、`error`、`warning`、`warn`、`notice`、`info`、`debug` 之一），以在故障排除时提高详细信息。
- 强制 **NRF** 重新注册（`/api/oam/nrf/reregister`）：重新注册 AMF 与 NRF。使用它来恢复丢失或过时的注册。

相关

SMF: 会话管理功能: AMF 选择 SMF 并将 PDU 会话请求中继给它。 UDM: 统一数据管理: AMF 在注册过程中使用的订阅者数据。
AUSF: 认证服务器功能: 代表 AMF 在注册过程中对 UE 进行认证。 NSSF: 网络切片选择功能: 为 AMF 解决切片选择。
← 5G 核心: 所有 NF 仪表板的概述。

AUSF: 认证服务器功能

AUSF 代表 AMF 对用户进行认证。当 UE 连接时，AMF 会要求 AUSF 为该用户运行 5G-AKA（或 EAP-AKA'）。AUSF 与 **UDM** 配合以获取密钥材料，推导出返回给 AMF 的锚定密钥，并确认认证结果。它为每个进行中或已建立的认证保持一个活动认证会话，以□运营商可以跟踪其进展和结果，并在需要时清除它。

← 5G 核心

在仪表板中

AUSF 仪表板顶部打开时显示标准健康卡（**API** 健康、**NRF** 注册（AUSF 是否已在 NRF 注册？）、**NF** 状态和 许可证），每个卡片按间隔轮询。它们下方是 AUSF 的数据部分，通过 OmniWeb 代理实时从其 OAM API 读取：

- 统计：AUSF 自己的计数器（`AUSF Statistics`），提供认证活动的实时视图。
- 活动 **AUSF** 认证会话：AUSF 当前持有的认证会话列表（`List Active AUSF Authentication Sessions`）。每行通过其会话标识符进行键控，以□运营商可以一目了然地查看哪些认证正在进行或已建立。

□□

□□□

BSF: 绑定支持功能

BSF 注册并解析 UE 的 PDU 会话与服务它的 PCF 之间的绑定。当会话建立时，BSF 记录哪个 PCF 正在处理该会话的策略，使用会话的标识符作为键：UE IP 地址、DNN 和 S-NSSAI。其他 NFs 和应用功能随后查询 BSF，以发现给定 UE 会话的正确 PCF，以□策略请求能够到达已经持有该会话上下文的 PCF，而不是任意的 PCF。BSF 每个活动 PDU 会话保持一个绑定，并将其与摘要统计信息一起公开，以□监控。

← 5G Core

在仪表板中

BSF 仪表板打开时，顶部有标准健康卡（**API** 健康、**NRF** 注册（BSF 是否已在 NRF 注册？）、**NF** 状态和 许可证），每个卡片按间隔轮询。在它们下面是 BSF 的数据部分，通过 OmniWeb 代理实时读取其 OAM API：

- **PCF** 绑定：BSF 当前持有的活动绑定列表（`List all PCF bindings with binding ID, UE IP, DNN, S-NSSAI, PCF FQDN/IP`）。每一行以其绑定 ID 为键，显示识别会话的 UE IP 地址、DNN 和 S-NSSAI，以及服务该会话的 PCF 的 FQDN 或 IP。这一部分可以一目了然地回答“哪个 PCF 正在处理该 UE 会话的策略？”选择一个绑定以打开其完整详细信息（`Get detailed PCF binding by binding ID`）。

- 统计信息：BSF 自身的计数器（`BSF statistics: total bindings, bindings by DNN`），提供了当前活动绑定的总数以及按 DNN 细分的情况。

操作

BSF 仪表板以读取和监控为导向。它展示绑定和统计信息以供检查，并不公开逐行或 NF 级别的破坏性清除操作。

操作

BSF 上可用的标准 OAM 控制：

- 强制 **NRF** 重新注册（`/api/oam/nrf/reregister`）：使 BSF 重新注册到 NRF，以□在其注册失效时恢复。

相关

- PCF: 策略控制：每个绑定指向的 NF。BSF 是消费者找到 UE 会话正确 PCF 的方式。
- SMF: 会话管理 和应用功能：Nbsf 消费者在会话进出时注册和查找绑定。
- ← 5G Core：5GC 仪表板概述和其他 NFs。

CHF：充电功能

CHF（充电功能）为5G核心提供了在线和离线充电的融合。SMF通过N40接口使用它：随着PDU会话承载流量，CHF管理使用配额，通过计费/充电引擎对其进行计费，并生成供计费和对账使用的CDR（充电数据记录）。其仪表板显示实时充电会话、与计费引擎的链接健康状况以及已完成的CDR历史。运营商可以在不离开OmniWeb的情况下回答“订阅者是否被正确计费，计费引擎是否可达？”的问题。

← 5G核心

在仪表板中

顶部是标准的健康卡（**API**健康、**NRF**注册（CHF是否已在NRF注册？）、**NF**状态和许可证），每个卡片按时间间隔轮询。在它们下面，CHF特定的数据部分会自动刷新：

- 活动充电会话：CHF正在计量的实时会话，每个会话显示其充电参考（`chargingDataRef`）、订阅者（SUPI）、DNN、累计使用量和开始/更新时间戳。这是“当前正在被收费的用户”的工作集。
- 统计信息：总会话、与计费/充电引擎的连接性和总计费量的摘要视图。
- 计费引擎连接健康：专门的健康检查，确认CHF可以到达执行实际计费的计费/充电引擎。如果此项不健康，CHF将无法对会话进行计费，充电将面临风险。
- 已完成**CDR**搜索：对最终CDR的可搜索视图，可按SUPI、DNN和日期范围进行过滤，以确认CHF在会话结束后记录的内容。

- 配置：CHF当前看到的运行时配置。

选择一个会话以通过充电数据参考打开其完整详细信息，显示该会话的完整使用和计量状态。

操作

- 中止充电会话：通过其`chargingDataRef`终止正在进行的充电会话。使用此功能清除SMF不再维护的卡住或孤立的会话，以□停止消耗配额和计量状态。
- 搜索**CDR**：按SUPI、DNN和日期范围查询已完成的CDR历史。在会话结束后使用此功能确认CHF计费和记录的使用情况。它支持计费查询、争议调查或对CHF正确写入充电的抽查。

操作

- 设置日志级别：在运行时更改CHF的日志详细程度（紧急、警报、关键、错误、警告、���意、信息、调试），以□在调查充电问题时收集更多详细信息，然后返回正常。
- 强制**NRF**重新注册：使CHF重新向NRF注册。使用它来恢复如果CHF已从注册表中掉出，SMF无法再发现它的情况。

相关

- SMF：作为PDU会话承载流量的N40消费者，驱动充电。
- PCF：管理CHF计量的政策和充电控制的政策方面。
- 计费/充电引擎（OCS）：CHF通过其进行计费的下游系统。计费引擎连接健康卡反映与其的链接。
- ← 5G核心：所有NF仪表板的概述。

NRF: 网络注册功能
整个5G核心围绕NRF注册表构建。在启动时，每个NF都会向NRF注册其NF配置文件：其类型、地址、PLMN、它提供的服务以及其容量和优先级。然后，它通过询问NRF可用的同伴来发现其对等体。NRF跟踪每个注册实例的状态。它持有状态变化订阅，因此可以在其依赖的对等体出现或消失时通知NF。它监控心跳以使停止检查的实例过期。当任何NF需要找到另一个时，NRF是关于什么是可用的以及如何到达它的真实来源。

← 5G核心

在仪表板中

NRF有自己专用的仪表板，比标准NF页面更丰富，因为它拥有其他核心通过的注册表。它以标准健康卡片打开：API健康、NRF注册（NRF本身是否已注册）、NF状态和许可证。每个卡片按间隔轮询。

在数据上方，它显示四个指标卡，总结注册表：NF类型、总实例、已注册（带有总百分比条）和服务（带有订阅计数）。它们下方是NRF的核心视图：

注册的NF实例：每个注册实例，按NF类型（AMF、SMF、UDM、PCF等）分组。仪表板通过类型对每个实例卡片进行颜色编码。卡片显示其注册状态、心跳计时器、服务计数和PLMN。选择一个实例以打开其完整的NF配置文件：NRF持有的详细记录，带有指

向该NF自己页面的打开仪表板链接和注销按钮。这是“哪些NF是可用的，它们都已注册吗？”的视图。

- 注册的服务：每个实例广告的每个服务的平面表，带有其版本和状态。因此，操作员可以查看核心当前在所有NF中提供的能力。
- 订阅：当前持有的NF状态变化订阅。每个都是NF的持续请求，以在对等体的状态变化时收到通知。
- 统计：NRF的实时计数器：按类型的总NF、订阅和发现请求，以快速了解注册表的大小和查找活动。

操作

仪表板提供管理注册表的操作。仪表板在运行每个操作之前会确认，因为它会实时更改注册状态：

- 注销**NF**实例（逐行）：从NRF中移除一个实例的注册。使用它来清除单个NF的过��或卡住的注册。该NF必须在其他NF可以再次发现它之前重新注册。
- 注销所有**NF**（批量）：一次性从NRF中移除每个注册。作为最后手段使用，以重置持有过时条目的注册表。每个NF必须重新注册。
- 移除订阅：删除一个状态变化订阅。使用它来清除一个不再需要的NF留下的过时或孤立的订阅。
- 更新**NF**配置文件：修补注册实例的配置文件（例如其容量、优先级或状态）。因此，操作员可以调整NRF如何引导发现朝向或远离一个实例，而无需注销。

操作

NRF的OAM API提供了操作员可以通过后端代理访问的进一步控制：

- 运行时诊断（`/api/oam/diagnostics`）：显示正在运行的服务的低级诊断。
- 资源使用（`/api/oam/resources`）：报告运行时的内存、进程和调度程序使用情况，以进行节点的健康检查。
- 手动心跳检查（`/api/oam/heartbeat`）：触发NF实例的按需心跳检查。它确认NF是否仍然存活，而不是等待其计时器。
- **NF**正常运行时间（`/api/oam/nf_uptime/{id}`）：显示实例的注册时间以及它已注册的时间，以确认NF已运行多长时间。
- 设置日志级别（`/api/oam/log_level`）：在运行时更改日志级别（`emergency`、`alert`、`critical`、`error`、`warning`、`warn`、`notice`、`info`、`debug`之一），以在故障排除时提高详细程度。
- 强制**NRF**重新注册（`/api/oam/nrf/reregister`）：重新注册NRF。使用它来恢复丢失或过时的自我注册。

相关

- AMF: 接入与移动管理功能：向NRF注册并通过它发现其对等体，像下面的每个NF一样。
- SMF: 会话管理功能：通过NRF发现以进行会话管理。

UDM: 统一数据管理: NRF持有注册的订户数据NF之一。
PCF: 策略控制功能: 向NRF注册以进行策略发现。
SCP: 服务通信代理: 使用NRF持有的注册和发现数据在NF之间路由信令。 ← 5G核心: 所有NF仪表板的概述。

NSSF: 网络切片选择功能

NSSF 选择网络切片实例和 UE 允许的 NSSAI。当 AMF 处理注册或切片请求时，它会请求 NSSF 根据为该 PLMN 配置的切片解析 UE 请求的 S-NSSAIs。NSSF 将每个 S-NSSAI 映射到其网络切片实例 (NSI) 和为其服务的 AMF 集，并返回 UE 可以使用的允许 NSSAI。它持有配置的切片定义，并跟踪每个 AMF 的 NSSAI 可用性，以□运营商可以推理和监控切片选择。

← 5G 核心

在仪表板中

NSSF 仪表板打开时，顶部显示标准健康卡（**API** 健康、**NRF** 注册（NSSF 是否已向 NRF 注册？）、**NF** 状态和 许可证），每个健康卡按间隔轮询。它们下方是 NSSF 的数据部分，通过 OmniWeb 代理实时读取其 OAM API：

- 切片：每个配置的 S-NSSAI，列出其 NSI 映射、为其服务的 AMF 集以及每个 PLMN 的���许 NSSAI（`List all configured S-NSSAIs with NSI mappings, AMF sets, and allowed NSSAI per PLMN`）。这是请求的切片如何解析为每个 PLMN 的切片实例和 AMF 集的权威视图。
- **NSSAI** 可用性：每个 AMF 的 NSSAI 可用性状态（`Per-AMF NSSAI availability state`），显示每个 AMF 报告的当前可以服务的切片。

- 统计信息：NSSF 自己的计数器（`NSSF statistics: total slices, NS selection request counts`），提供配置切片数量和切片选择请求量的实时视图。

一个单独的 切片配置 视图（`Query Slice Configuration`）显示 NSSF 的运行时切片配置以供参考。

操作

NSSF 仪表板以读取和监控为导向。它显示切片、NSSAI 可用性和统计信息，而没有逐项控制操作。

操作

OAM 控制 NSSF 暴露的操作包括：

- 查看运行时配置（`/api/oam/config`）：NSSF 的实时运行时配置。
- 强制 **NRF** 重新注册（`/api/oam/nrf/reregister`）：使 NSSF 重新向 NRF 注册，以□在其注册失效时恢复。

相关

- AMF: 接入与移动管理：查询 NSSF 将请求的 S-NSSAIs 解析为允许的 NSSAI 和为 UE 服务的 AMF 集。
- NRF: 网络存储库功能：NSSF 注册的地方，以□其他 NF 可以发现它。
- ← 5G 核心：5GC 仪表板概述和其他 NF。

PCF: 策略控制功能

PCF 负责做出其余 5G 核心所执行的策略决策。它通过 N15 向 AMF 回应 接入与移动 **(AM)** 策略：UE 在注册时获得的移动限制和 RFSP。它通过 N7 向 SMF 回应 会话管理 **(SM)** 策略：设置每个会话的 QoS、门控、计费控制和使用监控的 PCC 规则。PCF 通过 BSF 将 UE 的 SM 策略关联绑定回自身，以□任何 NF 都可以找到适合会话的正确 PCF。PCF 仪表板是回答“哪些策略是活动的，适用于哪些 UE 和会话，它们是否符合我的预期？”的地方，无需离开 OmniWeb。每个 OAM 响应都被包装为 `{status, response}`，仪表板会为您解包。

← 5G 核心

在仪表板中

顶部有四个标准健康卡（**API** 健康、**NRF** 注册（PCF 是否已在 NRF 注册？）、**NF** 状态和 许可证），每个卡片都在一个时间间隔内轮询。使用��题中的轮询指示器来暂停刷新或查看最后更新时间。卡片下方是 操作 栏（见下文），然后是 PCF 的数据部分，每个部分都在自动刷新。

统计信息：PCF 的实时计数器（`GET /api/statistics`），策略关联总数和当前计数。这是判断 PCF 是否积极提供 AM 和 SM 策略的最快方式。

AM 策略：每个活动的 AM 策略关联（`GET /api/am_policy`），每个 AMF 有 AM 策略的 UE 一行。这是 PCF 当前应用于每个注册 UE 的移动策略视图。

SM 策略：每个活动的 SM 策略关联（`GET /api/sm_policy`），每个 SMF 持有策略的 PDU 会话一行。选择一行以打开其详细信息（`GET /api/sm_policy/{id}`），返回该会话的完整 PCC 规则：SMF 执行的 QoS、门控、计费和使用监控决策。

策略上下文：活动策略上下文视图（`GET /api/policy_context`），PCF 在其 AM 和 SM 关联中持有的上下文。这对于调和 PCF 认为是活动的内容与 AMF 和 SMF 之间的差异非常有用。

配置：PCF 的运行时配置（`GET /api/oam/config`），服务当前运行的设置。

操作

每个行操作首先要求确认，因为删除活动关联会对其影响的 UE 或会话造成干扰。

移除 **AM** 策略：在任何 AM 策略行上，移除 删除该 AM 策略关联（`DELETE /api/am_policy/{id}`）。使用它来清除一个 UE 的卡住或过时的移动策略。

移除 **SM** 策略：在任何 SM 策略行上，移除 删除该 SM 策略关联（`DELETE /api/sm_policy/{id}`）。使用它来删除一个不会自行清除的会话策略。

更新 **SM** 策略：您还可以编辑 SM 策略关联。发送 `PATCH` 或 `PUT /api/oam/sm_policy/{id}` 来更新活动 SM 策略中的 PCC 规则，以□您可以调整会话的 QoS 或计费决策，而无需拆除关联。使用它来重新驱动策略到现有会话，而不是删除并重新创建它。

操作

操作部分包含每个 NF 通用的控制：

- 诊断（`GET /api/oam/diagnostics`）：服务的运行时诊断。
- 资源使用（`GET /api/oam/resources`）：运行服务的内存、进程和调度程序。
- 对等体（`GET /api/oam/peers`）：PCF 交谈的配置 NF 对等 URI 及其可达状态。
- **NRF** 发现缓存（`GET /api/oam/nrf_discovery`）：NRF 发现缓存，或 PCF 通过其解析对等体的配置 NF URI。
- 日志级别（`POST /api/oam/log_level`）：在运行时更改日志级别。选择紧急、警报、关键、错误、警告、注意、信息或调试之一。

- **NRF** 重新注册 (`POST /api/oam/nrf/reregister`): 强制 PCF 重新注册到 NRF，例如在 NRF 重启后使其失效。

相关

- SMF: 通过 N7 向 PCF 请求 SM 策略并执行 PCF 返回的 PCC 规则。
- AMF: 通过 N15 向 PCF 请求 AM 策略。
- BSF: PCF 注册 SM 策略关联的绑定功能，以□任何 NF 都可以找到提供服务的 PCF。
- CHF: 计费功能。PCF 的计费控制决策驱动 SMF 通过 N40 报告的内容。
- ← 5G 核心概述

SCP：服务通信代理

SCP 位于 5G 核心的网络功能之间，并为它们承载基于服务的流量。与其让每个消费者 NF 直接连接到每个生产者，不如通过 SCP 路由请求，SCP 将每个消息转发到目标 NF 类型的健康实例，进行负载均衡并在失败时重试。它可以代表消费者执行发现（委托发现），并缓存 NF 可达性，因此一旦知道目标类型，它就可以在后续请求中引导而无需重新查找。结果是间接通信：生产者和消费者不需要相互了解或保持连接，SCP 处理路由、负载均衡和缓存新鲜度。

← 5G 核心

在仪表板中

SCP 仪表板遵循与每个 5GC NF 页面相同的布局。四个 健康卡 横跨顶部（**API** 健康、**NRF** 注册（SCP 本身是否已在 NRF 注册？）、**NF** 状态和 许可证），每个卡片按间隔轮询。

在卡片下方，SCP 显示其自身的操作数据

- **NF** 健康：负载均衡器对其代理的 NFs 的视图，包含每个实例的健康和失败计数，以操作员可以查看 SCP 认为可达的生产者实例以及哪些实例出现故障。

- 发现缓存：SCP 的发现缓存内容，缓存了哪些 NF 类型、它们的 TTL 以及缓存命中/未命中率。这使得 SCP 能够在不重新发现的情况下引导重复请求。
- 统计信息：SCP 吞吐量、总代理请求、按目标 NF 类型的请求细分以及整体缓存命中率。
- 配置：SCP 当前的运行时配置。

每个部分会自动刷新，NF 类型值与该 NF 的仪表板交叉链接。

操作

SCP 仪表板不暴露破坏性 NF 级别或每行操作按钮。它代理流量而不是拥有操作员会清除的会话或订阅状态。然而，它的缓存是可管理的：OAM API 允许操作员查看发现缓存并驱逐单个过期条目，以 SCP 在下一个请求时重新发现该目标（见 操作）。要从已移动或被替换但仍被缓存为可达的生产者中恢复，请清除其条目。

操作

SCP 的 OAM API 暴露以下控制：

- 查看/管理发现缓存：读取当前发现缓存，并通过 id 删除单个缓存条目以强制重新发现该目标。
- 查看运行时配置：读取 SCP 的实时配置。
- 设置日志级别：在运行时更改日志详细程度。选择 `emergency`、`alert`、`critical`、`error`、`warning`、`warn`、`notice`、`info` 或 `debug` 之一。
- 强制 **NRF** 重新注册：使 SCP 重新注册到 NRF。这在 NRF 或 SCP 重启后，注册已过期时非常有用。

相关

- NRF：SCP 通过其发现并重新注册的注册表。
- AMF、SMF、UDM、AUSF、PCF、CHF、NSSF、BSF：SCP 可以代理其基于服务的流量并缓存其可达性的 NFs。
- ← 5G 核心：5GC 部分概述和共享仪表板布局。

SMF: 会话管理功能
SMF 拥有 PDU 会话。它建立、修改和释放每个 UE 的数据会话，从本地池中分配 UE 的 IP 地址，并通过 N4/PFCP 驱动用户平面。它为每个会话编程 UPF 的数据包检测、转发和 QoS 规则。它还与 PCF (N7) 进行会话策略的交互，并与 CHF (N40) 进行计费的交互。使用 SMF 仪表板回答“会话是否正在建立，SMF 是否仍与其 UPF 关联，以及是否快用完地址？”而无需离开 OmniWeb。SMF 将每个 OAM 响应包装为 {status, response}。仪表板会为您解包。

← 5G 核心

在仪表板中

顶部有四个标准健康卡：API 健康、NRF 注册（SMF 是否已注册到 NRF？）、NF 状态和 许可证。每个卡片都按间隔轮询。使用标题中的轮询指示器暂停刷新或读取最后更新时间。卡片下方是 操作 栏（见下文）。然后是 SMF 的数据部分，每个部分都自动刷新。

统计信息：SMF 的实时计数器 (GET /api/statistics): 会话建立/修改/释放总数和当前会话计数。这是判断 SMF 是否实际建立会话的最快方式。

PDU 会话：每个活动的 PDU 会话 (GET /api/pdu_session)，返回为 { pdu_sessions: [...], total }。每行包含一个 sm_context_ref（唯一标识 SM 上下文的 UUID）和一个 pdu_session_id

（3GPP PSI，一个小整数，在 UE 之间不唯一，因为每个 UE 从低基数编号其会话）。因此，每个会话操作（详细查找和释放）都以 `sm_context_ref` 为键。仪表板的每行 释放 操作传递该 UUID 而不是 PSI。除了标识符外，行中显示会话的 DNN、分配的 UE IP 和状态。

IP 池：SMF 从中分配 UE IP 的地址池（`GET /api/ip_pool/detail`）：池摘要（子网、总数、已分配和可用计数）以及当前已分配 IP 的列表。在这里，您可以看到 SMF 是否接近耗尽其地址空间。

UPF 关联：用户平面的 N4/PFCP 链路状态（`GET /api/upf`）：SMF 是否当前与其 UPF 关联。如果会话无法建立，请首先检查此项。

PFCP 对等体：PFCP 对等体（UPF）关联状态（`GET /api/oam/pfcp_peers`）：SMF 与每个通过 N4 关联的 UPF 的视图，包括关联状态。

操作

每个操作首先请求确认。多个操作会对活动会话造成破坏。

释放所有 **PDU** 会话：拆除每个 PDU 会话及其在 UPF 上的 PFCP 状态。使用此操作将 SMF 清理回干净状态，例如在 UPF 交换后或当您为维护排空节点时。

清除缓存：在不释放会话的情况下清除 SMF 的会话缓存。当仪表板或 SMF 的内部视图看起来过时或与现实不一致时使用。

PFCP 重新关联：重新建立与 UPF 的 PFCP 关联（SMF 发起）。当 UPF 关联已断开且新会话无法建立时使用。

重新关联 **UPF**：强制与配置的 UPF 进行 PFCP 重新关联。UPF 地址由配置驱动。这里没有 add-UPF 或 inject-UPF 操作。此操作将关联重新驱动到 SMF 配置中已存在的 UPF。实际上，它的恢复目的与 PFCP 重新关联相同。

按 **DNN** 释放：在可编辑的 **DNN** 字段中输入 DNN（例如 `internet`）。这将释放该 DNN 上的所有会话。使用此操作来排空或重置单个数据网络，例如强制 UE 退出一个 APN/DNN，而不影响其他 DNN 上的会话。

逐行释放：在任何 PDU 会话行上，释放 将拆除该会话及其在 UPF 上的 PFCP 上下文。它通过 `sm_context_ref` 释放，因此它始终精确针对该行中的会话，即使多个 UE 可能共享相同的 `pdu_session_id`。使用此操作来删除单个卡住的会话。

操作

操作部分包含每个 NF 通用的控制：

- 诊断（`GET /api/oam/diagnostics`）：服务的运行时诊断。

资源使用 (GET /api/oam/resources): 正在运行的服务的内存、进程和调度程序。
对等体 (GET /api/oam/peers): SMF 与之通信的配置 NF 对等体 URI（AMF、PCF、CHF、NRF，
以及通过上面的 PFCP 对等体与其 PFCP UPF 对等体）。
日志级别 (POST /api/oam/log_level): 在运行时更改日志级别。选择紧急、警报、关键、错误、警告、注意、信息或
调试之一。
NRF 重新注册 (POST /api/oam/nrf/reregister): 强制 SMF 重新注册到 NRF，例如在 NRF 重
启后使其过时。

相关

AMF: 通过 Nsmf 向 SMF 请求会话设置。
PCF: 通过 N7 向 SMF 提供会话策略。
CHF: SMF 通过 N40 报告使用情况的计费功能。
UPF: SMF 的 N4/PFCP 对等体。它是 SMF 编程和关联的用户平面。
← 5G 核心概述

UDM：统一数据管理

UDM 是 5G 核心的订阅数据权威。它管理每个订阅者的订阅配置文件。它跟踪每个 UE 由哪个服务 NF 处理，并针对订阅者注册 AMF 和 SMF。它提供用于挑战 UE 的认证数据。它从 **UDR** 中读取基础的订阅者记录，这是它的后端存储，并将其缓存以□快速查找。**AMF** 在注册期间咨询它。**SMF** 在会话设置期间咨询它。**AUSF** 从中提取其认证材料。当其他 NF 需要了解订阅者的配置文件或网络为他们提供服务的位置时，UDM 是回答的 NF。

← 5G 核心

在仪表板中

UDM 仪表板打开时显示四个标准健康卡：**API** 健康、**NRF** 注册（UDM 是否当前已注册到 NRF）、**NF** 状态和 许可证。每个卡片按间隔轮询。在它们下面，显示 UDM 拥有的数据：

- **UE** 列表：UDM 持有的每个 UE 上下文，以 SUPI 为键。这是“UDM 当前服务的订阅者”视图。UDM 还可以通过 SUPI 返回单个订阅者���详细上下文。它显示该订阅者的服务 NF 注册和缓存的订阅数据。
- 统计信息：UDM 的实时计数器，用于快速了解负载和活动。
- 配置：服务当前使用的运行时配置。

□□

□□□

UDR：统一数据存储

UDR 是一个持久的订阅、策略和应用数据存储，位于 UDM 和 PCF 之后。UDM 和 PCF 是其他网络功能（NF）交互的前端网络功能，而 UDR 是它们读取和写入的数据库。它是关于订阅者身份及其权益的唯一真实来源。在 OmniCore 中，UDR 与 **HSS** 共享其订阅者存储，因此一个统一的存储库同时保存 4G 和 5G 订阅者，而不是两个平行数据库。

← 5G 核心

在仪表板中

UDR 仪表板以标准的 NF 健康卡片打开，位于顶部（**API** 健康、**NRF** 注册（UDR 是否已在 NRF 注册？）、**NF** 状态和 许可证），每个卡片按间隔轮询。

卡片下方是两个 UDR 特定的数据部分：

- **HSS** 健康：一个连接健康检查，确认 UDR 可以访问它前端的共享 HSS 订阅者存储。这一部分可以一目了然地回答“订阅者数据库是否可达且健康？”。
- 订阅者：从 HSS 提取的订阅者列表，支持分页和通过 **IMSI** 搜索。选择一个订阅者以返回该 IMSI 的完整订阅者详细信息，以□操作员可以在不离开 OmniWeb 的情况下确认订阅者的配置。

操作

UDR 仪表板不暴露任何破坏性的 NF 级或逐行操作。它是对共享订阅者存储的读取和查找视图。它的价值在于查询：检查通过 HSS 健康部分是否可以访问存储，列出订阅者，并通过 IMSI 深入查看任何一个订阅者的完整详细信息。

操作

在数据部分旁边，UDR 执行每个 5GC 网络功能共同的操作：

- 设置日志级别：通过 `/api/oam/log_level` 提高或降低运行时日志的详细程度（`emergency`、`alert`、`critical`、`error`、`warning`、`warn`、`notice`、`info`、`debug`），以□在诊断问题时增加详细信息。
- 强制 **NRF** 重新注册：如果其注册已过期，则推动 UDR 重新注册到 NRF（`/api/oam/nrf/reregister`）。
- 查看运行时配置：通过 OAM 配置端点检查 UDR 的实时配置。

相关

- UDM: 统一数据管理：从这个存储中提供订阅数据的前端网络功能。
- PCF: 策略控制功能：读取保存在 UDR 中的策略数据。
- HSS: UDR 统一的共享订阅者数据库，因此 4G 和 5G 订阅者存储在一个存储库中。
- ← 5G 核心：完整的 5GC 仪表板概述。

API 参考（OpenAPI / Swagger）

OmniWeb 的控制器（中央后端）通过同一个 JWT 登录暴露了一个单一的 REST API，该登录控制着门户的其余部分。该 API 是自文档化的：

- **Swagger UI：** `/api/docs`。浏览每个端点。展开一个路由以查看其方法、路径/查询参数、是否需要令牌以及其摘要。点击 **Authorize** 并粘贴一个 Bearer JWT，以□实时尝试对运行实例的调用。
- **OpenAPI 3 规范：** `/api/openapi.json`。这是机器可读的文档。使用它导入到 Postman/Insomnia 或生成客户端。

← 返回操作指南

文档内容

该规范是 在运行时生成的，通过对实时路由图的反射，因此它始终与运行实例实际提供的端点匹配。没有手动维护的文件会漂移。对于每个路由，它捕获：

- HTTP 方法和路径（带有路径/查询参数），
- 从代码中提取的摘要和描述，

- 是否需要 **bearer JWT**，以及
- 在适用的情况下，路由强制执行的每个元素的 视图/控制 权限。

端点按区域分组（Auth、Admin、SIM Bank、Remote SIM、APDU、Test Devices、IR.38、RAEX、TAP 等），因此您可以快速找到功能的路由。

获取令牌

大多数端点需要一个 Bearer 令牌。使用 `POST /api/auth/login` 获取一个（与您用于门户的相同凭据），然后将其作为 `Authorization: Bearer <token>` 发送。在 Swagger UI 中，使用 **Authorize** 按钮，以每个“尝试一下”调用自动携带令牌。

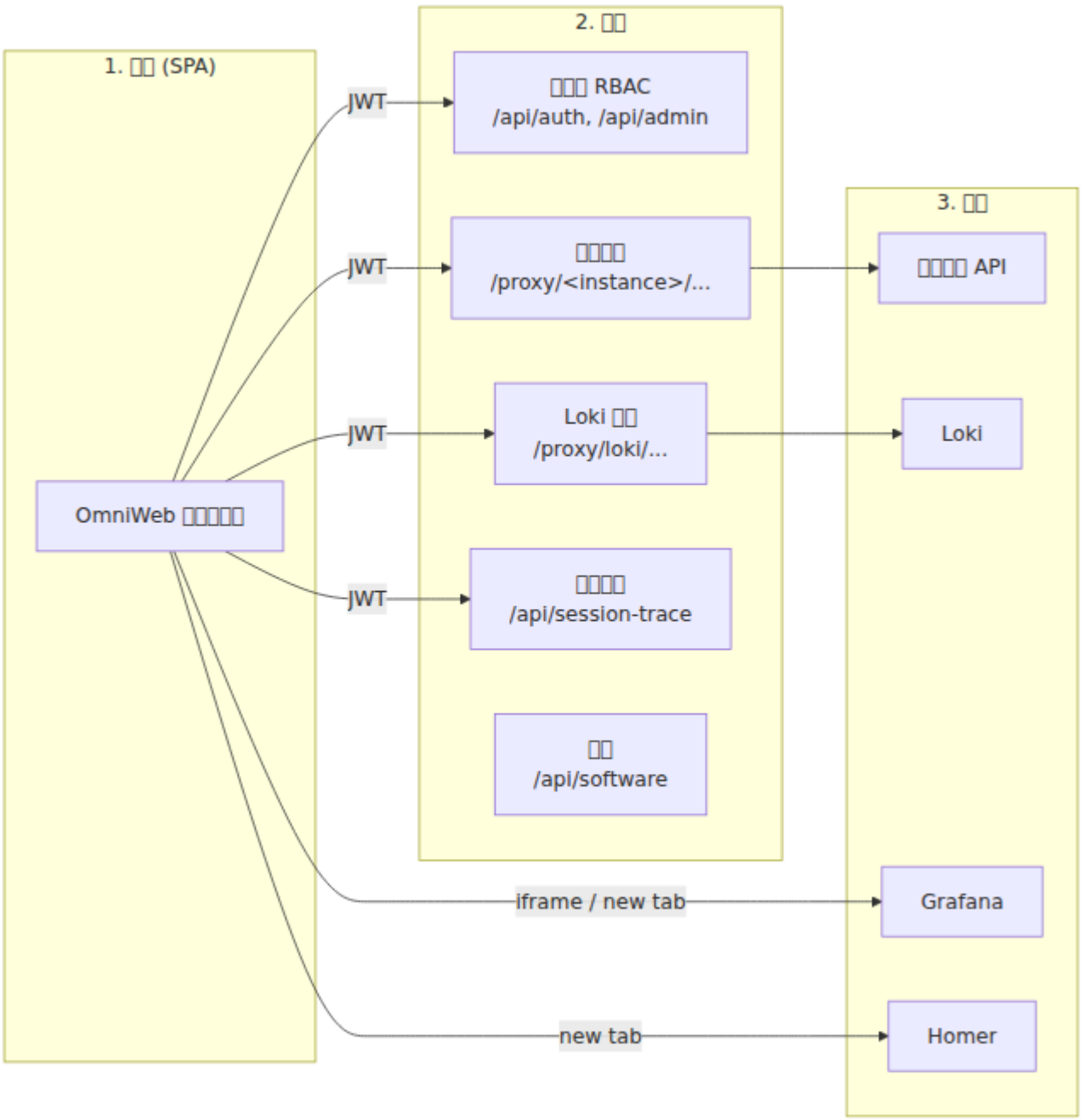
范围

这仅记录 控制器 API。运行在远程站点的设备代理不属于此 API：它通过 WebSocket 拨打 *out* 到控制器，并且不暴露任何入站 REST 端点，因此无法直接调用它。

OmniWeb 架构
本页面解释了 OmniWeb 的组成以及单个浏览器会话如何访问每个网络功能、Grafana 和 Loki。如果你只阅读一页来理解系统，请阅读这一页。
← 返回操作指南

组件

OmniWeb 有三个组成部分：



组件	角色
前端 **SPA**	用户界面。一个单页面 web 应用，渲染元素页面、拓扑、日志、跟踪和嵌入式仪表板。
后端	安全和集成层。它验证用户、强制执行 RBAC，并将每个请求反向代理到正确的元素 API、Loki 或 Grafana。
目标	被管理和观察的事物：网络元素自己的管理 API，以及 Grafana、Loki 和 Homer。

□□□□

□□□

```
{
  "elements": [
    {
      "type": "hss",
      "displayName": "HSS",
      "description": "□□□□□□□□",
      "instances": [
        {
          "id": "my-hss-01",
          "name": "my-hss-01",
          "baseUrl": "https://10.0.0.1:8443",
          "tags": ["primary"]
        }
      ],
      "defaults": {
        "pollIntervalMs": 5000,
        "timeoutMs": 10000
      }
    }
  ]
}
```

参数	类型	必需	默认	描述
`type`	字符串	是	-	元素类型。决定哪个 UI 模块渲染该元素。请参阅 支持的类型。
`displayName`	字符串	是	-	在侧边栏和拓扑中显示的人类可读名称。
`description`	字符串	否	-	在工具提示和概述页面中显示的更长描述。
`instances`	列表	是	-	每个部署节点的一个条目。请参阅下面的实例参数。
`defaults.pollIntervalMs`	整数	否	5000	操作页面自动刷新的频率，��毫秒为单位。
`defaults.timeoutMs`	整数	否	10000	此元素类型的代理超时。慢速 API（例如 OCS）使用更大的值。

实例参数：

参数	类型	必需	默认	描述
`id`	字符串	是	-	唯一的实例标识符。用于 URL（`/hss/<id>`）和代理路径（`/proxy/<id>/...`）。
`name`	字符串	是	-	实例的显示名称。
`baseUrl`	字符串	是	-	元素的管理 API 基础 URL。代理将请求转发到此处。接受自签名 TLS。
`tags`	列表	否	`[]`	自由格式标签（例如 `primary`，`geo-redundant`），以芯片形式显示。

支持的元素类型

`hss`, `mme`, `sgw-c`, `pgw-c`, `upf`, `pcscf`, `icscf`, `scscf`, `tas`, `epdg`, `entitlement`, `smsc`, `smsc-smpp`, `ipsmgw`, `msc`, `stp`, `hlr`, `camel-gw`, `dra`, `ocs`, `twag`, `ran-monitor`, `license`。

每种类型映射到一个具有自己选项卡的 UI 模块，但所有模块都通过相同的通用模式进行操作。请参阅 常见操作。

OmniWeb 如何与每个 NF 通信

后端代理与元素无关。它将前端模块请求的任何内容转发到元素的 `baseUrl`。这些调用的 □□ 取决于元素的原生 API:

API 风格	元素	��注
元素 API	所有网络功能	元素自己的管理 API，逐字代理在 `/proxy/<instance-id>/...` 下。OmniWeb 按照元素的期望转发 `GET`/`POST`/`PUT`/`PATCH`/`DELETE`；请求/响应的形状是该元素定义的任何内容。
日志查询 (LogQL)	所有（日志选项卡）	通过 `/proxy/loki/...` 路由到 Loki。请参阅 日志与跟踪。

由于所有内容都是代理的，因此添加实例仅仅是 `omniweb.json` 中的配置更改。管理另一个节点不需要代码更改。

API 参考 (OpenAPI)

一个合并的 OpenAPI/Swagger 文档 (`swagger-doc.json`) 随 OmniWeb 一起提供，并描述后端和元素架构（例如 SMSC 前端注册和 IMS 订阅者位置）。它是一个参考文档，而不是一个实时 API 服务器。

代理超时

每种元素类型都有一个可配置的代理超时 (`defaults.timeoutMs`)。大多数元素在 10 秒的默认时间内响应良好。查询较重的元素会有更多的缓冲时间:

元素	默认超时	原因
大多数元素	10 秒	标准 API 响应时间
OCS	180 秒	大数据集上的计费/CDR 查询

监控集成

OmniWeb 并不重新实现 Grafana、Loki 或 Homer。它集成了它们，���此单个登录可以跨越整个堆栈：

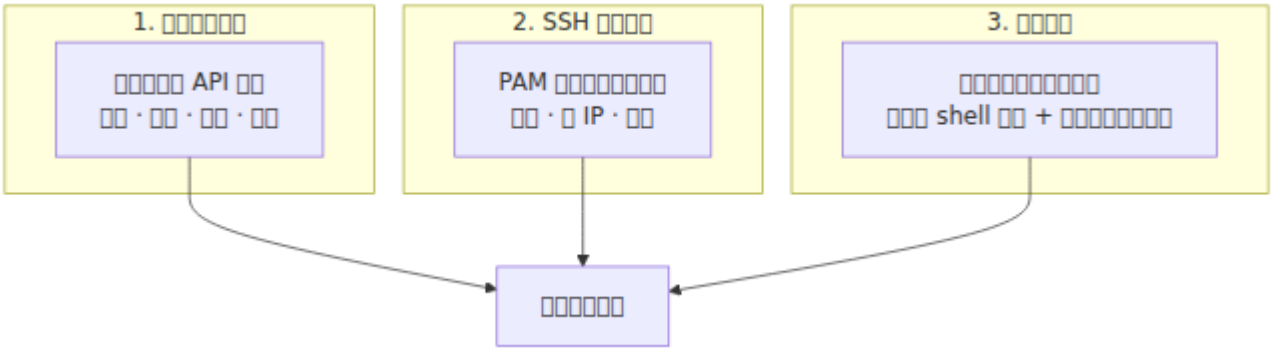
- **Grafana** 在经过身份验证的网关后提供，并作为 iframe 嵌入。每个请求都根据你的 OmniWeb 登录进行授权，因此没有第二个密码。请参阅 Grafana。
- **Loki** 通过后端的 `/proxy/loki/*` 网关访问，该网关代表操作员运行 LogQL 查询。请参阅 日志与跟踪。
- **Homer**（SIP 捕获）在启动时自动检测到（`/api/homer/status`），并在存在时在新选项卡中打开。它也根据你的 OmniWeb 登录进行授权。

环境参考

后端集成端点通过环境变量进行配置：

变量	默认	描述
`GRAFANA_URL`	`http://localhost:3000`	OmniWeb 代理的 Grafana 实例的基础 URL。
`LOKI_URL`	`http://localhost:3100`	用于日志和跟踪的 Loki 实例的基础 URL。
`LDAP_URI`	`ldap://localhost:389`	用户/SSH 密钥同步的 OpenLDAP 服务器（可选）。
`LDAP_BASE_DN`	`dc=omniweb,dc=local`	LDAP 基础 DN。
`LDAP_ADMIN_DN`	`cn=admin,dc=omniweb,dc=local`	LDAP 写入的绑定 DN。
`LDAP_ADMIN_PASSWORD`	`omniweb-admin`	LDAP 绑定密码（请更改此项）。
`AUDIT_API_KEY`	`omniweb-audit-key`	SSH 登录审计回调的共享密钥（请更改此项）。

请参阅 身份验证与访问控制 以获取 LDAP/SSH 和审计的详细信息。



审计日志

由于 OmniWeb 是网络的单一网关，因此也是记录活动的唯一地方。OmniWeb 中的审计有 三个层次，共同回答“谁在何处做了什么”的问题，涵盖门户和它管理的主机。

← 身份验证与访问控制 · ← 操作指南

三个层次

层次	捕获内容	出现位置
门户请求审计	通过 OmniWeb 采取的每个操作	设置 → 审计
SSH 登录审计	每个 SSH 登录到��管理主机	设置 → 审计（通过主机回调）
命令审计	在主机上运行的每个命令（输入 + 执行）	设置 → 命令

门户请求审计

每个通过 OmniWeb 代理的请求都会被记录，无论其是否成功、失败或被 RBAC 拒绝。每个条目捕获：

- 发出请求的 用户。
- 目标的 元素类型和实例。
- **HTTP** 方法（指示是查看、修改还是删除）。
- 结果（状态码）。
- 时间戳。

□□□

回调通过共享密钥进行身份验证，因此只有受信任的主机才能写入审计条目：

变量	默认值	描述
`AUDIT_API_KEY`	`omniweb-audit-key`	主机 PAM 钩子在报告登录时提供的共享密钥（作为 `X-Audit-Key`）。更改此值，并在每个主机上设置匹配值。

有了这个，每个 SSH 登录到受管理主机都会出现在 设置 → 审计 下，与门户操作一起，连接一个人的门户和主机活动。

命令审计

为了在主机上实现命令级可见性，OmniWeb 收集 两个互补的流，这两个流都发送到 Loki，并且可以在 设置 → 命令 下浏览，带有源切换：

来源	捕获内容	**Loki** 流
输入的命令	用户在交互式 shell 中输入的确切命令行，包括 **shell** 内置命令如 `echo`、`cd`、`export`	`job="cmdaudit"`
二进制执行	在主机上实际运行的每个二进制文件（脚本、工具、自动化）	`job="auditd"`

这两者并不相互替代：内置命令从不运行单独的二进制文件，因此只有输入命令流能看到它们；而从不处于交互提示下的自动化/脚本仅出现在二进制执行流中。它们共同覆盖了一个人输入了什么和实际执行了什么。

输入的命令 是通过轻量级交互式 shell 钩子捕获的，记录用户运行的每个命令（包括用户、工作目录和 TTY）。这是捕获内置命令的层，因为二进制跟踪器在结构上无法看到它们。

二进制执行 来自轻量级主机代理，记录在主机上运行的每个二进制文件。由于它在用户空间中工作，因此在没有内核审计支持的 LXC 容器内也能正常运行。每个条目捕获：

字段 意义

login 原始登录的用户；在 sudo / su 后仍然有效，因此特权更改不会隐藏谁在操作

uid 实际运行命令的有效 UID

filename 被执行的二进制文件

cwd 执行时的工作目录

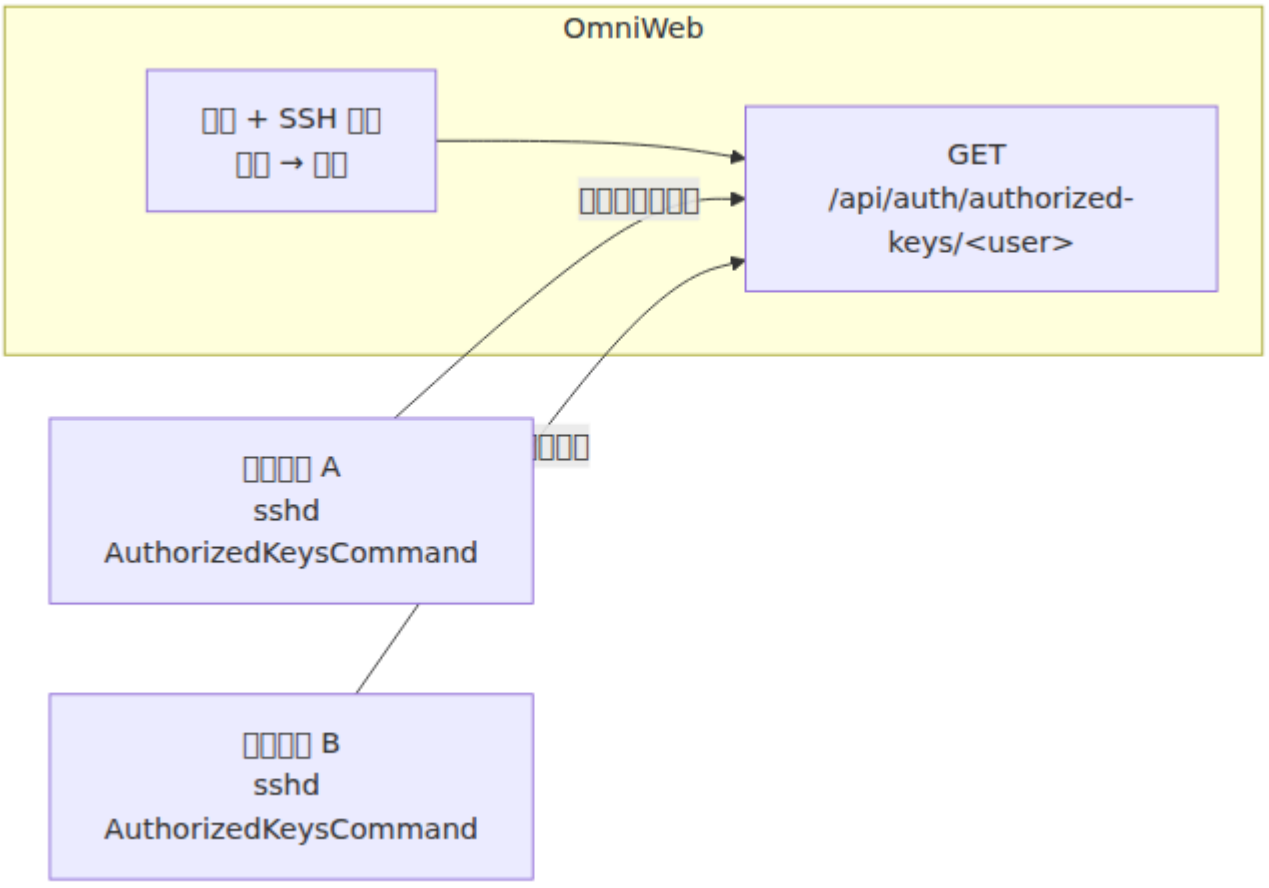
(在]: 之后) 完整命令行

一个代表性的执行条目：

```
2026-04-16T13:18:35 omni-stp01 [login:nickj uid:0 tty:(none)
cwd:/home/nickj filename:/usr/bin/sudo]: sudo tail -10
/var/log/auth
```

□□ → □□ □□□□

- SSH 密钥登录：主机活动的访问侧。
- RBAC：门户审计记录的权限使用。



SSH 密钥登录（主机访问）

OmniWeb 的访问控制超出了门户，延伸到运行网络的 主机。每个用户可以携带一个 **SSH** 公钥，受管主机在登录时会 实时从 **OmniWeb** 获取这些密钥。因此，OmniWeb 是管理 *□□□ SSH □□□* 的唯一地方，并且结合 审计日志，可以追踪实际执行的人。

不需要运行目录服务器，也不需要维护每个主机的 `authorized_keys` 文件。（这取代了早期的 OpenLDAP 同步设计；目录已消失，密钥通过 HTTPS 按需提供。）

← 身份验证与访问控制 · ← 操作指南

功能介绍

您只需在 OmniWeb 中为用户提供一次 SSH 公钥。每个受管主机的 `sshd` 被配置为在 登录时 向 OmniWeb 请求该用户的密钥（通过 OpenSSH 的 `AuthorizedKeysCommand`）。在 OmniWeb 中添加密钥后，用户可以 SSH 到每个注册的主机；禁用用户后，该访问权限将在他们的 下一个 登录尝试中消失，无需同步、无漂移，也无需清理密钥文件。

□□□□□□□

□□□ □□ → □□ □□□□□□□□□□□□□□□RBAC □□□/□□□□□□□□□□□□□□□□□□□□□□□□□□□ SSH □□□□□□□□□□ □□□□□□□□□

□□ → □□□□□□□□□□□□ SSH □□□

□□□□□□□

□□□□□□□□□□□□□□□□□□□ `sshd` □□□ `AuthorizedKeysCommand`□□□□□□□□□`sshd` □□□□□□□□ □□□ HTTPS □ OmniWeb □□□□□□□□□□□□□□□□□□□□□□

此流程的关键属性：

- 实时：密钥在每次登录时获取，因此更改会立即生效。
- 仅活跃用户：OmniWeb 仅返回 活跃 用户的密钥。当您在 OmniWeb 中禁用或删除用户时，这会立即拒绝他们在每个主机上的下一个登录。这是撤销按钮。
- 无枚举：未知或禁用的用户，或没有密钥的用户，返回空结果。登录简单地找不到密钥并被拒绝，因此端点不会泄露哪些用户名存在。
- 在 **OmniWeb** 停机时仍然有效：助手在主机上缓存每个用户的最后一个有效结果，因此短暂的 OmniWeb 停机不会锁定所有人。

帐户本身（Unix 用户、主目录、shell）由配置管理与 `sshd` 助手一起提供。OmniWeb 拥有 身份和密钥，而舰队自动化拥有每个主机上的 帐户存在。

配置

密钥服务端点由与 审计回调 相同的共享密钥保护：

变量	默认值	描述
`AUDIT_API_KEY`	`omniweb-audit-key`	每个主机的 `AuthorizedKeysCommand` 助手在获取密钥时呈现的共享密钥（作为 `X-Audit-Key`）。更改此项，并在每个主机上设置匹配的值。

因为 OmniWeb 是唯一应该被查询的对象，并且助手运行在受信任的主机上，所以端点通过 HTTPS 提供，密钥是网络路径上的第二道门。

为什么这很重要

一个地方授予/撤销 SSH 访问 整个舰队：用户的活动状态即他们的主机访问。
没有分散的密钥文件 在各个主机上漂移失去同步，也不需要操作和备份目录服务器。
一个单一身份 将个人的门户访问、SSH 访问以及通过 审计日志 记录的活动联系在一起。

相关

审计日志：记录 SSH 登录和在主机上运行的每个命令。
RBAC：控制相同用户在 OmniWeb 内部可以做什么。

登录与 JWT 会话

OmniWeb 使用用户名和密码对操作员进行身份验证，并发放 JSON Web Token (JWT)。该令牌证明了您在每个后续请求中的身份。至关重要的是，它是授权嵌入的 Grafana、Loki 和 Homer 的 凭证。一次登录覆盖整个技术栈。

← 身份验证与访问控制 · ← 操作指南

登录流程

令牌通过 `POST /api/auth/login` 发放。一旦获得，SPA 在每个 API 调用中呈现它，后端在□□行任何其他操作之前验证签名和过期时间。

□□□□□□□□□□□□□□□□□□□□□□□□□□□□ JWT□□□ API□Loki□Grafana □ Homer□

令牌的传递方式

后端在三个位置接受 JWT，这使得同一令牌可以用于 XHR API 调用、浏览器导航和嵌入的 iframe：

位置	用途
授权头	来自 SPA 的标准 API (XHR/fetch) 请求
Cookie (`access_token`, HttpOnly)	浏览器导航和嵌入内容（Grafana iframe、Homer 标签）
查询字符串	无法设置头或 Cookie 的情况

Cookie 是 **HttpOnly**（JavaScript 无法读取）并使用 `SameSite=Lax`，这保护了令牌免受跨站脚本访问的盗窃，同时仍允许对嵌入工具的顶级导航。

令牌生命周期

访问令牌具有可配置的过期时间，默认为 **24** 小时（`JWT_ACCESS_TOKEN_EXPIRES`，以秒为单位）。当它过期时，操作员将返回登录屏幕并重新进行身份验证。没有静默的无限会话；生命周期是一个故意的安全边界。

设置	默认值	描述
`JWT_ACCESS_TOKEN_EXPIRES`	`86400` (24 小时)	访问令牌的生命周期（以秒为单位）。降低它以缩短会话；□□高它以减少重新登录。
`JWT_SECRET_KEY`	*(□□□)*	用于签名和验证令牌的密钥。在生产环境中显式设置，以□令牌在后端重启后仍然有效，并在实例之间保持一致。

一次登录，整个技术栈

相同的 JWT 授权集成监控工具，因此操作员无需重复登录：

元素 API 和 Loki 通过后端代理访问，后端直接检查 JWT。
Grafana 和 Homer 通过经过身份验证的网关访问，网关在代理之前验证您的 OmniWeb 登录，无需第二个密码。请参见Grafana和Homer。

这就是为什么单个 OmniWeb 会话控制整个操作表面：仪表板、日志、跟踪和元素管理都依赖于同一个令牌。

首次登录与更改凭证

全新部署提供默认管理员帐户（admin / admin）。首次登录后立即更改此帐户，通过设置进行更改。默认帐户仅用于引导系统，绝不能在生产环境中存活。

登出与过期

登出会丢弃令牌。过期或无效的令牌会导致下一个请求被拒绝，SPA 返回登录屏幕。由于元素操作仅通过经过身份验证的、经过 RBAC 检查的代理调用执行，因此过期会话永远无法执行特权操作。

相关

基于角色的访问控制：登录用户被允许做什么。
审计日志：每个经过身份验证的操作都会被记录。

基于角色的访问控制（RBAC）

身份验证告诉 OmniWeb □□□。RBAC 决定 □□□□□□。访问权限是以细粒度授予的，按元素类型、按 **HTTP** 方法，这直接映射到操作员执行的真实操作：查看、修改或删除。此外，还有两个范围决定 □□□：操作员可以访问哪些 站点，以及他们可以使用哪些 测试设备。每个请求必须通过所有这些检查。

← 身份验证与访问控制 · ← 操作指南

权限级别

每种元素类型可以在三个级别中授予用户。级别以用户可以通过代理对该元素使用的 HTTP 方法集表示：

权限	允许的方法	操作员可以做什么
只读	`GET`	仅查看数据，无需更改
读写	`GET`, `POST`, `PUT`, `PATCH`	查看和修改：例如，添加订阅者、编辑路由、改变 QoS 规则
完全	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	包括删除和清除会话的所有操作

由于权限与 HTTP 方法相关联，因此它们与 通用编辑模型 完全一致：“添加”表单是 `POST`，“编辑”是 `PUT`/`PATCH`，“删除”/“清除”是 `DELETE`。

每元素粒度

权限是 独立于元素类型分配 的。用户可以在不同元素上持有不同级别：

在这个例子中，Jane 可以清除 UPF 会话，可以查看但不能更改 HSS，可以添加 SMSC 路由，并且根本看不到 OCS。这使得你可以给数据平面工程师完全控制 UPF，同时保持订阅者数据为只读。

站点范围（多站点部署）

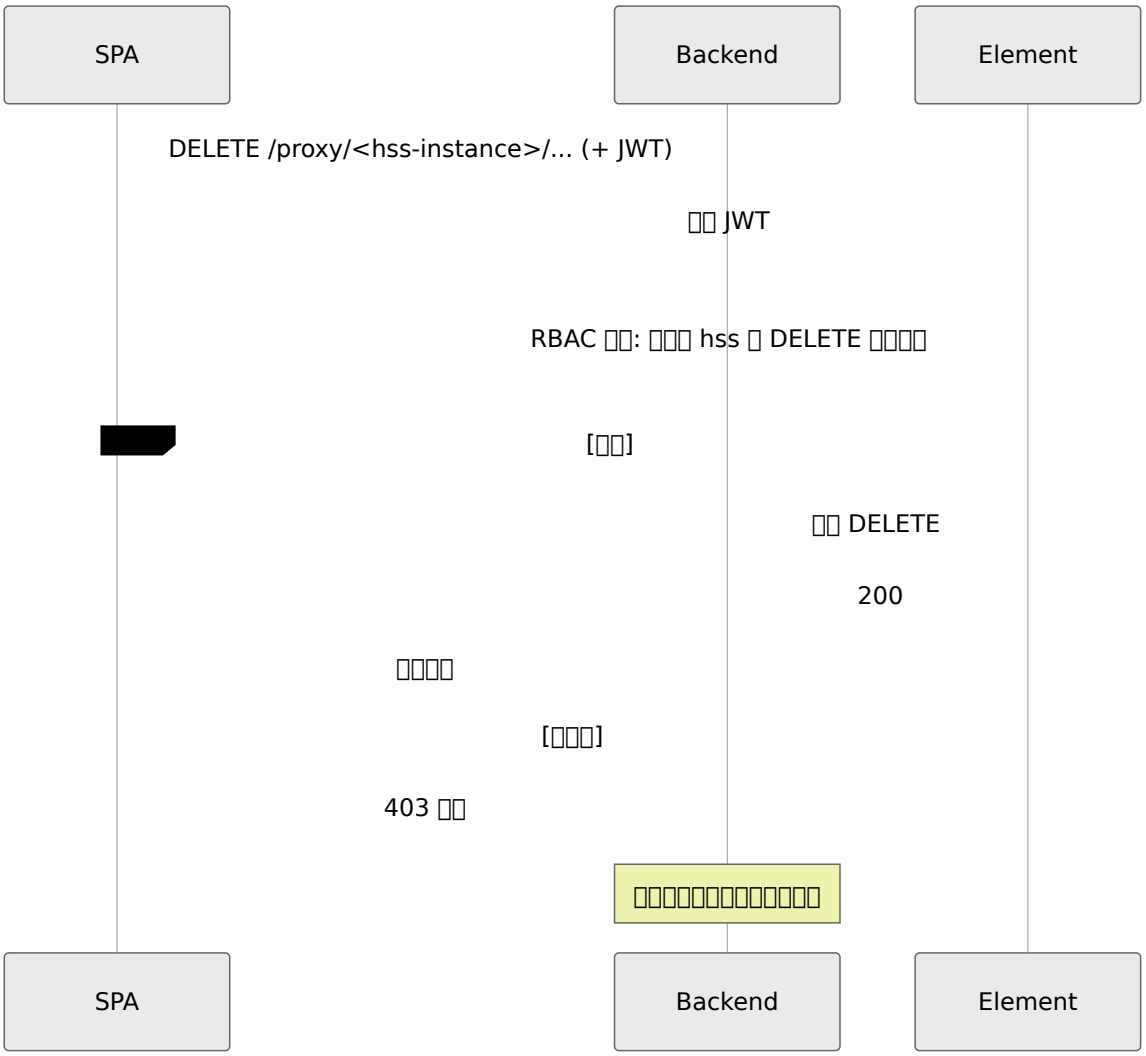
元素权限回答 *□□□□□□□□*。在一个有多个站点的系统中，第二个独立的轴回答 *□□□*：他们可以访问的站点集合。请求必须同时满足这两个条件。

默认情况下，用户是 无限制的 —— 他们可以访问每个站点，包括后续添加的站点。将用户限制到一个或多个站点将使他们仅限于这些站点，并且可以一次性授予整个客户，以□该客户的新站点自动包含在内。

□□□

□□□

□□□



SPA
Backend
Element
DELETE /proxy/<hss-instance>/... (+ JWT)
验证 JWT
RBAC 检查: 用户对 hss 有 DELETE 权限吗?
[允许]
转发 DELETE
200
代理结果
[不允许]
403 禁止
任何结果都记录在审计日志中
SPA
Backend
Element

□□ → □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

良好实践

- 最小权限：授予让某人完成工作所需的最低级别；仅在需要时扩大权限。
- 默认只读：对于操作员仅需观察的元素。
- 保留完全权限 **(DELETE)**：仅授予真正需要清除会话或删除记录的人。
- 少量管理员：使用针对性的按元素授予，而不是随意授予管理员权限。
- 按站点范围：在多站点舰队中：为客户的操作员提供他们自己的站点，以□错误无法影响其他部署。
- 按测试设备范围：将设备范围限制在某人负责的电话上，以□脚本运行无法干扰其他团队的工作台。
- 固定服务凭据：API 密钥可以限制在比其所有者更少的站点上，因此为一个部署发放的密钥无法在另一个部署上操作。密钥只能比其所属帐户更窄，绝不能更宽。

相关内容

- 登录与 JWT 会话：RBAC 构建的身份验证。
- 常见操作：权限如何塑造日常 UI。
- 审计日志：记录允许和拒绝的操作。

认证与访问控制

OmniWeb 是整个网络的唯一入口，因此访问控制是其最重要的职责之一。它使用基于 JWT 的登录、对每个元素的细粒度基于角色的访问控制 (RBAC)、用于主机访问的 SSH 密钥登录，以及跨门户和其管理的主机的统一审计日志。

该区域分为专注的页面：

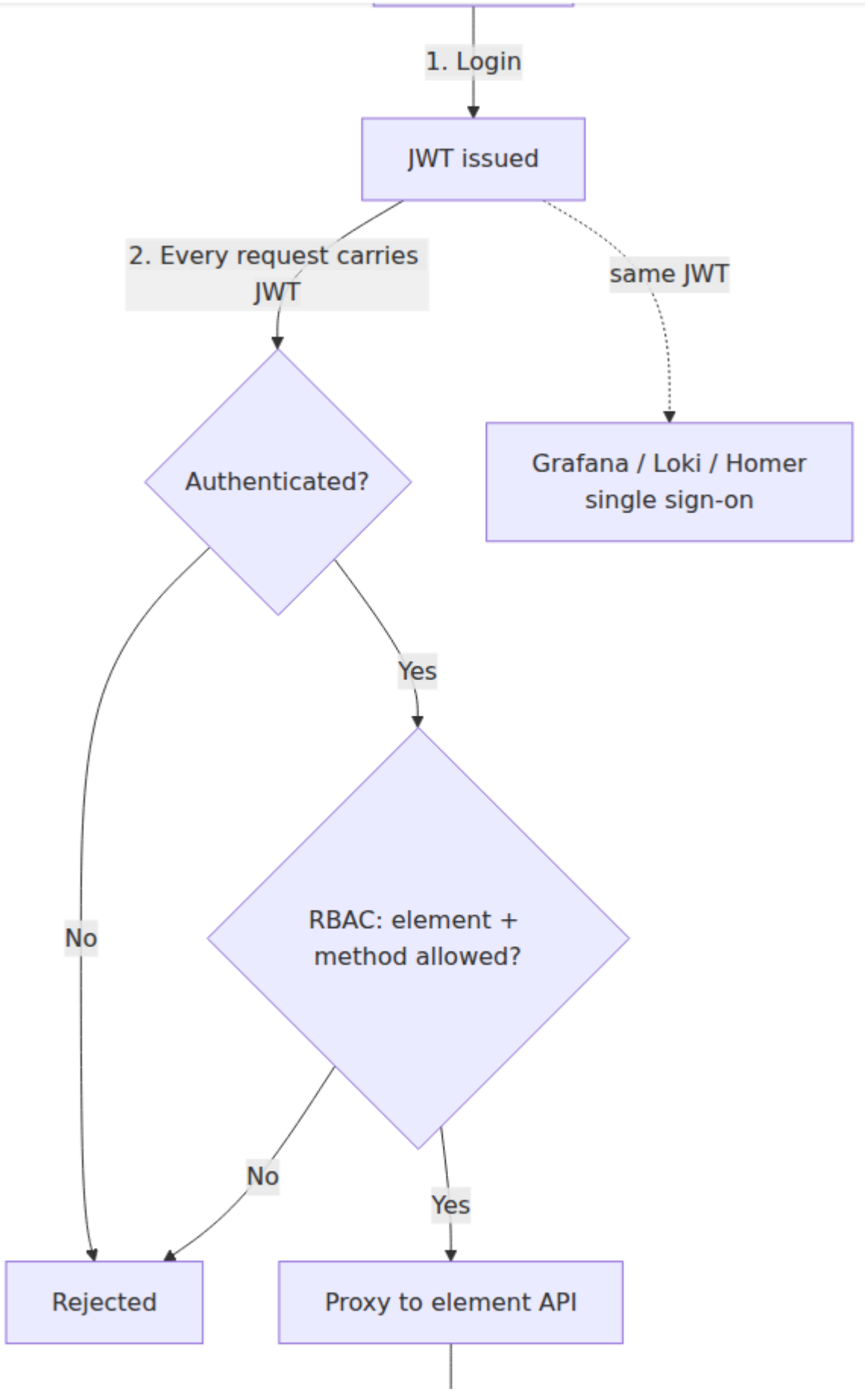
← 返回操作指南

本节内容

- 登录与 **JWT** 会话：操作员如何登录，JWT 的工作原理，令牌生命周期，以及单次登录如何跨越 Grafana、Loki 和 Homer。
- 基于角色的访问控制 **(RBAC)**：每个元素、每种方法的权限；如何授予这些权限；以及如何执行它们。
- **SSH** 密钥登录：管理的主机实时从 OmniWeb 获取每个用户的 SSH 公钥（AuthorizedKeysCommand），因此主机访问是集中授予/撤销的。
- 审计日志：审计的三个层次：门户请求审计、SSH 登录审计和命令审计。

访问控制模型

OmniWeb 分层了四个控制。请求必须在到达元素之前通过每一层，整个链条都会被记录。


1. Login
JWT issued
2. Every request carries JWT
same JWT
Authenticated?
Grafana / Loki / Homer single sign-on
Yes
No
RBAC: element + method allowed?
No
Yes
Rejected
Proxy to element API

层级	控制内容	页面
认证	你是谁，通过签名的 JWT 证明	登录与 JWT
授权 **(RBAC)**	你可以做什么，按元素类型和 HTTP 方法	RBAC
主机访问	谁可以 SSH 到哪里；密钥实时从 OmniWeb 提供	SSH 密钥登录
审计	实际发生了什么，跨门户和主机	审计日志

为什么这很重要

因为 OmniWeb 代理每个元素、Grafana 仪表板、Loki 查询和 Homer 会话，这条单一的访问控制链管理着网络的 □□ 操作表面。只有一个地方可以授予访问权限，一个地方可以撤销权限，以及一条记录谁在门户和底层主机上做了什么的轨迹。

□□□□□□□□□API □□□□□□SSH □□□□□□□□□□□□□□□□□□□□□□□□ IP□□□□ □□□□□

□ □□□ JWT □□ □□□

呼叫追踪 (SIP 追踪)
呼叫追踪 是 OmniWeb 工具，用于语音呼叫故障排除。它记录跨 IMS 的呼叫的 SIP 信令和 RTP 媒体。然后，它允许您搜索这些呼叫，打开每个呼叫的完整报告，沿着网络中的信令梯子跟踪呼叫，测量语音质量，收听音频，并下载原始数据包捕获 (PCAP)。

呼叫追踪是一个站点级工具。它在侧边栏的 会话追踪 下显示为 SIP 追踪。该工具仅在捕获服务为所选站点配置并可访问时显示。

← 操作指南

目录

它是什么
架构
搜索
呼叫详细信息
梯子 (会话追踪)
QoS 选项卡
收听
PCAP 下载
活动呼叫
实时嗅探器
远程捕获代理
录音规则和保留
隐私和合法拦截
呼叫追踪与 Homer 和会话追踪的比较

它是什么

呼叫追踪深入回答一个问题：这个呼叫发生了什么？对于任何录制的呼叫，它提供：

两个参与方、他们的号码、他们的 SIP 域和显示名称。
每个参与方的 SIP IP 地址，链接到其 OmniWeb 网络元素。
最终的 SIP 响应和断开原因（SIP 和 Q.850）。

每个媒体方向的语音质量：MOS、抖动、丢包和往返延迟。
跨每个触及呼叫的 IMS 元素的完整 SIP 消息流（梯子）。
录制的音频和原始 PCAP。

呼叫追踪第一手记录呼叫。因为它捕获了 SIP Call-ID 和线上的媒体，所以呼叫与其数据包捕获一一对应，无需猜测。

语音质量以 MOS（平均意见得分）报告。MOS 是一个 1 到 5 的评分。得分 4.0 或更高为良好，3.0 到 4.0 为一般，低于 3.0 为差。OmniWeb 对 MOS 值进行着色：绿色表示良好，琥珀色表示一般，红色表示差。在健康网络中，AMR-WB（宽带）呼叫的得分约为 4.5。

架构

呼叫追踪使用两个部分：

1. 捕获代理 在 IMS 元素（P-CSCF、S-CSCF 和 TAS）上运行。每个代理捕获其主机上看到的 SIP 和 RTP 数据包。代理不在本地存储或解析数据包。它们通过加密通道将原始数据包转发到中央捕获服务器。
2. 中央捕获服务器 解析每个数据包，计算语音质量，并将索引写入其数据库。它保存数据包捕获缓冲区和录制的媒体。OmniWeb 从这个服务器读取搜索、呼叫详细信息、梯子、QoS、音频和 PCAP。

这种设计将所有录制的数据保存在一个中央服务器上。IMS 元素不保留自己的捕获数据。

捕获代理为呼叫追踪提供了来自网络中多个点的视图。单个呼叫是从每个看到它的代理中拼接而成。这使得梯子能够显示跨 P-CSCF、S-CSCF 和 TAS 的多跳 SIP 流。

搜索

打开呼叫追踪以访问 搜索 视图。搜索在中央呼叫索引中查找已完成的呼叫。

搜索视图。每一行堆叠了呼叫者和被叫方（号码、域、名称、SIP IP 和用户代理），旁边是每个方向的 RTP 单元，显示源 IP、编解码器、三个 MOS 估计、抖动和丢失。

过滤器

设置一个或多个过滤器，然后选择 搜索。所有过滤器结合使用 AND。

过滤器	匹配内容
号码	呼叫者号码或被叫号码。
时间范围	预设窗口（过去 15 分钟到过去 7 天）或自定义开始和结束。
方向	入站、出站或内部。方向来自呼叫者和被叫方 IP 的角色。
最小 **MOS**	仅保留最差方向的 MOS 达到或超过此值的呼叫。使用此选项查找良好呼叫，或反向阅读以查找差呼叫。
最大丢失	仅保留最差方向的丢包率达到或低于此值的呼叫。

结果网格

每个结果行显示：

- 时间：呼叫开始和结束时间。
- 呼叫者 和 被叫：一个堆叠单元，包含号码和域（`num@domain`）、显示���称、SIP IP（链接到 OmniWeb 中的该元素）和用户代理。一个 挂断 标签标记发送 BYE 的方。
- 结果：最终的 SIP 响应代码和文本。
- **RTP A** 和 **RTP B**：每个媒体方向一个单元。每个单元显示源 IP、编解码器、三个 MOS 估计（固定 50 | 固定 200 | 自适应）、抖动和丢包计数。三个 MOS 值使用颜色编码。
- 时长 **(**秒**)**：呼叫持续时间（以秒为单位）。
- **PCAP**：每行的下载按钮，用于该呼叫的数据包捕获。

选择一行以打开 呼叫详细信息。

呼叫详细信息

呼叫详细信息视图是一个呼叫的完整报告。当您选择搜索结果时，它会打开。URL 带有呼叫标识符，因此您可以书签或分享呼叫。

呼叫详细信息视图。标题显示 Call-ID 和上下文。摘要条显示开始、持续时间、PDD、响铃、连接、最后的 SIP 响应和断开原因。两列表显示呼叫者 (A) 和被叫 (B) 的身份和语音质量。

标题和上下文
标题显示线上的 Call-ID。下面的上下文块显示呼叫 方向、拥有的 传感器（捕获代理）、哪个方 挂断、结束 时间和 呼叫者名称。

摘要条

摘要条是对呼叫的一行概述：

字段	意义
开始	呼叫开始的时间。
持续时间	呼叫的总长度。
PDD	拨号后延迟：从 INVITE 到第一次响铃指示的时间。
响铃	电话响铃多久后接听。
连接	呼叫连接（媒体流动）多久。
最后 **SIP** 响应	最终的 SIP 响应代码和文本。
SIP 原因	SIP 断开原因，当捕获引擎记录时。
Q.850 原因	Q.850 断开原因和文本（如果存在）。
呼叫者 和 被叫	两个参与方作为 `num@domain`。

身份和语音质量表

主表有两列：呼叫者 **(A)** 和 被叫 **(B)**。每个 IP 在已知元素时链接到其 OmniWeb 网络元素。表有三个组。

身份：

行	意义
SIP IP	参与方的 SIP 信令 IP。
RTP IP	参与方的 RTP 媒体 IP。
RTP 端口	RTP 媒体端口。
用户代理	参与方的 SIP 用户代理。
编解码器	音频���解码器，例如 AMR-WB。
接收的数据包	接收的 RTP 数据包计数。
丢失的数据包	丢失的 RTP 数据包计数。

MOS：三个 MOS 估计器，每个显示为 `average | minimum`：

行	意义
MOS 固定 50	在固定 50 数据包窗口内的 MOS。
MOS 固定 200	在固定 200 数据包窗口内的 MOS。
MOS 自适应 500	在自适应窗口内的 MOS，最多 500 数据包。

抖动和 **RTCP**：RTP 抖动（最大和平均）、RTCP 抖动、RTCP 丢失和丢失比例计数，以及 RTCP 往返延迟（最大和平均）。

梯子（会话追踪）

梯子 选项卡绘制呼叫作为时间排序的信令流。呼叫追踪从每个看到呼叫的捕获代理拼接 SIP 消息。结果是跨 IMS 元素的多跳梯子：例如从 P-CSCF 到 S-CSCF 再到 TAS。

□□□□□□□□□□□□□□ IMS □□□□□□□□□□□ SIP □□□□□□□□ INVITE □ 100 □ 180 □ 200 □ ACK □ BYE □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

每一列是一个 IMS 元素，标记其角色和主机名。每个梯级是从源到目的地的 SIP 消息。梯子显示：

- 每条消息的时间增量（自上条消息以来的间隔）。
- 每个响应的 请求到响应往返时间，与其请求配对。
- 绝对、相对 和 过去 时间模式的时间列。
- 内联数据包解码：选择一个梯级以查看完整的 SIP 消息文本和十六进制视图。

会话详细信息 面板列出梯子中的会话。对于单个呼叫，有一个会话，因此面板保持折叠。

梯子使用与网络范围内的会话追踪实时流相同的渲染。请参见 日志与订阅者追踪 以获取更广泛的会话追踪工具。

QoS 选项卡

QoS 选项卡显示呼叫生命周期中的语音质量。

QoS □□□□□□□□□□□□ PDV□□□□□□□□□□□□□□□□□□□□□□ MOS □□□□□□□□□□□□□□□

QoS 选项卡有三个部分：

- 一个交互式 延迟 / 抖动和 **MOS** 质量图，显示整个呼叫的情况。图是每个媒体方向的。您可以在呼叫的任何点读取延迟和 MOS，这显示了质量下降的地方。
- **PDV**（延迟）分布：有多少数据包��入每个延迟桶（例如 50 到 70 毫秒、70 到 90 毫秒，等等，直到超过 300 毫秒）。保持在低桶中的分布是健康的。
- 连续丢失 细分：有多少次 1、2、3 以及最多 10 个数据包连续丢失。孤立的单个丢失比长时间的丢失要少得多。

两个细分都是按方向（呼叫者和被叫）显示的，因此您可以判断哪个方向出现了问题。

收听

收听 面板在浏览器中播放录制的呼叫。音频是从捕获的 RTP 解码的。呼叫者是左声道，被叫者是右声道，因此您可以单独听到每一方。

收听仅在呼叫的媒体被录制且其编解码器可以解码时有效。请参见 录音规则和保留 以了解如何启动媒体捕获。

PCAP 下载

每个呼叫都有一个 下载 PCAP 按钮，既在搜索网格中，也在呼叫详细信息标题中。下载的是该呼叫的原始数据包捕获（SIP 和（当录制时） RTP）。使用 PCAP 在外部工具（如 Wireshark）中检查呼叫。

活动呼叫

活动呼叫 视图显示当前正在进行的呼叫。它从捕获代理读取实时呼叫列表，并在短时间间隔内刷新，因此随着呼叫的建立和拆除，行会出现和消失。

活动呼叫视图。每一行是一个实时呼叫，显示其状态（连接或设置）、两个参与方及其 IP 地址、方向、不断增长的持续时间、编解码器、实时 MOS 和拥有的捕获代理。

每一行显示呼叫的 状态（连接、设置或失败）、两个参与方、呼叫者到被叫的 IP 路径、方向、不断增长的 持续时间、编解码器、实时 MOS、最后的 SIP 响应和拥有的 传感器（捕获代理）。关闭 自动刷新 以保持当前列表。

实时嗅探器

实时嗅探器 视图显示中央捕获服务器及其捕获代理的健康状况。

实时嗅探器视图。中央服务器面板显示版本、正常运行时间、活动呼叫计数、吞吐量、数据包丢失和负载平均值。远程捕获代理表列出每个代理。缓冲区磁盘 I/O 面板显示利用率和吞吐量。

该视图显示：

中央服务器：版本和构建、正常运行时间、活动呼叫计数、捕获吞吐量、数据包丢失、负载平均值和最后一次写入呼叫记录的时间。
远程捕获代理：每个元素的代理及其状态（请参见 远程捕获代理）。
缓冲区磁盘 I/O：捕获缓冲区磁盘的利用率、读写吞吐量、IOPS、延迟、使用的容量和缓冲区级别。
正在进行的呼叫的实时活动反馈。

观察此视图以确认捕获引擎健康、未丢失数据包，并且缓冲区磁盘有余量。

远程捕获代理

远程捕获代理 表（在实时嗅探器视图中）列出在 IMS 元素上运行的捕获代理。每一行显示：

列	意义
代理	代理主机名。选择它以在主机列表中打开该主机。
传感器 **ID**	捕获索引中代理的数字标识符。
状态	活动、空闲或未知，基于实时呼叫和最近的呼叫记录推断。
活动呼叫	代理当前正在捕获的呼叫数量。
CDR	代理生成的呼叫记录数量。
最后看到	代理最后一次生成呼叫记录的时间。

使用此表确认每个 IMS 元素是否应捕获。意外空闲或缺失的代理意味着该元素的流量未被记录。

录音规则和保留

录音规则 视图控制哪些呼叫的 媒体 被录制，并显示捕获缓冲区和索引数据库的保留。

□□□□□□□□□□□□□□□□□□ IP□□□□□□ SIP □□□□□□ SIP □□□□□□□□□□□ RTP □□□□□□□□□□□ QoS □□□□□

录音规则

默认情况下，捕获引擎记录每个呼叫的 SIP 信令，但不记录 RTP 媒体。录音规则为特定目标启动媒体捕获。捕获引擎实时重新读取规则，无需重启。

规则按如何匹配呼叫分组：

组	匹配条件
按 **IP**	源或目标 IP 和掩码。
按号码	呼叫者或被叫号码前缀。
按 **SIP** 域	SIP 域。
按 **SIP** 头部	任意 SIP 头部值。

每条规则携带一组标志：

标志	效果
RTP	为匹配的目标启动 RTP 媒体捕获。这使您能够 收听 呼叫并获取完整的媒体 PCAP。全局关闭 RTP，并按目标启动。
跳过	完全丢弃匹配的目标：没有呼叫记录和捕获。将此用于已知的测试流量。
图表	保存匹配目标的细粒度 QoS 图表数据，驱动 QoS 图表。
rtcp	记录匹配目标的 RTCP 质��报告。
启用	打开或关闭规则而不删除它。

要为一个目标启动捕获，请在匹配组中添加一条规则，填写匹配值，并打开 **RTP**。要停止记录已知的测试流量，请添加一条规则并打开 跳过。

□□

□□□

默认情况下关闭 RTP 捕获，并按目标启动。将 RTP 保留设置为您政策允许的最短时间。遵循您当地的隐私法律和同意规则，以进行信令和媒体捕获。

呼叫追踪与 **Homer** 和会话追踪的比较

OmniWeb 有三种查看信令的方法。选择合适的一种：

	呼叫追踪 **(SIP** 追踪**)**	**Homer (SIP** 捕获**)**	会话追踪
范围	IMS 呼叫的 SIP 和 RTP 媒体	仅 SIP	整个网络: Diameter、GTP-C、PFCP、SIP、MAP
回答的问题	“这个呼叫做��什么，语音质量如何？”	“这个呼叫的 SIP 流做了什么？”	“这个订阅者在每个元素中发生了什么？”
语音质量 **(MOS)**	是	否	否
录制音频	是	否	否
PCAP 下载	是，按呼叫	否	否
最佳用途	诊断 VoLTE 呼叫的质量、媒体和流	快速查看 SIP 流	追踪一个订阅者的端到端

当您必须判断呼叫的 语音质量、收听音频或获取媒体 PCAP 时，请选择呼叫追踪。当您需要在整个堆栈中跟踪一个订阅者时，请选择 会话追踪。

相关

- 日志与订阅者追踪：网络范围的会话追踪和共享梯子。
- Homer: SIP 捕获：仅 SIP 的捕获工具。
- 网络拓扑：捕获代理链接到的主机列表。

常见操作
OmniWeb 中的每个网络元素在内部都是不同的，但您与它们的工作方式是故意保持一致的。此页面记录了所有元素共享的模式：查看数据、编辑和更改 NF 设置、读取配置、运行操作、查看日志，以及理解轮询和权限。学习这些一次，它们适用于 HSS、UPF、SMSC、MSC 和每个其他 NF。

下面的截图来自特定元素，但它们说明了通用模式：相同的控件出现，字段不同，适用于每个元素。

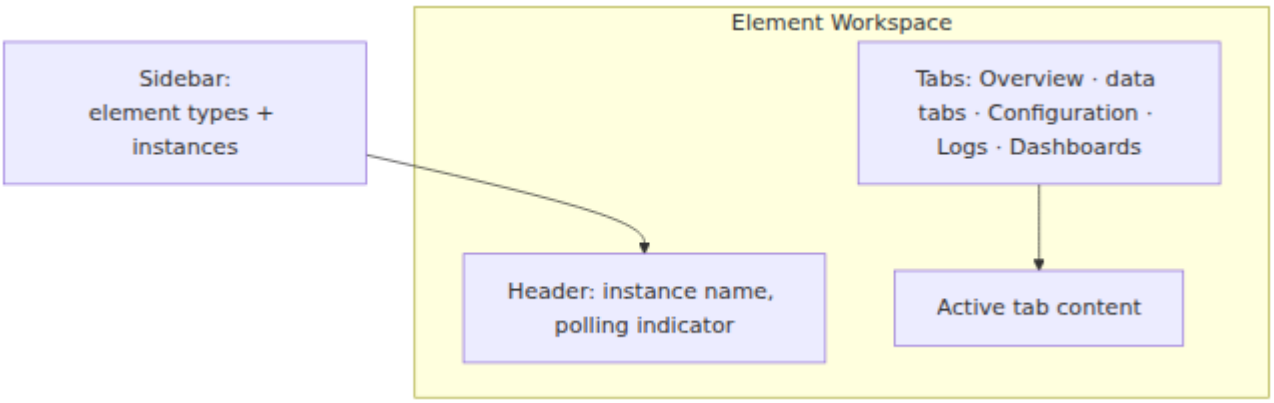
← 返回操作指南

目录

页面结构
查看数据
详细视图
编辑和更改 NF 设置
运行操作（清除、释放、测试、ping）
查看配置
每个元素的日志
每个元素的仪表板
实时轮询
权限和您可以更改的内容
多实例和车队视图

页面结构

在侧边栏中选择一个元素实例会打开其工作区。每个元素工作区共享相同的布局：


Element Workspace
Sidebar:
element types +
instances
Tabs: Overview · data
tabs · Configuration ·
Logs · Dashboards
Header: instance name,
polling indicator
Active tab content

- □□□□

□□□□

□□□

□□□□□□□□ HTTP □□□□□□□□□□□□□□□□ □□□

□□□□□□□□□□

□□□□□□□□□□□□□□ NF □ *□□* □□□

□□	□□	□□□□□□
□□/□□□□	HSS → □□□ → □□	□□□□□□IMSI□MSISDN□□□□□□□□□□→ □□ `POST`/`PUT` → □□□□
□□/□□□□	SMSC → □□ → □□□□ MSC → □□□	□□□□□□□□□□□□□□□□□□→ □□□□ → □□□□
□□/□□□□	UPF → □□□□ MSC → □□□	□□□□ → □□ → □□ `DELETE` → □□□□

□□□□□□□□□□□□□□□□□

运行操作

除了 CRUD，许多元素还暴露 操作性操作，这些操作不适合简单表单。这些操作以按钮的形式呈现，触发代理调用并在线显示结果。相同按钮操作模式的示例：

示例操作	元素	效果
强制释放呼叫	MSC → 呼叫	拆除一个活动呼叫
对 SIP 对等体进行 OPTIONS ping	MSC → SIP 对等体	测试 SIP 中继的可达性
对 Diameter 对等体进行 MAR 测试	TWAG → Diameter	发送测试多媒体认证请求
激活/停用重定向	UPF → 围墙花园	重定向或恢复订阅者
从节点 ping	UPF → 诊断	从元素本身运行 ping
断开会话	TWAG → 会话	断开已认证的 WiFi 会话
手动寻呼	MSC → 寻呼	触发寻呼请求

破坏性操作（释放、删除、停用）在运行之前始终需要明确确认。

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□/□□□□□□□□□□□□□□□ IP□□□□□□□□□□□□□□□□

查看配置

暴露其运行时配置的元素具有 配置 标签。OmniWeb 以结构化、可读的布局呈现，并提供 原始 **JSON** 切换以查看完整的底层文档。

有两个行为值得了解:

- 混合配置格式被规范化。一些元素返回的配置为 Python 风格的字典（`'key': True`, `None`），而不是严格的 JSON。OmniWeb 会自动将这些解析为干净的视图，并在无法解析值时优雅地回退。
- 机密被掩码。任何名称看起来敏感的字段（匹配 `password`、`secret`、`token` 或 `credential`）在配置视图和表单字段中显示为 `***` 而不是其真实值。

□□□□□□□□□□□□□□□□□□□□□□□□□□ JSON □□□□□□□□□□□□□□□□□□□□UPF□TAS□ePDG□SMSC □□□OCS□RAN □□□□□□□□□□□

□□□□□□□

□□□□□□□□□□ Loki □□□ □□ □□□□□□□□/□□□□□□□□□□□□□□□□□□□

*□□□

可以按页面切换轮询。围绕交互式或一次性操作构建的页面（控制台、诊断、JSON 执行器）默认不进行轮询，并手动刷新。当您希望在阅读大型表格时保持稳定视图或在追踪进行时暂停轮询时，请暂停轮询。

权限和您可以更改的内容

您在元素上可以 [] 的事情取决于您的角色。访问权限是 按元素类型、按 **HTTP** 方法 授予的：

权限	允许的方法	典型用途
只读	`GET`	查看数据，无更改
读写	`GET`、`POST`、`PUT`、`PATCH`	查看和修改（添加订阅者，编辑路由）
完全	`GET`、`POST`、`PUT`、`PATCH`、`DELETE`	所有操作，包括删除/清除

权限是独立分配给每个元素的：您可能对 UPF 拥有完全访问权限，但对 HSS 只有只读权限。如果某个操作对您的角色不允许，则其控件不可用。管理员对所有元素具有完全访问权限。请参见 身份验证和访问控制 来管理角色，并注意 每个代理请求都被审计日志记录□□无论角色如何。

多实例和车队视图

许多元素类型作为多个实例运行：多个 UPF 在 PGW-C 后面，一对 SMSC，冗余 STP。OmniWeb 在元素类型级别处理此问题：具有多个配置实例的类型会获得两种导航模式。

侧边栏和实例选择

当一个类型有多个实例时，侧边栏条目会展开以按名称列出每个实例。单击命名实例以直接打开该实例的工作区。工作区标题中还会出现一个实例下拉菜单。它允许您在不返回侧边栏的情况下在实例之间切换，这在比较节点之间的行为时非常有用，而不会丢失在特定标签上的位置。

工作区标题右上角的实例选择器。打开它会显示每个配置实例以及“所有实例”，以便在不离开当前标签的情况下跳回车队视图。

车队视图

单击侧边栏中的元素类型名称（而不是特定实例），或从下拉菜单中选择 所有实例，以打开该类型的 车队视图。车队视图显示每个实例的摘要卡，带有健康状态和关键指标，因此您可以在深入特定节点之前一目了然地评估整个车队。

UPF 车队视图：每个实例一张卡，所有卡并行轮询。单击任何实例卡或使用下拉菜单进行深入。

何时使用每种视图

情况 使用

检查整体车队健康 车队视图：一目了然的所有实例

调查特定节点 实例下拉菜单或侧边栏子项

比较两个 UPF 的会话计数 依次在实例下拉菜单中打开每个

在特定 UPF 上清除会话 导航到该实例，然后选择会话

配置档案：设备配置备份

配置档案 保留每个上传配置的网络设备的配置，并使收集内容可搜索、可排序和可比较。路由器根据自己的计划导出自己的配置并将其推送到 OmniWeb；页面显示到达的内容、其中的内容以及自上次以来的变化。

← 操作指南

它是什么

路由器和交换机无法运行日志代理或备份客户端，但它们都可以上传文件。因此，档案将这一能力转化为记录每个设备运行的所有配置。

投放在 **OmniWeb** 服务内部 运行。没有边车进程，没有额外的包，也不需要在主机上安装任何东西：监听器是应用程序的一部分，使用 Python 标准库编写。

为什么选择 **FTP**

RouterOS `/tool fetch` 通过 FTP 或 SFTP 上传文件。它也可以发送 HTTP POST，但主体来自 RouterOS 变量，而变量最多只能容纳 4 KB，远低于配置导出。因此，FTP 是设备和 OmniWeb 共同支持的唯一传输方式，适用于这种大小的文件。

FTP 以明文传输密码和配置。请在管理网络上运行，并在防火墙中限制源地址。

投放接受什么

监听器实现了设备需要传递文件的 FTP 部分，并拒绝其余部分。

操作	结果
`STOR` 一个文件	被接受，设备可以将其放置在任何位置。
`RETR`、`LIST`、`NLST`、`MLSD`	被拒绝。投放是只写的：无法通过 FTP 读取任何内容。
`DELE`、`RMD`、`RNFR`、`RNTO`	被拒绝。设备可以添加备份，但永远无法删除或重命名。
`CWD` 进入不存在的目录	被接受。树是虚拟的，路径变为设备名称。
`MKD`	被接受，但不创建任何内容。目录由上传隐含。
包含 `..` 的路径	在任何内容接触磁盘之前被规范化。上传进入档案内部。
超过大小限制的上传	被拒绝，返回 `552`，且不写入任何内容。

两种文件类型都被支持，档案对它们的处理方式不同：

- 文本，例如 RouterOS `/export`（`.rsc`），或任何 `.txt`、`.conf` 或 `.cfg`。文本被索引，因此可以搜索和比较。
- 二进制，例如 RouterOS `/system backup`。文件逐字保存以供恢复，并在列表中标记为二进制。

身份：地址，而不是名称

源地址是身份。一切都基于字节实际来自的地址：上传加入哪个系列，与什么进行比较，以及谁的保留计数。这是 TCP，因此发送者无法伪造地址而不持有它：握手必须完成。

名称只是一个声明。 RouterOS `dst-path=<identity>/<file>` 给出第一个路径元素，而裸 `edge-rtr09-20260910.rsc` 给出 `edge-rtr09`。任何发送者都可以声称任何名称，因此档案存储它、显示它和搜索它，而不以此为键。

这就是使开放投放安全运行的原因：

某人上传	发生的事情
从路由器自己的地址	加入该路由器的系列，作为下一个备份。
从不同地址，声称是路由器的名称	在真实系列旁边启动自己的系列。它无法伪造真实路由器的变化，也无法在真实路由器的历史中泛滥，直到保留将真实备份的历史老化。
从新地址	一个新系列，在 Slack 中宣布一次，因此意外的发送者是可见的，而不是沉默的。

源的标签最初是其上传所称呼的内容，这方□但不可信。为源固定一个真实名称，以阻止上传移动它。

这一模型的成本：真正更改地址的设备会启动一个新系列，因此其历史会分裂。为两者固定标签，或将旧系列视为已关闭。

配置

没有任何配置。投放在端口 2121 上运行，开放，一旦 OmniWeb 启动。将设备指向它并进行上传。

这是故意的，而不是捷径。保护档案的不是密码：FTP 以明文发送它，而路由器将其保存在它们上传的配置中，因此任何可以读取档案或嗅探管理网络的人都已经拥有它。保护档案的是，发送者只能写入其持有的地址的系列，这一点 TCP 使其真实持有。防火墙是重要的控制；将端口限制为您的设备。

设置密码以在地址检查之上要求一个，或设置 `OMNIWEB_CONFIG_ARCHIVE_FTP=0` 以保持档案页面没有监听器。表中的其余部分适用于不寻常的站点，以下每个值都是不需要设置的合理默认值。

环境变量	默认值	描[
`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD`	(空)	设置一个以[查之上要求[是正常运行[
`OMNIWEB_CONFIG_ARCHIVE_FTP_OPEN`	`1`	接受没有密[传。设置 `0` 码以要求一[
`OMNIWEB_CONFIG_ARCHIVE_FTP_USER`	`devbackup`	设备进行身[用户名。
`OMNIWEB_CONFIG_ARCHIVE_FTP_PORT`	`2121`	控制端口。[可以绑定特[使用 21[
`OMNIWEB_CONFIG_ARCHIVE_FTP_HOST`	`0.0.0.0`	监听的地址[
`OMNIWEB_CONFIG_ARCHIVE_PASV_MIN`	`40000`	第一个被动[口。为设备[围。
`OMNIWEB_CONFIG_ARCHIVE_PASV_MAX`	`40100`	最后一个被[口。
`OMNIWEB_CONFIG_ARCHIVE_ROOT`	`backend/data/config-archive`	文件存放的[个设备一个[
`OMNIWEB_CONFIG_ARCHIVE_MAX_BYTES`	`33554432`	大于此的上[绝。
`OMNIWEB_CONFIG_ARCHIVE_MAX_TEXT_BYTES`	`4194304`	文本大小最[以□进行搜[比较。更大[保存在磁盘[

环境变量	默认值	描[
`OMNIWEB_CONFIG_ARCHIVE_RETENTION_DAYS`	`365`	超过此年龄[被删除。
`OMNIWEB_CONFIG_ARCHIVE_KEEP_MINIMUM`	`10`	每个设备保[备份，无论[何。
`OMNIWEB_CONFIG_ARCHIVE_FTP`	`1`	设置为 `0` 案页面但从[听器。
`OMNIWEB_CONFIG_ARCHIVE_TIMEOUT`	`120`	在空闲控制[滞传输被丢[秒数。
`OMNIWEB_CONFIG_ARCHIVE_RETRY_SECONDS`	`20`	丢失绑定的[多长时间尝[这也是在持[作线程被回[放可以不被[间。
`OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK`	(空)	Slack [webho 表示没有通[
`OMNIWEB_PUBLIC_URL`	(空)	此 Omn 的公共基础 用于将 Sl 息链接回档[
`OMNIWEB_CONFIG_ARCHIVE_MAX_DIFF_BYTES`	`262144`	最大存储的[大的变化在[断。

环境变量	默认值	描[
`OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN`	(空)	Prome 必须提供的 Bearer 抓取指标。[开放。

OmniWeb 运行多个 gunicorn 工作线程，每个工作线程启动投放。恰好一个赢得绑定并提供服务；其他的待命并重试，因此监听器在工作线程被回收时仍然存活。页面报告每个进程的 `listening_here`，因此在一个请求上返回 `false` 并不是故障。

变更跟踪和 Slack

每次上传都会与 来自同一源 的上一个上传进行比较，类型相同。相同类型意味着相同扩展名，因此每晚发送文本导出和二进制备份的设备会将每个与其前一个版本进行比较，而不是在它们之间交替并将所有内容称为变化。相同的字���意味着没有变化，无论文件是什么。不同字节的文本文件会生成统一的差异和行计数，均存储在行上，因此页面和通知从不重新计算它们。不同的二进制文件会被记录为已更改，但没有差异，因为没有可读的内容可以显示。

什么不算作变化

设备在导出时会标记其运行时间。RouterOS 每次打开 `/export` 时都会写入

```
# sep/10/2026 08:25:00 by RouterOS 7.24.2
```

因此两次未触动路由器的导出因该行而不同，且没有其他变化，每次运行时都会以新名称写入文件。按原始比较，每个设备每晚都会报告变化，并将其发布到 Slack，并将唯一值得关注的信号淹没在每个设备的每日误报中。

因此，在进行任何比较之前，这些行会被删除，仅用于比较：存储的文件和可搜索的文本保留设备发送的内容。

被忽略	原因
`# <date> <time> by RouterOS <version>`	RouterOS 导出头。每次运行时都会变化。RouterOS 7 写入 ISO 日期（`2026-09-10 11:39:35`），RouterOS 6 写入 `sep/10/2026`；模式匹配它们共享的形状，而不是任何一种渲染。
`# software id = ...`	在某些 RouterOS 导出中存在。
`! Last configuration change at ...`	Cisco IOS。每次写入时都会变化���包括设备。
`! NVRAM config last updated at ...`	Cisco IOS。
`ntp clock-period ...`	Cisco IOS。自行漂移，与操作员无关。

文件名根本不参与比较：上传与来自同一源的上一个上传（具有相同扩展名）进行匹配，因此带有时间戳的名称不会改变任何内容。

设置 `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS` 为一个用 `|||` 分隔的正则表达式列表，以替换此列表以适应标记其他内容的供应商。

更改模式后，请重新哈希档案。每个备份存储其规范化配置的哈希，因此新模式会使每个存储的哈希过时：来自每个设备的下一个上传将不再与其历史匹配，存储重复文件并报告未发生的变化。

```
sudo -u omniweb /opt/omniweb/backend/venv/bin/python
/opt/omniweb/backend/manage.py \
  rehash_config_archive --dry-run     # 首先报告
sudo -u omniweb /opt/omniweb/backend/venv/bin/python
/opt/omniweb/backend/manage.py \
  rehash_config_archive
```

该比较驱动两个方面：

- 页面。每一行显示 `+N/-N` 当配置发生变化时，或当设备再次发送相同文件时显示一个勾号。仅变化 将列表缩小到实际更改了某些内容的上传。
- **Slack**。变化会发布到传入的 webhook，包含源、行计数、差异的前 40 行���及链接回档案。第一次听到的地址也会发布一次，首先命名地址，其次是它声称的内容。

□□□

呈现。未设置则保持开放，展现名称设备和地址，因此在任何可达的地方设置它。

```
scrape_configs:
  - job_name: omniweb_config_archive
    metrics_path: /api/config-archive/metrics
    static_configs:
      - targets: ['<omniweb-host>']
    authorization:
      credentials: '<OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN>'
```

指标 类型 描述

config_archive_last_upload_timestamp_seconds | Gauge

来自此源的最后上
传，无论是否更改。
这是需要警报的。
0 表示从未上传，
因此相同的警报捕获
从未启动的设备。

config_archive_last_change_timestamp_seconds | Gauge

最后一次配置不同的
上传。0 表示从未
更改。

config_archive_uploads_total | Counter

自源首次被看到以来
接收的上传。保留不
会降低它。

config_archive_changes_total | Counter | 更改了配置的上传。

config_archive_retained_backups | Gauge | 保留的备份，经过保

留处理。

config_archive_retained_bytes | Gauge | 保留的字节，经过保

留处理。

config_archive_sources | Gauge | 档案曾经听到的源。

config_archive_ftp_enabled | Gauge | 投放是否配置为运

行。

config_archive_ftp_bound | Gauge

投放套接字是否在主
机上接受连接。对此
进行警报。任何工作
线程都可以回答，因
为它是通过本地连接
测量的。

指标	类型	描述
`config_archive_ftp_listening_here`	Gauge	回应此抓取的工作线程是否是持有套接字的那个。仅用于调试：通过 nginx 的抓取落在池的任意工作线程上，因此这是一个抛硬币。永远不要对此发出警报。

每个系列都携带 `source`（地址，身份）和 `label`（显示名称，直到操作员固定它之前，这只是上传所声称的内容）。

值得关注的警报

```
# 设备停止备份，或从未启动。每日计划加上 Slack。
(time() - config_archive_last_upload_timestamp_seconds) > 172800

# 没有人在提供投放服务。
config_archive_ftp_bound == 0 and config_archive_ftp_enabled == 1

# 突然每次运行都变化的设备，这通常意味着其导出
# 携带时间戳，而不是有人在编辑它。
increase(config_archive_changes_total[1d]) > 3
```

保留

保留按 源 运行，这就是重点：一个发送者填充自己的系列永远无法使另一个发送者的备份过期。超过保留窗口的备份将被删除，除了每个源的最新几个备份始终保留。因此，停止上传的设备将永远保留其最后已知的良好配置，单靠年龄永远不会清空设备的历史。

相同 配置 的上传在磁盘上共享一个文件，以与变化相同的方式进行比较：去除导出的时间戳和其他易变行。这比听起来更重要。RouterOS 导出将其运行时间戳印在第一行，因此原始字节每晚都会有所不同；如果将存储键入它们，将会每晚为未触动的路由器配置写入新副本。

因此，每晚上传未更改的配置的路由器仍然会每晚获得一行，这就是使“我们听到了它”可见的原因，而字节只存储一次。

配置 MikroTik

在路由器上运行两个命令。将 `<omniweb-host>` 设置为您的 OmniWeb 地址。不需要密码，下面的凭据会被忽略：投放通过上传的地址识别设备。

```
/system script add name=config-backup policy=read,write,ftp,test
source=":local id [/system identity get name]; :local d [/system
clock get date]; :local t [/system clock get time]; :local base
(\$id . \"-\" . \$d . \"-\" . [:pick \$t 0 2] . [:pick \$t 3 5]);
/export file=\$base; :delay 5s; /tool fetch address=<omniweb-host>
port=2121 mode=ftp user=omniweb password=x src-path=(\$base .
\".rsc\") dst-path=(\$id . \"/\" . \$base . \".rsc\") upload=yes;
:delay 2s; /file remove [find name=(\$base . \".rsc\")];"

/system scheduler add name=config-backup interval=1d start-
time=02:15:00 on-event="/system script run config-backup"
policy=read,write,ftp,test comment="每晚配置导出到 OmniWeb 配置档案"
```

手动运行一次以验证路径，然后再信任计划：

```
/system script run config-backup
```

成功运行会打印 `status: finished` 及上传大小，设备会在几秒钟内出现在档案中。

为什么这样写

细节	原因
整个脚本是 一行	RouterOS CLI 拒绝在通过 SSH 到达的命令中使用反斜杠续行。跨多行编写的脚本在终端中粘贴正常，但从自动化中失败，出现简单的 `syntax error (line 1 column N)`。
`policy=read,write,ftp,test`	`fetch` 需要 `ftp` 和 `test`。没有它们，运行会因策略错误而失败，什么都不会上传。
`port=2121`	投放的默认值。`/tool fetch` 将端口与地址分开处理。
`user=omniweb password=x`	占位符。投放接受任何凭据，因为源地址是身份。`fetch` 仍然希望这些参数存在。
`[find name=...]` 在 `/file remove` 中	`/file remove` 需要一个内部 ID，而不是名称。直接传递名称会失败，导出将留在路由器上，随着时间的推移填满其存储。
`:delay 5s` 在 `/export` 之后	导出是异步写入的。立即上传可能会捕获部分文件。
`$d` 在文件名中	RouterOS 7 将日期呈现为 `2026-09-10`，因此文件自然排序。每次运行名称都会变化，这没关系：档案将上传与来自同一源的上一个上传进行匹配，而不是通过文件名。

在路由器之间错开 `start-time`，以它们不会同时上传。

要保留二进制备份，请添加 `/system backup save name=$base` 并以相同方式上传 `$base.backup`。文本导出是进行差异比较的，而二进制备份是恢复到相同硬件上的。

任何可以通过 FTP 上传的设备都以相同方式工作：将其指向主机和端口，让其命名自己的文件。

使用页面

配置档案 在侧边栏中，位于主机列表下。

控制 功能
静默横幅 | 命名每个在 48 小时内未上传的源，以及持续的时间。这是签入，因此仅在设备发送未更改的备份时停止发送时触发。
源 | 过滤到一个源地址。每个条目显示其最后推送的时间，并标记为静默。
名称、地址或文件 | 在声称的名称、源标签、地址和文件名中进行子字符串搜索。
配置中的文本 | 搜索配置本身，例如 IP 地址、ospf 或用户名。这是查找哪些设备携带设置的最快方法。
列标题 | 按设备、文件、接收时间或大小排序。
仅变化 | 将列表缩小到更改了配置的上传，隐藏未更改的每晚备份。
变化列 | 当配置发生变化时显示 +N/-N，当设备重新发送相同文件时显示勾号。
一行 | 打开配置，与该设备的上一个备份进行差异比较。
下载 | 文件与设备发送的内容完全相同。
添加文件 | 手动上传配置，适用于无法推送的设备。
The diff是赚钱的部分：它回答“这个路由器上发生了什么变化，以及何时发生的”而无需设备登录。

API

所有端点都需要经过身份验证的会话。

方法和路径	描述
`GET /api/config-archive/backups`	列出，包含 `source`、`address`、`q`、`content`、`changed`、`ordering`、`limit` 和 `offset`。
`POST /api/config-archive/backups`	手动添加备份：multipart `file`，可选 `device`。
`GET /api/config-archive/backups/<id>`	一个备份及其文本。
`GET /api/config-archive/backups/<id>/download`	存储的文件。
`GET /api/config-archive/backups/<id>/diff`	与之前备份的统一 diff，或 `?against=<id>`。
`GET /api/config-archive/sources`	每个源地址一行：备份计数、变化、最新上传、大小，以及其上传声明的每个名称。
`PATCH /api/config-archive/sources/<id>/label`	给源固定一个真实名称，以□上传停止移动它。
`GET /api/config-archive/status`	丢弃状态和归档总数。
`GET /api/config-archive/metrics`	Prometheus 文本展示。请参见 Check-in and metrics。

`changed=1` 返回变化信息：与设备之前备份不同的上传。

`ordering` 接受 `received_at`、`claimed_name`、`filename` 和 `size_bytes`，前面加 `-` 以反转。任何其他值将回退到最新优先。

故障排除

症状	检查
页面警告丢弃已关闭	`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD` 未设置。设置后重启 OmniWeb。
设备报告登录失败	确认用户名和密码，然后在 OmniWeb 日志中查找 `config archive ftp: login failed`。
传输开始但停滞	被动范围不可达。从设备打开 `OMNIWEB_CONFIG_ARCHIVE_PASV_MIN` 到 `..._MAX`。
上传到达时名称奇怪	设备发送了一个不以其身份开头的裸文件名。将 `dst-path` 设置为 `<identity>/<file>`，或在源上固定一个标签。
一个设备显示为两个源	它的地址发生了变化，因此开始了一个新系列。在两个上固定标签以使关系明显。
出现意外地址	其他人或其他东西可以访问该端口。检查 Slack 的“现在备份中”消息以了解何时开始，并限制该端口。
列表中缺少设备	它从未完成上传。在设备上手动运行脚本并查看其日志。
Slack 中没���任何消息	确认 `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` 已设置，然后检查上传是否为更改：未更改的备份设计上是静默的。失败记录为 `Slack post failed`。
每个备份都有 Slack 发布	设备在每个导出中印上某些内容，而这些内容不在忽略列表中。比较两个备份以查看哪些内容发生变化，然后将模式添加到 `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS`。

DRA: 直径路由代理

DRA 是核心的直径路由中心。与其让每个节点都保持一个完整的直径连接网，EPC 和 IMS 功能连接到 DRA，由它转发和路由它们的信令：**S6a** 在 MME 和 HSS 之间，**Gx/Gy** 到 PCF/PCRF 和 OCS，**Cx/Dx** 和 **Sh** 用于 IMS，等等。它根据路由规则（基于直径应用、领域或 AVP 匹配）和对等选择算法选择每条消息的去向，并可以使用 转换规则 重写消息。它是直径的 SS7 STP 对应物。OmniWeb 显示 DRA 的对等体、路由规则、实时状态和连接图。吞吐量和趋势图表在同一页面的 Grafana 仪表板上。

← 操作指南

DRA 是一个每实例元素页面，可以通过侧边栏在站点的库存中访问，具有舰队视图（网络图），其中部署了多个实例。所有流量通过 OmniWeb 后端代理到 DRA 的 API，因此它保持在单一的认证网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织成���个选项卡。

网络图

DRA 和它所知道的每个直径对等体的中心辐射视图，连接数量一目了然（例如 *5/6 □□□*）。连接的对等体用绿色链接到 DRA。一个管理上 禁用 或 断开 的对等体显示为灰色和虚线。它是最快的方式在一张图中查看哪些信令邻居处于活动状态。

状态

状态 选项卡报告 DRA 自身的身份和配置：它的 **Origin-Host**、领域、监听 **IP** 和端口（直径通常为 3868）、报告的 产品名称和正在使用的 对等选择算法（例如轮询）。在这里可以确认 DRA 正在运行并按预期配置。

对等体

每个直径对等体，每行显示对等体的 **Origin-Host**、**IP** 和端口、报告的 产品、传输（SCTP 或 TCP）、领域、协商的 直径应用和其 连接状态。对等体可以按名称、应用、领域或状态进行过滤。每个对等体都有一个 启用/禁用 切换。管理上禁用对等体会将其移出路由，而不拆除其配置，这就是如何为维护排空邻居。

规则

活动的 路由规则 和 转换规则，以及它们运行的 路由算法。每个路由规则基于过滤器（一个直径应用、一个 AVP 或所有流量）进行匹配，并解析到一个目标：要么是一个明确的对等体集合，要么是一个命名策略，如 *destination-host* 或 *destination-realm*。在这里可以确认，例如，S6a 被路由到 HSS，Gx 被路由到 PCF。

日志

日志 选项卡跟踪 DRA 的实时日志输出，以□在不离开 OmniWeb 的情况下排查单个路由代理的问题。

监控仪表板

DRA 的消息速率、每个接口的吞吐量和其他时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会本地重复这些图表。

相关

- **MME** 和 **HSS**：DRA 在它们之间转发 **S6a**。

PCF/PCRF (Gx) 和 OCS (Gy)：通过 DRA 路由的策略和计费对等体。 CSCF和HSS：Cx/Dx IMS 信令。
STP：信令平面中 DRA 的 SS7 路由对应物。

权限服务器：OmniSEP
权限服务器 (OmniSEP) 决定了订阅者及其设备可以使用哪些服务。当手机询问是否可以开启 VoWiFi、VoLTE 或 Wi‑Fi Calling，或运行 ODSA 设备配置以添加或激活设备时，它会向权限服务器进行检查。服务器通过 权限 (TS.43) 接口授权请求，通过 Diameter解析订阅者数据，并应用订阅者的 XCAP 服务配置。OmniWeb 在一个元素页面上展示其实时权限、活动、会话、令牌、Diameter 对等体和 XCAP 配置；流量和趋势图表则在从同一页面访问的 Grafana 仪表板上显示。

← 操作指南

OmniSEP 是一个每实例元素页面，可以通过侧边栏在站点的库存中访问。所有流量都通过 OmniWeb 后端代理到权限服务器的 API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。该页面分为多个选项卡。

概述

着陆选项卡是权限服务器的单屏健康读取：其 系统状态、活动 会话 和 令牌 的数量、携带自定义 权限 的订阅者，以及其 Diameter 对等体的健康状况。这是确认服务器正常运行并授权设备的最快方式。

权限

携带 自定义权限 的订阅者：每个订阅者的默认服务集的覆盖。打开一个订阅者以查看为他们启用的服务。操作员可以 删除所有权限，将订阅者恢复到网络默认。这在故障期间清除错误覆盖时非常有用。

活动

最近的 活动 记录：服务器处理的权限请求的馈送，每条记录显示订阅者或设备、请求的服务和结果。打开记录以查看详细信息。这是确认手机是否实际请求了 VoWiFi/VoLTE 及其收到的回答的审计轨迹。

会话

服务器为设备认证持有的活动 EAP‑AKA 会话，每个会话都有其订阅者身份和状态。可以从这里 过期 单个会话，以强制设备重新认证。这是清除卡住的会话的最快方法。

令牌

服务器在设备认证后发放的活动 认证令牌。每个令牌可以单独 撤销，这会撤销设备的授权并要求其重新认证。这是强制重新登录的权限等效项。

Diameter

权限服务器连接的 Diameter 对等体，用于获取订阅者数据，以及每个对等体的 连接状态。当权限决策因看似缺失的订阅者数据而开始失败时，此选项卡是确认 Diameter 路径正常的地方。

XCAP □□

XCAP □□□□

ePDG 和TWAG 提供权限服务器启用的 Wi‑Fi Calling 访问。 DRA 将权限服务器的 Diameter 信令中继到其对等体。

ePDG: 演进分组数据网关
ePDG 是 不受信任的 Wi‑Fi 访问 的安全网关：它是 Wi‑Fi 通话 (VoWiFi) 和不受信任 WLAN 数据背后的节点。手机通过任何互联网连接与 ePDG 建立 IPsec/IKEv2 隧道；ePDG 通过 Diameter (SWm/SWx) 对 AAA/HSS 进行用户身份验证，将会话锚定到分组核心 (S2b 到 PGW)，并强制执行每个用户的速率限制和地理 IP 策略。OmniWeb 显示 ePDG 的实时隧道、其 Diameter 对等体、速率限制和地理 IP 配置以及运行时设置；更长期的趋势可以在同一页面的 Grafana 仪表板上查看。

← 操作指南

ePDG 是一个每个实例的元素页面，可以通过侧边栏在站点的库存中访问。所有流量都通过 OmniWeb 后端代理，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织成多个选项卡。

概述

单屏健康读取：ePDG 的 状态、活动会话（IPsec 隧道）的数量，以及网关的操作状态摘要。这是确认 ePDG 正在运行并承载 Wi‑Fi 通话隧道的最快方式。

会话

每个活动会话：当前建立的 IPsec/IKEv2 隧道，按用户划分，显示隧道和承载状态。您可以检查会话以查看其详细信息。这是确认特定用户的 Wi‑Fi 通话隧道是否正常的地方。

Diameter

与 AAA/HSS 的 Diameter 对等连接，承载身份验证 (SWm/SWx)，以及每个对等体的连接状态。当 Wi‑Fi 通话身份验证失败时，这是首先查看的地方。

速率限制器

ePDG 终止不受信任的 Wi-Fi IPsec/IKEv2 隧道 (SWu) 并通过 S2b 将其桥接到 EPC，这使其暴露于任何手机（或任何来源）在开放互联网中。速率限制器 是防止客户端猛烈攻击隧道设置的防御：它限制 IKE 洪水，以□单个行为不当的手机或攻击源无法耗尽网关。该选项卡显示强制执行的 阈值，以及当前被 阻止的 **IP** 和 **IMSIs** 的实时计数。阈值是 每个 **IP** 和 每个 **IMSI** 的请求限制，每个限制表示在滚动 窗口 内的身份验证尝试次数，以及一旦超过限制应用的 阻止持续时间。

在阈值下方，您可以 查找 任何 IP 地址或 IMSI，以查看它是否被阻止以及它累计了多少次失败，并 清除 该阻止，以□未来的身份验证尝试再次被允许；单个 清除所有 操作会一次性删除所有阻止并重置所有失败计数器。这是操作员确认为什么用户的 Wi-Fi 通话隧道被拒绝的地方，并在问题源得到解决后释放阻止。

GeoIP

GeoIP 是 ePDG 的基于国家的准入控制：操作员如何通过将每个传入隧道的源 IP 与 GeoIP 数据库进行匹配，限制 VoWiFi 隧道的建立到允许的国家。该选项卡显示过滤是否 启用 以及数据库是否 准备就绪（已加载且可用）、模式 和 国家列表。模式可以是 白名单（仅列出的国家可以连接）或 黑名单（列出的国家被拒绝）。它还显示 正在使用的 **GeoIP** 数据库 以及是否允许或阻止 未知国家的 **IP**。这些是数据库无法解析为国家的源地址。

一旦 GeoIP 数据库文件在磁盘上更新，选项卡可以 重新加载 它，以新的映射生效而不干扰已建立的隧道。这是将 VoWiFi 隧道设置限制在操作员服务的区域的控制。

配置

ePDG 的运行时 配置、速率限制 规则（保护网关的每个用户/每个来源限制）和 地理 **IP** 策略（允许哪些源区域建立隧道）。这些是决定谁可以连接以及连接的激进程度的控制。

日志

日志 选项卡跟踪 ePDG 的实时日志输出，以□在不离开 OmniWeb 的情况下进行单个网关的故障排除。

监控仪表板

ePDG 的隧道速率、吞吐量和其他时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

- **PGW** 将 ePDG 的用户平面锚定在 **S2b** 上。
- **AAA/HSS** 保存 ePDG 的 Diameter 请求所解析的用户身份验证数据。

- TWAG□□□□□ Wi-Fi □□□

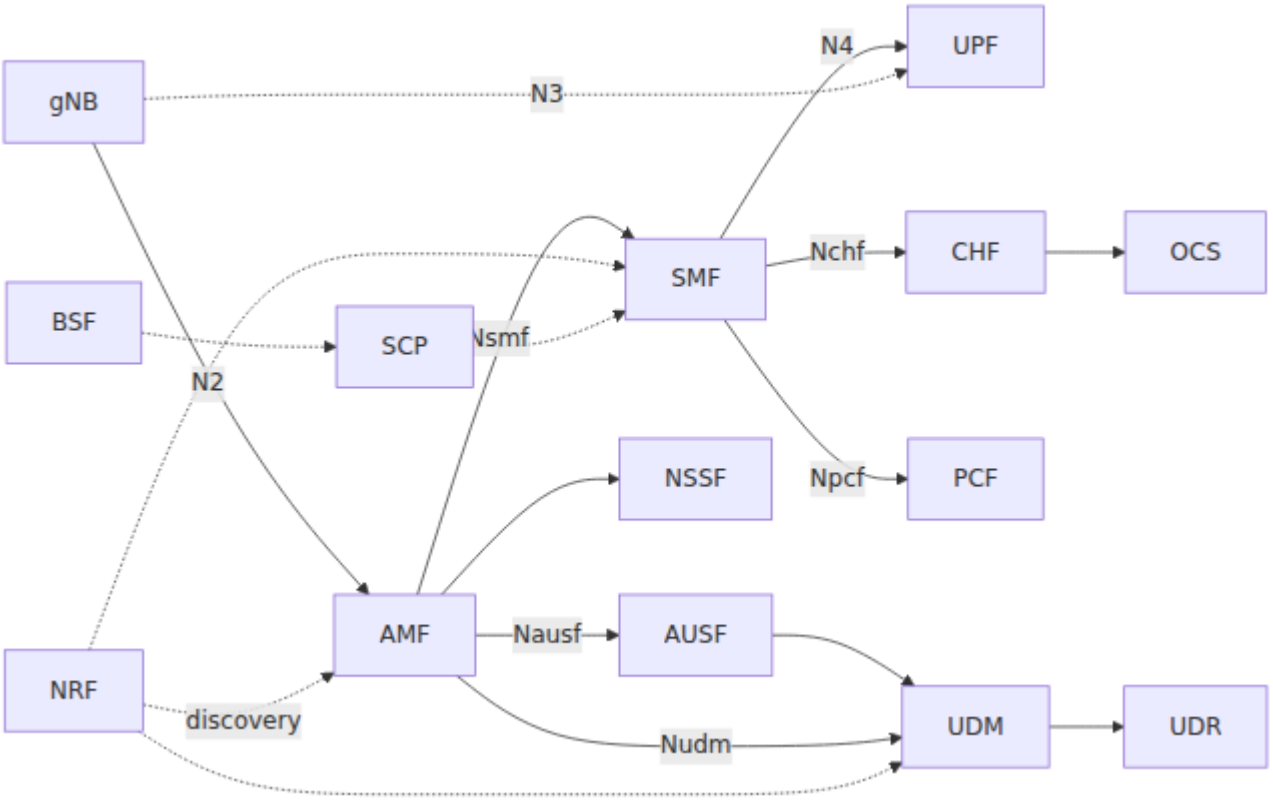
5G核心
5G核心部分为每个5GC网络功能（NF）提供自己的实时仪表板。每个仪表板显示健康状况、注册信息以及NF拥有的操作数据（UE上下文、 PDU会话、IP池、NRF注册、策略、计费会话）。它还提供每个NF和每个项目的清除状态操作。这是5GC相当于EPC/IMS功能的每个元素页面。它通过OmniWeb后端代理读取每个NF的OAM API。

← 操作指南

何时出现

5G核心组仅在选定站点实际运行5GC控制平面时在侧边栏中显示。OmniWeb根据站点库存中存在的AMF和/或SMF来判断。与 EPC共享的孤立UPF或CHF不是5GC，因此不显示此部分。

OmniWeb直接从站点的Ansible库存中推导出出现的NF及每个NF的OAM API地址：在主机文件中定义的5GC NF组。因此，添加或移动NF是库存更改，无需手动模板。每个NF解析为一个标签、描述、IP和端口。OmniWeb通过/api/5gc/nf-registry提供解析后的注册表。然后，仪表板通过代理查询每个NF的OAM API（/api/5gc/nf/<id>/…），因此所有流量都保持在单个经过身份验证的网关后面。请参见配置模型。运行无库存的部署（例如托管服务）将回退到OmniWeb配置中的静态 fivegc块。



NFs

每个NF都有自己的仪表板:

NF	功能	关键数据
NRF	网络存储库功能	注册的NF实例（按类型分组）、注册的服务、订阅：见下文
AMF	接入与移动管理	UE列表、连接的gNodeBs（带解码的gNB-ID / TAC / PLMN / SST）、统计信息、维护模式
SMF	会话管理	PDU会话、**IP**池、UPF关联、统计信息
UDM	统一数据管理	UE列表、统计信息
UDR	统一数据存储	HSS健康状况、订阅者
AUSF	认证服务器	AUSF（认证）会话、统计信息
PCF	策略控制	AM策略、SM策略、统计信息
CHF	计费功能	计费会话、CGrateS健康状况、CDR记录
NSSF	网络切片选择	切片、NSSAI可用性、统计信息
BSF	绑定支持	PCF绑定、统计信息
SCP	服务通信代理	NF健康状况、发现缓存、统计信息

并非每个部署都运行每个NF。仅在站点库存中定义的NF才会出现。每个NF都有自己的参考页面。请按照上面的链接进行访问。

SMF的**IP**池选项卡

作为这些仪表板展示的NF拥有数据的一个示例：SMF仪表板有一个**IP**池选项卡，显示SMF分配UE IP的地址池，以及其实时的**PDU**会话和**UPF**关联（与用户平面的N4/PFCP链接状态）。这些共同回答“SMF是否连接到其UPF，哪些会话处于活动状态，以及它是否快用完地址？”而无需离开OmniWeb。

一目了然的仪表板

每个NF仪表板遵循相同的布局：

1. 健康卡位于顶部：API健康状况、NRF注册（该NF是否已在NRF中注册？）、NF状态和许可证。每个卡片按间隔轮询。使用标题中的轮询指示器暂停或查看最后更新的时间（轮询是一个共享模式：请参见常见操作）。
2. 操作：NF级别的操作（见下文）。
3. 数据部分：API状态详细信息、NRF注册详细信息，以及上表中的NF特定表格，每个表格都自动刷新。表格会自动解码它们能解码的内容：PLMN/TAC/SST来自Erlang编码的S1AP术语，时间戳转换为相对时间，状态转换为彩色芯片，以及交叉链接（NF类型值链接到该NF的仪表板）。

操作

仪表板公开操作以清除NF状态。每个操作首先请求确认，因为它们是破坏性的：

NF NF级别操作 每行操作

AMF 清除所有UE上下文 · 清除缓存 注销一个UE

SMF 释放所有PDU会话 · 清除缓存 · PFCP重新关联（重新建立UPF关联） 释放一个PDU会话

NRF 注销所有NF 注销一个NF · 移除一个订阅

AUSF 清除所有认证会话 清除一个会话

UDM 清除订阅者缓存 -

PCF - 移除一个AM或SM策略

这些操作允许操作员从卡住的状态中恢复。例如，强制一个失去UPF的SMF重新关联，删除一个无法清除的UE上下文，或从NRF中注销一个过时的NF。

NRF仪表板

NRF获得更丰富的视图，因为它是整个5GC通过其发现的注册表：

指标卡：NF类型、总实例、注册（带百分比条）和服务/订阅。注册的NF实例：按NF类型分组。仪表板对每个实例卡进行颜色编码。卡片显示注册状态、心跳计时器、服务计数和PLMN。点击实例以查看其完整配置文件（带有打开仪表板链接到该NF和注销按钮）。
注册的服务：每个实例广告的每个服务的平面表格，包括其版本和状态。
注销所有NF：清除每个注册（每个NF必须重新注册）。

这使得NRF成为回答“哪些NF处于活动状态，它们都注册了吗，它们提供什么服务？”的地方。

相关

网络拓扑：链接到这些仪表板的拓扑视图。
常见操作：与每个元素页面共享的轮询、配置和RBAC模式。
PGW-C / SMF和UPF：用于融合EPC+5GC的EPC侧会话/用户平面页面。

Grafana 仪表板与统计信息

OmniWeb 将 Grafana 直接嵌入到门户中。操作员可以查看任何元素以及整个网络的仪表板和统计信息，而无需单独登录或打开浏览器标签。

← 返回操作指南

工作原理

Grafana 在经过身份验证的网关后提供服务，路径为 `/grafana/`，并作为 iframe 嵌入到 OmniWeb 中。身份验证是透明的：当您登录到 OmniWeb 时，Grafana 访问会自动根据您的 OmniWeb 登录进行授权。没有第二个密码。

OmniWeb 代理的 Grafana 实例由 `GRAFANA_URL` 环境变量配置（默认 `http://localhost:3000`）。网关透明地处理代理和单点登录检查。

两种访问仪表板的方法

1. 每个元素的仪表板标签

被标记为 Grafana 的元素在其工作区中显示 仪表板 标签。OmniWeb 查询 Grafana 以获取与该元素标签匹配的仪表板，并在内联中呈现相关的仪表板。这使得元素的统计信息与其操作数据紧密相邻。

标签匹配不区分大小写。代表性标签集：

元素	匹配的 **Grafana** 标签
UPF	`upf`
P-CSCF	`pcscf`, `cscf`
I-CSCF	`icscf`, `cscf`
S-CSCF	`scscf`, `cscf`
PGW-C, MME, SMSC, DRA, OCS, TAS	元素特定标签

要使仪表板出现在元素下，请在 Grafana 中使用该元素的标签标记它（例如，将 UPF 仪表板标记为 `upf`）。

2. Grafana 侧边栏

侧边栏的 **Grafana →** 仪表板 条目列出所有可用的仪表板。选择一个仪表板将在 OmniWeb 中内联打开，并且 URL 会更新以反映仪表板路径，以□您可以深度链接到特定仪表板。

统计信息

嵌入的仪表板是网络范围和每个元素的 统计信息 的所在：会话计数和速率、吞吐量、延迟、丢包率、Diameter/PFCP 对等体健康状况随时间变化、CDR 量、注册计数和容量趋势。OmniWeb 自身的元素页面为您提供 □□ 状态（并让您对此进行操作）；Grafana 为您提供 □□ 画面和趋势。它们旨在一起使用。通过跳转到元素的操作页面、日志和跟踪来调查 Grafana 警报。

警报

Grafana 内置的警报引擎处理所有基于阈值的警报。警报规则在 Grafana 中定义，并可以通过电子邮件、Slack、PagerDuty 或 webhook 进行通知。OmniWeb 不重复警报功能。它提供了调查警报触发时所需的操作上下文（元素页面、日志、跟踪）。

常见警报类别：

类别	示例
可用性	元素无法访问、Diameter 对等体宕机、PFCP 关联丢失
容量	IP 池耗尽、eBPF 映射利用率 > 80%、VLR 订阅者计数阈值
性能	会话建立延迟、XDP 丢包率、心跳失败
流量	异常 CDR 量、呼叫丢失率、SMS 投递失败

调查警报：推荐流程

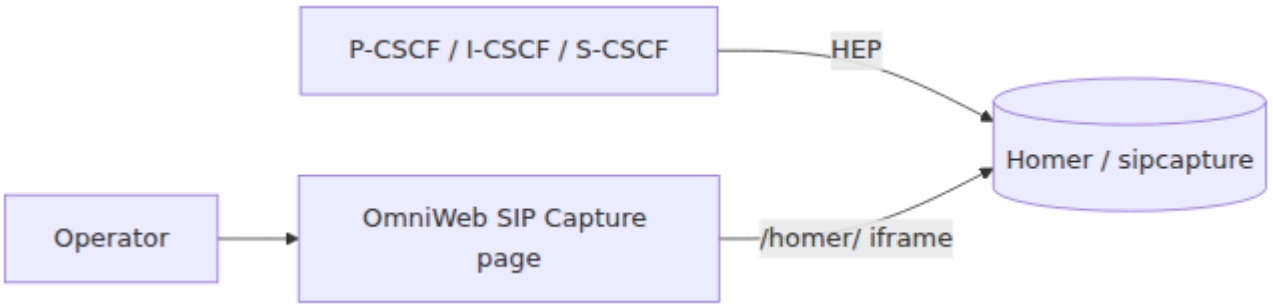
1. 在 Grafana 中确认趋势（仪表板）。
2. 检查元素概览中的当前状态。
3. 阅读警报时间段内的元素日志。
4. 如果是特定于订阅者的，运行会话跟踪。请参见 日志与订阅者跟踪。

Homer: SIP 捕获与呼叫流程分析
Homer 是一个 SIP 捕获和搜索系统 (HEP / sipcapture)。OmniWeb 直接嵌入了 Homer 的 Web UI，因此您可以搜索捕获的 SIP 流量，并在不离开门户或单独登录的情况下重建呼叫的信令流程。

← 操作指南

它是什么

Homer 从 IMS 收集 SIP 消息（通过 HEP 协议）并按呼叫 ID、来电/去电号码、时间等进行存储以供搜索。它的 Web UI 让您找到一个呼叫并绘制其完整的 流程图：每个端点与 CSCFs 之间的每个 SIP 消息，包含时间和任何故障/挂断原因。OmniWeb 并没有重新实现这些功能。它 在 SIP 捕获 下的 iframe 中 嵌入了 Homer 应用（在侧边栏的会话追踪下嵌套）。



单点登录

您不需要单独登录 Homer。OmniWeb 在 /homer/ 处代理 Homer 应用，并在传输过程中注入 auth-proxy 头，因此嵌入的 UI 已经通过身份验证，无需 Homer 登录提示。它通过与 Grafana 和 Loki 相同的经过身份验证的 OmniWeb 网关访问，因此一个 OmniWeb 登录也适用于它。

SIP 捕获 条目仅在 Homer 已配置并可访问 时出现在侧边栏中。OmniWeb 会探测它，并在不存在时隐藏该条目，因此您永远不会点击进入一个死页面。

Homer 与会话追踪

OmniWeb 有两种互补的方式来查看信令，了解何时使用哪种方式是有帮助的：

	Homer (SIP 捕获)	会话追踪
范围	仅 SIP，深入分析	整个网络：Diameter、GTP-C、PFCP、SIP、MAP
回答的问题	“这个 □□ 的 SIP 流每条消息做了什么，时间和挂断原因是什么？”	“这个 □□ 在每个元素中发生了什么？”
最佳用途	诊断 VoIP/VoLTE 呼叫、失败的注册、特定的挂断	追踪一个 IMSI/MSISDN 端到端通过核心

当您需要剖析一个呼叫时，请使用 Homer；当您需要在整个堆栈中跟踪一个用户时，请使用会话追踪。Homer 也可以从 日志与用户追踪指南中链接访问。

相关

- 日志与用户追踪：跨网络的会话追踪以及 Homer 的适用位置。
- Grafana 仪表板与统计：另一个嵌入的监控工具，以相同的经过身份验证的方式访问。

HSS：家庭用户服务器

HSS（家庭用户服务器）是移动核心的主用户数据库。它保存每个用户的身份（IMSI、MSISDN 和 SIM/ICCID）、证明他们身份的认证密钥材料，以及声明每个用户在网络上可以做什么的 EPC、IMS、PCRF 和漫游服务配置文件。MME 通过 S6a 读取它以验证和定位设备，并了解其 EPC 订阅。CSCF 通过 Cx 读取它以进行 IMS 注册和 iFC 服务触发。PCRF 从中提取其策略和计费规则。运营商使用其仪表板来配置和搜索用户，策划共享服务配置文件，并检查 HSS 自身的健康状况。

← 操作指南

仪表板是每个实例的元素页面。当 HSS 在站点的库存中运行时，它从侧边栏打开。所有流量都通过 OmniWeb 后端代理到 HSS 的 API，因此它保持在单一的经过身份验证的网关后面。响应以 `{status, response}` 信封的形式返回。页面头部的文档链接提供上下文帮助。页面有多个选项卡。

用户

着陆选项卡是用户目录。通过 **IMSI**、**MSISDN** 或 **ICCID** 搜索以查找记录。搜索还可以通过 **IP** 地址解析用户，当您追踪实时会话回到其所有者时。打开记录以显示用户概述：一个将用户与其身份（IMSI）、状态（启用，以及 IMS 是否启用）以及分配给它的 **EPC**、**IMS** 和漫游配置文件联系起来的关系图。页面在 EPC 配置文件下显示配置文件的 APN。HSS 保存敏感的密钥值，但不显示它们。您可以更新它们，但它们以编辑后的形式返回。

配置

从配置表单创建或编辑用户。该表单将身份、凭据、SIM 和配置文件汇集在一个地方：

- 用户身份：IMSI、用户名称，以及 启用 和 **IMS** 启用 开关。
- 认证密钥集：认证算法、**Ki** 和 **OPc**（或 **OP**）、**AMF**、**SQN**，以及用于 IMS 的 SIP 密码。
- **SIM** 卡：**ICCID**、是否为 eSIM、PIN/PUK 值以及批次和供应商详细信息。
- 电话号码：分配一个或多个 **MSISDN**。在输入时搜索现有号码，以重复创建号码。
- 分配配置文件：附加给用户的 **EPC**、**IMS** 和 漫游 配置文件，以提供其服务。

您可以以相同的方式更新现有用户。您可以从其记录中删除用户。

SIM 卡

SIM 库存保存 HSS 知道的每个 SIM。通过 ICCID 搜索。每个 SIM 都携带其 ICCID、eSIM 标志、批次名称和供应商、其传输密钥值（KIC、KID）和 eSIM LPA，以及完整的 ADM 密钥 集。您可以创建、编辑和删除 SIM 卡。与 SIM 记录配对的认证 密钥集 在其单独的选项卡上管理。

MSISDN

MSISDN 目录保存已配置电话号码的池。通过 数字 搜索以进行部分匹配，查找或检查号码，然后再分配它。您可以创建、编辑和删除号码。在配置过程中将号码附加到用户。

□□□

□□□

EPC 配置文件

MME 强制执行的分组核心订阅。**EPC** 配置文件 设置 网络接入模式、UE-AMBR 下行/上行 聚合带宽、**TAU** 间隔，以及用户可以使用的 **APN** 配置文件 列表。一个 APN 是 默认 **APN**。每个 **APN** 配置文件 将 **APN** 标识符 与 **APN QoS** 配置文件 和 **PCRF** 配置文件 关联。您可以将 APN 配置文件标记为默认。EPC 配置文件必须至少引用一个 APN 配置文件。默认 APN 必须是分配的 APN 之一。

展开 EPC 配置文件以列出其 APN 配置文件。添 **APN** 将 APN 附加到配置文件。每行的解除链接操作 仅从此 **EPC** 配置文件中移除它。HSS 保留 APN 配置文件本身。您可以稍后重新添加它，或者其他 EPC 配置文件可以重用它。配置文件必须保留至少一个 APN，因此您无法删除最后一个。HSS 自动清除默认 APN，如果您删除了它指向的 APN。

APN 配置文件

APN 配置文件选项卡独立列出每个 APN 配置文件，而不考虑使用它的 EPC 配置文件。它显示其 **APN** 标识符、**APN QoS** 配置文件 和 **PCRF** 配置文件。使用者 列命名每个引用 APN 的 EPC 配置文件。当没有 EPC 配置文件引用它时，它标记为 孤立。一旦您从最后一个使用它的 EPC 配置文件中删除它，APN 就会达到此状态。仅孤立 切换过滤列表，仅显示这些，以您可以查找并清理未使用的 APN。

您可以在此处创建配置文件、编辑它们和删除它们。新配置文件开始时未附加。要将其链接到用户的服务，请将其添加到 EPC 配置文件中。您无法删除仍链接到一个或多个 EPC 配置文件的 APN 配置文件。首先从这些配置文件中删除它，然后从此选项卡中删除它。

APN QoS 配置文件

APN QoS 配置文件选项卡管理 EPC 和 APN 配置文件指向的可重用 APN 级 QoS 模板。每个引用模板的用户的 APN 在其默认承载上获得相同的服务质量。每个模板携带一个 名称 和一个 **QCI**（QoS 类标识符，将承载映射到标准化的延迟和丢失行为）。它还携带一个 **ARP**（分配/保留优先级），具有 抢占能力 和 抢占脆弱性 标志。这些标志决定承载在资源稀缺时是否可以被其他承载抢占或抢占其他承载。每个模板还携带 **APN-AMBR** 上行和下行聚合速率，以及是否启用 在线 和 离线 计费。

您可以创建、编辑和删除模板。您还可以克隆模板以派生新变体。APN 配置文件引用 QoS 模板，而不是携带自己的副本。如果您编辑模板，则重新塑造每个使用它的 APN 的 QoS。您无法删除仍被 APN 配置文件引用的模板。首先重新分配这些 APN。

APN QoS 配置文件

每个 APN 配置文件指向的每个 APN 的服务质量设置: **QCI**、**ARP** 和抢占 能力/脆弱性、APN-AMBR 下行/上行 带宽，以及是否适用 在线（**Gy**）和 离线（**Rf**）计费。您可以克隆配置文件以从现有配置文件派生新变体。

IMS 配置文件

CSCF 通过 Cx 读取的 IMS 订阅。IMS 配置文件 携带一个 iFC 模板：初始过滤标准，决定哪些应用服务器接收用户的 SIP 流量。您可以创建、编辑和删除配置文件。

静态 IP

必须始终接收相同地址的用户的固定 IP 分配，与 EPC 订阅数据一起管理。

PCRF

PCRF 应用的策略层。关系视图链接三个部分：

PCRF 配置文件：用户的 APN 引用的命名策略，由一组计费规则组成。
计费规则：每个规则具有 规则类型 和 优先级、QCI 和 ARP、MBR/GBR 下行/上行 限制，以及用于计费的 评分组 和 服务
标识符。专用承载携带具有 MBR 或 GBR 的规则。
流信息规则：附加到计费规则的流量流模板，定义它匹配哪些数据包。

您可以创建、编辑和删除所有三者。如果您编辑计费规则，则会影响每个使用它的配置文件。

漫游

HSS 应用于入境和出境用户的漫游策略。漫游配置文件 设置 默认数据操作、默认 IMS 操作，以及 漫游规则 列表。每个规则基于 MCC/MNC 并设置该网络的 数据 和 IMS 操作。因此，您可以允许或阻止特定访问网络，同时配置文件默认覆盖其余部分。要添加规则，请使用运营商查找从运营商名称（来自 IR.21）查找网络的 MCC/MNC。规则是共享的。如果您编辑规则，则会影响每个使用它的配置文件。

EIR

设备身份注册。每个 EIR 规则 通过正则表达式匹配 IMEI 并设置一个 操作：允许或阻止。因此，您可以禁止某个设备型号或特定手机接入网络。设备型号搜索有助于构建 IMEI 模式。您可以创建、编辑和删除规则。

状态

HSS 自身的单屏健康读取：API、数据库 和 许可证 健康状况，以及 实体计数，包括总 用户、EPC 配置文件、IMS 配置文件、 SIM、MSISDN 和 漫游配置文件。这是确认 HSS 是否正常以及其承载量的最快方式。Grafana 嵌入提供监控和统计仪表板。

复制 选项卡显示数据库复制到任何对等 HSS 实例的状态。日志 选项卡尾随 HSS 的实时日志输出。使用它来排查单个实例，而无需离开 OmniWeb。

复制

复制选项卡读取 HSS 节点的用户数据库的 PostgreSQL 复制健康状况，并将其绘制为实时拓扑。每个节点显示其数据库是 主 还是 备用。备用是处于恢复状态的节点。它重放主节点的更改，而不是接受自己的写入。对于主节点，选项卡将每个连接的备用节点绘制为下游链接。该链接显示备用的 客户端地址、它通过的 复制槽、其 流状态 和与主节点当前 WAL 位置测量的 复制延迟。该选项卡以字节为单位显示延迟，因此落后的副本一目了然。每个复制槽当前是否 活动 决定其链接是否显示为健康或断开。

运营商使用此选项卡确认用户数据库在 HSS 集群中复制：在一个节点上配置的更改将到达其他节点，并且存在备用节点以进行故障转移。落后的副本显示增长的延迟数字。断开或失去连接的副本会丢失其链接。如果运行两个或多个 HSS 实例但没有一个进行复制，则该选项卡将整个集群标记为复制缺口。在数据丢失风险之前，请纠正此问题。

操作

两个用户级操作作用于实时会话，而不是存储记录：

取消位置（CLR）：向用户的服务 MME 发送 S6a 取消位置请求。这将使用户分离，因此它重新连接并获取更改的订阅数据。 PCRF 重新认证：请求 PCRF 重新授权用户的给定 PDN 会话。这将更新的策略或计费规则推送到活动会话。

相关

MME：通过 S6a 读取用户认证和 EPC 订阅数据。它是取消位置的目标。
CSCF：通过 Cx 读取 IMS 配置文件和 iFC 进行 IMS 注册和服务触发。
PCRF / PCF：应用此处保存的 PCRF 配置文件、计费规则和流规则。它是重新认证的目标。 UDR： HSS 在 5G 核心中前端的共享用户数据存储。
操作指南：返回元素索引。

LCS：位置服务（OmniLCS）

LCS 功能为核心提供 位置服务。它回答“这个用户在哪里？”并驱动蜂窝广播警告。它从服务小区（和配置的小区几何）解析用户设备的位置，处理来自网络的位置请求（即时和延迟），并向一个区域推送 商业移动警报 / 蜂窝广播 警告。OmniWeb 显示 LCS 的小区库存、实时和最近的位置修复、延迟位置请求、CAP 警报和广播；更长期的趋势可以在同一页面的 Grafana 仪表板上查看。

← 操作指南

LCS 是一个每实例元素页面，可以通过侧边栏访问，当在站点的库存中运行时。所有流量都通过 OmniWeb 后端代理，因此它保持在单一的身份验证网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织成多个选项卡。

概述

单屏健康读取���LCS 状态、活动和 完成 的位置会话、□载的小区数量，以及 小区同步 结果。这是 LCS 正常运行并具有当前小区几何的最快确认。

概述还显示 LCS 与核心其他部分的每个连接，每个连接的状态（已连接或 未连接）、地址，以及对于 SCTP 关联，关联 ID 和建立时间：

- **SBc-AP** 对等体：与每个 MME 的 4G 蜂窝广播关联。4G 警告广播只能到达与其 SBc-AP 关联已连接的 MME 的小区，因此当广播未能到达终端时，这是首先要检查的内容。
- **SLs** 对等体：与每个 MME 的 **LCS-AP** 关联，承载 LCS 与服务 MME 之间的定位（E-CID、OTDOA、A-GNSS）。
- **Diameter** 对等体：SLg/SLh Diameter 连接（例如到 DRA），包括对等体的产品和应用 ID。
- **CAP** 源：每个警报源的连接（见 CAP 源），以及其最后一次心跳或轮询的时间。

顶部的瓷砖计算每种类型的已连接对等体与配置总数的比较，当任何一个对等体宕机时会变红。

小区

LCS 定位的小区库存：每个小区的 ID、纬度/经度、半径、高度、TAC/LAC、PCI、EARFCN、方位角和 RAT。您可以在此处添加、编辑��删除小区。这些几何信息将服务小区 ID 转换为位置。

添□或编辑小区

1. 选择 无线电（2G、3G、4G 或 5G）。对话框显示该无线电使用的字段：2G/3G 的 LAC，4G/5G 的 TAC，以及匹配的信道号（ARFCN、UARFCN、EARFCN 或 NR-ARFCN）和物理小区身份。
2. 精确输入 小区 **ID**，与网络报告的完全一致。对于 4G，从 **eNB ID** 构建 **ECI** 会根据 eNB ID 和小区号计算出 ECI。
3. 输入 **TAC** 或 **LAC**。此小区的蜂窝广播将发送到该区域代码。
4. 放置小区：点击地图、拖动标记，或输入或粘贴纬度和经度（`lat, lon` 粘贴到任一框中将填充两个框）。设置覆盖 半径，对于扇区天线，设置 方位角；地图显示结果覆盖范围。

在小区可以保存之前，每个值都会检查其有效范围。当小区的位置在警报区域内时，CAP 警报才会到达该小区，因此没有位置的小区，或者 TAC 或 LAC 错误的小区，将不会接收到警报。

□□

□□□ □□□□

延迟

LCS 持有的 未完成的延迟位置请求。位置选项卡回答“这个用户 □□ 在哪里”，而 延迟 **MT-LR**（延迟移动终止位置请求）请求网络在 稍后，当触发条件满足时 报告用户的位置，而不是立即：GMLC 启动请求，并在条件满足时返回报告。常见的触发条件包括 **UE** 可用性（在请求时设备处于闲置或无法访问状态，报告设备下次可达时）、定期位置（在设定的 间隔 内报告设定的 报告数量）和区域/运动事件（当 UE 进入、离开或在指定区域内移动时报告）。这就是操作员为当前无法找到的用户或需要跟踪一段时间的用户安排定位的方式。

每行列出延迟会话的用户 **IMSI**、类型（定期或触发）、定位 方法、其计划（定期会话的报告间隔；触发会话的区域事件和轮询间隔）、剩余的 报告 数量、状态、请求客户端、何时 开始 和 最后修复 的时间。没有报告限��的触发会话显示 □□ 报告剩余。

操作员可以在此处 创建 一个新的延迟请求，命名目标 IMSI、类型和定位方法（小区、E-CID 、GNSS 或 OTDOA）：

- 定期：报告间隔（以秒为单位）和要发送的报告数量。
- 触发：区域事件（进入、离开 或 在内）、区域本身（由其中心和半径（米）给出的圆，或至少三个纬度/经度点的多边形）、最大报告数量（0 表示无限）以及 LCS 轮询用户位置的频率。

操作员还可以在任何时候 取消 未完成的会话，这将拆除已启动的请求，因此不再生成进一步的报告。列表会轮询，因此会话的状态会在网络启动它和触发条件满足时更新。

CAP 警报

LCS 接受的 公共警报协议 (CAP) 警报用于蜂窝广播，分为三组：

待批准：等待操作员的警报。批准 将警报广播到其警告区域内的小区；拒绝 则将其丢弃。
活动：正在广播的警报。停止广播 将警报从其发送的每个网络中撤下。
历史：已发送、被拒绝、取消（由发布机构或操作员）或 过期 的警报。

每个警报显示其来源（CAP 源或手动提交）、CAP 标识符和发送者，以及每种 语言 的一行：语言、蜂窝广播 消息标识符 以及发送到终端的文本。当警报被发送时，每一行还显示序列号和每个网络的结果。页脚提供网络代码、目标 TACs/LACs、与警告区域匹配的小区数量，以及警报的接收、发送、批准、过期和结束时间。

警报自动从 CAP 源 到达，或者操作员可以使用 CAP XML 提交警报。并非每个 CAP 消息都适用于终端。LCS 应用以下警报规则，未符合条件的提交将被报告而不是排队：

仅 实际 警报且具有 公共 范围的才会被广播。未用于广播的测试消息将被忽略；
对于加拿大（CAP-CP）警报，仅广播标记为无线分发的信息块，使用其无线文本；
每种语言作为其自己的广播发送：主语言在配置的消息标识符上（默认 4370），每种其他语言在匹配的附加语言标识符上（4383）；
发布机构的 取消 或 更新 停止早期警报的广播，警报在 过期 时停止广播；
相同的警报（相同的发送者和标识符）仅处理一次。

CAP 源

LCS 接收警报的 **CAP** 源。支持两种类型：

- **NAAD** 流（□拿大）：Pelmorex 国家警报聚合和传播（NAAD）系统。LCS 同时连接到每个流媒体站点（两个站点提供冗余），并期望每分钟接收一次心跳；如果某个站点沉默，则重新连接。每个心跳列出最新的警报，任何未在流中到达的警报将从 NAAD 存档中获取，因此在连接中断时发布的警报仍然会被接收。
- **CAP Atom** 源：以 Atom 格式的 CAP 源，按设定间隔轮询。

每个源显示其是否启用、批准设置，以及对于每个站点或 URL 的 连接状态、最后一次心跳（或轮询）的时间和计数器：接收的警报和心跳、提交用于广播的警报、忽略（不适用于终端）、取消、重复（来自其他站点的相同警报）以及从存档中 填补 的警报。

添□源 创建一个源。□拿大 **— Pelmorex NAAD** 按钮填充两个 NAAD 流媒体站点和两个存档地址。对于每个源，您设置其名称、类型、URL、是否启用及其 批准 行为：使用 LCS 全局设置、要求操作员批准每个警报，或无需批准直接广播。在此处添加的源可以编辑、启用或禁用，并可以删除。在 LCS 配置中定义的源标记为 来自配置，并在此处为只读。

广播

广播 选项卡显示 LCS 正在推送的 蜂窝广播 消息，每个网络一行：消息标识符及其名称（测试和演练标识符标记为 测试）、序列号、网络（2G 通过 CBSP、3G 通过 SABP、4G 通过 SBc-AP）、消息文本、状态以及发送时间。历史 视图列出过去的广播，包括其警告类型。

序列号以十六进制显示，带有 消息代码 和 更新编号；将鼠标悬停在上面可以查看地理范围。终端每个消息标识符和序列号仅显示一次。相同标识符和序列号发送多次的行标记为 重复 - 终端忽略：接收第一次发送的终端不会显示后续的发送。

操作员可以从其行 停止 活动广播；停止仅适用于该行的网络，因此在 3G 和 4G 上发送的消息会分别停止。

发送广播 开始一个新的广播：

- 消息 **ID**：从 3GPP 列表中选择（ETWS 地震/海啸、CMAS/WEA 总统、极端、严重、AMBER、每月测试、演练、操作员定义、公共安全、州/地方测试）或输入自定义值。对于 ETWS 标识符，选择 ETWS 警告类型。
- 语言：消息文本，以及任意数量的 附□语言。每种附加语言在与所选语言匹配的附加语言标识符上发送（例如 4370 → 4383），使用相同的序列号，并报告每种语言的结果。ETWS 和自定义标识符没有附加语言标识符。每个文本下方的计数器显示编码（GSM 7 位，或当文本包含某些重音字母等字符时为 UCS-2）和使用的页数，最多 15 页。
- 序列号：由 地理范围、消息代码（0–1023）和 更新编号（0–15）构建。新的警报将获得该标识符尚未使用的下一个消息代码。作为更新发送**...** 选择早期广播并保持其代码，更新编号增加 1，因此终端替换早期消息。当标识符和序列号已经发送时，会出现警告，因为终端会忽略该消息。
- 正在广播的网络的 **MCC** 和 **MNC**（始终需要，因此广播不会在错误的网络代码下发送）、要发送的网络，以及目标 **TACs**（4G）、**LACs**（2G/3G）和 **SACs**（3G）对于已勾选的网络。
- 消息重复的频率和次数（0 次重复直到停止）。

日志

日志 选项卡实时跟踪 LCS 的日志输出，以□在不离开 OmniWeb 的情况下进行故障排除。

监控仪表板

位置请求速率和其他时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生复制这些图表。

相关

MME 通过位置接口请求定位，并且是 LCS 的 Diameter 对等体。
CAP 警报 和 广播 为蜂窝广播警告系统提供支持。

许可证服务器：Omnitouch 许可

许可证服务器是 Omnitouch 许可机构，网络功能在此进行检查。每个 Omnitouch 产品（MME、HSS、DRA、PGW-C、UPF、SGW-C、SMSC、CSCF 等）在运行之前都会向许可证服务器验证其授权，询问某个 许可方 是否对该 产品 拥有许可，以及该许可证是否仍在有效期内。服务器持有经过加密 签名的许可证，每个许可证授予许可方一组产品，包含有效期和元数据，并且它会回答授权查询并记录每个请求。由于许可证只有在可信的时钟下才有意义，服务器还会跟踪 可信时间 源，以□无法通过回滚节点的时钟来恢复许可证。OmniWeb 显示已授权的内容及其健康状况、网络功能所做的授权请求日志、按需查询工具以及服务器的实时日志。

← 操作指南

许可证服务器是一个每个实例的元素页面，可以通过侧边栏访问，当在站点的库存中运行时，可以查看多个部署的舰队视图。��有流量都通过 OmniWeb 后端代理到许可证服务器的 API，因此它保持在单一的身份验证网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织为多个标签。

概述 / 状态

单屏读取服务器正在授权的内容以及其健康状况。摘要卡片给出 总产品 的数量、有效 和 无效 的数量，以及不同 许可方 的数量。可信时间 面板显示服务器时钟源的状态：有效、宽限期 或 无效。当可信时间不可用时，服务器无法安全地验证许可证，这会将页面的健康状况提升为警告或错误。

已授权产品 表列出每个已授权产品的一行，每行显示 产品、授予的 许可方、发行 时间、开始 和 到期 日期（带有“剩余天数”或“过期 N 天前”指示器，在到期前 30 天内变为琥珀色，过期后变为红色），以及其 有效/无效 状态。打开一行会展开完整详细信息：确切的有效性时间戳、□密签名 是否有效、任何产品元数据以及签名本身。这是确认网络功能均已授权且没有即将到期���最快方式。

请求日志

网络功能针对服务器所做的 授权请求 的审计跟踪。每行记录 时间戳、请求来源的 源 IP（哪个网络功能主机发出的请求）、询问的 许可方 和 产品、决策（允许 或 拒绝），以及对于拒绝的情况，原因。列表可以按决策、产品以及部分 源 IP 或 许可方 搜索进行过滤，并且是分页的。在这里，您可以看到，例如，某个新部署的功能因其产品从未获得许可而被拒绝，或确认某个功能正在成功检查。

许可证查询

按需 授权检查。输入 许可方 和 产品，该工具向服务器询问网络功能会问的相同问题（该许可方现在是否有权使用该产品），并返回裁决：有效 或 无效、许可证的 有效至 日期、响应 时间戳、任何 元数据 和 签名。这是确认特定授权的直接方式，无需等待拥有功能的检查，并且列出了已知的产品标识符（例如 `omnihss`、`omniupf`、`omnimme`），以便您可以查询确切的一个。

日志

日志 标签尾随许可证服务器的实时日志输出，以便在不离开 OmniWeb 的情况下进行单实例故障排除。

相关

- 每个 **Omnitouch** 网络功能：MME、HSS、DRA、PGW-C、UPF、SGW-C、SMSC、CSCF 等在此验证其授权；每个产品自己的 概述 / 状态 标签显示源自此检查的许可证健康徽章。
- 操作指南：返回元素索引。

日志与订阅者追踪

OmniWeb 为操作员提供了多个互补的实时视图，展示网络的运行状态：

1. 日志：由 Loki 提供的任何单个元素的结构化实时服务日志。
2. 会话追踪：跨网络的视图，跟踪一个订阅者在每个协议和元素中的活动（Diameter、GTP-C、PFCP、SIP、MAP）。
3. **Homer**：深度 SIP/VoIP 数据包捕获和呼叫流程分析。

← 返回操作指南

从 **NF** 跳转到订阅者

许多网络功能通过 IMSI 显示订阅者、用户设备（UE）或会话。这些包括 **MME**（UE）、**SGW-C**、**PGW-C** 和 **ePDG**（会话）、**MSC** 和 **TAS**（订阅者）、以及 **SMSC**（位置）。在每种情况下，一排快速链接按钮让你可以直接跳转到其他地方的该订阅者，而无需复制 IMSI：

- 转到 **HSS** 记录 打开订阅者在 HSS 上的配置记录（通过配置的 HSS 实例解析 IMSI）。
- 查看会话追踪 打开该 IMSI 的订阅者实时信令阶梯
- 查看日志 打开元素的日志选项卡，预先过滤到该 IMSI，因此你只会看到该订阅者的日志行。

每个按钮仅在适用时出现：IMS 是已知的，并且为该站点配置了 HSS 或会话追踪。因此，按钮集会根据部署情况进行调整。

订阅者快速链接（这里在 MME UE 上）：一键访问 HSS 记录、实时信令阶梯或该元素的日志，过滤到该订阅者。

实时日志（Loki）

每个元素都有一个 日志 选项卡。它从 Loki 查询元素的服务日志，并在新行到达时进行流式传输，因此你可以在进行更改或重现问题时实时查看元素。

□□□□□□□□□ UPF □□□□ Loki □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□IMSI□□□□□□□□□□□□□□□□□□

日志查询的工作原理

前端构建一个 LogQL 查询，并通过后端的 Loki 网关发送。���有任何内容直接从浏览器查询 Loki。它像其他请求一样被代理（因此经过身份验证和审计）。

后端的 Loki 目标由 `LOKI_URL` 环境变量设置（默认 `http://localhost:3100`）。查询使用 Loki 的范围查询 API，带有 LogQL 表达式、时间窗口、结果限制和方向（最新优先或最旧优先）。

选择器与管道过滤器

OmniWeb 从两种过滤器构建结构化查询：

过滤器位置	**LogQL** 位置	示例	用途
选择器	在流选择器内部 `{ … }`	`{hostname="omni-eval-upf01"}`	选择要读取的流（主机/服务）。已索引且快速。
管道	在 `|` 后	`| level="error"`	按结构字段过滤匹配的行。

典型的元素日志选项卡将主机/服务固定为选择器，并允许你在其上添加管道过滤器（严重性、组件、订阅者标识符）。由于 Omnitouch 服务发出 结构化 日志行，因此你可以根据真实字段进行过滤，而不是 grep 自由文本。

结构化日志数据

主机将结构化日志发送到 Loki（由 Ansible ���用角色配置）。两个特别有用的结构化来源：

- 服务日志：每个 NF 自己的结构化输出，按 `hostname`/服务标记，在该元素的日志选项卡上可用。
- 命令审计：在主机上执行的每个命令，包括谁登录（存活的 `sudo`/`su`）、有效 UID、二进制文件、工作目录和完整命令行。发送到 Loki。请参见 审计日志 以获取字段参考。

使用日志选项卡

1. 打开任何元素并选择 日志。
2. 查看器加载该元素的最近行并开始轮询新行。
3. 使用管道过滤器缩小视图（例如严重性，或如果服务日志包含 IMSI/MSISDN）。
4. 调整时间窗口以回顾过去的事件。
5. 暂停轮询（标题指示器），在阅读时保持稳定视图。

> 提示：在调查一个订阅者时，通过其 IMSI/MSISDN 过滤元素日志是快速的第一步；要查看该订阅者在□□元素中的活动，请使用下面的会话追踪。

会话追踪：跨网络跟踪订阅者

会话追踪 引擎将单个订阅者在多个元素和协议中的信令进行关联，提供从无线接入到身份验证、会话建立和呼叫/SMS 交付的统一时间线。这是回答“这个订阅者发生了什么？”的工具，而无需在元素 CLI 之��跳转。

□□□□□□ IMSI □ MSISDN □□□□□□□□□□ Diameter□GTP-C□PFCP□SIP □ MAP □□□□□□□□□□□□□□□

支持的协议

协议	显示内容	涉及的元素
Diameter	身份验证、策略、计费	HSS、DRA、PGW-C、PCRF、OCS、CSCF（Cx/Dx/Rx）
GTP-C	会话管理（S5/S8、S11）	SGW-C、PGW-C、MME
PFCP	用户平面会话规则（N4）	PGW-C/SMF ↔ UPF
SIP	IMS 呼叫控制	P-CSCF、I-CSCF、S-CSCF、TAS
MAP	SS7 位置、身份验证、SMS	MSC、HLR、CAMEL GW、IP-SM-GW

用户追踪

用户追踪 视图让你可以通过 **IMSI** 或 **MSISDN** 搜索，并查看该订阅者在网络中的每个关联协议交互。例如，单个接入会显示 Diameter 身份验证、GTP-C 会话创建和 PFCP 规则安装的一个连贯序列：

特定协议选项卡

每个协议都有自己的选项卡（**Diameter**、**GTP-C**、**PFCP**、**SIP**、**MAP**），以及一个 所有协议 概览。每个协议的选项卡是过滤视图。当你追踪特定协议的问题时（例如，仅 VoLTE 呼叫的 SIP 交换），它们会很有帮助，而不是在所有内容中跟踪单个订阅者。

PCAP 阶梯

PCAP 阶梯 选项卡将数据包捕获转换为阶梯：信令的时间顺序序列图。上传一个 PCAP 或 PCAPNG 捕获（例如来自网络探测器或元素级追踪），OmniWeb 解析数据包，通过 IP 地址和推断的角色（MSC/VLR、HSS、S-CSCF 等）识别信令节点，并将请求与其响应关联成会话。结果以时间顺序绘制为消息阶梯，因此你可以一目了然地阅读整个交换。

*PCAP □□□□

□□□□□□□□□□□□□□□□□□□□□□□□ IMSI□□□□□□□□□□□□□□□□□□□□□□□□□□□□

打开一个流，OmniWeb 将其重建为与 PCAP 相同的阶梯，但来自网络自己的遥测，无需捕获或上传。下面的示例是单个订阅者的 LTE 附加，跨越每个接触到它的元素进行关联：与 **eNodeB** 的 S1AP/NAS 交换、对 **HSS** 的 Diameter S6a 身份验证和位置更新，以及通过 **SGW-C** 和 **PGW-C** 的 GTP-C 会话设置。所有这些都出现在一个时间顺序阶梯上，每条消息的请求/响应往返时间和完整解码只需点击即可查看。

□□□□□□□□□□□□□□□□□□□ LTE □□□□ eNodeB□MME□HSS□SGW-C □ PGW-C□□□ S1AP□ Diameter S6a □ GTP-C□□

如果尚未流动信令遥测，则选项卡显示空状态；流会随着网络元素开始发出遥测而自动填充。

Homer: SIP 捕获与呼叫流程分析

OmniWeb 与 Homer 集成，这是一个开源 SIP 捕获和 VoIP 故障排除平台，用于深度呼叫流程可视化、协议解码和捕获的 SIP 信令搜索。当会话追踪为单个订阅者提供跨协议的□□时，Homer 提供逐条消息的 SIP 数据包详细信息。

可用性与访问

Homer ﷺ 可选 的并且会自动检测。在启动时，OmniWeb 检查 `/api/homer/status`：

- 如果 Homer 已配置（后端设置了 `HOMER_URL`）并且可访问，则侧边栏中会出现 **Homer** 条目。
- 如果 Homer 未部署，则该条目会被隐藏，且没有其他更改。

点击 **Homer** 会在新浏览器标签页中打开 Homer 网页 UI。身份验证是透明的：网关通过与 Grafana 相同的单点登录验证你的 OmniWeb 登录，因此无需第二次登录。后端的 `HOMER_URL`（以及设置时的 `HOMER_PROXY_SECRET`）配置集成。

用例

当问题出现在 SIP 层本身时，Homer 是你要使用的工具：

- **VoLTE** 呼叫流程分析：追踪 SIP `INVITE`/`BYE` 序列通过 P-CSCF、I-CSCF、S-CSCF 和 TAS。
- **VoWiFi** 故障排除：分析 ePDG ↔ P-CSCF 的 SIP 交互。
- **IMS** 注册调试：检查 `REGISTER` / `401` / `REGISTER` / `200 OK` 交换。
- 互联问题：捕获 MSC 与 SIP 对等体之间的 SIP 中继信令。

会话追踪与 **Homer**

两者都帮助故障排除，但它们回答不同的问题。它们是互补的，而不是替代品：

工具	最适合	范围	打开位置
会话追踪	“跟踪这个订阅者跨越整个网络”	Diameter、GTP-C、PFCP、SIP、MAP 按 IMSI/MSISDN 关联	在 OmniWeb 内联
Homer	“给我这个呼叫的确切 SIP 消息”	SIP/VoIP 信令，完整数据包解码（VoLTE/VoWiFi/IMS）	新标签（自动检测）

一个常见的流程是在会话追踪中发现与 SIP 相关的异常，然后跳转到 Homer 获取详细的呼叫流程。

故障排除

元素的日志选项卡上没有日志出现

症状：日志选项卡为空或显示“没有结果”。

可能的原因：

- 后端无法访问 Loki（`LOKI_URL` 配置错误）。
- 主机未将日志发送到 Loki（日志发送未运行/配置错误）。
- 选择的时间窗口早于可用日志，或主机标签不匹配。

解决方案：

1. 确认 `LOKI_URL` 指向可访问的 Loki 实例。
2. 验证元素的主机是否正在发送日志（检查该主机上的日志发送代理）。
3. 扩大时间窗口并移除管道过滤器以确认是否有行到达。

会话追踪对订阅者返回空结果

症状：按 IMSI/MSISDN 的用户追踪没有显示事件。

可能的原因：

- 在选择的窗口中，订阅者处于非活动状态。

标识符输入错误（IMSI 与 MSISDN）。
相关协议的追踪源未向引擎提供数据。

解决方案：

1. 重新检查标识符并尝试替代标识符（IMSI ↔ MSISDN）。
2. 扩大时间窗口。
3. 确认该订阅者在元素的日志选项卡中是否确实活跃。

侧边栏中缺少 Homer 条目

症状：没有 Homer 链接出现。

可能的原因：

Homer 未部署，或后端未设置 HOMER_URL。
Homer 无法访问，因此 /api/homer/status 报告其不可用。

解决方案：

1. 确认 Homer 已部署并且 HOMER_URL 已在 OmniWeb 后端设置。
2. 验证后端是否可以访问 Homer，然后重新加载 OmniWeb（检测在启动时运行）。

MME: 移动管理实体

MME 是 EPC 的控制平面锚。它终止与 eNodeB 的 **S1AP**，为每个 UE 执行附着、认证和移动程序，并为每个附着的用户持有 **UE** 上下文。它通过 **S6a**（Diameter）从 HSS 获取订阅和认证数据，通过 **S11** 在服务网关上设置承载，并协调通过 **S10/N26** 的 MME 之间和系统之间的切换。简而言之，它是决定每个订阅者如何以及何时附着、被寻呼和在网络中移动的节点。OmniWeb 显示 MME 的实时 eNodeB、UE 上下文、SGW 和 Diameter 对等体、接口状态和切换状态。长期趋势可以在同一页面的 Grafana 仪表板上查看。

← 操作指南

MME 是一个每实例元素页面，可以通过侧边栏在站点的库存中访问，当部署多个时，可以查看聚合状态的舰队视图。所有流量通过 OmniWeb 后端代理到 MME 的 API，因此它保持在单个经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织为多个选项卡。

概述

单屏健康读取：MME 的 **API** 状态和其实时负载的摘要，包括连接的 **eNodeB**、附着的 **UE**、**SGW** 对等体和其 **Diameter**（S6a）对等体的状态。这是确认 MME 是否正常运行以及它服务了多少接入网络的最快方式。

eNodeBs

每个与 MME 有 S1AP 关联的 eNodeB，每行显示 全球 eNB ID、名称和连接 状态。打开一个 eNodeB 以显示其上下文：服务的单元和 TAC 以及其上的 UE。操作员可以 更新 MME 向 eNodeB 广告的容量，这会调整 eNodeB 在 MME 池中如何负载均衡 UE（用于排空或加权 MME 进行维护或重新平衡）。

UEs

每个附着订阅者的 **UE** 上下文，每行按 **IMSI** 和 **GUTI** 键入，显示其连接和移动状态及服务的 eNodeB。打开一个 UE 显示其完整上下文。可用的每 UE 操作包括：

- 寻呼 UE。
- ���送到空闲：释放无线连接，同时保持上下文。
- 卸载 UE 到另一个 MME。
- 请求重新附着：强制 UE 重新附着。
- 发送短信 给 UE。
- 删除 UE 上下文：清除过期或卡住的订阅者。

您还可以 查找 **IMSI** 的运营商 **/ PLMN** 以识别本地与漫游订阅者。

S-GW 对等体

MME 通过 **S11**（GTP-C）与之通信的服务网关，每行显示对等体的 **IP**、存活状态 **/** 可达性、GTP 重启（恢复）计数 和该网关上锚定的 会话计数。当 S-GW 重启时，计数器递增，这会告诉 MME 重新建立它所持有的会话。对等体是通过 **DNS** 学习的还是 静态 条目显示在 MME 应用于本地和漫游订阅者的 S-GW 选择方法 旁边。打开一个对等体以列出它承载的 会话，每个会话通过 **IMSI** 及其 **S11 TEIDs**（MME 和 S-GW 侧隧道端点）进行标识。这里是操作员确认哪些 S-GW 正在运行并查看 UE 会话如何在它们之间分布的地方。这有助于在您平衡负载或诊断为什么一组订阅者的承载与单个网关一起下降时。

GUTI 重新分配和 S10 卸载

两个移动操作是由 IMSI 驱动的，而不是按行：

- **GUTI** 重新分配：重新分配连接订阅者的 **GUTI** 以刷新 UE 提供的临时身份（用于旋转标识符或清除身份不匹配时）。
- **S10** 卸载：强制卸载订阅者到 另一个 **MME**。这会通过 S10 将特定订阅者的上下文移出此 MME，并补充在排空 MME 时对 eNodeB 容量控制的作用。

S10

S10/N26 MME 之间接口是 UE 的上下文在 **TAU** 或 切换 期间在 MMEs 之间移动时重新定位的路径（并且通过 **N26** 在 MME 和 AMF 之间进行 EPC 到 5GC 的互通）。该选项卡分为两部分。活动切换 列出正在进行的重新定位，每个显示 源 和 目标 MME 以及正在移动的 **IMSI**，以□操作员可以观察移动事件的进展或发现卡住的事件。对等 **MME** 发现 显示 MME 如何找到其池对等体：它运行的 **DNS / NAPTR** 查找和任何 静态 配置的对等体，每个对等体的 FQDN 和地址。这里是您确认 MME 之间的移动是否正常，以及 MME 是否能够实���到达需要交付上下文的邻居的地方。它补充了从 UEs 选项卡驱动的每个订阅者的 **S10** 卸载操作。

Diameter

MME 的 Diameter 对等体，主要是通过 S6a 连接的 HSS，每行显示对等体的 主机、领域 和连接 状态。打开一个对等体以显示其详细信息。这里是您确认 HSS 的认证和订阅路径正常运行的地方，当附着失败时。

接口

接口 视图报告每个 MME 接口的状态：与 eNodeB 的 **S1AP**、与 SGW 的 **GTP-C**（S11）、用于 **S6a**（HSS）和 **SLg**（位置服务）的 **Diameter**、与 MSC 的 **SGsAP**（用于 CS 回退和 SMS）、**LCS-AP / SLs**（位置服务）和 **S10/N26**（MME 之间和 EPC 到 5GC 的切换）。这是确认 MME 的信令路径哪些正常运行、哪些不正常的单一屏幕。

日志

日志 选项卡尾随 MME 的实时日志输出，以□在不离开 OmniWeb 的情况下排查单个 MME 的问题。

监控仪表板

附着率、UE 数量、切换率和��他 MME 的时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生复制这些图表。

相关

- **HSS** 保存 MME 通过 **S6a** 获取的订阅和认证数据。

SGW‑C 是通过 S11 的控制对等体。MME 在其上驱动会话和承载的设置。
MSC通过SGsAP进行 CS 回退和 SMS。
其他 MMEs 通过 S10 进行 MME 之间的移动，AMF 通过 N26 进行 EPC 到 5GC 的切换。

Quectel EP06 AT 命令参考（蜂窝网络测试）

测试设备调制解调器控制台的参考。目标是 **Quectel EP06**（固件 `EP06ELAR04A05M4G`，IMEI `868186042000040`）在实验室容器中，但 适用于 EC25 / EG06 / EG06 / EM06 系列。下面的每个命令都在实时 EP06 上进行了测试；示例响应是 从该调制解调器捕获的真实响应（当时处于 无服务 / 搜索 状态，因此信号字段为空，解析器必须处理这种情况）。

中继是请求/响应：`sendModemAt(serial, command, readMs, timeoutMs)` → 后端 `modem_at` → 代理 `modem.run_at(serial, command, min_read, timeout)`。`min_read` 保持读取端口至少那么长的时间，以□在调用返回之前捕获异步 URC。没有 持久的 **URC** 流。请参见下面的“事件日志”。

设备 / SIM 信息

命令	目的	实时响应
`ATI`	制造商 / 型号 / 固件	`Quectel` / `EP06` / `Revision: EP06ELAR04A05M4G`
`AT+CGMM`	型号	`EP06`
`AT+CGMR`	固件版本	`EP06ELAR04A05M4G`
`AT+CGSN`	IMEI	`868186042000040`
`AT+CIMI`	IMSI	(SIM IMSI)
`AT+QCCID`	ICCID	(SIM ICCID)
`AT+CPIN?`	SIM PIN 状态	`+CPIN: READY`

信号 / 测量

命令	目的	实时响应
`AT+CSQ`	RSSI/BER（传统）	`+CSQ: 99,99`（99 = 无信号）。dBm = `-113 + 2*rssi`。
`AT+QCSQ`	每个 RAT 信号	`+QCSQ: "NOSERVICE"`。连接时：`+QCSQ: "LTE",<rssi>,<rsrp>,<sinr>,<rsrq>`。
`AT+QNWINFO`	当前 RAT / 频段 / 通道	`+QNWINFO: No Service`。连接时：`+QNWINFO: "FDD LTE","<mccmnc>","LTE BAND 3",1850`。
`AT+QENG="servingcell"`	完整的服务小区测量	`+QENG: "servingcell","SEARCH"`（空闲）。请参见下面的格式。
`AT+QENG="neighbourcell"`	邻居小区	`OK`（未驻留时无）。

`AT+QENG="servingcell"` LTE 格式

```
+QENG: "servingcell",<state>,"LTE",<is_tdd>,<MCC>,<MNC>,<cellID>,
<PCI>,
       <EARFCN>,<band>,<UL_BW>,<DL_BW>,<TAC>,<RSRP>,<RSRQ>,<RSSI>,
<SINR>,<srxlev>
```

- `RSRP` dBm，`RSRQ` dB，`RSSI` dBm（均为有符号整数）。
- `SINR` 是一个 转换 值：实际 dB = `(1/5)*SINR - 20`（范围 0..250 → -20..+30 dB）。
- `cellID`/`PCI`/`EARFCN` 通常是每个字段的十六进制/十进制；`band` 是 LTE 频段指示符。

`AT+QENG="neighbourcell"` LTE 格式

```
+QENG: "neighbourcell intra","LTE",<EARFCN>,<PCI>,<RSRQ>,<RSRP>,
<RSSI>,<SINR>,<srxlev>,...
+QENG: "neighbourcell inter","LTE",<EARFCN>,...
```

注册 / 附□

命令	目的	实时响应
`AT+CFUN?`	无线电功能	`+CFUN: 1`（全功能）。`0` = 最小/飞行模式。
`AT+CEREG?`	EPS 注册	`+CEREG: 2,2`（2 = 搜索中）。
`AT+CEREG=2`	启用带位置的注册 URC（TAC/cellID）	`OK`
`AT+CGATT?` / `AT+CGATT=1` / `=0`	PS 附加状态 / 附加 / 分离	`+CGATT: 0`
`AT+COPS?`	当前运营商选择	`+COPS: 0`（自动，未注册）。
`AT+COPS=?`	网络扫描（运营商搜索，慢）	`(stat,"long","short","numeric",AcT)` 元组列表。
`AT+COPS=0`	自动运营商选择	`OK`
`AT+COPS=1,2,"<mccmnc>"[,<AcT>]`	按数字 ID 手动选择	`OK`

小区 / 频段 / **RAT** 锁定

命令	目的	实时响应
`AT+QNWLOCK=?`	功能	`+QNWLOCK: "common/4g",<num of cells>,[[<freq>,<pci>],...]` 和 `+QNWLOCK: "common/lte"[,<action>[,<EARFCN>,<PCI>[,<status>]]]`
`AT+QNWLOCK="common/4g"`	查询小区锁定	`+QNWLOCK: "common/4g",0`（0 个小区 = 无锁定）；锁定后 `+QNWLOCK: "common/4g",1,1850,0`。
`AT+QNWLOCK="common/4g",<n>,<EARFCN>,<PCI>[,<EARFCN>,<PCI>...]`	锁定 n 个小区（在此固件上有效）	`OK`
`AT+QNWLOCK="common/4g",0`	解锁	`OK`（清除锁定）。
`AT+QNWLOCK="common/lte"`	查询单小区 LTE 锁定（只读）	`+QNWLOCK: "common/lte",0,0,0,0`。

> 固件行为（在 **`EP06ELAR04A05M4G`** 上验证）：**`common/4g`** 形式是接受此单元上的锁定 □□ 的形式。`AT+QNWLOCK="common/4g",1,<EARFCN>,<PCI>` 锁定（返回 `OK`，锁定持续）而 `AT+QNWLOCK="common/4g",0` 清除它。`common/lte` □□ 形式（`...,1,<EARFCN>,<PCI>` 和 `...,0`）在此固件上均返回 **`ERROR`**，因此 `common/lte` 仅为查询。UI 因此 使用 `common/4g` 进行锁定和解锁。 | `AT+QCFG="band"` | 查询频段掩码 | `+QCFG: "band",0x8d0,0x1a0880800d5,0x0` = （GSM 掩码，LTE 掩码，TDS 掩码）。 | | `AT+QCFG="band",0,<lte_hex_mask>,0` | 频段锁定（LTE）。 `0x0` LTE 掩码 = 所有频段。 | `OK` | | `AT+QCFG="nwscanmode"` | RAT 扫描模式 | `+QCFG: "nwscanmode",0`（0 = 自

> 动，1 = GSM，2 = WCDMA，3 = LTE）。 | | `AT+QCFG="nwscanmode",<m>[,1]` | 设置 RAT 偏好（`,1` = 立即生效） | `OK` | | `AT+QCAINFO` | 载波聚合信息 | `OK`（空闲时无聚合）。 |

LTE 频段掩码: 位 `(band-1)`，即频段 N → `1 << (N-1)`。例如 B3 = `0x4`，B7 = `0x40`，B28 = `0x8000000`。`0x0`（或全为 1）= 所有频段启用。

> 固件说明: `AT+QCFG="nwscanseq"` 在此 EP06 固件上返回 `ERROR`（`EP06ELAR04A05M4G`）。UI 不显示它。`AT+QSCAN` 也不支持此 EP06 固件（它是 RG/RM 5G 系列命令）。网络扫描使用 `AT+COPS=?` 加上 `AT+QENG`。

语音通话（**VoLTE / IMS**）

EP06 语音是仅 **VoLTE**: 它需要在 LTE 上注册 IMS。此单元上的 `AT+QCFG="ims"` 返回 `+QCFG: "ims",1,0`（IMS 通过配置启用，当前状态 0）。

命令	目的
`AT+QCFG="ims"`	查询/启用 IMS。`AT+QCFG="ims",1` 强制启用。
`ATD<number>;`	拨打语音电话（尾部 `;` = 语音，而不是数据）。
`ATA`	接听来电。
`ATH` / `AT+CHUP`	挂断。
`AT+CLCC`	列出当前通话: `+CLCC: <id>,<dir>,<state>,<mode>,<mpty>,"<number>",<type>`。空 `OK` = 无通话。
`AT+CLIP=1`	在 `RING` 时启用来电号码 ID URC（`+CLIP:`）。

`AT+CLCC` 通话状态: 0 活动，1 保持，2 拨号中，3 振铃，4 来电，5 等待。

短信（文本模式）

命令	目的	实时响应
`AT+CMGF=1`	文本模式（与 PDU 相对）	`OK`
`AT+CPMS?`	存储区域 / 计数	`+CPMS: "ME",0,255,"ME",0,255,"ME",0,255`
`AT+CMGL="ALL"`	列出消息（文本模式）	每条消息：`+CMGL: <index>,"<stat>","<sender>",,"<timestamp>"` 然后是正文行。
`AT+CMGR=<index>`	读取一条消息	`+CMGR: "<stat>","<sender>",,"<timestamp>"` + 正文。
`AT+CMGS="<number>"` 然后正文 + Ctrl-Z	发送（由代理 `send_sms` 处理）。	`+CMGS: <mr>`
`AT+CMGD=<index>[,<delflag>]`	删除消息（`delflag` 4 = 全部）。	`OK`
`AT+CNMI?` / `AT+CNMI=2,1,0,0,0`	新消息指示配置	`+CNMI: 2,1,0,0,0`

PDP / 数据

命令	目的	实时响应
`AT+CGDCONT?`	列出 PDP 上下文（APN）	`+CGDCONT: 1,"IPV4V6","ims",...`
`AT+CGDCONT=<cid>,"<type>","<apn>"`	设置上下文。类型：IP，IPV6，IPV4V6，非 IP。	`OK`
`AT+CGACT=1,<cid>` / `=0,<cid>`	激活 / 停用上下文。	`OK`
`AT+CGPADDR[=<cid>]`	显示分配的 IP。	`+CGPADDR: 1,"<ip>"`
`AT+CGCONTRDP=<cid>`	DNS / 网关 / PCO。	`+CGCONTRDP: ...`
`AT+QPING=1,"<host>"`	从调制解调器 ping（URC 回复；需要 `min_read`）。	`+QPING: ...`

事件日志（URCs）：以及中继限制

代理中继是 请求/响应，且每次调��时端口打开。它打开 串口，发送一个命令，读取直到 OK/ERROR（或 `min_read` 经过），然后关闭。它 不 保持端口打开以将非请求结果代码（URCs）流回浏览器。因此，通过此路径无法实现真正的实时事件馈送。

值得启用的 URC（每个都是一次性 `OK` 命令）：

命令	启用 **URC**
`AT+CEREG=2`	`+CEREG:` 注册变化（带 TAC/cellID）。
`AT+CGEREP=2,1`	`+CGEV:` PS/承载事件。
`AT+CLIP=1`	`+CLIP:` 来电号码在来电 `RING` 时。
`AT+CNMI=2,1,0,0,0`	`+CMTI:` 新 SMS 指示。
`AT+QINDCFG="all",1`	`+QIND:` Quectel 指示。

在 **UI** 中使用的务实方法：事件选项卡启用上述 URC，然后 轮询 调制解调器（`AT+CEREG?`，`AT+CLCC`，`AT+QENG`，`AT+CSQ`，`AT+CMGL`）并将状态变化渲染到带时间戳的日志中。每次轮询 还使用短的 `min_read` 窗口，因此在读取期间发生的任何 URC 都会被机会性捕获。这捕获状态转换（注册获得/丢失，通话开始/结束，新 SMS，信号变化）在轮询频率下，这对于实验室测试是足够的。该限制在 UI 中有文档说明。

MSC: 移动交换中心

MSC 是电路交换核心的呼叫控制中心。它保存当前在其服务区域内的用户位置寄存器（VLR），建立和拆除语音通话，传递短信，并管理这些用户的移动性（位置更新、寻呼和切换）。它通过**RAN/BSC** 连接（A 接口，通过 M3UA/SS7 驱动）连接到无线侧，将语音桥接到 IMS 并通过**SIP** 对等体进行互连，并通过一个或多个媒体网关引导实际媒体。OmniWeb 显示 MSC 的实时用户、通话、短信交易、RAN 和 SIP 对等体、路由表和待处理寻呼。长期趋势可以在同一页面访问的 Grafana 仪表板上查看。

← 操作指南

MSC 是一个每个实例的元素页面，可以通过侧边栏在网站的库存中访问，并且在多个实例部署时，可以查看聚合状态的车队视图。所有流量都通过 OmniWeb 后端代理到 MSC 的 API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此 ��面。它被组织成多个标签。

概述

单屏健康读取：MSC 的**API** 状态和当前处理的内容摘要，包括 VLR 中注册的用户、活跃通话、进行中的短信交易、实时的**RAN** 连接以及**SIP** 对等体和**STP** 信令链路的状态。这是确认 MSC 正在运行并一目了然地查看其实时负载的最快方式。

用户

VLR 当前持有的每个用户，每行以**IMSI**和**MSISDN**为键，显示其注册和位置状态。打开一个用户以显示其完整的 VLR 上下文。从这里，操作员可以：

- 清除 VLR 中的用户，以清除过时或卡住的注册，以□用户能够干净地重新注册。
- 对特定用户执行用户操作。
- 管理补充服务：检查和更改为用户激活的呼叫转移、阻止和相关服务。
- 向用户发送费用通知（**AoC**）。
- 发送静默短信（类型 **0**）或发起静默呼叫：一种不会提醒手机的定位/可达性探测。

通话

每个活跃通话，每行显示主叫和被叫方、通话状态及其持续时间。打开一个通话以显示其详细信息：通话腿、服务的 RAN 连接和媒体路径。操作员可以强制释放通话，以清除卡住或不需要的通话。

□□

MSC □□□□

RAN

MSC 的无线侧。它列出了活跃的RAN 连接（承载用户信令的实时 A 接口关联）和已知的BSC，这些信息是通过 SS7/M3UA 链路上的 RESET 交换学习到的。在这里，您可以确认基站控制器已连接，并查看哪些用户在哪个连接上。

SIP 对等体

MSC 通过其 SIP 对等体桥接语音的 IMS、软交换和互连干线，每行显示对等体的地址及其可达性状态。打开一个对等体以显示其详细信息。操作员可以在对等体上触发 OPTIONS ping，以主动测试可达性，这是在呼叫失败时证明 SIP 路径正常的最快方法。

□□□□

MSC □□□□

□□

MSC □□□□

寻呼

待处理的寻呼请求是 MSC 当前正在尝试通过无线网络定位的用户，以□接收来电或短信。操作员还可以直接从这里寻呼用户。

日志

日志标签实时跟踪 MSC 的日志输出，以□在不离开 OmniWeb 的情况下排查单个交换机的问题。

监控仪表板

呼叫速率、短信量、用户数量和其他时间序列数据通过 Grafana 仪表板呈现，可以从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

- **HSS** 保存 VLR 解析的用户数据，并且 MSC 注册为服务节点。
- **CSCF / IMS** 通过 MSC 的**SIP** 对等体桥接语音。

- **BSCs** 通过 A 接口在无线侧连接，承载在 SS7/M3UA 信令链路上。

网络测试（负载测试）

网络测试 在实时核心上驱动合成信令负载，以□您可以测量其在压力下的表现。它由 RAN Simulator 提供支持：虚拟 eNodeB 和 UE 通过完整的无线→核心路径（S1AP/NAS、GTP-U、IMS）进行测试，而不是单一接口。

← 操作指南

侧边栏中的 网络测试 组收集了 RAN Simulator 负载测试工具：

子标签	功能
RAN 负载测试	最近的负载测试作业 — 针对核心运行的附加、数据会话和 IMS 注册，及其结果和可下载的 pcap。
场景计划	定义定期场景运行（例如，每小时的附加批次），立即运行一个，并浏览运行历史。结果导出到 Prometheus 以进行警报。
RAN Simulator	启动虚拟 eNodeB/gNodeB 和 UE 并直接驱动它们。
RAN 无线	多 RAT 无线控制（5G NR / 2G GERAN / 3G UTRAN）。
RANsimware — IMS	在模拟舰队中进行 IMS ���册和 VoLTE 负载。

所有这些内容在 **RAN Simulator** 中都有深入的文档。

指向核心的运行

当您启动一个小区时，OmniWeb 提供一个下拉菜单，列出它可以拨打的核心节点 — 它在您的站点库存中找到的每个 **MME**、**AMF** 和 **STP** — 这样您就可以将运行指向正确的核心（`mme_ip` / `amf_ip` / `stp_ip`），而无需手动输入 IP。如果没有配置库存，该字段将回退为自由文本。

典型用法

1. 打开 **RAN Simulator**，启动一个 eNodeB/gNodeB 并指向核心进行测试。

2. 附加一批 UE 并运行一个场景（附加、数据、IMS 注册、VoLTE 或故障场景）。
3. 观察结果，并为信令细节下载运行的 pcap。
4. 为了常规覆盖，将场景保存为 场景计划，以它在一定时间间隔内运行并将通过/失败导出到 Prometheus。

相关

- RAN Simulator：用于整个无线→核心路径的功能和负载测试的虚拟 eNodeB/UE。
- Grafana 仪表板与统计：场景的通过/失败和时序导出到 Prometheus；在测试期间使用 Grafana 获取完整视图。

OmniRoam：漫游协议与电子邮件自动化
OmniRoam的协议部分将设置漫游合作伙伴的文书工作（电子邮件、AA.12/AA.13表格、IOT费率、SIM卡更换和配置工作）转变为每个合作伙伴的单一跟踪记录。它自动化了以前需要复制和粘贴的部分。它的主要技巧是：将合作伙伴的电子邮件转发给OmniRoam，它会读取线程，提取事实，并为您更新协议。然后，它生成并电子签署合同，归档它们，并提出工作订单以启动合作伙伴。

← 返回操作指南

两个不同的“OmniRoam”。本文档是关于OmniRoam的协议/电子邮件/文档部分（与漫游合作伙伴的商业和配置生命周期）。它不是与漫游测试书（IR.38 / IR.48 / VoLTE一致性测试）相同。这些内容在OmniRoam：漫游测试自动化中单
独涵盖。一个产品，两个任务：签署协议（在这里）和证明漫游有效（在那里）。

目录

大局
1. 收件电子邮件摄取：“提取数据”
2. 协议与合作伙伴
3. 自动文档生成与签署
4. 归档与存储
5. 工作订单与受让人通知
完整生命周期，端到端
您一次设置的内容

大局

OmniRoam中的一切都依赖于一个记录：协议，每个漫游合作伙伴一个。协议包含合作伙伴的名称、国家、TADIG(s)/PLMN、其生命周期状态、联系人、商定的商业费率、交换的SIM卡、生成和接收的文档、活动时间线以及使合作伙伴上线的工作订单。

您可以在UI中手动构建所有这些内容。但OmniRoam的重点是大部分内容通过电子邮件到达，而OmniRoam为您归档。

您正在使用的租户是运营商（您自己的网络，“本地”侧）。一切都以此为范围：您的信头和签署人在生成的文档中填写，您的入站地址驱动电子邮件自动化，您的团队是工作订单的受让人。

---

1. 收件电子邮件摄取：“提取数据”

您的操作

与合作伙伴的谈判是电子邮件对话。要将其引入OmniRoam，您只需做一件事：转发电子邮件，或在线程中抄送**OmniRoam**入站地址。就是这样。您的专用入站地址（例如`roaming@yourdomain`）为每个运营商配置一次（设置 → 文书工作详情，入站电子邮件）。

- 一次性转发整个线程，OmniRoam会根据引用消息中的历史记录构建协议。
- 在持续谈判中抄送该地址，每封新电子邮件都会保持记录的最新状态。状态推进，联系人和TADIG填充，费率到位，附加的文书工作逐封电子邮件归档。

您从未填写过表单来做到这一点。电子邮件□□输入。

OmniRoam的操作

Lexical error on line 7. Unrecognized text. ...oaming/inbound-email] HOOK --> EP ----------^

□试

逐步操作，一旦邮件到达OmniRoam：

1. 它确定邮件是针对哪个运营商（租户），通过将To/Cc地址与运营商的配置入站地址进行匹配。如果没有匹配，电子邮件将被记录为无运营商，并且□□□□□□：安全的无操作。
2. 它读取附件，而不仅仅是正文。商定的费率或签署的条款通常在附加的**AA.13 · IOT□□□**率表或电子表格中。因此，OmniRoam从PDF · Word · Excel和CSV附件中提取文本，并将其提供给提取器。签名块的徽标（PNG/JPG）被忽略。

3. 它使用**ChatGPT API**提取事实。提取器特别被告知外部发件人通常只是□□线程（通常是您自己的漫游经理），并读取整个引用历史。它将费率、联系人、地址和SIM卡归因于实际声明它们的人，而不是转发者。它返回一个结构化记录：合作伙伴名称、国家、地址、TADIG(s)/PLMN、最佳匹配的生命周期状态、商定的费率（仅在□□明确同意时）、合作伙伴联系人、交换/请求的SIM卡、是否附加了签署的协议，以及一行摘要。
4. 它找到正确的协议，或创建一个。匹配是故意宽容的，因此线程永远不会产生重复项：精确的合作伙伴名称，然后是“标准化名称”匹配（因此*AT&T Mobility*与*AT&T*合并），然后是共享**PLMN**（MCC+MNC）匹配。这是一个非常高精度的信号，因为PLMN唯一标识一个网络。无匹配→一个全新的协议。
5. 它仅合并新内容。对于新协议和现有协议，OmniRoam应用此电子邮件新揭示的内容，并从不覆盖现有值：
   - 状态仅在生命周期中□□移动（从不向后）。
   - 国家/地址在空白或更改时设置。
   - **TADIGs**添加，但仅限于IR.21目录中存在的代码（因此AI无法发明一个），并且绝不包括您自己本地网络的代码。
   - 联系人添加，或现有联系人□□（填充空白字段）。
   - **SIMs**记录（合作伙伴共享的测试SIM）和**SIM**请求（有人要求运送到某个地址的批次）。
   - 商定的费率成为费率层，仅在双方明确同意时，并且绝不重复现有层。
   - 一个签署的**AA.12/AA.13**（附加或在邮件中声明）将状态推进到*IRA□□*。
6. 它写入两个记录。协议时间线上的友好活动日志条目（“来自□□□□□*Jane*□□□□□（转发）：商定的数据费率；状态→rates_agreed，添加联系人Jane，记录商定的费率”），以及原始入站审计行（见下文）。

处理是幂等的：相同的电子邮件（按Message-ID）仅处理一次，因此抄送多个人员或重新转发线程永远不会重复计数。

电子邮件进入的三种方式

您只需一种。所有三种方式最终都调用相同的处理逻辑：

路径	工作原理	何时使用
Cloudflare电子邮件**Worker**	Cloudflare电子邮件路由将原始消息转发到一个小Worker，该Worker将`.eml`直接流式传输到OmniRoam webhook。	已经使用Cloudflare的域；没有邮箱进行轮询。
IMAP轮询器	OmniRoam每~60秒登录一个真实邮箱，处理未读消息，并将其标记为已读。	任何标准邮箱（隐式TLS、STARTTLS或普通）。
提供商入站解析	邮件提供商（Mailjet/SendGrid）将解析后的消息+附件POST到webhook。	如果您已经运行入站解析。

webhook`/api/roaming/inbound-email`

UI**AI**``

→

2.

TADIG/“”“”

*□□□

- 路由：DRA路由、SS7全球标题、DNS和IP范围用于配置（大部分来自合作伙伴的IR.21预填充）。

详细页面上的一切都是可编辑的。自动化为您提供了一个起点，您可以根据需要手动更正或添加。

IR.21目录

TADIG查找依赖于一个全球**IR.21**世界运营商目录，以TADIG为键（组织、网络、MCC/MNC、DNS、IP范围、SS7节点、联系人）。这就是OmniRoam验证AI提取的TADIG、发现合作伙伴的兄弟TADIG，并预填充路由数据的方式。

---

3. 自动文档生成与签署

生成文档

在协议的文档部分，您选择文档类型并单击生成。OmniRoam渲染真实的Word表单，填写双方的详细信息，准备签署：

类型	内容	格式
AA.12	GSMA AA.12 IREG漫游协议（真实表单，双方预填充）	.docx / PDF
AA.13	GSMA AA.13常见附录，包括计费/结算附录（见AA.13结算选项）	.docx / PDF
CLL	商业启动信（通用）	.docx / PDF
CLL（双边/单边，测试后）	启动信确认启动日期在成功的**IREG**和**TADIG**测试后	.docx / PDF
CLL（双边/单边，默认）	启动信默认启动，无需完成**IREG/TADIG**测试	.docx / PDF
TCC（**VoLTE**）	VoLTE测试呼叫完成	.docx / PDF
TADIG完成	TADIG完成表	.docx / PDF
TNS漫游协议表	TNS清算所请求（以传统.doc格式交付）	.doc
TNS 3G-4G请求	TNS清算所请求	.docx

字段如何填充。每个文档都是一个带有占位符的Word模板（docxtpl / Jinja）。OmniRoam从以下内容中填充它们：

- 本地侧：来自您的运营商记录：您的名称、法定名称、TADIG、PLMN、国家、签署人和职称、地点和地址。因为这来自租户，所以每个托管的运营商自动获得自己的信头和签署人。
- 合作伙伴侧：来自协议：合作伙伴名称、合同正文中使用的简写、TADIG(s)、PLMN(s)、国家和地址。合作伙伴的签署人/职称默认留空，以□他们可以签署。
- 派生值：生效日期、方向（双边/入站/出站）、中心公司、Diameter领域、货币和确认的IOT费率。

输出格式：默认**Word**，签署时为**PDF**

生成默认产生一个可编辑的**Word** `.docx`。这是您审查并在需要时手动编辑的工作副本。您仅在实际需要固定的最终渲染时才获得PDF：

- 在单击生成之前勾选**PDF**输出复选框，以渲染PDF而不是`.docx`。
- 电子签名流程始终使用PDF（签名的文档不得更改）。
- 按需下载/预览已归档的文档*□□PDF*。

一封漫游包电子邮件将AA.12/AA.13作为可编辑的`.docx`附加，以□合作伙伴可以审查和评论。这不是签署步骤，因此不会以PDF形式发送。

AA.13结算选项（附录**C.3.2**）

GSMA AA.13附录C.3.2（计费与结算）是每个合作伙伴谈判的选择菜��：哪种发票模型、哪种支付方式、结算阈值和周期、支付条款和利息。OmniRoam并不将一组选择锁定到模板中，而是将它们作为结算选项面板显示在文档部分：展开**AA.13**结算选项，为该合作伙伴设置值，然后单击生成**AA.13**。生成的附录仅包含您选择的选项。替代选项（以及GSMA“删除不适用的选项”框架）会自动删除。

每个字段都有合理的默认值，因此在不触及面板的情况下生成将产生标准条款；仅更改特定合作伙伴的不同内容。

选项	默认	描述
发票类型	单网络发票（SNI）	选择结算附录：单网络（**SNI**）→附录C.3.2 H，或多网络（**MNI**）→附录C.3.2 I。未使用的附录将被删除。
支付方式	净结算	结算机制：净结算、直接全额支付（无转换）、直接全额支付（带转换），或无转换的净结算。仅保留所选方法的条款。
阈值结算	选项1（净结算）	**选项1（净结算）**适用单一商定的低余额阈值；**选项2（直接支付）**使用每方（A方/B方）阈值。
阈值	50	结算货币（例如SDR）中的低余额结算阈值金额。低于此每月总额，结算可能会被推迟 ��?
周期开始 / 周期结束	一月 / 十二月	低于阈值的余额的非结算周期，通常是财务年度。
支付天数	60	从发票日期起，债务人必须支付的天数。
本地利息%	8	当本地运营商是债权人时，债权人可以对逾期余额收取的年利息。
合作伙伴利息%	8	当合作伙伴运营商是债权人时的年利息。
发送零值发票	关闭	关闭时，附录声明每方不会发送零（0.00）金额的每月发票。
TAP发票上的**BCE**	关闭	关闭时，附录声明BCE使用不会包含在TAP漫游发票中。

工作原理。选择作为覆盖传递给生成，叠加在内置默认值之上。AA.13模板将它们解析为完成的附录：选择正确的选项块，填写金额/周期/费率，并表述切换。结算货币本身来自协议配置的货币，而不是此面板。

用例。合作伙伴坚持90天条款、100 SDR阈值和四月-三月财务年度：打开面板，设置支付天数90，阈值100，周期开始四月，周期结束三月，然后生成。其他条款保持标准条款。

> **TNS**清算所表单是特殊的。两个TNS请求//docxtpl模板。它们是运营商的真实TNS表单，仅更改可填写字段并勾选正确的 ��选框，以TNS接收确切的预期布局。它们是**IOT**门控的：OmniRoam不会生成它们，直到协议有确认（商定）费率。尝试提前返回明确的“需要确认的IOT”消息。复选框状态（协议类型、方向、服务、LTE接口、GRX）是自动从协议中派生的，所有字段在生成时都是可覆盖的。

服务器上的无头LibreOffice负责PDF生成（以及TNS的传统.doc）。您只需获取完成的文件。

协议的文档部分。左侧生成合同；下方列出生成和接收的文档（带签署状态），每个文档可下载。

签署：在线或离线

OmniRoam支持两种签署方式：

在线电子签名（合作伙伴在浏览器中签署，无需登录）。从生成的AA.12/AA.13中，您单击发送签名请求，命名签署人及其电子邮件， OmniRoam：

1. 创建一个带有不透明令牌的签名请求，并向合作伙伴发送一封安全链接的电子邮件（无需账户）。
2. 当他们打开时，OmniRoam将请求标记为已查看并在时间线上记录。合作伙伴查看文档，可以选择更正其签署人姓名/职称/公司，并通过输入其姓名和/或绘制签名来签署。
3. OmniRoam生成签署的PDF并将其发送给双方（签署人+您运营商的返回邮箱），将其归档在协议上，并记录“由…在…签署”。
4. 合作伙伴也可以拒绝（附带理由），这也会被记录。

离线签署。更喜欢传统方式签署？下载生成的文档，外部签署，然后将签署的副本上传回协议。包含□□/□□/□□□的文件名被识别为签署副本。附加一个这样的文件的入站电子邮件会自动将状态推进到*IRA□□□*。

漫游包：一键首次联系

与其单独生成每个表单，不如发送漫游包电子邮件给合作伙伴联系人，将**AA.12 + AA.13 + IOT**报价一起发送在一条消息中。它实时生成合同作为PDF并附加您最近的IOT报价。选择一个联系人（或输入姓名＋电子邮件，作为联系人回填），OmniRoam使用您保存的模板措辞发送包。这是“让我们达成漫游交易”的开场电子邮件，从OmniRoam内部发送。

可编辑的电子邮件模板

三封自动电子邮件（签名请求、签署副本和漫游包）使用可编辑模板（每个运营商覆盖，否则为全局默认），带有占位符，如`{{ signer_name }}`、`{{ partner }}`、`{{ operator }}`、`{{ sign_url }}`和`{{ document_name }}`。在设置中调整措辞一次，每次发送都使用它。

> 电子邮件实际上是如何离开**OmniRoam**的。所有出站邮件通过**Mailjet HTTPS**发送**API**发送，而不是SMTP。托管平台（Railway）阻止出站SMTP端口，因此OmniRoam通过HTTPS向Mailjet发送POST。发送是尽力而为且非阻塞的：UI按钮立即返回，邮件在后台线程中发送，因此慢邮件服务器永远不会阻塞应用程序。

---

4. 归档与存储

每个文档直接归档在其所属的协议上。这包括生成的文档（AA.12、AA.13、CLL、TCC、TNS…）和接收的文档（附加在电子邮件中的签署副本、上传的IR.21、IOT表）。没有单独的文档存储需要管理：

- 文档作为blob存储在数据库中，带有类型标签`aa12`、`aa13`、`aa12_signed`、`iot`、`ir21`、`cll`、`other`等）、文件名、内容类型、大小，以及OmniRoam生成它的标记。
- 签署副本被特别标记（例如`aa12_signed`），因此签署集始终与草稿区分开。
- 入站附件去重：再次到达的相同副本（相同文件名＋字节长度）不会重新归档。
- 每次生成、上传、签名和IOT导出都会写入时间线条目，因此协议的活动日志是完整的文书记录，记录了什么被生成和接收，以及何时。

要检索文档，请打开协议的文档部分并下载它（生成的Word/PDF，或接收的原件）。通过在线签署流程生成的签署PDF存储在签署请求上，并且也会发送给双方。

您还可以将商定的费率导出为GSMA RAEX IOT 5.0 XML文件。这个费率选择与TNS表单使用的相同，因此导出的IOT和生成的表单始终一致。

5. 工作订单与受让人通知

让合作伙伴上线是工作：运输SIM、更改路由、运行IREG/TADIG测试、审计、追踪问题。在OmniRoam中，这项工作被跟踪为工作订单：漫游工作的单一跟踪单位。工作订单可以挂靠在协议（合作伙伴）上或独立存在。

工作订单视图。每个订单都有类型、优先级、状态、可选的合作伙伴链接和受让人：在分配时通知的方。

创建和分配

工作订单具有类型（SIM派遣、路由、IREG测试、TADIG测试、审计、问题）、标题、优先级、状态（打开/进行中/阻塞/完成/取消）、可选的合作伙伴（协议）链接、自由文本详细信息、截止日期和特定类型的结构化字段（例如，SIM派遣包含数量、邮寄地址、承运人和追踪）。

您将工作订单分配给方：一个命名的内部团队或外部联系人（例如“漫游NOC”、“TADIG管理员”），在设置中按运营商管理。您可以为每种工作订单类型设置默认受让人，因此新的SIM派遣会自动分配给处理派遣的人员，除非您覆盖它。

通知：**webhook +** 电子邮件

当工作订单被分配（创建时有受让人，或重新分配给新方）时，OmniRoam通过该方配置的任何渠道通知该受让人：

- **Webhook**：如果该方有一个webhook URL（例如**Slack**传入**webhook**），OmniRoam会POST一条消息，包含可读的`text`块∕完整的工作订单作为结构化JSON（类型、优先级、状态、合作伙伴、特定类型的有效负载、返回工作订单页面的链接）。
- 电子邮件：如果该方有电子邮件地址，OmniRoam将通过电子邮件发送相同的详细信息（通过Mailjet），主题为`[工作订单] <标题>分配给您`。

没有设置任何渠道的方只是一个静默受让人（无操作）。两种通知都是尽力而为且非阻塞的，因此慢webhook或邮件服务器永远不会阻塞应用程序。重新分配仅在受让人实际更改为新方时通知（因此编辑其他字段不会重新通知人员）。

> 从受让人的角度：您会在团队上收到一条Slack消息（或电子邮件），当工作落到您的团队时，包含您所需的一切：要做什么、为哪个合作伙伴、SIM数量和运输地址（或路由更改，或测试范围）、优先级和截止日期，以及直接链接到工作订单。

完整生命周期，端到端

将所有内容结合在一起，□□是从“合作伙伴给我们发电子邮件”到“合作伙伴上线”的旅程：

您转发到OmniRoam收件箱

抄送线程

在每一步，协议的时间线记录发生了什么，入站电子邮件日志保留了每封电子邮件贡献的原始证据。

您一次设置的内容

大多数自动化只需为每个运营商进行一次小配置（在设置中）：

设置	原因	使用位置
文书工作详情（法定名称、TADIG、PLMN、国家、签署人和职称、地点、地址）	填充每个生成文档的本地侧	文档生成
入站电子邮件[illegible]址	您转发/抄送合作伙伴邮件的地址	电子邮件摄取
签署返回邮箱	离线签署和签署副本电子邮件的去处	签署
电子邮件模板（签名请求、签署副本、漫游包）	您的措辞用于自动电子邮件	出站电子邮件
工作订单方 + 每种类型的默认受让人	每种工作类型的通知接收者	工作订单

有了这些设置，转发合作伙伴电子邮件确实变成了：[illegible] → [illegible] → [illegible] → [illegible]

另请参见

- OmniRoam：漫游测试自动化：[illegible]OmniRoam。它在实时网络上运行GSMA漫游测试书（IR.38 / IR.48 / VoLTE）。这是互补的：在这里签署协议，在那里证明它有效。
- 常见操作：在OmniWeb中共享的查看/编辑模式。

OmniRoam：漫游测试自动化

OmniRoam 是 OmniWeb 的漫游测试书自动化功能。它在实时网络上运行 GSMA 漫游合规测试书。它自动从测试设备驱动各个测试用例。它记录每个案例的通过/失败裁决及支持证据。然后，它生成一个完整的 GSMA 测试书工作簿，准备发送给漫游合作伙伴或中心。

简而言之：OmniRoam 将手动的多小时漫游合规工作变成一次按钮按压（或一个计划任务）。它返回同样的官方 GSMA 电子表格，测试人员本来需要手动填写。

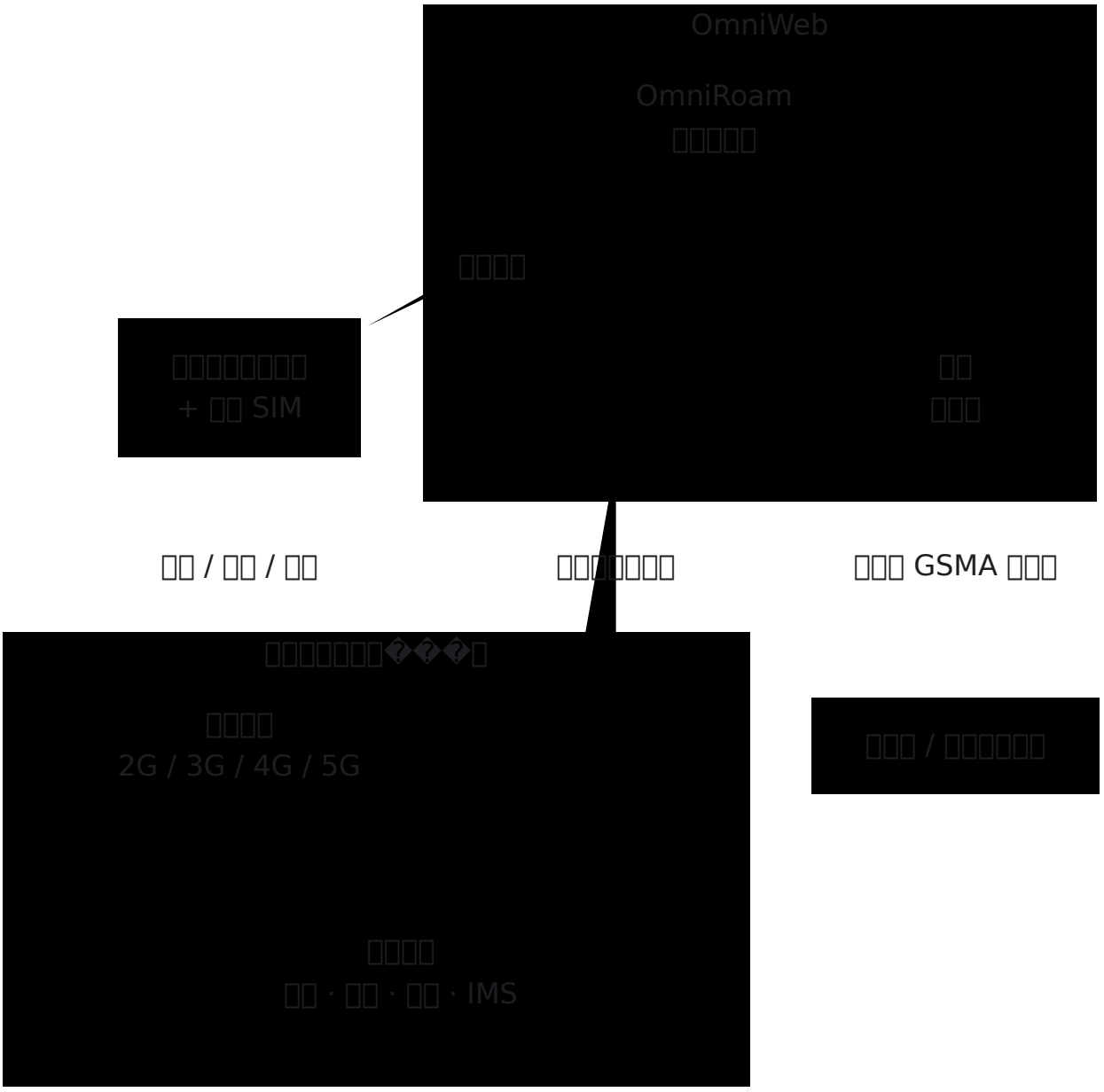
> **OmniRoam** 有两个方面。本文档涵盖 漫游测试书（IR.38 / IR.48 / VoLTE 合规测试：□□□□□□□□□）。另一个方面是 漫游协议与电子邮件自动化。它将合作伙伴电子邮件转变为签署的协议，生成 AA.12/AA.13/CLL/TCC/TNS 文件，以及使合作伙伴上线的工作订单。该内容在 漫游协议与电子邮件自动化 中单独记录。一个产品，���个任务：□□□□□□（那里）和 □□□□□□（这里）。

□□

快速链接

- 测试书：可用的书籍（IR.38、IR.48、VoLTE）及其包含的每个测试用例
- 运行测试：如何创建一本书，运行它，自定义案例集，以及安排例行运行

- □□□□



OmniWeb
OmniRoam
□□□□□□
□□□□
□□□□□□□□□□
+ □□ SIM
□□
□□□□
驻留 / 拨打 / 发送
读取□□并记录
完成的 GSMA 工作簿
□□□□□□□□□□□
□□□□
2G / 3G / 4G / 5G
□□□□
□□ · □□ · □□ · IMS
□□□ / □□□□□□□

关键概念

术语	含义
测试书	一组由 GSMA 定义的测试用例（例如 IR.38、IR.48、VoLTE）。见 测试书。
测试用例	一本书中的单个检查，通过其 GSMA 编号识别（例如 IR.48 案例 `2.3`，“禁止所有外拨电话”）。
运行	针对设备和 SIM 的一本书（或其选定子集）的执行。
裁决	案例的记录结果：`通过`、`失败` 或 `未执行`。
证据	为裁决捕获的支持细节：时序、吞吐量数据、网络原因、查询读取等。
家庭 **PLMN (a)**	拥有被测试用户的网络。
访问 **PLMN (b)**	用户正在漫游的网络。

自动化案例与手动案例

每本书中的大多数案例都是 自动驱动 的：OmniRoam 完成它们的端到端，并在没有操作员交互的情况下记录裁决——少数案例依赖于无法仅从测试设备诱导的网络条件（例如，选项 CAMEL 预付费负面测试或多媒体消息传递交付）。这些仍然是 手动 的。OmniRoam 仍然在书中列出它们，操作员手动记录结果，因此最终文档是完整的。

测试书浏览器 显示了书中哪些案例是自动化的以及每个案例如何驱动。

参考标准

OmniRoam 遵循 GSMA 永久参考文档和基础的 3GPP 规范：

参考	适用
GSMA IR.38	LTE 漫游数据测试书
GSMA IR.48 / IR.24	双边漫游（语音 / 短信 / MMS / 数据）测试书
GSMA BA.65	漫游 VoLTE 测试
GSMA IR.92	语音和短信的 IMS 配置文件（VoLTE 行为）
GSMA IR.88	LTE 漫游指南（接入拒绝原因）
3GPP TS 22.011	服务可达性（运营商确定的禁止）
3GPP TS 23.011	补充服务状态（活动/注册/已配置/静止）
3GPP TS 22.082	呼叫转移补充服务
3GPP TS 22.088	呼叫禁止补充服务

完成的测试书文档

OmniRoam 运行的最终产品是一个 完成的 **GSMA** 测试书工作簿：这是官方的 GSMA 电子表格，填充了运行的结果和所有相关细节，准备发送给漫游合作伙伴或中心。OmniRoam 通过一个 下载测试书 操作生成它。它不需要手动转录。

您将获得的内容

OmniRoam 使用官方的 GSMA 模板填充工作簿，因此结果是合作伙伴期望收到的相同工作簿（相同的工作表、相同的案例编号、相同的布局），但填充了真实的结果，而不是空白字段。

填充的内容

有三类信息被写入工作簿中。

1. 每个案例的结果

对于书中的每个案例，工作簿的结果单元格设置为记录的裁决（通过、未通过或未执行）。案例的评论单元格填充了在��行期间捕获的支持证据。

文档中的内容	来源
测试案例结果（通过 / 未通过 / 未执行）	案例裁决
测试案例评论	证据：时间、吞吐量、网络原因、询问读回等。

2. 身份和元数据

标题和操作员信息部分从运行中填充：

文档中的内容	来源
IMSI	测试 SIM
MSISDN	测试 SIM
本地 PLMN (a) / 访问 PLMN (b)	漫游合作伙伴 / 为书籍选择的 PLMN
测试日期	运行日期
测试者姓名、电话、电子邮件	书中的测试者详细信息
APN（如适用）	使用的数据配置

3. 测量值

对于数据和补充服务案例，GSMA 表格要求的特定测量值被写入其专用单元格：

文档中的内容	来源
数据会话开始 / 结束时间	数据会话
发送 / 接收的数据量	服务网关的计费记录
会话持续时间	数据会话
吞吐量 / 平均数据速率	吞吐量测量
服务成功指示（是/否）	案例结果

干净、可展示的输出

空白的 GSMA 模板在填充单元格中附带示例和占位符内容：样本时间和参考说明，旨在指导手动测试者。OmniRoam 在生成文档 ��删除这些占位符内容，因此完成的工作簿仅显示您的真实结果和未捕获值的空字段。它从不将供应商的示例数据带入您的交付报告，也从不覆盖 GSMA 标签、标题或结构。

removed

何时生成

您可以在任何时候下载文档。它始终反映运行的当前状态。一个典型的流程是运行书籍（或计划例程）、审查每个案例的裁决、重新运行需要关注的案例，然后在结果看起来正确后下载完成的工作簿。由于导出反映了实时运行，因此在重新运行后重新导出只会生成更新的文档。

文档中的手动案例

OmniRoam 无法自动驱动的案例仍然出现在工作簿中，带有其案例编号和标题，准备让测试者手动记录结果。这使得交付的文档保持完整：自动化案例填充了真实证据，而手动案例则在正确的位置呈现，供测试者完成。

请参阅 运行测试 了解裁决是如何���生的，以及 测试书浏览器 了解填充内容的确切单元格映射。

□□ OmniRoam □□

□□□

创建测试书

漫游测试书屏幕列出每本书的类型、家庭和访问网络、用户身份、测试者和当前状态。

测试书是从 漫游测试书 屏幕创建的。在创建书籍时，您需要选择：

字段 目的

书籍类型 要运行的 GSMA 书籍：IR.38、IR.48 或 VoLTE。这选择了用例集。

漫游合作伙伴 /
PLMN

家庭 (PLMN a) 和访问 (PLMN b) 网络。用于填充文档头并选择正确的吞吐量阈值。

SIM

要测试的用户 SIM。其 IMSI 和 MSISDN 在整个运行过程中读取并使用，并在最终文档中体现。

测试者详情 负责人的姓名、电话和电子邮件，写入完成的工作簿中。

一旦创建，书籍将列出所选 GSMA 书籍中的每个用例，每个用例都以“尚未执行”状态开始。

□□□□□

□□□□

在运行测试书时，屏幕会显示每个步骤的实时情况，当前步骤高亮显示，并为每个用例提供实时通过/失败指示。

自动化用例的驱动方式

每个自动化用例驱动测试设备，观察网络的行为，并将结果与 GSMA 预期结果进行比较。用例只有在有正面证据时才会通过。无法确认的步骤将记录为失败，并附上原因，而绝不会默默通过。

数据会话和吞吐量

对于数据用例，OmniRoam 建立一个数据包数据会话，运行流量以测量实□□□的下载/上传速率和延迟，然后断开连接，以□网络为该会话写入干净的计费记录。数据量和时间从服务网关的计费记录中读取。对于 IR.38 速度用例，测量的速率与家庭/访问距离的吞吐量下限进行比较。

语音通话

OmniRoam 从设备拨打电话到实验室接听服务，确认电话达到活动（已接听）状态，选择性地保持电话以确认稳定性，然后清除通话。裁决记录连接时间以及通话是否保持。

短信

OmniRoam 向实验室接听服务发送一条带有唯一内容的消息，并等待回复。回复的送达确认了移动发起和移动终止的短信端到端。缺少回复是明确的失败，并附上原因，而不是崩溃。

补充服务（通话阻止和转接）
OmniRoam 从测试设备本身通过空中配置补充服务，正如用户使用标准服务控制代码一样，然后进行测试：

OmniRoam 测试设备 网络

阻止所有外拨电话 (IR.48 2.3)
激活外拨电话阻止
配置阻止
尝试正常通话
通话被拒绝（被阻止）
尝试紧急通话
紧急连接
取消阻止
如果被阻止 + 紧急通话正常则通过

OmniRoam 测试设备 网络

对于 未回复时转接通话，OmniRoam 注册转接到目标号码并设置响铃计时器，然后查询服务并确认网络存储了注册的转接号码和计时器。

取消位置 (IR.38 3.1.2)

某些用例是从网络端驱动的，而不是设备端。对于 LTE 取消位置，OmniRoam 请求家庭用户服务器取消用户在访问网络上的位置，并在请求被接受时记录通过。这确认了家庭网络可以撤回漫游注册。

IMS 注册（VoLTE）

对于 VoLTE，OmniRoam 首先确认设备已注册到 IMS。这是 IMS 依赖用例的门控：如果未确认注册，则 VoLTE 通话和 SMS-over-IMS 用例将被报告为阻塞。

定制运行

运行不必覆盖整个书籍。使用 测试选择器，操作员可以精确选择要运行的用例。这对于以下情况非常有用：

- 仅重新���证之前失败的用例。
- 在故障排除期间仅运行语音用例或仅运行数据用例。
- 跳过依赖于尚未到位的安排的用例（例如，CAMEL 协议）。

被排除在范围之外的用例保持其现有裁决，并且不受影响。

重新运行单个用例

每个用例都有一个重新运行控制。选择它将仅再次运行该用例，针对相同的设备和 SIM，并仅更新该用例的裁决。这是确认修复的最快方式（例如，在运输更改后重新运行吞吐量用例），而无需重复整个书籍。

常规和计划运行

OmniRoam 可以 按计划无人值守地运行测试，以□持续验证漫游关系，而不是仅进行一次检查。

- 常规检查 运行一组紧凑的健康检查，针对设备（数据、速度、语音和短信）并报告组合的通过/失败。这些是完整书籍中使用的相同驱动，打包为快速的重复信心检查。
- 计划 自动在重复间隔上运行所选的常规。每个计划运行记录其自己的结果，随着时间的推移建立历史记录，以□回归（例如，吞吐量降至下限以下或短信送达失败）被捕获并可见，而无需任何人手动运行测试。

设置计划

计划在漫游测试下的 计划 屏幕上管理。计划定义：

设置	目的
名称	标识计划（并标记其指标和历史）。
调制解调器	常规运行所针对的测试设备。
检查	常规执行哪些检查：数据、速度测试、语音、短信。
间隔	常规运行的频率（例如，每小时）。

保存后，计划将在其间隔内自动运行，无需进一步交互。常规测试 屏幕显示运行历史：每次运行的组合通过/失败、测量的速度以及每个检查的详细信息。失败的运行会显示与交互式运行相同的证据。

Prometheus 监控

计划的常规结果作为 **Prometheus** 指标 导出，因此漫游健康可以被警报和与网络的其余部分一起仪表板显示，方式与测试设备上的计划测试监控相同。暴露在 `/api/ir38/routine/metrics` 提供（读取每个计划和调制解调器的最新计划运行）：

指标	类型	意义
`omniweb_ir38_routine_pass`	gauge	最新的计划常规结果（1 = 通过，0 = 失败）
`omniweb_ir38_routine_check_pass`	gauge	��新运行的每个检查结果（标签 `check`：数据/速度测试/语音/短信）
`omniweb_ir38_routine_download_mbps`	gauge	最新运行中测量的下载速率
`omniweb_ir38_routine_upload_mbps`	gauge	最新运行中测量的上传速率
`omniweb_ir38_routine_latency_ms`	gauge	最新运行中测量的延迟
`omniweb_ir38_routine_last_run_timestamp_seconds`	gauge	最新计划运行的 Unix 时间

每个系列都带有 `schedule`、`serial`、`modem` 和 `imsi` 标签（每个检查指标上还有 `check`），因此您可以按计划、按设备或按家庭用户进行警报。该端点无需登录（抓取程序无法携带登录信息），并且在需要时可以通过承载令牌进行门控。

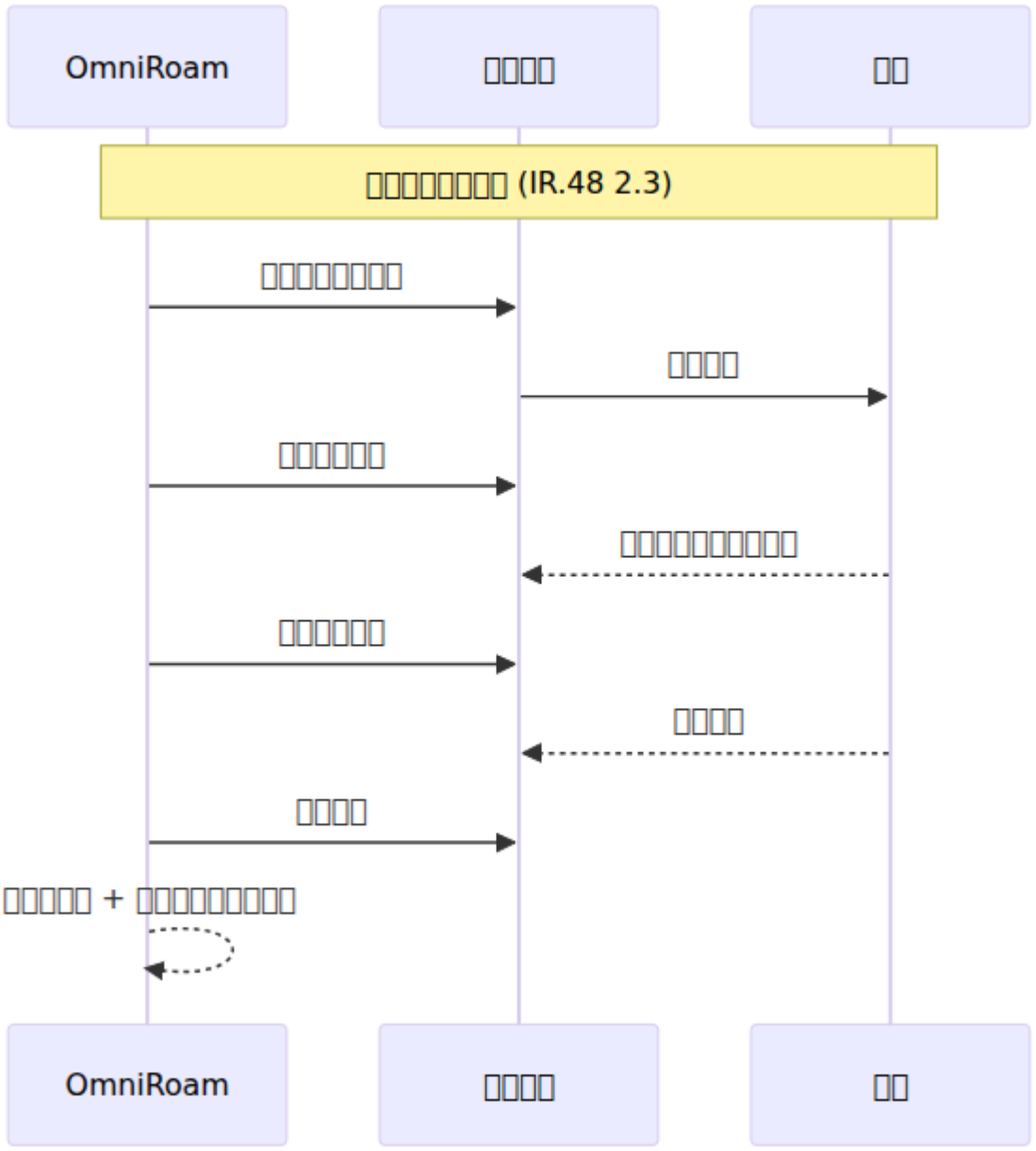
示例警报：在设备上漫游语音已失败 15 分钟：

```
omniweb_ir38_routine_check_pass{check="voice"} == 0
```

计划结果累积成历史记录，可以随时查看，失败的运行会显示与交互式运行相同的证据。

读取结果

每个用例显示其裁决（通过、失败或未执行）以及其背后的证据：



- 通过：确认了 GSMA 预期结果，并附有支持数据。
- 失败：未达到预期结果；原因已记录（例如，“吞吐量低于下限”、“无回声回复”或未连接通话的网络释放原因）。
- 未执行：该用例未运行，或是等待测试者的手动用例。

当结果看起来正确时，生成完成的文档。请参见 完成的测试书文档。

测试书浏览器
测试书浏览器是一个只读参考视图，显示每本测试书的具体测试内容及其方式。它回答了操作员在信任自动运行之前通常会问的三个问题：

1. 这本书中包含哪些案例，哪些是自动化的？
2. 每个案例实际上是如何执行的？
3. 最终文档中包含什么内容，它来自哪里？

可以通过浏览书籍从漫游测试书屏幕访问浏览器，并允许您在 IR.38、IR.48 和 VoLTE 之间切换。

浏览器显示 IR.48 书籍。每个案例列出其是否为自动化或手动，并描述其驱动方式。

测试

测试视图列出了书中每个案例，包括：

- 案例编号和标题（与 GSMA 规范匹配），
- 案例是自动化还是手动，以及
- 如何驱动的简单描述：例如“数据会话 + 收费记录检查”、“语音通话”、“禁止激活和呼叫尝试”或“测试人员记录结果”用于手动案例。

这是快速查看 OmniRoam 为您执行的给定书籍的内容以及哪些仍需手动检查的方式。

如何运行

如何运行视图显示了完整运行书籍时将执行的步骤顺序，依次为：准备设备、数据会话、吞吐量检查、语音和 SMS 驱动、补充服务驱动等。它反映了当前在范围内的案例，因此在您开始运行之前，它是对运行将执行内容的准确预览。

此视图有助于理解运行的形状，并确认自定义范围将执行您所期望的步骤。

表单字段

表单字段视图列出了 OmniRoam 填充的完成 GSMA 工作簿中的每个单元格，每个单元格附有：

- GSMA 模板中的工作表和单元格，
- **GSMA** 字段标签（从模板本身读取），以及

- 值的来源：例如订阅者 MSISDN、测试日期、每个案例的通过/失败裁决，或测量值如数据量。

因为这个列表是基于生成文档的相同逻辑得出的，所以它不能与实际导出脱节：浏览器所说的将被填充的内容正是实际填充的容。请参见 已完成的测试书文档以获取文档本身。

下载模板

浏览器还提供下载模板操作，下载所选书籍的空白 GSMA 工作簿：官方模板，去除了供应商的示例/占位符内容，准备在需要时手动填写。这是运行生成的已完成文档的空白对应物（见 已完成的测试书文档）。

重要性

接受已完成测试书的漫游合作伙伴需要对结果的真实性和文档忠实代表所测试内容的信心。浏览器使映射透明：每个自动化案例都可以从 GSMA 案例编号追溯，通过其驱动方式，直到它在最终文档中落入的确切单元格。

OmniRoam 测试书籍
OmniRoam 提供三本 GSMA 漫游测试书籍。每本书都是官方的 GSMA 测试集，案例通过其 GSMA 案例编号进行标识，因此完成的文档与发布的规范一一对应。

IR.38: LTE 漫游数据测试
IR.48: 双边漫游（语音 / 短信 / 彩信 / 数据）
VoLTE: 漫游 VoLTE 测试

有关每个自动化案例的实际驱动和判断方式，请参见 运行测试。要交互式浏览书籍中的案例，请使用 测试书籍浏览器。

在下面的表格中，驱动 表示 OmniRoam 是否自动执行该案例 (自动) 或者留给测试人员记录 (手动)。

IR.38: LTE 漫游数据测试

基于 GSMA IR.38 v3.0。证明漫游用户可以在访问的 LTE 网络上附加数据，通过家庭网络访问服务，并接收可接受的吞吐量。它还证明了电路交换回退语音和 SMS，以及 2G/3G 数据（如果在范围内）。

案例	标题	驱动	证明内容
`3.1.1`	LTE 速度测试（数据 + 吞吐量）	自动	数据会话通过家庭网关建立，传输流量，并满足吞吐量底线。
`3.1.2`	LTE 取消位置	自动	家庭网络可以取消在访问网络上的用户位置（从家庭用户服务器触发）。
`3.1.3`	LTE 运营商确定的阻止	手动	在家庭用户记录中应用的运营商确定的阻止得到遵守。
`3.2.2`	CS 回退：移动发起语音通话	自动	用户发起的语音通话通过 CS 回退成功。
`3.2.3`	CS 回退：移动终止语音通话	手动	对用户的呼叫通过 CS 回退成功。
`3.2.4`	SMS 通过 SGs	自动	移动发起和终止的 SMS 通过 SGs 接口正常工作。
`3.3.1`	使用 HPLMN 中的 PGW 访问 2G/3G 数据	自动	2G/3G 数据会话通过家庭网关访问服务。
`3.4`	通过 S8 访问 4G + 5G NSA 数据	自动	数据包可用并连接到互联网（通过连接检查确认的数据会话）。

取消位置 **(3.1.2)**

OmniRoam 通过请求家庭用户服务器取消用户在访问网络上的位置来自动化取消位置，然后确认请求已被接受。这是家庭网络发起的漫游注册移除（根据 3GPP TS 29.272 中的位置取消程序）。

吞吐量 **KPI**

案例 `3.1.1` 不仅确认数据会话。它测量实际下载速率并将其与 IR.38 吞吐量底线进行比较。底线取决于家庭网络和访问网络之间的地理距离（更长的路径允许更低的速率）：

协议	距离 **< 4000 km**	距离 **≥ 4000 km**
HTTP	≥ 11 Mbit/s	≥ 5 Mbit/s
FTP	≥ 13.5 Mbit/s	≥ 6 Mbit/s

OmniRoam 根据家庭和访问网络的身份估算距离，并自动选择正确的阈值；当默认值与测试设置不匹配时，运营商可以覆盖距离或协议。在没有将速度与底线进行测试的情况下记录速度永远不会被视为通过。

IR.48: 双边漫游（语音 / 短信 / 彩信 / 数据）

基于 **GSMA IR.48 v2.1**（内部为 IR.24 测试集）。经典的 2G/3G 双边漫游书籍：基本通话、补充服务、短信和数据包，针对漫游到访问网络的用户进行测试。

案例	标题	驱动	证明内容
`2.1`	MS1(a) 呼叫 MS2(a)，均漫游在 VPLMN(b)	自动	成功建立并保持基本语音通话。
`2.2`	CAMEL 负面测试（MOC，预付���，无协议）	手动	在没有有效 CAMEL 协议的情况下，预付费通话被正确阻止。
`2.3`	阻止所有外拨通话（BAOC）	自动	在外拨通话阻止激活的情况下，正常通话失败，而紧急通话仍然成功。
`2.4`	无回复呼叫转移（CFNRY）	自动	可以注册并查询无回复呼叫转移，确认存储的配置。
`2.5`	移动发起 / 终止的 SMS	自动	从漫游用户发送的 SMS 被送达，并收到回复。
`2.6`	CAMEL 负面测试（SMS-MO，预付费）	手动	在没有有效 CAMEL 协议的情况下，预付费 SMS 行为。
`2.7`	使用家庭网关访问内网 / ISP	自动	数据会话通过家庭网关访问互联网/内网。
`2.8`	使用家庭网关和 MMSC 的 MMS	手动	多媒体消息通过家庭 MMSC 发送。

IR.48 中的补充服务

两个补充服务案例是完全自动化的：

- **BAOC (2.3)**：阻止所有外拨通话。 OmniRoam 在测试用户上激活外拨通话阻止，确认网络拒绝正常外拨通话，确认紧急通话仍然连接（所需的例外），然后移除阻止以保持 SIM 干净。
- **CFNRY (2.4)**：无回复呼叫转移。 OmniRoam 注册无回复呼叫转移到目标号码并设置响铃计时器，然后查询该服务（相当于拨打 `*#61#` 状态代码）并确认网络存储了注册的转移号码和计时器。观察实时转移需要来自第三方的入站呼叫，因此最后一步留给手动检查；配置和查询是自动化的。

OmniRoam 使用四个标准 3GPP 标志报告每个补充服务的状态：已配置、已注册、已激活和静默（见 3GPP TS 23.011）。

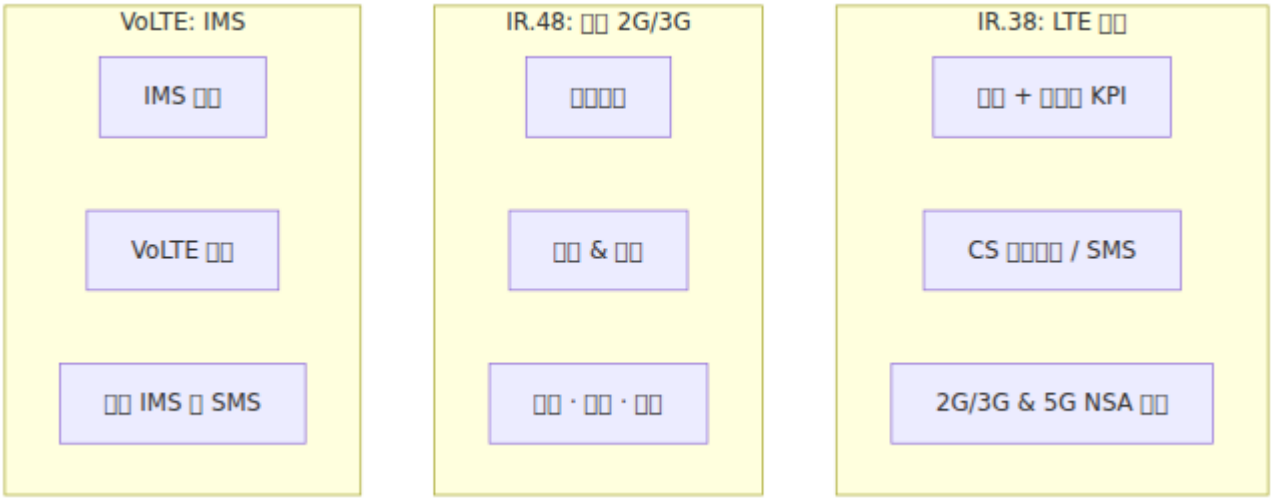
VoLTE: 漫游 VoLTE 测试

基于 **GSMA BA.65 §5.3**，VoLTE 行为根据 **GSMA IR.92**。证明用户在漫游时可以注册到 IMS 并进行/接收 VoLTE 通话和 SMS-over-IMS。

案例	标题	驱动	证明内容
`ims_reg`	漫游中的 IMS 注册	自动	设备在漫游时注册到 IMS（所有 VoLTE 服务的前提条件）。
`mo_call`	VoLTE 移动发起通话	自动	用户发起的 VoLTE 通话成功建立并保持。
`mt_call`	VoLTE 移动终止通话	手动	对用户的 VoLTE 呼叫成功建立。
`sms_ims`	通过 IMS 的 SMS (SMSoIP)	自动	SMS 通过 IMS 网络发送。
`emergency`	VoLTE 紧急呼叫	手动	紧急呼叫通过 VoLTE 成功（从未自动拨打）。

IMS 注册门

VoLTE 服务依赖于 IMS 注册。OmniRoam 首先运行 `ims_reg` 作为门：如果设备未注册 IMS，则 IMS 依赖的案 ��（`mo_call`、`sms_ims`）将被报告为阻塞而不是失败。当 IMS 故障时拨打 VoLTE 通话没有价值，阻塞结果准确告知运营商原因。



各书籍的比较

书籍	主要领域	最适合
IR.38	LTE / EPC 数据	验证新的 LTE 漫游数据关系和吞吐量
IR.48	2G/3G 电路交换 + 数据包	验证语音、补充服务、短信和基本数据
VoLTE	IMS	验证 VoLTE 漫游，一旦 IMS 互联建立

OTA SIM 管理：空中 RFM/RAM

OTA 模块通过空中管理 SIM：它读取和编辑远程卡上的文件。它发送 安全数据包（ETSI TS 102 225 / 3GPP TS 31.115, "03.48" / SCP80），携带远程文件管理（RFM）和远程应用程序管理（RAM）命令。卡片验证并解密每个数据包，执行命令，并返回签名的 收据证明（**POR**）。

实际上，它提供与离线 SIM 文件系统浏览器 相同的文件级编辑：浏览文件树，解码 EF，编辑字段，写回去。不同之处在于 OTA 通过中央主机上的 PC/SC 读卡器、远程 代理 的读卡器，或通过 **SMPP** 远程访问现场的 SIM。

它基于与 SIM 密钥存储 相同的每个 ICCID 密钥存储。配置文件指明 [redacted]，密钥存储持有该卡的实际 **KIC/KID**。引擎从不记录或返回密钥。它仅返回生成的密文和 POR。

什么是安全数据包

安全数据包保护命令 APDU 的端到端，独立于（明文）承载。引擎已针对物理 ISIM 卡进行了验证。

```
Command Packet  =  CPL | CHL | SPI | KIc | KID | TAR(3) | CNTR(5)
| PCNTR(1)
                      | RC/CC/DS | APDUs
```

CPL 计算其后每个八位字节的数量；**CHL** 从 SPI 开始计算到 RC/CC/DS（包括在内）。当加密开启时，从 CNTR 到结束的所有内容都被加密并填充到加密块大小，**PCNTR** 记录添加了多少个八位字节。

- **TAR**（工具包应用程序参考，3 字节）将数据包路由到卡上的服务：特定的 RFM 应用程序或 RAM（卡管理器）。
- **SPI** 标志选择加密、完整性检查、计数器策略，以及 PoR 必须包含的内容。
- **KIc / KID** 指示卡使用哪个传输（加密）和认证密钥集；值来自每个 ICCID 的密钥存储。

完整的安全设置

下面的每个开关都可以在配置文件中设置，所有组合都已实现。卡片供应商将这些称为四个十六进制八位字节 — MSL，PoR，KIc，KID — 配置文件以这种方式接受它们：将 `15213505` 粘贴到 **SPI** 字段中，所有开关都从中设置。该字段也可以反向工作，显示四个八位字 ���在您更改开关时的更新，因此可以根据个性化表读取设置。

SPI 八位字节	设置	选项
MSL	完整性	无、冗余检查（RC）、密码校验和（CC）
MSL	加密	开 / 关
MSL	计数器	无计数器；存在但未选中；必须更高；必须高一个
PoR	要求	从不；始终；仅在错误时
PoR	响应完整性	无、RC、CC
PoR	加密	开 / 关
PoR	承载	SMS-DELIVER-REPORT 或 SMS-SUBMIT
KIc	加密算法	DES-CBC、三重 DES-CBC 2-key、三重 DES-CBC 3-key、DES-ECB、AES-CBC
KIc	密钥版本	1–3
KID	校验和算法	DES-CBC、三重 DES-CBC 2-key、三重 DES-CBC 3-key、AES-CMAC
KID	冗余算法	CRC 16、CRC 32
KID	密钥版本	1–3

KID 八位字节在 MSL 的两侧有不同的含义：当完整性选择为 **CC** 时，它命名一个校验和算法，而当为 **RC** 时，相同的位命名一个 CRC。配置文件编辑器交换选项以匹配，RC 长度随之而来 — CRC 16 为两个八位字节，CRC 32 为四个。

密钥版本停止在 3，因为卡片记录持有三个密钥集；SPI 本身允许 1–15。

每个密钥集的参数

卡片是通过每个密钥集的算法进行个性化的 — 密钥集 1 可能是三重 DES 加 CRC，而密钥 3 是 AES 加 CMAC。这与密钥有关，而不是与偶然选择它们的配置文件有关，因此 SIM 密钥存储中的每个密钥集都携带其自己的 SPI。

当密钥集记录一个时，它的 算法和密钥版本 会替代配置文件的，因为使用其他任何东西构建的数据包会被卡片拒绝。所有真正是运营商选择的内容 — TAR、PoR 策略、计数器策略、是否加密、命令格式 — 仍然来自配置文件。预览报告哪些设置来自哪里，因此与卡片不一致的配置文件在发送任何内容之前就会显示，而不是在之后作为失败交付。

没有记录 SPI 的密钥集不会改变任何内容：配置文件保持原样。

收据证明 是根据相同的设置解码的，包括验证其 RC 或 CC。状态八位字节以规范自己的措辞报告 — *PoR OK、RC/CC/DS □□、CNTR □、CNTR □、CNTR □□□、□□□□、□□□□□□□□、□□□□、□□□□□□、TAR □□、□□□□□□*。

远程命令格式

命令脚本默认使用 紧凑 格式：C-APDUs 一个接一个。配置文件可以选择 扩展 格式（ETSI TS 102 226），它将每个 C-APDU 包装在 `22` TLV 内部的 `AA` 命令脚本模板中，选项为不定长编码（`AE`）。卡片以 `AB` 或 `AF` 模板回复，每命令持有一个 `23` R-APDU，因此可以追踪失败的脚本到失败的命令，而不仅仅是最后的状态字。有些 TAR 不接受其他格式。

内部的 APDU 是普通的 C-APDU 脚本：`SELECT` + `READ BINARY` 用于 RFM 读取，`SELECT` + `UPDATE BINARY` 用于写入，GlobalPlatform `DELETE` / `INSTALL` 用于 RAM。

在网络上传输（SMS-PP）数据包在 TP-用户数据中携带 UDH 命令数据包标识符（IEI `0x70`）、PID `0x7F`（SIM 数据下载）、DCS `0xF6`（8 位，消息类别 2）。在壳内，它作为 CAT `ENVELOPE(SMS-PP-Download)` APDU 交付，PoR 同步返回。

对于一个短消息过长的数据包会自动拆分，使用 8 位连接头或 — 通过 SMPP — 使用 `sar_*` 参数，以 SMSC 重新组装。

配置文件、上下文和自动路由

OTA 配置文件 是可重用的安全预设。它 不包含密钥材料：

字段	意义
`tar`	3 字节工具包应用程序参考（目标服务）。
`kic_index` / `kid_index`	哪个密钥集（1/2/3）→ `KIC{n}`/`KID{n}` 来自卡片的密钥存储行。
`cipher_algo` / `cc_algo`	加密和校验��算法（`triple_des_cbc2`，`aes_cbc` 等）。
`ciphering`，`rc_cc_ds`，`counter_mode`	SPI：加密？CC vs RC vs 无？重放计数器策略。
`por`，`por_ciphered`，`por_rc_cc_ds`	需要 PoR？加密？签名？

有两个预设，匹配在 sysmoISIM 上验证的值：

- **RFM-USIM-3DES-keyset3**：TAR `B00011`，密钥集 3，3DES，加密 + CC，要求 PoR + 加密 + CC。操作在 **ADF.USIM** 内。

- **RFM-SIM-3DES-keyset2**: TAR `B00010`，密钥集 2。在 **MF-rooted** 2G 树（DF.GSM / DF.TELECOM）上操作。

不同的应用程序需要不同的服务，因此浏览器 根据文件自动路由配置文件和 **SELECT** 上下文，根据文件的应用程序：

文件应用程序	上下文	配置文件（按 **TAR**）	**ENVELOPE** 之前的预选择
`ADF.USIM`	`usim`	TAR `B00011`	`SELECT ADF.USIM`（按 AID）
`DF.GSM`、`DF.TELECOM`	`sim`	TAR `B00010`	无（MF-rooted）
`ADF.ISIM`	`isim`	TAR `B00013`	`SELECT ADF.ISIM`（按 AID）

每个上下文映射到您的配置文件之一（默认通过匹配 TAR，浏览器中可覆盖）。选择一张卡并单击任何文件（USIM、GSM 或 TELECOM）。OmniWeb 应用正确的配置文件、密钥集和 SELECT，而无需切换任何内容。ISIM 在您为其创建配置文件后即可工作（其 TAR 根据卡片而异）。

传输

传输负责传递安全数据包，并在承载允许的情况下收集 POR。可插拔适配器共享一个接口：

类型	到达	**POR**	备注
`local_pcsc`	中央主机上的 PC/SC 读卡器中的卡	同步	直接连接的验证路径。
`agent_reader`	远程代理中的读卡器中的卡	同步	通过与 测试设备 / SIM 银行 相同的代理 WebSocket 传递（`session_apdu` 中继）。
`smpp`	通过 SMPP `submit_sm` 的 现场 **SIM**	异步	MT SMS 到 SMSC; PoR 稍后作为 MO SMS 返回，或在绑定为收发器时在同一连接上返回。请参见下面的 **SMPP** 参数。
`http_admin`	通过 **HTTP**（**SCP81**）的 现场 **SIM**	异步	触发 SMS 使卡通过 TLS-PSK 拨打远程管理服务器；脚本 + 响应在此流动。请参见下面的 **HTTP OTA**。

浏览器 仅使用壳内传输（它需要同步的 PoR）；活动 可以使用任何传输，包括 SMPP。

SMPP 参数

OTA 短消息与普通消息在少数参数上有所不同，SMSC 将接受一个错误的消息并安静地不将其交付给卡片。所有这些都是可设置的：

参数	默认值	重要性
`esm_class`	`0x40`	标记用户数据以头部开始。没有它，卡片永远看不到命令数据包标识符。
`protocol_id`	`0x7F`	（U）SIM 数据下载。
`data_coding`	`0xF6`	8 位，消息类别 2 — 将消息路由到 SIM 而不是收件箱。
`dest_addr_subunit`	`0x02`	目标子单元是 SIM。此参数在数据包被接受但从未到达时最常缺失。
`user_message_reference`	未设置	通过大多数 SMSC 传递到 MO PoR，这就是如何将异步 PoR 匹配回其工作。
`registered_delivery`、`validity_period`、`priority_flag`、`service_type`、`schedule_delivery_time`、`replace_if_present_flag`、`sm_default_msg_id`	SMSC 默认值	普通 submit_sm 控制。

长数据包通过三种方式分段：用户数据中的 8 位连接头（默认），`sar_msg_ref_num` / `sar_total_segments` / `sar_segment_seqnum` 参数，以□ SMSC 重新组装，或单个 `message_payload`，在 SMSC 支持的情况下。可以按名称添加任何其他可选参数。

在发送之前，传输将报告有效但不会到达 SIM 的设置 — 缺少头部标志、数据编码落入收件箱、目标子单元不是 SIM。

发现卡片的参数

无法询问卡片使用哪个 TAR 和安全设置进行个性化。当一批到达时带有密钥但没有文档，配置文件 → 发现参数 通过���测找到它们：它尝试每个卡片的密钥集与合理的参数空间进行匹配并报告卡片接受的内容。结果可以直接转换为配置文件，使用 使用。

这需要壳内传输 — 存储转发承载无法回答每个探测。

两个因素使得简单的扫描无效，发现运行处理这两个因素：

- 计数器过低会被静默拒绝。当安全级别要求 □□□□□□□ 时，给定计数器等于或低于其存储值的卡片不会返回任何内容 — 没有错误，没有收据证明。这与错误的密钥或错误的 TAR 无法区分。因此，发现从高计数器开始；由于计数器只会增加，从高开始不会造成任何成本。
- **PoR** 字节决定答案返回的位置。当第 6 位清除时，卡片在 ENVELOPE 响应中回答；当它设置时，卡片会主动提升一个发送短消息，并且 ENVELOPE 响应为空。仅监视一条路径，正确答案是不可见的，因此两者都被搜索。

CNTR 低 的状态被视为成功而不是失败：这意味着密钥、TAR、算法和安全级别都被接受，只有计数器错误。发现在此停止，通过加倍计数器解决，这需要几轮往返，而不是继续扫描。

如果没有任何内容被接受，这确实不会告诉您哪个参数错误 — 沉默是卡片对每种错误的��应。

> 每个被接受的探测都会增加卡片的计数器，计数器永远不会下降。

通过 **EF_SMS** 交付

数据包也可以直接写入读卡器中的 `EF_SMS`（`3F00/7F10/6F3C`）的记录中，记录标记为未读。卡片处理它就像是通过空中到达的一样 — 没有 SMSC 和无线电。这是针对桌面或银行中的卡片执行脚本的实用方法。

浏览器

`src/pages/ota/OtaExplorer.tsx`：远程 SIM 文件编辑器。

1. 选择一个 目标 **ICCID**（来自 SIM 密钥存储）和一个 传输。
2. 浏览 文件目录：每个已知的 EF 来自离线文件模型（ADF.USIM、ADF.ISIM、DF.GSM、DF.TELECOM），按应用程序分组并可通过代码 / 名称 / 描述搜索。
3. 选择一个文件 → 通过 **OTA** 读取。安全的 RFM 读取被交付，POR 被解码，EF 被呈现：POR 状态、最后的 SW、原始十六进制 + ASCII，以及 类型字段表单（解码为命名字段）。
4. 编辑 字段（自动重新编码）或 原始十六进制，然后 通过 **OTA** 写入。安全的 RFM `UPDATE` 被发送，文件会 自动读取，以□您在写入后查看卡上的状态。

读取/写入受 `ota` 控制权限的限制；所有内容都记录为 作业。

活动

`src/pages/ota/OtaCampaigns.tsx`: 跨–`[illegible]` SIM 的保存操作: 目标查询 → 操作 → 配置文件 → 传输。

- 目标查询 在运行时针对 SIM 银行 库进行评估: ICCID 列表 / 前缀、IMSI 前缀或范围、代理、银行。空查询故意匹配不到任何内容（没有意外的扩展）。
- 操作 是 RFM/RAM 命令（读取/更新二进制或记录，GP 删除 / 获取状态 / 安装）。
- 运行 为每个匹配的卡创建一个 作业。SMPP 活动是即发即忘（POR 稍后作为 MO SMS 到达）。

运行是有限制的（`CAMPAIGN_MAX_TARGETS`），因此一个错误的查询不能在一个请求中冲击数千张卡片。

作业

`src/pages/ota/OtaJobs.tsx`: 每个 OTA 交付（浏览器读取/写入和活动运行）及其状态和 POR。详细抽屉显示 安全请求数据包（密文）、收据证明 和解码结果（执行的命令、最后的 SW、响应数据）。卡片密钥 从不 存储在作业中: 仅存储密文和 POR。

REST API (`/api/ota`, JWT, RBAC 元素类型 `ota`)

方法	路由	目的
GET	`/profiles` · POST · `/profiles/<id>` PUT/DELETE	OTA 安全配置文件。
GET	`/campaigns` · POST · `/campaigns/<id>` GET/PUT/DELETE	活动。
GET	`/campaigns/<id>/targets`	预览当前匹配的 SIM。
POST	`/campaigns/<id>/run`	执行：每个匹配卡一个作业。
GET	`/jobs`、`/jobs/<id>`	作业历史（按 `campaign_id` / `iccid` 过滤）。
GET	`/files/catalog`	可浏览的 EF 目录（离线文件模型）。
POST	`/explore/read`	通过 OTA 读取一个 EF；返回作业 + 解码 EF。
POST	`/execute`	针对一张卡运行一个操作（RFM 更新、RAM、原始）。
POST	`/preview`	构建安全数据包 而不 发送 — 返回密文、SMS 框架、SPI 细分、使用的计数器和下一个计数器。
POST	`/spi`	将四个 SPI 八位字节解码为命名设置，或根据设置构建八位字节。纯算术；不涉及卡片或密钥材料。
POST	`/discover`	探测卡片接受的 TAR 和 SPI，仅给定其密钥。需要壳内传输；增加卡片的计数器。
POST	`/decode` · `/encode`	解码 EF 字节 ↔ 类型字段（离线）。

RBAC 镜像 `simbank/ir38`：管理员始终通过；否则，JWT 权限与 `element_type == "ota"` 授予查看权限，而其方法中的 `POST` 授予控制。读取被视为控制（它们向卡片传输数据包）。路由在 API 参考 中自动记录。

数据库架构

表	行	关键列
`ota_profiles`	一个安全预设	`name`、`tar`、`kic_index`/`kid_index`、算法、SPI 标志。
`ota_campaigns`	一个保存的扩展	`name`、`profile_id`、`target_query`（JSON）、`operation`（JSON）、`transport`（JSON）、`status`。
`ota_jobs`	一次交付到一张卡	`iccid`、`operation`、`request_hex`（密文）、`response_hex`（POR）、`por_status`、`result`（JSON）、`status`。

密钥存储在现有的 `simbank_keys` 表中（SIM 密钥存储），按 ICCID 通过配置文件的密钥集索引引用。它们在此 不 重复。

工作原理

OTA 引擎处理加密、安全数据包结构、CAT/SMS TLV 和构建和解码 03.48/SCP80 RFM/RAM 数据包所需的离线文件模型。它在代理角色后端服务中运行，并共享壳内传输的代理连接。交付在本地读卡器、远程代理读卡器和 SMPP 传输之间是可插拔的。

安全说明

- 卡片密钥（KIC/KID）从密钥存储中读取以构建数据包，但 从不 写入审计日志或在任响应中返回。仅存储密文请求和 POR。
- 写入文件是破坏性的；浏览器在每次写入之前确认，并读取结果。
- 安全数据包是真正的 03.48：篡改一个字节，卡片会拒绝它（CC 失败）；加密开启时，明文 APDU 永远不会出现在网络上。

HTTP OTA (SCP81 / RAM-over-HTTP)

除了通过 SMS/读卡器的 SCP80，OmniWeb 还支持 **SCP81** — 基于 HTTP 的 OTA，符合 **GlobalPlatform Card Spec v2.3 Amendment B**。卡片打开一个通过 **TLS-PSK** 的 **HTTP** 管理会话，而不是一个安全的 SMS，运行整个脚本。

```
 trigger SMS (SCP80) ─▶ card ─BIP OPEN CHANNEL─▶ TLS-PSK ─▶ Remote Admin Server
                                                          RAS 服务命令脚本，收集响应，最后以 204 结束
```

- 触发 — 一个 `http_admin` 操作发送一个安全的 SMS，携带修正案 B 的 □□□□□□□（RAS 主机/URI、`psk_id`、重试策略）通过相同的 SMPP 承载，然后排队一个管理会话。
- **TLS-PSK** — 预共享密钥 源自卡片的 **KIC/KID** OTA 密钥集；没有证书。TLS 配置文件符合 **GlobalPlatform Amendment B §3.3.2**（规范 ETSI TS 102 226 推迟到）：TLS 1.2 使用 `TLS_PSK_WITH_AES_128_CBC_SHA256` / `TLS_PSK_WITH_NULL_SHA256`，对于 TLS 1.0/1.1 卡片回退到 RFC 4279 套件。`NULL`（仅完整性）套件在此有效 — 脚本已经在 SCP80 下安全。
- 管理循环 — 卡片向 RAS 发送 POST，请求排队的命令脚本，并收集每个响应，直到会话完成。
- 管理会话 视图（`/ota/admin-sessions`）显示每个会话的实时状态、脚本进度和命令→响应阶梯。链接的 作业 承载最终结果，完全像其他传输一样。

加密（PSK 派生、安全触发）保留在 OTA 侧车中；面向公众的 **RAS**（`omniweb-ota-scp81`，一个 Elixir/OTP 服务）不持有密钥 — 它终止 TLS-PSK，并通过 localhost 从后端提取脚本。适用于经典 UICC RFM/RAM 和 eUICC（SGP.02）。请参见 `docs/ota-specs/HTTP_OTA_PLAN.md`。

PGW-C: PDN 网关（控制平面）

PGW-C 是 EPC **PDN** 网关的控制平面部分。它是每个用户数据会话的锚点：它终止与 SGW-C 的 **S5/S8**，建立并保持每个 **PDN** 连接，从运营商的 **IP** 池中分配 UE 的 IP 地址，并通过 **Sx/PFCP** 选择和控制用户平面（**UPF**）。它还通过 Diameter 运行会话的策略和计费：**Gx** 到 PCF/PCRF 进行策略和 QoS，**Gy** 到 OCS 进行在线计费。它还会生成 **CDR** 进行离线计费。在 5G 核心中，相应的功能是 **SMF**。OmniWeb 显示 PGW-C 的实时会话、IP 池、UPF 和 Diameter 对等体、拓扑图和会话历史，以及诊断工具。从同一页面访问的 Grafana 仪表板显示了长期趋势。

← 操作指南

PGW-C 是一个按实例划分的元素页面，可以通过侧边栏在站点的库存中访问，具有多个实例部署的舰队视图。所有流量通过 OmniWeb 后端代理到 PGW-C 的 API，因此它保持在单一的经过身份验证的网关后面。��面头部的文档链接（上下文帮助按钮）打开此页面。它被组织成多个选项卡。

概述

单屏健康读取：PGW-C 的 **API** 状态和其实时状态的摘要（活动会话计数、IP 池利用率、UPF 对等体和 Diameter 对等体）。这是确认节点正常运行并承载会话的最快方式。

会话

每个活动 PGW 会话，每行以订阅者的 **IMSI** 和 **MSISDN** 为键，显示其分配的 **UE IP** 和 **APN**。可以通过 IMSI、UE IP、MSISDN 或 APN 搜索会话。打开会话显示其完整状态：PDN 连接和承载、服务 SGW 和选定 UPF，以及实时的 Gx/Gy 策略和计费上下文。您可以在此处编辑会话。运营商可以调整实时状态，例如会话的 **AMBR**（这会将新的 APN-AMBR 推送到 UPF）和请求的 **Gx** 事件触发器，以控制位置变化报告。运营商还可以 删除 会话，以强制释放卡住或表现不佳的订阅者。由于运营商直接对实时状态进行编辑，因此更改会立即生效。

在多个 PGW-C 部署的情况下，舰队视图中的相同选项卡在一个表��列出所有会话，并在每行显示服务 PGW-C。搜索会传递到每个实例，因此运营商可以在不知道哪个 PGW-C 锚定他们的情况下找到订阅者；打开一行会转到其自身实例的会话。无法访问的实例在表上方命名，因此短列表不会被误认为是安静的网络。

IP 池

运营商从中分配 UE 地址的 PGW-C 的 IP 池，每个池显示其 大小、分配 计数和 利用率。打开一个池会列出单个分配的地址。在这里，您可以确认池没有耗尽（耗尽的池是会话建立失败的常见原因），并查看哪个订阅者持有给定地址。

UPF 对等体

PGW-C 通过 Sx/PFCP 控制的用户平面 (UPF) 对等体，每个显示其 IP 地址 和 PFCP 关联状态。打开一个对等体显示其详细信息。在这里，您可以确认承载每个会话用户平面的 PFCP 关联是否正常。

Diameter

PGW-C 与之通信的 Diameter 对等体（通过 **Gx** 与 **PCF/PCRF** 进行策略和通过 **Gy** 与 **OCS** 进行在线计费），每个都有其 主机名 和 连接状态。打开一个对等体显示其详细信息。当会话被拒绝或限流时，在这里您可以确认策略和计费路径是否正常。

历史

可搜索的分页日志，记录会话生命周期 事件：创建、修改、删除、切换和失败。您可以按类型过滤事件，并通过 IMSI、MSISDN、IP 地址或 TEID 搜索它们。在这里，您可以重建特定订阅者会话随时间的变化，包括失败情况。

拓扑

PGW-C 及其合作邻居的地图：它为其锚定会话的 SGW、它控制的 UPF 以及其 Diameter 对等体。它提供了一个图像视图，显示节点连接的信令和用户平面邻居。

UPF 选择

决定新会话放置在哪个 UPF 的规则，以及每个候选 UPF 的当前 健康状态 和 PGW-C 返回给 UE 的 PCO（协议配置选项）配置。在这里，您可以确认会话为何落在特定 UPF 上，并检查所有候选者是否健康。

UE 搜索

通过 IMSI、MSISDN 或 IP 地址 直接查找单个订阅者，返回该 UE 在 PGW-C 上的信息。这是查找单个订阅者会话的最快方式，而无需滚动完整的会话列表。

计费

每个活动会话的实时 在线计费 (Gy/OCS) 状态，每行以 IMSI 和 MSISDN 为键，并可通过任一项搜索。每个会话一目了然地显示 Gy 在线计费是否开启（包括其 会话 ID、OCS 主机 和 域），是否也在运行 离线 (Gz) 计费，以及 OCS 是否将订阅者推入 围墙花园 重定向。打开会话会展开其完整计费详细信息：每个 URR 授予 配额与 使用 流量（上行、下行和总字节），OCS 设置的 最终单位操作 以防止信用耗尽，离线 (Gz) 计数器，以及任何重定向目标。这是您读取订阅者实时信用控制状态的方式：他们是否有信用，他们消耗了多少授予额度，以及他们为何可能被限流或重定向。

紧急情况：暂停在线计费。在选项卡顶部有一个节点级开关，可以暂停整个 PGW-C 的在线计费。当 OCS 无法响应且订阅者否则将失去服务时，请使用它。

当开关处于激活状态时，PGW-C 在附加时不会发送 CCR-I，在实时会话中不会发送 CCR-U。它释放围墙花园并解锁受限承载，因此流量在没有 OCS 授权的情况下被传输。离线计费不受影响：使用仍然记录到 CDR 中，并可以稍后进行计费。

要激活开关，请提供两项内容：

字段	必需	描述
暂停时间	是	开关保持激活的时间。时间到后会自动解除激活。节点设置其接受的最长值。
原因	是	暂停计费的原因。会记录在覆盖中。
激活者	否	谁激活了它。默认为您的地址。
在分离时发送 Gy CCR-T	否	默认关闭。打开以报告 OCS 从未授权的使用。

给出真实的理由。 原因和操作员会被记录，并且它们的有效期超过激活开关的班次。

面板显示开关激活时剩余的时间。按 恢复计费 立即解除激活。开关在时间到期时也会自动解除激活，这可以防止遗忘的覆盖变成永久免费的服务。

CDRs

PGW-C 为计费写入的离线 ���费记录：每个会话 开始、中间 和 停止 事件一行，最新的在前，并可通过 **IMSI** 或 **MSISDN** 进行过滤。每条记录包含订阅者的 **IMSI**、**MSISDN** 和 **IMEI**，**APN** 和 **QCI**，将会话记录关联在一起的 计费 **ID**，该时间段内计算的 上行/下行字节，**S-GW**、**PGW** 和 **UE** 的 IP 地址，以及读取记录的 源文件。在这里，您可以将订阅者的数据使用情况与运营商计费的离线 (Gz) 进行对账，并追踪特定会话落入的记录文件。

Gy 测试

一个运营商工具，向 OCS 发出 **Gy** 信用控制请求 以验证在线计费路径的端到端。您提供一个 **IMSI**（可选提供 MSISDN 和请求/使用的字节计数）并选择请求类型。使用 初始 **(CCR-I)** 来打开会话并请求单位，更新 **(CCR-U)** 来报告使用情况并请求更多，或 终止 **(CCR-T)** 来报告最终使用情况并关闭它。然后发送。PGW-C 默认设置计费组、服务上下文 ID 和授权应用 ID。解析后的 信用控制响应 会在同一屏幕上返回。与其他选项卡不同，这个选项卡 在载时不会获取任何内容：这是一个提交的表单。当在线计费出现问题时，这是证明 OCS 可达并授予信用的最快方式。

P-CSCF 监控

P-CSCF 发现监控的状态和指标。PGW-C 在 PDN 设置期间向 VoLTE 设备返回 P-CSCF 地址，此选项卡确认发现是否正常，以 IMS 注册可以继续。

日志

日志 选项卡跟踪 PGW-C 的实时日志输出，以在不离开 OmniWeb 的情况下排除单个节点的故障（会话建立失败、PFCP 和 Diameter 错误）。

监控

PGW-C 的会话计数趋势、吞吐量和其他时间序列以 Grafana 仪表板的形式呈现，从元素页面访问。OmniWeb 不会本地重复这些图表。

相关

- **SGW-C** 是通过 **S5/S8** 进行控制的对等体；它锚定 PGW-C 连接到 PDN 的接入侧承载。

UPF 是 PGW-C 通过 Sx/PFCP 选择和控制的用户平面。 PCF/PCRF 通过 Gx 提供策略和 QoS。
CHF/OCS 通过 Gy 执行在线计费；PGW-C 还会生成离线计费的 CDR。

RAN 模拟器

RAN 模拟器让您在没有物理无线电或手机的情况下测试实时核心网络。它建立虚拟 **eNodeB** 和 **UE**，与 MME 进行真实的 S1AP/NAS 通信，并通过 GTP-U 与网关通信，因此您可以驱动附加、数据会话、IMS 注册、短信和通话。可以将其用于功能测试、负载测试或重现现场场景，所有操作均可通过 OmniWeb 进行。

← 操作指南

它是什么

模拟器与其目标核心并行运行。在 OmniWeb 中，它作为独立的 **RAN** 模拟器区域出现（网络地图、eNodeB、UE、IMS、负载测试、场景计划）。由于模拟的 UE 行为类似于设备，因此其 UE 也出现在 测试设备 ���，您可以从与真实手机相同的地方驱动它们。

默认情况下，它以 没有 **eNodeB** 开始。您可以精确设置所需的拓扑。

eNodeB

启动 eNodeB 将其连接到 MME（S1 设置）。一个 eNB 可以连接到 多个 **MME**（MME 池）。网络地图显示 eNB 归属的所有 MME 的完整集合。

启动是一次性操作：OmniWeb 请求模拟器启动 eNB，然后返回；S1 链路在后台建立（请查看网络地图 / eNodeB 列表以确认它已启动）。

断开 eNodeB

您可以通过两种方式关闭 eNB，这模拟了不同的现实世界事件：

操作	模拟	对 UE 的影响
干净的 S1 断开	有序的 eNB 关闭 / S1 重置	UE 被干净释放并存活。当链路可用时，它们会重新附加
掉链路	eNB 突然失去其 S1（光纤切断、断电）	S1 关联被中止；UE 存活，在 eNB 消失后重新附加，而不是被拆除

关键是，关闭 eNB 并不会销毁其 UE。UE 会持续存在并重新附加，因此您可以模拟传输中断，而无需重建您的用户群。

UE

每个模拟的 UE 都有一个可以直接驱动的生命周期：

- 附□ / 分离：加入或离开网络。
- 发送到空闲：移动到 ECM-IDLE（就像真实 UE 在活动之间所做的那样）。分页或新活动会将其带回。
- 超出覆盖范围：无线电的 □□□ 丢失（UE 在没有信令的情况下掉线），以测试核心如何处理简单消失的 UE。附加会将其带回覆盖范围。

对于每个 UE，模拟器显示其附加的 服务 **MME**：MME 组 ID 和 MME 代码（从 UE 的 GUTI 解码）。因此，在池化部署中，您可以看到哪个 MME 接管了每个用户。

IMS 注册与位置

模拟的 UE 可以注册到 IMS 并发送短信/通话。当它注册时，它包括其 小区位置（`P-Access-Network-Info`，带有其服务小区的 `utran-cell-id-3gpp`），与真实 UE 完全相同。因此，S-CSCF 的第三方 REGISTER 将该位置传播到 SMSc、TAS 和其他应用服务器。这使您能够测试位置依赖的 IMS 行为，从头到尾而无需真实无线电。

从设备驱动 UE

由于模拟的 UE 只是另一种设备，它在 测试设备 中显示为标记为模拟器的设备，并可以过滤到那里。无论您是从 RAN 模拟器的网络地图还是从设备群中打开 UE，您都使用 相同的 **UE** 控制面板。这是附加/分离、空闲、驱动超出覆盖范围、注册到 IMS、发送短信或拨打电话以及查看操作日志的一个地方。

□□□□□□□□ RAN □□□ UE□□□□□□□□□□□□□□□□□□

计划场景

场景 是一个保存的测试配方：一系列命名的 UE 操作（附加、空闲、唤醒、IMS 注册、通话、短信、切换、分离），模拟器将在核心上执行。模拟器提供了一组预设库，按类别分组（例如附加生命周期、VoLTE 和负面拒绝案例）。可以从负载测试视图中运行一次场景，或在重复计划上运行以持续监控核心。

场景计划 页面（侧边栏：负载测试 → 场景计划）管理重复运行。对于每个计划，您选择一个场景以及运行频率。OmniWeb 记录每次运行的通过或失败结果，并将其导出到 Prometheus，以□您可以对此进行警报和绘图��

运行是 串行化 的。OmniWeb 一次运行一个计划场景，因为一个场景可以启动多个 UE，并对核心施加真实负载。如果在下一个计划到期时运行仍处于活动状态，OmniWeb 将等待并在下一个空闲周期启动它。使用 立即运行 按钮在保存的计划上立即启动。

计划参数

字段	类型	必需	默认	描述
名称	字符串	是	-	计划的唯一标签。也是导出指标上的 `schedule` 标签。
场景	字符串	是	-	要运行的预设场景。选择器按类别分组场景。
每隔（秒）	整数	否	3600	场景的运行频率，以秒为单位。最小 60。
UE 数量	整数	否	100	场景运行的用户数量。
RPS	数字	否	10	每秒目标新场景数量。
并发	整数	否	50	同时在飞行中的最大场景数量。
APN	列表	否	场景默认	要附加的 APN，以逗号分隔的列表。覆盖场景默认值。

通过和失���

当模拟器报告每个断言都通过且没有用户场景中止时，计划运行 通过。如果任何断言失败或任何场景中止，则运行 失败。如果场景没有断言，只要没有场景中止，就会通过。如果 OmniWeb 无法启动运行，或运行未能按时完成，OmniWeb 将该运行记录为 错误。

该页面显示一个 最近运行 表，包含结果、断言计数、中止场景数量和每次运行的持续时间。

指标

OmniWeb 在 `/api/loadtest/ran-metrics` 中以 Prometheus 格式公开每个计划的最新结果。Prometheus 将其作为 `ransim_scenarios` 作业抓取，监控角色会自动配置。

指标：`ransim_scenario_pass` 类型：Gauge 描述：最近一次计划运行的结果：`1` 表示通过，`0` 表示未通过 标签：

- `schedule`：计划名称
- `scenario`：运行的场景 ID
- `category`：场景类别
- `status`：运行结果（`passed`、`failed` 或 `error`）

伴随的计量表共享相同的标签：

指标	描述
`ransim_scenario_duration_ms`	上次运行的持续时间，以毫秒为单位
`ransim_scenario_assertions_passed`	上次运行中通过的断言
`ransim_scenario_assertions_failed`	上次运行中失败的断言
`ransim_scenario_scenarios_aborted`	上次运行中中止的用户场景
`ransim_scenario_last_run_timestamp`	上次运行的 Unix 时间

示例查询：

```
# 最近一次运行未通过的场景
ransim_scenario_pass == 0

# 所有计划场景中的总断言失败
sum(ransim_scenario_assertions_failed)

# 在过去两个小时内未运行的计划
time() - ransim_scenario_last_run_timestamp > 7200
```

Grafana 仪表板

监控角色提供了一个 **RAN** 模拟器场景 仪表板（Grafana 文件夹 **RAN**）。它读取上述指标并显示通过或失败的时间线、每个计划的最新结果、断言失败、场景新鲜度和运行持续时间。在顶部按类别、场景或计划进行过滤。请参见 Grafana。

典型用途

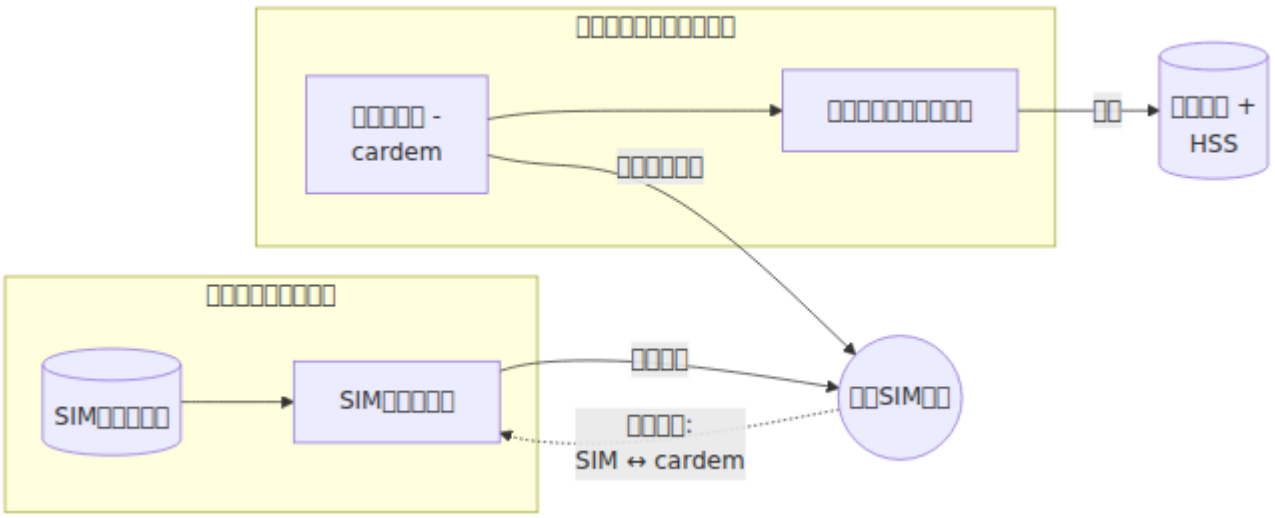
- 功能测试：启动一个 eNB 和一个 UE，附加，建立数据会话，注册到 IMS，发送短信，然后确认每个核心元素的行为。
- 负载测试：启动多个 UE 以对核心生成附加/会话/IMS 负载（请参见负载测试视图）。
- 场景重现：模拟中断（掉链路、超出覆盖范围）和池化 MME 行为，以重现和诊断现场问题。
- 持续监控：安排场景在定时器上运行，并对通过或失败指标进行警报（请参见 计划场景）。

相关

- 测试设备：真实手机和模拟 UE，从一个地方驱动。
- 会话跟踪：关联模拟器生成的信令。

□□SIM□□□SIM

OmniWeb□□□



SIM OmniWeb SIM

SIM	SIM
cardem	USB SIM
	“SIM cardem”
cardem	cardem SIM
SIM	SIM OmniWeb cardem SIM

SIM□□□□□□□□□

SIM□□□□□□□□□

远程**SIM**：将**SIM**连接到**cardem**

远程**SIM**页面是您将SIM绑定到cardem的地方。绑定跨代理和站点工作：SIM可以在一个位置的读取器中，而cardem/调制解调器在另一个位置。

步骤

1. 在持有读取器的代理上启动**SIM**银行（启动**bankd**）。这将发布其读取器插槽。
2. 启动**cardem**客户端以使用您想要的卡片仿真器（启动客户端）。这将绑定cardem，以□可以将SIM映射到它。
3. 在连接**SIM**下，选择一个已发布的插槽并选择要绑定的cardem。映射被创建并在活动映射下显示为**ACTIVE**。
4. cardem现在将该SIM呈现给其调制解调器。重置调制解调器（参见cardem控制台），以□它读取新呈现的SIM并连接。

全局重置会拆除所有映射并将每个cardem返回到空闲状态。使用它来从混乱的测试台中恢复。

字段（活动映射）	意义
状态	一旦cardem呈现SIM，则为`ACTIVE`。
SIM（银行/插槽）	卡片所在的代理的银行和插槽。
ICCID	呈现的SIM。
Cardem（客户端/插槽）	哪个cardem（以及哪个代理）正在呈现它。
由	创建映射的操作员。

Cardem控制台

在设备中，OmniWeb将卡片仿真器显示为其自己的设备类型（`ngff-cardem`），与调制解调器和手机并排。它从不作为手机打开。OmniWeb会简单地标记未知设备类型，而不是猜测它们。

打开cardem以获取仿真器及其调制解调器的专用控制台。

控制	功能
启动客户端	将cardem绑定为远程SIM客户端，以□可以将SIM映射到它。
重置调制解调器	重新呈现仿真卡，这使调制解调器重新读取SIM并重新运行附加。这是您在不接触硬件的情况下“更换SIM”的方法。
远程**SIM**	连接或断开呈现给此cardem的远程SIM。

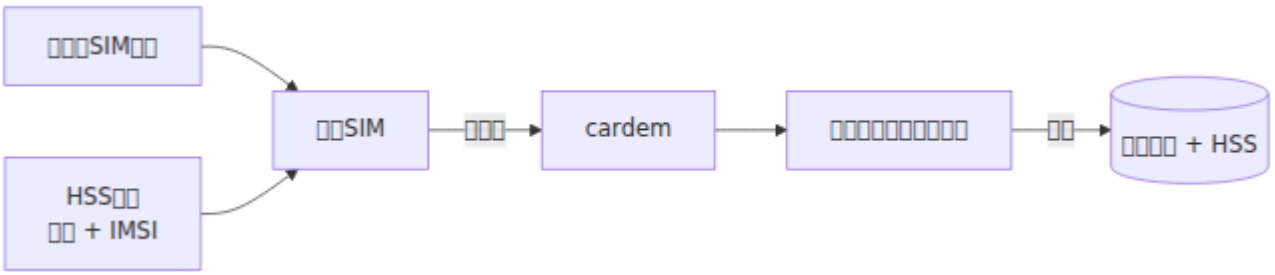
SIM源面板诚实地说明什么可用，什么不可用：cardem向调制解调器提供一个□□SIM。控制台尚未提供呈现□□卡片的选项，该卡片插入在仿真器板上。控制台会这样说明，而不是显示一个无效的控制。

虚拟**SIM**：没有物理卡的用户

虚拟**SIM**允许调制解调器作为您没有**SIM**的用户进行附加。OmniWeb从您已经拥有的两样东西构建它：

1. 一个基础**SIM**图像：真实卡片文件结构的保存快照（任何兼容的测试SIM都可以作为基础；参见**SIM**图像）。
2. 用户的身份和**HSS**中的密钥：已经在网络中配置的用户的IMSI和认证密钥。

OmniWeb将它们组合成一个软件卡。该卡从图像中回答调制解调器的文件读取，并使用HSS密钥回答网络的认证挑战。它覆盖所选用户的IMSI。通过cardem，调制解调器无法分辨它与塑料SIM的区别：它读取IMSI，运行认证，并连接到实时网络。



何时使用它

- 在没有其物理SIM来源的情况下，重现特定用户的漫游或附加行为。
- 针对一个调制解调器，逐个测试多个已配置的用户。
- 测试仅存在于HSS中的配置（新配置、发货前）。

它证明了什么。测试台上的调制解调器已作为HSS用户连接到实时网络（`已注册，主网络`），而没有物理SIM存在。它读取了该用户的IMSI，并完全通过虚拟卡完成了网络的认证。

> 一个专用的虚拟**SIM**读取器元素是此功能的下一步。在那里，您可以“加载”来自所选图像和用户的虚拟SIM，并像其他读取器插槽一样呈现它。今天，OmniWeb通过上述相同的远程SIM代理和cardem路径连接虚拟卡。

在漫游测试书中使用**SIM**

漫游测试书（GSMA IR.38 / IR.48）可以在运行过程中驱动SIM呈现。在测试书的运行测试面板中，您可以选择：

- 一个**SIM**（按**ICCID / IMSI**）：通过身份跟踪，其当前读取器在运行时自动解析，以及
- 一个**Cardem**调制解调器：SIM被仿真到的cardem。

将**SIM**呈现给**cardem**在您测试之前建立映射。开始：运行所有测试首先呈现SIM（当选择了SIM和cardem时），然后读取IMSI并运行数据用例。如果SIM当前不在读取器中，或者cardem的客户端未运行，面板会准确说明原因。它不会在错误的卡上静默运行。

请参见测试设备和测试书文档以获取IR.38流程的其余部分。

故障排除

SIM未出现在银行中

症状：读取器已插入，但没有插槽（或空插槽）显示。

可能的原因及解决方案：

- 卡片未就位，或读取器/卡片配对无法为卡片供电。插槽显示卡片存在或空。重新插入SIM。
- 读取器刚刚插入。OmniWeb在热插拔时重新扫描读取器，但您可以通过代理组上的重新扫描强制执行。

连接**SIM**后调制解调器未附

可能的原因及解决方案：

- 调制解调器尚未重新读取SIM。使用cardem控制台上的重置调制解调器重新呈现卡片。
- 映射不是**ACTIVE**。在远程SIM页面的活动映射下确认SIM是否绑定到正确的cardem。
- 用户在服务网络的HSS中未配置（或被禁止）。

读取器上的“卡片存在（不可读）”

症状：检测到卡片，但无法读取其身份。

解决方案：该读取器无法与该卡片通信（通常是廉价读取器上的电压/协议不匹配）。将SIM移动到银行中的其他读取器。

虚拟**SIM**：调制解调器读取卡片但未附

可能的原因及解决方案：

- 选择的用户必须在服务网络的HSS中启用并完全配置（带有数据配置文件）。
- 基础图像必须来自兼容的卡片类型。如果初始化停滞，请从已知良好的SIM重新捕获基础图像。

SCEF: 服务能力暴露功能

SCEF（服务能力暴露功能），Omnitouch 的 **OmniSCEF**，是网络的 物联网北向网关。它通过在 TS 29.122 中定义的 **3GPP T8** RESTful API 向外部应用服务器暴露核心网络能力，以□机器对机器平台可以订阅有关一组设备的事件，并与它们交换少量数据，而无需使用 Diameter 或 GTP。它前置了两类服务。监控事件请求网络在设备可达、失去连接、位置变化等情况下进行报告。**非 IP 数据传输（NIDD）**通过控制平面与受限的 NB-IoT 设备之间传输小的非 IP 负载。内部 SCEF 通过 **T6a** Diameter 接口（TS 29.128）与 MME 连接。OmniWeb 显示其状态、应用服务器创建的 T8 资源以及它正在承载的实时 NIDD 会话。

← 操作指南

仪表板是一个每个实例的元素页面，可以通过侧边栏访问，当 SCEF 在站点的库存中□□□行时。所有流量都通过 OmniWeb 后端代理到 SCEF 的 T8 API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接提供上下文帮助。页面组织成多个选项卡。

SCS/AS ID 模型

每个 T8 资源（每个监控订阅和每个 NIDD 配置）都是 作用于 **SCS/AS** 身份，即应用服务器注册的身份（□□□□□□□ / □□□□□）。T8 API 没有列举正在使用的 **SCS/AS ID** 的端点，因此 OmniWeb 无法为您发现它们：操作员 在页面上设置 **SCS/AS ID**，并且 OmniWeb 会 跨 **SCEF** 选项卡记住它，这样您只需设置一次，它就会从概览到监控事件再到 NIDD 进行传递。在设置 SCS/AS ID 之前，作用域选项卡会提示输入一个，而不是显示空列表。资源存在于您必须命名的身份下。输入应用服务器的 SCS/AS ID（例如 `iot-platform-01@omnitouch`），以□与该平台的订阅和配置进行交互。

概览

SCEF 本身的单屏健康读取：其 状态、产品 名称、许可证 状态和用于 T6a 连接 MME 的 Diameter 主机。其下是 应用上下文（上述描述的 SCS/AS ID 字段），一旦设置了 SCS/AS ID，当前为该应用服务器持有的 监控订阅 和 NIDD 配置 的计数。这是确认 SCEF 是否正常运行以及给定平台承载量的最快方式。监控和统计仪表板作为 Grafana 嵌入提供，可以从同一页面访问。

监控事件

应用服务器为当前 SCS/AS ID 创建的 监控事件订阅。每个订阅请求网络报告一类事件并将其 POST 到应用服务器；每行显示：

事件类型：监控类型，例如 UE 可达性、连接丢失、位置报告、DDN 失败后的可用性、漫游状态 或 区域内 UE 数量。
目标：订阅监控的设备或组，通过 外部 ID、MSISDN 或整个车队的 外部组 ID 进行识别。
通知目标：SCEF POST 每个事件报告的 回调 URL。它必须是应用服务器公开的绝对 http(s) 地址。
最大报告 和对于可达性订阅的 可达性类型（SMS 或 DATA）。连同监控的 持续时间/到期，这些限制了发送的事件数量及订阅的有效
期。

可以创建、编辑和删除订阅；删除一个订阅将停止应用服务器接收这些事件报告。

NIDD

NIDD 配置是应用服务器为当前 SCS/AS ID 创建的非 IP 数据传输绑定。配置授权与设备通过控制平面交换小的非 IP 负载。每行显示：

- 目标：通过 外部 **ID**、**MSISDN** 或 外部组 **ID** 识别的设备。
- **DNN / APN**：NIDD PDN 连接使用的数据网络名称（APN）（例如 `nidd.iot.omnitouch`）。
- 状态：`ACTIVE`，或终止状态（`TERMINATED`，`TERMINATED_UE_NOT_AUTHORIZED`）。
- 最大数据包：非 IP 负载可以达到的 最大数据包大小（以字节为单位）。
- **RDS**：是否启用 可靠数据服务。它在非 IP 链路上添加了一个轻量级的确认传输，具有源/目标端口。

配置还携带一个 **PDN** 建立选项，决定在设备没有 NIDD PDN 连接时下行数据到达时会发生什么：等待 **UE** 建立连接、指示错误，或通过分页设备 建立 **PDN** 连接。

下行数据传输

从 NIDD 配置中，您可以 将下行负载传送到设备。将负载作为文本输入。SCEF 在通过 NIDD 发送之前会对其进行 base64 编码，每次传送可以携带一个 优先级 和一个 最大延迟。最近的传送列出其 传送状态：SUCCESS、BUFFERING、SENDING，或某个失败原因，例如 FAILURE_UE_NOT_REACHABLE。您可以取消排队或缓冲的传送。这是平台向没有 IP 地址的受限设备推送命令或固件更新的方式。

NIDD 会话

实时 **T6a NIDD** 会话是 SCEF 当前与 MME 持有的活动非 IP 数据传输绑定。与 NIDD 配置不同，后者是作用于 SCS/AS ID 的 T8 资源，这些是 服务器全局运行时状态：它们是 只读 的，并且不按 SCS/AS ID 进行作用域，因此此选项卡显示每个活动会话，而不管您正在查看哪个应用上下文。每行显示设备的 **IMSI**、NIDD PDN 连接使用的 **APN**、**EPS** 承载标识（**EBI**）、会话 状态（`ACTIVE`、`IDLE`）、**T6a** 会话 **ID**、服务 **MME** 主机 和 **MME** 领域，以及会话设置时使用的 配置 **ID**。这□□□查看哪些设备实际上具有实时非 IP 绑定以及通过哪个 MME 的最快方式。

日志

日志选项卡跟踪 SCEF 的实时日志输出，以□在不离开 OmniWeb 的情况下进行单实例故障排除。

监控仪表板

SCEF 的 T8 请求率、事件报告吞吐量和 NIDD 传输计数以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

- **MME**：SCEF 通过 **T6a** 与其连接，以设置 NIDD PDN 连接并收集此处报告的监控事件。每个会话使用的 MME 主机和领域在 NIDD 会话选项卡上显示。
- **HSS**：持有 SCEF 的监控和 NIDD 服务所依赖的订阅数据（外部标识符、NIDD 授权）。
- **PGW-C / SMF** 和 **UPF**：承载普通 IP 数据平面。NIDD 刻意绕过它们，以□通过控制平面传输小的非 IP 负载。
- 操作指南：返回元素索引。

SGW-C: 服务网关（控制平面）
SGW-C 是 EPC 服务网关的控制平面部分。它在接入网络和数据包网关之间锚定每个订阅者的承载：它终止与 MME 的 S11（会话和承载信令）、与 PGW‑C 的 S5/S8（PDN 连接），并编程用户平面（SGW‑U），该平面通过 S1‑U 将流量转发到 eNodeB。简而言之，它是持有每个附加订阅者的实时承载状态的节点，并保持 MME、PGW 和用户平面步调一致。OmniWeb 显示 SGW‑C 的实时会话、会话计数和日志；长期趋势（吞吐量、会话增长）可在同一页面的 Grafana 仪表板上查看。

← 操作指南

SGW‑C 是一个每实例元素页面，通过侧边栏在站点的库存中访问。当部署多个实例时，它还提供聚合状态的舰队视图。所有流量通过 OmniWeb 后端代理到 SGW‑C 的 API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织为多个选项卡。

概述

单屏健康读取：SGW‑C 的 API 状态、活动会话计数，以及从实时会话得出的摘要：唯一 MME 的数量（不同的 S11 对等体）、唯一 PGW 的数量（不同的 S5/S8 对等体）和当前锚定的 总承载。这是确认 SGW‑C 是否正常、它持有多少会话以及它正在与多少 MME 和 PGW 工作的最快方式。

会话

每个锚定会话，每行以订阅者 **IMSI** 和 **MSISDN** 为键，显示其连接状态。打开会话可查看其完整的承载状态：**S11** 控制端点（MME 侧和 SGW 侧 F-TEID）、每个 **PDN** 连接（APN、默认承载以及与 PGW 的 S5/S8 控制 F-TEID）以及每个承载（EBI、S1-U 和 S5/S8 用户平面 F-TEID 及其 QoS）。在这里，您可以确认特定订阅者的承载是否已建立，并查看哪个 MME 和 PGW 正在为其服务。

当部署多个 SGW-C 时，舰队视图中的同一选项卡在一个表中列出所有 SGW-C 的每个会话，服务 SGW-C 显示在每行旁边，因此操作员可以在不知道哪个 SGW-C 正在锚定他们的情况下找到订阅者。打开一行将转到该会话的独立实例。无法访问的实例在表上方命名，当一个实例持有的会话超过组合视图提取的行限制时，单实例行限制也会显示在上方。

日志

日志选项卡跟踪 SGW-C 的实时日志输出，以□在不离开 OmniWeb 的情况下进行单个网关的故障排除。

监控仪表板

SGW-C 的吞吐量、会话计数趋势和其他时间序列以 Grafana 仪表板的形式呈现，从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

MME：通过 S11 的控制对等体；它驱动 SGW‑C 上的会话和承载设置。 PGW‑C通过S5/S8锚定 PDN 连接。
SGW‑U / UPF 是 SGW‑C 编程以在 S1‑U 上转发流量的用户平面。

SIM卡工具：文件系统、APDU和eSIM

OmniWeb不仅仅是发现和展示SIM卡。它为您提供了一套低级卡工具，可以通过任何代理上的任何读卡器直接与卡片进行通信。您可以浏览和编辑其文件系统，手动发送原始APDU，查看远程SIM会话的实时APDU跟踪，并管理eUICC上的eSIM配置文件。本页面是这些工具的操作指南。

← 操作指南

这些工具与现有的SIM功能并排放置并重用它们。从这里开始了解更大的图景：

- **SIM**银行：库存：每个代理中哪些SIM卡在何处。此页面上的每个工具都针对该库存中的一个读卡器，SIM银行的每个插槽操作直接链接到它们。
- **SIM**图像（**SAIP**配置包）：如何将读取的文件系统保存为可移植图像，以及如何浏览或比较保存的图像。
- 远程**SIM**和虚拟**SIM**：如何通过卡片模拟器通过网络将SIM（真实或虚拟）呈现给调制解调器。
- **OTA SIM**管理：相同的文件级编辑，但它通过安全的（03.48 / SCP80）数据包通过空中访问卡片，而不是本地读卡器。

下面的四个工具在侧边栏的**SIMs**组下。

一次一个读卡器，一个消费者

一次只能有一个东西驱动物理PC/SC读卡器。此页面上的工具可能需要一个被其他东西占用的读卡器：另一个读取它的操作员，或一个将其呈现给调制解调器的实时远程SIM银行会话。该工具然后显示谁持有它以及为什么，并提供明确的接管选项。没有静默踢出：当您接管时，OmniWeb会取消其他会话（对于银行会话，断开该SIM↔cardem链接）。编辑或发送是一个控制操作，受SIM银行控制权限的限制。没有它，您可以查看读卡器，但无法驱动卡片。

SIM文件系统浏览器

选择一个读卡器并读取其卡片的整个文件树：MF、DF.GSM / DF.TELECOM、ADF.USIM和ADF.ISIM及其所有EF，每个可读文件解码为命名字段。完整读取会接触许多文件，因此进度条会��示读取进度（“读取X个文件中的Y个：EF....”）。

- 按文件代码（**FID**）、短名称或描述搜索树。搜索“紧急呼叫代码”会找到EF.ECC，而不仅仅是`6FB7`。
- **PIN**保护的文件会被标记，永远不会被读取：浏览器不会消耗PIN重试次数。
- 编辑**EF**（需要控制权限）：详细面板提供一个基于模式的表单（解码字段，类型），如果可用，回退为原始十六进制。写入是破坏性的，并会要求确认。如果EF需要身份验证，请先使用验证**CHV/ADM**。它会测试PIN/ADM密钥与卡片的匹配（报告剩余尝试次数，并且永远不会消耗最后一次重试）。一旦验证通过，浏览器将重用它进行写入。SIM密钥存储会自动提供卡片的ICCID的保存密钥。
- 保存图像快照解码的树作为命名的SIM图像。与图像比较将实时卡与保存的卡进行比较。保存的图像打开图像库。您还可以将保存的图像□□树（`?image=<id>`）打开，以浏览您不再在读卡器中的卡片。

读卡器必须是空闲的（未被远程SIM会话占用），否则您可以按照上述方式接管。

APDU终端

APDU终端是卡片的手动控制台：输入一个原始APDU的十六进制，将其发送到所选读卡器中���卡片，并查看解码的响应。解码显示命令的INS名称、状态字及其含义，以及任何响应数据的扩展解释（FCP TLV树、解码的EF字段或AUTHENTICATE结果）。预设按钮（SELECT MF、STATUS、READ BINARY、GET RESPONSE等）填充常见命令。输入对空格/冒号宽容并经过验证（完整字节，至少CLA/INS/P1/P2）。

两种模式：

模式	行为	用途
单次	每个APDU是自包含的；卡片在发送之间重置为MF。	一次性探测。
会话	打开一个持久的、独占的卡片会话，以□状态（选择、身份验证）在APDU之间持续：一个SELECT然后一个READ BINARY有效，而一个VERIFY与后续的UPDATE共享其身份验证。读卡器保持占用状态，直到您关闭会话。	有状态序列。

SIM银行的每个插槽**APDU**操作直接链接到此，预先选择了该确切的读卡器。适用相同的一消费者/接管规则。

APDU日志

当终端是您驱动一张卡片时，**APDU**日志是一个被动的实时跟踪，记录在调制解调器与（远程）**SIM**之间通过远程SIM/卡片模拟链交换的命令/响应APDU。打开捕获，它会跟踪交换：每一行将`modem→card`命令与其解码的状态字配对，以及与终端相同的��应解码（FCP树、EF字段、ATR/复位事件）。您可以暂停视图（捕获继续运行）、按命令/十六进制/SW过滤，并自动滚动。

使用它来查看调制解调器在附加或运行IR.38测试时实际上向SIM询问了什么：选择了哪些文件，哪里VERIFY失败，AUTHENTICATE是否成功。您不必对调制解调器进行仪器化。它自然与远程SIM配对，后者设置了调制解调器↔SIM链接，日志随后进行跟踪。

---

eSIM（LPA）

eSIM工具通过代理的本地配置助手（**LPA**）管理**eUICC**。eUICC是您读卡器中的一个物理eSIM芯片。它持有多个配置文件，但一次只能激活一个。

- **eUICC**卡片：显示芯片的**EID**。
- 已安装的配置文件：卡片上的每个配置文件：其状态（激活/禁用）、昵称、提供商、名称和ICCID。每个配置文件您可以启用（使其成为活动eSIM）、禁用、重命名（昵称）或删除。删除会将配置文件从eUICC中移除且不可逆，因此会先进行确认。
- 下载配置文件：从操作员的SM-DP+拉取新配置文件并安装到卡片上。使用完整的激活代码（`LPA:1$smdp.example.com$MATCHING-ID`）或拆分的**SM-DP+**地址 **+** 匹配**ID**，可选的确认代码。

这专门用于eSIM（eUICC）卡片。要进行经典SIM/UICC文件编辑，请使用上述文件系统浏览器。要远程编辑卡片，请使用OTA。

SIM工具包（STK）

SIM工具包客户端驱动SIM卡上的STK小程序。它向卡片发送终端配置文件，然后将每个主动命令呈现为交互式屏幕：菜单、文本显示、单键输入和文本输入。使用它来导航运营商驻留的服务、触发OTA配置流程或测试SIM驻留的小程序逻辑。

请参见**SIM工具包**获取完整的操作指南。

相关

SIM银行：这些工具所针对的读卡器/SIM库存。
SIM图像：保存、浏览和比较读取的文件系统。远程SIM和虚拟SIM：通过网络将SIM呈现给调制解调器（APDU日志跟踪的链接）。 OTA SIM管理：通过空中进行相同的文件编辑。
SIM工具包：与读卡器中卡片上的STK小程序进行交互。

SIM 图像：SAIP 配置文件包

SIM 图像是卡片整个文件系统的保存快照。OmniWeb 将每个图像存储为 **SAIP** 未保护配置文件包 **(UPP)**，采用 DER 编码。这是 eUICC 配置文件使用的相同可互操作格式，由 TCA *eUICC* [illegible] 定义。一个捕获的卡片变成一个可移植的 `.der` 文件，任何支持 SAIP 的工具都可以读取。

本页面是操作指南。它涵盖了如何捕获、导出、上传、浏览和比较 SIM 图像，以及如何使用保存的图像来支持一个 虚拟 SIM。SIM 银行 涵盖了实时读取器库存。

目录

- 为什么选择 SAIP UPP
- 架构概述
- 图像中包含什么
- 捕获图像
- 导出图像
- 上传图像
- 在资源管理器中浏览图像
- 比较两个图像
- 用图像支持虚拟 SIM
- 配置文件元素参考
- 故障排除

为什么选择 SAIP UPP

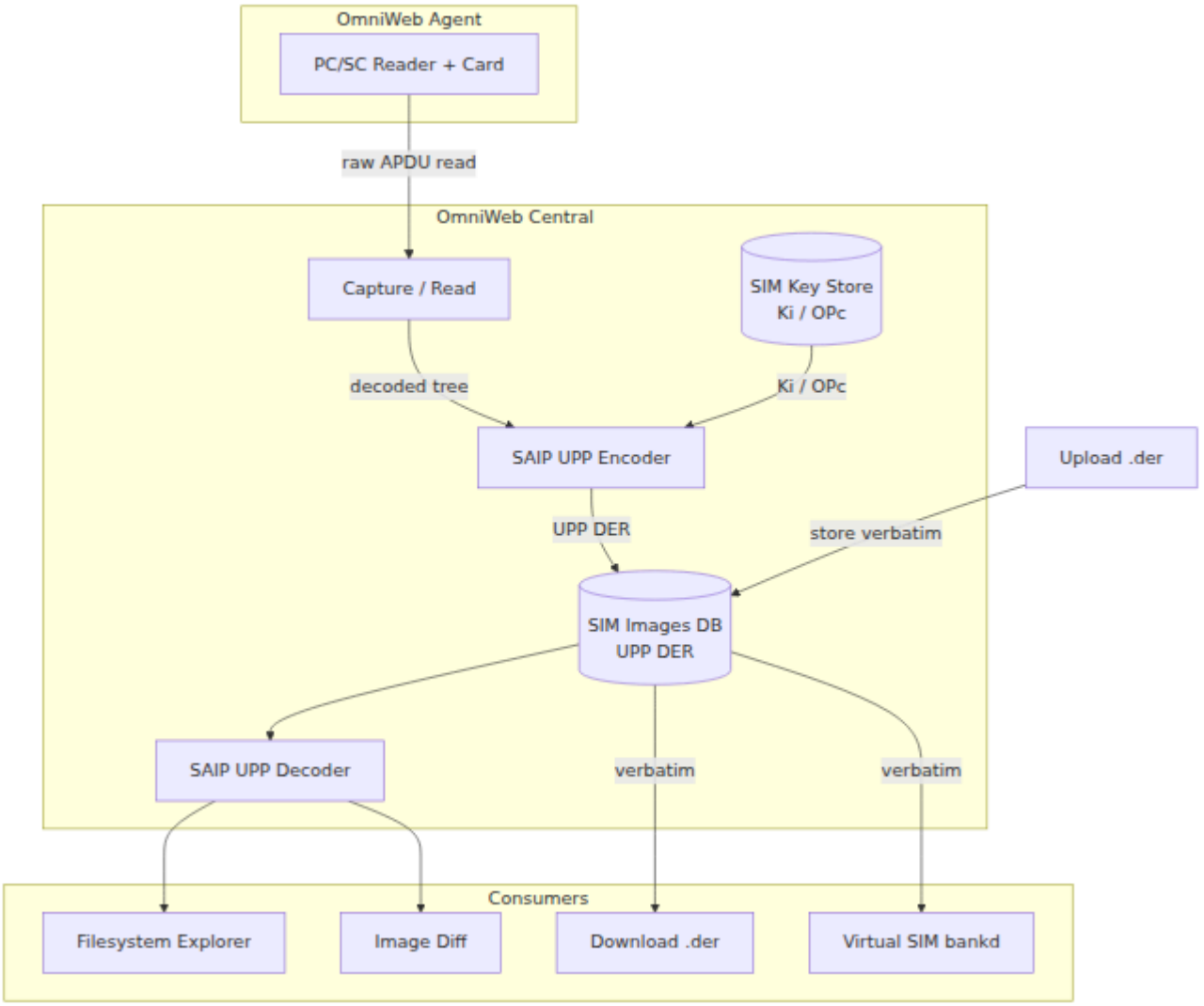
早期版本将 SIM 图像存储为仅用于比较的解码 JSON 树。该格式是 OmniWeb 私有的，任何外部工具都无法使用。

当 OmniWeb 将图像存储为 **SAIP UPP** 时，您将获得：

- 可移植性：导出的 `.der` 是标准配置文件包。它可以在 SAIP 配置文件验证器和任何符合 SAIP 的工具链中加载。
- 统一格式：操作员下载的相同 `.der` 是支持虚拟 SIM 的文件，也是文件系统资源管理器呈现的内容。没有第二个不同的表示。
- 重新配置：当卡片的认证密钥已知时（见 捕获图像），UPP 包含一个 `PE-AKAParameter` 元素，携带 Ki 和 OPc。该包描述的是一个完整的、可安装的配置文件，而不是只读转储。

该包是 DER 编码配置文件元素的原始串联。它 不是 加密的（它是一个未保护配置文件包）。请像对待任何包含 Ki/OPc 的文件一样小心处理导出的.der。请参见 故障排除。

架构概述



捕获读取卡片，编码器生成一个 UPP（如果可用，它会从 SIM 密钥存储中折叠 Ki/OPc），然后 OmniWeb 存储该包。每个消费者都从该单一存储包中读取。资源管理器和比较工具按需将其解码为树形结构。下载和虚拟 SIM 银行直接使用字节。

图像中包含什么

捕获的图像包含卡片的标准 MF / ADF.USIM 布局：

元素	**SAIP** 配置文件元素	内容
文件系统	`PE-GenericFileManagement`	每可达的 EF：其文件控制参数 (FCP) 和原始内容（透明 EFs）或每条记录（线性/循环 EFs）
身份	`PE-Header`	卡片的 ICCID
认证	`PE-AKAParameter`	用于 Milenage 的 Ki 和 OPc。仅在卡片的密钥在 **SIM** 密钥存储中时存在

文件是通过 `PE-GenericFileManagement` 创建的（每个 DF 一个操作组），而不是标准化的 SAIP 文件系统模板：卡片读取恢复原始字节，而不是配置文件创建者最初使用的模板，因此通用表示始终是准确的。

捕获图像

捕获可以通过 SIM 文件系统 资源管理器或 SIM 银行插槽操作进行：

1. 在资源管理器中读取卡片的文件系统。
2. 选择 保存图像 并给它一个标签。

解码的文件系统被编码为 UPP 并存储。如果存在一个针对卡片 ICCID 的 SIM 密钥存储 条目，并且同时具有 **Ki** 和 **OPc**，则这些密钥会写入 `PE-AKAParameter` 中，因此生成的包是完全可安装的。如果没有密钥存储条目，包仍然捕获完整的文件系统；仅认证元素被省略。

身份列（ICCID、IMSI、卡片类型、文件计数）是在捕获时从文件系统派生的，因此图像列表和比较头永远不需要重新解包。

导出图像

保存的图像列表中的每一行都有一个 下载 操作，原样提供存储的包，命名为 `UPP_<iccid>.der`。

下载的 `.der` 是标准 SAIP UPP，可以使用任何符合 SAIP 的配置文件工具进行检查。

工作原理：该文件是捕获（或上传）时存储的确切字节，下载时没有重新编码，因此往返下载与存储的内容字节完全相同。

上传图像

保存的图像页面有一个 上传 **.der** 操作，接受 SAIP UPP 文件并将其存储为新图像。使用它可以引入其他地方生成的配置文件：例如 GSMA TS.48 *□□ eUICC □□□□□□* 包，或由其他 SAIP 工具生成的 UPP。

在上传时，OmniWeb：

1. 验证文件以 SAIP 配置文件元素标签（上下文类构造标签：`A0`、`A1` 或 `B0`）开头。
2. 原样存储该包。
3. 解码 `PE-Header` 以填充 ICCID 列（如果存在）。

上传的图像是一个一流图像：它可以被下载、在资源管理器中浏览、比较、编辑，并用于支持一个虚拟 SIM，就像捕获的图像一样。

编辑图像

保存的图像是一个 文件，而不是卡片。编辑时仅更改存储的配置文件包，并 从不写入任何 **SIM**。从保存的图像列表中，编辑文件系统 操作以编辑模式打开 SIM 文件系统 资源管理器 (`?image=<id>&edit=1`)。不涉及读取器和代理卡访问。

您可以：

- 编辑文件内容：更改任何 EF 的字节。与实时卡片一样，编辑器提供基于模式的 表单、整个记录的 **JSON** 视图和 原始十六进制 逃生舱。没有 PIN/ADM 提示（文件没有访问条件需要满足）。
- 添□文件：在任何 DF/MF/ADF 下创建新的 EF（透明或记录结构）或 DF，并给出其 FID、结构和初始内容。
- 删除文件：删除任何 EF 或 DF（MF 根是整个图像，无法删除）。
- 重命名 图像（仅元数据）从列表中。

浏览器在您 保存图像（就地覆盖）或 另存为副本（分叉新图像并保持原始不变）之前保持更改。在保存时，OmniWeb 将编辑后的文件系统树重新编码为 SAIP UPP。它在已知时从 SIM 密钥存储 中折叠 Ki/OPc。它逐字保留树未建模的任何配置文件元素（PIN、PUK、安全域、模板），因此编辑从不丢失配置文件的其余部分。

表单 **/ JSON** 字段离线编辑。将 EF 解码为命名字段并重新编码使用与实时编辑器相同的文件模型，在任何在线代理上运行，但 不需要卡片：图像已经包含字节，因此代理只运行编解码器。如果没有代理在线，编辑将回退到原始十六进制，这不需要任何外部内容。

在资源管理器中浏览图像

每个保存的图像都有一个 在文件系统资源管理器中浏览 操作。它打开针对存储包的 SIM 文件系统 资源管理器。不需要物理卡和读取器。OmniWeb 将包解码回与资源管理器为实时卡呈现的相同文件系统树，因此您可以离线检查每个 EF 的原始内容。

比较两个图像

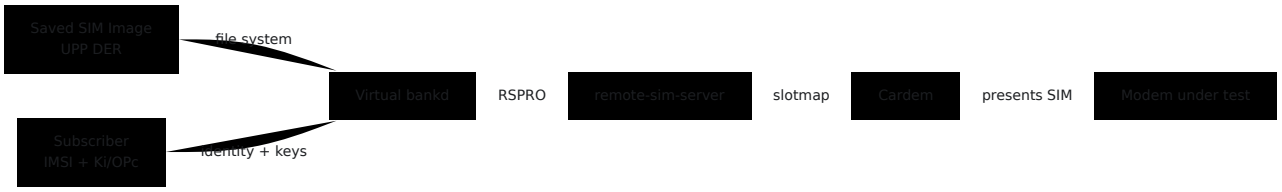
保存的图像页面允许您选择两个图像并进行比较。两个包被解���为文件系统树并按 EF 路径对齐，因此比较是逐文件的，无论捕获顺序如何：

状态	意义
`same`	EF 在两个图像中都存在且内容相同
`changed`	EF 在两个图像中都存在，内容不同
`only_a`	EF 仅存在于第一个图像中
`only_b`	EF 仅存在于第二个图像中

对于 **changed** EF，比较报告不同的字节范围（以及记录结构文件的每条记录增量），因此您可以确切看到哪些字节发生了变化：例如，个人化更改前后的测试 SIM，或两个运营商的 SIM 并排比较。

用图像支持虚拟 SIM

保存的图像可以在呈现 虚拟 SIM 时代替物理卡。在虚拟 SIM 组合器中，保存的图像与捕获的 rspro 图像一起作为可选择的文件系统源出现。将一个与订阅者身份（来自 HSS 或 SIM 密钥存储）配对，OmniWeb 启动一个由该图像文件系统支持的虚拟 `bankd`，并叠加订阅者的 Ki/OPc 进行认证。


Saved SIM Image
UPP DER
file system
Subscriber
IMSI + Ki/OPc
identity + keys
Virtual bankd
RSPRO
remote-sim-server
slotmap
Cardem
presents SIM
Modem under test

□□□

解决方案：

1. 将卡片的 Ki 和 OPc 添加到 SIM 密钥存储中，以其 ICCID 为键。
2. 重新捕获图像。新的捕获将密钥折叠到 `PE-AKAParameter` 中。
3. 或者，在虚拟 SIM 呈现时提供密钥（来自 HSS 或显式覆盖）。

上传被拒绝，提示“看起来不像 SAIP UPP”

症状：上传文件时返回验证错误。

可能原因：

- 文件不是 SAIP UPP：它没有以配置文件元素标签（`A0`、`A1` 或 `B0`）开头。
- 文件是 □□□ 的配置文件包（加密），而不是 □□□ 的。

解决方案：

1. 确认文件是 未保护 的配置文件包，采用 DER 编码。
2. 验证它以 `PE-Header`（`A0`）开头。大多数格式良好的 UPP 都是这样。
3. 如果包是受保护/加密的，则无法存储或浏览；仅支持未保护的包。

浏览上传的图像时按 FID 显示文件，而不是按名称

症状：资源管理器中的 EFs 以文件标识符（例如 `EF.6FXX`）标记，而不是友好名称。

可能原因：

- 卡片读取恢复文件标识符和原始内容，而不是配置文件创建者使用的符号名称。OmniWeb 将众所周知的 USIM EFs 映射到友好名称，任何不在该映射中的 EF 都按其 FID 显示。

解决方案：不需要采取任何行动。FID 是权威标识符，原始内容是准确的。这对于非标准或供应商特定文件是预期的。

安全处理导出的包

导出的 UPP 是 未□密 的，当捕获时密钥可用时，包含 Ki 和 OPc。请将下载的 `.der` 视为敏感密钥材料：

- 不要通过不受信任的渠道发送。
- 不再需要时删除本地副本。

更倾向于将图像保留在 OmniWeb 中（访问由 SIM 银行权限控制）而不是分发.der 文件。

SIM银行：分布式SIM库存

SIM银行显示每个OmniWeb代理中的每个智能卡读卡器中的每个SIM。每个代理扫描其本地PC/SC读卡器，读取每个SIM的身份，并像报告调制解调器/电话作为设备一样将库存报告给中央。中央按代理聚合库存，并持久化一个以ICCID为键的SIM数据库，因此“哪些SIM在何处”的视图在读卡器和代理断开连接时仍然存在。

这是一个分布式远程SIM测试床的库存部分。远程SIM卡仿真/银行层允许您通过网络将任何**SIM**连接到任何卡仿真。远程SIM单独记录该层。此页面涵盖发现和库存。SIM图像（SAIP配置包）涵盖如何将卡的文件系统保存、导出和重用为□携式配置包。

该页面是以读卡器为中心的：每个物理读卡槽一行，按代理分组。所有空的、不可读的和正在使用的槽都显示。银行布局是真实的，而不仅仅是填充的槽。

代理如何读取SIM

代理扫描仪镜像调制解调器扫描仪：枚举速度较慢，因此结果被缓存并在间隔内重新扫描。

对于主机上的每个PC/SC读卡器：

1. 枚举连接到主机的PC/SC读卡器。
2. 探测每个读卡器，进行□□连接。
    - 没有卡 → `present=false`。

- 连接引发共享冲突 → 读卡器被另一个进程（例如远程SIM `bankd`或卡仿真会话）占用 → `present=true, in_use=true`，并且不尝试读取。忙碌的读卡器永远不会崩溃扫描。
- 卡存在且空闲 → 读取它。

3. 读取SIM身份，使用一组自包含的原始APDU：
   - UICC与经典SIM检测（选择`3F00`；`6E00` → 经典GSM，因此使用`CLA=A0`和经典选择模式），
   - EF.ICCID (`2FE2`)，EF.IMSI (`6F07`)，EF.SPN (`6F46`)，
   - `EF.AD` (`6FAD`)用于MNC长度（以□正确拆分MCC/MNC），
   - 在锁定卡上进行安全默认PIN (`0000`) 验证。它首先探测重试计数器（一个不递减的空验证），如果只剩一个重试，则拒绝，因此它永远不会烧掉最后一个重试或触及PUK（SIM银行不能使卡砖），
   - 卡的ATR。

每个读卡器成为一个字典：

```
{
  "reader_name": "Identiv SCR35xx USB Smart Card Reader …",
  "reader_index": 0,
  "present": true,
  "in_use": false,
  "iccid": "8961…", "imsi": "505…", "mcc": "505", "mnc": "01",
  "country": "Australia", "spn": "Telstra", "atr": "3b9f96…"
}
```

该列表作为`sims`消息（与设备列表一起）发送到中央，在注册时以及每当它更改时；`simbank_rescan`命令强制立即进行未缓存的扫描。

读卡能力

主机通过其PC/SC智能卡堆栈读取SIM。当需要更深层的卡解码时，代理使用一个可选的、单独授权的智能卡库，与代理的其余部分隔离（它没有合并到OmniWeb自己的代码中）。没有智能卡堆栈的主机仍然可以正常运行代理，并简单地报告没有SIM。SIM银行是每个主机的可选功能，就像调制解调器一样。

参考读卡器是SCM/Identiv SCR35xx。每个主机支持多个读卡器。

库存 → 中央 → 用户界面流程

- 代理通过它用于电话的相同WebSocket拨出到中央(`/api/android/agent`)。SIM库存通过该连接传输。没有新的传输。
- 中央在内存中的`android.Registry`中保持每个代理读卡器的实时快照（`update_sims` / `all_sims`），并通过`simbank.record_sims`将每个ICCID镜像到持久的`simbank_sims`表中。
- 由于这依赖于单进程代理注册表，SIM银行API仅由代理角色后端进程提供（与测试设备相同的约束）。

REST API (`/api/simbank`, JWT, RBAC元素类型`simbank`)

方法	路由	目的
GET	`/sims`	所有代理中的每个SIM（包括离线持久化的SIM），实时显示存在/使用状态。
GET	`/readers`	每个连接代理上的每个PC/SC读卡器（实时），包括空读卡器和正在使用的读卡器。
GET	`/sims/<iccid>`	一个SIM。
PATCH	`/sims/<iccid>`	���辑操作员分配的字段（今天的备注）。如果ICCID未见，则创建该行。
DELETE	`/sims/<iccid>`	忘记一个SIM（删除持久记录；如果仍然插入，则在下次扫描时重新出现）。
POST	`/agents/<id>/rescan`	强制在一个代理上立即进行未缓存的PC/SC重新扫描并返回其新库存。

RBAC镜像`ir38`/`android-control`：管理员始终通过；否则，具有`element_type == "simbank"`的JWT权限授予查看权限，方法中的`POST`授予控制权限。

前端

`src/pages/simbank/SimBank.tsx`：一个可搜索、可过滤的所有SIM的表格：状态（存在/使用中/离线）、代理/站点、读卡器、ICCID、IMSI、MCC/MNC、国家、SPN、可编辑备注、最后一次看到。每个代理的重新扫描按钮。路由在`/simbank`，并从侧边栏链接到漫游测试 **›** **SIM**银行。

数据库架构

`simbank_sims`：每个曾见过的ICCID一行：

列	备注
`iccid` (PK)	SIM序列号。
`imsi`, `mcc`, `mnc`, `country`, `spn`, `atr`	最后已知身份（仅在非空读取时覆盖）。
`notes`	操作员分配的，可编辑。
`last_agent_id`, `last_site`, `last_reader_name`, `last_reader_index`	最后（或当前）看到的位置。
`first_seen`, `last_seen`	时间戳��UTC）。
`remsim_bank_id`, `remsim_slot_nr`, `remsim_mapped_cardem`	第二阶段保留（可为空，未使用）。

空的和正在使用的读卡器不携带任何ICCID，因此它们不会作为SIM持久化。它们仅出现在实时的`/readers`快照中。

未来：远程**SIM**

第二阶段将物理读卡器/SIM映射到远程SIM银行，以□一个站点中的SIM可以呈现给另一个站点的调制解调器/电话（远程SIM）。钩子已经到位。搜索代码中的`# TODO remsim`：

- `simbank_sims.remsim_bank_id` / `remsim_slot_nr` / `remsim_mapped_cardem`（可为空列，在`to_dict`和TS `SimRow`类型中显示为`null`），
- 代理的每个读卡器`in_use`标志已经区分了被`bankd`/仿真会话占用的读卡器。这就是第二阶段将映射的读卡器，
- `PATCH /api/simbank/sims/<iccid>`是编辑remsim映射的地方。

今天没有任何东西驱动remsim；该形状被保留，以□映射可以在不重新处理库存热路径的情况下插入。

站点编辑器：站点配置查看器

站点编辑器显示当前选定站点的原始配置文件：定义该部署的网络功能、基础设施和设置的YAML主机/库存文件。这是一个只读的、语法高亮的视图，因此您可以准确查看OmniWeb为站点所使用的内容，而无需在主机上打开shell。

← 操作指南

它显示了什么

OmniWeb通过每个站点的配置文件驱动每个站点。该文件列出了站点的元素（哪些网络功能存在以及位于哪些地址）、其基础设施主机、监控角色、`fivegc`块（参见5G核心）等：侧边栏、拓扑、元素页面和仪表板所依赖的一切。

站点编辑器为顶部栏站点下拉菜单中选择的站点加载该文件，并在一个完整的编辑器面板（Monaco，与VS Code使用的相同编辑器）中显示，具有YAML高亮、行号、折叠和小地图。标题显示客户、站点和源文件名。

Parse error on line 3: ... SE -->|/api/sites/{customer}/{site}/ra ----------------------^ Expecting 'SQE', 'DOUBLECIRCLEEND', 'PE', '-)', 'STADIUMEND', 'SUBROUTINEEND', 'PIPE', 'CYLINDEREND', 'DIAMOND_STOP', 'TAGEND', 'TRAPEND', 'INVTRAPEND', 'UNICODE_TEXT', 'TEXT', 'TAGSTART', got 'DIAMOND_START'

□试

如果没有选择站点，页面会提示您先从下拉菜单中选择一个。

设计为只读

站点编辑器是一个查看器：该面板是只读的（在标题中标记为只读）。它用于□□有效配置，而不是更改它。

站点配置不能通过浏览器进行编辑。如本指南中所述，OmniWeb的部署和配置是通过**Ansible**管理的。请勿直接在主机上编辑配置文件，添加或更改元素是通过该管道进行的配置更改（参见配置模型）。站点编辑器允许您读取所选站点的该管道结果。

何时使用它

- 确认站点的配置：OmniWeb认为存在哪些元素、主机和5GC网络功能，以及它们位于哪些地址。

- 根据配置排查**UI**问题：如果缺少元素、侧边栏条目或5GC部分，或指向错误的主机，原始文件是检查的真实来源。
- 在准备**Ansible**更改时引用确切的文件名和内容。

相关

- 架构：配置模型：站点配置如何驱动OmniWeb以及如何管理。
- 5G核心：站点配置的 `fivegc` 块及其呈现内容��
- 网络拓扑：基于相同站点配置构建的拓扑和主机列表视图。

SMPP 网关
SMPP 网关 将外部 SMPP 对等体与消息核心连接起来。外部应用程序和互通合作伙伴，即 ESMEs（外部短消息实体），通过 SMPP 连接，既可以作为网关拨出的客户端，也可以作为网关接受绑定的服务器，网关将它们的短消息传递到 SMSC 和从 SMSC。每个连接都是一个 SMPP 绑定（收发器、发件人或接收者）。网关保持这些绑定的活跃状态，进行身份验证和管理，并将流量传递给消息核心。 OmniWeb 显示实时绑定状态、配置的客户端和服务器对等体，以及网关的日志。

← 操作指南

SMPP 网关是一个每个实例的元素页面，可以从侧边栏访问，当在站点的库存中运行时，可以查看多个已部署的实例。所有流量通过 OmniWeb 后端代理传递到网关的 API，因此它保持在单个经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织成多个标签。

概述

一个屏幕的健康状态读取聚合绑定统计信息：总绑定数量和按 客户端（出站）和 服务器（入站）绑定分割的 连接 / 断开连接 细分。这是确认网关正常运行及其对等体已绑定的最快方法，并且可以一目了然地发现任何预期连接是否已断开。

绑定状态

每个启用的绑定，客户端和服务器，及其当前 连接状态、底层 会话详情 和每个绑定的 指标。这是当前谁已绑定的实时视图。从这里，操作员可以对绑定进行操作：

断开 活动绑定。对于客户端绑定，这将终止出站连接。对于服务器绑定，它将断开所有活动客户端连接。使用它来清除卡住或表现不佳的连接。
重新连接 客户端绑定。这强制客户端（出站）绑定重新拨号其远程主机，这是在网络波动后将出站对等体快速恢复的最快方法。

客户端对等体

配置的出站 SMPP 客户端 连接是网关拨出的对等体。每个显示其 名称、远程 主机 和 端口、绑定的 系统 **ID** 和 绑定类型（收发器、发件人或接收者）。客户端对等体在这里可以完全编辑：操作员可以 添 一个对等体，编辑 现有的对等体（主机、端口、凭据、绑定类型、查询链接间隔、TPS 限制和其他绑定参数），以及 删除 一个不再需要的对等体。启用对等体将其出站绑定投入服务。禁用它将对等体移除，但不丢弃其配置。

服务器对等体

配置的入站 SMPP 服务器 授权是绑定到网关的对等体的凭据和规则。每个条目定义一个 系统 **ID** 和密码、允许的绑定类型，以及管理入站绑定的保护措施：一个 **IP** 白名单，允许的源地址，以及一个 源地址白名单，允许的来源地址模式，外加一个 **TPS** 限制。服务器对等体在这里以相同的方式可编辑（添□、编辑 和 删除），因此操作员可以接入新的入站合作伙伴、收紧其白名单或撤销它。启用和禁用授权控制该合作伙伴是否被允许绑定。

日志

日志 标签实时跟踪网关的日志输出，以□在 OmniWeb 中排查单个网关的问题（绑定失败、身份验证拒绝和断开连接）。

监控

SMPP 网关的消息速率、吞吐量和其他时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

SMSC 是网关传递短消息的消息核心。
IP‑SM‑GW 通过 IMS 为 VoLTE 设备传递 SMS，并补充了与外部对等体的 SMPP 路径。

SMSC: 短信服务中心

SMSC（短信服务中心）是短信核心的存储和转发中心。它接收来自网络的消息（通过SS7（MAP）从移动端、通过Diameter和通过SMPP从应用前端）。然后它路由、翻译并交付这些消息。它会保存任何无法立即交付的消息，并重试直到消息被交付、过期或被丢弃。在此过程中，它跟踪每条消息的交付状态，翻译呼叫和被呼叫号码，与对等SMSC进行联合，以□将消息交给能够到达收件人的节点，并推动批量短信活动。OmniWeb通过单个实例页面展示所有这些内容：实时消息状态、订阅者位置、前端注册、Diameter和联合健康、路由和翻译规则集，以及活动管理。

← 操作指南

SMSC是一个每个实例的元素页面，可以从侧边栏访问，当在站点的库存中运行时，可以查看多个已部署的实例。所有流量都通过OmniWeb后端代理到SMSC的API，因此它保持在单个经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织为多个选项卡。

概述

着陆选项卡是节点的单屏健康读取：当前消息计数和交付状态，前端和对等健康一目了然，以及按MSISDN的搜索，可查看存储的消息和订阅者位置。这是回答“此订阅者的短信现在发生了什么”的最快方式。

消息

SMSC持有或处理的每条消息，每行显示发送和接收号码、消息状态（待处理、已交付、失败、过期、丢弃或自动回复）、交付尝试的次数及其年龄。您可以按状态、按SMSC进行过滤，并包括死信或未路由流量，并按MSISDN、节点名称或消息ID进行搜索。选择一条消息以打开其详细信息，包括解码的明文。操作员可以重新路由消息，以强制其重新经过路由，例如在修复路由规则后。

前端

当前与SMSC注册的应用和SMPP前端是提交和接收消��的客户端。每个条目显示其主机名、最后一次见到的时间以及其注册过期的时间，因此您可以确认消息处理前端已连接且其注册是有效的。

位置

SMSC已学习的订阅者位置是每个订阅者按**IMSI**和**MSISDN**的最后已知服务位置。SMSC使用此信息来联系收件人。您可以按IMSI或MSISDN进行搜索，并过滤以包括过期条目。在这里，您可以确认SMSC知道订阅者的位置，以□能够向他们交付。

Diameter

SMSC用于消息传递的Diameter对等连接，每行显示对等体的领域、**IP**地址、传输、连接发起方向、报告的产品名称、协商的应用**ID**和连接状态。在这里，您可以确认SMSC所依赖的Diameter路径是否正常。

联合

联合视图显示此SMSC如何与对等SMSC合作，以□将消息交给能够到达收件人的任意节点。它报���此节点、健康、降级和不健康对等体的计数、缓存的联合消息数量（当不为零时突出显示）、正在使用的发现方法（DNS域或静态对等体），以及每个对等体的节点名称、状态、最近的故障、最后一次成功的健康检查和每个对等体提供的前端的表格。这是查看联合中的SMSC是否彼此可达的最快方式。

路由

决定每条消息去向的SMS路由规则，按优先级列出。每条规则匹配呼叫和被呼叫号码模式（可选的源SMSC或源类型，如SS7或电路交换），并解析为一个目标（目标SMSC或ENUM查找），带有描述和启用状态。规则是完全可编辑的：操作员可以添加、编辑、启用、禁用或删除它们，并导出和重新导入规则集。

□□

□□□

活动

批量SMS活动是在此选项卡中创建和推动的。定义一个新活动，包括名称和描述、发送者号码、源SMSC、接收者列表、受众（仅活跃接收者或列表中的所有人）、每秒的滴水速率、消息有效性窗口、可选的延迟交付时间和消息模板。创建后，可以从这里控制活动（开始、暂停、恢复或取消）。您可以检查其目标，以查看每个接收者的发送和交付状态，随着活动的进行而变化。

□□□□

□□□

NAPTR 测试

NAPTR 测试选项卡是一个操作员工具，通过ENUM/NAPTR DNS解析E.164号码（或域），以查看SMSC将如何路由消息。输入要查询的电话号码和ENUM域（默认是e164.arpa），然后提交。在您提交之前不会获取任何内容。SMSC将号码的数字反转到ENUM区域，查找发布的NAPTR记录，并按顺序和优先级返回它们。每条记录携带其标志、服务、重写的正则表达式和替换，以及记录指向的解析的结果域。在这里，您可以确认路由规则背后的ENUM数据确实将号码解析为您期望的URI或路由，然后再在生产中依赖它。

MWI

MWI选项卡为订阅者发送消息等待指示更新：设置或清除手机上的“等待消息”标志的通知，通常是在留下或收集语音邮件后。提供要通知的目标 MSISDN和来源的MSISDN，选择指示类型（语音邮件、传真、电子邮件或其他），并设置指示器是否应为活动（开启）或清除（关闭），可选的消息正文和来源SMSC。这是一个提交表单：只有在您发布时，更新才会被发送。这是手动提升或清除订阅者等待消息指示器的直接方式。

系统日志

系统日志选项卡是SMSC自己的API支持的日志视图。您可以按级别（调试、信息、警告、错误）和限制返回的行数进行过滤，因此您可以在调查特定问题时仅提取最近的错误或更全面的跟踪，而无需离开OmniWeb。

更多工具

除了上述选项卡，SMSC页面还提供了一些专注的工具：

- 提交：一个表单，直接从OmniWeb发送一次性SMS（发件人、收件人和消息文本），以测试向特定接收者的交付。
- 操作：节点范围的维护操作，包括清除注册的前端���存储的消息、路由规则和翻译规则。每个操作都是破坏性的，并首先要求确认。

日志

日志选项卡实时跟踪SMSC的日志输出，以□在不离开OmniWeb的情况下排查单个节点的问题。要查看同一节点的过滤API支持视图，请使用上面的系统日志。

监控

SMSC的消息吞吐量、交付成功率、队列深度和其他时间序列以Grafana仪表板的形式呈现，可以从元素页面访问。OmniWeb不会原生重复这些图表。

相关

HSS：持有SMSC交付所需的订阅者数据和路由信息。
DRA：中继SMSC用于消息传递的Diameter信令。
STP：SMSC与移动网络交换MAP消息的SS7信令路径。
CSCF/TAS：IMS侧为VoLTE订阅者发起和终止消息传递。

软件管理与生命周期
OmniWeb 提供了一个统一的地方来查看和管理整个系统中运行的软件：软件包版本、可用更新和许可证。网络软件的生命周期可以通过用于操作它的同一门户进行查看。

← 返回操作指南

软件页面 (APT 仓库)

软件页面是 Omnitouch 软件包的 APT 仓库浏览器。它连接到配置的 APT 仓库服务器，并显示它管理的软件包的以下信息：

可用软件包 在仓库中。
版本 提供，包括最新可用版本。
更新状态：是否存在比已部署版本更新的版本。

这使得操作员可以一目了然地看到哪些 Omnitouch 组件有待更新，哪些版本是当前的，从而提供软件生命周期的库存侧。主机上的软件包安装/升级通过标准的 APT/ dpkg 工具进行（通常通过 Ansible 自动化）；OmniWeb 提供了对已发布和当前内容的可视化层。

□□□□□□□ Omnitouch □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□/□□□□□□□□□□□□□□□□□□□□ `omni-upf` □ `omni-msc` □□□□□

□□□□□□□□□□

□□□□ **APT** □□□□ □□□□□□□□□□□□□□□□□□□□

同步在缓存镜像本身上运行（OmniWeb 触发它并流式传输进度）；镜像从构建仓库拉取更新的 `.deb`，并重新生成其索引。现场的主机随后像往常一样从缓存中安装更新的软件包。

版本控制

OmniWeb 报告其自身的构建版本（版本、提交和构建日期），以□操作员可以确认他们正在运行的门户的确切构建。这是报告问题或协调门户自身升级时的参考点。

许可证管理

许可证服务器通过 OmniWeb 像其他元素一样进行管理，使用相同的通用模式（请参见 常见操作）。它显示：

*□□□

SS7：信令栈（STP / HLR / IP-SM-GW / CAMEL-GW）

SS7栈（OmniSS7）终止SIGTRAN传输（承载**M3UA**的SCTP关联），并在信令网络中路由SS7/MAP流量。一个服务提供整个栈，OmniWeb将其呈现为四个元素视图，以适应其不同的角色：**STP**（信令传输点，SS7路由器）、**HLR**（家庭位置注册）、**IP-SM-GW**（IP短消息网关）和**CAMEL-GW**（CAMEL网关）。所有四个视图都由相同的共享客户端支持，因此它们共享的SIGTRAN传输和路由是从不同角度看到的相同底层栈。

← 操作指南

每个视图都是一个实例元素页面，当SS7栈在站点的库存中运行时，可以从侧边栏访问。所有流量都通过OmniWeb后端代理到栈的API，因此它保持在单一的经过身份验证的网关后面。响应以`{status, response}`封装返回。每个元素页面头部的文档链接（上下文帮助按钮）打开此页面。每个视图组织为选项卡。消息速率和其他时间序列以Grafana仪表板的形式呈现，从元素页面访问。OmniWeb不会原生复制这些图表。

一瞥栈

每个角色下面的SIGTRAN传输是相同的，因此对等体和**SCTP**连接选项卡出现在所有四个视图中，并读取相同的数据。

对等体选项卡报告M3UA对等体状态（`/api/m3ua-status`）：每个M3UA/M2PA对等体，包含其**ASP**状态、关联状态、本地和远程端点、路由上下文、协议和模式，以及每个对等体的正常运行时间统计信息。在这里，您可以确认每个信令邻居的应用服务器进程是否正常运行并处于服务状态。

SCTP连接选项卡列出底层传输（`/api/sctp-connections`）：每个SCTP关联的状态、角色、本地和远程**IP/**端口、入站和出站流计数、发送和接收的字节和消息、最后活动以及任何最后错误，以及所有连接的汇总总数。当一个对等体显示为离线时，请检查这一层以查看SCTP关联本身是否��建立。

STP：路由

STP视图是SS7路由器。除了共享传输选项卡外，它还包含路由选项卡，以及网络地图、概述和**SS7**事件馈送。

路由选项卡显示完整的M3UA路由配置（`/api/routing`）：配置的对等体、点码（**PC**）路由和全局标题（**GT**）路由。

- 点码路由通过目标对等体将流量定向到目标点码（`dest_pc`），并带有网络指示符、点码掩码和优先级。操作员可以添□一个PC路由（`POST /api/routing/pc-routes`，提供目标点码和目标对等体）并删除一个（`DELETE /api/routing/pc-routes/{dest_pc}-{peer_id}`）。
- 全局标题路由匹配GT前缀并将其转发到目标对等体，带有优先级和可选的SSN、翻译类型和地址性质详细信息及描述。操作员可以添□一个GT路由（`POST /api/routing/gt-routes`，提供前缀和目标对等体）并删除一个（`DELETE /api/routing/gt-routes/{prefix}:{peer_id}`）。

在这里，您可以确认并调整STP如何将SS7消息转发到每个目标。

HLR

HLR视图显示注册表的活动订阅者和与HLR后端的链接��旁边是共享传输选��卡、概述和**SS7**客户端选项卡。

订阅者选项卡列出活动订阅者注册（/api/subscribers）：每个已发送UpdateLocation且尚未发送 CancelLocation的订阅者，每行显示IMSI、VLR、服务MSC、注册时间和持续时间，以及唯一VLR和MSC的计数。操作员可以清除所有跟踪的活动订阅者（DELETE /api/subscribers）以重置注册表的视图。

HLR链接选项卡检查与配置的HLR API的连接性（`/api/hlr-links`）：状态（正常、降级或离线）、测量的延迟、报告的版本和目标主机。这是确认栈可以访问HLR后端的最快方式。

IP-SM-GW

IP-SM-GW视图是短消息网关。它承载SMSc订阅者跟踪器和与SMSc后端的链接，旁边是共享传输选项卡和概述。

SMSc链接选项卡检查与配置的SMSc API的连接性（`/api/smsc-links`）：状态（正常、降级或离线）、延迟、报告的版本和目标主机。这是SMS路径等同于HLR链接检查。

SMSc订阅者选项卡列出由SMSc订阅者跟踪器跟踪的订阅者（/api/smsc-subscribers）：每个订阅者都有 MSISDN、IMSI、HLR GT和VLR GT、发送和接收的消息、状态和最后更新，以及活动/失败和唯一HLR计数。操作员可以清除所有跟踪的SMSc订阅者（DELETE /api/smsc-subscribers）。

CAMEL-GW

CAMEL-GW视图显示网关正在运行的CAMEL会话，旁边是共享传输选项卡和概述。

CAMEL会话选项卡列出网关管理的所有活动CAMEL会话（`/api/camel-sessions`）：每个会话的状态、**CAP**版本、服务密钥、**IMSI**、主叫和被叫号码、开始时间和持续时间，以及发起和应答的会话计数。在这里，您可以实时观察CAMEL呼叫处理。

状态

状态端点（`/api/status`）报告概述选项卡总结的整体节点健康状况：节点份和角色，服务是否正常，其正常运行时间，以及对等体摘要，显示有多少信令对等体处于活动状态。这是确认栈正在运行及其对等体处于服务状态的第一步。

相关

- **STP**：SS7路由元素（点码和全局标题路由）。
- **HLR**：家庭位置注册元素（活动订阅者注册和HLR链接）。
- **IP-SM-GW**：IP短消息网关元素（SMSc订阅者和链接）。
- **CAMEL-GW**：CAMEL网关元素（实时CAMEL会话）。
- **MSC/VLR**发起UpdateLocation和CAMEL信令，该栈路由和跟踪。
- **SMSc**是IP-SM-GW的SMSc链接和订阅者跟踪器解析的后端。
- ← 操作指南

SIM工具包（STK）客户端

OmniWeb 包含一个交互式 **SIM**工具包 客户端。使用它可以在连接的代理的 PC/SC 读卡器中插入的任何物理 SIM 卡上导航和驱动 STK 小程序。STK 客户端向卡片发送终端配置文件，然后将每个主动命令呈现为交互式屏幕。您像终端一样进行响应，因此小程序会推进到下一个步骤。

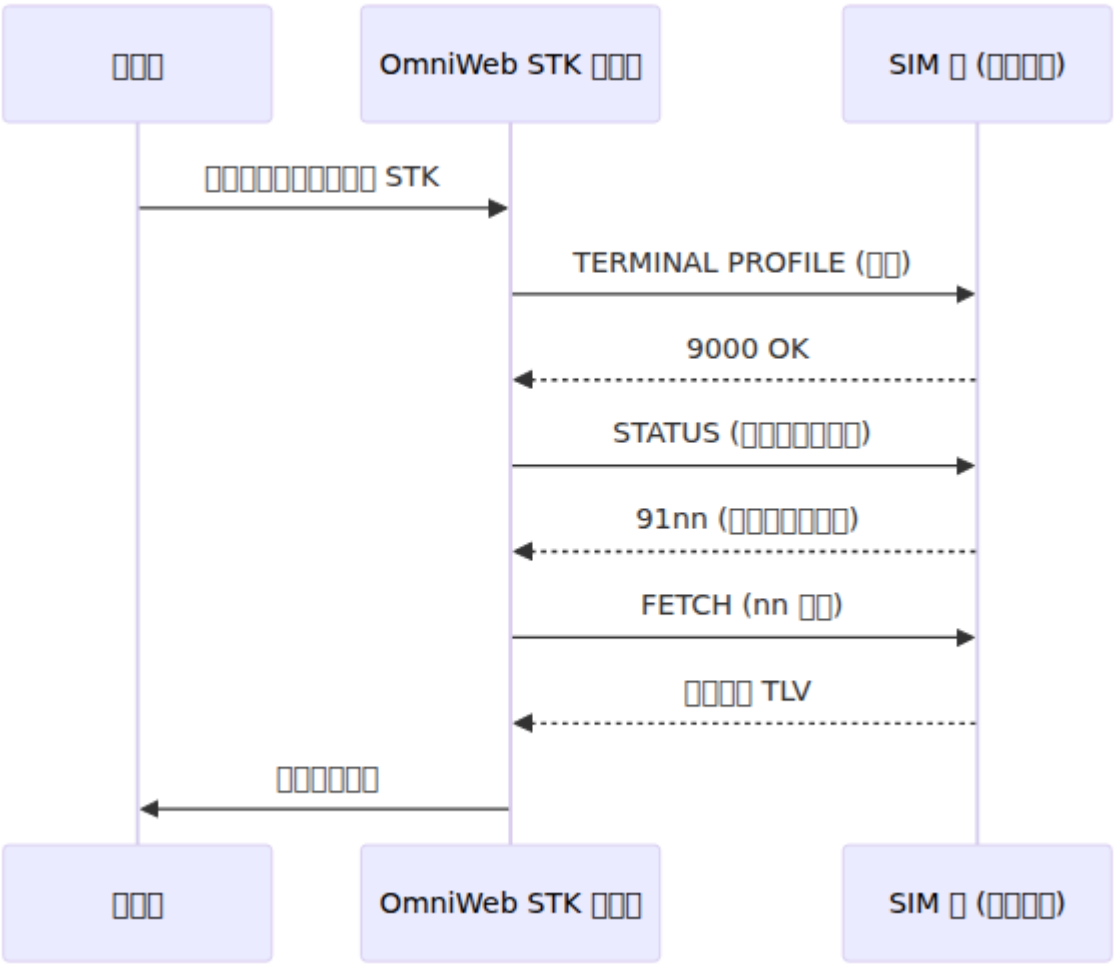
该工具位于侧边栏的 **SIMs - SIM**工具包 下，与 APDU终端和SIM文件系统浏览器 一起显示。

什么是 **SIM**工具包?

SIM 应用工具包 (STK) 是在 ETSI TS 102.223 中定义的标准，允许 SIM 卡在终端上发起操作。SIM 小程序发出 主动命令 - 请求，例如“显示此文本”或“显示此菜单” - 终端则以用户的选择或输入进行响应。常见用例包括运营商充值菜单、余额查询、OTA 配置触发器和 SIM 驻留服务门户。

要求

- 一台带有包`` STK 小程序的 SIM 卡的读卡器。
- **SIM** 银行控制 权限。没有此权限，您可以看到读卡器，但无法打开会话或驱动卡片。
- 读卡器不能被其他工具占用。如果被占用，OmniWeb 会显示谁在占用并提供 接管 选项。接管会取消其他会话。



打开会话

1. 从 读卡器 下拉菜单中选择读卡器。只有插入卡片的读卡器会出现。
2. 点击 开始 **STK**。OmniWeb 在卡片上打开独占会话，发送终端配置文件，并轮询第一个主动命令。
3. 与每个屏幕进行交互。OmniWeb 在每个步骤后发送 TERMINAL RESPONSE，并自动获取下一个命令。
4. 当卡片发出 END SESSION 命令时，或当您点击 结束会话 时，会话结束。

命令屏幕

OmniWeb 将每个主动命令呈现为交互式屏幕。下表列出了支持的命令类型。

命令	描述	用户操作
显示文本	卡片显示一条消息。	点击 确定 以确认，或点击 返回 以返回上一步。
选择项目 / 设置菜单	卡片呈现一个编号选项列表。	点击您想选择的项目。
获取按键	卡片请求一个按键输入。	输入一个字符并点击 发送，或选择 是 / 否 进行是非提示。
获取输入	卡片请求一个指定长度的文本字符串。	输入文本并点击 发送。该字段显示最小和最大字符数。

如果卡片发出客户端未以交互方式呈现的命令类型（例如发送短消息或设置呼叫），OmniWeb 会显示原始命令数据，并自动发送 **OK** 响应，以□会话可以继续。

会话历史

一旦您开始交互，右侧会出现 会话历史 面板。它记录每个命令类型和您给出的响应（选择的项目、输入文本或 OK/返回）。使用它可以追溯菜单树中的路径。

结束会话

会话以三种方式结束：

- 卡片发起结束：小程序发出 END SESSION 主动命令。OmniWeb 会自动关闭会话并显示完成消息。
- 操作员结束：随时点击 结束会话。OmniWeb 会向卡片发送会话终止结果并���闭读卡器会话。
- 向后导航超出根节点：在第一个屏幕上点击 返回 会向卡片发送向后移动结果。卡片决定如何响应 - 它可能会显示上一个屏幕或结束会话。

会话结束后，读卡器再次可用于其他工具。

与其他 SIM 工具的关系

工具	目的
SIM工具包（此页面）	交互式驱动 STK 小程序。
APDU终端	手动发送原始 APDU，一次一个或在持久会话中。
SIM 文件系统浏览器	浏览和编辑卡片的文件系统。
APDU 日志	被动跟踪调制解调器与远程 SIM 之间的命令。

故障排除

启动 STK 失败，显示“TERMINAL PROFILE 失败”

卡片拒绝了终端配置文件或代理无法到达卡片。检查以下内容：

- 卡片是否正确放置在读卡器中。
- 没有其他工具占用读卡器。如果有，请使用 接管。
- 拥有读卡器的代理是否在线（检查 SIM 银行页面）。

会话在第一个命令后停止

某些 SIM 小程序如果终端配置文件未声明小程序所需的能力，则会立即结束会话。客户端声明了一组广泛的能力，���某些卡片会检查特定位。如果发生这种情况，请在会话模式下使用 APDU终端 手动发送 TERMINAL PROFILE 和 FETCH，并检查原始主动命令数据。

返回意外屏幕

返回 操作向卡片发送结果代码 0x11（向后移动）。卡片控制这意味着什么。一些小程序返回到上一个菜单；其他小程序从根菜单重新启动会话；少数小程序忽略向后移动并重新发出相同命令。

GET INPUT 拒绝我的文本

卡片设置了最小和最大字符数。输入字段显示两者。如果卡片还限制为仅数字，字段标签会显示 仅限数字。输入一个在要求范围内的值。

TAS：电话应用服务器

TAS（电话应用服务器）是IMS应用服务器，提供用户的电话体验。它处理呼叫控制和附□服务（呼叫转移、呼叫限制、呼叫等待、保持等），运行会议，接收和播放语音邮件，为每个呼叫记录**CDR**，解决路由和号码翻译，并通过Diameter与**OCS**通信，以□实时计费。当CSCF决定□□信号化呼叫时，TAS决定□□□□□。OmniWeb在一个元素页面上显示其实时呼叫、用户注册、网关、Diameter对等体和配置。呼叫量和趋势图表在同一页面的Grafana仪表板上显示。

← 操作指南

TAS是一个每实例元素页面，可以通过侧边栏在站点的库存中访问。所有流量通过OmniWeb后端代理进入TAS的API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它被组织为多个选项卡。

概述

着陆选项卡是应用服务器的单屏健康读取：活跃呼叫、注册用户、正在运行的会议和存储的语音邮件记录、**Diameter**对等体的健康状况和**SIP**网关、以及许可证状态。这是确认TAS正常运行并承载流量的最快方式。

□□□□

□□□

CDR

TAS□□□

用户

TAS已知的用户注册，每个注册包含用户身份、注册状态和当前联系方式。打开一个用户以获取完整的注册详细信息。在追踪服务为何对他们不起作用之前，这里是确认用户已注册到应用服务器的地方。

Diameter

TAS连接的Diameter对等体，包括通往OCS的计费路径和HSS的用户数据，每个对等体的主机名和连接状态。打开一个对等体以获取其详细信息。当计费或用户查找失败时，此选项卡是确认基础Diameter路径是否正常的地方。

网关

TAS用于连接其他网络和中继的SIP网关，每个网关显示其名称和当前状态。打开一个网关以获取其详细信息。使用此选项卡确认互联网关已注册并可用，然后再诊断失败的外网呼叫。

□□

□□□

语音邮件

存储的语音邮件记录，按用户分类。每条记录可以单独删除，例如清除错误留下的消息或释放已满的邮箱。

OCS测试

TAS持有的活跃**OCS**（在线计费系统）会话，以□您查看哪些呼叫正在消耗实时余额。可以从这里终止单个计费会话。这对于清除在呼叫结束后仍然保持打开状态的会话非常有用。

路由

TAS路由呼叫的拨号计划模板。列表显示每个模板；打开一个以阅读其内容。这是号码匹配和呼叫发送位置的参考。与号码翻译工具一起阅读，以确认给定号码按预期路由。

配置

TAS正在运行的应用配置，按应用分组。打开一个条目以阅读其设置。这是确认服务器按预期配置的读取参考，而无需离开OmniWeb。

提示

TAS播放给呼叫者的文本到语音提示录音，公告和菜单提示，以及每个提示的状态。使用此选项卡确认预期的提示是否存在并已正确呈现。

工具

除了上述选项卡，TAS页面还提供了一组按需工具，用于验证路由和用户数据。每个工具都包含一个小表单，通过OmniWeb代理向应用服务器发送请求，并在页面上显示结果。

呼叫模拟器

通过TAS进行测试呼叫，以验证路由和媒体。输入一个目标（可选输入源号码、源IP和强制处置）。模拟器在拨号计划中处理呼叫而不响铃任何人。它返回解析的呼叫类型（MT、MO或紧急），在线/离线决策、每个设置的拨号计划变量以及逐步的处理说明列表，以□您可以准确查看一个号码在真实呼叫之前将如何处理。可以跳过OCS授权和HLR查找，以隔离一个阶段。单独的**��声测试呼叫**操作响铃目标并将参与者自己的音频回送，这确认了到手持设备的实时语音路径。

Sh查询

通过Sh接口查询HSS以获取用户数据。输入用户的公共身份并选择要获取的数据引用，从完整的存储库数据到特定元素，如IMS用户状态、服务 S-CSCF名称、初始过滤标准、MSISDN或IMSI。该工具返回HSS持有的透明和存储库服务数据。使用它确认当服务未按预期运行时，应用服务器对用户所看到的数据。

HLR□□

□□SS7 MAP□□**HLR**□□□

号码翻译

测试拨打的号码如何被TAS路由规则规范化和翻译。输入国家代码、电话号码和可选的处置。该工具返回拨号计划将使用的翻译号码。与路由选项卡一起阅读，以确认给定号码按预期匹配和重写。

ESL

一个交互式控制台，用于向TAS引擎发出媒体服务器风格的命令以进行诊断。输入命令并按Enter。输出将在控制台中打印，向上/向下箭头可回忆先前的命令。提供示例命令，如`status`、`sofia status`、`show channels`和`show registrations`，作为一键式按钮。这是运行引擎的最低级别视图，用于直接确认实时通道、网关状态和注册。

日志

日志选项卡跟踪TAS的实时日志输出，以□在不离开OmniWeb的情况下对单个应用服务器进行故障排除。

监控仪表板

TAS的呼叫量、每项服务计数器和其他时间序列以Grafana仪表板的形式呈现，从元素页面访问。OmniWeb不会原生重复这些图表。

相关

- **CSCF**信号化TAS应用服务的呼叫。两者共同提供IMS语音。
- **HSS**持有TAS解析的用户和Sh用户数据。

- **OCS**实时��过Diameter对TAS的呼叫进行计费和收费。
- **DRA**将TAS的Diameter信号（Sh、Gy）转发给这些对等体。

测试设备

测试设备 将远程站点的真实 Android 手机转变为可远程控制的测试农场。在 OmniWeb 中，您可以实时观看手机屏幕，控制手机（点击、滑动、输入、硬件键），拨打电话和发送短信，并运行定期健康检查。这些检查涵盖 VoLTE 注册、信号和连接性。OmniWeb 将其通过/失败结果导出到 Prometheus 以进行警报和仪表板。

← 返回操作指南

它的存在是为了回答 NOC 不断询问的一个问题：“□□□□□□□□□□□□□□□□□□□□” 手机必须注册 VoLTE，并能够拨打电话、发送短信和访问互联网。没有人需要开车到现场。

架构

每个通过 ADB 连接手机的主机都运行一个轻量级的 代理。代理拨打 □□ 到中央 OmniWeb，因此 NAT 后面的站点无需入站访问。实时视频使用 **WebRTC**（UDP），因此它比 TCP 屏幕共享更好地适应丢包和高延迟的链接。中央中继输入和测试结果。

> 网络路径很重□□□。Web UI、输入和呼叫设置（“信令”）通过 HTTPS 在控制平面上传输到 OmniWeb 服务器。然而，实时屏幕视频 直接在操作员的浏览器和代理主机之间通过 **UDP** 流式传输。它不会经过服务器。如果浏览器可以访问服务器但无法通过 UDP 访问代理主机，控制台将停留在“连接中…”。请参见 网络要求 以获取请求的防火墙规则以及如何识别问题。

组件	角色
手机代理	发现 ADB 设备，捕获屏幕，注入输入，运行主机测试脚本。每个站点一个；由 `device_tester` Ansible 角色安装。
中央 **OmniWeb**	设备注册，WebRTC 信令中继，脚本调度，结果历史，Prometheus 指标。
Prometheus	从 `/api/android/metrics` 抓取定期测试结果。

□□□□

□□□

4. 手机显示 *“□□ USB □□□”* 提示，显示主机的 RSA 密钥。勾选 始终允许来自此计算机的连接 并接受。（如果没有勾选，每次重新连接时都会返回提示，设备显示为 `unauthorized`。）

普通手机无需其他设置。测试脚本和实时屏幕仅使用标准 ADB。首次连接时保持屏幕解锁，以□可以接受提示。

2. 将 USB 设备传递给代理主机

如果代理在裸机上运行，则跳过此��骤。如果代理主机是虚拟机或容器，虚拟机监控程序拥有 USB 端口，因此您必须转发设备：

平台	如何转发设备
Proxmox（虚拟机）	`qm set <vmid> -usbN host=<bus>-<port>` 绑定物理端口（该映射在更换该端口上的手机时保持不变），或 `host=<vendor>:<product>` 跟踪特定设备。使用 `lsusb` 在 Proxmox 主机上查找 ID。
Proxmox（**LXC** 容器）	添加到 `/etc/pve/lxc/<ctid>.conf`：USB 的设备 cgroup 允许（`lxc.cgroup2.devices.allow: c 189:* rwm`）和 USB 总线的绑定挂载（`lxc.mount.entry: /dev/bus/usb/<bus> dev/bus/usb/<bus> none bind,optional,create=dir`），然后重启容器。将设备重新插入不同总线需要挂载匹配的总线。
VMware	在虚拟机运行时，**VM → 可移动设备 → <phone> → 连接**（或添加 USB 控制器并在虚拟机设置中连接设备）。

> USB 调制解调器和旧 Android 加密狗以相同方式转发。它们显示为相同的 USB 设备类别，因此传递的总线可以携带手机、调制解调器和加密狗。

3. 确认设备出现

在代理主机上，`adb devices` 应该将手机列为 `device`（而不是 `unauthorized` 或 `offline`）。几秒钟内，它会出现在该站点的 车队视图 中。如果没有，请参见 故障排除。

车队视图

测试设备 视图列出了所有站点的每个连接手机，按站点分组。每个卡片显示型号、制造商、Android 版本、屏幕分辨率、网络运营商、电池和构建。您可以一目了然地看到哪些手机在线且健康。

*□□□□□□□□□□□□“□□ 12”□“□□□□□”□□□□□□□□□□□□

设备控制台

点击手机会打开其 控制台：屏幕的实时视图，具有完全的远程控制。

*□□□

同时查看多个手机

要同时观看几部手机（例如，测试通话的两端），打开一部手机的控制台并点击 额外手机（右上角）。从列表中选择另一部手机，其实时屏幕会与第一部手机并排打开，具有自己的完整控制：点击/滑动/输入、硬件键、快速操作、音频监听和流统计信息。列表保持打开状态，因此您可以继续添加，屏幕在页面上平铺——没有固定限制，因此可以添加尽可能多的手机。

要一次打开整个组，请在测试设备列表中勾选您想要的手机，然后点击 查看所选：第一部成为主设备（工具列作用于该设备），其余设备并排显示。

每个额外的屏幕都有自己的选择器来 切换 显示的手机和一个 ✕ 来关闭它。该排列在页面地址中捕获（`?with=…`），因此可以书签或共享特定的多手机布局。

选项卡工具面板（蜂窝、脚本、Shell 等）始终作用于 主 手机，即您打开的手机。面板标题会标明它，以□清楚地知道脚本或命令将运行在哪里。

控制台工具

在屏幕旁边，一个 选项卡工具面板 将每个设备的工具集中在一起。切换选项卡而不丢失每个工具的状态：

选项	功能
蜂窝	呼叫/短信/ping/速度测试验证工具（如下）
脚本	在此设备上运行库脚本并查看其完整运行历史，任何过去运行的脚本都可以一键重新运行
Shell	设备的交互式命令/响应控制台
Logcat	带有文本 ＋ 级别过滤的实时设备日志流
文件	浏览、下载、上传、重命名和删除设备上的文件
录制	捕获点击/滑动序列作为可重放的脚本行

蜂窝验证面板

内置工具用于操作员手动运行的检查，每个工具接受您所期望的输入：

工具	输入	功能
呼叫	号码、保持时间	拨打电话，确认电话接通，保持，挂断
短信	号码、消息	发送短信并确认其离开设备
Ping	主机、计数	通过设备的数据连接 ping 主机
速度测试	测试 URL	测量通过设备的数据链路的下载吞吐量

号码 框记住您最近拨打或发送短信的号码（仅保存在您的浏览器中，而不在服务器上），并以下拉列表的形式提供，因此重新拨打测试号码只需一次点击。

脚本

脚本 选项卡在此设备上运行任何库脚本，并保持其完整运行史，而无需离开控制台。您可以按来源、状态和测试过滤该历史记录。每个过去的运行都有一个 重新运行 按钮，因此重复检查（或刚刚失败的脚本）只需一次点击。需要输入的脚本会重新提示输入。

Shell

Shell 选项卡是设备的交互式命令/响应控制台。输入命令，查看其输出和退出代码，使用 ↑/↓ 回忆历史。它是设备的调制解调器 AT 控制台的类比，适用于快速命令比编写脚本更快的情况。

Logcat

Logcat 选项卡流式传输设备的实时系统日志。按自由文本和最小级别（详细 → 致命）过滤。级别以颜色编码。开始/停止 控制流。停止时保留您在屏幕上捕获的内容，以您可以向后滚动查看。

文件

文件 选项卡是设备的文件管理器。浏览目录（从 `/sdcard` 开始），下载 文件到您的计算机，上传 文件到设备，并 重命名、删除 或创建文件夹。对于从设备提取捕获或诊断文件，或将配置推送到设备非常有用。

手势录制

切换 录制，在屏幕上执行点击/滑动序列，控制台会发出等效的 adb input 行。将它们粘贴到文件夹脚本中，以将手动 UI 流转化为可重复的测试。

USB 调制解调器控制台

USB 蜂窝调制解调器（Quectel EP06 等）在车队中显示为 调制解调器，并打开蜂窝控制台而不是屏幕。代理通过其串行（AT）端口将 AT 命令中继到调制解调器。它将每个命令和响应记录到 终端 选项卡作为审计跟踪。

选项卡	功能
状态	一次性读取型号/固件/IMEI/IMSI/SIM、信号（CSQ + 每个 RAT QCSQ）、运营商、EPS 注册、附加、IMS、IP、APN、DNS/PCO
操作	设置 APN（预设或自定义，带有 **PDP / IP** 类型）、附加/分离数据、显示 IP + DNS、ping、发送短信、无线电（飞行模式/重启）
网络	运营商扫描（`AT+COPS=?`）和服务/邻居小区测量（`AT+QENG`）→ EARFCN / PCI / 频段 / RSRP / RSRQ / SINR 表
小区锁定	锁定特定 **EARFCN (+PCI)**（`AT+QNWLOCK`）、频段锁定（`AT+QCFG="band"`）、RAT 优先级，或释放回自动
呼叫	拨打/接听/挂断，`AT+CLCC` 呼叫表，以及启用/禁用 **VoLTE** 控制（`AT+QCFG="ims"`）
短信	读取收件箱（`AT+CMGL`）、删除和发送
事件	启用相关的 URC，并将其轮询到带时间戳的日志中（注册/呼叫/信号/新短信变化）
终端	原始 AT 输入以及完整的请求/响应日志

完整的 AT 命令参考以及真实的 EP06 响应在 **modem-at-commands.md** 中。

> **VoLTE**：EP06 仅支持 VoLTE/IMS 语音。*□□ VoLTE* 设置 `AT+QCFG="ims",1`；可能需要 `AT+CFUN=1,1` 重启以（去）注册 IMS，并且只有在网络 + SIM 提供它并选择正确的运营商 MBN 时才会注册。

旧 **Android** □密狗（屏幕捕获模式）

□宜的 ~$10 LTE “MiFi” 加密狗（例如 UZ801，Qualcomm msm8916）运行 **Android 4.4 (API 19)**，这对于实时屏幕查看来说太旧。这些设备回退到 屏幕捕获 控制台：代理轮询 `adb screencap` 获取帧（每秒几帧，因为 `screencap` 本身是该硬件的瓶颈），并注入 `adb input` 进行控制。您可以获得点击以进行点击、输入以输入文本的视图。虽然不是流畅的视频，但足以进行操作���

代理在主机端平滑处理这些加密狗的粗糙边缘：

- **ADB** 解锁：它们以 RNDIS 模式出厂。一个由 udev 触发的服务 `curl` 加密狗的 `usbdebug.html` 将其切换到 ADB 模式。请参见 agent/host-setup/mifi-dongle。
- 自动英语：它们以中文出厂。代理在第一次看到 API-<21 设备时将 `persist.sys.language` 设置为 `en-US`（通过 `OMNIWEB_DONGLE_AUTO_ENGLISH=0` 禁用）。

脚本

测试是运行在 代理主机 上的 bash 脚本（因此可以使用主机工具如 `grep`/`awk`），并通过 ADB 针对设备进行。分为两种类型：

- 文件夹脚本：出现在库中、扇出运行器和调度程序的健康检查。有些只与设备一起运行（设备连接、VoLTE 注册、报告信号强度）。其他则接受可选输入（`@param`）。Ping 测试接受主机和计数。数据吞吐量测试接受 URL。连接性和语音测试（Ping、数据吞吐量、发送短信、拨打电话）是文件夹脚本，因此您可以将它们安排在调度程序中，也可以手动运行。两个飞机模式恢复测试确认设备在失去无线电后恢复。飞机模式切换 → **Ping** 恢复 打开飞行模式，然后关闭，等待数据重新连接，然后 ping。飞机模式切换 → **IMS** 恢复 也是如此，然后确��� VoLTE 重新注册。
- 内置工具：应用打开快捷方式（拨号、短信、设置）和控制台快速操作中的普通飞行模式切换。每个操作执行一个 UI 操作，没有通过或失败的结果，因此不在库或调度程序中。

脚本通过 退出代码 报告其结果：`0` 为通过，其他任何值为失败。其捕获的输出显示在结果表中。

定期测试

定期测试在脚本目录中的 `schedules.json` 中以声明方式定义。该文件在每个周期重新读取，因此编辑会立即生效，无需重启。每个条目在指定的时间间隔内针对其目标设备运行一个文件夹脚本。

配置

```
{
  "schedules": [
    {
      "name": "VoLTE 注册",
      "script": "volte_registration.sh",
      "interval_seconds": 120,
      "serials": [],
      "enabled": true
    }
  ]
}
```

参数	类型	必需	默认	描述
`name`	字符串	是	-	调度的唯一标签。作为导出指标的 `schedule` 标签出现。
`script`	字符串	是	-	要运行的脚本目录中的文件夹脚本的文件名。
`interval_seconds`	整数	否	300	运行脚本的频率，以秒为单位。最小为 30。
`serials`	列表	否	`[]`	目标设备的序列号。空列表表示所有当前连接的设备，因此调度会自动跟随任何插入的手机。
`params`	对象	否	`{}`	声明 `@param` 值的脚本的输入。键是参数名称。例如，Ping 测试接受 `host` 和 `count`。
`enabled`	布尔值	否	true	调度是否处于活动状态。设置为 `false` 以暂停而不删除条目。
`exclusive`	布尔值	否	false	在该测试持续期间保留手机。当独占测试运行时，设备上不会启动其他调度测试，独占测试本身在开始之前会等待设备空闲。将其用于破坏性测试——例如飞机模式切换或重启——这可能会破坏同时在同一手机上运行的其他测试（例如 VoLTE 呼叫）。

示例：跨站点的 **VoLTE** 检查

```
{
  "name": "VoLTE Registration",
  "script": "volte_registration.sh",
  "interval_seconds": 120,
  "serials": [],
  "enabled": true
}
```

工作原理：调度程序每 120 秒运行一次 `volte_registration.sh`，针对每个连接的手机。该脚本检查设备是否在 LTE 上以 VoPS（语音覆盖 PS）支持进行语音注册（`IN_SERVICE`），如果 VoLTE 已注册，则退出 `0`。结果成为每个设备的 Prometheus 指标。

用例：持续证明某个站点的真实手机可以注册 VoLTE，并在无法注册时发出警报。

示例：对每部手机进行 **Ping** 测试

```
{
  "name": "Ping Test",
  "script": "ping_test.sh",
  "interval_seconds": 120,
  "serials": [],
  "params": { "host": "8.8.8.8", "count": "5" },
  "enabled": true
}
```

工作原理：调度程序每 120 秒在每个连接的手机上运行 `ping_test.sh`。`params` 提供脚本输入。该脚本对 `8.8.8.8` 进行五次 ping 测试，如果收到回复则退出 `0`。更改 `host` 以测试特定目标。

用例：证明某个站点的真实手机具有正常的数据连接，并在数��包丢失时发出警报。

在手机使用时自动暂停

打开手机的实时屏幕会暂停 该手机 的计划测试。对正在被某人观看和点击的手机进行测试会与他们争夺屏幕，并记录一个无意义的通过或失败，因此调度程序会跳过任何有实时查看者的手机，并在视图关闭后立即恢复。

- 暂停是针对每部手机的。调度目标的其他手机会继续按正常间隔运行。
- 跳过的运行不会计入完成：一旦手机空闲，调度将在下一个周期触发，而不是等待完整的间隔。
- 当屏幕打开时，已经在运行的测试将继续完成。

关闭手机视图（或导航离开）后，测试将在大约一分钟内恢复。如果浏览器在未正常关闭的情况下消失，暂停将自动解除。
立即运行 不受影响——显式请求的运行始终会进行。

手机的计划测试标签在暂停生效时会显示横幅，车队会标记 正在使用 的手机及其持有者。

指标

中央 OmniWeb 在 /api/android/metrics 以 Prometheus 格式公开每个计划测试的最新结果，按设备分类。 Prometheus 将其作为 android_device_tests 作业抓取（由监控角色自动配置）。

指标： omniweb_android_test_pass 类型： Gauge 描述：最近一次计划运行的结果：1 表示通过，0 表示失败标签：

phone：设备型号（例如 SM-A536E）
serial：设备序列号
site：代理的站点标签（例如 Cell Site 12）
agent：设备连接的代理主机
script：运行的脚本
schedule：计划名称
status：运行结果（passed，failed，timeout 或 error）

伴随的指标共享相同的标签：

指标 描述

omniweb_android_test_duration_ms 最近一次运行的持续时间，以毫秒为单位

omniweb_android_test_last_run_timestamp 最近一次运行的 Unix 时间

一个单独的指标报告当前被查看者持有的手机，因此一个过时警报可以区分故意暂停的手机和故障测试：

指标 描述 标签

omniweb_android_device_in_use

当有人打开手机屏幕时为 1（其
计划测试被暂停），否则为 0

serial，phone，
site，agent

示例查询：

```
# 当前未能通过 VoLTE 注册的手机
omniweb_android_test_pass{schedule="VoLTE Registration"} == 0

# 按站点分组的失败测试
count by (site) (omniweb_android_test_pass == 0)

# 最近没有运行的测试（过时的代理或设备离线）
time() - omniweb_android_test_last_run_timestamp > 600

# 同上，忽略当前有人打开的手机（这些测试被暂停）
(time() - omniweb_android_test_last_run_timestamp > 600)
  unless on (serial) omniweb_android_device_in_use == 1

# 当前正在使用的手机
omniweb_android_device_in_use == 1
```

Grafana 仪表板

监控角色提供一个 手机 **/** 设备测试 仪表板（Grafana 文件夹 **Devices**）。它读取上述指标，并显示每部手机和计划：

- 通过或失败状态的时间线，
- 每部手机和测试的最新结果，
- 测试新鲜度（自上次运行以来的时间，以捕捉停滞的代理），
- 随时间变化的运行持续时间。

在顶部按站点、手机或测试过滤仪表板。仪表板会自动配置。请参见 Grafana。

故障排除

手机未出现在车队中

症状：设备已在某个站点插入，但未在测试设备下列出。

可能原因：

- 手机未在代理主机上授权 ADB

- 代理未运行或无法连接中央
- 手机处于离线/未授权的 ADB 状态
- 中央测试设备服务未运行（测试设备由其自己的专用后端服务提供，与主请求池分开）

解决方案：

1. 确认手机在代理主机的 ADB 中显示为 `device`（而不是 `unauthorized`/`offline`），如有需要，请在手机上接受 RSA 提示。
2. 检查代理服务是否正在运行，以及其配置的中央 URL 和令牌是否正确。
3. 在中央确认测试设备服务正在运行，并且网关将 `/api/android/*` 路由到该服务。如果代理已注册但车队为空，则此服务通常是原因。
4. 验证手机的 USB 连接；如果显示为离线，请重新插入电缆。

控制台屏幕停留在“连接中”

症状：设备控制台打开，但屏幕从未出现，而其余 UI（车队列表、设备详细信息、输入）正常工作，设备显示为 在线。

可能原因：

- 浏览器网络与代理主机之间的 UDP 被阻止（实时视频流 直接 从浏览器 → 代理主机，而不是通过服务器，这是最常见的原因）
- 代理无法在该手机上启动屏幕捕获

这 不是 SSL 或 MTU 问题：TLS 已证明正常工作（UI 已加载），而在 MTU 问题下，视频会连接然后 □ 断开，而不是从未启动。明显的迹象是设备在车队中显示为 在线，但其实时视图无法启动。

解决方案：

1. 确认浏览器网络可以通过 **UDP**（视频路径）访问代理主机。这通常意味着防火���/VLAN 规则允许操作员的子网通过 UDP 访问测试主机。请参见 网络要求 以获取请求的确切规则以及如何确认修复。
2. 检查代理日志以获取屏幕捕获错误。一些手机无法通过 ADB 捕获其屏幕。

VoLTE / 信号检查报告“不可读取”

症状：VoLTE 或信号脚本因无法读取电话状态而失败。

可能原因：

- 手机限制了对电话状态的特权访问

解决方案：

1. 使用能够将电话状态暴露给 ADB 的测试手机。供应商锁定的消费设备可能在没有特权访问的情况下隐藏此信息。

测试设备：网络要求

在测试设备中实时查看电话使用两个独立的网络路径。了解这种分割以□在防火墙和VLAN之间正常工作。此分割还帮助您诊断最常见的症状，即控制台永远停留在**“连接中……”**。

← 返回测试设备

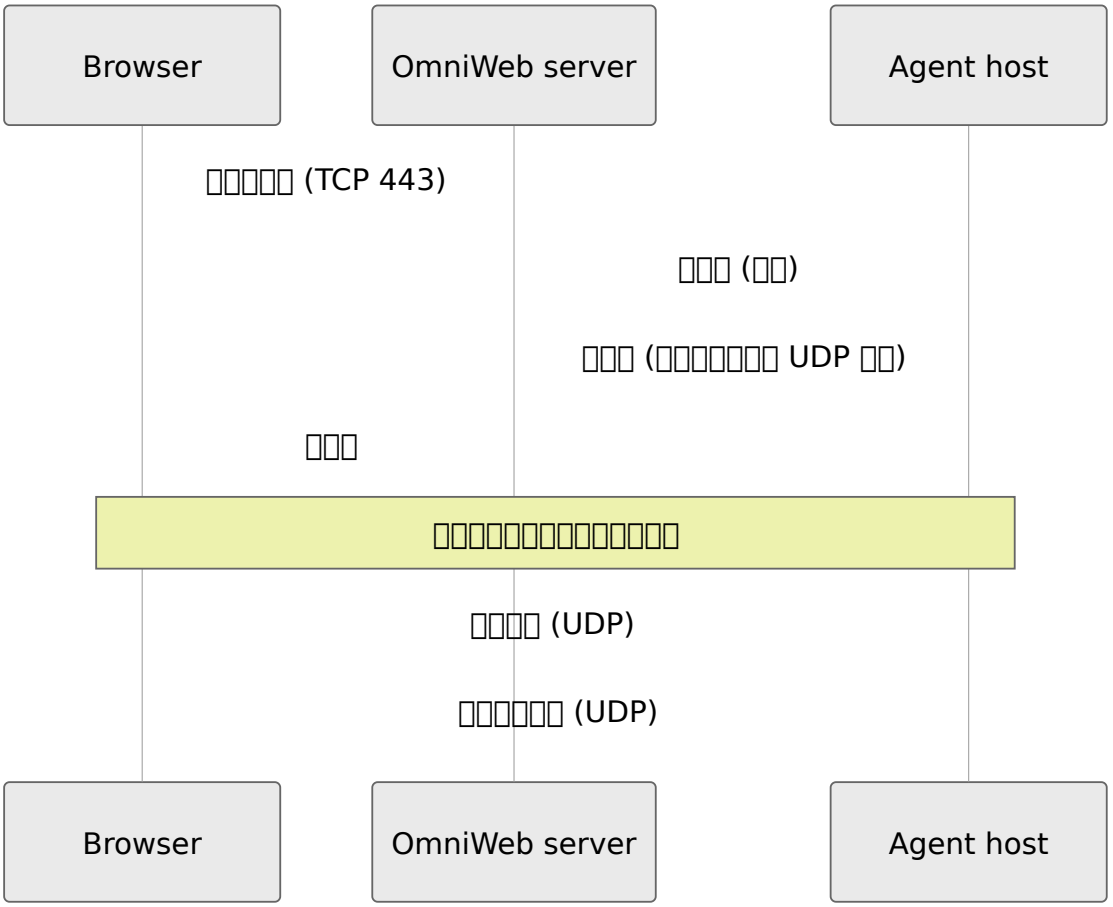
两条路径

路径	承载内容	方向	传输	终端
控制平面	网络用户界面、登录、设备列表、远程输入、测试结果和实时查看的呼叫设置（“信令”）	浏览器 → OmniWeb 服务器	**TCP 443 (HTTPS)**	OmniWeb 服务器
媒体平面	实时屏幕视频	浏览器 ⇄ 代理主机（电话插入的测试台）	**UDP** (WebRTC)	代理主机，不是服务器

关键点：实时视频不通过 **OmniWeb** 服务器传输。一旦服务器建立了连接，视频流直接在操作员的浏览器和代理主机之间通过 UDP 传输。如果网络允许浏览���访问□□□但无法访问□□□□，则加载用户界面，显示设备列表，然后停留在“连接中……”上。

为什么媒体路径是直接的

实时屏幕视频通过**WebRTC over UDP**进行点对点传输，因此它比通过中央服务器的 TCP 中继在远程基站的高延迟和丢包链路中更具生存能力。权衡是操作员的浏览器需要直接的 **UDP** 路径到代理主机。中间没有媒体中继可以回退。


Browser
OmniWeb server
Agent host
□□□□□□ (TCP 443)
□□□ (□□)
□□□ (□□□□□□□□ UDP □□)
□□□
□□□□□□□□□□□□□□□□□□
□□□□ (UDP)
□□□□□□ (UDP)
Browser
OmniWeb server
Agent host

□□□□

□□□□□□□□□□□□□□□□□□

控制平面（通常已经开放）

字段	值
操作	允许（有状态）
协议	TCP
源	操作员 / 客户端 VLAN(s)
目的地	OmniWeb 服务器
目的地端口	`443`

如果 OmniWeb 用户界面能够加载，这条路径已经开放。无需更改。

媒体平面（通常缺失的那条）

字段	值
操作	允许（有状态，因此返回视频自动允许）
协议	**UDP**
源	操作员 / 客户端 VLAN(s)，浏览器运行的地方
目的地	设备测试台主机子网（代理主机），例如 `10.0.20.0/24`
目的地端口	**`32768–60999`**（代理从中提取媒体端口的默认 Linux 短暂范围）

浏览器始终发起媒体连接，因此在 `client → agent host` 的 UDP 上的有状态允许也自动允许代理的返回视频。没有 STUN/TURN 或其他端口涉及。

> 不要更改端口 **443**。信令已经通过控制平面传输。只有到代理主机的 UDP 媒体路径需要开放。

推荐：固定媒体端口范围

打开整个短暂范围（`32768–60999`）是比较宽泛的。您可以配置代理从一个小的固定范围中提取其媒体端口。这将防火墙规则缩小到一个整齐的块：

字段	值
操作	允许（有状态）
协议	UDP
源	操作员 / 客户端 VLAN(s)
目的地	设备测试台主机子网
目的地端口	**`50000–50100`**（固定范围）

这是交给网络团队的首选形式。100个端口到一个子网比整个短暂范围更容易批准和审计。固定范围在代理主机上设置。与维护测试台的人员协调确切范围，以□防火墙规则和代理配置匹配。

识别问题

症状：设备控制台打开，但屏幕从未出现。它无限期停留在**“连接中……”**。其他一切正常：舰队列表、设备详细信息，甚至远程输入设置。

这几乎总是媒体平面 UDP 路径被阻塞。它不是 TLS/证书问题，也不是 MTU 问题：

怀疑原因	为什么不是这个	如果是的话您实际会看到什么
SSL / 证书	用户界面、登录、设备列表和信令都通过 HTTPS 成功，因此 TLS 显然在工作	页面本身将无法加载，或显示证书警告
MTU / 分片	MTU 仅在视频数据包流动时才重要。在这里没有视频 ��据包到达	视频会连接，然后停滞或撕裂，而不是停留在“连接中……”
代理 / 电话故障	设备在舰队中显示为在线，并有实时电池/操作员数据	设备会在舰队中缺失，或标记为离线
UDP 路径被阻塞 ✓	浏览器可以访问服务器（用户界面加载）但无法通过 UDP 访问代理主机	永久“连接中……”，正是这种症状

一个有用的迹象：设备图块显示电话为在线（因此代理和电话是健康的，服务器可以看到它们），但实时查看单独不会启动。该组合明确指向媒体平面防火墙路径。

□□□□

□□□

网络拓扑与单一视图

OmniWeb 的拓扑视图是整个网络的“单一视图”入口。它们展示了元素之间的连接，哪些元素已部署，并允许您直接从地图上的节点跳转到该元素的工作区。

← 返回操作指南

拓扑视图

着陆/拓扑页面通过四个域选项卡展示网络。每个选项卡都是相关元素及其接口的交互式地图。

EPC □□□UE → eNB → MME → SGW-C → PGW-C → UPF□□□ DRA □□□□□□□ HSS□□□□□ □□□□□□□□□□□□□□

选项卡	显示的元素
核心 **(EPC)**	UE → eNB → MME → SGW-C → PGW-C → UPF; DRA ↔ HSS; OCS; TWAG; RAN 监控
IMS	P-CSCF → I-CSCF → S-CSCF; DRA ↔ HSS; TAS; IMS SMSc → SMSC → SMPP GW; OCS; 权限 (OmniSEP)
CS 核心	BTS → BSC → MSC; STP ↔ HLR / CAMEL GW / IP-SM-GW; HSS; SMSC; OCS
5G 核心	gNB → AMF → SMF → UPF; NRF, SCP, AUSF, UDM, UDR, PCF; CHF → OCS; NSSF; BSF

阅读地图

- 活动元素 是指在 `omniweb.json` 中声明的实例。它们显示彩色边框和一个显示实例数量的徽章。点击一个元素会打开一个弹出窗口，提供每个实例的直接链接。您可以从拓扑直接导航到元素的页面。
- 未配置元素 显示为灰色，因此地图还可以作为已部署和未部署的快速清单。
- 连接 表示元素之间的接口（例如 SIP、Diameter、PFCP、GTP-C、SS7），区分信令类型。

这使得拓扑页面成为自然的起点：查看网络的形状，识别已部署的内容，并深入了解。

元素级拓扑

某些元素还提供自己的专注拓扑视图。例如，**PGW-C → 拓扑** 选项卡显示该节点与其 SGW-C、UPF 和 Diameter 对等体的关系，并注释实时会话计数和利用率。这为该元素的邻域提供了本地化的单一视图。

PGW-C □□□SGW-C□UPF □ Diameter □□□□□□□□□□□□□□□□□□

主机列表与基础设施

除了网络功能本身，主机列表 页面是运行它们的 *□□□□* 的单一视图。它按类别列出所有基础设施主机，每个主机都有直接链接到其 Web UI:

类别	示例
监控	Grafana, Prometheus, Loki
SIP 捕获	Homer Web UI
计费	OCS Web UI
DNS	DNS 服务器
虚拟化	Proxmox 虚拟机监控台
带外管理	iDRAC 服务器管理
路由器	MikroTik WebFig, Peplink
微波	SAF, Ubiquiti AirFiber 链接
NAS	Synology DSM

□□ Web UI□Grafana□Prometheus□Loki□□□ API □□□

□□□□□□□□□□□□□□□□□□□

TWAG: 受信 WLAN 访问网关
TWAG（受信 WLAN 访问网关）将受信的 Wi‑Fi 访问引入移动核心。它通过 Diameter 对 AAA/HSS 进行 EAP‑AKA/AKA′ 认证 Wi‑Fi 设备，通过 DHCP 为每个经过认证的客户端分配一个 IP 地址，并通过 GTP 隧道将其数据锚定回数据包核心到 PGW。因此，在 Wi‑Fi 上的订阅者享有与蜂窝网络相同的 APN、策略和计费。它的仪表板是查看谁已连接、 Diameter 和 GTP 路径是否健康以及清除单个会话的地方。

← 操作指南

仪表板是一个每个实例的元素页面，当 TWAG 在站点的库存中运行时可以从侧边栏访问。所有流量通过 OmniWeb 后端代理到 TWAG 的 API，因此它保持在单一的经过身份验证的网关后面。它被组织成多个选项卡。

概述

着陆选项卡是一个单屏健康读取：活动和总 会话、连接/断开连接的 Diameter 对等体、接受的 订阅者、接入点 数量、DHCP 租约计数、GTP 隧道状态及其 PGW 地址、正在使用的 认证模式（例如 EAP‑AKA）、进出 流量、正常运行时间，以及一个实时的 最近活动认证和会话开始/停止的动态信息流。

会话

每个经过认证的 Wi‑Fi 会话，每行显示订阅者 身份（网络接入标识符）、状态、分配的 IP、客户端 MAC、SSID、服务 NAS IP、会话 持续时间 和 进出字节。操作员可以 删除 会话以强制断开客户端，例如清除卡住或表现不佳的设备。

接入点

当前连接到网关的 WLAN 接入点（NAS 设备）。每个接入点可以在接入点退役或需要清除时单独 删除。

计费

TWAG 记录的计费会话：为经过认证的客户端生成的使用记录。可以 删除 单个计费会话。

Diameter

与 AAA/HSS 的 Diameter 对等连接，承载认证，显示连接和断开连接的计数。此选项卡还提供 Diameter 测试。它发送测试多媒体认证请求（MAR）以确认到 AAA/HSS 的认证路径是否正常，这是在认证失败时证明 Diameter 连接性的最快方法。

DHCP

TWAG 已向 Wi-Fi 客户端发放的 DHCP 租约，包括每个租约的地址、客户端和租约状态，以□您确认客户端是否被分配地址，并查看池中使用了多少。

日志

日志选项卡实时跟踪 TWAG 的日志输出，以□在不离开 OmniWeb 的情况下进行单个网关的故障排除。

操作

每个操作首先要求确认：

- 删除会话：强制断开一个经过认证的 Wi-Fi 会话（会话选项卡，每行）。
- 删除接入点：清除单个接入点 / NAS 条目（接入点选项卡，每行）。
- 删除计费会话：删除单个计费记录（计费选项卡，每行）。
- **Diameter** 测试：发送测试 MAR 以验证到 AAA/HSS 的 Diameter 路径（Diameter 选项卡）。

相关

PGW 通过 GTP 锚定 TWAG 的用户平面。请参阅数据包核心元素。 HSS 保存 TWAG 的 Diameter 请求所解析的订阅者认证数据。 ePDG：Wi‑Fi 通话的非受信 Wi‑Fi 对应物。

UPF: 用户平面功能

UPF（用户平面功能）是移动核心的分组转发节点。它承载每个用户的实际流量：它接收来自接入网络的 GTP-U 隧道（在 EPC 中为 S1-U），转发数据网络的进出数据包，应用每流的 QoS 和流量计量，并在设备空闲时缓冲下行数据包。它没有自己的逻辑。控制平面（在 EPC 中为通过 **Sxa** 的 **SGW-C**，或在 5G 核心中通过 **N4** 的 **SMF**）完全通过 **PFCP** 对其进行编程。控制平面安装描述 UPF 如何处理每个会话流量的分组检测、转发、QoS 和使用报告规则。Omnitouch 的 **OmniUPF** 将转发路径实现为内核中的 **eBPF/XDP** 数据平面，因此控制平面安装的规则变成 eBPF 映射中的条目，XDP 程序在每个数据包上进行查询。OmniWeb 显示 UPF 的 PFCP 关联和会话、实时 eBPF 映射内容、数据平面统计信息、路由、下行缓冲区、围墙花园状态和配置。它从同一页面访问 Grafana 仪表板上的吞吐量和趋势图表。

← 操作指南

UPF 是一个每实例元素页面，可以通过侧边栏访问，当在网站的库存中���行时，可以选择多个已部署的实例，并查看聚合状态的舰队视图。所有流量都通过 OmniWeb 后端代理到 UPF 的 API，因此它保持在单一的经过身份验证的网关后面。页面头部的文档链接（上下文帮助按钮）打开此页面。它组织为多个选项卡。

舰队和实例选择

当一个站点运行多个 UPF 时，舰队视图一目了然地列出每个实例及其健康状况。这是确认整个用户平面正常运行的最快方式，然后再深入到一个节点。

从任何选项卡，页面头部的 实例选择器 切换页面读取的 UPF。下面的所有内容（会话、关联、eBPF 映射、统计信息）都与所选实例相关，因此您只需选择一次节点，整个页面将随之更新。

概述

UPF 的单屏健康读取：其 健康 状态、与控制平面对等体保持的 **PFCP** 关联 数量、这些对等体的总 活动会话 数量，以及 **XDP** 动作计数器：数据平面已传递、丢弃、重���向、传输或中止的数据包数量，这是确认流量实际流动的最快方式。在其下方，每个 **PFCP** 对等体列出其关联状态、会话计数和任何丢失的心跳，**eBPF** 映射大小 显示 PDR、FAR、QER 和 URR 映射的容量以及最大会话计数。搜索框可以通过 **UE IP** 或 **TEID** 直接跳转到会话，节点报告 操作向第一个活动的控制平面对等体发送 PFCP 节点报告请求。

会话

每个 PFCP 会话：控制平面已安装的每承载 / 每 PDU 会话用户平面状态。每行按其 本地和远程 SEID 键入，并显示会话的 IMSI、APN/DNN、关联（哪个控制平面对等体拥有它）以及它携带的 分组检测、转发动作、QoS 执行和 使用报告 规则的计数。按 UE IP 或 TEID 搜索以查找为特定设备或隧道提供服务的会话。

当部署多个 UPF 时，舰队视图中的同一选项卡在一个表中列出所有 PFCP 会话，每行显示承载 UPF。UE IP 和 TEID 在每个 UPF 上进行搜索；IMSI 和 APN/DNN 在综合列表中匹配。打开一行将转到该会话在其自身实例上的详细信息。无法访问的 UPF 在表格上方命名，因此短列表不会被误认为是空闲用户平面。

会话详细信息

打开会话显示其完整的规则状态。会话规则映射 描绘每个 分组检测规则 **(PDR)** 如何引用 转发动作规则 **(FAR)**、**QoS** 执行规则 **(QER)** 和 使用报告规则 **(URR)**。单击任何节点以突出显示仅与其连接的规则，以□您可以追踪单个流在数据平面中的路径。在映射下方，四个表提供详细信息：

- 分组检测规则 **(PDR)**：UPF 如何分类传入数据包。这涵盖方向（上行 / 下行）、它们匹配的 UE IP 或入站 TEID、SDF 过滤器（协议和端口范围），以及它们解析到的 FAR、QER 和 URR。
- 转发动作规则 **(FAR)**：匹配数据包的处理方式。动作为 转发、丢弃、缓冲 或 通知 **CP**，包括出站 GTP-U 隧道的详细信息（远程 IP 和 TEID）及网络实例。您可以就地编辑 FAR。
- **QoS** 执行规则 **(QER)**：每流的 QoS。这涵盖 **QFI**、上行和下行 门 状态（打开 / 关闭）以及 最大 和 ��证比特率。您可以就地编辑 QER。
- 使用报告规则 **(URR)**：流量计数器。这些是当前和最后报告的上行和下行字节以及报告序列号，这是 UPF 反馈给控制平面的计费和配额信息。

从会话头部，您还可以 激活或移除特定会话的围墙花园重定向（见下面的围墙花园）。

关联

PFCP 关联：UPF 与其控制平面对等体（SGW-C 或 SMF）之间的 Sxa/N4 关系。每行显示对等体的 远程 IP 和端口、会话计数、当前是否 关联、丢失的心跳 数量，以及最后 连接 或 断开 的时间。在这里，您可以确认用户平面和控制平面是否步调一致。您还可以发现一个心跳失效的对等体。

统计信息

数据平面的实时数字。eBPF 映射使用 显示每个映射的满度（会话、PDR、FAR、QER 和 URR），作为使用与容量的条形图，当接近其限制时变为琥珀色和红色，因此您可以在 UPF 开始拒绝会话之前看到它接近其设计容量。XDP 统计信息 列出通过 / 丢弃 / 重定向 / TX / 中止的数据包计数器，指标 部分显示 UPF 的 Prometheus 计数器作为单独的数字。

容量检查读取相同的使用与容量模型。一目了然，您可以判断限制资源是会话表还是某个规则映射。

路由

引导用户流量进出 UPF 的路由。活动 **UE IP** 路由 表列出 UPF 当前持有的分配 UE IP 池的路由，同步路由 操作将其与数据平面进行协调。在其下方，**FRR** 控制台 提供一个上下文 vtysh 终端，与 UPF 的路由守护进程进行交互。要检查路由状态，输入 `show` 命令（例如 `show ip route` 或 `show ip ospf neighbor`），支持标签补全和命令历史。要进行更改，请切换到 配置模式。这就是 UPF 如何在不离开 OmniWeb 的情况下将其 UE 池广告到周围网络。

缓冲区

下行数据包缓冲区。当下行数据到达空闲设备（没有活动隧道）时，数据平面将这些数据包���存在相关的 FAR 下，并请求控制平面对设备进行寻呼。一旦隧道重新建立，UPF 将刷新缓冲的数据包（这是 下行数据通知 的用户平面部分）。该选项卡显示 总缓冲数据包 和 总 **FAR**，持有数据包的 每个 **FAR** 和 总 缓冲限制，以及 按 **FAR ID** 查找 以查看特定 FAR 持有多少数据包。缓冲区可以 单独刷新 或 批量清除。

eBPF 映射

直接浏览 UPF 的 eBPF 映射。这些是 XDP 程序为每个数据包查询的原始内核侧条目，分为多个选项卡：

上行 PDR：按入站 TEID 键入，将隧道映射到其 PDR 和 FAR。
下行 PDR：按 UE IP 键入，将用户的下行流量映射到其 PDR 和 FAR。
FAR：转发动作，带有解码的动作、远程 IP、出站 TEID 和外部头创建。
QER：QoS 条目，带有 QFI、门状态和比特率限制。
URR：使用计数器，带有当前和最后报告的上行/下行流量。

单击任何行以 编辑原始映射条目，这是一个低级故障排除和修复工具。PFCP 通常完全驱动映射，因此您手动编辑条目用于诊断，而非常规操作。

配置

UPF 配置的只读视图：其 网络 身份（节点 ID、PFCP 地址和端口、API 端口、N3 和 N9 地址）、已启用的 功能（FTUP、 UEIP、路由管理器及其类型，以及 XDP 附加模式：本地、通用或卸载）、PFCP 心跳 间隔、超时和重试设置，以及 数据平面 N3/N9 地址。原始 JSON 切换显示完整的配置文档以供支持。在这里，您可以确认 UPF 的尺寸和地址是否如预期。

诊断

从 UPF 节点向目标主机运行 ping。输入目标和数据包计数，原始 ping 输出将返回成功/失败的判决。这是确认 UPF 从数据网络（例如到 DNS 服务器或上游网关）具有可达性的快速方法，而无需进入节点。

□□□□

□□□

日志

日志 选项卡跟踪 UPF 的实时日志输出，以□在不离开 OmniWeb 的情况下故障排除单个实例。

监控仪表板

UPF 的吞吐量、每接口数据包速率、会话计数趋势和其他时间序列以 Grafana 仪表板的形式呈现，可以从元素页面访问。OmniWeb 不会原生重复这些图表。

相关

- **SGW-C**：通过 **Sxa/PFCP** 编程此 UPF 的 EPC 控制对等体（作为 SGW-U）并在 **S1-U / N3** 上转发流量。
- **PGW-C / SMF**：锚定 PDN 连接，并作为 SMF，通过 **N4/PFCP** 编程 5G 用户平面。
- **MME**：驱动承载设置，最终安装此处看到的会话。
- **SCEF**：通过控制平面承载小的非 IP 负载，并故意绕过此用户平面。
- 操作指南：返回元素索引。