UZ801 LTE MiFi dongle — Habilitação automática do ADB (lado do host)

Dongles Qualcomm LTE MiFi baratos de ~$10 (`05c6:90b6`, "Android"/UZ801, msm8916) inicializam em **modo RNDIS** com uma interface web em `http://192.168.100.1`. Ao acessar `http://192.168.100.1/usbdebug.html`, eles são convertidos para **modo ADB** (e já iniciam como root). Ref: https://nickvsnetworking.com/adventures-with-a-10-lte-mifi-dongle/

O passo de habilitação deve ser executado no **host USB** (o hipervisor Proxmox), porque apenas o host possui o link RNDIS para `192.168.100.1` — o agente de telefone OmniWeb executa no LXC não privilegiado (CT 102) e alcança o dongle apenas como um dispositivo USB uma vez que está em modo ADB. Portanto, esta automação é udev + systemd do lado do host, não código do agente.

Arquivos

- `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
```

Fluxo: dongle conectado (RNDIS) → udev é acionado → `mifi-adb-enable.service` → script ativa a iface RNDIS, faz curl em `usbdebug.html` → dongle reinicializa em modo ADB → reenumera com a interface ADB → a regra udev CT-102 (abaixo) entrega o nó para o contêiner → o `adb` do agente o vê. Na reenumeração em modo adb, o script é executado novamente, detecta a interface ADB (`ff/42/01`) e sai — sem loop.

Alteração udev de passthrough USB do CT-102 (REQUERIDO)

O VID Qualcomm do dongle `05c6` deve ser passado para o contêiner, e o grupo **deve ser plugdev (gid do host 100046)**, não root do contêiner, ou o adb do agente (usuário `omniweb-agent`, um membro do plugdev) não poderá abrir o nó. O mesmo se aplica às regras do telefone Android: elas eram `GROUP="100000"` (root do contêiner) que o agente não pode acessar — os dispositivos só funcionavam enquanto o adb mantinha o fd do tempo de enumeração e caíam em cada reenumeração. Corrigido para `GROUP="100046"`.

Em `/etc/udev/rules.d/99-ct102-android.rules`, todas as regras de telefone usam `OWNER="100000", GROUP="100046", MODE="0660"`, além do VID do dongle:

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

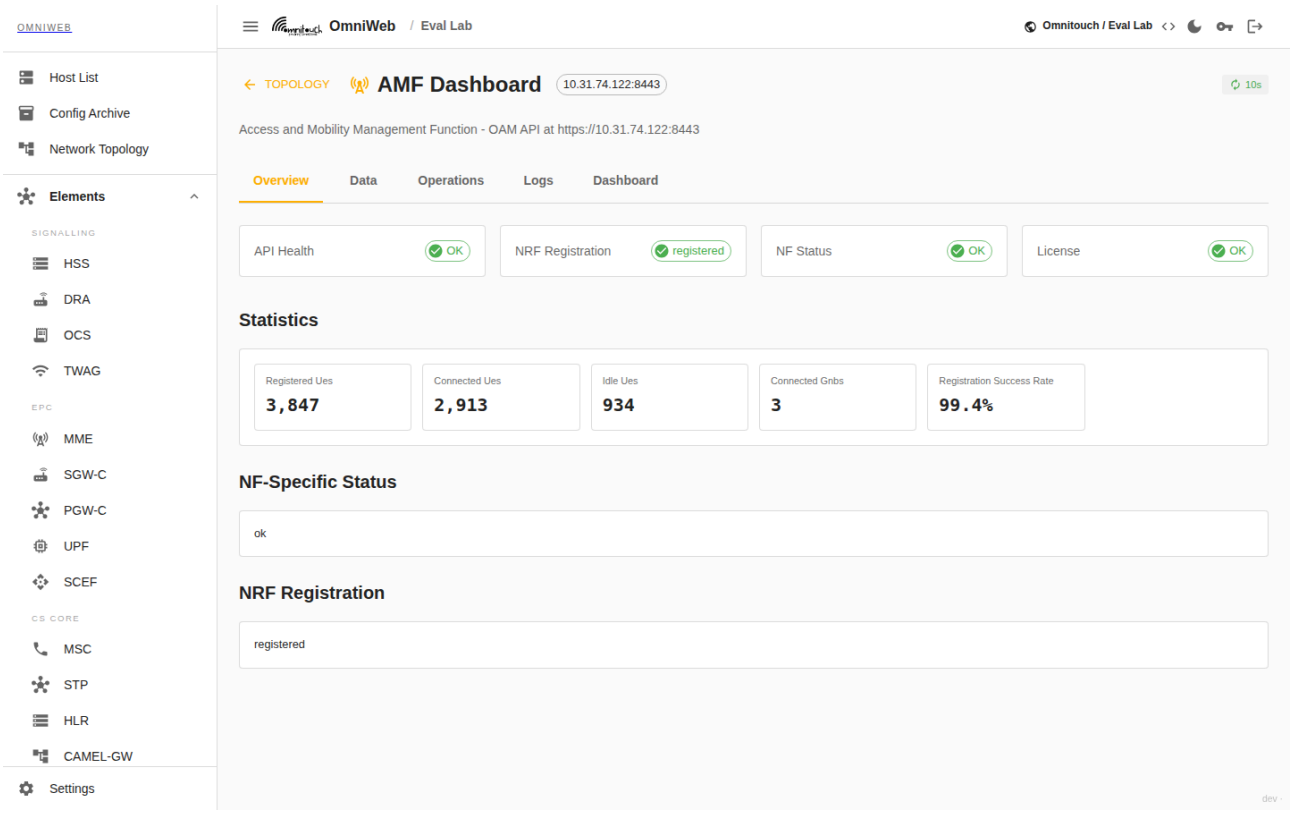
> Essas alterações no host são aplicadas ao vivo no laboratório, mas devem ser codificadas no OmniCore ansible (papel de monitoramento/host) para que sobrevivam a uma reconstrução do host.

AMF: Função de Gerenciamento de Acesso e Mobilidade

O **AMF** é o ponto de ancoragem do plano de controle do núcleo 5G. Ele termina a sinalização **N1** para o UE e a associação **N2** (NGAP) para cada gNodeB. Ele gerencia o registro e a conexão: conecta UEs, mantém-nos acessíveis e os chama quando estão ociosos. Ele possui os **contextos de UE** (um por assinante registrado, indexado por SUPI) e as **associações gNB** (uma por rádio conectado, indexada pela associação SCTP). Ele seleciona o SMF para cada sessão PDU e retransmite solicitações de sessão entre o UE e o SMF. Quando um assinante está na rede, o AMF é o NF que sabe onde ele está e como alcançá-lo.

← Núcleo 5G

No painel



O painel do AMF abre com os quatro cartões de saúde padrão: **Saúde da API**, **Registro NRF** (se o AMF está atualmente registrado com o NRF), **Status NF** e **Licença**. Cada um faz uma consulta em um intervalo. Abaixo deles, ele mostra os dados que o AMF possui:

- **Lista de UEs**: cada contexto de UE que o AMF possui, indexado por SUPI, com seu estado de registro e conexão. Esta é a visão de "quem está conectado agora". Selecione um UE para abrir seu contexto detalhado. O AMF também pode listar as sessões PDU ativas de um UE por SUPI.
- **gNodeBs**: os rádios conectados, uma linha por associação SCTP. A tabela decodifica os valores NGAP brutos em **gNB-ID**, **TAC** (área de rastreamento), **PLMN** e **SST** (tipo de fatia/serviço). Um operador pode, portanto, confirmar quais células estão ativas e quais áreas de rastreamento e fatias elas atendem sem decodificar identificadores manualmente. Selecione uma linha para abrir o gNB detalhado por seu ID de associação SCTP.
- **Estatísticas**: os contadores ao vivo do AMF (UEs registradas, gNBs conectados e volumes de sinalização), para uma leitura rápida sobre carga

e atividade.

- **Modo de Manutenção**: se o AMF está em manutenção. Use-o para drenar ou manter um nó durante trabalhos planejados.
- **Configuração**: a configuração em tempo de execução que o serviço está usando atualmente.

Ações

O painel expõe ações para recuperar de estado preso. O painel confirma cada uma antes de executá-la, uma vez que elas limpam o estado ao vivo:

- **Limpar Todos os Contextos de UE** (em massa): remove todos os contextos de UE do AMF. Use-o como último recurso para recuperar um nó que mantém contextos obsoletos ou corrompidos. Cada UE afetada deve se registrar novamente.
- **Limpar Cache** (em massa): limpa o cache de descoberta de NF do AMF e os caches de UE. Use-o quando o AMF agir com dados de pares ou de pesquisa obsoletos, por exemplo, após um NF ter mudado ou se registrado novamente.
- **Desregistrar** (por UE): desregistra um único UE e limpa seu estado. Use-o para descartar o contexto de um assinante que não será limpo por conta própria, em vez de redefinir todo o nó.

Além dos botões do painel, a API OAM do AMF expõe controles de recuperação mais detalhados que um operador pode acessar através do proxy de backend:

- **Desconectar forçadamente um gNB**: derruba um único gNB por seu ID de associação SCTP. Use-o para limpar uma associação de rádio presa ou com mau funcionamento sem tocar nas outras.
- **Liberar forçadamente uma sessão PDU**: libera uma sessão PDU por seu identificador `supi:psi`. Use-o para descartar uma sessão que está presa do lado do AMF enquanto o UE permanece registrado.
- **Desregistrar ou chamar um UE**: força um UE a desregistrar, ou chama um UE ocioso para trazê-lo de volta à conexão. Use a chamada para testar a acessibilidade. Use a desregistrar forçada para expulsar um UE de forma limpa.

Operações

- **Diagnósticos em tempo de execução** (`/api/oam/diagnostics`): mostra diagnósticos de baixo nível para o serviço em execução.
- **Uso de recursos** (`/api/oam/resources`): relata o uso de memória, processo e agendador em tempo de execução para uma verificação de saúde no nó.
- **Pares** (`/api/oam/peers`): lista os URIs de pares NF configurados e descobertos e as associações SCTP atuais, para que um operador possa ver com quem o AMF se comunica.
- **Cache de descoberta NRF** (`/api/oam/nrf_discovery`): mostra o conteúdo do cache de descoberta: quais instâncias de NF o AMF aprendeu com o NRF.
- **Definir nível de log** (`/api/oam/log_level`): altera o nível de log em tempo de execução (um dos `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar os detalhes enquanto você soluciona problemas.
- **Forçar re-registro NRF** (`/api/oam/nrf/reregister`): re-registra o AMF com o NRF. Use-o para recuperar um registro perdido ou obsoleto.

Relacionados

- SMF: Função de Gerenciamento de Sessão: o AMF seleciona o SMF e retransmite solicitações de sessão PDU para ele.
- UDM: Gerenciamento de Dados Unificado: os dados do assinante que o AMF usa durante o registro.
- AUSF: Função de Servidor de Autenticação: autentica o UE durante o registro em nome do AMF.
- NSSF: Função de Seleção de Fatias de Rede: resolve a seleção de fatias para o AMF.
- ← Núcleo 5G: a visão geral de todos os painéis NF.

AUSF: Função do Servidor de Autenticação

O **AUSF** autentica assinantes em nome do AMF. Quando um UE se conecta, o AMF pede ao AUSF para executar 5G-AKA (ou EAP-AKA') para esse assinante. O AUSF trabalha com o **UDM** para obter o material da chave, deriva a chave âncora que retorna ao AMF e confirma o resultado da autenticação. Ele mantém uma sessão de autenticação ativa para cada autenticação em andamento ou estabelecida, para que um operador possa acompanhar seu progresso e resultado e, se necessário, encerrá-la.

← 5G Core

No painel

O painel do AUSF abre com os cartões de saúde padrão na parte superior (**Saúde da API**, **Registro NRF** (o AUSF está registrado no NRF?), **Status NF**, e **Licença**), cada um fazendo polling em um intervalo. Abaixo deles estão as seções de dados do AUSF, lidas ao vivo de sua API OAM através do proxy OmniWeb:

- **Estatísticas**: os próprios contadores do AUSF (`AUSF Statistics`), que fornecem uma visão em tempo real da atividade de autenticação.
- **Sessões de autenticação ativas do AUSF**: a lista de sessões de autenticação que o AUSF atualmente mantém (`List Active AUSF Authentication Sessions`). Cada linha é identificada pelo seu identificador de sessão, para que um operador possa ver quais autenticações estão em andamento ou estabelecidas à primeira vista.

Ações

Ambas as ações limpam o estado de autenticação e pedem confirmação primeiro, uma vez que são destrutivas:

- **Limpar uma sessão de autenticação específica** (por linha): remove uma única sessão de autenticação pelo seu identificador. Use isso para descartar uma sessão presa ou obsoleta sem perturbar a autenticação de outros assinantes.
- **Limpar Todas as Sessões de Autenticação**: remove todas as sessões de autenticação que o AUSF mantém. Use isso para recuperar o AUSF de um estado preso generalizado. Cada assinante afetado re-autentica em sua próxima tentativa.

Operações

Controles OAM padrão disponíveis no AUSF:

- **Diagnósticos** (`/api/oam/diagnostics`): diagnósticos em tempo de execução para o serviço.
- **Recursos** (`/api/oam/resources`): o uso de recursos do serviço.

- **Forçar re-registro NRF** (`/api/oam/nrf/reregister`): faz o AUSF re-registrar-se no NRF, para se recuperar se seu registro estiver obsoleto.

Relacionados

- AMF: Gerenciamento de Acesso e Mobilidade: solicita autenticação do AUSF para cada UE que se conecta.
- UDM: Gerenciamento de Dados Unificado: fornece o material da chave que o AUSF usa para autenticar um assinante.
- ← 5G Core: a visão geral do painel 5GC e os outros NFs.

BSF: Função de Suporte de Vinculação

O **BSF** registra e resolve a vinculação entre a sessão PDU de um UE e o PCF que a atende. Quando uma sessão é estabelecida, o BSF registra qual PCF está gerenciando a política para essa sessão, com base nos identificadores da sessão: o endereço IP do UE, o DNN e o S-NSSAI. Outros NFs e funções de aplicação consultam o BSF para descobrir o PCF correto para uma determinada sessão de UE, de modo que os pedidos de política cheguem ao PCF que já possui o contexto dessa sessão, em vez de um arbitrário. O BSF mantém uma vinculação por sessão PDU ativa e as expõe, juntamente com estatísticas resumidas, para monitoramento.

← 5G Core

No painel

O painel do BSF abre com os cartões de saúde padrão na parte superior (**Saúde da API**, **Registro do NRF** (o BSF está registrado no NRF?), **Status do NF**, e **Licença**), cada um consultando em um intervalo. Abaixo deles estão as seções de dados do BSF, lidas ao vivo de sua API OAM através do proxy OmniWeb:

- **Vinculações do PCF**: a lista de vinculações ativas que o BSF atualmente possui (`List all PCF bindings with binding ID, UE IP, DNN, S-NSSAI, PCF FQDN/IP`). Cada linha é identificada pelo seu ID de vinculação e mostra o endereço IP do UE, DNN e S-NSSAI que identificam a sessão, juntamente com o FQDN ou IP do PCF que a atende. Isso responde "qual PCF está gerenciando a política para esta sessão de UE?" à primeira vista. Selecione uma vinculação para abrir seus detalhes completos (`Get detailed PCF binding by binding ID`).
- **Estatísticas**: os próprios contadores do BSF (`BSF statistics: total bindings, bindings by DNN`), que fornecem uma visão em tempo real de quantas vinculações estão ativas no total e como elas se dividem por DNN.

Ações

O painel do BSF é orientado para leitura e monitoramento. Ele exibe vinculações e estatísticas para inspeção e não expõe ações destrutivas por linha ou a nível de NF.

Operações

Controles OAM padrão disponíveis no BSF:

- **Forçar re-registro do NRF** (`/api/oam/nrf/reregister`): faz com que o BSF se re-registre no NRF, para recuperar caso seu registro tenha se tornado obsoleto.

Relacionados

- PCF: Controle de Política: o NF para o qual cada vinculação aponta. O BSF é como os consumidores encontram o PCF certo para uma sessão de UE.
- SMF: Gerenciamento de Sessão e funções de aplicação: consumidores Nbsf que registram e consultam vinculações à medida que as sessões entram e saem.
- ← 5G Core: a visão geral do painel 5GC e os outros NFs.

CHF: Função de Cobrança

A **CHF** (Função de Cobrança) fornece cobrança online e offline convergente para o Core 5G. O SMF a consome através da interface N40: à medida que as sessões PDU transportam tráfego, a CHF gerencia cotas de uso, avalia esse uso através do mecanismo de avaliação/cobrança e gera os CDRs (Registros de Dados de Cobrança) que alimentam a faturação e a reconciliação. Seu painel exibe as sessões de cobrança ao vivo, a saúde do link para o mecanismo de avaliação e o histórico de CDRs concluídos. Um operador pode então responder "um assinante está sendo cobrado corretamente, e o mecanismo de avaliação é acessível?" sem sair do OmniWeb.

← Core 5G

No painel

Na parte superior estão os **cartões de saúde** padrão (**Saúde da API**, **Registro NRF** (a CHF está registrada no NRF?), **Status NF** e **Licença**), cada um fazendo polling em um intervalo. Abaixo deles, as seções de dados específicas da CHF se atualizam automaticamente:

- **Sessões de cobrança ativas**: as sessões ao vivo que a CHF está medindo, cada uma mostrando sua referência de cobrança (`chargingDataRef`), o assinante (SUPI), o DNN, o uso acumulado e os timestamps de início/atualização. Este é o conjunto de trabalho de "quem está sendo cobrado agora".
- **Estatísticas**: uma visão resumida do total de sessões, conectividade com o mecanismo de avaliação/cobrança e volume total cobrado.
- **Saúde da conectividade do mecanismo de avaliação**: uma verificação de saúde dedicada que confirma se a CHF pode alcançar o mecanismo de avaliação/cobrança que realiza a avaliação real. Se isso estiver com problemas, a CHF não pode avaliar sessões e a cobrança está em risco.
- **Busca de CDRs concluídos**: uma visão pesquisável sobre os CDRs finalizados, filtrável por SUPI, DNN e intervalo de datas, para confirmar o que a CHF registrou após o fechamento de uma sessão.
- **Configuração**: a configuração em tempo de execução da CHF conforme o serviço a vê atualmente.

Selecione uma sessão para abrir seus detalhes completos por referência de dados de cobrança, que mostra o estado completo de uso e medição para essa sessão.

Ações

- **Abortar uma sessão de cobrança**: termina uma sessão de cobrança em andamento pela sua `chargingDataRef`. Use isso para limpar uma sessão presa ou órfã que o SMF não mantém mais, para que pare de consumir cota e estado de medição.
- **Buscar CDRs**: consulta o histórico de CDRs concluídos por SUPI, DNN e intervalo de datas. Use isso após o término de uma sessão para confirmar qual uso a CHF avaliou e registrou. Suporta consultas de faturamento,

investigação de disputas ou uma verificação pontual de que a CHF escreve a cobrança corretamente.

Operações

- **Definir nível de log**: altera a verbosidade do log da CHF em tempo de execução (emergência, alerta, crítico, erro, aviso, advertência, informação, depuração) para coletar mais detalhes enquanto você investiga um problema de cobrança, e depois retornar ao normal.
- **Forçar re-registro NRF**: faz com que a CHF se registre novamente no NRF. Use isso para recuperar se a CHF saiu do registro e o SMF não consegue mais descobri-la.

Relacionados

- SMF: o consumidor N40 que impulsiona a cobrança à medida que as sessões PDU transportam tráfego.
- PCF: o lado de política do controle de política e cobrança que governa o que a CHF mede.
- O mecanismo de avaliação/cobrança (OCS): o sistema a jusante pelo qual a CHF avalia. O cartão de saúde da conectividade do mecanismo de avaliação reflete o link para ele.
- ← Core 5G: a visão geral de todos os painéis NF.

NRF: Função de Repositório de Rede

Todo o núcleo 5G é construído em torno do registro **NRF**. Na inicialização, cada NF registra seu **perfil NF** no NRF: seu tipo, endereços, PLMNs, os **serviços** que oferece e sua capacidade e prioridade. Em seguida, ele descobre seus pares perguntando ao NRF quem está disponível. O NRF rastreia o **status** de cada instância registrada. Ele mantém **assinaturas de mudança de status**, para que possa informar a uma NF quando um par do qual depende entra ou sai. Ele observa **batimentos cardíacos** para expirar instâncias que param de se reportar. Quando qualquer NF precisa encontrar outra, o NRF é a fonte da verdade sobre o que está ativo e como alcançá-lo.

← Núcleo 5G

No painel

O NRF possui seu próprio painel dedicado, mais rico do que a página padrão da NF porque é ele quem possui o registro que o restante do núcleo descobre. Ele abre com os cartões de saúde padrão: **Saúde da API**, **Registro NRF** (se o próprio NRF está registrado), **Status NF** e **Licença**. Cada um faz uma consulta em um intervalo.

Acima dos dados, ele mostra quatro **cartões de métrica** que resumem o registro: **Tipos de NF**, **total de instâncias**, **registradas** (com uma barra de porcentagem do total) e **serviços** (com a contagem de assinaturas). Abaixo deles estão as principais visualizações do NRF:

- **Instâncias NF registradas**: cada instância registrada, agrupada por **tipo de NF** (AMF, SMF, UDM, PCF, e assim por diante). O painel codifica por cores cada cartão de instância por tipo. O cartão mostra seu status de registro, temporizador de batimento cardíaco, contagem de serviços e PLMN. Selecione uma instância para abrir seu **perfil NF** completo: o registro detalhado que o NRF mantém, com um link **Abrir Painel** para a própria página daquela NF e um botão **Desregistrar**. Esta é a visão "quais NFs estão ativas e todas estão registradas?".
- **Serviços registrados**: uma tabela plana de cada serviço que cada instância anuncia, com suas versões e status. Um operador pode, portanto, ver quais capacidades o núcleo atualmente oferece em todas as NFs.
- **Assinaturas**: as assinaturas de mudança de status da NF atualmente mantidas. Cada uma é um pedido em andamento de uma NF para ser notificada quando o status de um par muda.
- **Estatísticas**: os contadores ao vivo do NRF: total de NFs por tipo, assinaturas e solicitações de descoberta, para uma leitura rápida sobre o tamanho do registro e a atividade de pesquisa.

Ações

O painel expõe ações para gerenciar o registro. O painel confirma cada uma antes de executá-la, uma vez que altera o estado de registro ao vivo:

- **Desregistrar uma instância NF** (por linha): remove o registro de uma instância do NRF. Use-o para limpar um registro obsoleto ou travado de

uma única NF. Essa NF deve então re-registrar antes que outras NFs possam descobri-la novamente.

- **Desregistrar Todas as NFs** (em massa): remove todos os registros do NRF de uma vez. Use-o como último recurso para redefinir um registro que contém entradas obsoletas. Cada NF deve então re-registrar.
- **Remover uma assinatura**: exclui uma assinatura de mudança de status. Use-o para limpar uma assinatura obsoleta ou órfã deixada por uma NF que não a necessita mais.
- **Atualizar um perfil NF**: atualiza o perfil de uma instância registrada (por exemplo, sua capacidade, prioridade ou status). Os operadores podem, portanto, ajustar como o NRF direciona a descoberta para ou longe de uma instância sem uma desregistrar.

Operações

A API OAM do NRF expõe mais controles que um operador pode acessar através do proxy de backend:

- **Diagnósticos em tempo de execução** (`/api/oam/diagnostics`): mostra diagnósticos de baixo nível para o serviço em execução.
- **Uso de recursos** (`/api/oam/resources`): relata o uso de memória, processo e agendador do tempo de execução para uma verificação de saúde no nó.
- **Verificação manual de batimento cardíaco** (`/api/oam/heartbeat`): aciona uma verificação de batimento cardíaco sob demanda para uma instância NF. Ele confirma se a NF ainda está ativa em vez de esperar pelo seu temporizador.
- **Tempo de atividade da NF** (`/api/oam/nf_uptime/{id}`): mostra o tempo de registro de uma instância e há quanto tempo ela está registrada, para confirmar há quanto tempo uma NF está ativa.
- **Definir nível de log** (`/api/oam/log_level`): altera o nível de log em tempo de execução (um dos `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar os detalhes enquanto você soluciona problemas.
- **Forçar re-registro do NRF** (`/api/oam/nrf/reregister`): re-registra o NRF. Use-o para recuperar um auto-registro perdido ou obsoleto.

Relacionados

- AMF: Função de Gerenciamento de Acesso e Mobilidade: registra-se no NRF e descobre seus pares através dele, como todas as NFs abaixo.
- SMF: Função de Gerenciamento de Sessão: descoberto através do NRF para gerenciamento de sessão.
- UDM: Gerenciamento de Dados Unificado: uma das NFs de dados de assinante para as quais o NRF mantém registros.
- PCF: Função de Controle de Políticas: registrado no NRF para descoberta de políticas.
- SCP: Proxy de Comunicação de Serviço: roteia sinalização entre NFs usando os registros e dados de descoberta que o NRF mantém.
- ← Núcleo 5G: a visão geral de todos os painéis NF.

NSSF: Função de Seleção de Fatiamento de Rede

O **NSSF** seleciona a(s) instância(s) de fatiamento de rede e o NSSAI permitido para um UE. Quando o AMF lida com um registro ou um pedido de fatiamento, ele solicita ao NSSF que resolva os S-NSSAIs solicitados pelo UE em relação aos fatiamentos configurados para aquele PLMN. O NSSF mapeia cada um para sua instância de fatiamento de rede (NSI) e para o conjunto de AMF que a atende, e retorna o NSSAI permitido que o UE pode usar. Ele mantém as definições de fatiamento configuradas e rastreia a disponibilidade de NSSAI por AMF para que um operador possa raciocinar e monitorar a seleção de fatiamento.

← 5G Core

No painel

O painel do NSSF é aberto com os cartões de saúde padrão na parte superior (**Saúde da API**, **Registro NRF** (o NSSF está registrado no NRF?), **Status NF**, e **Licença**), cada um fazendo polling em um intervalo. Abaixo deles estão as seções de dados do NSSF, lidas ao vivo de sua API OAM através do proxy OmniWeb:

- **Fatiamentos**: cada S-NSSAI configurado, listado com seus mapeamentos de NSI, os conjuntos de AMF que o atendem e o NSSAI permitido por PLMN (`List all configured S-NSSAIs with NSI mappings, AMF sets, and allowed NSSAI per PLMN`). Esta é a visão autoritativa de como os fatiamentos solicitados se resolvem em instâncias de fatiamento e conjuntos de AMF para cada PLMN.
- **Disponibilidade de NSSAI**: o estado de disponibilidade de NSSAI por AMF (`Per-AMF NSSAI availability state`), que mostra quais fatiamentos cada AMF relatou que pode atender atualmente.
- **Estatísticas**: os próprios contadores do NSSF (`NSSF statistics: total slices, NS selection request counts`), que fornecem uma visão contínua do número de fatiamentos configurados e do volume de pedidos de seleção de fatiamento.

Uma visão separada de **configuração de fatiamento** (`Query Slice Configuration`) exibe a configuração de fatiamento em tempo de execução do NSSF para referência.

Ações

O painel do NSSF é orientado à leitura e monitoramento. Ele exibe fatiamentos, disponibilidade de NSSAI e estatísticas sem ações de controle por item.

Operações

Os controles OAM que o NSSF expõe são:

- **Ver configuração em tempo de execução** (`/api/oam/config`): a configuração ao vivo em tempo de execução do NSSF.

- **Forçar re-registro NRF** (`/api/oam/nrf/reregister`): faz com que o NSSF se re-registre no NRF, para recuperar caso seu registro tenha expirado.

Relacionados

- AMF: Gerenciamento de Acesso e Mobilidade: consulta o NSSF para resolver S-NSSAIs solicitados no NSSAI permitido e conjunto de AMF que atende um UE.
- NRF: Função de Repositório de Rede: onde o NSSF se registra para que outros NFs possam descobri-lo.
- ← 5G Core: a visão geral do painel 5GC e os outros NFs.

PCF: Função de Controle de Políticas

O **PCF** toma as decisões de políticas que o restante do Core 5G aplica. Ele responde ao AMF via N15 para **política de acesso e mobilidade (AM)**: as restrições de mobilidade e RFSP que um UE recebe ao se registrar. Ele responde ao SMF via N7 para **política de gerenciamento de sessão (SM)**: as regras de PCC que definem a QoS de cada sessão, controle de gating, controle de cobrança e monitoramento de uso. O PCF vincula as associações de política SM de um UE de volta a si mesmo através do BSF, para que qualquer NF possa encontrar o PCF correto para uma sessão. O painel do PCF é o lugar para responder "quais políticas estão ativas, para quais UEs e sessões, e são elas o que eu espero?" sem sair do OmniWeb. Cada resposta OAM é envolta em `{status, response}`, e o painel a desenrola para você.

← Core 5G

No painel

Na parte superior estão os quatro cartões de saúde padrão (**Saúde da API**, **Registro NRF** (o PCF está registrado no NRF?), **Status NF**, e **Licença**), cada um fazendo polling em um intervalo. Use o indicador de polling no cabeçalho para pausar a atualização ou ler o horário da última atualização. Abaixo dos cartões está a barra de **Ações** (veja abaixo), seguida pelas seções de dados do PCF, cada uma se atualizando automaticamente.

Estatísticas: os contadores ao vivo do PCF (`GET /api/statistics`), os totais de associação de políticas e contagens atuais. Esta é a leitura mais rápida para saber se o PCF está servindo ativamente as políticas AM e SM.

Políticas AM: cada associação de política AM ativa (`GET /api/am_policy`), uma linha por UE para a qual o AMF possui uma política AM. Esta é a visão do PCF sobre a política de mobilidade atualmente aplicada a cada UE registrado.

Políticas SM: cada associação de política SM ativa (`GET /api/sm_policy`), uma linha por sessão PDU para a qual o SMF possui uma política. Selecione uma linha para abrir seus detalhes (`GET /api/sm_policy/{id}`), que retorna as

regras completas de PCC para essa sessão: as decisões de QoS, gating, cobrança e monitoramento de uso que o SMF aplica.

Contexto da Política: a visão dos contextos de pol��tica ativos (`GET /api/policy_context`), os contextos que o PCF mantém em suas associações AM e SM. É útil para reconciliar o que o PCF acredita estar ativo em relação ao AMF e SMF.

Configuração: a configuração em tempo de execução do PCF (`GET /api/oam/config`), as configurações com as quais o serviço está atualmente em execução.

Ações

Cada ação por linha pede confirmação primeiro, uma vez que remover uma associação ativa é disruptivo para o UE ou sessão que afeta.

Remover uma política AM: em qualquer linha de Políticas AM, **Remover** exclui essa associação de política AM (`DELETE /api/am_policy/{id}`). Use isso para limpar uma política de mobilidade presa ou obsoleta para um UE.

Remover uma política SM: em qualquer linha de Políticas SM, **Remover** exclui essa associação de política SM (`DELETE /api/sm_policy/{id}`). Use isso para descartar a política de uma sessão que não será limpa por conta própria.

Atualizar uma política SM: você também pode editar uma associação de política SM. Envie `PATCH` ou `PUT /api/oam/sm_policy/{id}` para atualizar as regras de PCC em uma política SM ativa, para que você possa ajustar as decisões de QoS ou cobrança de uma sessão sem desmontar a associação. Use isso para reimpulsionar a política em uma sessão existente em vez de removê-la e recriá-la.

Operações

A seção de Operações contém os controles comuns a cada NF:

- **Diagnósticos** (`GET /api/oam/diagnostics`): diagnósticos em tempo de execução para o serviço.
- **Uso de recursos** (`GET /api/oam/resources`): memória, processos e escalonadores do serviço em execução.
- **Pares** (`GET /api/oam/peers`): os URIs de pares NF configurados com os quais o PCF se comunica e seu status de acessibilidade.
- **Cache de descoberta NRF** (`GET /api/oam/nrf_discovery`): o cache de descoberta NRF, ou os URIs NF configurados que o PCF resolve através de pares.
- **Nível de log** (`POST /api/oam/log_level`): alterar o nível de log em tempo de execução. Escolha um entre emergência, alerta, crítico, erro, aviso, advertência, informação ou depuração.
- **Re-registro NRF** (`POST /api/oam/nrf/reregister`): forçar o PCF a re-registrar-se no NRF, por exemplo, após um reinício do NRF deixá-lo obsoleto.

Relacionados

- SMF: solicita política SM do PCF via N7 e aplica as regras de PCC que o PCF retorna.
- AMF: solicita política AM do PCF via N15.
- BSF: a função de vinculação com a qual o PCF registra associações de políticas SM para que qualquer NF possa encontrar o PCF que está servindo.
- CHF: a função de cobrança. As decisões de controle de cobrança do PCF determinam o que o SMF relata via N40.
- ← visão geral do Core 5G

SCP: Proxy de Comunicação de Serviço

O **SCP** fica entre as funções de rede do Core 5G e transporta seu tráfego baseado em serviço. Em vez de cada NF consumidora se conectar diretamente a cada produtora, as solicitações podem ser roteadas através do SCP, que encaminha cada mensagem para uma instância saudável do tipo NF alvo, equilibrando a carga entre as instâncias e re-tentando em caso de falhas. Ele pode realizar a descoberta em nome de um consumidor (descoberta delegada) e armazena em cache a acessibilidade da NF para que, uma vez que conheça um tipo alvo, direcione solicitações posteriores sem uma nova busca. O resultado é comunicação indireta: produtores e consumidores não precisam conhecer ou manter conexões entre si, e o SCP gerencia o roteamento, o balanceamento e a atualização do cache.

← Core 5G

No painel

O painel do SCP segue o mesmo layout que cada página de NF do 5GC. Quatro **cartões de saúde** estão dispostos na parte superior (**Saúde da API**, **Registro NRF** (o SCP está registrado no NRF?), **Status da NF**, e **Licença**), cada um fazendo polling em um intervalo.

Abaixo dos cartões, o SCP apresenta seus próprios dados operacionais:

- **Saúde da NF**: a visão do balanceador de carga das NFs para as quais faz proxy, com contagens de saúde e falhas por instância, para que um operador possa ver quais instâncias produtoras o SCP considera acessíveis e quais estão falhando.
- **Cache de Descoberta**: o conteúdo do cache de descoberta do SCP, quais tipos de NF estão armazenados, seus TTLs e as taxas de acerto/perda do cache. Isso é o que permite que o SCP direcione solicitações repetidas sem uma nova descoberta.
- **Estatísticas**: throughput do SCP, total de solicitações proxy, uma divisão das solicitações por tipo de NF alvo e a taxa geral de acerto do cache.
- **Configuração**: a configuração atual em tempo de execução do SCP.

Cada seção se atualiza automaticamente, e os valores do tipo NF estão interligados ao painel daquela NF.

Ações

O painel do SCP não expõe botões de ação destrutiva em nível de NF ou por linha. Ele faz proxy de tráfego em vez de possuir estado de sessão ou de assinante que um operador limparia. Seu cache, no entanto, é gerenciável: a API OAM permite que um operador visualize o cache de descoberta e remova uma única entrada obsoleta para que o SCP redescubra aquele alvo na próxima solicitação (veja **Operações**). Para recuperar de um produtor que se moveu ou foi substituído, mas ainda está armazenado como acessível, limpe sua entrada.

Operações

A API OAM do SCP expõe os seguintes controles:

- **Visualizar / gerenciar cache de descoberta**: ler o cache de descoberta atual e excluir uma entrada de cache individual por id para forçar a redescoberta daquele alvo.
- **Visualizar configuração em tempo de execução**: ler a configuração ao vivo do SCP.
- **Definir nível de log**: alterar a verbosidade do log em tempo de execução. Escolha um de `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, ou `debug`.
- **Forçar re-registro NRF**: fazer o SCP se re-registrar no NRF. Isso é útil após o NRF ou o SCP ter reiniciado e o registro ter se tornado obsoleto.

Relacionados

- NRF: o registro que o SCP descobre e se re-registra.
- AMF, SMF, UDM, AUSF, PCF, CHF, NSSF, BSF: as NFs cujo tráfego baseado em serviço o SCP pode fazer proxy e cuja acessibilidade ele armazena em cache.

- ← Core 5G: a visão geral da seção 5GC e o layout do painel compartilhado.

SMF: Função de Gerenciamento de Sessão

O **SMF** é responsável pela sessão PDU. Ele estabelece, modifica e libera a sessão de dados de cada UE, aloca o endereço IP da UE a partir de um pool local e controla o plano do usuário através do N4/PFCP. Ele programa o UPF com as regras de detecção de pacotes, encaminhamento e QoS para cada sessão. Também se comunica com o PCF (N7) para políticas de sessão e com o CHF (N40) para cobrança. Use o painel do SMF para responder "as sessões estão sendo criadas, o SMF ainda está associado ao seu UPF e está ficando sem endereços?" sem sair do OmniWeb. O SMF encapsula cada resposta OAM `{status, response}`. O painel a desencripta para você.

← 5G Core

No painel

Na parte superior estão os quatro cartões de saúde padrão: **Saúde da API**, **Registro NRF** (o SMF está registrado no NRF?), **Status NF** e **Licença**. Cada um faz polling em um intervalo. Use o indicador de polling no cabeçalho para pausar a atualização ou ler o horário da última atualização. Abaixo dos cartões está a barra de **Ações** (veja abaixo). Em seguida, vêm as seções de dados do SMF, cada uma se atualizando automaticamente.

Estatísticas: os contadores ao vivo do SMF (`GET /api/statistics`): totais de estabelecimento / modificação / liberação de sessão e contagens de sessão atuais. Esta é a leitura mais rápida para saber se o SMF realmente configura sessões.

Sessões PDU: cada sessão PDU ativa (`GET /api/pdu_session`), retornada como `{ pdu_sessions: [...], total }`. Cada linha contém tanto um `sm_context_ref` (um UUID que identifica exclusivamente o contexto SM) quanto um `pdu_session_id` (o PSI 3GPP, um pequeno inteiro que **não** é único entre UEs, uma vez que cada UE numera suas próprias sessões a partir de uma base baixa). Portanto, cada operação por sessão (consulta de detalhes e liberação) é baseada em `sm_context_ref`. A ação **Liberar** por linha do painel

passa esse UUID em vez do PSI. Ao lado dos identificadores, uma linha mostra o DNN da sessão, o IP da UE alocado e o estado.

Pool de IP: o pool de endereços do qual o SMF aloca IPs de UE (`GET /api/ip_pool/detail`): o resumo do pool (sub-rede, total, contagens alocadas e disponíveis) além da lista de IPs atualmente alocados. Aqui você vê se o SMF está perto de esgotar seu espaço de endereços.

Associação UPF: o estado do link N4/PFCP para o plano do usuário (`GET /api/upf`): se o SMF está atualmente associado ao seu UPF. Se as sessões falharem ao estabelecer, verifique isso primeiro.

Pares PFCP: o status de associação do par PFCP (UPF) (`GET /api/oam/pfcp_peers`): a visão do SMF de cada UPF com o qual se associa via N4, incluindo o estado da associação.

Ações

Cada ação pede confirmação primeiro. Várias são destrutivas para sessões ativas.

Liberar Todas as Sessões PDU: derruba todas as sessões PDU e seu estado PFCP no UPF. Use isso para limpar o SMF de volta a um estado limpo, por exemplo, após uma troca de UPF ou quando você drena um nó para manutenção.

Limpar Cache: limpa os caches de sessão do SMF sem uma liberação de sessão. Use isso quando o painel ou a visão interna do SMF parecerem desatualizados ou inconsistentes com a realidade.

Reassociar PFCP: restabelece a associação PFCP com o UPF (iniciada pelo SMF). Use isso quando a associação UPF tiver caído e novas sessões não puderem ser estabelecidas.

Re-associar UPF: força uma re-associação PFCP com o UPF **configurado**. O endereço UPF é determinado pela configuração. Não há ação de adicionar-UPF ou injetar-UPF aqui. Isso redireciona a associação para o UPF já na configuração

do SMF. Na prática, serve ao mesmo propósito de recuperação que a Reassociação PFCP.

Liberar por DNN: digite um DNN no campo **DNN** editável (por exemplo, `internet`). Isso libera **todas** as sessões naquele DNN. Use isso para drenar ou redefinir uma única rede de dados, por exemplo, para forçar UEs a sair de um APN/DNN, sem tocar nas sessões em outros DNNs.

Liberação por linha: em qualquer linha de Sessões PDU, **Liberar** derruba aquela sessão e seu contexto PFCP no UPF. Ela libera por `sm_context_ref`, portanto sempre mira exatamente a sessão naquela linha, mesmo que várias UEs possam compartilhar o mesmo `pdu_session_id`. Use isso para derrubar uma única sessão presa.

Operações

A seção de Operações contém os controles comuns a cada NF:

- **Diagnósticos** (`GET /api/oam/diagnostics`): diagnósticos em tempo de execução para o serviço.
- **Uso de recursos** (`GET /api/oam/resources`): memória, processos e escalonadores do serviço em execução.
- **Pares** (`GET /api/oam/peers`): os URIs de pares NF configurados com os quais o SMF se comunica (AMF, PCF, CHF, NRF e seus pares PFCP UPF via Pares PFCP acima).
- **Nível de log** (`POST /api/oam/log_level`): altera o nível de log em tempo de execução. Escolha um entre emergência, alerta, crítico, erro, aviso, advertência, informação ou depuração.
- **Re-registro NRF** (`POST /api/oam/nrf/reregister`): força o SMF a re-registrar-se no NRF, por exemplo, após uma reinicialização do NRF deixá-lo desatualizado.

Relacionados

- AMF: solicita a configuração de sessão do SMF via Nsmf.
- PCF: fornece a política de sessão ao SMF via N7.

- CHF: a função de cobrança à qual o SMF reporta o uso via N40.
- UPF: o par N4/PFCP do SMF. É o plano do usuário que o SMF programa e associa.
- ← visão geral do 5G Core

UDM: Gerenciamento Unificado de Dados

O **UDM** é a autoridade de dados de assinatura do núcleo 5G. Ele gerencia os perfis de assinatura de cada assinante. Ele rastreia quais NFs de serviço lidam com cada UE e registra o AMF e o SMF contra um assinante. Ele fornece os dados de autenticação usados para desafiar a UE. Ele lê os registros subjacentes de assinantes do **UDR**, seu armazenamento de apoio, e os armazena em cache para uma rápida consulta. O **AMF** o consulta durante o registro. O **SMF** o consulta durante a configuração da sessão. O **AUSF** obtém seu material de autenticação dele. Quando outro NF precisa saber o perfil de um assinante ou onde a rede o atende, o UDM é o NF que responde.

← Núcleo 5G

No painel

O painel do UDM abre com os quatro cartões de saúde padrão: **Saúde da API**, **Registro NRF** (se o UDM está atualmente registrado no NRF), **Status NF** e **Licença**. Cada um faz uma consulta em um intervalo. Abaixo deles, ele mostra os dados que o UDM possui:

- **Lista de UE**: cada contexto de UE que o UDM possui, indexado por SUPI. Esta é a visão "quais assinantes o UDM está atendendo atualmente". O UDM também pode retornar um contexto detalhado para um único assinante por SUPI. Ele mostra os registros de NF de serviço desse assinante e os dados de assinatura em cache.
- **Estatísticas**: os contadores ao vivo do UDM, para uma leitura rápida sobre carga e atividade.
- **Configuração**: a configuração em tempo de execução que o serviço está utilizando atualmente.

Ações

O painel expõe ações para limpar os dados de assinantes em cache. O painel confirma cada uma antes de executá-la, uma vez que ela remove o estado ao vivo:

- **Limpar Cache de Assinante** (em massa): limpa todo o cache de dados de assinantes. Use-o quando o UDM atender perfis desatualizados, por exemplo, após registros de assinatura terem mudado no UDR e o UDM deve reler esses registros em vez de servir suas cópias em cache.

Além do botão do painel, a API OAM do UDM expõe um controle mais detalhado que um operador pode acessar através do proxy de backend:

- **Limpar o cache de um UE** (`/api/oam/ue_cache/{id}`): remove os dados de assinante em cache para um único assinante por SUPI. Use-o para forçar uma releitura para um assinante cujo perfil mudou, em vez de limpar o cache para todos.

Operações

- **Diagnósticos em tempo de execução** (`/api/oam/diagnostics`): mostra diagnósticos de baixo nível para o serviço em execução.
- **Uso de recursos** (`/api/oam/resources`): relata o uso de memória, processo e agendador em tempo de execução para uma verificação de saúde do nó.
- **Definir nível de log** (`/api/oam/log_level`): altera o nível de log em tempo de execução (um dos `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar os detalhes enquanto você faz a solução de problemas.
- **Forçar re-registro NRF** (`/api/oam/nrf/reregister`): re-registra o UDM com o NRF. Use-o para recuperar um registro perdido ou desatualizado.

Relacionados

- UDR: Repositório de Dados Unificado: o armazenamento de apoio do qual o UDM lê os registros de assinantes.
- AUSF: Função de Servidor de Autenticação: obtém seu material de autenticação do UDM.
- AMF: Função de Gerenciamento de Acesso e Mobilidade: consulta o UDM durante o registro e se registra como um NF de serviço.
- SMF: Função de Gerenciamento de Sessão: consulta o UDM durante a configuração da sessão e se registra como um NF de serviço.
- ← Núcleo 5G: a visão geral de todos os painéis NF.

UDR: Repositório de Dados Unificado

O **UDR** é o armazenamento persistente de dados de assinatura, política e aplicação que fica atrás do UDM e PCF. Onde o UDM e o PCF são as funções de rede de front-end com as quais outras NFs se comunicam, o UDR é o banco de dados que elas leem e escrevem. É a única fonte de verdade sobre quem é um assinante e a que ele tem direito. No núcleo do Omnitouch, o UDR compartilha seu armazenamento de assinantes com o **HSS**, de modo que um repositório unificado contém assinantes de 4G e 5G em vez de dois bancos de dados paralelos.

← 5G Core

No painel

O painel do UDR é aberto com os cartões de saúde padrão de NF na parte superior (**Saúde da API**, **Registro NRF** (o UDR está registrado no NRF?), **Status da NF** e **Licença**), cada um fazendo polling em um intervalo.

Abaixo dos cartões estão as duas seções de dados específicas do UDR:

- **Saúde do HSS**: uma verificação de saúde de conectividade que confirma se o UDR pode alcançar o armazenamento de assinantes compartilhado do HSS que ele representa. Isso responde "o banco de dados de assinantes é acessível e saudável?" à primeira vista.
- **Assinantes**: a lista de assinantes extraída do HSS, paginada e pesquisável por **IMSI**. Selecione um assinante para retornar os detalhes completos do assinante para aquele IMSI, para que um operador possa confirmar a provisão de um assinante sem sair do OmniWeb.

Ações

O painel do UDR não expõe ações destrutivas em nível de NF ou por linha. É uma visão de leitura e consulta sobre o armazenamento de assinantes compartilhado. Seu valor está na interrogação: verifique se o armazenamento é acessível através da seção de saúde do HSS, liste os assinantes e aprofunde-se nos detalhes completos de qualquer assinante por IMSI.

Operações

Ao lado das seções de dados, o UDR carrega as operações comuns a cada função de rede 5GC:

- **Definir nível de log**: aumentar ou diminuir a verbosidade do log em tempo de execução (`emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) via `/api/oam/log_level`, para aumentar os detalhes enquanto você diagnostica um problema.
- **Forçar re-registro NRF**: empurrar o UDR para re-registrar-se no NRF (`/api/oam/nrf/reregister`) se seu registro estiver desatualizado.
- **Ver configuração em tempo de execução**: inspecionar a configuração ao vivo do UDR através do endpoint de configuração OAM.

Relacionados

- UDM: Gerenciamento de Dados Unificado: a função de rede de front-end que serve dados de assinatura a partir deste armazenamento.
- PCF: Função de Controle de Políticas: lê os dados de políticas mantidos no UDR.
- HSS: o banco de dados de assinantes compartilhado com o qual o UDR se unifica, de modo que assinantes de 4G e 5G vivam em um único repositório.
- ← 5G Core: a visão geral completa do painel 5GC.

Referência da API (OpenAPI / Swagger)

O controlador do OmniWeb (backend central) expõe uma única API REST por trás do mesmo login JWT que governa o restante do portal. Essa API é auto-documentada:

- **Swagger UI:** `/api/docs`. Navegue por cada endpoint. Expanda uma rota para ver seu método, parâmetros de caminho/query, se precisa de um token e seu resumo. Clique em **Authorize** e cole um JWT bearer para tentar chamadas ao vivo contra a instância em execução.
- **Especificação OpenAPI 3:** `/api/openapi.json`. Este é o documento legível por máquina. Use-o para importar no Postman/Insomnia ou para gerar clientes.

← Voltar ao Guia de Operações

O que está documentado

A especificação é **gerada em tempo de execução** ao introspectar o mapa de rotas ao vivo, então ela sempre corresponde aos endpoints que a instância em execução realmente serve. Nenhum arquivo mantido manualmente pode desviar. Para cada rota, ela captura:

- o método HTTP e o caminho (com parâmetros de caminho/query),
- um resumo e descrição retirados do código,
- se um **bearer JWT** é necessário, e
- onde aplicável, a permissão de **visualização/controle** por elemento que a rota impõe.

Os endpoints são agrupados por área (Auth, Admin, SIM Bank, Remote SIM, APDU, Test Devices, IR.38, RAEX, TAP, e assim por diante) para que você possa encontrar rapidamente as rotas de uma funcionalidade.

Obtendo um token

A maioria dos endpoints requer um token bearer. Obtenha um com `POST /api/auth/login` (as mesmas credenciais que você usa para o portal), e então envie-o como `Authorization: Bearer <token>`. No Swagger UI, use o botão **Authorize** para que cada chamada "Try it out" carregue o token automaticamente.

Consultando Loki e Prometheus diretamente

Os back-ends de monitoramento são acessíveis através do portal com as mesmas credenciais, então scripts e ferramentas como logcli nunca precisam de uma rota para o host de monitoramento em si. Envie o token bearer acima, ou uma chave de API de **Configurações → Chaves de API** como `X-API-Key`, e mantenha GET no tipo de elemento **Loki** ou **Prometheus**.

- **Loki**: `/loki/api/v1/...` é a própria API do Loki, caminho por caminho, servida do Loki do host do portal. Para um site específico, use `/proxy/loki/loki/api/v1/...` com o cabeçalho `X-Omniweb-Site` definido como `<customer>::<site>`.
- **Prometheus**: `/prometheus/api/v1/...` é a própria API do Prometheus (somente leitura), com a mesma forma por site em `/proxy/prometheus/api/v1/...`.

Chamadas não autenticadas recebem 401; um login sem a concessão recebe 403.

Escopo

Isso documenta apenas a API do **controlador**. O agente do dispositivo que roda em locais remotos não faz parte desta API: ele se conecta *para fora* ao controlador através de um WebSocket e não expõe nenhum endpoint REST de entrada, então não há nada para chamar diretamente.

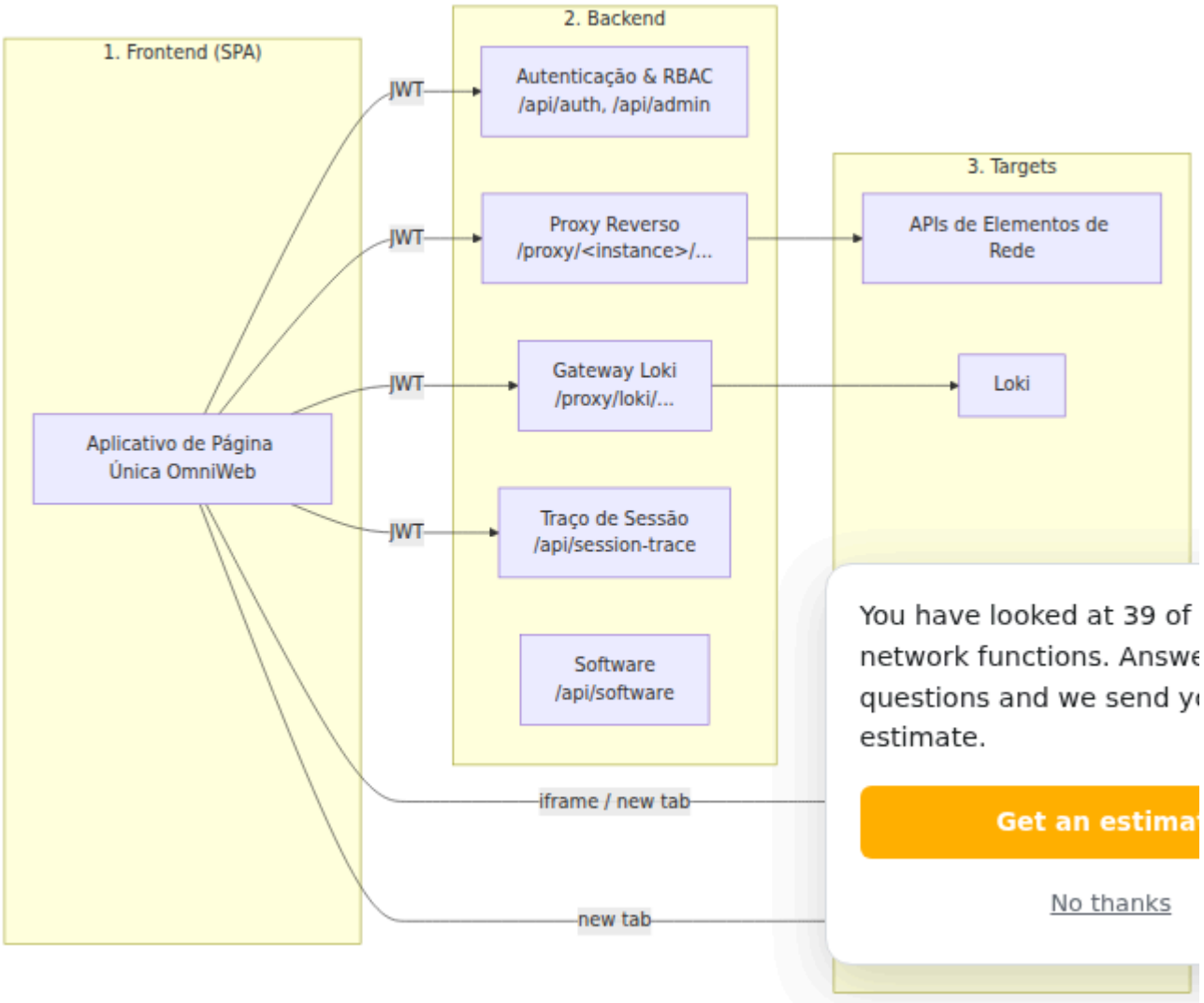
Arquitetura do OmniWeb

Esta página explica como o OmniWeb é estruturado e como uma única sessão de navegador alcança cada função de rede, Grafana e Loki. Se você ler apenas uma página para entender o sistema, leia esta.

← Voltar ao Guia de Operações

Componentes

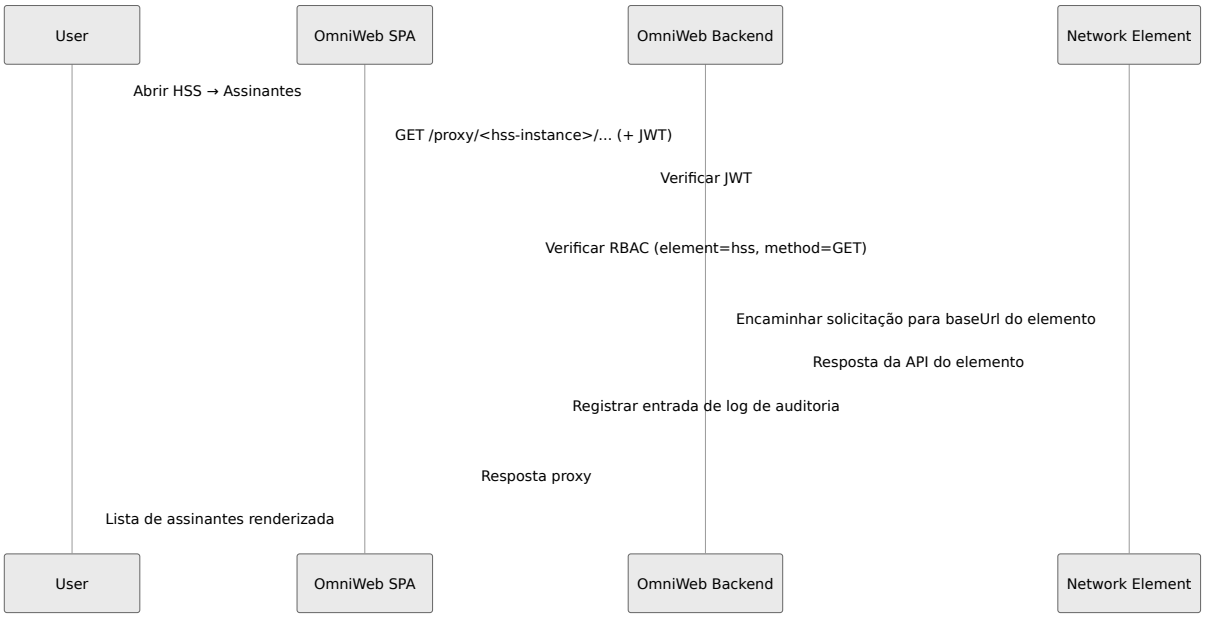
O OmniWeb possui três partes móveis:



Componente	Função
Frontend SPA	A interface do usuário. Um aplicativo web de página única que renderiza páginas de elementos, topologia, logs, traços e painéis incorporados.
Backend	A camada de segurança e integração. Autentica usuários, aplica RBAC e faz proxy reverso de cada solicitação para a API de elemento correta, Loki ou Grafana.
Targets	As coisas que estão sendo gerenciadas e observadas: as próprias APIs de gerenciamento dos elementos de rede, além de Grafana, Loki e Homer.

Fluxo de Solicitação

Cada solicitação operacional segue o mesmo caminho. Nada no navegador se comunica diretamente com um elemento. Sempre passa pelo backend para que a autenticação, autorização e auditoria sejam aplicadas centralmente.



O caminho do proxy codifica o **ID da instância**, para que o OmniWeb possa gerenciar muitas instâncias do mesmo tipo de elemento (por exemplo, vários nós HSS) e direcionar cada solicitação para o backend correto.

O Modelo de Configuração

O OmniWeb é **dirigido por configuração**. O conjunto de elementos, suas instâncias e onde suas APIs residem é declarado em um único arquivo: `public/config/omniweb.json`. O backend o carrega na inicialização e o frontend o utiliza para construir a barra lateral, topologia e alvos de proxy.

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

Parâmetro	Tipo	Obrigatório	Padrão	Descriç
`type`	String	Sim	-	Tipo de elen Determina c módulo de U renderiza o elemento. V tipos suport
`displayName`	String	Sim	-	Nome legíve humanos ex na barra late na topologia
`description`	String	Não	-	Descrição m longa exibid dicas de ferramentas páginas de v geral.
`instances`	Lista	Sim	-	Uma entrad nó implanta deste tipo. V parâmetros instância ab
`defaults.pollIntervalMs`	Inteiro	Não	5000	Com que frequência a páginas operacionais atualizam automaticar em milissegund

Parâmetro	Tipo	Obrigatório	Padrão	Descriç
`defaults.timeoutMs`	Inteiro	Não	10000	Tempo limite proxy para e tipo de elem APIs lentas (exemplo, OC usam um va maior.

Parâmetros da instância:

Parâmetro	Tipo	Obrigatório	Padrão	Descrição
`id`	String	Sim	-	Identificador único da instância. Usado em URLs (`/hss/<id>`) e no caminho do proxy (`/proxy/<id>/...`).
`name`	String	Sim	-	Nome exibido para a instância.
`baseUrl`	String	Sim	-	A URL base da API de gerenciamento do elemento. O proxy encaminha solicitações aqui. TLS autoassinado é aceito.
`tags`	Lista	Não	`[]`	Rótulos de forma livre (por exemplo, `primary`, `geo-redundant`) exibidos como chips.

Tipos de Elementos Suportados

`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`.

Cada tipo mapeia para um módulo de UI com seu próprio conjunto de abas, mas todos são operados através dos mesmos padrões genéricos. Veja Operações Comuns.

Como o OmniWeb se Comunica com Cada NF

O proxy do backend é agnóstico ao elemento. Ele encaminha o que o módulo frontend solicitar para o `baseUrl` do elemento. A *forma* dessas chamadas depende da API nativa do elemento:

Estilo da API	Elementos	Notas
API do Elemento	Todas as funções de rede	A própria API de gerenciamento do elemento, proxied verbatim sob `/proxy/<instance-id>/...`. O OmniWeb encaminha `GET`/`POST`/`PUT`/`PATCH`/`DELETE` como o elemento espera; a forma da solicitação/resposta é o que aquele elemento define.
Consulta de log (LogQL)	Todos (aba de Logs)	Roteado através de `/proxy/loki/...` para Loki. Veja Logs & Tracing.

Como tudo é feito por proxy, adicionar uma instância é puramente uma mudança de configuração em `omniweb.json`. Nenhuma mudança de código é necessária para gerenciar outro nó.

Referência da API (OpenAPI)

Um documento consolidado OpenAPI/Swagger (`swagger-doc.json`) é enviado com o OmniWeb e descreve os esquemas do backend e dos elementos (por exemplo, registros de frontend SMSC e locais de assinantes IMS). É um artefato de referência, em vez de um servidor de API ativo.

Tempos Limite do Proxy

Cada tipo de elemento tem um tempo limite de proxy configurável (`defaults.timeoutMs`). A maioria dos elementos responde bem dentro do padrão de 10 segundos. Elementos com consultas mais pesadas recebem mais margem:

Elemento	Tempo Limite Padrão	Por quê
A maioria dos elementos	10 segundos	Tempo de resposta padrão da API
OCS	180 segundos	Consultas de classificação/CDR sobre grandes conjuntos de dados

Integração de Monitoramento

O OmniWeb não reimplementa Grafana, Loki ou Homer. Ele os integra para que um único login abranja toda a pilha:

- **Grafana** é servido atrás do gateway autenticado e incorporado como um iframe. Cada solicitação é autorizada contra seu login do OmniWeb, então não há segunda senha. Veja Grafana.
- **Loki** é acessado através do gateway `/proxy/loki/*` do backend, que executa consultas LogQL em nome do operador. Veja Logs & Tracing.
- **Homer** (captura SIP) é detectado automaticamente na inicialização (`/api/homer/status`) e, quando presente, abre em uma nova aba. Também

é autorizado contra seu login do OmniWeb.

Referência do Ambiente

Os pontos de integração do backend são configurados através de variáveis de ambiente:

Variável	Padrão	Descriçã
`GRAFANA_URL`	`http://localhost:3000`	URL base da instâ Grafana que o On proxy.
`LOKI_URL`	`http://localhost:3100`	URL base da instâ Loki usada para lo rastreamento.
`LDAP_URI`	`ldap://localhost:389`	Servidor OpenLDA sincronização de usuário/chave SS (opcional).
`LDAP_BASE_DN`	`dc=omniweb,dc=local`	DN base do LDAP.
`LDAP_ADMIN_DN`	`cn=admin,dc=omniweb,dc=local`	DN de ligação par gravações LDAP.
`LDAP_ADMIN_PASSWORD`	`omniweb-admin`	Senha de ligação (mude isso).
`AUDIT_API_KEY`	`omniweb-audit-key`	Segredo compart callbacks de audi login SSH (mude
`OMNIHSS_API_KEY`	Nenhum	Chave que o Omn envia para o Omn cabeçalho `x-omni` O OmniCore a gra `/etc/omniweb/om` Se não estiver de OmniWeb não en solicitações ao On Veja RBAC.

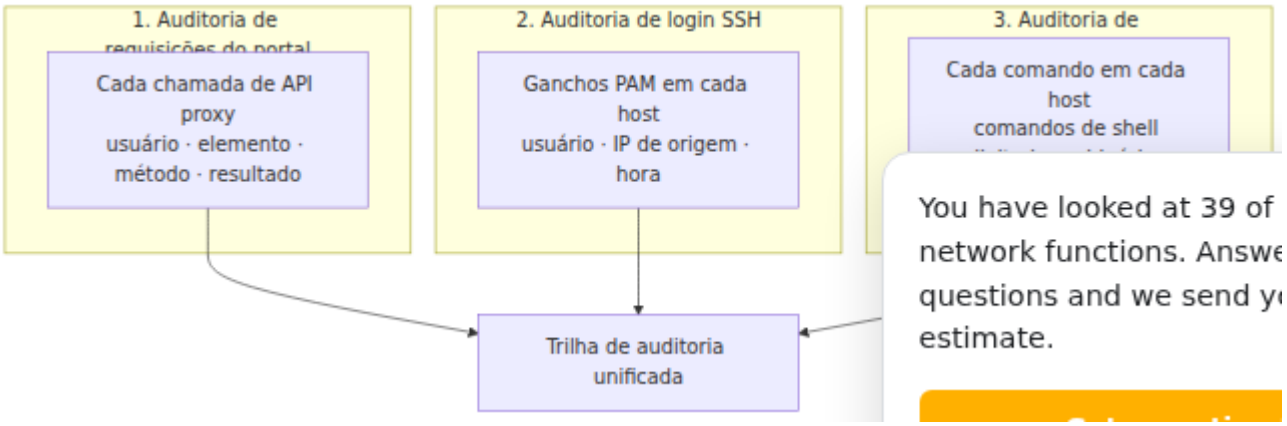
Veja Autenticação & Controle de Acesso para os detalhes de LDAP/SSH e auditoria.

Registro de Auditoria

Como o OmniWeb é o único gateway para a rede, ele também é o único lugar onde a atividade pode ser registrada. A auditoria no OmniWeb possui **três camadas** que juntas respondem "quem fez o que, onde" tanto no portal quanto nos hosts que ele gerencia.

← Autenticação & Controle de Acesso · ← Guia de Operações

As Três Camadas



Camada	Captura	Onde aparece
Auditoria de requisições do portal	Cada ação realizada *através* do OmniWeb	Configurações → Auditoria
Auditoria de login SSH	Cada login SSH *em um host gerenciado*	Configurações → Auditoria (via callback do host)
Auditoria de comandos	Cada comando *executado em um host* (digitado + executado)	Configurações → Comandos

Auditoria de Requisições do Portal

Cada requisição que passa pelo proxy do OmniWeb é registrada, independentemente de ter sido bem-sucedida, falhada ou rejeitada pelo RBAC. Cada entrada captura:

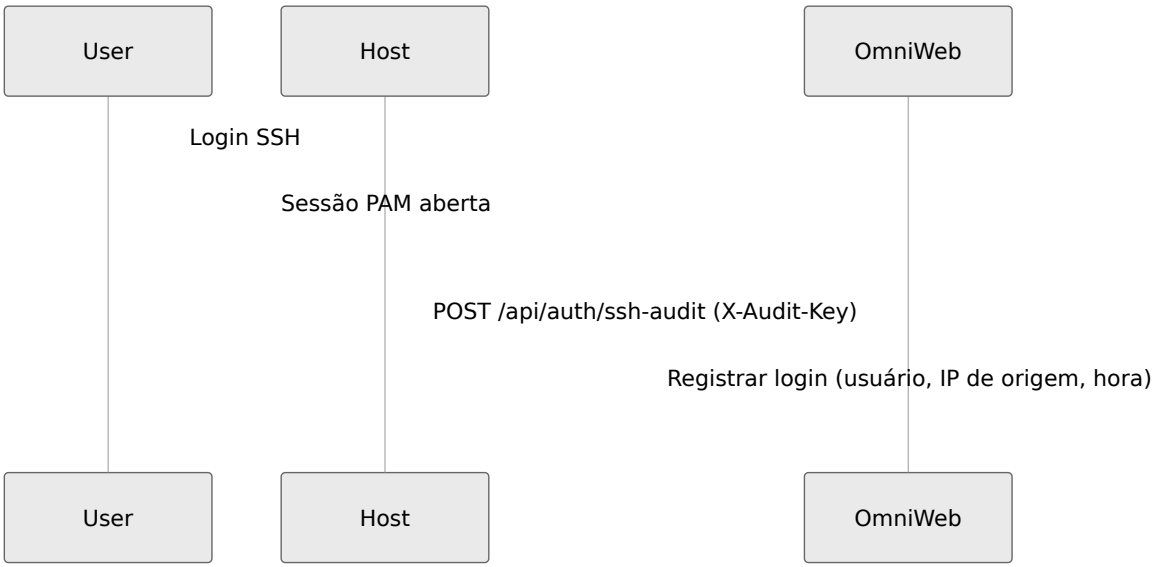
- O **usuário** que fez a requisição.
- O **tipo e instância do elemento** alvo.
- O **método HTTP** (que indica se foi uma visualização, uma alteração ou uma exclusão).
- O **resultado** (código de status).
- O **timestamp**.

Isso fornece um registro completo de quem mudou o que, onde e quando, dentro do portal. Ele está localizado em **Configurações → Auditoria**. Como leituras (`GET`), gravações (`POST`/`PUT`/`PATCH`) e exclusões são todas distinguíveis por método, o log de auditoria também serve como um histórico de mudanças para a rede.

A Trilha de Auditoria (Configurações → Auditoria): cada ação com o usuário, tipo de evento, elemento/instância, método HTTP, resultado e IP de origem. Observe a `DELETE` negada (403), os eventos `permission_changed` e `ssh_login` ao lado de requisições API comuns. Filtre por tipo de evento, usuário, elemento ou intervalo de datas.

Auditoria de Login SSH

Os hosts podem relatar logins SSH de volta ao OmniWeb para que o acesso ao host apareça na mesma visualização de auditoria que a atividade do portal. Um pequeno gancho PAM em cada host chama o OmniWeb quando uma sessão é aberta, relatando o nome de usuário, IP de origem e detalhes do serviço.



O callback é autenticado com um segredo compartilhado, para que apenas hosts confiáveis possam escrever entradas de auditoria:

Variável	Padrão	Descrição
`AUDIT_API_KEY`	`omniweb-audit-key`	Segredo compartilhado que o gancho PAM do host apresenta (como `X-Audit-Key`) ao relatar um login. **Altere isso**, e defina o valor correspondente em cada host.

Com isso em vigor, cada login SSH em um host gerenciado aparece em **Configurações → Auditoria** ao lado das ações do portal, conectando a

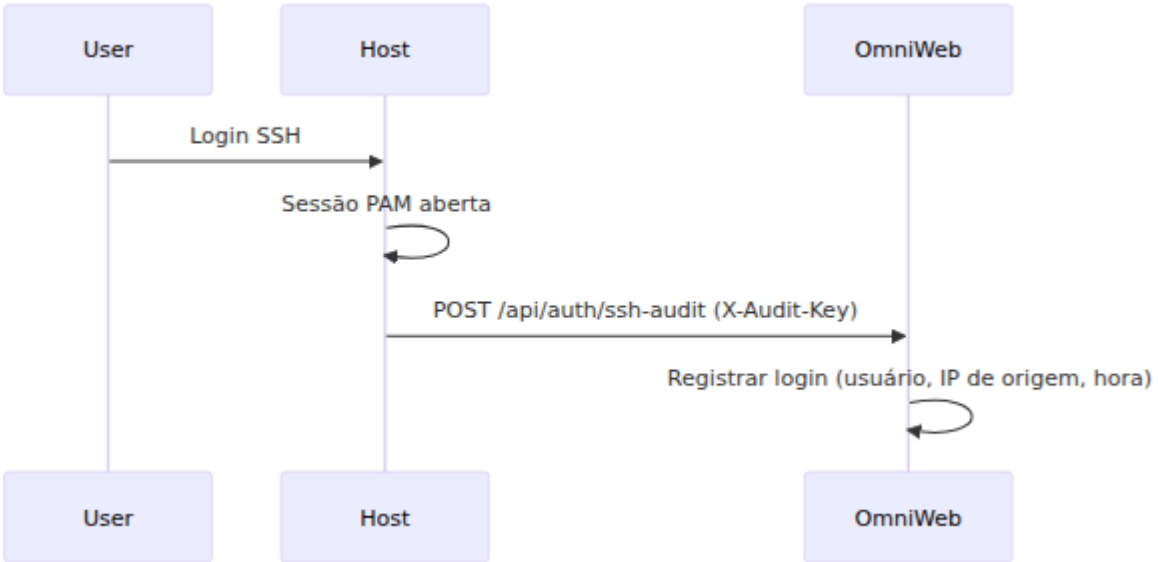
atividade de uma pessoa no portal e no host.

Auditoria de Comandos

Para visibilidade em nível de comando nos hosts, o OmniWeb coleta **duas correntes complementares**, ambas enviadas para o Loki e navegáveis em **Configurações → Comandos** com um alternador de fonte:

Fonte	Captura	Fluxo Loki
Comandos digitados	As linhas de comando exatas que um usuário digita em um shell interativo, **incluindo built-ins de shell** como `echo`, `cd`, `export`	`job="cmdaudit"`
Execuções de binários	Cada binário que realmente foi executado no host (scripts, ferramentas, automação)	`job="auditd"`

Nenhuma substitui a outra: built-ins nunca executam um binário separado, então apenas o fluxo de comandos digitados os vê; e automação/scripts que nunca ficam em um prompt interativo aparecem apenas no fluxo de execução de binários. Juntas, elas cobrem *o que uma pessoa digitou* e *o que realmente foi executado*.



Comandos digitados são capturados por um gancho leve de shell interativo que registra cada comando que um usuário executa (com usuário, diretório de trabalho e TTY). Esta é a camada que captura built-ins que um rastreador de binários estruturalmente não pode ver.

Execuções de binários vêm de um agente leve do host que registra cada binário executado no host. Como funciona no espaço do usuário, funciona dentro de contêineres LXC sem suporte de auditoria do kernel. Cada entrada captura:

Campo	Significado
`login`	O usuário que originalmente fez login; **sobrevive a** `sudo`/`su`, então mudanças de privilégio não ocultam quem está agindo
`uid`	UID efetivo que o comando realmente foi executado
`filename`	O binário que foi executado
`cwd`	Diretório de trabalho no momento da execução
(após `]:`)	A linha de comando completa

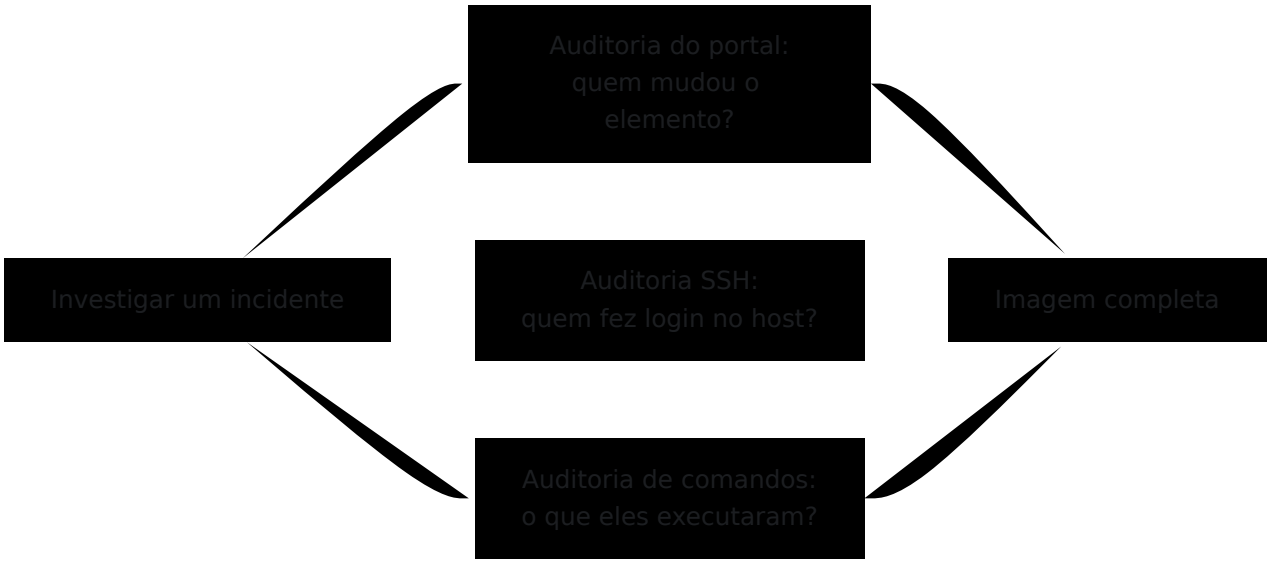
Uma entrada de execução representativa:

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

A visualização **Configurações → Comandos** tem como padrão o fluxo de comandos digitados e permite que você filtre por host, busque por usuário ou comando, e acompanhe a atividade em tempo real em toda a frota, com o alternador de fonte para mudar para a visualização de execução de binários brutos quando você quiser ver exatamente o que foi executado.

> **Nota:** os fluxos de comando são uma ajuda de visibilidade para o operador capturada no espaço do usuário. Um usuário root determinado pode ignorá-los; a auditoria em nível de kernel é o passo de endurecimento se você precisar de captura não contornável. Para o registro estruturado relevante à segurança (logins, mudanças de permissão, negações), confie na **Auditoria do Portal** e na **Auditoria de Login SSH** acima, que são escritas no próprio banco de dados do OmniWeb.

Como as Camadas se Conectam



- Uma mudança de configuração feita **através do OmniWeb** → auditoria de requisições do portal.
- Uma mudança feita **manualmente em um host** → auditoria de login SSH (quem entrou) + auditoria de comandos (o que eles fizeram).

Juntas, elas n��o deixam pontos cegos entre "mudou na interface" e "mudou na máquina".

Relacionados

- Logs & Rastreio de Assinantes: o explorador de logs geral por trás dos fluxos de comando.
- Login com Chave SSH: o lado de acesso da atividade do host.
- RBAC: as permissões cujo uso é registrado pela auditoria do portal.

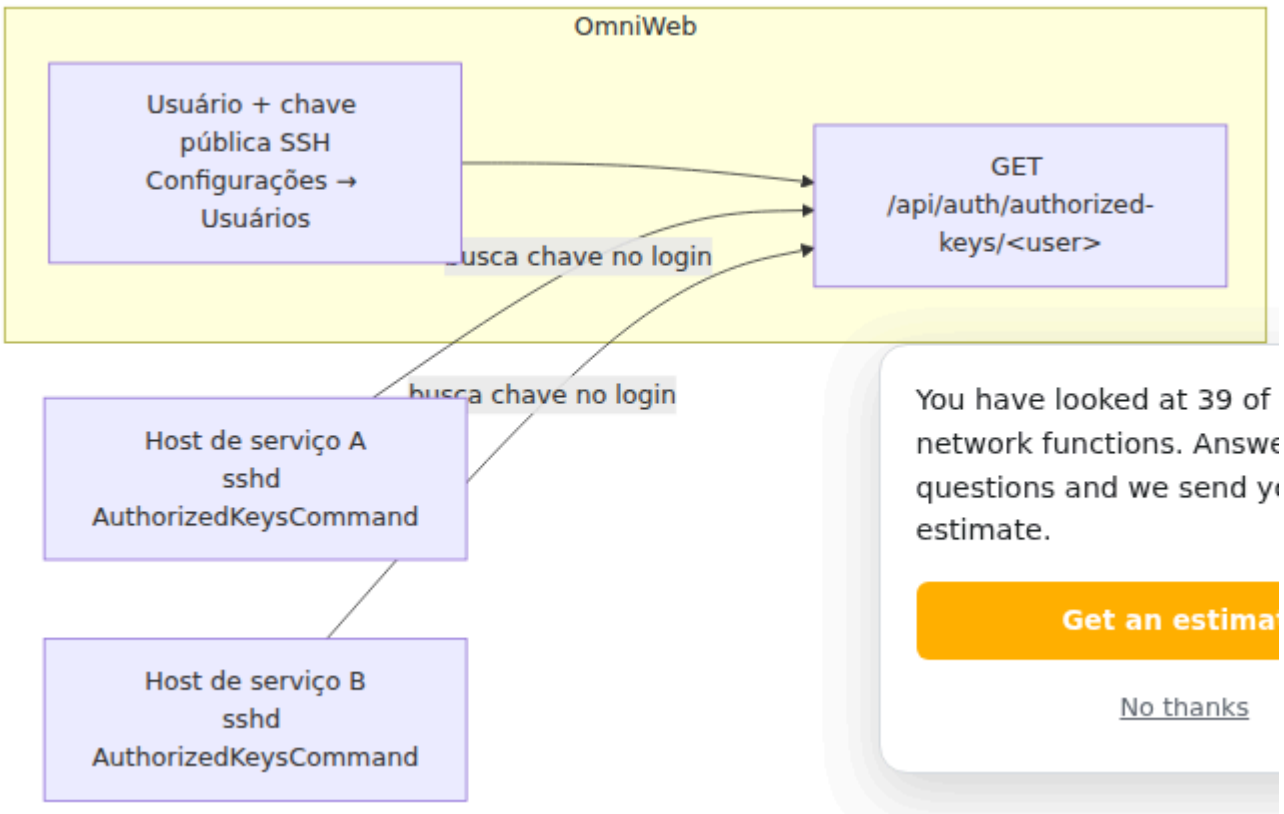
Login com Chave SSH (Acesso ao Host)

O controle de acesso do OmniWeb se estende além do portal para os **hosts** que executam a rede. Cada usuário pode ter uma **chave pública SSH**, e os hosts gerenciados buscam essas chaves **ao vivo do OmniWeb** no momento do login. Assim, o OmniWeb é o único lugar para gerenciar *quem pode SSH onde*, e, combinado com registro de auditoria, quem realmente fez.

Não há servidor de diretório para executar e nenhum arquivo `authorized_keys` por host para manter. (Isso substitui um design anterior de sincronização com OpenLDAP; o diretório foi removido e as chaves são fornecidas sob demanda via HTTPS.)

← Autenticação & Controle de Acesso · ← Guia de Operações

O Que Faz



Você fornece a um usuário uma chave pública SSH no OmniWeb uma vez. O `sshd` de cada host gerenciado é configurado para solicitar a chave desse usuário ao OmniWeb **no momento do login** (via `AuthorizedKeysCommand` do OpenSSH). Adicione uma chave no OmniWeb e o usuário pode SSH para cada host inscrito; desative o usuário e esse acesso desaparece em toda parte em sua **próxima** tentativa de login, sem sincronização, sem desvio e sem arquivos de chave para limpar.

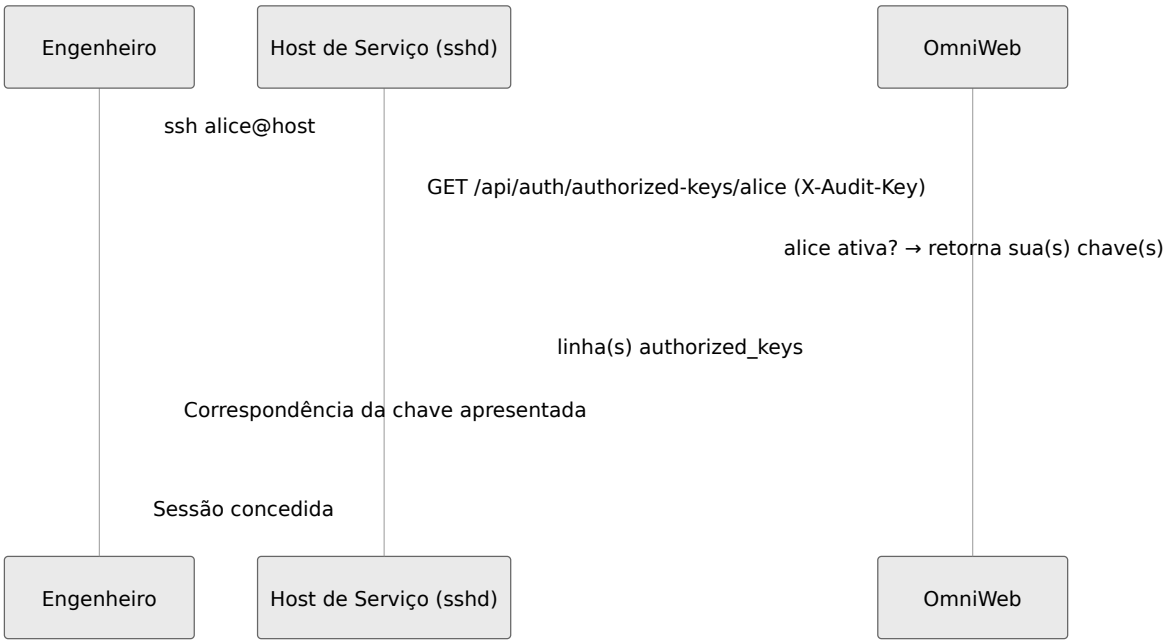
Definindo a Chave de um Usuário

As chaves são gerenciadas em **Configurações → Usuários**, a mesma tela que gerencia contas do portal, RBAC e estado ativo/desativado. Cada linha de usuário mostra se uma chave SSH está configurada; crie ou edite um usuário para colar uma.

Configurações → Usuários: cada usuário com a configuração de uma chave pública SSH. A chave que você colar aqui é a chave que concede acesso ao host; não há outro lugar para mantê-la.

Como os Hosts Consomem

Cada host gerenciado executa um pequeno helper conectado ao `sshd` como seu `AuthorizedKeysCommand`. Quando alguém se conecta, o `sshd` executa o helper, que busca as chaves autorizadas desse usuário no OmniWeb via HTTPS e as devolve para a correspondência:



Propriedades chave desse fluxo:

- **Ao vivo**: a chave é buscada por login, então as mudanças têm efeito imediato.
- **Apenas usuários ativos**: o OmniWeb só retorna chaves para usuários **ativos**. Quando você desativa ou exclui um usuário no OmniWeb, isso nega seu próximo login em todos os hosts de uma vez. Este é o botão de revogação.
- **Sem enumeração**: um usuário desconhecido ou desativado, ou um sem chave, retorna um resultado vazio. O login simplesmente não encontra chave e é negado, então o endpoint não vaza quais nomes de usuário existem.
- **Sobrevive a uma interrupção do OmniWeb**: o helper armazena em cache o último resultado bom por usuário no host, então uma breve interrupção do OmniWeb não bloqueia todos.

A conta em si (o usuário Unix, diretório home, shell) é provisionada pela gestão de configuração junto com o helper `sshd`. O OmniWeb possui a **identidade e as chaves**, e a automação da frota possui **a existência da conta** em cada host.

Configuração

O endpoint que fornece as chaves é protegido pelo mesmo segredo compartilhado que o callback de auditoria:

Variável	Padrão	Descrição
`AUDIT_API_KEY`	`omniweb-audit-key`	Segredo compartilhado que o helper `AuthorizedKeysCommand` de cada host apresenta (como `X-Audit-Key`) ao buscar chaves. **Altere isso**, e defina o valor correspondente em cada host.

Como o OmniWeb é a única coisa que deve ser consultada e o helper é executado em hosts confiáveis, o endpoint é fornecido via HTTPS e o segredo é um segundo portão além do caminho da rede.

Por Que Isso Importa

- **Um lugar para conceder/revogar acesso SSH** em toda a frota: o estado ativo do usuário *é* seu acesso ao host.
- **Sem arquivos de chave espalhados** que ficam fora de sincronia em hosts individuais, e sem servidor de diretório para operar e fazer backup.
- **Uma única identidade** ligando o acesso ao portal de uma pessoa, seu acesso SSH e, através do registro de auditoria, sua atividade registrada.

Relacionado

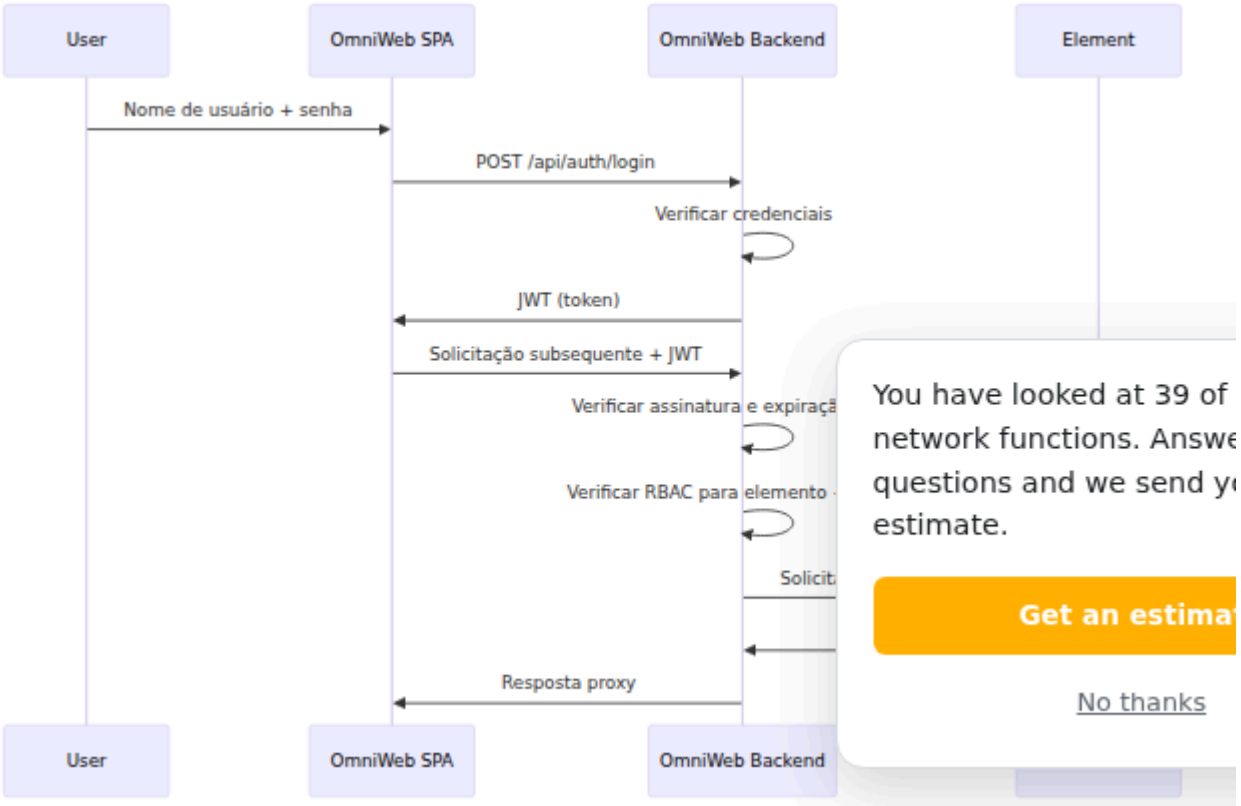
- Registro de Auditoria: registre logins SSH e cada comando executado nos hosts.
- RBAC: controle o que os mesmos usuários podem fazer *dentro* do OmniWeb.

Login e Sessões JWT

OmniWeb autentica operadores com um nome de usuário e senha e emite um JSON Web Token (JWT). Esse token prova quem você é em cada solicitação subsequente. Crucialmente, é a *mesma* credencial que autoriza o Grafana, Loki e Homer incorporados. Um login abrange toda a pilha.

← Autenticação e Controle de Acesso · ← Guia de Operações

Fluxo de Login



O token é emitido por `POST /api/auth/login`. Uma vez obtido, a SPA o apresenta em cada chamada de API, e o backend verifica a assinatura e a expiração antes de fazer qualquer outra coisa.

A tela de login. A autenticação aqui gera o JWT que governa toda a pilha: APIs de elementos, Loki, Grafana e Homer.

Como o Token É Transportado

O backend aceita o JWT em três locais, o que permite que o mesmo token funcione para chamadas de API XHR, navegações no navegador e iframes incorporados:

Localização	Usado para
Cabeçalho de Autorização	Solicitações padrão de API (XHR/fetch) da SPA
Cookie (`access_token`, HttpOnly)	Navegações no navegador e conteúdo incorporado (iframe do Grafana, aba do Homer)
String de consulta	Casos em que nem um cabeçalho nem um cookie podem ser definidos

O cookie é **HttpOnly** (não legível por JavaScript) e usa `SameSite=Lax`, o que protege o token contra roubo via acesso a scripts de sites cruzados, enquanto ainda permite navegações de nível superior para as ferramentas incorporadas.

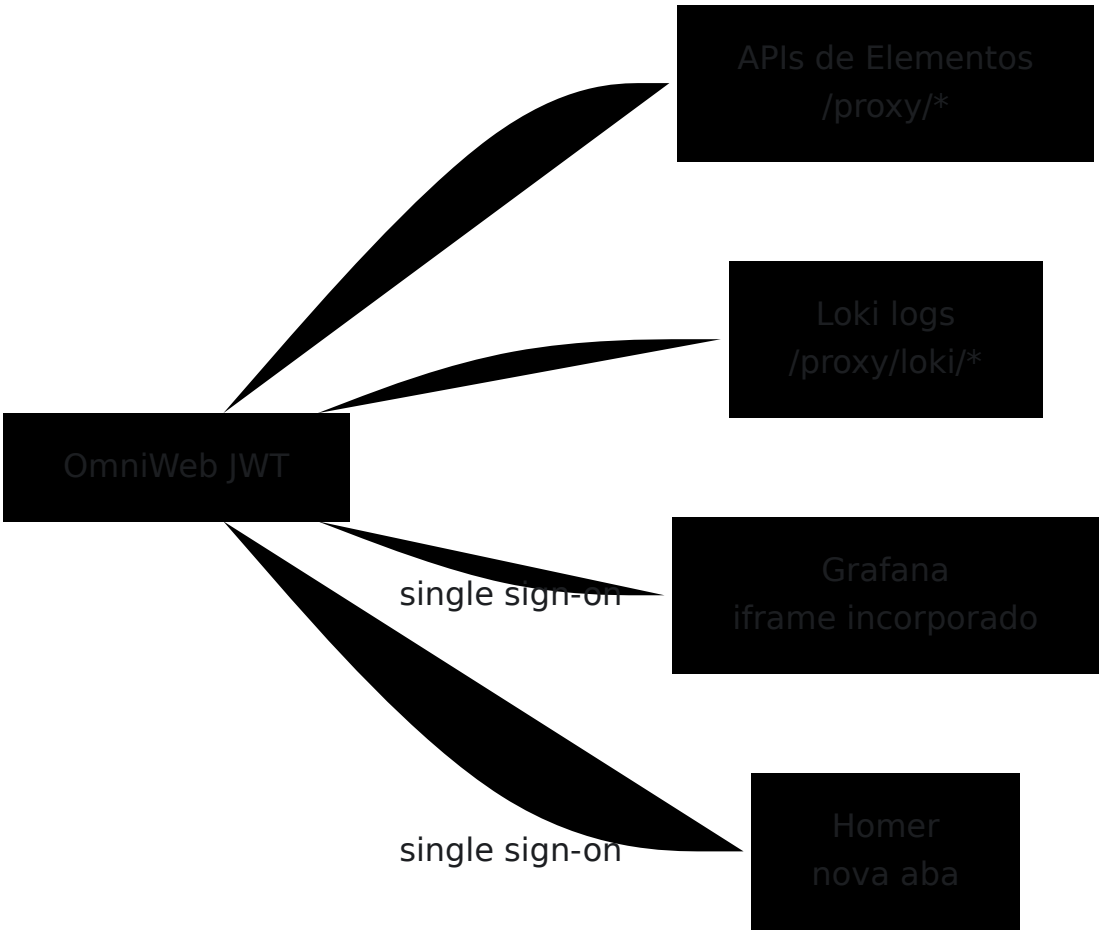
Vida Útil do Token

O token de acesso tem uma expiração configurável, **24 horas por padrão** (`JWT_ACCESS_TOKEN_EXPIRES`, em segundos). Quando expira, o operador é retornado à tela de login e reautentica. Não há sessão silenciosa indefinida; a vida útil é uma fronteira de segurança deliberada.

Configuração	Padrão	Descrição
`JWT_ACCESS_TOKEN_EXPIRES`	`86400` (24 h)	Vida útil do token de acesso em segundos. Reduza para sessões mais restritas; aumente para menos re-logins.
`JWT_SECRET_KEY`	*(gerado)*	Segredo usado para assinar e verificar tokens. Defina explicitamente em produção para que os tokens sobrevivam a uma reinicialização do backend e sejam consistentes entre instâncias.

Um Login, Toda a Pilha

O mesmo JWT autoriza as ferramentas de monitoramento integradas, de modo que os operadores nunca fazem login duas vezes:



- **APIs de Elementos e Loki** são acessadas através do proxy do backend, que verifica o JWT diretamente.
- **Grafana e Homer** são acessados através do gateway autenticado, que verifica seu login no OmniWeb antes de fazer o proxy, sem uma segunda senha. Veja Grafana e Homer.

É por isso que uma única sessão do OmniWeb governa toda a superfície operacional: painéis, logs, rastreamentos e gerenciamento de elementos tudo depende do mesmo token.

Primeiro Login e Mudança de Credenciais

Uma nova implantação é enviada com uma conta de administrador padrão (`admin` / `admin`). **Altere isso imediatamente** após o primeiro login, via Configurações. O padrão existe apenas para inicializar o sistema e não deve sobreviver em produção.

Logout e Expiração

Fazer logout descarta o token. Um token expirado ou inválido faz com que a próxima solicitação seja rejeitada e a SPA retorne à tela de login. Como as ações de elementos são sempre realizadas através de uma chamada proxy autenticada e verificada pelo RBAC, uma sessão expirada nunca pode realizar uma ação privilegiada.

Relacionados

- Controle de Acesso Baseado em Funções: o que um usuário autenticado pode fazer.
- Registro de Auditoria: cada ação autenticada é registrada.

Controle de Acesso Baseado em Função (RBAC)

Estar autenticado informa ao OmniWeb *quem* você é. O RBAC decide *o que você pode fazer*. O acesso é concedido de forma detalhada, **por tipo de elemento, por método HTTP**, que mapeia diretamente as operações reais que um operador realiza: visualizar, modificar ou excluir. Além disso, dois escopos decidem *onde*: quais **sites** um operador pode acessar e quais **dispositivos de teste** eles podem usar. Cada solicitação deve passar por todos eles.

← Autenticação & Controle de Acesso · ← Guia de Operações

Níveis de Permissão

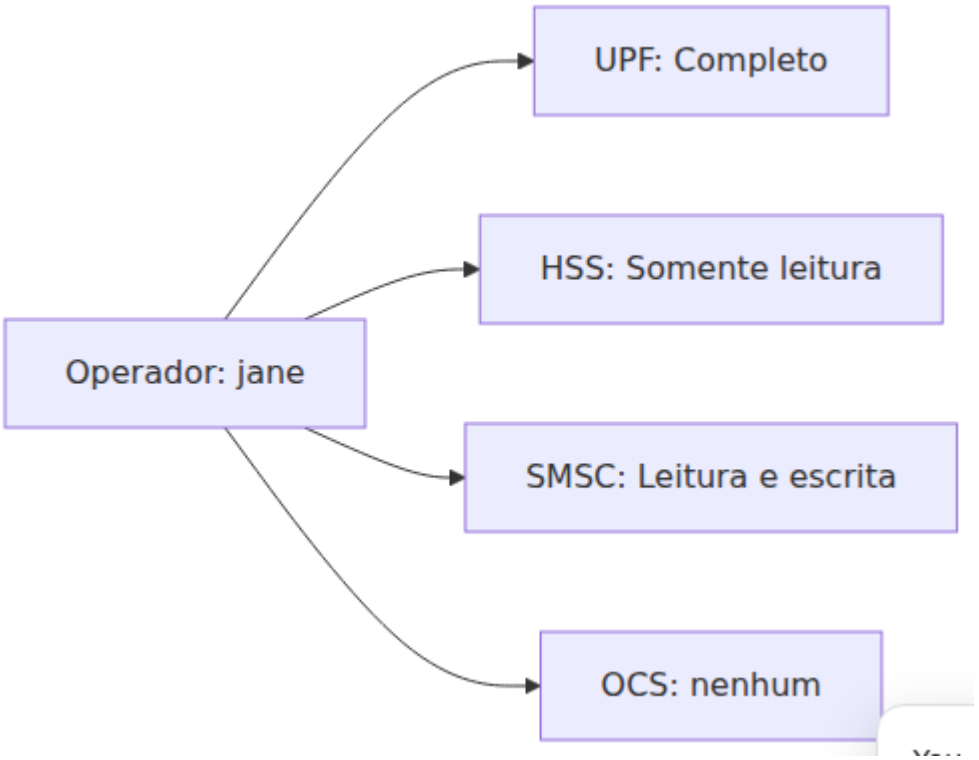
Cada tipo de elemento pode ser concedido a um usuário em um de três níveis. O nível é expresso como o conjunto de métodos HTTP que o usuário pode usar contra esse elemento através do proxy:

Permissão	Métodos permitidos	O que o operador pode fazer
Somente leitura	`GET`	Visualizar dados apenas, sem alterações
Leitura e escrita	`GET`, `POST`, `PUT`, `PATCH`	Visualizar e modificar: por exemplo, adicionar um assinante, editar uma rota, alterar uma regra de QoS
Completo	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	Tudo, incluindo exclusão e limpeza de sessões

Como as permissões estão vinculadas aos métodos HTTP, elas se alinham exatamente com o modelo de edição genérico: um formulário "Adicionar" é um `POST`, um "Editar" é um `PUT`/`PATCH`, e um "Excluir"/"limpar" é um `DELETE`.

Granularidade por Elemento

As permissões são atribuídas **independentemente por tipo de elemento**. Um usuário pode ter diferentes níveis em diferentes elementos:



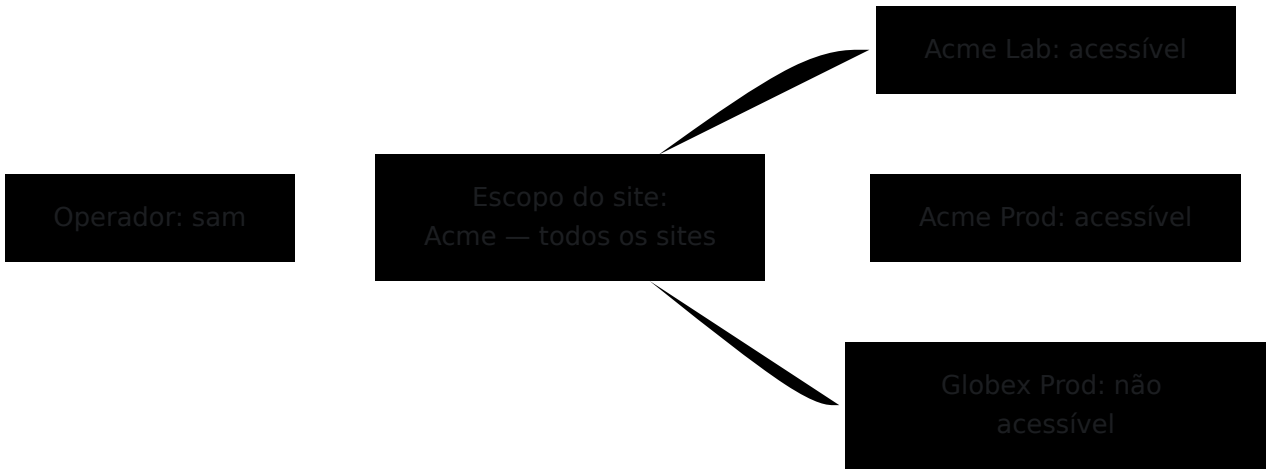
Neste exemplo, Jane pode limpar sessões do UPF, pode visualizar mas não alterar o HSS, pode adicionar rotas ao SMSC e não pode ver o OCS de forma alguma. Isso permite que você conceda, por exemplo, a um engenheiro de dataplane controle total do UPF enquanto mantém os dados do assinante como somente leitura.

Escopo do Site (Implantações Multi-Site)

As permissões de elemento respondem *o que* um operador pode fazer. Em uma frota com mais de um site, um segundo eixo independente responde *onde*: o

conjunto de sites que eles podem acessar. Uma solicitação deve satisfazer ambos.

Por padrão, um usuário é **sem restrições** — ele pode acessar todos os sites, incluindo sites adicionados posteriormente. Restringir um usuário a um ou mais sites limita-o exatamente a esses, e um cliente inteiro pode ser concedido de uma só vez, de modo que novos sites para esse cliente sejam incluídos automaticamente.



Um operador com escopo vê apenas seus próprios sites no seletor de sites; os outros não são listados, e os elementos, logs, métricas, inventário de software e rastreamentos de chamadas por trás deles são recusados no lado do servidor. Administradores acessam todos os sites, independentemente do escopo.

O escopo do site é gerenciado em **Configurações → Usuários**, a partir da ação do globo na linha de um usuário. Marque os sites que eles podem acessar ou deixe tudo desmarcado para deixá-los sem restrições.

Escopo do Dispositivo de Teste (Fazenda de Telefones)

A fazenda de telefones é um único tipo de elemento — **Dispositivos de Teste** — cobrindo cada bancada, telefone e modem, suas ferramentas e seus testes programados. Concedê-lo segue a mesma regra por método que qualquer outro elemento:

Permissão	O que o operador pode fazer com os telefones
Somente leitura	Listar as bancadas e dispositivos, assistir à tela de um telefone, ler logs, baixar arquivos e visualizar resultados de testes
Leitura e escrita	Também digitar em um telefone, enviar comandos AT e SMS, fazer upload de arquivos e executar um script de teste
Completo	Também remover um registro de dispositivo e limpar seus metadados atribuídos

Assistir à tela de um telefone é tratado como uma **leitura**, não uma alteração — um operador que pode apenas observar ainda pode ver o que uma bancada está fazendo. Digitar no telefone é uma ação separada, de nível de escrita.

Como toda a fazenda é um tipo de elemento, uma concessão é, de outra forma, tudo ou nada. Para dar a alguém apenas *alguns* dos telefones, defina um **escopo de dispositivo**: marque os dispositivos individuais que eles podem usar, agrupados por bancada. Não marcar nada os deixa sem restrições — cada dispositivo, incluindo aqueles adicionados posteriormente.

Um operador com escopo de dispositivo vê apenas seus próprios dispositivos na lista da frota, vê cada bancada limitada àqueles dispositivos (e bancadas sem nenhum deles não são vistas de forma alguma) e é recusado se nomear outro dispositivo diretamente. Executar um script em vários telefones é recusado imediatamente se qualquer um deles estiver fora de seu escopo, em vez de ser executado silenciosamente no subconjunto — uma execução parcial seria lida como uma aprovação completa. Editar a lista de programação substitui todo o conjunto, de modo que isso permanece com operadores que possuem todos os dispositivos.

O escopo do site e o escopo do dispositivo são independentes: a fazenda de telefones é deliberadamente independente do site, uma vez que uma bancada não faz parte de uma implantação de rede.

Ambos são definidos em **Configurações → Usuários**, a partir da ação do globo na linha de um usuário.

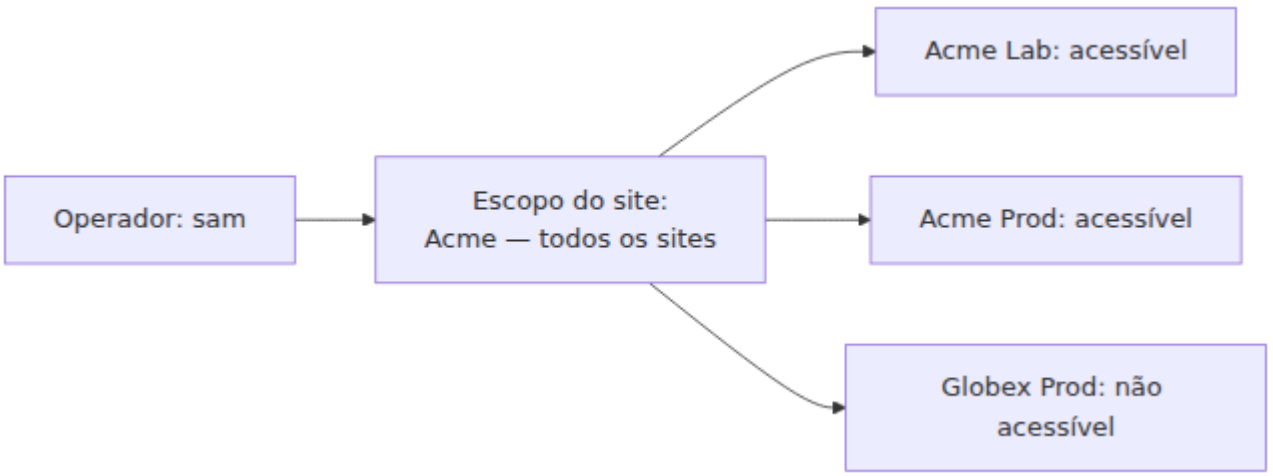
> **Na atualização:** a fazenda de telefones anteriormente precisava apenas de um login, então cada conta que existia antes dessa mudança mantém acesso total aos Dispositivos de Teste, registrado como uma concessão normal. Reforce da mesma forma que qualquer outro elemento: revogue **Dispositivos de Teste** de quem não deve ter os telefones e defina um escopo de dispositivo para quem deve ter apenas alguns. Contas criadas posteriormente começam sem acesso até serem concedidas.

Administradores

Os administradores têm acesso total a todos os tipos de elementos automaticamente. O papel de administrador também é o que concede acesso à gestão de usuários e permissões. Mantenha o número de administradores pequeno e prefira concessões específicas por elemento para todos os outros.

Gerenciando Funções e Permissões

As permissões são gerenciadas em **Configurações → Permissões**. Para cada usuário que você escolher, por tipo de elemento, se eles têm acesso somente leitura, leitura e escrita ou total (ou nenhum).

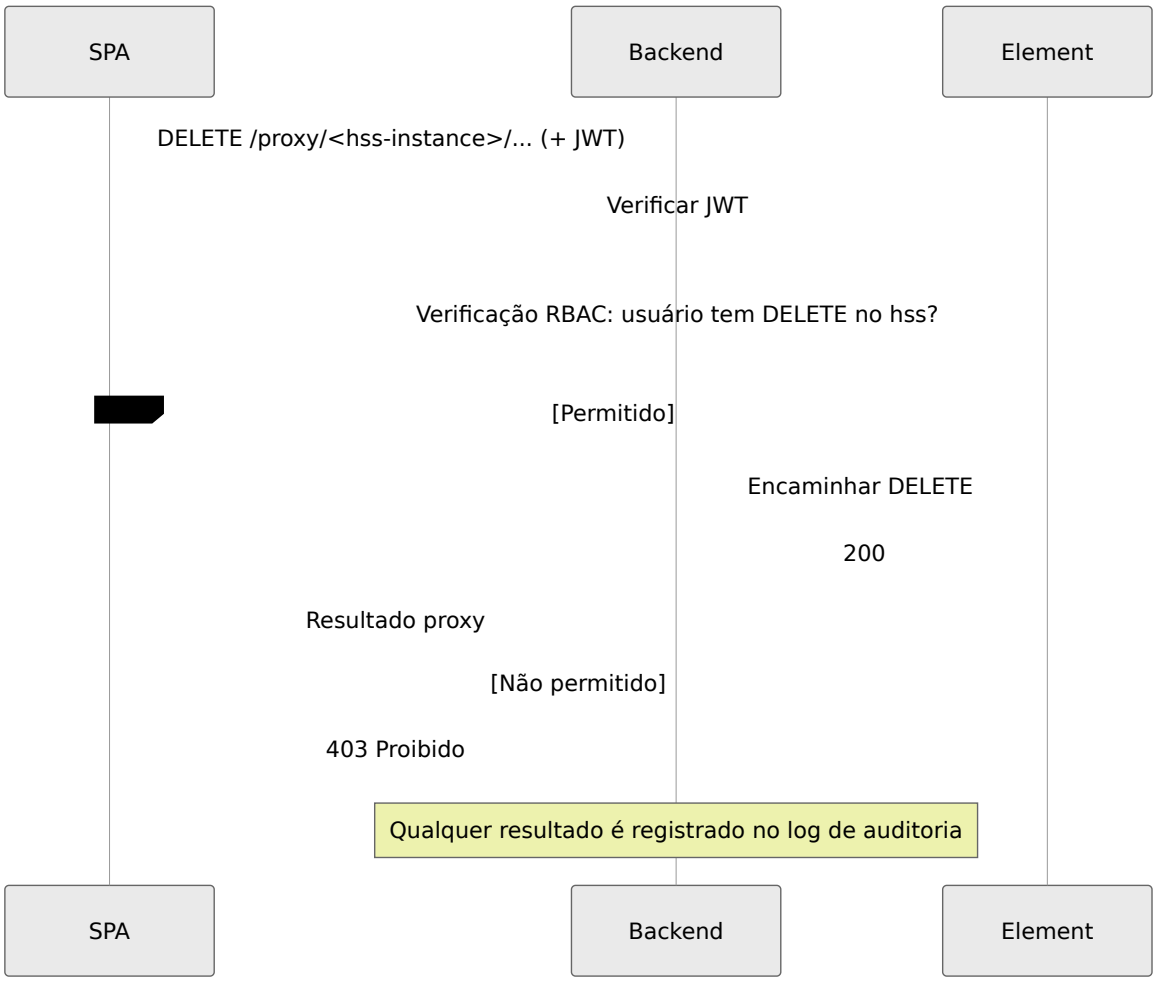


Como a Aplicação Funciona

O RBAC é aplicado em dois lugares complementares:

1. **Na interface do usuário**: controles para ações que você não pode realizar não são exibidos. Se você tiver apenas acesso de leitura ao HSS, não verá botões Adicionar/Editar/Excluir lá.
2. **No backend**: cada solicitação proxy é re-verificada em relação às suas permissões *no lado do servidor*. Mesmo uma solicitação elaborada para contornar a interface do usuário é rejeitada se seu papel não permitir aquele elemento/método — ou se nomear um elemento em um site fora do seu escopo de site. O site em que uma solicitação atua é retirado da própria solicitação, portanto, é verificado em vez de confiável.

Essa "defesa em profundidade" significa que a interface do usuário é uma conveniência, não o limite de segurança. O proxy do backend é o limite.



Configurações → Permissões: selecione um usuário e, em seguida, conceda um nível (somente leitura, leitura e escrita ou total) por tipo de elemento.

Credenciais Enviadas para Elementos

O proxy não envia suas credenciais do OmniWeb para um elemento. Antes de encaminhar uma solicitação, ele remove estes itens:

- O cabeçalho `Authorization` (seu JWT do OmniWeb).
- O cabeçalho `X-API-Key` (sua chave de API pessoal do OmniWeb).
- Todos os cookies, que incluem o cookie `access_token` do OmniWeb.
- Os cabeçalhos `x-omnihss-key` e `x-omnihss-user`. Apenas o OmniWeb define esses cabeçalhos. Um valor que vem do navegador é sempre removido.

OmniHSS

A API do OmniHSS usa controle de acesso baseado em função. Cada cliente deve enviar sua própria chave. O OmniWeb envia esses cabeçalhos em cada solicitação para uma instância do OmniHSS:

Cabeçalho	Valor
`x-omnihss-key`	A chave do OmniWeb para o OmniHSS, de `OMNIHSS_API_KEY`.
`x-omnihss-user`	Seu nome de usuário do OmniWeb. O OmniHSS registra como o usuário que realizou a ação. Este é o mesmo nome que o log de auditoria do OmniWeb mostra.

O OmniWeb lê `OMNIHSS_API_KEY` de `/etc/omniweb/omniweb.env`. O OmniCore escreve esse valor quando o inventário do site tem um grupo `hss`. O OmniHSS dá a essa chave o papel `oam`.

O OmniWeb também envia a chave quando o backend chama o próprio OmniHSS: a guia Estado ao Vivo do HSS, a verificação da versão do elemento, as buscas de assinantes do SIM Virtual e o teste IR.38 Cancelar Localização.

Se `OMNIHSS_API_KEY` não estiver definido, o OmniWeb não envia a solicitação para o OmniHSS. O proxy retorna `502` com uma mensagem de erro que nomeia `OMNIHSS_API_KEY`, e o log do backend registra o mesmo erro. O OmniWeb não grava o valor da chave em um log.

Boas Práticas

- **Menor privilégio**: conceda o nível mais baixo que permita a alguém fazer seu trabalho; amplie apenas quando necessário.
- **Somente leitura por padrão** para elementos que um operador só precisa observar.
- **Reserve Completo (DELETE)** para aqueles que realmente precisam limpar sessões ou remover registros.

- **Poucos administradores**: use concessões direcionadas por elemento em vez de distribuir admin.
- **Escopo por site** em uma frota multi-site: dê aos operadores de um cliente seus próprios sites, para que um erro não possa alcançar outra implantação.
- **Escopo dispositivos de teste** para os telefones pelos quais alguém é responsável, para que a execução de um script não possa perturbar a bancada de outra equipe.
- **Fixar credenciais de serviço**: uma chave de API pode ser restrita a menos sites do que seu proprietário, para que uma chave emitida para uma implantação não possa agir em outra. Uma chave só pode ser mais restrita do que a conta a que pertence, nunca mais ampla.

Relacionados

- Login & Sessões JWT: autenticação na qual o RBAC se baseia.
- Operações Comuns: como as permissões moldam a interface do dia a dia.
- Registro de Auditoria: tanto ações permitidas quanto negadas são registradas.

Autenticação & Controle de Acesso

OmniWeb é a única porta de entrada para toda a rede, portanto, o controle de acesso é uma de suas responsabilidades mais importantes. Ele utiliza login baseado em JWT, controle de acesso baseado em funções (RBAC) detalhado sobre cada elemento, login com chave SSH para acesso ao host e um registro de auditoria unificado que abrange o portal e os hosts que gerencia.

Esta área está dividida em páginas focadas:

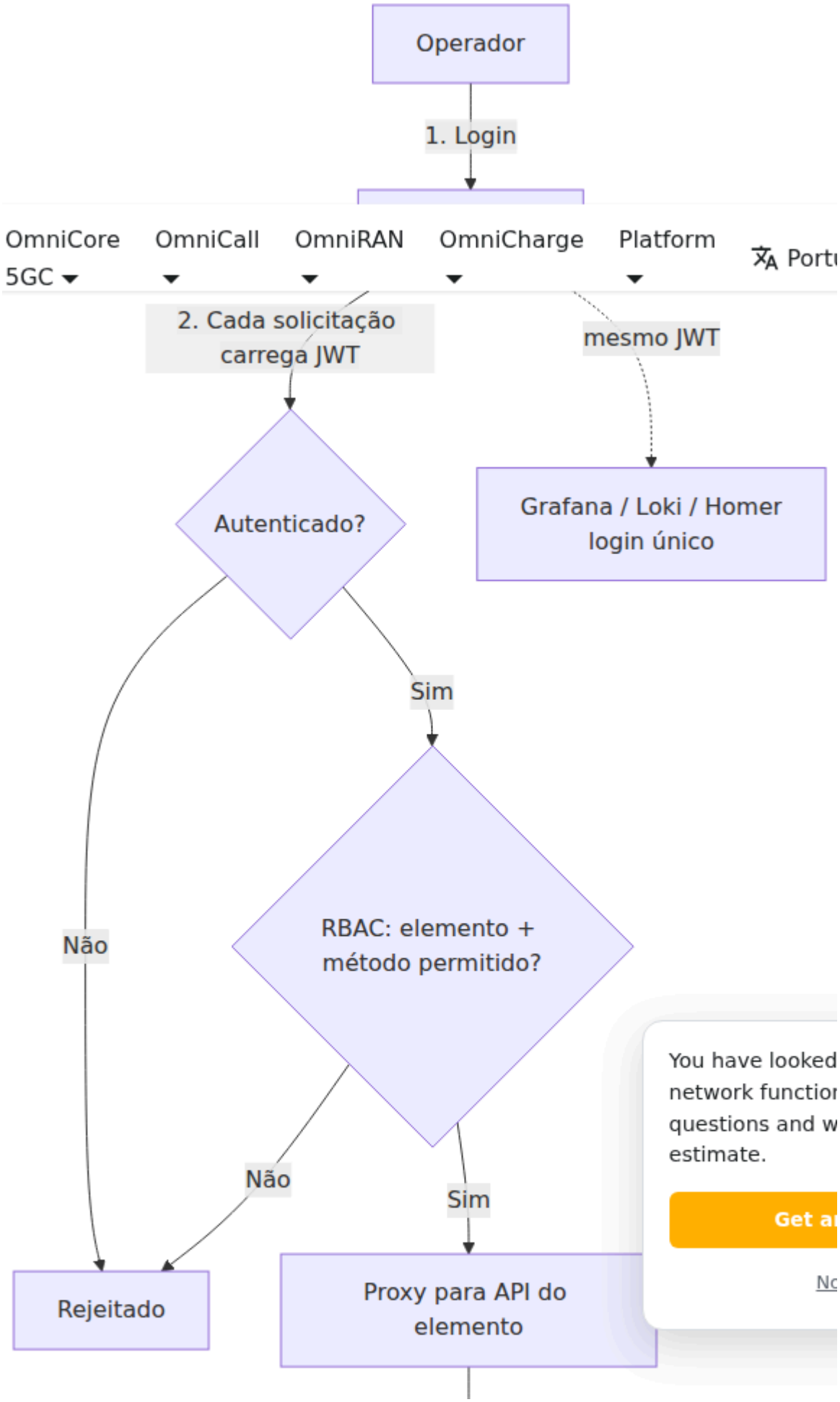
← Voltar ao Guia de Operações

Nesta Seção

- **Login & Sessões JWT**: Como os operadores fazem login, como o JWT funciona, duração do token e como um único login abrange Grafana, Loki e Homer.
- **Controle de Acesso Baseado em Funções (RBAC)**: Permissões por elemento e por método; como concedê-las; e como são aplicadas.
- **Login com Chave SSH**: Hosts gerenciados buscam a chave pública SSH de cada usuário ao vivo do OmniWeb (AuthorizedKeysCommand), portanto, o acesso ao host é concedido/revogado centralmente.
- **Registro de Auditoria**: As três camadas de auditoria: auditoria de solicitação do portal, auditoria de login SSH e auditoria de comandos.

O Modelo de Controle de Acesso

OmniWeb sobrepõe quatro controles. Uma solicitação deve passar por cada um antes de alcançar um elemento, e toda a cadeia é registrada.


Operador
1. Login
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Portu
2. Cada solicitação carrega JWT
mesmo JWT
Autenticado?
Grafana / Loki / Homer login único
Sim
Não
RBAC: elemento + método permitido?
Não
Sim
Rejeitado
Proxy para API do elemento



Camada	O que controla	Página
Autenticação	Quem você é, provado por um JWT assinado	Login & JWT
Autorização (RBAC)	O que você pode fazer, por tipo de elemento e método HTTP	RBAC
Acesso ao host	Quem pode SSH onde; chaves servidas ao vivo do OmniWeb	Login com Chave SSH
Auditoria	O que realmente aconteceu, através do portal e dos hosts	Registro de Auditoria

Por Que Isso É Importante

Como o OmniWeb faz proxy para cada elemento, painel do Grafana, consulta do Loki e sessão do Homer, essa única cadeia de controle de acesso governa toda a superfície operacional da rede. Há um lugar para conceder acesso, um lugar para revogá-lo e um registro que documenta quem fez o quê, no portal e nos hosts subjacentes.

Um registro para tudo: solicitações de API, logins, logins SSH e mudanças de permissão, com usuário, elemento, método, resultado e IP de origem. Veja Registro de Auditoria.

Comece com Login & Sessões JWT.

Rastreio de Chamadas (SIP Trace)

Rastreio de Chamadas é a ferramenta OmniWeb para solução de problemas de chamadas de voz. Ela registra o sinal SIP e a mídia RTP das chamadas que cruzam o IMS. Em seguida, permite que você pesquise essas chamadas, abra um relatório completo por chamada, siga a chamada como uma escada de sinalização através da rede, meça a qualidade da voz, ouça o áudio e baixe a captura de pacotes brutos (PCAP).

O Rastreio de Chamadas é uma ferramenta de nível de site. Ele aparece na barra lateral sob **Rastreio de Sessão** como **SIP Trace**. A ferramenta só aparece quando o serviço de captura está configurado e acessível para o site selecionado.

← Guia de Operações

Conteúdo

- O que é
- Arquitetura
- Pesquisa
- Detalhes da chamada
- Escada (Rastreio de Sessão)
- Aba QoS
- Ouvir
- Download de PCAP
- Chamadas Ativas
- Sniffer Ao Vivo
- Registros
- Agentes de Captura Remota
- Regras de Gravação e Retenção

- Privacidade e interceptação legal
- Como o Rastreio de Chamadas se compara ao Homer e ao Rastreio de Sessão

O que é

O Rastreio de Chamadas responde a uma pergunta em profundidade: **o que aconteceu com esta chamada?** Para qualquer chamada gravada, ele fornece:

- As duas partes, seus números, seus domínios SIP e o nome exibido.
- O endereço IP SIP de cada parte, vinculado ao seu elemento de rede OmniWeb.
- A resposta SIP final e o motivo da desconexão (SIP e Q.850).
- A qualidade da voz de cada direção de mídia: MOS, jitter, perda de pacotes e atraso de ida e volta.
- O fluxo completo de mensagens SIP (escada) através de cada elemento IMS que tocou a chamada.
- O áudio gravado e o PCAP bruto.

O Rastreio de Chamadas registra chamadas em primeira mão. Como captura o SIP Call-ID e a mídia na rede, uma chamada se mapeia para sua captura de pacotes sem adivinhações.

A qualidade da voz é relatada como **MOS** (Mean Opinion Score). MOS é uma pontuação de 1 a 5. Uma pontuação de 4.0 ou mais é boa, de 3.0 a 4.0 é razoável, e abaixo de 3.0 é ruim. O OmniWeb colore os valores MOS: verde para bom, âmbar para razoável e vermelho para ruim. Chamadas AMR-WB (wideband) em uma rede saudável pontuam cerca de 4.5.

Arquitetura

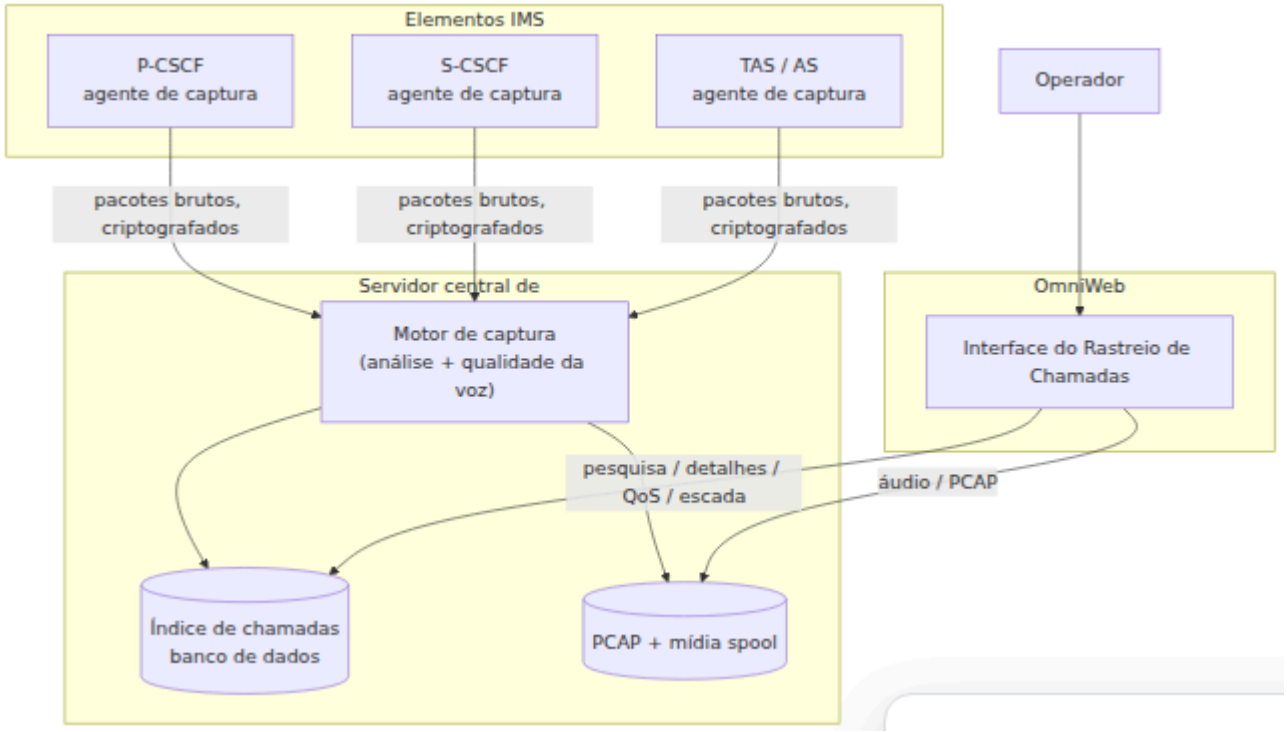
O Rastreio de Chamadas utiliza duas partes:

1. **Agentes de captura** que rodam nos elementos IMS (P-CSCF, S-CSCF e o TAS). Cada agente captura os pacotes SIP e RTP que vê em seu host. Os

agentes não armazenam ou analisam pacotes localmente. Eles encaminham os pacotes brutos para o servidor central de captura através de um canal criptografado.

2. O **servidor central de captura** analisa cada pacote, calcula a qualidade da voz e escreve um índice em seu banco de dados. Ele mantém o spool de captura de pacotes e a mídia gravada. O OmniWeb lê este único servidor para pesquisa, detalhes da chamada, escada, QoS, áudio e PCAP.

Esse design mantém todos os dados gravados em um único servidor central. Os elementos IMS não mantêm dados de captura próprios.



Os agentes de captura dão ao Rastreio de Chamadas uma visão de muitos pontos na rede. Uma única chamada é montada a partir de cada agente que a viu. Isso é o que permite que a escada mostre o fluxo SIP de múltiplos saltos através do P-CSCF, do S-CSCF e do TAS.

Pesquisa

Abra o Rastreio de Chamadas para acessar a visualização de **Pesquisa**. A pesquisa encontra chamadas concluídas no índice central de chamadas.

Visualização de Pesquisa. Cada linha empilha a parte chamadora e chamada (número, domínio, nome, IP SIP e agente de usuário) ao lado de células RTP por direção que mostram IP de origem, codec, três estimativas de MOS, jitter e perda.

Filtros

Defina um ou mais filtros e, em seguida, selecione **Pesquisar**. Todos os filtros combinam com AND.

Filtro	O que corresponde
Número	O número do chamador OU o número do chamado.
Intervalo de Tempo	Uma janela pré-definida (Últimos 15m a Últimos 7d) ou um início e fim personalizados.
Direção	Inbound, Outbound ou Interno. A direção vem do papel do IP do chamador e do chamado.
Min MOS	Mantenha apenas chamadas cuja pior direção de MOS esteja neste valor ou acima. Use isso para encontrar boas chamadas, ou inverta sua leitura para encontrar as ruins.
Max perda	Mantenha apenas chamadas cuja pior direção de perda de pacotes esteja neste valor ou abaixo.

Grade de resultados

Cada linha de resultado mostra:

- **Hora**: o início e o fim da chamada.
- **Chamador** e **Chamado**: uma célula empilhada com o número e domínio (`num@domain`), o nome exibido, o IP SIP (um link para aquele elemento no OmniWeb) e o agente de usuário. Um chip de **desconexão** marca a parte que enviou o BYE.
- **Resultado**: o código e texto da resposta SIP final.
- **RTP A** e **RTP B**: uma célula por direção de mídia. Cada célula mostra o IP de origem, o codec, três estimativas de MOS (fixo 50 | fixo 200 | adaptativo), o jitter e a contagem de pacotes perdidos. Os três valores de MOS são codificados por cor.
- **Dur (s)**: a duração da chamada em segundos.
- **PCAP**: um botão de download por linha para a captura de pacotes daquela chamada.

Selecione uma linha para abrir os detalhes da chamada.

Detalhes da chamada

A visualização de detalhes da chamada é o relatório completo para uma chamada. Ela é aberta quando você seleciona um resultado de pesquisa. A URL carrega o identificador da chamada, para que você possa adicionar aos favoritos ou compartilhar uma chamada.

Visualização de detalhes da chamada. O cabeçalho mostra o Call-ID e o contexto. A faixa de resumo mostra Início, Duração, PDD, Tocando, Conectado, a última resposta SIP e os motivos da desconexão. A tabela de duas colunas mostra Identidade e qualidade de voz para as pernas Chamador (A) e Chamado (B).

Cabeçalho e contexto

O cabeçalho mostra o **Call-ID** da rede. Um bloco de contexto abaixo dele mostra a **Direção** da chamada, o **Sensor** proprietário (o agente de captura), qual parte **Desconectou**, o tempo **Encerrado** e o **Nome do Chamador**.

Faixa de resumo

A faixa de resumo é uma visão geral de uma linha da chamada:

Campo	Significado
Início	Quando a chamada começou.
Duração	Duração total da chamada.
PDD	Atraso pós-discagem: o tempo desde o INVITE até a primeira indicação de toque.
Tocando	Quanto tempo o telefone tocou antes de ser atendido.
Conectado	Quanto tempo a chamada esteve conectada (fluxo de mídia).
Última resposta SIP	O código e texto da resposta SIP final.
Motivo SIP	A causa da desconexão SIP, quando o motor de captura registra uma.
Motivo Q.850	A causa e texto da desconexão Q.850, quando presente.
Chamador e **Chamado**	As duas partes como `num@domain`.

Tabela de Identidade e qualidade de voz

A tabela principal tem duas colunas: **Chamador (A)** e **Chamado (B)**. Cada IP se vincula ao seu elemento de rede OmniWeb quando o elemento é conhecido. A tabela tem três grupos.

Identidade:

Linha	Significado
IP SIP	O IP de sinalização SIP da parte.
IP RTP	O IP de mídia RTP da parte.
Porta RTP	A porta de mídia RTP.
Agente de Usuário	O agente de usuário SIP da parte.
Codec	O codec de áudio, por exemplo, AMR-WB.
Pacotes recebidos	A contagem de pacotes RTP recebidos.
Pacotes perdidos	A contagem de pacotes RTP perdidos.

MOS: três estimadores de MOS, cada um mostrado como `média | mínimo`:

Linha	Significado
MOS fixo 50	MOS sobre uma janela fixa de 50 pacotes.
MOS fixo 200	MOS sobre uma janela fixa de 200 pacotes.
MOS adaptativo 500	MOS sobre uma janela adaptativa de até 500 pacotes.

Jitter e RTCP: o jitter RTP (máximo e médio), o jitter RTCP, a contagem de perda e fração de pacotes perdidos do RTCP, e o atraso de ida e volta do RTCP (máximo e médio).

Escada (Rastreio de Sessão)

A aba **Escada** desenha a chamada como um fluxo de sinalização ordenado por tempo. O Rastreio de Chamadas costura as mensagens SIP juntas de cada agente de captura que viu a chamada. O resultado é uma escada de múltiplos saltos através dos elementos IMS: por exemplo, de P-CSCF para S-CSCF para TAS.

A aba Escada. As colunas são os elementos IMS pelos quais a chamada passou. Cada rampa é uma mensagem SIP. A escada mostra o fluxo de INVITE para 100 para 180 para 200 para ACK para BYE, com deltas de tempo por mensagem e o atraso de ida e volta da solicitação à resposta.

Cada coluna é um elemento IMS, rotulado com seu papel e nome do host. Cada rampa é uma mensagem SIP desenhada da origem ao destino. A escada mostra:

- O **delta de tempo por mensagem** (o intervalo desde a mensagem anterior).
- O **atraso de ida e volta da solicitação à resposta** para cada resposta, pareado de volta à sua solicitação.

- Modos de tempo **absoluto**, **relativo** e **passado** para a coluna de tempo.
- **Decodificação de pacotes inline**: selecione uma rampa para ver o texto completo da mensagem SIP e uma visualização em hex.

Um painel de **Detalhes da Sessão** lista as sessões na escada. Para uma única chamada, há uma sessão, então o painel permanece recolhido.

A escada usa a mesma renderização que os Fluxos Ao Vivo de Rastreio de Sessão em toda a rede. Veja Logs & Rastreio de Assinantes para a ferramenta de Rastreio de Sessão mais ampla.

Aba QoS

A aba **QoS** mostra a qualidade da voz ao longo da vida da chamada.

A aba QoS. As tabelas mostram os buckets de distribuição de PDV (atraso) e a divisão de perda em sequência para cada direção. Um gráfico interativo de qualidade de atraso e MOS é desenhado ao longo da duração da chamada abaixo das tabelas.

A aba QoS tem três partes:

- Um **gráfico de qualidade RTP** interativo por fluxo de mídia, disposto da mesma forma que a GUI do VoIPmonitor. Os fluxos principais do chamador (A) e do chamado (B) vêm primeiro, seguidos por quaisquer outros fluxos na chamada. Cada painel desenha o atraso de cada pacote, sombreia cada coluna de 20 pacotes que perdeu pacotes (colorido pela quantidade perdida), passa os três estimadores de MOS (fixo 50, fixo 200, adaptativo 500) pelos seus intervalos de 10 segundos, e marca bits e DTMF ao longo do topo. Passe o mouse para valores e arraste a faixa abaixo dos painéis para ampliar.
- A **distribuição de PDV (atraso)**: quantos pacotes caíram em cada bucket de atraso (por exemplo, 50 a 70 ms, 70 a 90 ms, e assim por diante até mais de 300 ms). Uma distribuição que permanece nos buckets baixos é saudável.
- A divisão de **perda em sequência**: quantas vezes 1, 2, 3 e até 10 pacotes foram perdidos consecutivamente. Perdas isoladas são muito menos audíveis do que longas sequências de perda.

Ambas as divisões são mostradas por direção (Chamador e Chamado), para que você possa identificar qual perna teve o problema.

Ouvir

O painel **Ouvir** reproduz a chamada gravada no navegador. O áudio é decodificado da RTP capturada. O chamador é o canal esquerdo e o chamado é o canal direito, para que você possa ouvir cada lado separadamente.

Ouvir só funciona quando a mídia da chamada foi gravada e seu codec pode ser decodificado. Veja Regras de Gravação e Retenção para como a captura de mídia é armada.

Download de PCAP

Cada chamada tem um botão **Baixar PCAP**, tanto na grade de pesquisa quanto no cabeçalho de detalhes da chamada. O download é a captura de pacotes brutos (SIP e, quando gravado, RTP) daquela única chamada. Use o

PCAP para inspecionar a chamada em uma ferramenta externa como o Wireshark.

Chamadas Ativas

A visualização **Chamadas Ativas** mostra chamadas que estão em andamento agora. Ela lê a lista de chamadas ao vivo dos agentes de captura e atualiza em um curto intervalo, então linhas aparecem e desaparecem conforme as chamadas são configuradas e encerradas.

Visualização de Chamadas Ativas. Cada linha é uma chamada ao vivo com seu estado (Conectado ou Configuração), as duas partes e seus endereços IP, a direção, a duração crescente, o codec, o MOS ao vivo e o agente de captura proprietário.

Cada linha mostra o **Estado** da chamada (Conectado, Configuração ou Falhando), as duas partes, o caminho IP do chamador para o chamado, a **Direção**, a **Duração** crescente, o **Codec**, o **MOS** ao vivo, a última resposta SIP e o **Sensor** proprietário (agente de captura). Desligue o **Auto-atualizar** para manter a lista atual.

Sniffer Ao Vivo

A visualização **Sniffer Ao Vivo** mostra a saúde do servidor central de captura e seus agentes de captura.

Visualização Sniffer Ao Vivo. O painel do Servidor Central mostra versão, tempo de atividade, contagem de chamadas ativas, throughput, perdas de pacotes e média de carga. A tabela de Agentes de Captura Remota lista cada agente. O painel de I/O de disco do Spool mostra utilização e throughput.

A visualização mostra:

- **Servidor Central**: versão e build, tempo de atividade, contagem de chamadas ativas, throughput de captura, perdas de pacotes, média de carga e a última vez que um registro de chamada foi escrito.
- **Agentes de Captura Remota**: os agentes por elemento e seu status (veja Agentes de Captura Remota).
- **I/O de Disco do Spool**: a utilização, throughput de leitura e escrita, IOPS, latência, capacidade utilizada e nível de buffer do disco de spool de captura.
- Um feed de atividade ao vivo das chamadas em andamento.

Observe esta visualização para confirmar que o motor de captura está saudável, não está descartando pacotes e tem espaço livre no disco do spool.

Registros

A visualização **Registros** mostra quem está registrado no IMS e quem está falhando, conforme os agentes de captura viram na rede. É independente do que o HSS acredita: o HSS registra o que o S-CSCF lhe disse, esta visualização registra as solicitações e respostas REGISTER em si.

Ela é acessada através de **Monitoramento → Registros** e está disponível quando o servidor de captura está rodando com rastreamento de registro ativado.

O servidor de captura mantém três registros, e a visualização lê todos eles:

- **Transições de estado**: uma linha cada vez que um registro muda de estado. Registrado, Falhado, Expirado, Não Registrado e Inundação de Registro (um dispositivo se registrando com muita frequência).
- **Tentativas falhadas**: solicitações REGISTER que foram recusadas, agrupadas em rajadas com uma contagem de tentativas.
- **Contagem ativa**: o número de registros ativos que cada agente de captura mantém, uma vez por minuto.

Um registro é visto duas vezes em um núcleo IMS: o próprio REGISTER do dispositivo no P-CSCF, e o REGISTER de terceiros do S-CSCF para o servidor de aplicação. O interruptor **Assinantes** mostra apenas o primeiro, então cada linha é um dispositivo; **Todas as pernas** adiciona o segundo, para seguir um registro através do núcleo.

O que a página mostra

- **Tiles**: assinantes registrados agora, registros e tentativas falhadas na última hora, expirações e desregistros na última hora, e quando o rastreamento começou.
- **Registros ativos ao longo do tempo**: por agente de captura, a partir da contagem de minutos do servidor.

- **Mudanças de estado ao longo do tempo**: transições por estado e tentativas falhadas, ao longo do intervalo selecionado (1 hora a 7 dias).
- **Ativos**: cada registro cujo último estado é Registrado e cuja expiração ainda está por vir, com o endereço do dispositivo, quando se registrou, sua expiração e o tempo restante.
- **Eventos**: cada transição, a mais nova primeiro, filtrada por estado.
- **Falhados**: rajadas de REGISTER recusadas com a contagem de tentativas e o domínio.

Pesquise por IMSI, MSISDN ou nome de usuário SIP, e restrinja a um agente de captura. Selecione uma linha para abrir o histórico próprio daquele assinante: se está registrado agora, cada mudança de estado e cada tentativa falhada.

Quando o HSS e o sniffer discordam

Um assinante que o HSS mostra como registrado, mas o sniffer não viu o registro, ou o inverso, aponta para o elemento entre eles. Um registro que chega ao P-CSCF, mas nunca produz um estado Registrado, com falhas crescendo, é um problema de autenticação ou roteamento no I-CSCF ou S-CSCF. Um dispositivo se registrando a cada poucos segundos é o estado de Inundação de Registro, e geralmente um problema de dispositivo.

Agentes de Captura Remota

A tabela **Agentes de Captura Remota** (na visualização Sniffer Ao Vivo) lista os agentes de captura que rodam nos elementos IMS. Cada linha mostra:

Coluna	Significado
Agente	O nome do host do agente. Selecione-o para abrir aquele host na Lista de Hosts.
ID do Sensor	O identificador numérico do agente no índice de captura.
Status	Ativo, Ocioso ou Desconhecido, derivado de chamadas ao vivo e registros de chamadas recentes.
Chamadas ativas	Quantas chamadas o agente está capturando agora.
CDRs	Quantos registros de chamadas o agente produziu.
Última vez visto	Quando o agente produziu pela última vez um registro de chamada.

Use esta tabela para confirmar que cada elemento IMS que deveria capturar está capturando. Um agente que está inesperadamente Ocioso ou ausente significa que o tráfego daquele elemento não está sendo gravado.

Regras de Gravação e Retenção

A visualização **Regras de Gravação** controla quais chamadas têm sua **mídia** gravada e mostra a retenção do spool de captura e do banco de dados de índice.

Visualização de Regras de Gravação. As regras são agrupadas por tipo de correspondência: Por IP, Por número e Por domínio SIP (também existe um grupo Por cabeçalho SIP). Cada regra arma a captura de mídia RTP, pula um alvo ou salva os dados do gráfico QoS.

Regras de gravação

Por padrão, o motor de captura grava a sinalização SIP para cada chamada, mas **não** grava a mídia RTP. Uma regra de gravação arma a captura de mídia para um alvo específico. O motor de captura lê as regras ao vivo, sem necessidade de reiniciar.

As regras são agrupadas por como correspondem a uma chamada:

Grupo	Corresponde a
Por IP	Um IP de origem ou destino e máscara.
Por número	Um prefixo de número do chamador ou chamado.
Por domínio SIP	Um domínio SIP.
Por cabeçalho SIP	Um valor de cabeçalho SIP arbitrário.

Cada regra carrega um conjunto de flags:

Flag	Efeito
RTP	Arma a captura de mídia RTP para o alvo correspondente. Isso é o que permite que você ouça a chamada e obtenha o PCAP completo da mídia. Mantenha o RTP desativado globalmente e arme-o por alvo.
Pular	Descartar o alvo correspondente completamente: sem registro de chamada e sem captura. Use isso para tráfego de teste conhecido.
Gráfico	Salvar os dados do gráfico QoS detalhados para o alvo correspondente, que impulsiona o gráfico QoS.
rtcp	Registrar os relatórios de qualidade RTCP para o alvo correspondente.
habilitado	Ativar ou desativar a regra sem excluí-la.

Para armar a captura para um alvo, adicione uma regra no grupo correspondente, preencha o valor de correspondência e ative **RTP**. Para parar de gravar tráfego de teste conhecido, adicione uma regra com **Pular** ativado.

Retenção

O painel de Retenção mostra por quanto tempo os dados gravados são mantidos. A retenção é definida centralmente no servidor de captura. O painel é somente leitura no OmniWeb.

As configurações de retenção controlam duas coisas: os limites de tamanho e idade do spool em disco (dividido por SIP, RTP e dados de gráfico), e o limite de idade do índice de chamadas e linhas de qualidade por fluxo no banco de dados. A tabela abaixo lista as configurações que o painel reporta:

Configuração	Significado
`maxpoolsize_gb`	Tamanho máximo total do spool, em GB. Os dados mais antigos são removidos quando isso é alcançado.
`maxpooldays`	Idade máxima de qualquer dado do spool, em dias.
`maxpoolsipsize_gb`	Tamanho máximo do spool SIP, em GB.
`maxpoolsipdays`	Idade máxima do spool SIP, em dias.
`maxpoolrtpsize_gb`	Tamanho máximo do spool RTP (mídia), em GB.
`maxpoolrtpdays`	Idade máxima do spool RTP, em dias.
`maxpoolgraphsize_gb`	Tamanho máximo do spool do gráfico QoS, em GB.
`maxpoolgraphdays`	Idade máxima do spool do gráfico QoS, em dias.
`cleandatabase_cdr_days`	Idade máxima dos registros de chamadas no banco de dados de índice, em dias.
`cleandatabase_rtp_stat_days`	Idade máxima das linhas de qualidade por fluxo no banco de dados, em dias.

Dados de mídia (RTP) são grandes. Mantenha a retenção de RTP mais curta do que a retenção de SIP e arme a captura de RTP apenas para os alvos que você precisa.

Privacidade e interceptação legal

Gravar a **mídia** de chamadas é uma decisão de interceptação legal. A captura de sinalização registra quem ligou para quem e quando. A captura de mídia registra o **conteúdo** da chamada: o áudio da voz. Arme a captura de mídia (uma regra de gravação de **RTP**) apenas para os alvos que você está autorizado a gravar, e apenas pelo tempo que você está autorizado.

Mantenha a captura de RTP desligada por padrão e arme-a por alvo. Defina a retenção de RTP para o menor período que sua política permitir. Siga a legislação local de privacidade e as regras de consentimento tanto para captura de sinalização quanto para captura de mídia.

Como o Call Trace se compara ao Homer e ao Session Trace

OmniWeb tem três maneiras de olhar para a sinalização. Escolha a certa:

	Call Trace (SIP Trace)	Homer (SIP Capture)	Session Trace
Escopo	SIP e mídia RTP para chamadas IMS	Apenas SIP	Toda a rede: Diameter, GTP-C, PFCP, SIP, MAP
Pergunta que responde	"O que esta chamada fez e quão boa foi a voz?"	"O que o fluxo SIP desta chamada fez?"	"O que aconteceu com este assinante em todos os elementos?"
Qualidade de voz (MOS)	Sim	Não	Não
Áudio gravado	Sim	Não	Não
Download de PCAP	Sim, por chamada	Não	Não
Melhor para	Diagnosticar a qualidade, mídia e fluxo de uma chamada VoLTE	Uma rápida olhada em um fluxo SIP	Acompanhar um assinante de ponta a ponta

Escolha o Call Trace quando você precisar julgar a **qualidade da voz** de uma chamada, ouvir o áudio ou obter o PCAP de mídia. Escolha o Session Trace quando você acompanhar um assinante em toda a pilha.

Relacionados

- Logs & Subscriber Tracing: o Session Trace em toda a rede e a escada compartilhada.

- Homer: SIP Capture: a ferramenta de captura apenas de SIP.
- Network Topology: a Lista de Hosts que os agentes de captura se conectam.

Operações Comuns

Cada elemento de rede no OmniWeb é diferente por dentro, mas a forma como você *trabalha* com eles é deliberadamente a mesma. Esta página documenta os padrões compartilhados por todos os elementos: visualização de dados, edição e alteração de configurações de NF, leitura de configuração, execução de ações, visualização de logs e compreensão de polling e permissões. Aprenda isso uma vez e se aplica ao HSS, ao UPF, ao SMSC, ao MSC e a qualquer outro NF.

As capturas de tela abaixo vêm de elementos específicos, mas ilustram o padrão *genérico*: os mesmos controles aparecem, com campos diferentes, em cada elemento.

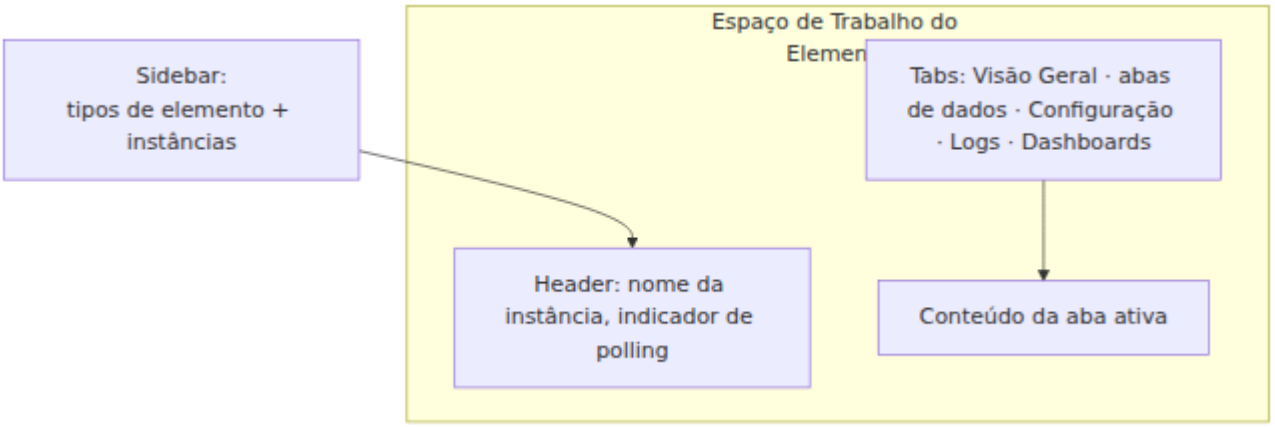
← Voltar ao Guia de Operações

Índice

- Anatomia da Página
- Visualizando Dados
- Visualizações de Detalhe
- Editando & Alterando Configurações de NF
- Executando Ações (limpar, liberar, testar, pingar)
- Visualizando Configuração
- Logs em Cada Elemento
- Dashboards em Cada Elemento
- Polling em Tempo Real
- Permissões & O Que Você Pode Alterar
- Visualizações de Múltiplas Instâncias & Frota

Anatomia da Página

Selecionar uma instância de elemento na barra lateral abre seu espaço de trabalho. Cada espaço de trabalho de elemento compartilha o mesmo layout:



- **Visão Geral**: a aba de aterrissagem: saúde, contagens principais e status do componente para essa instância.
- **Abas de Dados**: as visualizações específicas do elemento (sessões, assinantes, pares, roteamento, etc.).
- **Configuração**: uma visão estruturada da configuração de tempo de execução do elemento (onde exposta).
- **Logs**: um visualizador de logs ao vivo do Loki limitado a esse elemento.
- **Dashboards**: dashboards do Grafana incorporados para esse elemento (quando as tags do Grafana correspondem).

As entradas da barra lateral são links comuns, então você pode **Ctrl/Cmd-click** (ou clique do meio, ou clique direito → *Abrir em nova aba*) em qualquer um deles para abrir esse espaço de trabalho em uma nova aba do navegador. Isso é útil para observar dois elementos ao mesmo tempo.

Visualizando Dados

Os dados operacionais são apresentados em uma tabela consistente e classificável em todo o OmniWeb. As tabelas fornecem:

- **Classificação** por coluna.
- **Paginação** para grandes conjuntos de resultados.

- **Pesquisa / filtragem** onde a API do elemento suporta (por exemplo, pesquisa por IMSI/MSISDN ou IP do UE).
- **Carregamento esquelético** enquanto os dados estão sendo buscados, e um **estado vazio** claro quando não há nada para mostrar.
- **Clique em linha** para uma visualização de detalhe onde uma existe.

Os valores são formatados para legibilidade: timestamps como hora local, durações como `h m s`, contagens de bytes como KB/MB/GB, e números grandes com separadores de milhar.

O padrão de lista genérico (aqui, uma lista de assinantes): pesquisável, classificável, paginada, com clique em linha e edição inline. A mesma tabela impulsiona sessões, pares, rotas e qualquer outra listagem.

As tabelas podem renderizar células mais ricas: aqui, barras de utilização por linha. O padrão é o mesmo; apenas as colunas diferem.

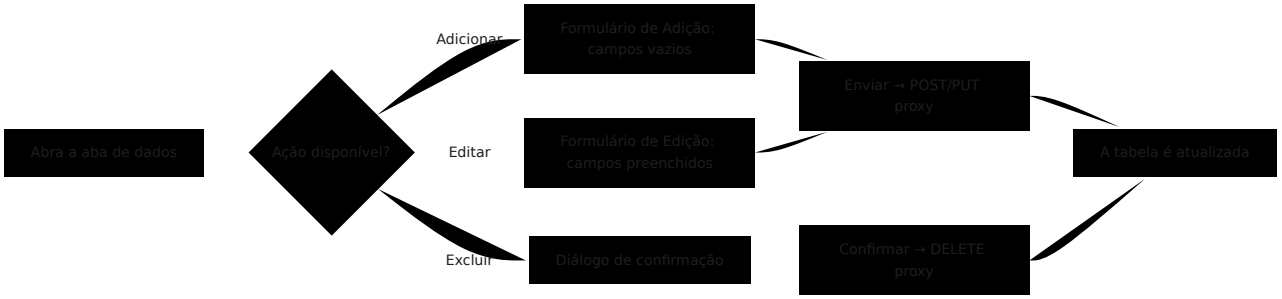
Visualizações de Detalhe

Onde uma linha tem mais a mostrar, clique nela para abrir uma visualização de detalhe. Estas reutilizam o mesmo chrome (cabeçalho, polling, ações) mas apresentam o único registro em profundidade, por exemplo, um mapa de relacionamento interativo para um objeto complexo:

Uma visualização de detalhe aberta a partir de uma linha de tabela: aqui, um mapa interativo das regras internas de uma sessão. As visualizações de detalhe são acessadas da mesma forma em todos os lugares: clique na linha.

Editando & Alterando Configurações de NF

Onde quer que a API de um elemento suporte modificação, o OmniWeb a expõe através de um **formulário de ação** consistente. O mesmo componente de formulário impulsiona "adicionar um assinante", "adicionar uma rota", "editar uma regra de QoS" e "alterar um perfil". Apenas os campos diferem.



Os formulários de ação suportam estes tipos de campo: **texto**, **número**, **selecionar** (dropdown), **booleano** (toggle), **senha** (mascarada, com um toggle de mostrar/ocultar), e **texto de múltiplas linhas**. Cada campo pode ser marcado como obrigatório, ter um placeholder e mostrar texto de ajuda. O formulário mostra um estado de carregamento enquanto está sendo enviado e relata sucesso ou falha através de uma notificação na tela.

O método HTTP por trás de cada ação mapeia para um nível de permissão. Veja Permissões.

O mesmo padrão, três elementos

Estes ilustram a *mesma* mecânica aplicada a diferentes NFs:

Tarefa	Onde	O que acontece
Adicionar/editar um assinante	HSS → Assinantes → Adicionar	Preencha o formulário (IMSI, MSISDN, perfil, chaves) → POST/PUT proxy → a lista é atualizada
Adicionar/alterar uma rota	SMSC → Roteamento → Adicionar (ou MSC → Roteamento)	Preencha a regra (padrão, destino, prioridade) → gravação proxy → a tabela é atualizada
Limpar/liberar uma sessão	UPF → Sessões (ou MSC → Chamadas)	Selecione o registro → confirme → DELETE proxy → a lista é atualizada

As mecânicas são idênticas: formulário ou diálogo de confirmação, gravação proxy, atualização da tabela. Apenas o elemento e os campos mudam.

Alterar o roteamento é o mesmo padrão de edição: a tabela de roteamento é uma lista que você adiciona e edita; alguns elementos adicionalmente analisam destinos em chips legíveis e oferecem um simulador para testar uma alteração antes de entrar em operação.

Executando Ações

Além do CRUD, muitos elementos expõem **ações operacionais** que não se encaixam em um formulário simples. Estas são apresentadas como botões que acionam uma chamada proxy e mostram o resultado inline. Exemplos do mesmo padrão de botão-ação:

Ação de exemplo	Elemento	Efeito
Forçar a liberação de uma chamada	MSC → Chamadas	Encerra uma chamada ativa
Pingar um par SIP	MSC → Pares SIP	Testa a alcançabilidade de um tronco SIP
Testar um par Diameter	TWAG → Diameter	Envia um pedido de teste de Multimedia-Auth-Request
Ativar/desativar um redirecionamento	UPF → Jardim Murado	Redireciona ou restaura um assinante
Pingar do nó	UPF → Diagnósticos	Executa um ping do próprio elemento
Desconectar uma sessão	TWAG → Sessões	Encerra uma sessão WiFi autenticada
Paginação manual	MSC → Paginação	Aciona um pedido de paginação

Ações destrutivas (liberar, excluir, desativar) sempre requerem confirmação explícita antes de serem executadas.

As ações operacionais aparecem como botões ao lado dos dados que afetam: aqui, ativando/desativando redirecionamentos de assinantes e gerenciando IPs na lista branca. Ações destrutivas solicitam confirmação primeiro.

Visualizando Configuração

Elementos que expõem sua configuração de tempo de execução têm uma aba de **Configuração**. O OmniWeb a renderiza em um layout estruturado e legível com um toggle de **JSON Bruto** para o documento subjacente completo.

Dois comportamentos valem a pena conhecer:

- **Formatos de configuração mistos são normalizados.** Alguns elementos retornam configuração como dicionários no estilo Python (`'key': True`, `None`) em vez de JSON estrito. O OmniWeb analisa isso em uma visualização limpa automaticamente e recua graciosamente se não puder analisar um valor.
- **Segredos são mascarados.** Qualquer campo cujo nome pareça sensível (correspondendo a `senha`, `segredo`, `token` ou `credencial`) é exibido como

`***` em vez de seu valor real, tanto nas visualizações de configuração quanto nos campos de formulário.

A visualização de configuração genérica: configurações em um layout estruturado, com um toggle de JSON Bruto e valores sensíveis mascarados. Elementos que expõem configuração (UPF, TAS, ePDG, frontends do SMSC, OCS, RAN Monitor) usam todos esse padrão.

Logs em Cada Elemento

Cada elemento tem uma aba de **Logs** apoiada pelo Loki. Ela consulta os logs de serviço desse elemento por host/label, suporta filtragem estruturada e transmite novas linhas à medida que chegam. Como o modelo de log é idêntico entre os elementos, ele é documentado completamente em sua própria página:

➡ **Logs & Rastreio de Assinantes**

Cada aba de Logs de elemento usa o mesmo visualizador: logs estruturados, codificados por cores, transmitidos ao vivo do Loki com filtragem de serviço e severidade.

Dashboards em Cada Elemento

Elementos marcados para Grafana mostram uma aba de **Dashboards**. O OmniWeb descobre dashboards correspondentes por tag e os renderiza inline, para que você possa ver as estatísticas de um elemento sem sair de seu espaço de trabalho. Veja:

➡ **Dashboards & Estatísticas do Grafana**

Polling em Tempo Real

Páginas operacionais se atualizam automaticamente. O **Indicador de Polling** no cabeçalho de cada página mostra:

- **Ativo (ponto verde)** ou **pausado**.

- O **intervalo** (padrão de 5 segundos, definido por elemento via `pollIntervalMs`).
- Um **spinner** enquanto uma busca está em andamento.
- O **timestamp** da última atualização bem-sucedida.

O polling pode ser alternado por página. Páginas construídas em torno de ações interativas ou de um único uso (consoles, diagnósticos, executores JSON) não fazem polling por padrão e são atualizadas manualmente. Pause o polling quando você quiser uma visualização estável enquanto lê uma tabela grande ou enquanto um rastreio está em andamento.

Permissões & O Que Você Pode Alterar

O que você pode *fazer* em um elemento depende do seu papel. O acesso é concedido **por tipo de elemento, por método HTTP**:

Permissão	Métodos permitidos	Uso típico
Somente leitura	`GET`	Visualizar dados, sem alterações
Leitura e escrita	`GET`, `POST`, `PUT`, `PATCH`	Visualizar e modificar (adicionar assinante, editar rota)
Total	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	Tudo, incluindo exclusão / limpeza

As permissões são atribuídas independentemente por elemento: você pode ter acesso total ao UPF, mas somente leitura no HSS. Se uma ação não for permitida para o seu papel, seu controle não estará disponível. Administradores têm acesso total a todos os elementos. Veja Autenticação & Controle de Acesso para gerenciar papéis, e note que **toda solicitação proxy é registrada em auditoria** independentemente do papel.

Visualizações de Múltiplas Instâncias & Frota

Muitos tipos de elementos funcionam como múltiplas instâncias: vários UPFs atrás de um PGW-C, um par de SMSCs, STPs redundantes. O OmniWeb lida com isso no nível do tipo de elemento: um tipo com mais de uma instância configurada obtém dois modos de navegação.

Seleção de Barra Lateral & Instância

Quando um tipo tem várias instâncias, a entrada da barra lateral se expande para listar cada uma pelo nome. Clique em uma instância nomeada para abrir diretamente o espaço de trabalho dessa instância. Um dropdown de instância também aparece no cabeçalho do espaço de trabalho. Ele permite que você troque entre instâncias sem voltar para a barra lateral, o que é útil quando você compara o comportamento entre nós sem perder sua posição em uma aba específica.

O seletor de instância no canto superior direito do cabeçalho do espaço de trabalho. Abrindo-o mostra cada instância configurada além de "Todas as

Instâncias" para voltar à visualização da frota, sem sair da sua aba atual.

Visualização da Frota

Clique no nome do tipo de elemento na barra lateral (em vez de uma instância específica), ou selecione **Todas as Instâncias** no dropdown, para abrir a **visualização da frota** para esse tipo. A visualização da frota mostra um cartão resumo por instância com status de saúde e métricas principais, para que você possa avaliar toda a frota de relance antes de aprofundar em um nó específico.

Visualização da frota UPF: um cartão por instância, todas consultadas em paralelo. Clique em qualquer cartão de instância ou use o dropdown para aprofundar.

Quando Usar Cada Visualização

Situação	Uso
Verificando a saúde geral da frota	Visualização da frota: todas as instâncias de relance
Investigando um nó específico	Dropdown de instância ou sub-item da barra lateral
Comparando contagens de sessão de dois UPFs	Abra cada um no dropdown de instância em turnos
Limpando uma sessão em um UPF específico	Navegue até essa instância, depois Sessões

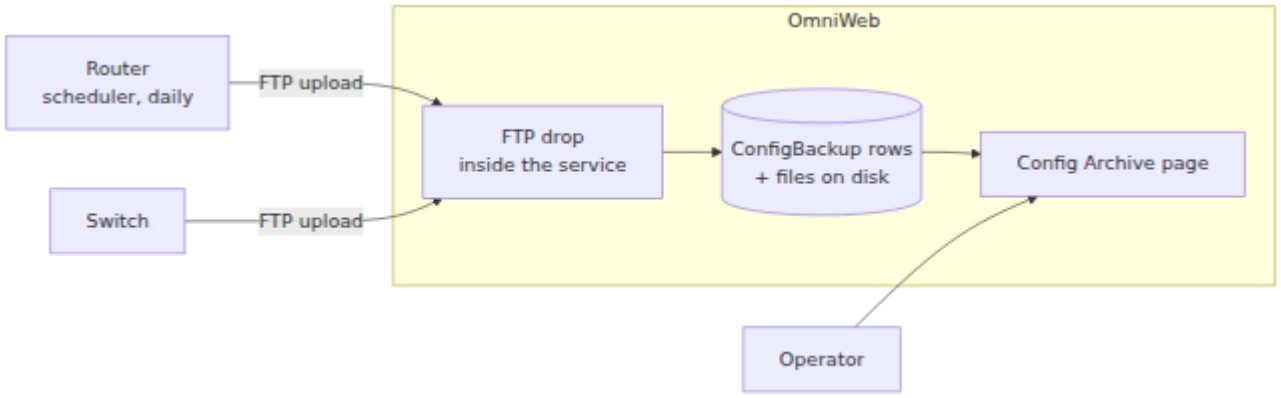
Arquivo de Configuração: Backups de Configuração de Dispositivos

Arquivo de Configuração mantém a configuração de cada dispositivo de rede que faz o upload, e torna a coleção pesquisável, ordenável e comparável. Um roteador exporta sua própria configuração em sua própria programação e a envia para o OmniWeb; a página mostra o que chegou, o que está dentro e o que mudou desde a última vez.

← Guia de Operações

O que é

Roteadores e switches não podem executar um agente de log ou um cliente de backup, mas todos podem fazer upload de um arquivo. Assim, o arquivo transforma essa única capacidade em um registro de cada configuração que o patrimônio executou.



O drop funciona **dentro do serviço OmniWeb**. Não há processo auxiliar, nenhum pacote extra e nada para instalar no host: o listener é parte da aplicação, escrito contra a biblioteca padrão do Python.

Por que FTP

RouterOS `/tool fetch` faz upload de um arquivo via FTP ou SFTP. Ele também pode enviar um HTTP POST, mas o corpo vem de uma variável do RouterOS, e uma variável tem no máximo 4 KB, muito abaixo de uma exportação de configuração. Portanto, o FTP é o único transporte que os dispositivos e o OmniWeb falam para um arquivo desse tamanho.

O FTP transporta a senha e a configuração em texto claro. Execute-o em uma rede de gerenciamento e restrinja os endereços de origem no firewall.

O que o drop aceita

O listener implementa a parte do FTP que um dispositivo precisa para entregar um arquivo e recusa o restante.

Ação	Resultado
`STOR` um arquivo	Aceito, onde quer que o dispositivo o coloque.
`RETR`, `LIST`, `NLST`, `MLSD`	Recusado. O drop é somente para gravação: nada pode ser lido de volta via FTP.
`DELE`, `RMD`, `RNFR`, `RNTO`	Recusado. Um dispositivo pode adicionar um backup e nunca pode remover ou renomear um.
`CWD` para um diretório que não existe	Aceito. A árvore é virtual, e o caminho se torna o nome do dispositivo.
`MKD`	Aceito, e não cria nada. Diretórios são implícitos pelos uploads.
Um caminho com `..` nele	Normalizado antes de qualquer coisa tocar o disco. O upload cai dentro do arquivo.
Um upload além do limite de tamanho	Recusado com `552`, e nada é escrito.

Ambos os tipos de arquivo são suportados, e o arquivo os trata de maneira diferente:

- **Texto**, como um RouterOS `/export` (`.rsc`), ou qualquer `.txt`, `.conf` ou `.cfg`. O texto é indexado, para que possa ser pesquisado e comparado.
- **Binário**, como um RouterOS `/system backup`. O arquivo é mantido byte a byte para restauração e é marcado como binário na lista.

Identidade: o endereço, não o nome

O endereço de origem é a identidade. Tudo se baseia no endereço de onde os bytes realmente vieram: a qual série um upload se junta, com o que é

comparado e de quem conta a retenção. Isso é TCP, então um remetente não pode forjar o endereço sem possuí-lo: o handshake precisa ser concluído.

O nome é apenas uma alegação. RouterOS `dst-path=<identity>/<file>` fornece o primeiro elemento do caminho, e um simples `edge-rtr09-20260910.rsc` dá `edge-rtr09`. Qualquer remetente pode alegar qualquer nome, então o arquivo o armazena, o exibe e o pesquisa, e não se baseia nele.

Isso é o que torna um drop aberto seguro para executar:

Alguém faz upload	O que acontece
Do próprio endereço de um roteador	Junta-se à série desse roteador, como seu próximo backup.
De um endereço diferente, alegando o nome de um roteador	Inicia sua própria série ao lado da real. Não pode falsificar uma mudança no roteador real, e não pode inundar o histórico do roteador real até que a retenção envelheça os backups genuínos.
De um novo endereço	Uma nova série, anunciada uma vez no Slack, para que um remetente inesperado seja visível em vez de silencioso.

O rótulo de uma fonte começa como qualquer coisa que seus uploads chamam, o que é conveniente e não confiável. Prenda um nome verdadeiro na fonte para impedir que uploads o movam.

O custo desse modelo: um dispositivo que realmente muda de endereço inicia uma nova série, então seu histórico se divide. Prenda rótulos em ambos, ou trate a série antiga como fechada.

Configuração

Não há nada para configurar. O drop funciona na porta 2121, aberta, assim que o OmniWeb inicia. Aponte um dispositivo para ele e ele faz o upload.

Isso é deliberado, não um atalho. Uma senha não é o que protege o arquivo: o FTP a envia em claro, e os roteadores a mantêm nas próprias configurações que fazem upload, então qualquer um que possa ler o arquivo ou espionar a rede de gerenciamento já a possui. O que protege o arquivo é que um remetente só escreve na série para o endereço que possui, o que o TCP faz manter de verdade. O firewall é o controle que importa; restrinja a porta aos seus dispositivos.

Defina uma senha para exigir uma além da verificação de endereço, ou `OMNIWEB_CONFIG_ARCHIVE_FTP=0` para manter a página do arquivo sem listener algum. O restante da tabela está lá para o site incomum, e cada valor abaixo é um padrão sensato que não precisa ser configurado.

Variável de ambiente	Padrão	D
`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD`	(vazio)	Defina exigir além d de enc é a ma de ope
`OMNIWEB_CONFIG_ARCHIVE_FTP_OPEN`	`1`	Aceita sem u Defina senha uma.
`OMNIWEB_CONFIG_ARCHIVE_FTP_USER`	`devbackup`	Nome com o dispos autent
`OMNIWEB_CONFIG_ARCHIVE_FTP_PORT`	`2121`	Porta d Use 21 serviç vincul privile
`OMNIWEB_CONFIG_ARCHIVE_FTP_HOST`	`0.0.0.0`	Endere escuta
`OMNIWEB_CONFIG_ARCHIVE_PASV_MIN`	`40000`	Primei dados este in os disp
`OMNIWEB_CONFIG_ARCHIVE_PASV_MAX`	`40100`	Última dados

Variável de ambiente	Padrão	D
`OMNIWEB_CONFIG_ARCHIVE_ROOT`	`backend/data/config-archive`	Onde c são ma diretór dispos
`OMNIWEB_CONFIG_ARCHIVE_MAX_BYTES`	`33554432`	Um up que iss recusa
`OMNIWEB_CONFIG_ARCHIVE_MAX_TEXT_BYTES`	`4194304`	Texto a taman indexa pesqui Texto r mantic apenas
`OMNIWEB_CONFIG_ARCHIVE_RETENTION_DAYS`	`365`	Um ba dessa remov
`OMNIWEB_CONFIG_ARCHIVE_KEEP_MINIMUM`	`10`	Backup recent dispos perma indepe da ida
`OMNIWEB_CONFIG_ARCHIVE_FTP`	`1`	Defina mante arquiv abrir o
`OMNIWEB_CONFIG_ARCHIVE_TIMEOUT`	`120`	Segun que ur

Variável de ambiente	Padrão	D
		de con ou um transfe parada descar
`OMNIWEB_CONFIG_ARCHIVE_RETRY_SECONDS`	`20`	Com q um tra perdeu tenta r Isso ta quanto drop p ser ate trabalh detinh recicla
`OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK`	(vazio)	Webho entrad Vazio s notifica
`OMNIWEB_PUBLIC_URL`	(vazio)	URL ba deste usada uma m Slack arquiv
`OMNIWEB_CONFIG_ARCHIVE_MAX_DIFF_BYTES`	`262144`	Maior armaz mudar trunca

Variável de ambiente	Padrão	D
`OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN`	(vazio)	Token Prome aprese coletar Vazio c aberta

OmniWeb executa vários trabalhadores gunicorn, e cada trabalhador inicia o drop. Exatamente um vence a vinculação e atende; os outros ficam de prontidão e tentam novamente, para que o listener sobreviva a um trabalhador sendo reciclado. A página relata `listening_here` por processo, então um `false` em uma solicitação não é uma falha.

Rastreamento de mudanças e Slack

Cada upload é comparado com o upload anterior **da mesma fonte**, do mesmo tipo, à medida que chega. Mesmo tipo significa a mesma extensão, então um dispositivo que envia uma exportação de texto e um backup binário toda noite compara cada um com seu próprio predecessor em vez de alternar entre eles e chamar tudo de uma mudança. Bytes idênticos significam nenhuma mudança, seja qual for o arquivo. Bytes diferentes em um arquivo de texto produzem um diff unificado e uma contagem de linhas, ambos armazenados na linha, então a página e a notificação nunca os recalculam. Um arquivo binário que difere é registrado como alterado sem diff, porque não há nada legível para mostrar.

O que não conta como uma mudança

Um dispositivo carimba sua exportação com o horário em que foi executado. RouterOS abre cada `/export` com

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

então duas exportações de um roteador intocado diferem por essa linha e nada mais, e ele escreve o arquivo sob um novo nome a cada execução. Comparado de forma bruta, cada dispositivo relataria uma mudança toda noite, postaria no Slack e enterraria o único sinal que vale a pena ter sob um falso positivo diário por dispositivo.

Portanto, essas linhas são removidas antes que qualquer coisa seja comparada, e somente para comparação: o arquivo armazenado e o texto pesquisável mantêm exatamente o que o dispositivo enviou.

Ignorado	Por quê
`# <data> <hora> by RouterOS <versão>`	O cabeçalho de exportação do RouterOS. Muda a cada execução. RouterOS 7 escreve uma data ISO (`2026-09-10 11:39:35`), RouterOS 6 escreve `sep/10/2026`; o padrão corresponde à forma que eles compartilham em vez de qualquer renderização.
`# software id = ...`	Presente em algumas exportações do RouterOS.
`! Última alteração de configuração em ...`	Cisco IOS. Muda quando qualquer coisa é escrita, incluindo pelo dispositivo.
`! Configuração NVRAM atualizada pela última vez em ...`	Cisco IOS.
`ntp clock-period ...`	Cisco IOS. Desvia por conta própria, sem envolvimento do operador.

O nome do arquivo não faz parte da comparação: um upload é correspondido com o upload anterior da mesma fonte com a mesma extensão, então um nome com um timestamp nele não muda nada.

Defina `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS` para uma lista de expressões regulares separadas por `|||` para substituir esta lista para um fornecedor que carimba algo diferente.

Após alterar os padrões, rehash o arquivo. Cada backup armazena um hash de sua configuração normalizada, então um novo padrão deixa todos os hashes armazenados obsoletos: o próximo upload de cada dispositivo não corresponderia mais ao seu próprio histórico, armazenando um arquivo duplicado e relatando uma mudança que nunca aconteceu.

```
sudo -u omniweb /opt/omniweb/backend/venv/bin/python
/opt/omniweb/backend/manage.py \
  rehash_config_archive --dry-run     # reportar primeiro
sudo -u omniweb /opt/omniweb/backend/venv/bin/python
/opt/omniweb/backend/manage.py \
  rehash_config_archive
```

Essa comparação impulsiona duas coisas:

- **A página.** Cada linha mostra `+N/-N` quando a configuração se moveu, ou uma marca quando o dispositivo enviou o mesmo arquivo novamente. **Mudanças apenas** reduz a lista para uploads que realmente mudaram algo.
- **Slack.** Uma mudança é postada em um webhook de entrada, com a fonte, as contagens de linhas, as primeiras 40 linhas do diff e um link de volta ao arquivo. Um endereço ouvido pela primeira vez também posta uma vez, nomeando o endereço primeiro e o que alega ser em segundo.

Um backup noturno inalterado não posta nada. Um patrimônio que faz backup toda noite, de outra forma, preencheria um canal com "nada aconteceu", e todos o silenciariam. O que chega em vez disso é apenas o que um operador gostaria de ser interrompido.

```
*core-rtr01 (10.64.10.1)* configuração alterada (+3/-1)
`core-rtr01-2026-09-10-0215.rsc` recebido em 2026-09-10 02:15
Backup anterior: 2026-09-09 02:15
```

seguido pelo diff e um link para o arquivo.

Defina `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` para um webhook de entrada do Slack para ativar isso, e `OMNIWEB_PUBLIC_URL` para que a mensagem vincule de volta a este OmniWeb. Sem webhook definido, o arquivo ainda rastreia mudanças e a página ainda as mostra; nada é postado.

O POST é fire and forget em uma thread de fundo, então um Slack lento ou inacessível nunca pode atrasar um upload ou perder um backup.

Check-in e métricas

Dois fatos, e o monitoramento precisa de ambos:

Fato	Campo	O que o silêncio significa
Ouvimos dele	`last_upload_at`, aumentado em **cada** upload, mudado ou não	Uma falha. O dispositivo, sua programação ou o caminho aqui parou de funcionar.
Sua configuração se moveu	`last_change_at`, aumentado apenas em uma mudança	Nada. Um dispositivo cuja configuração nunca muda é um dispositivo saudável.

Alerta no primeiro e nunca no segundo, ou um roteador estável te alerta toda noite.

Contadores (`upload_count`, `change_count`) vivem na fonte em vez de serem contados a partir das linhas, então a retenção podando backups antigos não pode fazê-los cair. Um arquivo que precede esses campos é preenchido a partir dos backups que já possui quando a migração é executada.

Coleta

`GET /api/config-archive/metrics` retorna a exposição de texto do Prometheus. É um endpoint simples sem dependências, e não usa a sessão: defina `OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN` e o Prometheus o apresenta

como um bearer. Não definido deixa-o aberto, e a exposição nomeia dispositivos e endereços, então defina-o em qualquer coisa acessível.

```
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>'
```

Métrica	Tipo	Descrição
`config_archive_last_upload_timestamp_seconds`	Gauge	Último upload desta fonte, mudado ou não. **Este é o que deve ser alertado.** `0` quando nunca fez upload, então o mesmo alerta pega um dispositivo que nunca começou.
`config_archive_last_change_timestamp_seconds`	Gauge	Último upload cuja configuração diferiu. `0` quando nunca mudou.
`config_archive_uploads_total`	Counter	Uploads recebidos desde que a fonte foi vista pela primeira vez. A retenção não a reduz.

Métrica	Tipo	Descrição
`config_archive_changes_total`	Counter	Uploads que mudaram a configuração.
`config_archive_retained_backups`	Gauge	Backups mantidos após a retenção.
`config_archive_retained_bytes`	Gauge	Bytes mantidos após a retenção.
`config_archive_sources`	Gauge	Fontes que o arquivo já ouviu.
`config_archive_ftp_enabled`	Gauge	Se o drop está configurado para funcionar.
`config_archive_ftp_bound`	Gauge	Se o socket do drop está aceitando conexões no host. **Alerta neste.** Qualquer trabalhador pode respondê-lo, porque é

Métrica	Tipo	Descrição
		medido com uma conexão local.
`config_archive_ftp_listening_here`	Gauge	Se o trabalhador que respondeu a essa coleta é o que detém o socket. Apenas para depuração: uma coleta através do nginx cai em um trabalhador arbitrário do pool, então isso é um jogo de azar. Nunca alerte sobre isso.

Cada série carrega `source` (o endereço, a identidade) e `label` (o nome de exibição, que é apenas o que os uploads alegam até que um operador o prenda).

Alertas que valem a pena ter

```
# Um dispositivo parou de fazer backup, ou nunca começou.
Programação diária mais slack.
(time() - config_archive_last_upload_timestamp_seconds) > 172800

# Ninguém está atendendo o drop.
config_archive_ftp_bound == 0 and config_archive_ftp_enabled == 1

# Um dispositivo que muda repentinamente a cada execução, o que
geralmente significa que sua exportação
# carrega um timestamp em vez de que alguém esteja editando.
increase(config_archive_changes_total[1d]) > 3
```

Retenção

A retenção funciona **por fonte**, que é o ponto: um remetente preenchendo sua própria série nunca pode envelhecer os backups de outro remetente. Um backup mais antigo que a janela de retenção é removido, exceto que os mais novos de cada fonte sempre permanecem. Um dispositivo que para de fazer upload, portanto, mantém sua última configuração conhecida como boa para sempre, e a idade sozinha nunca esvazia o histórico de um dispositivo.

Uploads da mesma **configuração** compartilham um arquivo no disco, comparados da mesma forma que as mudanças são: com o próprio timestamp da exportação e outras linhas voláteis removidas. Isso importa mais do que parece. Uma exportação do RouterOS carimba o horário em que foi executada em sua primeira linha, então os bytes brutos diferem todas as noites; basear o armazenamento neles escreveria uma nova cópia da configuração de um roteador intocado todas as noites para sempre.

Um roteador que faz upload de uma configuração inalterada toda noite, portanto, ainda recebe uma linha toda noite, o que torna "ouvimos dele" visível, enquanto os bytes são armazenados uma vez.

Configurando um MikroTik

Dois comandos, executados no roteador. Defina `<omniweb-host>` para o endereço do seu OmniWeb. Nenhuma senha é necessária, e as credenciais abaixo são ignoradas: o drop identifica um dispositivo pelo endereço de onde faz o upload.

```
/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="Exportação noturna de
configuração para o Arquivo de Configuração do OmniWeb"
```

Execute uma vez manualmente para provar o caminho antes de confiar na programação:

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

Uma execução bem-sucedida imprime `status: finished` com o tamanho do upload, e o dispositivo aparece no arquivo em segundos.

Por que está escrito assim

Detalhe	Razão
O script inteiro é **uma linha**	O CLI do RouterOS rejeita continuações de barra invertida quando um comando chega via SSH. Um script escrito em várias linhas cola bem em um terminal e falha na automação, com um simples `syntax error (line 1 column N)`.
`policy=read,write,ftp,test`	`fetch` precisa de `ftp` e `test`. Sem eles, a execução falha com um erro de política e nada é enviado.
`port=2121`	O padrão do drop. `/tool fetch` aceita a porta separadamente do endereço.
`user=omniweb password=x`	Marcadores. O drop aceita quaisquer credenciais, porque o endereço de origem é a identidade. `fetch` ainda quer que os argumentos estejam presentes.
`[find name=...]` em `/file remove`	`/file remove` aceita um id interno, não um nome. Passar o nome diretamente falha e a exportação é deixada no roteador, preenchendo seu armazenamento ao longo do tempo.
`:delay 5s` após `/export`	A exportação escreve de forma assíncrona. Fazer upload imediatamente pode capturar um arquivo parcial.
`$d` no nome do arquivo	RouterOS 7 renderiza a data como `2026-09-10`, então o arquivo classifica naturalmente. O nome muda a cada execução e isso é bom: o arquivo

Detalhe	Razão
	corresponde a um upload com o anterior da mesma fonte, nunca pelo nome do arquivo.

Espalhe o `start-time` entre os roteadores para que não façam upload todos ao mesmo tempo.

Para manter um backup binário também, adicione `/system backup save name=$base` e faça upload de `$base.backup` da mesma forma. A exportação de texto é a que deve ser comparada; o binário é o que deve ser restaurado em hardware idêntico.

Qualquer dispositivo que possa fazer upload via FTP funciona da mesma maneira: aponte-o para o host e porta e deixe-o nomear seu próprio arquivo.

Usando a página

Arquivo de Configuração está na barra lateral, sob Lista de Hosts.

Controle	O que faz
Banner silencioso	Nomeia cada fonte que não fez upload por 48 horas, com quanto tempo passou. Este é o check-in, então dispara para um dispositivo que envia backups inalterados apenas se parar de enviá-los.
Fonte	Filtra para um endereço de fonte. Cada entrada mostra quando foi a última vez que enviou, e marca uma silenciosa.
Nome, endereço ou arquivo	Pesquisa por substring no nome alegado, no rótulo da fonte, no endereço e no nome do arquivo.
Texto dentro da configuração	Pesquisa as próprias configurações, por exemplo, um endereço IP, `ospf` ou um nome de usuário. Esta é a maneira mais rápida de encontrar quais dispositivos possuem uma configuração.
Cabeçalhos de coluna	Ordena por dispositivo, arquivo, hora recebida ou tamanho.
Mudanças apenas	Reduz a lista para uploads que mudaram a configuração, ocultando os inalterados noturnos.
Coluna de mudança	`+N/-N` quando a configuração se moveu, uma marca quando o dispositivo reenviou o mesmo arquivo.
Uma linha	Abre a configuração, com um diff em relação ao backup anterior daquele dispositivo.
Download	O arquivo exatamente como o dispositivo o enviou.
Adicionar um arquivo	Fazer upload de uma configuração manualmente, para um dispositivo que não pode enviar.

O diff é a parte que justifica sua existência: ele responde "o que mudou neste roteador e quando" sem um login no dispositivo.

API

Todos os endpoints precisam de uma sessão autenticada.

Método e caminho	Descrição
`GET /api/config-archive/backups`	Lista, com `source`, `address`, `q`, `content`, `changed`, `ordering`, `limit` e `offset`.
`POST /api/config-archive/backups`	Adicionar um backup manualmente: multipart `file`, `device` opcional.
`GET /api/config-archive/backups/<id>`	Um backup, com seu texto.
`GET /api/config-archive/backups/<id>/download`	O arquivo armazenado.
`GET /api/config-archive/backups/<id>/diff`	Diff unificado em relação ao backup anterior, ou `?against=<id>`.
`GET /api/config-archive/sources`	Uma linha por endereço de origem: contagem de backups, mudanças, upload mais recente, tamanho e cada nome que seus uploads reivindicaram.
`PATCH /api/config-archive/sources/<id>/label`	Fixar um nome verdadeiro a uma origem, para que os uploads parem de movê-lo.
`GET /api/config-archive/status`	Estado do drop e totais do arquivo.
`GET /api/config-archive/metrics`	Exposição de texto do Prometheus. Veja Check-in e metrics.

`changed=1` retorna o feed de mudanças: uploads que diferem do backup anterior do dispositivo.

`ordering` aceita `received_at`, `claimed_name`, `filename` e `size_bytes`, com um `-` na frente para inverter. Qualquer outro valor volta para o mais recente primeiro.

Solução de Problemas

Sintoma	Verifique
A página avisa que o drop está desligado	`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD` não está definido. Defina-o e reinicie o OmniWeb.
O dispositivo relata uma falha de login	Confirme o nome de usuário e a senha, depois procure por `config archive ftp: login failed` no log do OmniWeb.
A transferência começa e para	O intervalo passivo não é acessível. Abra `OMNIWEB_CONFIG_ARCHIVE_PASV_MIN` para `..._MAX` a partir do dispositivo.
Os uploads chegam com um nome reivindicado estranho	O dispositivo enviou um nome de arquivo simples que não começa com sua identidade. Defina `dst-path` para `<identity>/<file>`, ou fixe um rótulo na origem.
Um dispositivo aparece como duas fontes	Seu endereço mudou, então começou uma nova série. Fixe rótulos em ambos para tornar a relação óbvia.
Um endereço inesperado aparece	Alguém ou algo mais pode acessar a porta. Verifique a mensagem "agora fazendo backup" no Slack para saber quando começou, e restrinja a porta.
Um dispositivo está faltando na lista	Ele nunca completou um upload. Execute o script manualmente no dispositivo e observe seu log.
Nada chega no Slack	Confirme que `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` está definido, depois verifique se os uploads são

Sintoma	Verifique
	mudanças: um backup inalterado é silencioso por design. Falhas são registradas como `Slack post failed`.
O Slack publica em cada backup	O dispositivo carimba algo em cada exportação que não está coberto pela lista de ignorados. Compare dois backups para ver o que muda, depois adicione um padrão a `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS`.

DRA: Agente de Roteamento Diameter

O **DRA** é o hub de roteamento Diameter do núcleo. Em vez de cada nó manter uma malha completa de conexões Diameter, as funções EPC e IMS se conectam ao DRA, que retransmite e roteia seus sinais: **S6a** entre o MME e o HSS, **Gx/Gy** para o PCF/PCRF e OCS, **Cx/Dx** e **Sh** para o IMS, e assim por diante. Ele escolhe para onde cada mensagem vai a partir de **regras de roteamento** (correspondendo à aplicação Diameter, domínio ou AVP) e um algoritmo de seleção de pares, e pode reescrever mensagens com **regras de transformação**. É o contraparte Diameter de um STP SS7. O OmniWeb exibe os pares do DRA, regras de roteamento, status ao vivo e um mapa de conexões. Gráficos de throughput e tendência estão nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

O DRA é uma página de elemento por instância acessada a partir da barra lateral quando se navega no inventário do site, com uma visão da frota (o mapa da rede) onde vários estão implantados. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do DRA, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Está organizada em abas.

Mapa da Rede

Uma visão de hub e spoke do DRA e de cada par Diameter que ele conhece, com a contagem de conexões à primeira vista (por exemplo, *5/6 conectados*). Os pares conectados estão ligados ao DRA em verde. Um par **desativado** ou **desconectado** é mostrado em cinza e tracejado. É a maneira mais rápida de ver, em uma imagem, quais vizinhos de sinalização estão ativos.

Status

A aba **Status** relata a própria identidade e configuração do DRA: seu **Origin-Host**, **domínio**, o **IP e porta de escuta** (Diameter geralmente é 3868), o **nome do produto** reportado e o **algoritmo de seleção de pares** em uso (por exemplo, round-robin). É aqui que você confirma que o DRA está em execução e configurado conforme esperado.

Pares

Cada par Diameter, com cada linha mostrando o **Origin-Host** do par, **IP e porta**, **produto** reportado, **transporte** (SCTP ou TCP), **domínio**, as **aplicações Diameter** negociadas e seu **estado de conexão**. Os pares podem ser filtrados por nome, aplicação, domínio ou estado. Cada par tem um botão de **habilitar/desabilitar**. Desabilitar um par administrativamente o retira do roteamento sem desmontar sua configuração, que é como você drena um vizinho para manutenção.

Regras

As **regras de roteamento** e **regras de transformação** ativas, e o **algoritmo de roteamento** sob o qual elas operam. Cada regra de roteamento corresponde a um filtro (uma aplicação Diameter, um AVP ou todo o tráfego) e resolve para um destino: seja um conjunto explícito de pares ou uma estratégia nomeada como *destination-host* ou *destination-realm*. É aqui que você confirma, por exemplo, que S6a é roteado para o HSS e Gx para o PCF.

Logs

A aba **Logs** exibe o log ao vivo do DRA para solucionar problemas de um único agente de roteamento sem sair do OmniWeb.

Painéis de Monitoramento

As taxas de mensagens, throughput por interface e outras séries temporais para o DRA são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **MME** e o **HSS**: o DRA retransmite **S6a** entre eles.
- O **PCF/PCRF** (**Gx**) e **OCS** (**Gy**): pares de política e cobrança roteados através do DRA.
- O **CSCF** e **HSS**: sinalização IMS **Cx/Dx**.
- **STP**: o contraparte de roteamento SS7 do DRA no plano de sinalização.

Servidor de Autorização: OmniSEP

O **Servidor de Autorização** (**OmniSEP**) decide quais serviços um assinante e seu dispositivo estão autorizados a usar. Quando um celular pergunta se pode ativar **VoWiFi**, **VoLTE** ou **Chamadas via Wi-Fi**, ou executa o provisionamento de dispositivo **ODSA** para adicionar ou ativar um dispositivo, ele consulta o servidor de autorização. O servidor autoriza a solicitação através da interface de **autorização (TS.43)**, resolve os dados do assinante via **Diameter** e aplica os perfis de serviço **XCAP** do assinante. O OmniWeb exibe suas autorizações ativas, atividades, sessões, tokens, pares Diameter e perfis XCAP em uma única página de elemento; gráficos de volume e tendência estão disponíveis nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

OmniSEP é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do servidor de autorização, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

A aba de entrada é uma leitura de saúde em uma única tela para o servidor de autorização: seu **status do sistema**, a contagem de **sessões** e **tokens** ativos, assinantes com **autorizações** personalizadas e a saúde de seus pares **Diameter**. É a maneira mais rápida de confirmar que o servidor está ativo e autorizando dispositivos.

Autorizações

Os assinantes que possuem **autorizações personalizadas**: substituições para o conjunto de serviços padrão, por assinante. Abra um assinante para ver quais serviços estão habilitados para ele. Um operador pode **deletar todas as autorizações** de um assinante para retorná-lo ao padrão da rede. Isso é útil para limpar uma substituição ruim durante uma falha.

Atividade

Os registros de **atividade** recentes: um feed das solicitações de autorização que o servidor tratou, cada uma mostrando o assinante ou dispositivo, o serviço solicitado e o resultado. Abra um registro para ver seus detalhes. Este é o histórico de auditoria para confirmar se um celular realmente pediu VoWiFi/VoLTE e qual resposta foi dada.

Sessões

As **sessões EAP-AKA** ativas que o servidor está mantendo para autenticação de dispositivos, cada uma com sua identidade de assinante e estado. Uma sessão individual pode ser **expirada** a partir daqui para forçar um dispositivo a reautenticar. Esta é a maneira mais rápida de limpar uma sessão que ficou presa.

Tokens

Os **tokens de autenticação** ativos que o servidor emitiu para dispositivos após eles se autenticarem. Cada token pode ser **revogado** individualmente, o que retira a autorização de um dispositivo e exige que ele se autentique novamente. Este é o equivalente de autorização a forçar um novo login.

Diameter

Os **pares Diameter** aos quais o servidor de autorização se conecta para dados de assinantes, com o **estado de conexão** de cada par. Quando as decisões de autorização começam a falhar por razões que parecem dados de assinantes ausentes, esta aba é onde você confirma que o caminho Diameter está ativo.

Perfis XCAP

Os **perfils XCAP**: as configurações de serviço por assinante (como configuração de serviço suplementar) que o servidor de autorização aplica. Abra um perfil para lê-lo. Um perfil pode ser **deletado** para limpar as configurações armazenadas de um assinante e retornar ao padrão.

Logs

A aba de **Logs** exibe a saída de log ao vivo do servidor de autorização para solucionar problemas de um único servidor sem sair do OmniWeb.

Painéis de monitoramento

As taxas de solicitação, contadores por serviço e outras séries temporais para o servidor de autorização são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **HSS** mantém os dados do assinante que as solicitações Diameter do servidor de autorização resolvem.
- O **CSCF** e o **TAS** entregam os serviços VoLTE/VoWiFi que o servidor de autorização autoriza.
- O **ePDG** e o **TWAG** transportam o acesso a Chamadas via Wi-Fi que o servidor de autorização habilita.
- O **DRA** retransmite o sinalização Diameter do servidor de autorização para seus pares.

ePDG: Gateway de Dados de Pacote Evoluído

O **ePDG** é o gateway seguro para **acesso Wi-Fi não confiável**: o nó por trás da Chamada Wi-Fi (VoWiFi) e dados de WLAN não confiáveis. Um dispositivo móvel estabelece um túnel IPsec/IKEv2 para o ePDG através de qualquer conexão com a internet; o ePDG autentica o assinante contra o AAA/HSS via Diameter (SWm/SWx), ancla a sessão ao núcleo de pacotes (S2b para o PGW) e impõe limites de taxa por assinante e política de geo-IP. O OmniWeb exibe os túneis ativos do ePDG, seus pares Diameter, configuração de limitação de taxa e geo-IP, e configurações em tempo de execução; tendências de longo prazo estão nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

O ePDG é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status** do ePDG, o número de **sessões ativas** (túneis IPsec), e um resumo do estado operacional do gateway. Esta é a confirmação mais rápida de que o ePDG está ativo e transportando túneis de chamadas Wi-Fi.

Sessões

Cada sessão ativa: os túneis IPsec/IKEv2 atualmente estabelecidos, identificados por assinante, com o estado do túnel e do portador. Você pode inspecionar uma sessão para ver seus detalhes. É aqui que você confirma se o túnel de chamada Wi-Fi de um assinante específico está ativo.

Diameter

As conexões de pares Diameter para o AAA/HSS que carregam autenticação (SWm/SWx), com o estado de conexão de cada par. Este é o primeiro lugar a olhar quando as autenticações de chamadas Wi-Fi estão falhando.

Limitador de Taxa

O ePDG termina túneis IPsec/IKEv2 de Wi-Fi não confiável (SWu) e os conecta ao EPC via S2b, o que o torna exposto a qualquer dispositivo móvel (ou qualquer fonte) na internet aberta. O **Limitador de Taxa** é a defesa contra um cliente sobrecarregando a configuração do túnel: ele limita a inundação de IKE para que um único dispositivo mal comportado ou fonte atacante não possa esgotar o gateway. A aba mostra os **limites** impostos ao lado de uma contagem ao vivo de quantos **IPs** e **IMSIs** estão **atualmente bloqueados**. Os limites são os limites de requisições **por IP** e **por IMSI**, cada um expresso como um número de tentativas de autenticação dentro de uma **janela** móvel, e a **duração do bloqueio** aplicada uma vez que um limite é ultrapassado.

Abaixo dos limites, você pode **procurar** qualquer endereço IP ou IMSI para ver se está bloqueado e quantas falhas acumulou, e **limpar** esse bloqueio para que futuras tentativas de autenticação a partir dele sejam permitidas novamente; uma única ação de **Limpar Tudo** remove todos os bloqueios e redefine todos os contadores de falhas de uma vez. É aqui que um operador confirma por que o túnel de chamada Wi-Fi de um assinante está sendo recusado e libera um bloqueio uma vez que a fonte ofensiva se estabilizou.

GeoIP

GeoIP é o controle de admissão baseado em país do ePDG: como um operador restringe o estabelecimento de túneis VoWiFi a países permitidos, comparando o IP de origem de cada túnel de entrada com um banco de dados GeoIP. A aba mostra se o filtro está **habilitado** e se o banco de dados está **pronto** (carregado e utilizável), o **modo**, e a **lista de países** à qual o modo se aplica. O modo é **lista branca** (apenas os países listados podem se conectar) ou **lista preta** (os países listados são recusados). Também mostra o **banco de dados GeoIP em uso** e se **IPs de países desconhecidos** são permitidos ou bloqueados. Estes são endereços de origem que o banco de dados não consegue resolver para um país.

Uma vez que o arquivo do banco de dados GeoIP foi atualizado no disco, a aba pode **recarregar** para que o novo mapeamento entre em vigor sem perturbar os túneis estabelecidos. Este é o controle que mantém a configuração do túnel VoWiFi confinada às regiões que um operador atende.

Configuração

A **configuração** em tempo de execução do ePDG, regras de **limitação de taxa** (limites por assinante / por fonte que protegem o gateway) e política de **geo-IP** (quais regiões de origem são permitidas a estabelecer túneis). Estes são os controles que definem quem pode se conectar e quão agressivamente.

Logs

A aba **Logs** exibe a saída de log ao vivo do ePDG para solucionar problemas de um único gateway sem sair do OmniWeb.

Painéis de monitoramento

As taxas de túnel, throughput e outras séries temporais para o ePDG são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **PGW** ancla o plano de usuário do ePDG sobre **S2b**.
- O **AAA/HSS** mantém os dados de autenticação do assinante que as requisições Diameter do ePDG resolvem.
- TWAG: o contraparte de Wi-Fi *confiável*.

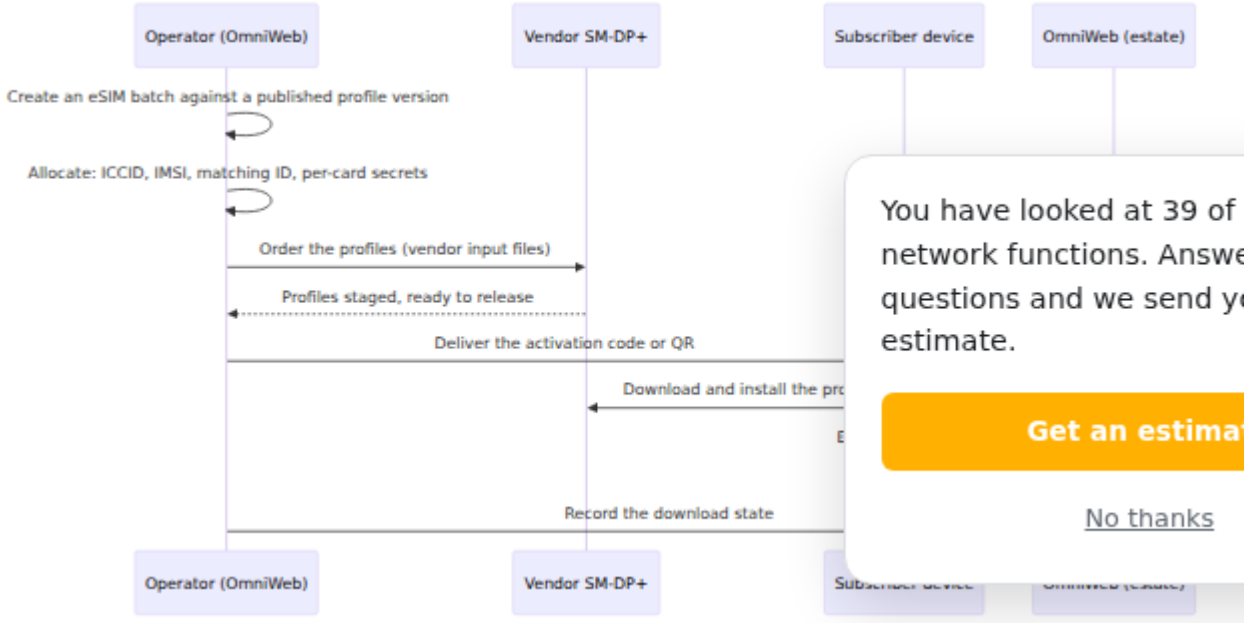
eSIM (GSMA SGP.22)

Um **eSIM** é um perfil baixado em um **eUICC**: um chip soldado em um dispositivo, ou um cartão removível que pode conter vários perfis e executar um deles de cada vez. A OmniWeb emite e gerencia perfis de eSIM através do mesmo ciclo de vida que cartões físicos, e os gerencia via over-the-air posteriormente da mesma forma.

O sabor alvo é **GSMA SGP.22 consumer**. Os perfis são encomendados de um **fornecedor SM-DP+**. A OmniWeb não hospeda um SM-DP+. Ela mantém o endereçamento, as credenciais e o estado, e é o sistema de registro para ambos.

> SGP.02 (M2M) e SGP.32 (IoT) não estão no escopo.

Como um eSIM chega a um assinante



Uma vez que o perfil está instalado e habilitado, o cartão é um cartão comum no que diz respeito à gestão. Veja Após a instalação: gerenciando um eSIM via over-the-air.

Emitindo um lote de eSIM

Um lote de eSIM é criado exatamente como um lote físico, descrito em Ciclo de Vida do SIM. O produto do cartão carrega a forma `esim`, e o lote carrega o SM-DP+ onde o fornecedor irá preparar os perfis.

A alocação registra o seguinte por cartão, além de tudo que um cartão físico recebe:

Campo	Descrição
EID	O identificador eUICC do chip para o qual o perfil é destinado, quando conhecido com antecedência.
SM-DP+ FQDN	O endereço que o dispositivo contata para baixar o perfil.
Matching ID	Um token de ativação imprevisível. Um por perfil.
Código de ativação	A string completa `LPA:1$<sm-dp+>$<matching-id>`, que é o que um código QR codifica.
Código de confirmação	Um segundo fator opcional que o assinante deve inserir para completar o download.
Estado de download	Onde este perfil chegou. Veja abaixo.

Estado de download	Significado
`released`	Preparado no SM-DP+ e disponível para download.
`downloaded`	O dispositivo puxou o perfil.
`installed`	O perfil está no chip.
`enabled`	O perfil é o ativo no chip.
`deleted`	O perfil foi removido.

Entregando o código de ativação

A exportação de **Dados de Impressão** do lote carrega o EID e o código de ativação por cartão, juntamente com o ICCID, IMSI, MSISDN e os códigos PIN e PUK. Não carrega nenhuma chave ADM e nenhuma chave OTA, porque nada que chega a uma impressora precisa delas.

Anexe a arte da folha ao lote com o tipo `qr_sheet`, e aprove-a lá, para que a trilha de aprovação permaneça com a produção.

Trate um código de ativação como uma credencial. Um matching ID é de uso único e imprevisível, e qualquer um que o possua pode baixar esse perfil.

O que o perfil deve conter

Duas coisas sobre um perfil de eSIM emitido decidem se você ainda pode gerenciá-lo após a instalação. Ambas são definidas na emissão, e nenhuma pode ser adicionada posteriormente via over-the-air.

- **O perfil deve carregar um aplicativo de gerenciamento de arquivos remoto.** Sem um não há endereço para enviar uma operação de arquivo, e o sistema de arquivos é inacessível, não importa quão boas sejam as

chaves. A OmniWeb emite um para tipos de cartão que estão configurados para isso.

- **As chaves OTA e os códigos do cartão devem ser por cartão.** Uma versão de perfil é compartilhada por todo um lote, então o PIN, PUK, ADM e as chaves OTA escritas nele podem ser apenas marcadores. A alocação substitui os próprios valores de cada cartão. Um lote que enviou um conjunto de chaves compartilhadas funcionaria perfeitamente, e permitiria que qualquer um que lesse um perfil dirigisse OTA contra cada cartão no lote.

Após a instalação: gerenciando um eSIM via over-the-air

Um perfil de eSIM instalado é um sistema de arquivos ETSI como qualquer outro. O gerenciamento de arquivos remoto via SMS (SCP80) e via HTTP (SCP81) o alcança exatamente como alcança um cartão físico, e a mesma campanhas de convergência se aplicam a ele.

As diferenças entre eSIM e plástico estão todas no início do ciclo de vida, não no final do OTA.

O ICCID do cartão permanece o endereço que todo o sistema usa, incluindo como a identidade em uma sessão de administração HTTP. Uma campanha nunca o escreve.

Onde o eSIM aparece na OmniWeb

Página	Para o que serve
Lotes	Encomendar perfis de eSIM, alocar IDs correspondentes e códigos de ativação, exportar os dados de impressão.
Estate	Cada eSIM emitido, seu estado de download e se está atrás de sua versão de perfil.
Convergência	Trazer perfis de eSIM instalados de volta em sincronia.
eSIM (LPA)	Dirigir um eUICC **em um dos seus leitores**: listar os perfis no chip, baixar um, habilitar, desabilitar, renomear ou excluir.

A página **eSIM (LPA)** é uma ferramenta do lado do cartão para um chip que você está segurando. Não é o caminho de emissão, e não altera o registro do estate. Use-a para provar um perfil, não para executar uma produção.

Notas práticas

- **Um perfil é baixado uma vez.** Uma segunda tentativa contra um código de ativação já baixado falha no SM-DP+, não no dispositivo. Emita um novo ICCID e um matching ID em vez de reutilizar um.
- **Habilitar um perfil desabilita o que está em uso.** Um eUICC executa um perfil de cada vez, e se recusa a uma troca direta. Desabilite primeiro, depois habilite.
- **Um download falhado consome o código de ativação.** A nova tentativa é recusada antes da primeira tentativa, com uma mensagem de que o perfil não foi liberado. Isso parece uma falha de plataforma e não é. Emita um novo código de ativação para o mesmo cartão e baixe-o.
- **Exclua um perfil para liberar espaço.** A exclusão precisa que o perfil esteja desabilitado primeiro. Alguns chips mais antigos recusam o pedido

mesmo assim, então planeje a iteração em torno da emissão de um novo perfil em vez de reinstalar sobre um antigo.
- **"Memória insuficiente para o perfil" pode significar slots, não bytes.** O chip relatou isso com dez perfis instalados e 170 KB ainda livres. Exclua um perfil que você não precisa mais e baixe novamente.
- **Registre o EID quando você o aprender.** É a única maneira de vincular um perfil ao chip físico em que ele acabou. Corrija-o na página Estate.

Quando uma instalação falha

Um eUICC relata uma das apenas duas falhas, e não nomeia nem o arquivo nem o campo. Leia-os como categorias, não como mensagens:

O que o dispositivo relata	O que significa
Erro de processamento de elemento de perfil	Uma parte do perfil está malformada.
Desajuste de dados	Uma verificação cruzada contra os metadados do perfil falhou.

Um **desajuste de dados** é um desacordo entre os próprios arquivos do perfil e os metadados que o SM-DP+ possui para ele. A cláusula 5.5.5 do GSMA SGP.22 define as verificações. Duas consequências são importantes na prática:

- O chip **ignora o ICCID no cabeçalho do perfil** e verifica o ICCID *arquivo* em vez disso. Um perfil cujo cabeçalho está correto e cujo arquivo está errado falha aqui, e o relatório é idêntico a um ICCID genuinamente errado.
- Quando os metadados nomeiam um proprietário de perfil, o chip também verifica se o código de rede nele corresponde ao arquivo de identidade do assinante, e se o identificador de grupo serviços na tabela de serviços concordam com os metadados.

A OmniWeb bloqueia uma exportação que carrega uma falha conhecida desse tipo em vez de deixar que ela chegue a um cartão, e nomeia o arquivo e a

regra na recusa. Se uma exportação for recusada, leia a mensagem: ela é mais específica do que qualquer coisa que o cartão lhe dirá depois.

Um perfil instala e então todos os arquivos são ilegíveis

Sintomas: Baixar e habilitar ambos têm sucesso. O cartão se conecta. Ler qualquer arquivo retorna um erro de status de segurança, que parece um problema de PIN.

Possíveis causas:

- O arquivo de regra de acesso do perfil não é estruturado como registros inteiros, então o cartão não pode analisar as regras e recusa todos os arquivos que as referenciam.
- Um arquivo aponta para um registro de regra de acesso que não concede acesso de leitura.

Resolução: Publique uma nova versão do perfil. A OmniWeb reconstrói as regras de acesso corretamente e verifica o layout antes da exportação. Uma versão já publicada é imutável, então a correção chega a um estate como uma nova versão, nunca como uma edição da que os cartões já apontam.

Um serviço é anunciado, mas seu arquivo está faltando

Sintomas: O cartão funciona. Um recurso do telefone que depende de um arquivo se comporta como se o arquivo estivesse corrompido, ou uma leitura dele falha.

Possíveis causas: A tabela de serviços anuncia um serviço cujo arquivo o perfil nunca criou. A cláusula 4.2 do 3GPP TS 31.102 torna cada um desses arquivos obrigatório exatamente quando seu serviço é lido como disponível, então uma tabela que promete demais não está em conformidade. Nada nos relatórios de instalação indica isso.

Resolução: Publique uma nova versão do perfil. A OmniWeb restringe a tabela de serviços aos arquivos que o perfil realmente contém. Se você quiser o

serviço em vez da restrição, adicione o arquivo ao perfil e publique novamente: o serviço então permanece anunciado porque seu arquivo existe.

Plataforma testada

Download de eSIM, instalação e ambos os portadores OTA são comprovados de ponta a ponta em um **Kigen eUICC**. Veja Cartões suportados e plataformas testadas.

Relacionado

- Ciclo de Vida do SIM - perfis, emissão, o estate e convergência.
- Gerenciamento de SIM OTA - como uma mudança chega a um perfil instalado.
- Ferramentas de Cartão SIM - ferramentas por cartão, incluindo a página eSIM (LPA).

5G Core

A seção **5G Core** fornece a cada função de rede 5GC (NF) seu próprio painel ao vivo. Cada painel mostra a saúde, registro e os dados operacionais que a NF possui (contextos de UE, sessões de PDU, pools de IP, registros de NRF, políticas, sessões de cobrança). Também fornece ações por NF e por item para limpar o estado. É o equivalente 5GC das páginas por elemento para funções EPC/IMS. Ele lê a API OAM de cada NF através do proxy de backend OmniWeb.

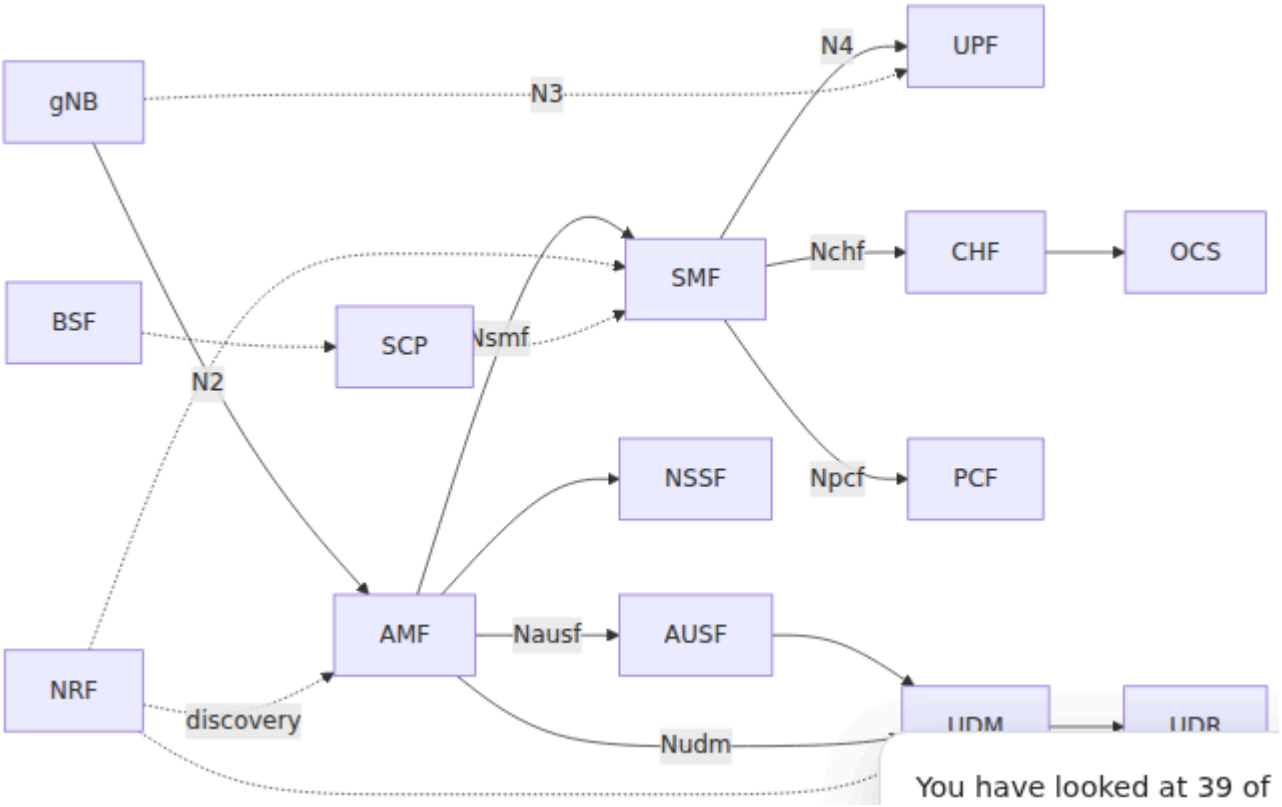
← Guia de Operações

Quando aparece

O grupo **5G Core** só aparece na barra lateral quando o site selecionado realmente executa um plano de controle 5GC. O OmniWeb determina isso pela presença de um **AMF e/ou SMF** no inventário do site. Um único UPF ou CHF compartilhado com o EPC não é um 5GC e não mostra esta seção.

O OmniWeb deriva quais NFs aparecem e o endereço da API OAM de cada NF, **diretamente do inventário Ansible do site**: os grupos de NF 5GC definidos no arquivo de host. Portanto, adicionar ou mover uma NF é, na verdade, uma mudança de inventário sem nada para modelar manualmente. Cada NF se resolve em um rótulo, descrição, IP e porta. O OmniWeb serve o registro resolvido via `/api/5gc/nf-registry`. Os painéis então consultam a API OAM de cada NF através do proxy (`/api/5gc/nf/<id>/…`), de modo que todo o tráfego permaneça atrás do único gateway autenticado. Veja o modelo de configuração. Implantações que não executam inventário (por exemplo, o serviço hospedado) voltam a um bloco estático `fivegc` na configuração do OmniWeb.

As NFs



Cada NF tem seu próprio painel:

NF	Função	Dados principais exibidos
NRF	Função de Repositório de Rede	Instâncias de NF registradas (agrupadas por tipo), serviços registrados, assinaturas: veja abaixo
AMF	Gerenciamento de Acesso e Mobilidade	Lista de UE, gNodeBs conectados (com gNB-ID / TAC / PLMN / SST decodificados), estatísticas, modo de manutenção
SMF	Gerenciamento de Sessões	Sessões de PDU, **Pools de IP**, associação de UPF, estatísticas
UDM	Gerenciamento de Dados Unificado	Lista de UE, estatísticas
UDR	Repositório de Dados Unificado	Saúde do HSS, assinantes
AUSF	Servidor de Autenticação	Sessões AUSF (auth), estatísticas
PCF	Controle de Políticas	Políticas de AM, políticas de SM, estatísticas
CHF	Função de Cobrança	Sessões de cobrança, saúde do CGrateS, registros de CDR
NSSF	Seleção de Fatiamento de Rede	Fatiamentos, disponibilidade de NSSAI, estatísticas
BSF	Suporte a Vinculação	Vínculos de PCF, estatísticas
SCP	Proxy de Comunicação de Serviço	Saúde da NF, cache de descoberta, estatísticas

Nem toda implantação executa todas as NFs. Apenas as NFs definidas no inventário do site aparecem. Cada NF tem sua própria página de referência. Siga os links acima.

A aba Pools de IP do SMF

Como exemplo dos dados de propriedade da NF que esses painéis exibem: o painel do SMF tem uma aba **Pools de IP** mostrando os pools de endereços dos quais o SMF aloca IPs de UE, juntamente com suas **Sessões de PDU** ao vivo e sua **Associação de UPF** (o estado do link N4/PFCP para o plano de usuário). Juntas, essas informações respondem "o SMF está conectado ao seu UPF, quais sessões estão ativas e está ficando sem endereços?" sem sair do OmniWeb.

Um painel em um relance

Cada painel de NF segue o mesmo layout:

1. **Cartões de saúde** na parte superior: Saúde da API, Registro de NRF (esta NF está registrada no NRF?), Status da NF e Licença. Cada um faz polling em um intervalo. Use o **Indicador de Polling** no cabeçalho para pausar ou ver o horário da última atualização (polling é um padrão compartilhado: veja Operações Comuns).
2. **Ações**: operações em nível de NF (veja abaixo).
3. **Seções de dados**: o detalhe do status da API, detalhe do registro de NRF e as tabelas específicas da NF da tabela acima, cada uma atualizando automaticamente. As tabelas auto-decodificam o que podem: PLMN/TAC/SST de termos S1AP codificados em Erlang, timestamps para tempo relativo, status para chips coloridos e links cruzados (um valor de tipo NF se vincula ao painel daquela NF).

Ações

Os painéis expõem ações para limpar o estado da NF. Cada uma pede confirmaç��o primeiro, pois são destrutivas:

NF	Ações em nível de NF	Ações por linha
AMF	Limpar todos os contextos de UE · Limpar cache	Desregistrar um UE
SMF	Liberar todas as sessões de PDU · Limpar cache · Reassociar PFCP (restabelecer a associação de UPF)	Liberar uma sessão de PDU
NRF	Desregistrar todas as NFs	Desregistrar uma NF · Remover uma assinatura
AUSF	Limpar todas as sessões de autenticação	Limpar uma sessão
UDM	Limpar cache de assinantes	-
PCF	-	Remover uma política de AM ou SM

Essas ações permitem que um operador se recupere de um estado travado. Por exemplo, forçar um SMF que perdeu seu UPF a reassociar, descartar um contexto de UE que não será limpo ou desregistrar uma NF obsoleta do NRF.

O painel do NRF

O NRF obtém uma visão mais rica porque é o registro que todo o 5GC descobre através de:

- **Cartões de métrica**: tipos de NF, total de instâncias, registradas (com uma barra de porcentagem do total) e serviços/assinaturas.
- **Instâncias de NF registradas**: agrupadas por tipo de NF. O painel codifica por cores cada cartão de instância. O cartão mostra o status de registro, temporizador de heartbeat, contagem de serviços e PLMN. Clique em uma instância para seu perfil completo (com um link **Abrir Painel** para aquela NF e um botão **Desregistrar**).

- **Serviços registrados**: uma tabela plana de cada serviço que cada instância anuncia, suas versões e status.
- **Desregistrar Todas as NFs**: limpa cada registro (cada NF deve então se registrar novamente).

Isso torna o NRF o lugar para responder "quais NFs estão ativas, todas estão registradas e quais serviços estão oferecendo?"

Relacionados

- Topologia de Rede: as visualizações de topologia que se conectam a esses painéis.
- Operações Comuns: os padrões de polling, configuração e RBAC compartilhados com cada página de elemento.
- PGW-C / SMF e UPF: as páginas de sessão/plano de usuário do lado EPC para um EPC+5GC convergente.

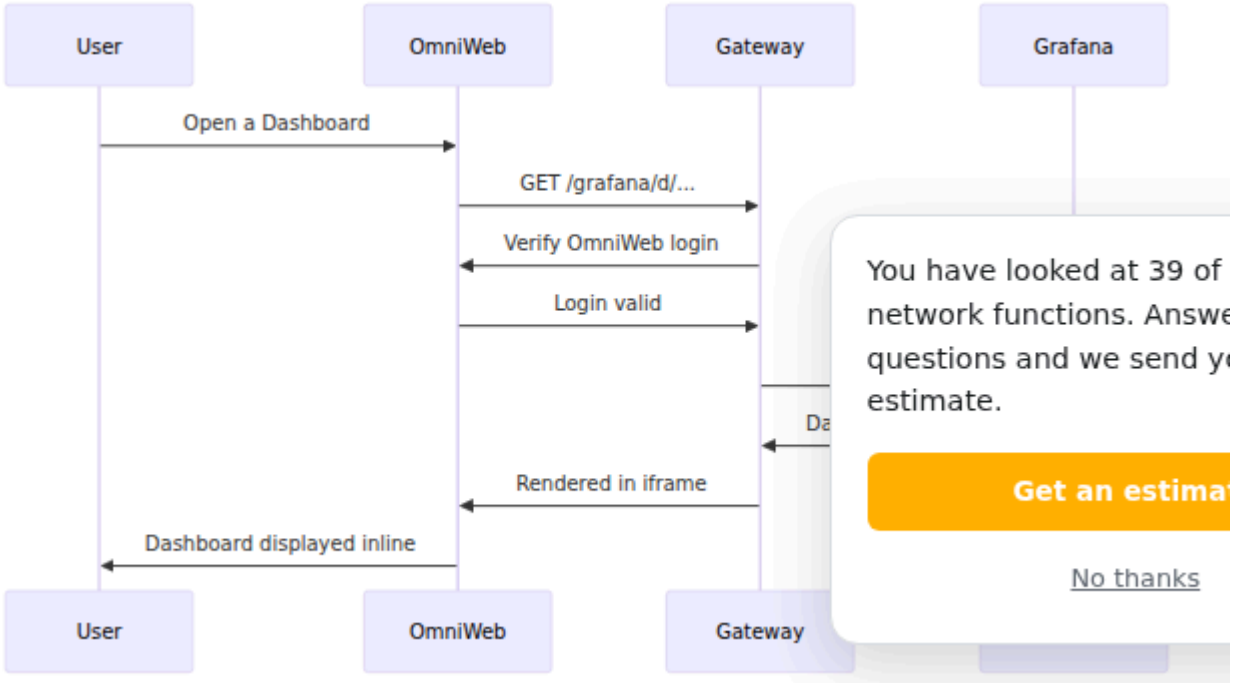
Painéis e Estatísticas do Grafana

OmniWeb incorpora o Grafana diretamente no portal. Os operadores podem ver painéis e estatísticas para qualquer elemento e para a rede como um todo, sem a necessidade de um login ou aba do navegador separada.

← Voltar ao Guia de Operações

Como Funciona

O Grafana é servido atrás do gateway autenticado no caminho `/grafana/` e incorporado como um iframe dentro do OmniWeb. A autenticação é transparente: quando você está logado no OmniWeb, o acesso ao Grafana é autorizado automaticamente com base no seu login do OmniWeb. Não há uma segunda senha.



A instância do Grafana à qual o OmniWeb faz proxy é configurada pela variável de ambiente `GRAFANA_URL` (padrão `http://localhost:3000`). O gateway lida com o proxy e a verificação de login único de forma transparente.

Duas Maneiras de Acessar Painéis

1. Aba de Painéis por Elemento

Elementos que são marcados para o Grafana exibem uma aba **Painéis** em seu espaço de trabalho. O OmniWeb consulta o Grafana para painéis que correspondem às tags desse elemento e renderiza o relevante inline. Isso mantém as estatísticas de um elemento ao lado de seus dados operacionais.

A correspondência de tags é insensível a maiúsculas e minúsculas. Conjuntos de tags representativas:

Elemento	Tags do Grafana correspondidas
UPF	`upf`
P-CSCF	`pcscf`, `cscf`
I-CSCF	`icscf`, `cscf`
S-CSCF	`scscf`, `cscf`
PGW-C, MME, SMSC, DRA, OCS, TAS	tags específicas do elemento

Para fazer um painel aparecer sob um elemento, marque-o no Grafana com a tag desse elemento (por exemplo, marque um painel UPF como `upf`).

2. Barra Lateral do Grafana

A entrada **Grafana → Painéis** na barra lateral lista todos os painéis disponíveis. Selecionar um abre-o inline dentro do OmniWeb, e a URL é atualizada para refletir o caminho do painel, permitindo que você faça links diretos para um painel específico.

Prometheus e Loki

O Grafana é a visão do dia a dia de métricas e logs, mas os serviços Prometheus e Loki por trás dele também são acessíveis através do OmniWeb, atrás do mesmo login. Nenhum deles é exposto em sua própria porta.

- **Interface nativa do Prometheus** - **Monitoramento → UI do Prometheus** na barra lateral abre a própria interface do Prometheus (navegador de expressões, alvos, regras, alertas, status do TSDB) em `/prometheus/` em uma nova aba. A página **Monitoramento → Prometheus** do OmniWeb permanece a visão resumida dos mesmos dados.
- **API do Loki** - O Loki não tem uma interface web própria; sua interface é a visão Explore do Grafana. Sua API HTTP é servida em `/loki/api/v1/...` para ferramentas como logcli e scripts. Autentique-se com sua sessão do OmniWeb ou passe um token do OmniWeb como um token bearer; chamadas não autenticadas recebem 401.

Ambos requerem um login no OmniWeb e são concedidos por usuário como qualquer elemento: em **Configurações → Permissões**, os tipos de elemento **Prometheus** e **Loki** controlam quem pode abrir a UI do Prometheus e a página, usar a API do Loki e visualizar as abas de **Logs** por elemento. Contas que existiam antes deste lançamento mantêm o acesso que tinham. Quando a sessão expira, o navegador é enviado para a página de login e retornado à página que solicitou.

A entrada **Monitoramento → Loki** na barra lateral abre a visão Explore do Grafana na fonte de dados Loki do site selecionado, que é a interface de consulta do Loki.

Estatísticas

Os painéis incorporados são onde as **estatísticas** de rede ampla e por elemento residem: contagens e taxas de sessões, throughput, latência, taxas de perda, saúde de pares Diameter/PFCP ao longo do tempo, volumes de CDR, contagens de registro e tendências de capacidade. As próprias páginas de elementos do OmniWeb fornecem o estado *atual* (e permitem que você atue

sobre ele); o Grafana fornece a imagem *histórica* e as tendências. Eles foram projetados para serem usados em conjunto. Investigue um alerta do Grafana pulando para as páginas operacionais do elemento, logs e rastros.

Alerta

O mecanismo de alerta embutido do Grafana lida com todos os alertas baseados em limites. As regras de alerta são definidas no Grafana e podem notificar por e-mail, Slack, PagerDuty ou webhook. O OmniWeb não duplica alertas. Ele fornece o contexto operacional (páginas de elementos, logs, rastros) necessário para investigar quando um alerta é disparado.

Categorias comuns de alerta:

Categoria	Exemplos
Disponibilidade	Elemento inacessível, par Diameter fora do ar, associação PFCP perdida
Capacidade	Exaustão do pool de IP, utilização do mapa eBPF > 80%, limite de contagem de assinantes do VLR
Desempenho	Latência de configuração de sessão, taxa de perda de XDP, falhas de heartbeat
Tráfego	Volume anormal de CDR, taxa de perda de chamadas, falhas na entrega de SMS

Investigando um Alerta: Fluxo Recomendado



1. Confirme a tendência no Grafana (Painéis).

2. Verifique o estado atual na Visão Geral do elemento.
3. Leia os Logs do elemento em torno do horário do alerta.
4. Se específico para assinantes, execute um Rastro de Sessão. Veja Logs & Rastreio de Assinantes.

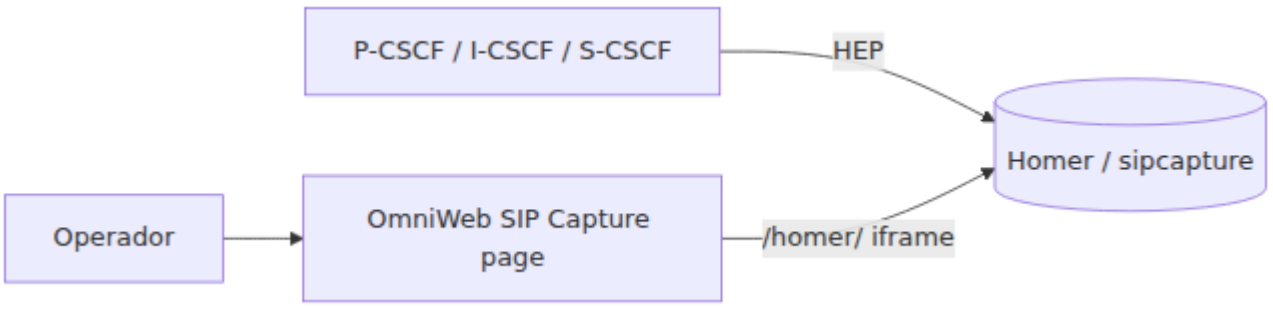
Homer: Captura de SIP e Análise de Fluxo de Chamadas

Homer é um sistema de captura e busca de SIP (HEP / sipcapture). O OmniWeb incorpora a interface web do Homer diretamente, para que você possa pesquisar o tráfego SIP capturado e reconstruir a escada de sinalização de uma chamada sem sair do portal ou fazer login separadamente.

← Guia de Operações

O que é

Homer coleta mensagens SIP do IMS (via o protocolo HEP) e as armazena de forma pesquisável por call-id, número de origem/destino, horário e mais. Sua interface web permite que você encontre uma chamada e desenhe seu **diagrama de fluxo** completo: cada mensagem SIP entre os pontos finais e os CSCFs, com tempos e qualquer causa de falha/desconexão. O OmniWeb não reimplementa nada disso. Ele **incorpora o aplicativo Homer** em um iframe sob **Captura de SIP** (aninhado sob Rastreamento de Sessão na barra lateral).



Autenticação única

Você não faz login no Homer separadamente. O OmniWeb proxy o aplicativo Homer em `/homer/` e injeta os cabeçalhos de auth-proxy no caminho, de modo

que a interface incorporada já esteja **autenticada**, sem prompt de login do Homer. Ela é acessada através do mesmo gateway autenticado do OmniWeb que Grafana e Loki, portanto, um login no OmniWeb também o governa.

A entrada **Captura de SIP** só aparece na barra lateral quando o Homer está **configurado e acessível** para a implantação. O OmniWeb o verifica e oculta a entrada se não estiver presente, para que você nunca clique em uma página inativa.

Homer vs Rastreamento de Sessão

O OmniWeb tem duas maneiras complementares de olhar para a sinalização, e é útil saber qual delas usar:

	Homer (Captura de SIP)	**Rastreamento de Sessão**
Escopo	Apenas SIP, em profundidade	Toda a rede: Diameter, GTP-C, PFCP, SIP, MAP
Pergunta que responde	"O que fez o fluxo SIP desta *chamada*, mensagem por mensagem, com tempo e causa de desconexão?"	"O que aconteceu com este *assinante* em cada elemento?"
Melhor para	Diagnosticar uma chamada VoIP/VoLTE, um registro falhado, uma desconexão específica	Acompanhar um IMSI/MSISDN de ponta a ponta pelo núcleo

Use o Homer quando tiver uma chamada para dissecar; use o Rastreamento de Sessão quando estiver acompanhando um assinante por toda a pilha. O Homer também está vinculado ao guia Logs & Rastreamento de Assinantes.

Relacionado

- Logs & Rastreamento de Assinantes: Rastreamento de Sessão entre redes e onde o Homer se encaixa.
- Painéis e Estatísticas do Grafana: a outra ferramenta de monitoramento incorporada, acessada da mesma maneira autenticada.

HSS: Servidor de Assinantes Residenciais

O **HSS** (Servidor de Assinantes Residenciais) é o banco de dados mestre de assinantes para o núcleo móvel. Ele armazena as identidades de cada assinante (IMSI, MSISDN e SIM/ICCID), o material da chave de autenticação que prova quem eles são, e os perfis de serviço EPC, IMS, PCRF e roaming que indicam o que cada assinante pode fazer na rede. O MME lê isso através do S6a para autenticar e localizar um dispositivo e para aprender sobre sua assinatura EPC. O CSCF lê isso através do Cx para registro IMS e gatilhos de serviço iFC. O PCRF extrai suas regras de política e cobrança a partir disso. Um operador usa seu painel para provisionar e pesquisar assinantes, curar os perfis de serviço compartilhados e verificar a saúde do HSS.

← Guia de Operações

O painel é uma página de elemento por instância. Ele é aberto a partir da barra lateral quando um HSS está em inventário do site. Todo o tráfego passa pelo proxy de backend OmniWeb para a API do HSS, assim permanece atrás do único gateway autenticado. As respostas retornam em um envelope `{status, response}`. Um link de documentação no cabeçalho da página fornece ajuda em contexto. A página possui abas.

Assinantes

A aba de entrada é o diretório de assinantes. Pesquise **por IMSI, MSISDN ou ICCID** para encontrar um registro. A pesquisa também resolve um assinante **por endereço IP** quando você rastreia uma sessão ativa de volta ao seu proprietário. Abra um registro para mostrar a visão geral do assinante: um diagrama de relacionamento que liga o assinante à sua **identidade** (IMSI), seu **status** (ativado, e se IMS está ativado), e os perfis **EPC**, **IMS** e **roaming** atribuídos a ele. A página mostra os APNs do perfil abaixo do perfil EPC. O HSS mantém valores de chave sensíveis, mas não os exibe. Você pode atualizá-los, mas eles são retornados como redigidos.

Provisionamento

Crie ou edite um assinante a partir do formulário de provisionamento. O formulário reúne a identidade, credenciais, SIM e perfis em um só lugar:

- **Identidade do assinante**: IMSI, um nome de assinante, e os interruptores **ativado** e **ativado IMS**.
- **Conjunto de chaves de autenticação**: o algoritmo de autenticação, **Ki** e **OPc** (ou **OP**), **AMF**, **SQN**, e a senha SIP usada para IMS.
- **Cartão SIM**: o **ICCID**, se é um eSIM, os valores PIN/PUK e os detalhes do lote e do fornecedor.
- **Números de telefone**: atribua um ou mais **MSISDNs**. Pesquise números existentes enquanto digita para que você não crie um número duas vezes.
- **Atribuir perfis**: anexe os perfis **EPC**, **IMS** e **roaming** que dão ao assinante seu serviço.

Você pode atualizar assinantes existentes da mesma forma. Você pode excluir um assinante de seu registro.

SIMs

O inventário de SIM mantém cada **SIM** que o HSS conhece. Pesquise **por ICCID**. Cada SIM carrega seu **ICCID**, sinal de eSIM, nome do lote e fornecedor, seus valores de chave de transporte (**KIC**, **KID**) e eSIM **LPA**, e o conjunto completo de **chaves ADM**. Você pode criar, editar e excluir SIMs. Os conjuntos de chaves de autenticação que os registros de SIM emparelham são gerenciados em sua própria aba.

MSISDNs

O diretório MSISDN mantém o pool de números de telefone provisionados. Pesquise **por dígitos** para uma correspondência parcial para encontrar ou verificar um número antes de atribuí-lo. Você pode criar, editar e excluir números. Você anexa números a assinantes durante o provisionamento.

Conjuntos de Chaves

O diretório de conjuntos de chaves é o armazenamento de credenciais de autenticação ao qual cada registro de assinante aponta. Cada entrada contém o **algoritmo** (Milenage ou Digest-MD5), o material da chave, o **AMF** e o contador de sequência **SQN**, e o contador OTA de SIM opcional. Filtre a página **por ID, algoritmo ou AMF**. Você pode criar, editar e excluir conjuntos de chaves.

O material da chave é somente para gravação. **Ki**, **OPc**, **OP** e a senha SIP nunca são mostrados — eles são retornados como redigidos, e uma edição que deixa um em branco mantém o valor armazenado em vez de limpá-lo. Excluir um conjunto de chaves que um assinante ainda referencia impede que esse assinante se autentique, então verifique antes de remover um.

Perfis de Serviço

Os perfis de serviço são os blocos de construção reutilizáveis que indicam o que um assinante pode fazer. Um assinante os referencia em vez de carregar

sua própria cópia. Portanto, uma alteração em um perfil se aplica a todos que o utilizam.

Perfis EPC

A assinatura do núcleo de pacotes que o MME impõe. Um **perfil EPC** define o **modo de acesso à rede**, a largura de banda agregada **downlink/uplink** UE-AMBR, o **intervalo TAU**, e a lista de **perfils APN** que o assinante pode usar. Um APN é o **APN padrão**. Cada **perfil APN** vincula um **identificador APN** a um **perfil QoS APN** e um **perfil PCRF**. Você pode marcar um perfil APN como padrão. Um perfil EPC deve referenciar pelo menos um perfil APN. O APN padrão deve ser um dos APNs atribuídos.

Expanda um perfil EPC para listar seus perfis APN. **Adicionar APN** anexa um APN ao perfil. A ação de desvincular em cada linha **remove-o apenas deste perfil EPC**. O HSS mantém o perfil APN em si. Você pode re-adicioná-lo mais tarde, ou outros perfis EPC podem reutilizá-lo. Um perfil deve manter pelo menos um APN, então você não pode remover o último. O HSS limpa o APN padrão automaticamente se você remover o APN ao qual ele apontava.

Perfis APN

A aba Perfis APN lista cada perfil APN independentemente dos perfis EPC que o utilizam. Ela mostra seu **identificador APN**, **perfil QoS APN** e **perfil PCRF**. A coluna **Usado Por** nomeia cada perfil EPC que referencia o APN. Ela marca o APN como **Orfão** quando nenhum perfil EPC o referencia. Um APN atinge esse estado uma vez que você o remove do último perfil EPC que o utilizou. O filtro **Apenas Orfão** filtra a lista apenas para esses, para que você possa encontrar e limpar APNs não utilizados.

Você pode criar perfis aqui, editá-los e excluí-los. Um novo perfil começa sem vínculo. Para vinculá-lo ao serviço de um assinante, adicione-o a um perfil EPC. Você não pode excluir um perfil APN que ainda está vinculado a um ou mais perfis EPC. Primeiro, remova-o desses perfis, depois exclua-o desta aba.

Perfis QoS APN

A aba Perfis QoS APN gerencia os modelos de QoS em nível de APN reutilizáveis que os perfis EPC e APN apontam. Cada assinante cujo APN referencia um modelo recebe a mesma qualidade de serviço em seu portador padrão. Cada

modelo contém um **nome** e um **QCI** (o Identificador de Classe QoS que mapeia o portador a um comportamento padronizado de atraso e perda). Ele também contém um **ARP** (a prioridade de alocação/manutenção), com bandeiras de **capacidade de pré-empcão** e **vulnerabilidade à pré-empcão**. Essas bandeiras decidem se o portador pode ser elevado, ou ser elevado por outros quando os recursos são escassos. Cada modelo também contém as taxas agregadas de uplink e downlink **APN-AMBR**, e se a cobrança **online** e **offline** estão habilitadas.

Você pode criar, editar e excluir modelos. Você também pode clonar um modelo para derivar uma nova variante. Um perfil APN referencia um modelo QoS em vez de carregar sua própria cópia. Se você editar um modelo, você reconfigura a QoS de cada APN que o utiliza. Você não pode excluir um modelo que um perfil APN ainda referencia. Primeiro, reatribua esses APNs.

Perfis QoS APN

As configurações de qualidade de serviço por APN que um perfil APN aponta: o **QCI**, **ARP** e **capacidade/vulnerabilidade de pré-empcão**, a largura de banda **downlink/uplink** APN-AMBR, e se a cobrança **online (Gy)** e **offline (Rf)** se aplicam. Você pode clonar um perfil para derivar uma nova variante de um existente.

Perfis IMS

A assinatura IMS que o CSCF lê através do Cx. Um **perfil IMS** contém um **modelo iFC**: os Critérios de Filtro Iniciais que decidem quais servidores de aplicação recebem o tráfego SIP de um assinante. Você pode criar, editar e excluir perfis.

IPs Estáticos

Alocações de IP fixos para assinantes que devem sempre receber o mesmo endereço, gerenciados juntamente com os dados de assinatura EPC.

PCRF

A camada de política que o PCRF aplica. Uma visão de relacionamento liga as três partes:

- **Perfis PCRF**: a política nomeada que o APN de um assinante referencia, composta por um conjunto de regras de cobrança.
- **Regras de cobrança**: cada uma com um **tipo de regra** e **precedência**, um **QCI** e **ARP**, limites **downlink/uplink** MBR/GBR, e um **grupo de classificação** e **identificador de serviço** para cobrança. Um portador dedicado transporta uma regra com um MBR ou GBR.
- **Regras de informação de fluxo**: os modelos de fluxo de tráfego anexados a uma regra de cobrança que definem quais pacotes ela corresponde.

Você pode criar, editar e excluir todos os três. Se você editar uma regra de cobrança, você afeta cada perfil que a utiliza.

Roaming

A política de roaming que o HSS aplica a assinantes inbound e outbound. Um **perfil de roaming** define uma **ação de dados padrão**, uma **ação IMS padrão**, e uma lista de **regras de roaming**. Cada regra se baseia em um **MCC/MNC** e define a **ação de dados** e **ação IMS** para aquela rede. Você pode, portanto, permitir ou bloquear redes visitadas específicas enquanto a ação padrão do perfil cobre o restante. Para adicionar uma regra, use a pesquisa de operador para encontrar o MCC/MNC de uma rede a partir de um nome de operador (do IR.21). As regras são compartilhadas. Se você editar uma regra, você afeta cada perfil que a utiliza.

EIR

O Registro de Identidade de Equipamento. Cada **regra EIR** corresponde a um **IMEI** por expressão regular e define uma **ação**: permitir ou bloquear. Você pode, portanto, barrar um modelo de dispositivo ou um handset específico da rede. Uma pesquisa de modelo de dispositivo ajuda a construir o padrão IMEI. Você pode criar, editar e excluir regras.

Status

Uma leitura de saúde em tela única do próprio HSS: a saúde da **API**, **banco de dados** e **licença**, e as **contagens de entidades** para total de **assinantes**, **perfís EPC**, **perfís IMS**, **SIMs**, **MSISDNs** e **perfís de roaming**. É a confirmação mais rápida de que o HSS está ativo e quanto ele carrega. As integrações do Grafana fornecem os painéis de monitoramento e estatísticas.

A aba **Replicação** mostra o status da replicação do banco de dados para quaisquer instâncias HSS pares. A aba **Logs** exibe a saída de log ao vivo do HSS. Use-a para solucionar problemas de uma única instância sem sair do OmniWeb.

Replicação

A aba Replicação lê a saúde da replicação PostgreSQL do banco de dados de assinantes do nó HSS e a representa como uma topologia ao vivo. Cada nó mostra se seu banco de dados é **primário** ou **standby**. Um standby é um nó que está em recuperação. Ele reproduz as alterações do primário em vez de aceitar gravações próprias. Para um primário, a aba desenha cada standby conectado como um link a jusante. O link mostra o **endereço do cliente** do standby, o **slot de replicação** pelo qual ele transmite, seu **estado de streaming**, e o **atraso de replicação** medido em relação à posição WAL atual do primário. A aba mostra o atraso em bytes, então um replica que fica para trás se destaca à primeira vista. Se cada slot de replicação está atualmente **ativo** determina se seu link é lido como saudável ou quebrado.

Um operador usa esta aba para confirmar que o banco de dados de assinantes se replica através do cluster HSS: que uma alteração provisionada em um nó alcançará os outros, e que um standby existe para falhar. Um replica com atraso mostra um número de atraso crescente. Um replica quebrado ou desconectado perde seu link. Se duas ou mais instâncias HSS estiverem em execução, mas nenhuma delas replicar, a aba sinaliza todo o cluster como uma

lacuna de replicação. Corrija isso antes que se torne um risco de perda de dados.

Operações

Duas operações em nível de assinante atuam em uma sessão ativa em vez de no registro armazenado:

- **Cancelar Localização (CLR)**: envia um Pedido de Cancelamento de Localização S6a para o MME que atende o assinante. Isso desanexa o assinante, para que ele se reanexe e pegue os dados de assinatura alterados.
- **Re-autenticação PCRF**: solicita que o PCRF re-autentique um assinante para uma sessão PDN dada. Isso empurra regras de política ou cobrança atualizadas para uma sessão ativa.

Relacionados

- **MME**: lê dados de autenticação de assinantes e dados de assinatura EPC através do **S6a**. É o alvo de um Cancelamento de Localização.
- **CSCF**: lê o perfil IMS e iFC através do **Cx** para registro IMS e acionamento de serviço.
- **PCRF / PCF**: aplica os perfis PCRF, regras de cobrança e regras de fluxo mantidas aqui. É o alvo de uma Re-autenticação.
- **UDR**: o armazenamento de dados de assinantes compartilhados que o HSS front-end em um núcleo 5G.
- Guia de Operações: voltar ao índice de elementos.

I-CSCF: Interrogando a Função de Controle de Sessão de Chamadas

O **I-CSCF** (Interrogating Call Session Control Function), o **OmniCSCF** da Omnitouch em seu papel de interrogação, é o **gateway da rede doméstica para o IMS**. É o endereço publicado no DNS para o domínio IMS do operador, de modo que qualquer registro ou chamada que chegue para um assinante doméstico passe primeiro pelo I-CSCF, seja encaminhado pelo próprio P-CSCF do assinante ou vindo de outra rede de operador. Sua função é a **seleção do S-CSCF**: em um REGISTER, ele consulta o **HSS** através da interface **Cx** para descobrir a qual S-CSCF servidora um assinante está (ou deve ser) atribuído, e em uma chamada terminante, pergunta ao HSS qual S-CSCF está atualmente servindo o chamado, e então encaminha a solicitação para lá (TS 23.228, TS 29.228). O OmniWeb exibe o pool de S-CSCF do qual ele escolhe, sua conectividade Cx com o HSS, a segurança interdomínio que aplica e as sessões que está atualmente roteando.

← Guia de Operações

O painel é uma página de elemento por instância acessada a partir da barra lateral quando um I-CSCF está em execução no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API de gerenciamento do I-CSCF, portanto, permanece atrás do único gateway autenticado. Um link de documentação no cabeçalho da página fornece ajuda contextual. A página está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela do I-CSCF: a versão e o tempo de atividade do **motor SIP**, o número de **S-CSCFs** no pool do qual ele pode selecionar, e a contagem de **sessões** que está atualmente roteando. O I-CSCF é sem estado entre transações: ele seleciona um S-CSCF e sai do caminho. Portanto, isso é principalmente uma confirmação de que o gateway está ativo e pode alcançar tanto o HSS quanto a camada de serviço.

Lista de S-CSCF

O **pool de S-CSCFs servidora** entre os quais o I-CSCF escolhe. Quando o HSS retorna *capacidades* em vez de um nome específico de S-CSCF para um assinante, o I-CSCF escolhe um servidor deste pool cujas **capacidades** anunciadas atendem ao requisito. Cada linha mostra o **nome** de um S-CSCF, seu **URI SIP** (o endereço para o qual o I-CSCF encaminha), o **conjunto de capacidades** que ele anuncia e seu **status**. É aqui que você confirma a camada de serviço pela qual o I-CSCF pode distribuir registros e identifica um S-CSCF que saiu do pool.

Domínios NDS

A configuração de **Segurança de Domínio de Rede (NDS/IP)**: os domínios pares com os quais o I-CSCF troca sinalização e as associações de segurança **IPsec** que protegem esse tráfego entre gateways de segurança (TS 33.210). Como o I-CSCF é a borda da rede para sinalização IMS, é aqui que a proteção interoperadora e interdomínio é aplicada. Cada entrada descreve um **domínio** par e o estado da associação de segurança que transporta tráfego para ele. Em uma implantação de operador único, esta lista geralmente está vazia, o que é esperado.

Sessões

As **transações que o I-CSCF está atualmente lidando**: registros e chamadas em andamento, cada uma mostrando a identidade do assinante envolvido e o **S-CSCF** que o I-CSCF selecionou para ela. É uma visão ao vivo das decisões de roteamento que o gateway está tomando agora, útil para confirmar que o tráfego para um determinado assinante está sendo direcionado para o S-CSCF servidora esperado.

Diameter

A conectividade **Diameter** do I-CSCF: sua peering **Cx** em direção ao **HSS** (diretamente, ou via um **DRA**). Cx é a interface que o I-CSCF usa para **Autorização de Usuário (UAR/UAA)** no registro e **Informação de Localização (LIR/LIA)** em uma chamada terminante, portanto, cada decisão de seleção de S-CSCF depende dela. Cada linha mostra o **host** de um par, **domínio**, as **aplicações Diameter** que ele suporta e o **estado de conexão**. Um par Cx que está fora do ar aqui significa que o I-CSCF não pode resolver qual S-CSCF usar, e registros e chamadas terminantes falharão.

Logs

A aba **Logs** exibe a saída do log ao vivo do I-CSCF. Solucione problemas de uma única instância sem sair do OmniWeb: uma seleção de S-CSCF falhada, um tempo limite Cx ou uma solicitação de entrada rejeitada.

Painéis de Monitoramento

As taxas de registro e roteamento de chamadas, a latência de transação Cx e os resultados da seleção de S-CSCF para o I-CSCF são apresentados como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **HSS**: o I-CSCF o consulta através do **Cx** (UAR/LIR) para selecionar ou resolver o S-CSCF servidora; a aba Diameter mostra essa peering.
- **S-CSCF**: a camada servidora para a qual o I-CSCF distribui registros e encaminha chamadas terminantes; seus membros estão listados na aba Lista de S-CSCF.
- **P-CSCF**: encaminha o REGISTER inicial de um UE para a rede doméstica onde o I-CSCF realiza a seleção do S-CSCF.
- **DRA**: pode estar entre o I-CSCF e o HSS para roteamento e balanceamento de carga do tráfego Diameter Cx.
- Guia de Operações: de volta ao índice de elementos.

LCS: Serviços de Localização (OmniLCS)

A função **LCS** fornece **serviços de localização** para o núcleo. Ela responde "onde está este assinante?" e aciona avisos de transmissão celular. Ela resolve a posição de um UE a partir da célula de serviço (e da geometria da célula configurada), atende a solicitações de localização da rede (imediatas e adiadas) e envia avisos de **Alertas Móveis Comerciais / transmissão celular** para uma área. O OmniWeb exibe o inventário de células do LCS, correções de localização ao vivo e recentes, solicitações de localização adiadas, alertas e transmissões CAP; tendências de longo prazo estão nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

O LCS é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda contextual) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status** do LCS, sessões de localização **ativas** e **concluídas**, o número de **células carregadas** e o resultado da **sincronização de células**. Esta é a confirmação mais rápida de que o LCS está ativo e possui geometria de célula atual.

A visão geral também mostra cada conexão que o LCS mantém com o resto do núcleo, cada uma com seu estado (**Conectado** ou **Desconectado**), endereço e, para associações SCTP, o id da associação e o tempo em que foi estabelecida:

- **Pares SBc-AP**: a associação de **transmissão celular** 4G para cada MME. Uma transmissão de aviso 4G só pode alcançar as células de um MME cuja associação SBc-AP esteja conectada, então isso é a primeira coisa a verificar quando uma transmissão não chega aos dispositivos.
- **Pares SLs**: a associação **LCS-AP** para cada MME, que transporta posicionamento (E-CID, OTDOA, A-GNSS) entre o LCS e o MME de serviço.
- **Pares Diameter**: as conexões Diameter SLg/SLh (por exemplo, para o DRA), com os ids de produto e aplicação do par.

- **Feeds CAP**: cada conexão a uma fonte de alerta (veja Feeds CAP), com o tempo de seu último heartbeat ou poll.

Os tiles na parte superior contam os pares conectados de cada tipo em relação ao total configurado, ficando vermelhos quando algum está fora do ar.

Células

O **inventário de células** contra o qual o LCS posiciona: id de cada célula, latitude/longitude, raio, altura, TAC/LAC, PCI, EARFCN, azimute e RAT. Você pode adicionar, editar e remover células aqui. Esta geometria é o que transforma um id de célula de serviço em uma posição.

Adicionando ou editando uma célula

1. Escolha o **rádio** (2G, 3G, 4G ou 5G). A caixa de diálogo mostra os campos que esse rádio utiliza: LAC para 2G/3G, TAC para 4G/5G, e o número de canal correspondente (ARFCN, UARFCN, EARFCN ou NR-ARFCN) e a identidade física da célula.
2. Insira o **ID da Célula** exatamente como a rede o reporta. Para 4G, **Construir ECI a partir do ID do eNB** calcula o ECI a partir do ID do eNB e do número da célula.
3. Insira o **TAC** ou **LAC**. As transmissões de células para esta célula vão para este código de área.
4. Posicione a célula: clique no mapa, arraste o marcador ou digite ou cole a latitude e longitude (`lat, lon` colado em qualquer uma das caixas preenche ambas). Defina o **raio** de cobertura e, para uma antena setorizada, o **azimute**; o mapa mostra a cobertura resultante.

Cada valor é verificado em relação ao seu intervalo válido antes que a célula possa ser salva. Um alerta CAP chega a uma célula quando a posição da célula está dentro da área de alerta, então uma célula sem posição, ou com o TAC ou LAC errados, não recebe alertas.

Localização

Correções de localização recentes: assinante de cada correção, célula resolvendo, posição computada, precisão e método. Uma localização pode ser **solicitada** para um assinante a partir daqui, e abrir uma correção mostra sua posição autoritativa mais recente conhecida. É aqui que um operador confirma um resultado de posicionamento.

Adiado

As **solicitações de localização adiadas pendentes** que o LCS está segurando. Enquanto a aba Localização responde "onde está este assinante *agora*", uma **MT-LR adiada** (solicitação de localização móvel terminada adiada) pede à rede para relatar a posição de um assinante **mais tarde, quando um gatilho for acionado**, em vez de imediatamente: o GMLC arma a solicitação e o relatório retorna quando a condição é atendida. Os gatilhos comuns são **disponibilidade do UE** (relatar na próxima vez que o dispositivo se tornar acessível, tendo estado ocioso ou inacessível quando a solicitação foi feita), localização **periódica** (relatar em um **intervalo** fixo por um **número** definido de relatórios) e eventos de área/movimento (relatar quando o UE entra, sai ou se move dentro de uma área designada). É assim que um operador agenda o posicionamento para um assinante que não pode ser encontrado no momento ou que precisa ser rastreado ao longo do tempo.

Cada linha lista o assinante da sessão adiada por **IMSI**, seu **tipo** (periódico ou acionado), o **método** de posicionamento, seu cronograma (o intervalo de relatório para uma sessão periódica; o evento de área e o intervalo de poll para uma acionada), os **relatórios restantes** do total, seu **status**, o cliente

solicitante, quando **começou** e o tempo da **última correção**. Uma sessão acionada sem limite de relatório mostra *infinidade* de relatórios restantes.

Um operador pode **criar** uma nova solicitação adiada a partir daqui, nomeando o IMSI alvo, o tipo e o método de posicionamento (célula, E-CID, GNSS ou OTDOA):

- **Periódico**: o intervalo de relatório em segundos e o número de relatórios a serem enviados.
- **Acionado**: o evento de área (**entrando**, **saindo** ou **estando dentro**), a própria área (um círculo dado pelo seu centro e raio em metros, ou um polígono de pelo menos três pontos de latitude/longitude), o número máximo de relatórios (0 para ilimitado) e com que frequência o LCS poll a posição do assinante.

Um operador também pode **cancelar** uma sessão pendente a qualquer momento, o que desarma a solicitação armada para que nenhum relatório adicional seja produzido. A lista faz polling para que o status de uma sessão seja atualizado à medida que a rede a arma e o gatilho é acionado.

Alertas CAP

Os **alertas do Protocolo Comum de Alerta (CAP)** que o LCS aceitou para transmissão celular, em três grupos:

- **Aguardando aprovação**: alertas aguardando um operador. **Aprovar** transmite o alerta para as células dentro de sua área de aviso; **Rejeitar** descarta-o.
- **Ativos**: alertas sendo transmitidos. **Parar Transmissão** retira um alerta do ar em cada rede na qual foi enviado.
- **Histórico**: alertas que foram enviados, rejeitados, **cancelados** (pela autoridade emissora ou um operador) ou **expirados**.

Cada alerta mostra de onde veio (um feed CAP ou uma submissão manual), o identificador e remetente CAP, e uma linha por **idioma**: o idioma, o **identificador de mensagem** de transmissão celular pelo qual é enviado e o texto enviado para os dispositivos. Quando um alerta foi enviado, cada linha também mostra o número de série e o resultado por rede. O rodapé fornece o código da rede, os TACs/LACs alvo, quantas células corresponderam à área de aviso e quando o alerta foi recebido, enviado, aprovado, expirou e finalizado.

Os alertas chegam automaticamente dos feeds CAP, ou um operador pode **Submeter Alerta** com XML CAP. Nem toda mensagem CAP é para dispositivos. O LCS aplica as regras de alerta abaixo, e uma submissão que não se qualifica é reportada em vez de enfileirada:

- apenas alertas **Atuais** com escopo **Público** são transmitidos. Mensagens de teste que não são destinadas à transmissão são ignoradas;
- para alertas canadenses (CAP-CP), apenas blocos de informação sinalizados para distribuição sem fio são transmitidos, usando seu texto sem fio;
- cada idioma é enviado como sua própria transmissão: o idioma primário no identificador de mensagem configurado (4370 por padrão) e cada outro idioma no identificador de idioma adicional correspondente (4383);
- um **Cancelar** ou **Atualizar** da autoridade emissora interrompe a transmissão do alerta anterior, e um alerta para de ser transmitido quando **expira**;
- o mesmo alerta (mesmo remetente e identificador) é processado apenas uma vez.

Feeds CAP

Os **feeds CAP** dos quais o LCS recebe alertas. Dois tipos são suportados:

- **Fluxo NAAD (Canadá)**: o Sistema Nacional de Agregação e Disseminação de Alertas Pelmorex (NAAD). O LCS se conecta a todos os sites de streaming ao mesmo tempo (os dois sites oferecem redundância) e espera um heartbeat de cada um a cada minuto; um site que fica em silêncio é reconectado. Cada heartbeat lista os alertas mais recentes, e qualquer um que não chegou no fluxo é buscado no arquivo NAAD, então um alerta emitido enquanto uma conexão estava fora ainda é recebido.
- **Feed Atom CAP**: um feed CAP em formato Atom, polled em um intervalo definido.

Cada feed mostra se está habilitado, sua configuração de aprovação e, para cada site ou URL, o **estado de conexão**, o tempo do último heartbeat (ou poll) e contadores: alertas e heartbeats recebidos, alertas **submetidos** para transmissão, **ignorados** (não para dispositivos), **cancelados**, **duplicados** (o mesmo alerta do outro site) e alertas **preenchidos** do arquivo.

Adicionar Feed cria um feed. O botão **Canadá — Pelmorex NAAD** preenche ambos os sites de streaming NAAD e ambos os endereços de arquivo. Para cada feed você define seu nome, tipo, URLs, se está habilitado e seu comportamento de **aprovação**: usar a configuração de todo o LCS, exigir que um operador aprove cada alerta ou transmitir sem aprovação. Feeds adicionados aqui podem ser editados, habilitados ou desabilitados, e excluídos. Feeds definidos na configuração do LCS são marcados como **Da configuração** e são somente leitura aqui.

Transmissões

A aba **Transmissões** mostra as mensagens de **transmissão celular** que o LCS está enviando, uma linha por rede: o identificador da mensagem e seu nome (identificadores de teste e exercício são marcados como **teste**), o número de série, a rede (2G sobre CBSP, 3G sobre SABP, 4G sobre SBc-AP), o texto da mensagem, seu status e quando foi enviada. A visão de **Histórico** lista transmissões passadas, incluindo seu tipo de aviso.

O número de série é mostrado em hex com seu **código de mensagem** e **número de atualização**; passe o mouse sobre ele para ver o escopo geográfico. Um dispositivo mostra uma mensagem apenas uma vez para cada identificador de mensagem e número de série. Uma linha onde o mesmo identificador e número de série foram enviados mais de uma vez é marcada como **duplicado – dispositivos ignoram**: dispositivos que receberam o primeiro envio não exibiram os posteriores.

Um operador pode **parar** uma transmissão ativa a partir de sua linha; a parada se aplica apenas à rede daquela linha, então uma mensagem enviada tanto em 3G quanto em 4G é parada em cada uma separadamente.

Enviar Transmissão inicia uma nova:

- **ID da Mensagem**: escolha a partir da lista 3GPP (ETWS terremoto/tsunami, CMAS/WEA presidencial, extremo, severo, AMBER, teste mensal, exercício, definido pelo operador, segurança pública, teste estadual/local) ou insira um valor personalizado. Para identificadores ETWS, escolha o **tipo de aviso** ETWS.
- **Idiomas**: o texto da mensagem, além de qualquer número de **idiomas adicionais**. Cada idioma adicional é enviado no identificador de idioma adicional que corresponde ao escolhido (por exemplo, 4370 → 4383), com o mesmo número de série, e o resultado de cada idioma é reportado. Identificadores ETWS e personalizados não têm identificador de idioma adicional. Sob cada texto, um contador mostra a codificação (GSM 7-bit, ou UCS-2 quando o texto tem caracteres como algumas letras acentuadas) e as páginas usadas, até 15.
- **Número de série**: construído a partir do **escopo geográfico**, um **código de mensagem** (0–1023) e um **número de atualização** (0–15). Um novo alerta recebe o próximo código de mensagem ainda não utilizado para aquele identificador. **Enviar como atualização de…** seleciona uma transmissão anterior e mantém seu código com o número de atualização aumentado em um, para que os dispositivos substituam a mensagem

anterior. Um aviso aparece quando o identificador e o número de série já foram enviados, porque os dispositivos ignorariam a mensagem.
- **MCC e MNC** da rede para a qual está sendo transmitido (sempre necessário, para que uma transmissão nunca saia sob o código de rede errado), as redes para enviar e os **TACs** alvo (4G), **LACs** (2G/3G) e **SACs** (3G) para as redes selecionadas.
- Com que frequência e quantas vezes a mensagem se repete (0 repetições até ser parada).

Logs

A aba **Logs** acompanha a saída do log ao vivo do LCS para solução de problemas sem sair do OmniWeb.

Painéis de monitoramento

As taxas de solicitações de localização e outras séries temporais são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **MME** solicita posicionamento através das interfaces de localização e é o par Diameter do LCS.
- **Alertas CAP** e **transmissões** alimentam o sistema de aviso de transmissão celular.

Servidor de Licenças: Licenciamento Omnitouch

O **Servidor de Licenças** é a autoridade de licenciamento Omnitouch contra a qual as funções da rede verificam. Cada produto Omnitouch (o MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF e outros) valida sua concessão contra o Servidor de Licenças antes de ser executado, perguntando se um determinado **licenciado** está licenciado para esse **produto** e se a licença ainda está dentro do seu período de validade. O servidor mantém **licenças** criptograficamente **assinadas**, cada uma concedendo a um licenciado um conjunto de produtos com um período de validade e metadados, e responde a consultas de concessão e registra cada solicitação que recebe. Como uma licença só é significativa em relação a um relógio confiável, o servidor também rastreia uma fonte de **tempo confiável** para que uma licença não possa ser revivida retrocedendo o relógio de um nó. O OmniWeb exibe o que está licenciado e sua saúde, o registro de solicitações de concessão feitas pelas funções da rede, uma ferramenta de consulta sob demanda e os logs ao vivo do servidor.

← Guia de Operações

O Servidor de Licenças é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, com uma visão de frota onde vários estão implantados. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do Servidor de Licenças, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Está organizada em abas.

Visão Geral / Status

Uma leitura de tela única do que o servidor está licenciando e se está saudável. Os cartões de resumo fornecem a contagem de **produtos totais**, quantos são **válidos** e **inválidos**, e o número de **licenciados** distintos. Um painel de **tempo confiável** mostra o estado da fonte de relógio do servidor: **válido**, **período de carência** ou **inválido**. Quando o tempo confiável não está disponível, o servidor não pode validar licenças com segurança, e isso eleva a saúde da página para um aviso ou erro.

A tabela de **Produtos Licenciados** lista uma linha por produto licenciado, cada uma mostrando o **produto**, o **licenciado** a quem é concedido, quando foi **emitido**, suas datas de **início** e **expiração** (com um indicador de "dias restantes" ou "expirou há N dias" que fica âmbar dentro de 30 dias da expiração e vermelho uma vez passado), e seu status de **válido/inválido**. Abrir uma linha expande o detalhe completo: os timestamps exatos de validade, se a **assinatura criptográfica** é válida, quaisquer metadados do produto e a própria assinatura. Esta é a confirmação mais rápida de que as funções da rede estão todas licenciadas e que nada está prestes a expirar.

Registros de Solicitações

A trilha de auditoria das **solicitações de concessão** que as funções da rede fizeram contra o servidor. Cada linha registra o **timestamp**, o **IP de origem** de onde a solicitação veio (qual host da função de rede perguntou), o **licenciado** e o **produto** sobre o qual perguntou, a **decisão** (**permitido** ou **rejeitado**), e, para uma rejeição, a **razão**. A lista pode ser filtrada por decisão, por produto e por uma pesquisa parcial de **IP de origem** ou **licenciado**, e é paginada. É aqui que você vê, por exemplo, que uma função recém-implantada está sendo rejeitada porque seu produto nunca foi licenciado, ou confirmar que uma função está verificando com sucesso.

Consulta de Licença

Uma **verificação de concessão** sob demanda. Insira um **licenciado** e um **produto** e a ferramenta pergunta ao servidor a mesma questão que uma função de rede faria (este licenciado tem direito a este produto agora) e retorna o veredicto: **válido** ou **inválido**, a data **válido até** da licença, o **timestamp** da resposta, quaisquer **metadados**, e a **assinatura**. É a maneira direta de confirmar uma concessão específica sem esperar que a função proprietária verifique, e lista os identificadores de produtos conhecidos (por exemplo, `omnihss`, `omniupf`, `omnimme`) para que você possa consultar exatamente um.

Logs

A aba de **Logs** exibe a saída de log ao vivo do Servidor de Licenças para solucionar problemas de uma única instância sem sair do OmniWeb.

Relacionados

- **Cada função de rede Omnitouch**: o MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF e outros validam sua concessão aqui; a própria aba **Visão Geral / Status** de cada produto mostra um distintivo de saúde da licença derivado dessa verificação.
- Guia de Operações: voltar ao índice de elementos.

Logs & Rastreio de Assinantes

OmniWeb oferece aos operadores várias visões complementares e em tempo real do que a rede está fazendo:

1. **Logs**: logs de serviço estruturados e ao vivo para qualquer elemento único, alimentados pelo Loki.
2. **Rastreio de Sessão**: uma visão de rede cruzada que segue um assinante através de todos os protocolos e elementos (Diameter, GTP-C, PFCP, SIP, MAP).
3. **Homer**: captura profunda de pacotes SIP/VoIP e análise de fluxo de chamadas.

← Voltar ao Guia de Operações

Ir para um Assinante a partir de um NF

Muitas funções de rede mostram um assinante, UE ou sessão por IMSI. Isso inclui o **MME** (UEs), **SGW-C**, **PGW-C** e **ePDG** (Sessões), **MSC** e **TAS** (Assinantes), e **SMSC** (Localização). Em cada caso, uma linha de botões de link rápido permite que você vá diretamente para esse assinante em outro lugar, sem precisar copiar o IMSI:

- **Ir para Registro HSS** abre o registro de provisionamento do assinante no HSS (resolvido por IMSI através das instâncias HSS configuradas).
- **Ver Rastreio de Sessão** abre a escada de sinalização ao vivo do assinante no Rastreio de Sessão, restrita a esse IMSI.
- **Ver Logs** abre a aba de Logs *deste* elemento pré-filtrada para esse IMSI, para que você veja apenas as linhas de log para esse assinante.

Cada botão aparece apenas quando se aplica: o IMSI é conhecido e um HSS ou Rastreio de Sessão está configurado para o site. O conjunto, portanto, se adapta à implantação.

Os links rápidos de assinante (aqui em um MME UE): um clique para o registro HSS, a escada de sinalização ao vivo ou os logs deste elemento filtrados para o assinante.

Logs em Tempo Real (Loki)

Cada elemento tem uma aba de **Logs**. Ela consulta os logs de serviço do elemento a partir do Loki e transmite novas linhas à medida que chegam, para que você possa assistir a um elemento ao vivo enquanto faz uma alteração ou reproduz um problema.

A aba de Logs (aqui em um UPF): linhas de log estruturadas e codificadas por cores transmitidas do Loki, com filtros de serviço, severidade, protocolo e assinante (IMSI). Cada elemento expõe o mesmo visualizador.

Como funcionam as consultas de log

O frontend constrói uma consulta LogQL e a envia através do gateway Loki do backend. Nada consulta o Loki diretamente do navegador. É proxy (e, portanto, autenticado e auditado) como qualquer outra solicitação.



O gateway envia a consulta para o Loki do **site selecionado** (o host de monitoramento desse site, porta 3100). As consultas usam a API de consulta de intervalo do Loki com uma expressão LogQL, uma janela de tempo, um limite de resultados e uma direção (mais recente primeiro ou mais antigo primeiro).

Para ler logs, um usuário precisa da permissão **Logs (Loki)** (`GET`) e acesso ao site selecionado, ambos configurados em Configurações → Permissões. Os administradores já a possuem. O gateway é somente leitura: ele recusa os

endpoints de push e delete do Loki. Métricas através de `/proxy/prometheus` funcionam da mesma forma, com a permissão **Métricas (Prometheus)**.

Seletores vs. filtros de pipeline

OmniWeb constrói consultas estruturadas a partir de dois tipos de filtro:

Colocação do filtro	Posição LogQL	Exemplo	Uso
Selector	Dentro do seletor de stream `{ … }`	`{hostname="omni-eval-upf01"}`	Escolher quais streams (qual host/serviço) ler. Indexado e rápido.
Pipeline	Após um `|`	`| level="error"`	Filtrar as linhas correspondentes por um campo estruturado.

Uma aba típica de Logs de elemento fixa o host/serviço como um seletor e permite que você adicione filtros de pipeline (severidade, componente, identificadores de assinante) por cima. Como os serviços Omnitouch emitem linhas de log **estruturadas**, você pode filtrar em campos reais em vez de grepar texto livre.

Dados de log estruturados

Os hosts enviam logs estruturados para o Loki (configurado pelo papel comum do Ansible). Duas fontes estruturadas especialmente úteis:

- **Logs de serviço**: a própria saída estruturada de cada NF, rotulada por `hostname`/serviço, disponível na aba de Logs desse elemento.
- **Auditoria de comandos**: cada comando executado em um host, incluindo quem fez login (sobrevivendo a `sudo`/`su`), o UID efetivo, o binário, o diretório de trabalho e a linha de comando completa. Enviados para o Loki. Veja Registro de Auditoria para a referência de campo.

Usando a aba de Logs

1. Abra qualquer elemento e selecione **Logs**.
2. O visualizador abre **Pausado** nos últimos cinco minutos. Mude para **Ao Vivo** para consultar novas linhas e segui-las; **limpar** mantém apenas o que chega a partir daquele momento.
3. Afine a visualização com os filtros ou digite um IMSI, MSISDN, Call-ID ou tipo de mensagem na caixa de pesquisa e **Aplicar**. O visualizador reconhece o identificador e aplica o filtro correspondente; qualquer outra coisa é uma correspondência de texto livre.
4. Ajuste a janela de tempo para olhar para um evento passado. Cada filtro, a janela de tempo e o estado Ao Vivo vivem na URL da página, então uma visualização pode ser atualizada, marcada ou colada em um ticket.
5. Rolando para cima enquanto ao vivo mantém seu lugar. Um pílula de **novas linhas** conta o que chegou e volta para o final quando clicado.

> **Dica:** Ao investigar um assinante, filtrar logs de elementos pelo seu IMSI/MSISDN é o primeiro passo rápido; para ver o assinante em *múltiplos* elementos ao mesmo tempo, use o Rastreio de Sessão abaixo.

Rastreio de Sessão: Siga um Assinante pela Rede

O motor de **Rastreio de Sessão** correlaciona a sinalização para um único assinante através de múltiplos elementos e protocolos, fornecendo uma linha do tempo unificada desde a conexão de rádio até a autenticação, estabelecimento de sessão e entrega de chamadas/SMS. Esta é a ferramenta para responder "o que aconteceu com este assinante?" sem pular entre CLIs de elementos.

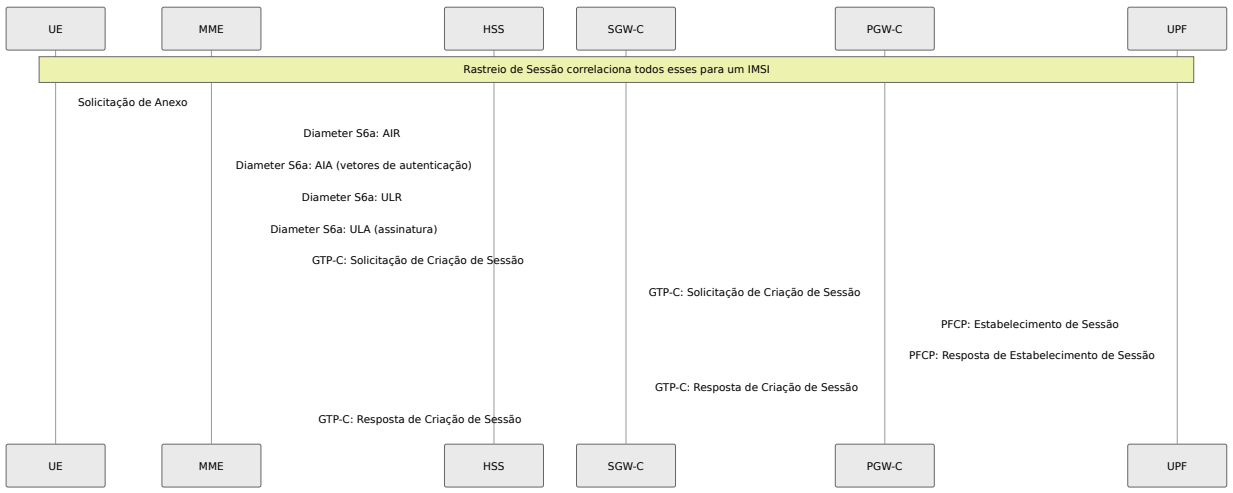
Rastreio de Sessão: pesquise por IMSI ou MSISDN e correlacione a atividade de um assinante através de Diameter, GTP-C, PFCP, SIP e MAP, com abas por protocolo na parte superior.

Protocolos suportados

Protocolo	O que mostra	Elementos envolvidos
Diameter	Autenticação, política, cobrança	HSS, DRA, PGW-C, PCRF, OCS, CSCF (Cx/Dx/Rx)
GTP-C	Gerenciamento de sessão (S5/S8, S11)	SGW-C, PGW-C, MME
PFCP	Regras de sessão de plano de usuário (N4)	PGW-C/SMF ↔ UPF
SIP	Controle de chamada IMS	P-CSCF, I-CSCF, S-CSCF, TAS
MAP	Localização SS7, autenticação, SMS	MSC, HLR, CAMEL GW, IP-SM-GW

Rastreio de Usuário

A visualização de **Rastreio de Usuário** permite que você pesquise por **IMSI** ou **MSISDN** e veja cada interação de protocolo correlacionada para esse assinante através da rede. Um único anexo, por exemplo, revela a autenticação Diameter, a criaç��o da sessão GTP-C e a instalação da regra PFCP como uma sequência coerente:



Abas específicas de protocolo

Cada protocolo tem sua própria aba (**Diameter, GTP-C, PFCP, SIP, MAP**), além de uma visão geral de **Todos os Protocolos**. As abas por protocolo são visualizações filtradas. Elas ajudam quando você persegue um problema específico de protocolo (por exemplo, apenas a troca SIP de uma chamada VoLTE) em vez de seguir um único assinante em tudo. Uma aba cujo protocolo nenhum elemento no site emite diz isso em vez de mostrar uma lista vazia.

Cada linha é disposta em colunas fixas: tempo, elemento, protocolo e interface, tipo de mensagem, direção, e então um resumo de uma linha do quadro. Linhas consecutivas para um grupo de assinantes sob um cabeçalho IMSI com **Abrir como escada**, que abre a escada de Fluxos Ao Vivo desse assinante em uma nova aba naquele momento; o mesmo link está no final de cada linha de assinante. Batimentos cardíacos e outras conversas internas são ocultados até que **Mostrar internos** esteja ativado.

Escada PCAP

A aba **Escada PCAP** transforma uma captura de pacotes em uma escada: um diagrama de sequência ordenado por tempo da sinalização. Carregue uma captura PCAP ou PCAPNG (por exemplo, de um tap de rede ou de um rastreio em nível de elemento) e o OmniWeb analisa os pacotes, identifica os nós de sinalização por endereço IP e função inferida (MSC/VLR, HSS, S-CSCF, e assim por diante), e correlaciona solicitações com suas respostas em sessões. O resultado é desenhado como uma escada de mensagens através desses nós, ordenada no tempo, para que você possa ler toda uma troca de cima para baixo em um relance.

Escada PCAP: uma captura carregada renderizada como uma escada através dos nós detectados. Clique em qualquer mensagem para ver seu quadro decodificado e hex.

Clique em uma mensagem na escada para abrir sua decodificação completa e hex, o mesmo detalhe que você obteria de um analisador de protocolo. A ferramenta reconhece as famílias de sinalização que você encontra em um núcleo móvel: MAP, CAMEL, TCAP, Diameter, SIP, GTP-C, PFCP e GSM SMS. Cada captura que você carrega é listada na aba para que possa ser reaberta ou compartilhada com um colega em vez de passar o arquivo por aí.

Fluxos Ao Vivo

A aba **Fluxos Ao Vivo** mostra a mesma visualização de escada, mas proveniente ao vivo dos logs de sinalização estruturados da rede (via Loki) em vez de um arquivo carregado. À medida que os elementos da rede emitem telemetria de sinalização, fluxos de chamadas recentes por assinante aparecem aqui automaticamente, agrupados por IMSI, sem necessidade de captura para carregar. Selecione um fluxo para reconstruí-lo na mesma escada que um PCAP, de modo que um fluxo ao vivo seja tão rico quanto um lido de um arquivo, até a decodificação e hex por mensagem.

Fluxos Ao Vivo: fluxos de chamadas recentes extraídos diretamente da telemetria de sinalização da rede. Filtre por IMSI, nó ou protocolo, e depois abra um fluxo para renderizar sua escada ao vivo.

Abra um fluxo e o OmniWeb o reconstrói na mesma escada que um PCAP, mas a partir da própria telemetria da rede, sem nada para capturar ou carregar. O exemplo abaixo é o anexo LTE de um único assinante, correlacionado através de cada elemento que o tocou: a troca S1AP/NAS com o **eNodeB**, a autenticação Diameter S6a e a atualização de localização contra o **HSS**, e a configuração da sessão GTP-C através do **SGW-C** e **PGW-C**. Tudo isso aparece em uma escada ordenada por tempo, com tempos de ida e volta de solicitação/resposta por mensagem e decodificação completa a um clique de distância.

Um fluxo ao vivo aberto em sua escada: o anexo LTE de um assinante através do eNodeB, MME, HSS, SGW-C e PGW-C, correlacionando S1AP, Diameter S6a e GTP-C. Clique em qualquer mensagem para sua decodificação e hex, ou em qualquer nó para focar suas trocas.

Se nenhuma telemetria de sinalização estiver fluindo ainda, a aba mostra um estado vazio; os fluxos se populam sozinhos à medida que os elementos da rede começam a emitir telemetria.

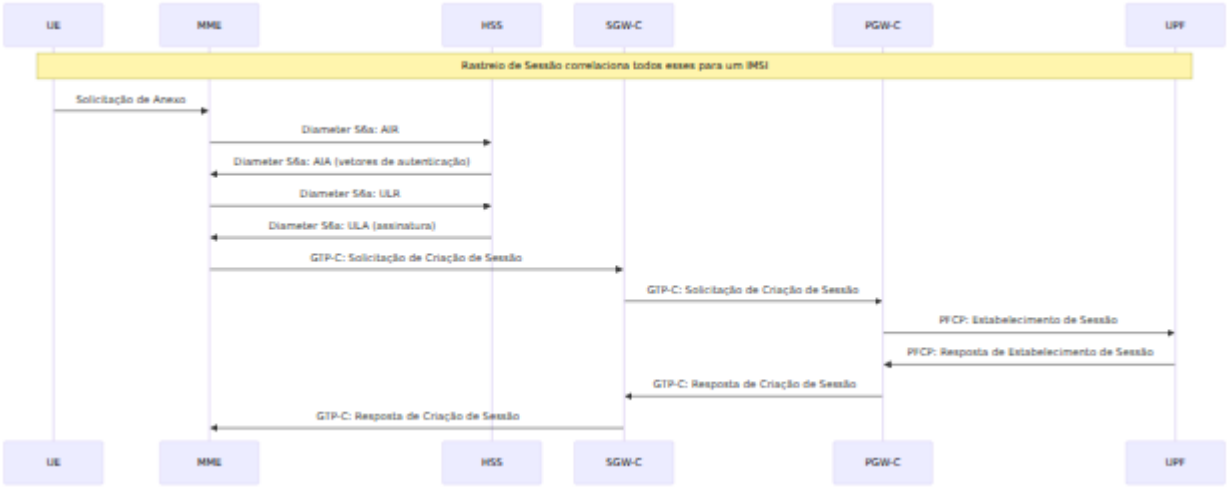
Homer: Captura SIP & Análise de Fluxo de Chamadas

OmniWeb integra-se ao Homer, a plataforma de captura SIP e solução de problemas VoIP de código aberto, para visualização profunda de fluxo de chamadas, decodificação de protocolos e pesquisa através da sinalização SIP capturada. Onde o Rastreio de Sessão fornece um *resumo* interprotocolar para um assinante, o Homer fornece o detalhe completo do pacote SIP, mensagem por mensagem.

Disponibilidade & acesso

Homer é **opcional** e detectado automaticamente. Na inicialização, o OmniWeb verifica `/api/homer/status`:

- Se o Homer estiver configurado (`HOMER_URL` definido no backend) e acessível, uma entrada **Homer** aparece na barra lateral.
- Se o Homer não estiver implantado, a entrada simplesmente fica oculta, e nada mais muda.



Clicar em **Homer** abre a UI web do Homer em uma nova aba do navegador. A autenticação é transparente: o gateway verifica seu login no OmniWeb através do mesmo single sign-on usado para o Grafana, então não há segundo login. O `HOMER_URL` do backend (e `HOMER_PROXY_SECRET`, quando definido) configuram a integração.

Casos de uso

Homer é a ferramenta a ser utilizada quando um problema está na camada SIP em si:

- **Análise de fluxo de chamadas VoLTE**: rastrear sequências SIP `INVITE`/`BYE` através de P-CSCF, I-CSCF, S-CSCF e TAS.
- **Solução de problemas VoWiFi**: analisar interações SIP entre ePDG ↔ P-CSCF.
- **Depuração de registro IMS**: inspecionar trocas `REGISTER` / `401` / `REGISTER` / `200 OK`.

- **Problemas de interconexão**: capturar sinalização de tronco SIP entre o MSC e pares SIP.

Rastreio de Sessão vs. Homer

Ambos ajudam na solução de problemas, mas respondem a perguntas diferentes. Eles são complementares, não alternativas:

Ferramenta	Melhor para	Escopo	Onde abre
Rastreio de Sessão	"Siga este assinante por toda a rede"	Diameter, GTP-C, PFCP, SIP, MAP correlacionados por IMSI/MSISDN	Inline no OmniWeb
Homer	"Mostre-me as mensagens SIP exatas para esta chamada"	Sinalização SIP/VoIP, decodificação completa de pacotes (VoLTE/VoWiFi/IMS)	Nova aba (detectada automaticamente)

Um fluxo comum é identificar uma anomalia relacionada ao SIP no Rastreio de Sessão e, em seguida, pular para o Homer para o fluxo de chamadas detalhado.

Solução de Problemas

Nenhum log aparece na aba de Logs de um elemento

Sintomas: A aba de Logs está vazia ou mostra "sem resultados".

Possíveis causas:

- O Loki não é acessível a partir do backend (`LOKI_URL` mal configurado).
- O host não está enviando logs para o Loki (envio de logs não está em execução / mal configurado).
- A janela de tempo selecionada é anterior aos logs disponíveis, ou o rótulo do host não corresponde.

Resolução:

1. Confirme que `LOKI_URL` aponta para uma instância Loki acessível.
2. Verifique se o host do elemento está enviando logs (verifique o agente de envio de logs nesse host).
3. Amplie a janela de tempo e remova filtros de pipeline para confirmar se alguma linha chega.

O Rastreio de Sessão não retorna nada para um assinante

Sintomas: Um Rastreio de Usuário por IMSI/MSISDN não mostra eventos.

Possíveis causas:

- O assinante estava inativo na janela selecionada.
- O identificador está digitado incorretamente (IMSI vs. MSISDN).
- Fontes de rastreio para o protocolo relevante não estão alimentando o motor.

Resolu��ão:

1. Verifique novamente o identificador e tente o alternativo (IMSI ↔ MSISDN).
2. Amplie a janela de tempo.
3. Confirme com a própria aba de Logs do elemento que o assinante estava ativo.

A entrada do Homer está faltando na barra lateral

Sintomas: Nenhum link **Homer** aparece.

Possíveis causas:

- O Homer não está implantado, ou `HOMER_URL` não está definido no backend.
- O Homer não é acessível, então `/api/homer/status` o reporta como indisponível.

Resolução:

1. Confirme que o Homer está implantado e `HOMER_URL` está definido no backend do OmniWeb.
2. Verifique se o backend pode alcançar o Homer e, em seguida, recarregue o OmniWeb (a detecção ocorre na inicialização).

MME: Entidade de Gerenciamento de Mobilidade

A **MME** é o ponto de ancoragem do plano de controle do EPC. Ela termina o **S1AP** para os eNodeBs, executa os procedimentos de anexação, autenticação e mobilidade para cada UE, e mantém um **contexto de UE** para cada assinante conectado. Ela busca dados de assinatura e autenticação do HSS através do **S6a** (Diameter), configura portadoras no Gateway de Serviço através do **S11**, e coordena transferências inter-MME e inter-sistema através do **S10/N26**. Em resumo, é o nó que decide onde e como cada assinante se conecta, é chamado e se move pela rede. O OmniWeb exibe os eNodeBs ativos da MME, contextos de UE, SGW e pares Diameter, estados de interface e status de transferência. Tendências de longo prazo estão nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

A MME é uma página de elemento por instância acessada a partir da barra lateral quando se navega no inventário do site, e, onde várias estão implantadas, uma visão de frota para status agregado. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API da MME, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status da API** da MME e um resumo de sua carga ativa, incluindo **eNodeBs** conectados, **UEs** anexados, **pares SGW** e o estado de seus pares **Diameter** (S6a). É a maneira mais rápida de confirmar que a MME está ativa e ver quanta da rede de acesso ela está atendendo.

eNodeBs

Cada eNodeB com o qual a MME tem uma associação S1AP, cada linha mostrando o **ID global de eNB**, nome e **estado** de conexão. Abra um eNodeB para mostrar seu contexto: as células atendidas e TACs e as UEs nele. Um operador pode **atualizar a capacidade da MME** anunciada a um eNodeB, o que ajusta como o eNodeB distribui a carga das UEs pela pool da MME (usado para drenar ou ponderar uma MME para manutenção ou reequilíbrio).

UEs

O **contexto de UE** de cada assinante anexado, cada linha identificada por **IMSI** e **GUTI** com seu estado de conexão e mobilidade e eNodeB atendido. Abrir uma UE mostra seu contexto completo. Uma variedade de ações por UE está disponível:

- **Chamar** a UE.
- **Enviar para inativo**: liberar a conexão de rádio enquanto mantém o contexto.
- **Transferir** a UE para outra MME.
- **Solicitar reanexação**: forçar a UE a reanexar.
- **Enviar SMS** para a UE.
- **Excluir** o contexto da UE: limpar um assinante obsoleto ou preso.

Você também pode **consultar o operador / PLMN** para um IMSI para identificar assinantes locais versus em roaming.

Pares S-GW

Os Gateways de Serviço com os quais a MME se comunica via **S11** (GTP-C), cada linha mostrando o **IP** do par, sua **atividade / acessibilidade**, o **contador de reinicialização (recuperação)** do GTP e a **contagem de sessões** ancoradas naquele gateway. O contador aumenta quando o S-GW reinicia, o que informa a MME para restabelecer as sessões que estava mantendo. Se um par foi aprendido por **DNS** ou é uma entrada **estática** é mostrado ao lado do **método de seleção** do S-GW que a MME aplica para assinantes locais e em roaming. Abra um par para listar as **sessões** que ele carrega, cada uma identificada por **IMSI** com seus **TEIDs S11** (os pontos finais do túnel do lado da MME e do S-GW). É onde um operador confirma quais S-GWs estão ativos e vê como as sessões de UE estão distribuídas entre eles. Isso ajuda ao equilibrar a carga ou diagnosticar por que portadoras para um grupo de assinantes falharam com um único gateway.

Reatribuição de GUTI e Offload S10

Duas ações de mobilidade são impulsionadas por IMSI em vez de por linha:

- **Reatribuição de GUTI**: reatribuir o **GUTI** de um assinante conectado para atualizar a identidade temporária que a UE apresenta (usado ao girar identificadores ou limpar uma incompatibilidade de identidade).
- **Offload S10**: forçar a transferência de um assinante para **outra MME**. Isso move o contexto de um assinante específico para fora desta MME via S10, e complementa o controle de capacidade do eNodeB quando você drena uma MME.

S10

A interface **S10/N26 inter-MME** é o caminho pelo qual o contexto de uma UE é realocado quando ela se move entre MMEs em uma pool durante um **TAU** ou **transferência** (e, via **N26**, entre a MME e um AMF para interoperação EPC-para-5GC). A aba tem duas partes. **Transferências ativas** lista as realocações em andamento, cada uma mostrando a MME **de origem** e **destino** e o **IMSI** que está sendo movido, para que um operador possa acompanhar um evento de mobilidade ou identificar um que está preso. **Descoberta de pares MME** mostra como a MME encontra seus pares na pool: as consultas **DNS / NAPTR** que ela executa e quaisquer pares **estáticos** configurados, com o FQDN e endereço de cada par. É onde você confirma que a

mobilidade inter-MME está saudável e que a MME pode realmente alcançar os vizinhos que precisa para transferir contextos. Complementa a ação de **offload S10** por assinante impulsionada a partir da aba UEs.

Diameter

Os pares Diameter da MME, principalmente o HSS via **S6a**, cada linha mostrando o **host** do par, **domínio** e **estado** de conexão. Abra um par para mostrar seus detalhes. É onde você confirma que o caminho de autenticação e assinatura para o HSS está ativo quando as anexações estão falhando.

Interfaces

A visualização de **Interfaces** relata o estado de cada interface da MME em um só lugar: **S1AP** para os eNodeBs, **GTP-C** (S11) para o SGW, **Diameter** para **S6a** (HSS) e **SLg** (serviços de localização), **SGsAP** (para o MSC para fallback CS e SMS), **LCS-AP / SLs** (serviços de localização), e **S10/N26** (transferência inter-MME e EPC-para-5GC). É a tela única para confirmar quais dos caminhos de sinalização da MME estão ativos e quais estão inativos.

Logs

A aba **Logs** acompanha a saída do log ativo da MME para solucionar problemas de uma única MME sem sair do OmniWeb.

Painéis de monitoramento

Taxas de anexação, contagens de UE, taxas de transferência e outras séries temporais para a MME são apresentadas como painéis do Grafana, acessados a

partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **HSS** mantém os dados de assinatura e autenticação que a MME busca via **S6a**.
- O **SGW-C** é o par de controle via **S11**. A MME controla a configuração de sessão e portadora nele.
- O **MSC** é acessado via **SGsAP** para fallback CS e SMS.
- Outras **MMEs** são acessadas via **S10** para mobilidade inter-MME, e o **AMF** via **N26** para transferência EPC-para-5GC.

Quectel EP06 Referência de Comandos AT (teste de rede celular)

Referência para o console do modem dos Dispositivos de Teste. Destina-se ao **Quectel EP06** (firmware `EP06ELAR04A05M4G`, IMEI `868186042000040`) no contêiner de laboratório, mas aplica-se à família EC25 / EG06 / EG06 / EM06. Cada comando abaixo foi testado contra o EP06 ao vivo; as respostas de exemplo são as **respostas reais capturadas desse modem** (ele estava em um estado de `NO SERVICE / SEARCH` na época, então os campos de sinal estavam vazios, e os analisadores devem lidar com isso).

O relé é de solicitação/resposta: `sendModemAt(serial, command, readMs, timeoutMs)` → backend `modem_at` → agente `modem.run_at(serial, command, min_read, timeout)`. `min_read` continua lendo a porta por pelo menos esse tempo para que URCs assíncronas sejam capturadas antes que a chamada retorne. Não há **fluxo URC persistente**. Veja "Registro de eventos" abaixo.

Informações do Dispositivo / SIM

Comando	Propósito	Resposta ao vivo
`ATI`	Fabricante / modelo / firmware	`Quectel` / `EP06` / `Revisão: EP06ELAR04A05M4G`
`AT+CGMM`	Modelo	`EP06`
`AT+CGMR`	Revisão do firmware	`EP06ELAR04A05M4G`
`AT+CGSN`	IMEI	`868186042000040`
`AT+CIMI`	IMSI	(IMSI da SIM)
`AT+QCCID`	ICCID	(ICCID da SIM)
`AT+CPIN?`	Estado do PIN da SIM	`+CPIN: READY`

Sinal / medição

Comando	Propósito	Resposta ao vivo
`AT+CSQ`	RSSI/BER (legado)	`+CSQ: 99,99` (99 = sem sinal). dBm = `-113 + 2*rssi`.
`AT+QCSQ`	Sinal por RAT	`+QCSQ: "NOSERVICE"`. Quando conectado: `+QCSQ: "LTE", <rssi>,<rsrp>,<sinr>, <rsrq>`.
`AT+QNWINFO`	RAT / banda / canal atual	`+QNWINFO: No Service`. Quando conectado: `+QNWINFO: "FDD LTE","<mccmnc>","LTE BAND 3",1850`.
`AT+QENG="servingcell"`	Medições completas da célula servidora	`+QENG: "servingcell","SEARCH"` (ocioso). Veja o formato abaixo.
`AT+QENG="neighbourcell"`	Células vizinhas	`OK` (nenhuma quando não acampada).

Formato LTE de `AT+QENG="servingcell"`

```
+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 (todos inteiros com sinal).
- `SINR` é um valor **convertido**: dB real = `(1/5)*SINR - 20` (faixa 0..250 → -20..+30 dB).

- `cellID`/`PCI`/`EARFCN` são geralmente hexadecimais/decimais por campo; `band` é o indicador da banda LTE.

Formato LTE de `AT+QENG="neighbourcell"`

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

Registro / conexão

Comando	Propósito	Resposta ao vivo
`AT+CFUN?`	Funcionalidade do rádio	`+CFUN: 1` (total). `0` = mínimo/avião.
`AT+CEREG?`	Registro EPS	`+CEREG: 2,2` (2 = procurando).
`AT+CEREG=2`	Habilitar URC de registro **com localização** (TAC/cellID)	`OK`
`AT+CGATT?` / `AT+CGATT=1` / `=0`	Estado de conexão PS / conectar / desconectar	`+CGATT: 0`
`AT+COPS?`	Seleção do operador atual	`+COPS: 0` (automático, não registrado).
`AT+COPS=?`	**Escaneamento de rede** (busca de operador, lento)	lista de tuplas `(stat,"long","short","numeric",AcT)`
`AT+COPS=0`	Seleção automática do operador	`OK`
`AT+COPS=1,2,"<mccmnc>"[,<AcT>]`	Seleção manual por ID numérico	`OK`

Bloqueio de célula / banda / RAT

Comando	Propósito	Resposta ao vivo
`AT+QNWLOCK=?`	Capacidades	`+QNWLOCK: "common/4g", <num de células>, [[<freq>,<pci>],...]` e `+QNWLOCK: "common/lte" [,<action>[,<EARFCN>, <PCI>[,<status>]]]`
`AT+QNWLOCK="common/4g"`	Consultar bloqueio de célula	`+QNWLOCK: "common/4g",0` (0 células = sem bloqueio); após bloqueio `+QNWLOCK: "common/4g",1,1850,0`.
`AT+QNWLOCK="common/4g", <n>,<EARFCN>,<PCI>[, <EARFCN>,<PCI>...]`	**Bloquear** em n células (funciona neste firmware)	`OK`
`AT+QNWLOCK="common/4g",0`	**Desbloquear**	`OK` (limpa o bloqueio).
`AT+QNWLOCK="common/lte"`	Consultar bloqueio de LTE de célula única (somente leitura)	`+QNWLOCK: "common/lte",0,0,0,0`.

> **Comportamento do firmware (verificado ao vivo no `EP06ELAR04A05M4G`):** a forma `common/4g` é a que aceita uma *ação* de bloqueio nesta unidade. `AT+QNWLOCK="common/4g",1,<EARFCN>,<PCI>` bloqueia (retorna `OK`, o bloqueio persiste) e `AT+QNWLOCK="common/4g",0` limpa. As formas de *conjunto* `common/lte` (`...,1,<EARFCN>,<PCI>` e

> `...,0`) todas retornam **`ERROR`** neste firmware, então `common/lte` é somente consulta aqui. A interface de usuário, portanto, usa `common/4g` tanto para bloquear quanto para desbloquear. | `AT+QCFG="band"` | Consultar máscara de banda | `+QCFG: "band",0x8d0,0x1a0880800d5,0x0` = (máscara GSM, máscara LTE, máscara TDS). | | `AT+QCFG="band",0,<lte_hex_mask>,0` | **Bloqueio de banda** (LTE). `0x0` máscara LTE = todas as bandas. | `OK` | | `AT+QCFG="nwscanmode"` | Modo de escaneamento RAT | `+QCFG: "nwscanmode",0` (0 = automático, 1 = GSM, 2 = WCDMA, 3 = LTE). | | `AT+QCFG="nwscanmode",<m>[,1]` | Definir preferência de RAT (`,1` = efetivo imediatamente) | `OK` | | `AT+QCAINFO` | Informações de agregação de portadora | `OK` (nenhuma agregada quando ocioso). |

Máscara de banda LTE: bit `(band-1)`, ou seja, banda N → `1 << (N-1)`. por exemplo, B3 = `0x4`, B7 = `0x40`, B28 = `0x8000000`. `0x0` (ou todos um) = todas as bandas habilitadas.

> **Nota do firmware:** `AT+QCFG="nwscanseq"` retorna `ERROR` neste firmware EP06 (`EP06ELAR04A05M4G`). A interface de usuário **não** expõe isso. `AT+QSCAN` também não é suportado neste firmware EP06 (é um comando da série RG/RM 5G). O escaneamento de rede usa `AT+COPS=?` mais `AT+QENG` em vez disso.

Chamadas de voz (VoLTE / IMS)

A voz do EP06 é **somente VoLTE**: precisa de IMS registrado sobre LTE. `AT+QCFG="ims"` nesta unidade retorna `+QCFG: "ims",1,0` (IMS habilitado por configuração, status atual 0).

Comando	Propósito
`AT+QCFG="ims"`	Consultar/habilitar IMS. `AT+QCFG="ims",1` para forçar a habilitação.
`ATD<number>;`	Discar uma chamada de voz (o `;` final = voz, não dados).
`ATA`	Atender uma chamada recebida.
`ATH` / `AT+CHUP`	Desligar.
`AT+CLCC`	Listar chamadas atuais: `+CLCC: <id>,<dir>,<state>,<mode>,<mpty>,"<number>",<type>`. `OK` vazio = sem chamadas.
`AT+CLIP=1`	Habilitar URC de identificação da linha de chamada (`+CLIP:`) em `RING`.

Estados de chamada do `AT+CLCC`: 0 ativa, 1 em espera, 2 discando, 3 alertando, 4 recebendo, 5 aguardando.

SMS (modo texto)

Comando	Propósito	Resposta ao vivo
`AT+CMGF=1`	Modo texto (vs PDU)	`OK`
`AT+CPMS?`	Áreas de armazenamento / contagens	`+CPMS: "ME",0,255,"ME",0,255,"ME",0,255`
`AT+CMGL="ALL"`	Listar mensagens (modo texto)	por mensagem: `+CMGL: <index>,"<stat>","<sender>",,"<timestamp>"` então linha do corpo.
`AT+CMGR=<index>`	Ler uma mensagem	`+CMGR: "<stat>","<sender>",,"<timestamp>"` + corpo.
`AT+CMGS="<number>"` então corpo + Ctrl-Z	Enviar (manipulado pelo agente `send_sms`).	`+CMGS: <mr>`
`AT+CMGD=<index>[,<delflag>]`	Deletar mensagem (`delflag` 4 = todas).	`OK`
`AT+CNMI?` / `AT+CNMI=2,1,0,0,0`	Configuração de indicação de nova mensagem	`+CNMI: 2,1,0,0,0`

PDP / dados

Comando	Propósito	Resposta ao vivo
`AT+CGDCONT?`	Listar contextos PDP (APNs)	`+CGDCONT: 1,"IPV4V6","ims",...`
`AT+CGDCONT=<cid>,"<type>","<apn>"`	Definir contexto. tipos: IP, IPV6, IPV4V6, Non-IP.	`OK`
`AT+CGACT=1,<cid>` / `=0,<cid>`	Ativar / desativar contexto.	`OK`
`AT+CGPADDR[=<cid>]`	Mostrar IP atribuído.	`+CGPADDR: 1,"<ip>"`
`AT+CGCONTRDP=<cid>`	DNS / gateway / PCO.	`+CGCONTRDP: ...`
`AT+QPING=1,"<host>"`	Ping do modem (respostas URC; precisa de `min_read`).	`+QPING: ...`

Registro de eventos (URCs): e a limitação do relé

O relé do agente é **solicitação/resposta com uma porta por chamada aberta**. Ele abre a porta serial, envia um comando, lê até OK/ERROR (ou `min_read` expira), então fecha. Ele **não** mantém a porta aberta para transmitir códigos de resultado não solicitados (URCs) de volta para o navegador. Portanto, um verdadeiro feed de eventos ao vivo não é possível por esse caminho sem alterações no agente.

URCs que valem a pena habilitar (cada um é um comando `OK` de um único uso):

Comando	Habilita URC
`AT+CEREG=2`	`+CEREG:` alterações de registro (com TAC/cellID).
`AT+CGEREP=2,1`	`+CGEV:` eventos PS/bearer.
`AT+CLIP=1`	`+CLIP:` identificação de chamador em `RING`.
`AT+CNMI=2,1,0,0,0`	`+CMTI:` nova indicação de SMS.
`AT+QINDCFG="all",1`	`+QIND:` indicações Quectel.

Abordagem pragmática usada na interface de usuário: a aba Eventos habilita os URCs acima, então **consulta** o modem em um intervalo (`AT+CEREG?`, `AT+CLCC`, `AT+QENG`, `AT+CSQ`, `AT+CMGL`) e renderiza mudanças de estado em um log com timestamp. Cada consulta também usa uma janela curta de `min_read` para que qualquer URC que chegue durante a leitura seja capturada oportunisticamente. Isso captura transições de estado (registro ganho/perdido, chamada iniciada/terminada, novo SMS, mudança de sinal) na cadência de consulta, o que é suficiente para testes em laboratório. A limitação é documentada na interface de usuário.

MSC: Centro de Comutação Móvel

O **MSC** é o coração do controle de chamadas do núcleo comutado por circuito. Ele mantém o registro de localização do visitante (VLR) para os assinantes atualmente em sua área de serviço, estabelece e encerra **chamadas de voz**, transporta **SMS** e gerencia a **mobilidade** (atualizações de localização, paginação e transferências) para esses assinantes. Ele alcança o lado rádio por meio de conexões **RAN/BSC** (interface A, conduzida por M3UA/SS7), conecta a voz ao IMS e interconecta através de **pares SIP**, e direciona a mídia real através de um ou mais **gateways de mídia**. O OmniWeb exibe os assinantes ativos do MSC, chamadas, transações de SMS, RAN e pares SIP, tabela de roteamento e páginas pendentes. Tendências de longo prazo estão nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

O MSC é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, e, onde vários estão implantados, uma visão de frota para status agregado. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do MSC, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status da API** do MSC e um resumo do que ele está lidando atualmente, incluindo **assinantes** registrados no VLR, **chamadas ativas**, transações de **SMS** em andamento, **conexões RAN** ativas e o estado dos **pares SIP** e links de sinalização **STP**. É a maneira mais rápida de confirmar que o MSC está ativo e ver, à primeira vista, sua carga ao vivo.

Assinantes

Cada assinante que o VLR atualmente mantém, cada linha identificada por **IMSI** e **MSISDN** com seu estado de registro e localização. Abra um assinante para mostrar seu contexto completo no VLR. A partir daqui, um operador pode:

- **Eliminar** um assinante do VLR para limpar um registro obsoleto ou preso, para que o assinante se registre novamente de forma limpa.
- Executar uma **ação de assinante** contra um assinante específico.
- Gerenciar **serviços suplementares**: inspecionar e alterar o encaminhamento de chamadas, bloqueios e serviços relacionados ativos para o assinante.
- Enviar **Aviso de Cobrança (AoC)** para o assinante.
- Enviar um **SMS silencioso (Tipo 0)** ou iniciar uma **chamada silenciosa**: uma sondagem de localização/acessibilidade que não alerta o dispositivo.

Chamadas

Cada chamada ativa, cada linha mostrando as partes **chamadoras** e **chamadas**, o **estado** da chamada e sua **duração**. Abra uma chamada para mostrar seu detalhe completo: as pernas, a conexão RAN servidora e o caminho da mídia. Um operador pode **forçar a liberação** de uma chamada para limpar uma chamada presa ou indesejada.

SMS

As transações de SMS que o MSC está atualmente lidando, cada uma mostrando o **originador**, **destinatário** e **estado de entrega**, para que você possa confirmar que as mensagens estão sendo transportadas e identificar aquelas que estão presas.

RAN

O lado rádio do MSC. Ele lista as **conexões RAN** ativas (as associações de interface A ao vivo que transportam sinalização de assinantes) e os **BSCs** conhecidos, aprendidos a partir das trocas RESET nos links SS7/M3UA. É aqui que você confirma que os controladores de estação base estão conectados e vê quais assinantes estão em qual conexão.

Pares SIP

Os pares SIP pelos quais o MSC transporta voz são o IMS, softswitches e troncos de interconexão, cada linha mostrando o **endereço** do par e seu **status** de acessibilidade. Abra um par para mostrar seu detalhe. Um operador pode **disparar um ping OPTIONS** em um par para testar ativamente a acessibilidade, que é a maneira mais rápida de provar que um caminho SIP está ativo quando as chamadas para ele estão falhando.

Gateways de Mídia

Os gateways de mídia pelos quais o MSC direciona os portadores de voz, cada linha mostrando o gateway e seu **status**, para que você possa confirmar que o plano de mídia está disponível para a configuração de chamadas.

Roteamento

A tabela de roteamento de números do MSC contém as regras que decidem, por prefixo de número discado, para onde uma chamada é enviada. Cada regra mostra seu **prefixo** e **destino**. Um operador pode:

- **Adicionar uma rota**: um novo prefixo e seu destino.
- **Remover uma rota** por prefixo.
- **Testar uma pesquisa de rota** para um número: insira um número e veja qual rota ele resolve, para confirmar planos de discagem antes ou depois de uma mudança.

Paginação

As solicitações de paginação pendentes são os assinantes que o MSC está atualmente tentando localizar na rede rádio para uma chamada ou SMS recebidos. Um operador também pode **pagar um assinante** diretamente daqui.

Logs

A aba **Logs** exibe a saída de log ao vivo do MSC para solucionar problemas de um único switch sem sair do OmniWeb.

Painéis de monitoramento

Taxas de chamadas, volumes de SMS, contagens de assinantes e outras séries temporais para o MSC são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **HSS** mantém os dados dos assinantes contra os quais o VLR resolve e onde o MSC se registra como o nó servidor.
- O **CSCF / IMS** é interconectado através dos **pares SIP** do MSC para voz.
- Os **BSCs** conectam-se no lado rádio através da interface A, transportados nos links de sinalização SS7/M3UA.

Teste de Rede (Teste de Carga)

Teste de Rede gera carga de sinalização sintética em um núcleo ao vivo para que você possa medir como ele se comporta sob estresse. É alimentado pelo RAN Simulator: eNodeBs e UEs virtuais que exercitam todo o caminho rádio→núcleo (S1AP/NAS, GTP-U, IMS) em vez de uma única interface.

← Guia de Operações

O grupo **Teste de Rede** na barra lateral coleta as ferramentas de teste de carga do RAN Simulator:

Sub-aba	O que faz
Teste de Carga RAN	Trabalhos recentes de teste de carga — anexos, sessões de dados e registros IMS executados contra o núcleo, com seus resultados e um pcap para download.
Agendas de Cenário	Defina execuções de cenário recorrentes (por exemplo, um lote de anexos a cada hora), execute uma agora e navegue pelo histórico de execuções. Os resultados são exportados para o Prometheus para alertas.
RAN Simulator	Configure eNodeBs/gNodeBs e UEs virtuais e dirija-os diretamente.
RAN Rádio	Controle de rádio Multi-RAT (5G NR / 2G GERAN / 3G UTRAN).
RANsimware — IMS	Registro IMS e carga VoLTE em toda a frota simulada.

Todos estes estão documentados em profundidade em **RAN Simulator**.

Apontando uma execução para um núcleo

Quando você ativa uma célula, o OmniWeb oferece um menu suspenso dos nós do núcleo que pode discar — cada **MME**, **AMF** e **STP** que encontra em seus inventários de site — para que você aponte a execução para o núcleo correto (`mme_ip` / `amf_ip` / `stp_ip`) em vez de digitar um IP. Sem inventário configurado, o campo volta a texto livre.

Uso Típico

1. Abra o **RAN Simulator**, ative um eNodeB/gNodeB e aponte-o para o núcleo para testar.
2. Anexe um lote de UEs e execute um cenário (anexo, dados, registro IMS, VoLTE ou um cenário de falha).
3. Observe os resultados e, para detalhes de sinalização, baixe o pcap da execução.
4. Para cobertura rotineira, salve o cenário como uma **Agenda de Cenário** para que ele seja executado em um intervalo e exporte sucesso/falha para o Prometheus.

Relacionados

- RAN Simulator: eNodeBs/UEs virtuais para testes funcionais e de carga em todo o caminho rádio→núcleo.
- Grafana Dashboards & Statistics: sucesso/falha do cenário e tempos são exportados para o Prometheus; use o Grafana para ter uma visão completa durante um teste.

OmniRoam: Acordos de Roaming & Automação de Email

O lado de **acordos** do OmniRoam transforma a papelada de configuração de um parceiro de roaming (os emails, os formulários AA.12/AA.13, as tarifas IOT, as trocas de SIM e o trabalho de provisionamento) em um único registro rastreado por parceiro. Ele automatiza as partes que costumavam ser copiadas e coladas. Seu truque principal: **encaminhe um email de parceiro para o OmniRoam e ele lê a conversa, extrai os fatos e atualiza o acordo para você**. Em seguida, gera e assina eletronicamente os contratos, arquiva-os e cria as ordens de trabalho para que o parceiro seja lançado.

← Voltar ao Guia de Operações

> **Dois "OmniRoam" diferentes.** Este documento é sobre o lado de **acordos / email / documentos** do OmniRoam (o ciclo de vida comercial e de provisionamento com um parceiro de roaming). Não é **a mesma coisa** que os **livros de teste de roaming** (IR.38 / IR.48 / testes de conformidade VoLTE). Esses são abordados separadamente em OmniRoam: Automação de Testes de Roaming. Um produto, dois trabalhos: *obter o acordo assinado* (aqui) e *provar que o roaming funciona* (lá).

Índice

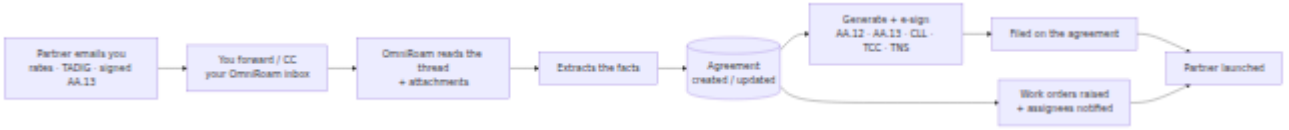
- A Grande Imagem
- 1. Ingestão de Email Inbound: "extraindo os dados"
- 2. Acordos & Parceiros
- 3. Geração Automática de Documentos & Assinatura
- 4. Arquivamento & Armazenamento
- 5. Ordens de Trabalho & Notificações de Atribuição
- O Ciclo de Vida Completo, de Ponta a Ponta

- O Que Você Configura Uma Vez

A Grande Imagem

Tudo no OmniRoam gira em torno de um registro: o **Acordo**, um por parceiro de roaming. Um acordo contém o nome do parceiro, país, TADIG(s)/PLMN, seu **status** de ciclo de vida, seus contatos, as **tarifas** comerciais acordadas, os SIMs trocados, os **documentos** gerados e recebidos, uma **linha do tempo** de atividades e as **ordens de trabalho** que tornam o parceiro ativo.

Você pode construir tudo isso manualmente na interface do usuário. Mas o ponto do OmniRoam é que a maior parte chega *por email*, e o OmniRoam arquiva isso para você.



O inquilino com o qual você está trabalhando é um **Operador** (sua própria rede, o lado "doméstico"). Tudo está escopado a isso: seu cabeçalho e signatário preenchem os documentos gerados, seu endereço de entrada impulsiona a automação de email, e suas equipes são os responsáveis pelas ordens de trabalho.

---

1. Ingestão de Email Inbound: "extraindo os dados"

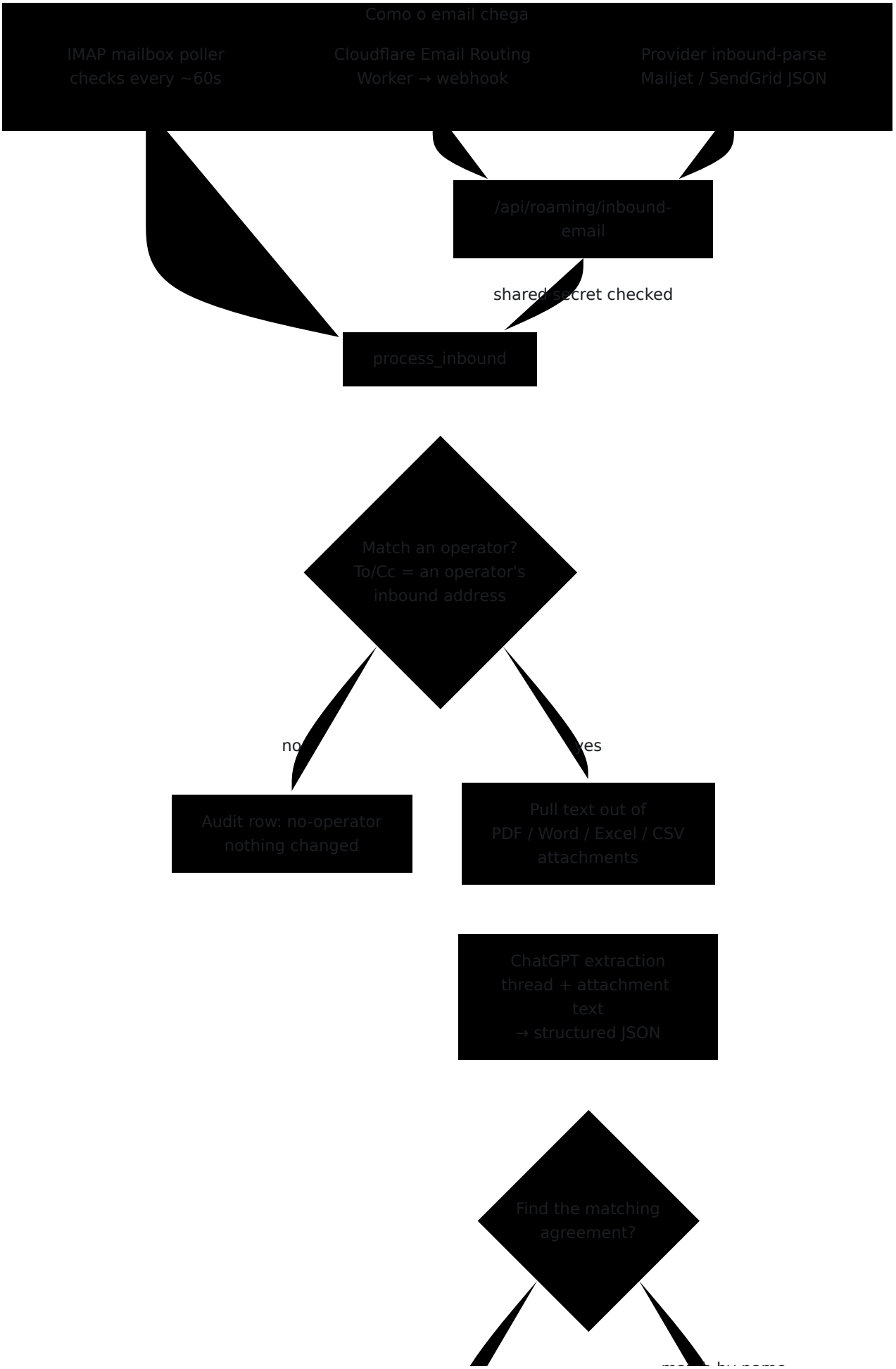
O que você faz

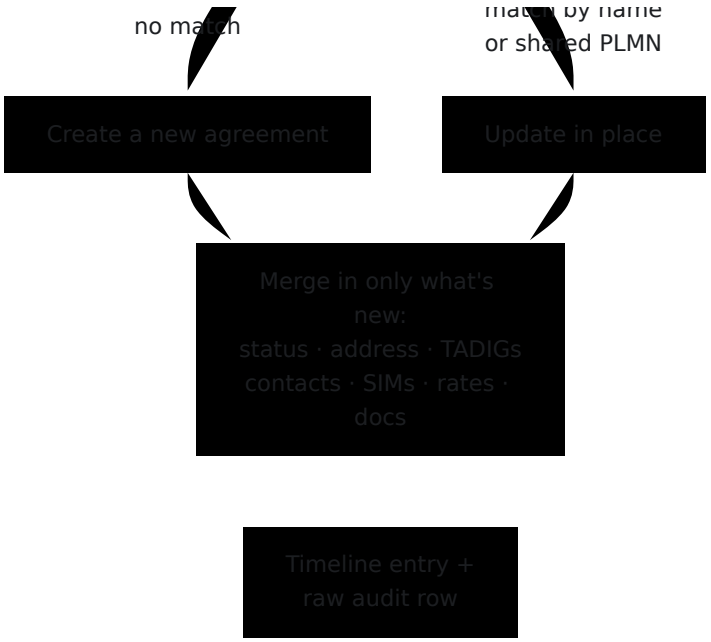
Negociar com um parceiro é uma conversa por email. Para trazê-la para o OmniRoam, você faz uma coisa: **encaminhe o email ou CC o endereço de entrada do OmniRoam na conversa**. É isso. Seu endereço de entrada dedicado (por exemplo, `roaming@seudominio`) é configurado uma vez por operador (Configurações → detalhes da papelada, `Email inbound`).

- **Encaminhe toda uma conversa** uma vez e o OmniRoam constrói o acordo a partir do histórico enterrado nas mensagens citadas.
- **CC o endereço em uma negociação em andamento** e cada novo email mantém o registro atualizado. O status avança, contatos e TADIGs são preenchidos, tarifas chegam e a papelada anexada é arquivada, email por email.

Você nunca preenche um formulário para fazer isso. O email *é* a entrada.

O que o OmniRoam faz


Como o email chega
IMAP mailbox poller
checks every ~60s
Cloudflare Email Routing
Worker → webhook
Provider inbound-parse
Mailjet / SendGrid JSON
/api/roaming/inbound-email
shared secret checked
process_inbound
Match an operator?
To/Cc = an operator's inbound address
no
yes
Audit row: no-operator
nothing changed
Pull text out of
PDF / Word / Excel / CSV
attachments
ChatGPT extraction
thread + attachment text
→ structured JSON
Find the matching agreement?



Passo a passo, uma vez que um email chega ao OmniRoam:

1. **Ele descobre para qual operador (inquilino) o email é** correspondendo um endereço To/Cc ao endereço de entrada configurado de um operador. Se nada corresponder, o email é registrado como `no-operator` e *nada é alterado*: uma operação segura.
2. **Ele lê os anexos, não apenas o corpo.** As tarifas acordadas ou os termos assinados estão frequentemente dentro de um **AA.13** anexado, uma **planilha de tarifas IOT** ou uma planilha. Portanto, o OmniRoam extrai o texto de anexos PDF, Word, Excel e CSV e alimenta isso para o extrator também. Logotipos de bloco de assinatura (PNG/JPG) são ignorados.
3. **Ele extrai os fatos** usando a API ChatGPT. O extrator é especificamente informado de que o remetente externo geralmente está apenas *encaminhando* a conversa (frequentemente seu próprio gerente de roaming) e deve ler o **todo o histórico citado**. Ele atribui tarifas, contatos, endereços e SIMs a quem realmente os declarou, nunca ao encaminhador. Retorna um registro estruturado: nome do parceiro, país, endereço, TADIG(s)/PLMN, status de ciclo de vida mais adequado, tarifas acordadas (somente se *ambas* as partes concordaram explicitamente), contatos do parceiro, SIMs trocados/solicitados, se um acordo assinado está anexado e um resumo de uma linha.
4. **Ele encontra o acordo certo ou cria um.** A correspondência é deliberadamente tolerante para que uma conversa nunca gere um

duplicado: nome exato do parceiro, depois uma correspondência de "nome normalizado" (então *AT&T Mobility* se junta a *AT&T*), depois uma correspondência de **PLMN compartilhado** (MCC+MNC). Este é um sinal de alta precisão, uma vez que um PLMN identifica exclusivamente uma rede. Sem correspondência → um novo acordo.

5. **Ele mescla apenas o que é novo.** Para acordos novos e existentes, o OmniRoam aplica o que *este* email revela de novo e **nunca sobrescreve** valores existentes:
   - **Status** só avança *para frente* ao longo do ciclo de vida (nunca para trás).
   - **País / endereço** são definidos se em branco ou alterados.
   - **TADIGs** adicionados, mas apenas códigos que existem no catálogo IR.21 (portanto, a IA não pode inventar um), e nunca os códigos da sua própria rede doméstica.
   - **Contatos** adicionados ou existentes *enriquecidos* (campos em branco preenchidos).
   - **SIMs** registrados (test SIMs que o parceiro compartilhou) e **solicitações de SIM** (lotes que alguém pediu para serem enviados para um endereço).
   - **Tarifas acordadas** tornam-se um nível de tarifa, somente quando ambas as partes concordaram explicitamente, e nunca um duplicado de um nível existente.
   - Um **AA.12/AA.13 assinado** (anexado ou declarado no email) avança o status para *IRA Assinado*.
6. **Ele escreve dois registros.** Uma amigável **entrada de log de atividade** na linha do tempo do acordo ("Email de *Jane no Parceiro* (encaminhado): tarifa de dados acordada; status → rates_agreed, contato Jane adicionado, tarifas acordadas registradas"), e uma **linha de auditoria inbound** bruta (veja abaixo).

O processamento é **idempotente**: o mesmo email (por Message-ID) é processado apenas uma vez, portanto, CC'ing várias pessoas ou reencaminhar uma conversa nunca conta duas vezes.

Três maneiras de o email entrar

Você só precisa de uma. Todas as três acabam chamando a mesma lógica de processamento:

Caminho	Como funciona	Quando usá-lo
Cloudflare Email Worker	O Cloudflare Email Routing encaminha a mensagem bruta para um pequeno Worker que transmite o `.eml` diretamente para o webhook do OmniRoam.	Domínios que já usam Cloudflare; sem caixa de correio para verificar.
IMAP poller	O OmniRoam faz login em uma caixa de correio real a cada ~60 s, processa mensagens não lidas e as marca como lidas.	Qualquer caixa de correio padrão (TLS implícito, STARTTLS ou simples).
Provider inbound-parse	Um provedor de email (Mailjet/SendGrid) POSTs a mensagem analisada + anexos para o webhook.	Se você já executa inbound-parse.

O webhook (`/api/roaming/inbound-email`) é protegido por um **segredo compartilhado**, portanto, apenas seu caminho de email configurado pode postar nele.

O Log de Email Inbound: seu registro de auditoria

Cada email processado, sucesso *ou* falha, escreve uma linha no **Log de Email Inbound** (na interface do usuário sob a visualização de Emails do operador). Cada linha mostra o remetente, destinatários, assunto, anexos, se a **extração de IA foi bem-sucedida**, exatamente o que foi extraído e o que o email **mudou** (ou por que não fez nada: `no-operator`, `no-partner`). Esta é sua janela para a automação: se uma tarifa não foi capturada, o log informa o que o extrator realmente viu.

O Log de Email Inbound: uma linha por email processado, com o resultado da extração e as mudanças que fez. Este é o registro de auditoria para toda a automação de email→acordo.

---

2. Acordos & Parceiros

A lista de **Acordos** é seu livro de parceiros de roaming para o operador atual. Cada linha é um parceiro, com seu **status** de ciclo de vida, TADIG/país, prioridade e em quem a próxima ação está aguardando ("Nós" ou "Eles").

Lista de Acordos. Os status vão da esquerda para a direita ao longo do ciclo de vida; a barra de filtro estreita por status. Você cria acordos aqui manualmente, ou eles chegam automaticamente de um email inbound.

O ciclo de vida (status)

Um acordo avança através dessas etapas. A automação de email só avança o status, então o registro reflete o ponto mais avançado que a conversa alcançou:

`Consultado → Negociação IOT → IOT Pendente de Assinatura → Negociação IRA → Aguardando Assinaturas IRA → IRA Assinado → Tarifas Acordadas → Troca de SIM → Testes → Lançado` (mais `Lançamento Padrão`, `Suspenso`, `Terminado`).

Abrindo um parceiro

Clique em um parceiro para abrir sua página de **detalhes**: um conjunto de abas/seções cobrindo tudo sobre o relacionamento:

- **Visão geral & linha do tempo**: status, prioridade, notas e o log de atividades (cada email, documento gerado, assinatura e nota manual em ordem de data).
- **TADIGs**: os códigos de rede do parceiro (com MCC/MNC, tipo de conexão e direção). Uma ação de **"encontrar candidatos"** pode puxar os outros TADIGs do operador parceiro do catálogo IR.21 para você revisar e adicionar.
- **Contatos**: pessoas de roaming/comerciais/técnicas no parceiro.
- **Tarifas**: os níveis de tarifas comerciais acordadas (dados/SMS/vídeo, moeda, unidade).
- **SIMs & Solicitações de SIM**: SIMs de teste trocados e lotes solicitados para envio.
- **Documentos**: papelada gerada e recebida (veja abaixo).
- **Roteamento**: rotas DRA, títulos globais SS7, DNS e faixas de IP para provisionamento (muito disso é pré-preenchido a partir do IR.21 do parceiro).

Tudo na página de detalhes é **editável**. A automação lhe dá um bom começo, e você corrige ou adiciona manualmente conforme necessário.

O catálogo IR.21

As consultas TADIG utilizam um **catálogo global de operadores IR.21** indexado por TADIG (organização, rede, MCC/MNC, DNS, faixas de IP, nós SS7, contatos). É assim que o OmniRoam valida um TADIG que a IA extraiu, descobre os TADIGs irmãos de um parceiro e pré-preenche os dados de roteamento.

---

3. Geração Automática de Documentos & Assinatura

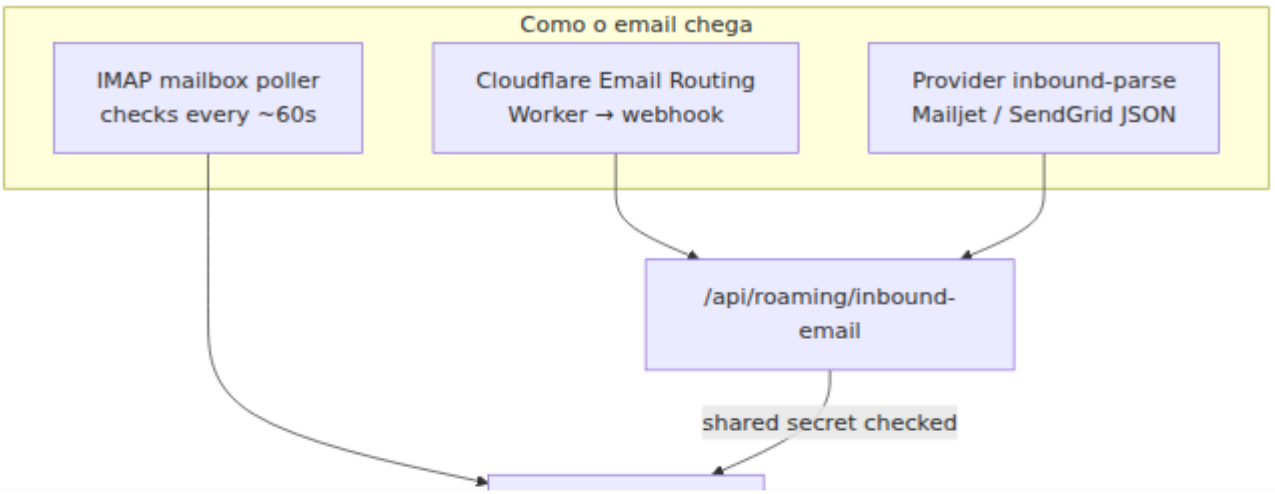
Gerando um documento

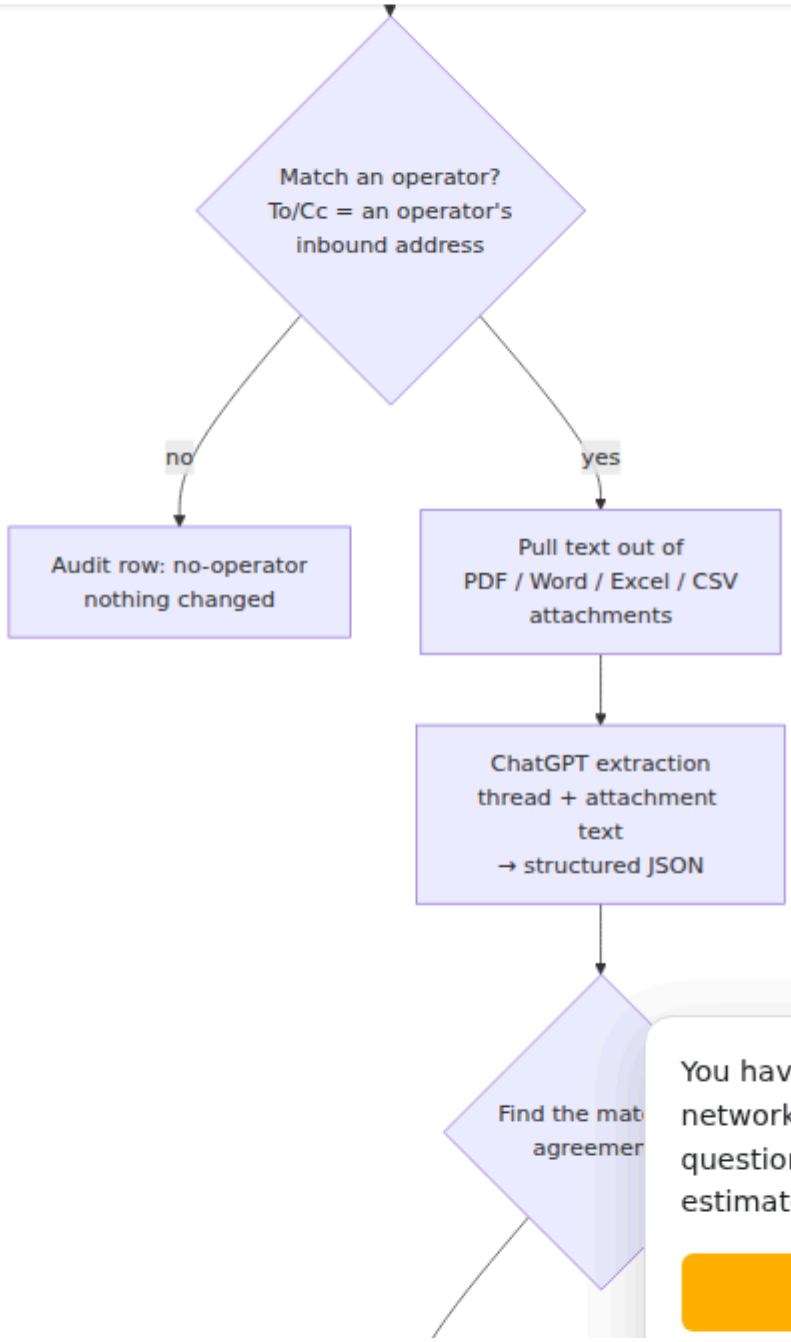
Na seção **Documentos** de um acordo, você escolhe um tipo de documento e clica em **Gerar**. O OmniRoam renderiza o verdadeiro formulário Word, preenchido com os detalhes de ambos os lados, pronto para assinatura:

Tipo	O que é	Formato
AA.12	Acordo de roaming GSMA AA.12 IREG (o formulário real, ambos os lados pré-preenchidos)	.docx / PDF
AA.13	Anexos comuns GSMA AA.13, incluindo o anexo de faturamento/ajuste (veja opções de ajuste AA.13)	.docx / PDF
CLL	Carta de Lançamento Comercial (genérica)	.docx / PDF
CLL (Bilateral / Unilateral, após testes)	Carta de lançamento confirmando a data de início **após testes bem-sucedidos de IREG & TADIG**	.docx / PDF
CLL (Bilateral / Unilateral, padrão)	Carta de lançamento para um lançamento **por padrão, sem completar os testes de IREG/TADIG**	.docx / PDF
TCC (VoLTE)	Conclusão de Chamada de Teste VoLTE	.docx / PDF
Conclusão TADIG	Formulário de conclusão TADIG	.docx / PDF
Formulário de Acordo de Roaming TNS	Solicitação de clearing-house TNS (entregue como legado .doc)	.doc
Solicitação TNS 3G-4G	Solicitação de clearing-house TNS	.docx

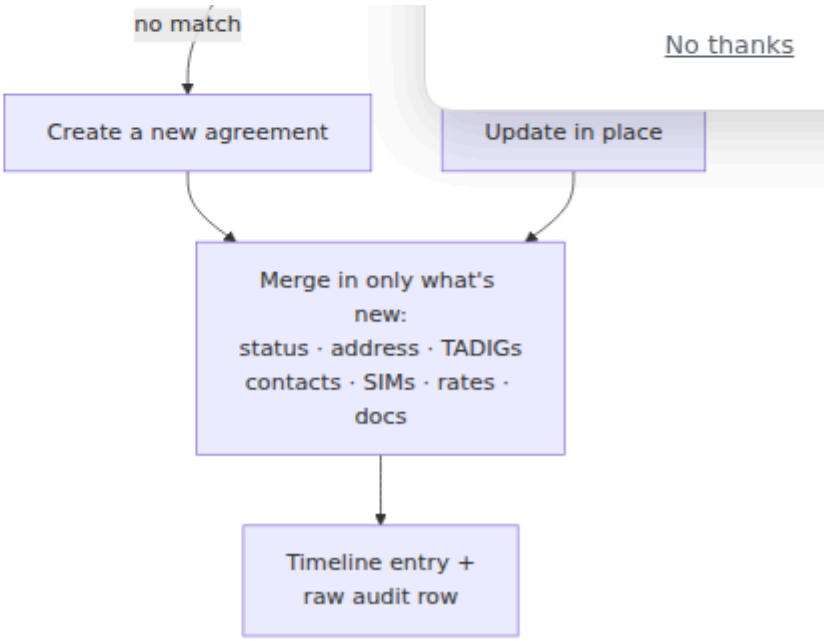
Como os campos são preenchidos. Cada documento é um modelo Word com espaços reservados (docxtpl / Jinja). O OmniRoam os preenche a partir de:

- **O lado doméstico**: do seu registro de **Operador**: seu nome, nome legal, TADIG, PLMN, país, **signatário & título**, local e endereço. Como isso vem do inquilino, cada operador hospedado recebe seu *próprio* cabeçalho e signatário automaticamente.
- **O lado do parceiro**: do **Acordo**: nome do parceiro, sua abreviação de forma curta usada no corpo do contrato, TADIG(s), PLMN(s), país e endereço. O signatário/título do parceiro fica em branco por padrão, para que essa linha fique pronta para eles assinarem.
- **Valores derivados**: data efetiva, direção (bilateral/inbound/outbound), empresa hub, domínios Diameter, moeda e a tarifa IOT confirmada.





You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima



Formato de saída: Word por padrão, PDF para assinatura

A geração produz um **.docx** Word **editável** por padrão. Essa é a cópia de trabalho que você revisa e edita manualmente, se necessário. Você recebe um PDF somente quando realmente precisa de uma renderização fixa e final:

- Marque a caixa de **saída PDF** antes de clicar em Gerar para renderizar um PDF em vez do `.docx`.
- O fluxo de **assinatura eletrônica** sempre usa PDF (o artefato assinado não deve mudar).
- **Baixe / visualize** um documento arquivado *como PDF* sob demanda.

Um email de **Pacote de Roaming** anexa o AA.12/AA.13 como um `.docx` editável para que o parceiro possa revisar e comentar. Não é a etapa de assinatura, portanto, não é enviado como PDF.

Opções de ajuste AA.13 (Anexo C.3.2)

O Anexo C.3.2 do GSMA AA.13 (faturamento e ajuste) é um **menu de escolhas** que cada parceiro negocia: qual modelo de fatura, qual método de pagamento, o limite e o período de ajuste, termos de pagamento e juros. Em vez de travar um conjunto de escolhas no modelo, o OmniRoam os expõe como um painel de opções de ajuste na seção **Documentos**: expanda **opções de ajuste AA.13**, defina os valores para este parceiro e clique em **Gerar AA.13**. O anexo gerado

contém apenas as opções que você escolheu. As alternativas (e a estrutura "GSMA delete those which do not apply") são descartadas automaticamente.

Cada campo tem um padrão sensato, então gerar sem tocar no painel resulta nos termos padrão; mude apenas o que difere para um determinado parceiro.

Opção	Padrão	Descrição
Tipo de fatura	Fatura de rede única (SNI)	Seleciona o anexo de ajuste: **Rede única (SNI)** → Anexo C.3.2 H, ou **Rede múltipla (MNI)** → Anexo C.3.2 I. O anexo n��o utilizado é removido.
Método de pagamento	Ajuste líquido	O mecanismo de ajuste: **Ajuste líquido**, **Pagamento direto total (sem conversão)**, **Pagamento direto total (com conversão)**, ou **Liquidação sem conversão**. Somente a cláusula do método escolhido é mantida.
Limite de ajuste	Opção 1 (Liquidação)	**Opção 1 (Liquidação)** aplica um único limite de saldo baixo acordado; **Opção 2 (Pagamento direto)** utiliza limites por parte (Parte A / Parte B).
Limite	50	Montante do limite de saldo baixo, na moeda de ajuste do acordo (por exemplo, SDR). Abaixo deste total mensal, o ajuste pode ser adiado.
Início do período / **Fim do período**	Janeiro / Dezembro	O período não de ajuste para saldos abaixo do limite, tipicamente o ano financeiro.
Dias de pagamento	60	Dias a partir da data da fatura dentro dos quais o devedor deve pagar.
Juros domésticos %	8	Juros anuais que o credor pode cobrar sobre saldos em atraso quando o operador **doméstico** é o credor.

Opção	Padrão	Descrição
Juros do parceiro %	8	Juros anuais quando o operador **parceiro** é o credor.
Enviar faturas de valor zero	Desligado	Quando desligado, o anexo afirma que cada parte **não enviará** faturas mensais com um valor zero (0,00).
BCE na fatura TAP	Desligado	Quando desligado, o anexo afirma que o uso de BCE **não será** incluído na Fatura de Roaming TAP.

Como funciona. As escolhas são passadas para a geração como substituições sobre os padrões embutidos. O modelo AA.13 resolve-as no anexo final: seleciona os blocos de opção corretos, preenche os montantes/períodos/tarifas e formula os alternadores. A própria moeda de ajuste vem da moeda configurada do acordo, não deste painel.

Caso de uso. Um parceiro insiste em termos de 90 dias, um limite de 100 SDR e um ano financeiro de abril a março: abra o painel, defina **Dias de pagamento** 90, **Limite** 100, **Início do período** abril, **Fim do período** março e gere. Cada outra cláusula permanece nos termos padrão.

> **Os formulários de clearing-house TNS são especiais.** Os dois pedidos TNS *não* são modelos docxtpl. Eles são os genuínos formulários TNS do operador com apenas os campos preenchíveis alterados e as caixas de seleção corretas marcadas, para que o TNS receba exatamente o layout que espera. Eles são **bloqueados por IOT**: o OmniRoam não os gera até que o acordo tenha uma **tarifa confirmada (acordada)**. Tentar antes retorna uma mensagem clara "é necessário um IOT confirmado". Os estados das caixas de seleção (tipo de acordo, direção, serviços, interfaces LTE, GRX) são derivados automaticamente do acordo, e todos os campos são substituíveis no momento da geração.

O LibreOffice sem cabeça no servidor faz a geração de PDFs (e o legado `.doc` para TNS). Você apenas recebe o arquivo final.

Seção Documentos de um acordo. Gere um contrato à esquerda; documentos gerados e recebidos (com status de assinatura) listados abaixo, cada um baixável.

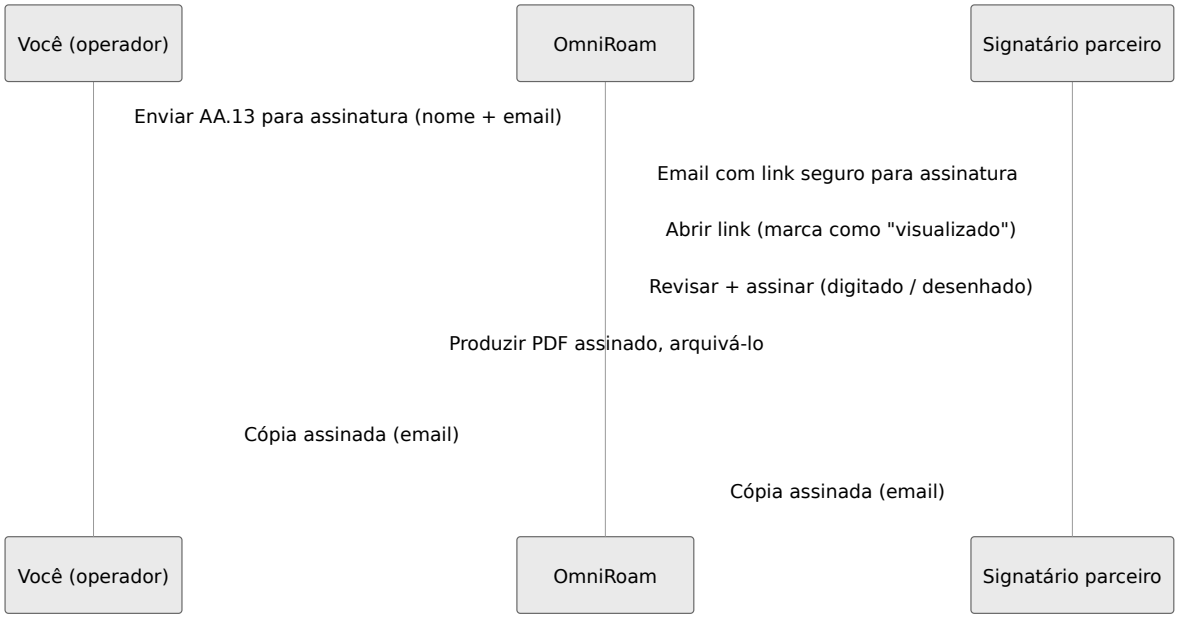
Assinatura: online ou offline

O OmniRoam suporta duas rotas de assinatura:

Assinatura eletrônica online (o parceiro assina no navegador, sem login). A partir de um AA.12/AA.13 gerado, você clica em **Enviar para assinatura**, nomeia o signatário e seu email, e o OmniRoam:

1. Cria um pedido de assinatura com um token opaco e envia um **link seguro** por email ao parceiro (sem necessidade de conta).
2. Quando eles o abrem, o OmniRoam marca o pedido como *visualizado* e o registra na linha do tempo. Eles revisam o documento, opcionalmente corrigem seu nome/título/empresa de signatário e **assinam** digitando seu nome e/ou desenhando uma assinatura.
3. O OmniRoam produz o **PDF assinado** e o envia por email para **ambas as partes** (signatário + caixa de retorno do seu operador), arquiva-o no acordo e registra "Assinado por … em …".

4. O parceiro também pode **recusar** (com um motivo), o que também é registrado.



Assinatura offline. Prefere assinar da maneira antiga? Baixe o documento gerado, assine-o externamente e faça o upload da cópia assinada de volta ao acordo. Um nome de arquivo contendo *assinado*/*executado*/*contrassinado* é reconhecido como uma cópia assinada. Um email inbound que anexa um avança o status para *IRA Assinado* automaticamente.

O Pacote de Roaming: primeiro contato com um clique

Em vez de gerar cada formulário separadamente, **Enviar pacote de roaming** envia a um contato parceiro o **AA.12 + AA.13 + oferta IOT** juntos em uma única mensagem. Ele gera os contratos como PDFs instantaneamente e anexa sua oferta IOT mais recente. Escolha um contato (ou digite um nome + email, que é preenchido como um contato) e o OmniRoam envia o pacote com a redação do seu modelo salvo. Este é o email de abertura "vamos fazer um acordo de roaming", enviado de dentro do OmniRoam.

Modelos de email editáveis

Os três emails automatizados (**pedido de assinatura**, **cópia assinada** e **pacote de roaming**) usam modelos editáveis (substituição por operador, senão um padrão global), com espaços reservados como `{{ signer_name }}`,

`{{ partner }}`, `{{ operator }}`, `{{ sign_url }}` e `{{ document_name }}`. Ajuste a redação uma vez nas Configurações e cada envio a utiliza.

> **Como o email realmente sai do OmniRoam.** Todo email de saída vai via a **Mailjet HTTPS Send API**, não SMTP. Plataformas de hospedagem (Railway) bloqueiam portas SMTP de saída, então o OmniRoam POSTs para o Mailjet via HTTPS. Os envios são **de melhor esforço e não bloqueantes**: o botão da interface do usuário retorna imediatamente e o email é enviado em uma thread de fundo, então um servidor de email lento nunca trava o aplicativo.

---

4. Arquivamento & Armazenamento

Cada documento é arquivado **diretamente no acordo** ao qual pertence. Isso cobre documentos **gerados** (AA.12, AA.13, CLL, TCC, TNS…) e documentos **recebidos** (uma cópia assinada anexada a um email, um IR.21 enviado, uma planilha IOT). Não há um armazenamento de documentos separado para gerenciar:

- Os documentos são armazenados como blobs **no banco de dados**, marcados com um **tipo** (`aa12`, `aa13`, `aa12_signed`, `iot`, `ir21`, `cll`, `outro`, …), nome do arquivo, tipo de conteúdo, tamanho e se o OmniRoam **gerou**.
- Cópias assinadas são marcadas distintamente (por exemplo, `aa12_signed`) para que o conjunto assinado seja sempre distinguível de rascunhos.
- **Anexos inbound são deduplicados**: uma cópia idêntica (mesmo nome de arquivo + comprimento de byte) que chega novamente não é re-arquivada.
- Cada geração, upload, assinatura e exportação IOT escreve uma **entrada de linha do tempo**, então o log de atividades do acordo é uma trilha de papel completa do que foi produzido e recebido, e quando.

Para recuperar um documento, abra a seção **Documentos** do acordo e faça o download (Word/PDF gerado ou o original recebido). PDFs assinados produzidos

pelo fluxo de assinatura online são armazenados na solicitação de assinatura e também enviados por email para ambas as partes.

Você também pode **exportar a tarifa acordada como um arquivo XML GSMA RAEX IOT 5.0** do acordo. Esta é a mesma seleção de tarifas que os formulários TNS usam, então o IOT exportado e os formulários gerados sempre concordam.

---

5. Ordens de Trabalho & Notificações de Atribuição

Tornar um parceiro ativo é *trabalho*: envio de SIMs, alteração de roteamento, execução de testes IREG/TADIG, auditorias, resolução de problemas. No OmniRoam, esse trabalho é rastreado como **Ordens de Trabalho**: a única unidade rastreada de trabalho de roaming. Uma ordem de trabalho pode estar vinculada a um acordo (um parceiro) ou ser independente.

Visualização de Ordens de Trabalho. Cada ordem tem um tipo, prioridade, status, link opcional para parceiro e um responsável: a parte notificada quando

é atribuída.

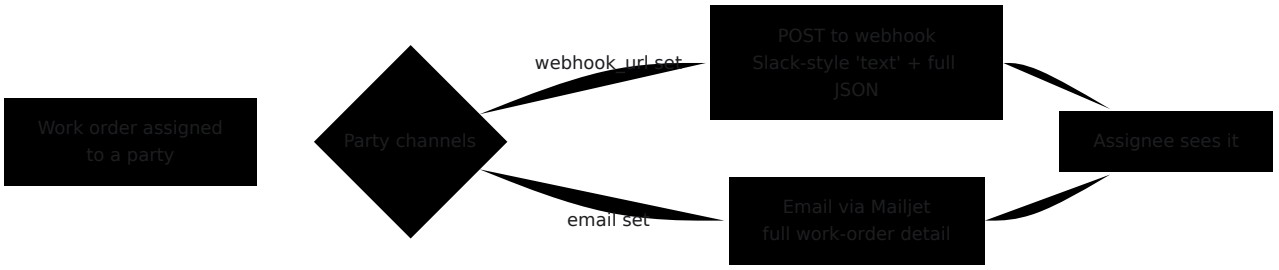
Criando e atribuindo

Uma ordem de trabalho tem um **tipo** (Envio de SIM, Roteamento, Teste IREG, Teste TADIG, Auditoria, Questão), um título, prioridade, status (Aberta / Em Progresso / Bloqueada / Concluída / Cancelada), um link opcional para parceiro (acordo), detalhes em texto livre, uma data de vencimento e campos estruturados específicos do tipo (por exemplo, um Envio de SIM contém quantidade, endereço postal, transportadora e rastreamento).

Você atribui uma ordem de trabalho a uma **parte**: uma equipe interna nomeada ou contato externo (por exemplo, "Roaming NOC", "admin TADIG") gerenciada por operador em **Configurações**. Você pode definir um **responsável padrão por tipo de ordem de trabalho**, então um novo Envio de SIM é automaticamente atribuído a quem lida com o envio, a menos que você o substitua.

A notificação: webhook + email

Quando uma ordem de trabalho é **atribuída** (criada com um responsável ou reatribuída a uma nova parte), o OmniRoam **notifica esse responsável** através de quaisquer canais que a parte tenha configurado:



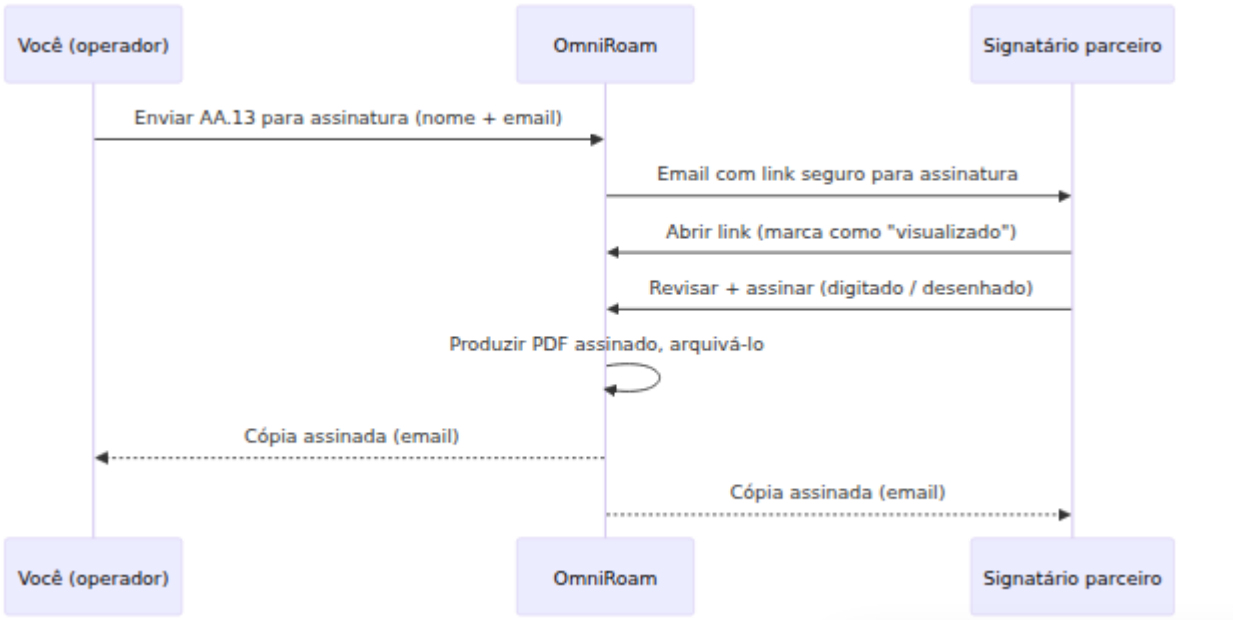
- **Webhook**: se a parte tiver uma URL de webhook (por exemplo, um **webhook de entrada do Slack**), o OmniRoam POSTs uma mensagem com um bloco `text` legível por humanos *e* a ordem de trabalho completa como JSON estruturado (tipo, prioridade, status, parceiro, carga útil específica do tipo, um link de volta para a página de Ordens de Trabalho).
- **Email**: se a parte tiver um endereço de email, o OmniRoam envia os mesmos detalhes por email (via Mailjet), assunto `[Ordem de Trabalho] <título> atribuída a você`.

Uma parte com **nenhum** canal configurado é simplesmente um responsável silencioso (sem operação). Ambas as notificações são de melhor esforço e não bloqueantes, portanto, um webhook lento ou servidor de email nunca pode travar o aplicativo. A reatribuição notifica apenas quando o responsável realmente **muda** para uma nova parte (portanto, editar outros campos não re-notifica as pessoas).

> **Da cadeira do responsável:** você recebe uma mensagem no Slack (ou email) no momento em que um trabalho chega à sua equipe, com tudo que você precisa: o que fazer, para qual parceiro, a contagem de SIM e endereço de envio (ou a alteração de roteamento, ou o escopo do teste), a prioridade e a data de vencimento, e um link direto para a ordem de trabalho.

O Ciclo de Vida Completo, de Ponta a Ponta

Colocando tudo junto, esta é a jornada de "um parceiro nos enviou um email" para "o parceiro está ativo":



Em cada etapa, a **linha do tempo** do acordo registra o que aconteceu, e o **log de email inbound** mantém a evidência bruta do que cada email contribuiu.

O Que Você Configura Uma Vez

A maior parte da automação só precisa de uma pequena configuração única por operador (em **Configurações**):

Configuração	Por quê	Onde é usada
Detalhes da papelada (nome legal, TADIG, PLMN, país, **signatário & título**, local, endereço)	Preenche o lado doméstico de cada documento gerado	Geração de documentos
Email inbound	O endereço para o qual você encaminha/CC o email do parceiro	Ingestão de email
Caixa de correio de retorno assinada	Para onde vão os emails de cópias assinadas e assinadas offline	Assinatura
Modelos de email (pedido de assinatura, cópia assinada, pacote de roaming)	Sua redação para os emails automatizados	Email de saída
Partes da ordem de trabalho + responsáveis padrão por tipo	Quem é notificado para cada tipo de trabalho	Ordens de trabalho

Com isso em vigor, encaminhar um email de parceiro realmente se torna: *email entra → acordo sai → contratos gerados e assinados → ordens de trabalho levantadas e sua equipe notificada.*

Veja Também

- OmniRoam: Automação de Testes de Roaming: o *outro* OmniRoam. Ele executa os livros de teste de roaming GSMA (IR.38 / IR.48 / VoLTE) contra uma rede ao vivo. Isso é complementar: assine o acordo aqui, prove que funciona lá.
- Operações Comuns: os padrões de visualização/edição compartilhados em toda a OmniWeb.

OmniRoam: Automação de Testes de Roaming

OmniRoam é o recurso de automação de livros de testes de roaming do OmniWeb. Ele executa os livros de testes de conformidade de roaming da GSMA contra uma rede ao vivo. Ele aciona os casos de teste individuais automaticamente a partir de um dispositivo de teste. Ele registra um veredicto de aprovação/reprovação com evidências de suporte para cada caso. Em seguida, produz um workbook de teste da GSMA completo, pronto para ser enviado a um parceiro ou hub de roaming.

Em resumo: o OmniRoam transforma um exercício manual de conformidade de roaming de várias horas em um pressionar de botão (ou um trabalho agendado). Ele devolve a mesma planilha oficial da GSMA que um testador preencheria manualmente.

> **OmniRoam tem dois lados.** Este documento cobre os **livros de testes de roaming** (IR.38 / IR.48 / testes de conformidade VoLTE: *o roaming realmente funciona?*). O outro lado é a **automação de acordos de roaming e e-mails**. Ele transforma um e-mail de parceiro em um acordo assinado, gerando a documentação AA.12/AA.13/CLL/TCC/TNS e as ordens de trabalho para colocar o parceiro em operação. Isso está documentado separadamente em **Acordos de Roaming & Automação de E-mail**. Um produto, dois trabalhos: *fazer o acordo ser assinado* (lá) e *provar que o roaming funciona* (aqui).

A tela dos Livros de Testes de Roaming. Cada linha é um livro executado contra um parceiro de roaming, com seu status atual.

Links Rápidos

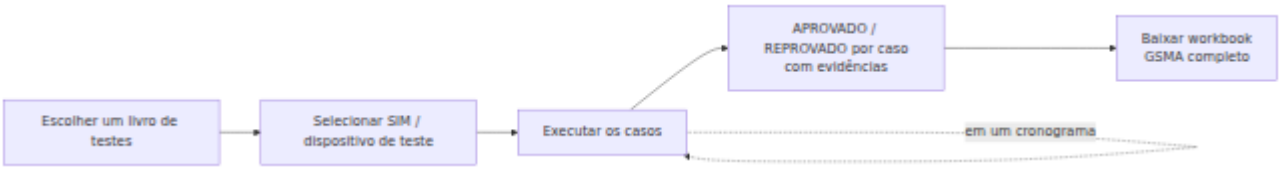
- **Livros de Testes**: os livros disponíveis (IR.38, IR.48, VoLTE) e cada caso de teste que eles contêm
- **Executando Testes**: como criar um livro, executá-lo, personalizar o conjunto de casos e agendar execuções rotineiras
- **Explorador de Livros de Testes**: como inspecionar o que cada livro testa e como cada caso é acionado
- **Documentos de Teste-Book Completos**: como o OmniRoam gera o workbook da GSMA preenchido
- **Acordos de Roaming & Automação de E-mail**: o *outro* lado do OmniRoam. Encaminhe um e-mail de parceiro → acordo criado, contratos gerados e assinados eletronicamente, arquivados e ordens de trabalho levantadas

O Que o OmniRoam Faz

Um livro de testes de roaming é uma lista de verificação definida pela GSMA: uma lista de casos de teste que provam que um assinante de uma rede (o **Home PLMN**, "PLMN(a)") recebe os serviços esperados enquanto está em roaming em outra rede (o **Visited PLMN**, "PLMN(b)"). Historicamente, cada caso é realizado manualmente e o resultado é escrito em uma planilha.

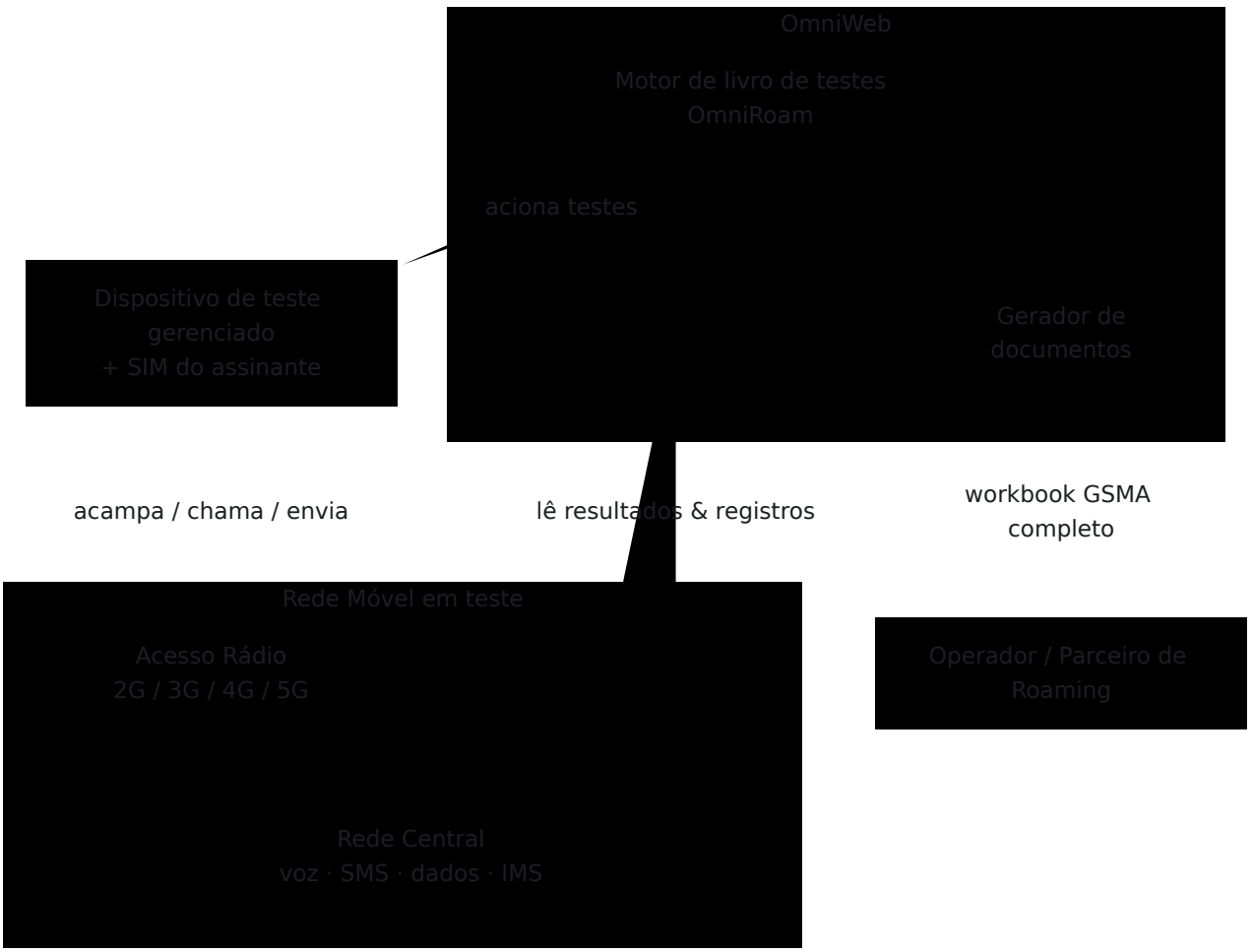
O OmniRoam automatiza três coisas:

1. **Acionando o teste**: ele faz a chamada, envia o SMS, executa a sessão de dados ou provisiona o serviço suplementar em um dispositivo de teste.
2. **Julgando o resultado**: ele compara o que aconteceu com o resultado esperado da GSMA. Ele registra **APROVADO**, **REPROVADO** ou **NÃO REALIZADO**, com as evidências de suporte (tempos, taxa de transferência, causas de liberação da rede, e assim por diante).
3. **Produzindo o documento**: ele preenche o workbook oficial da GSMA com os resultados e todos os metadados circundantes (identidades, datas, detalhes do testador).



Onde Se Encaixa

O OmniRoam exerce um assinante real na rede real usando um dispositivo de teste gerenciado. Cada caso automatizado aciona o dispositivo, depois lê o resultado de volta do dispositivo e, quando aplicável, dos próprios registros da rede (por exemplo, os registros de cobrança do gateway de serviço para uma sessão de dados). Nada é simulado: uma chamada que é relatada como conectada realmente se conectou.


OmniWeb
Motor de livro de testes
OmniRoam
aciona testes
Dispositivo de teste
gerenciado
+ SIM do assinante
Gerador de
documentos
acampa / chama / envia
lê resultados & registros
workbook GSMA
completo
Rede Móvel em teste
Acesso Rádio
2G / 3G / 4G / 5G
Rede Central
voz · SMS · dados · IMS
Operador / Parceiro de
Roaming

Conceitos Chave

Termo	Significado
Livro de testes	Um conjunto de casos de teste definido pela GSMA (por exemplo, IR.38, IR.48, VoLTE). Veja Livros de Testes.
Caso de teste	Uma verificação única dentro de um livro, identificada pelo seu número GSMA (por exemplo, caso IR.48 `2.3`, "Proibição de Todas as Chamadas de Saída").
Execução	Uma execução de um livro (ou um subconjunto escolhido de seus casos) contra um dispositivo e SIM.
Veredicto	O resultado registrado de um caso: `APROVADO`, `REPROVADO` ou `NÃO REALIZADO`.
Evidência	O detalhe de suporte capturado para um veredicto: tempos, números de taxa de transferência, causas da rede, leituras de interrogação, etc.
Home PLMN (a)	A rede que possui o assinante sendo testado.
Visited PLMN (b)	A rede na qual o assinante está em roaming.

Casos Automatizados vs. Manuais

A maioria dos casos em cada livro é **auto-acionada**: o OmniRoam os executa de ponta a ponta e registra o veredicto sem interação do operador. Alguns casos dependem de condições da rede que você não pode induzir apenas a partir de um dispositivo de teste (por exemplo, os testes negativos opcionais de CAMEL pré-pagos, ou a entrega de mensagens multimídia). Estes permanecem **manuais**. O OmniRoam ainda os lista no livro e o operador

registra o resultado manualmente, para que o documento final esteja completo.

O Explorador de Livros de Testes mostra exatamente quais casos em um livro são automatizados e como cada um é acionado.

Normas Referenciadas

O OmniRoam segue os Documentos de Referência Permanentes da GSMA e as especificações subjacentes da 3GPP:

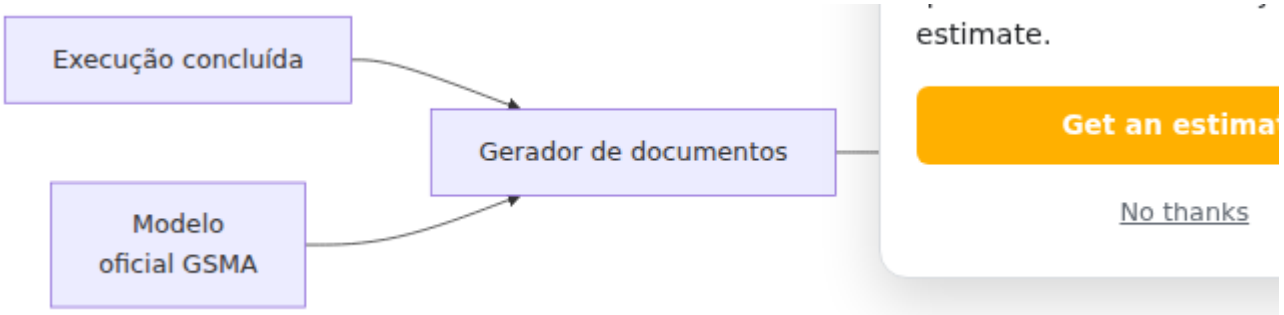
Referência	Aplica-se a
GSMA IR.38	Livro de testes de dados de roaming LTE
GSMA IR.48 / IR.24	Livro de testes de roaming bilateral (voz / SMS / MMS / dados)
GSMA BA.65	Testes de Roaming VoLTE
GSMA IR.92	Perfil IMS para voz e SMS (comportamento VoLTE)
GSMA IR.88	Diretrizes de roaming LTE (causas de rejeição de anexação)
3GPP TS 22.011	Acessibilidade do serviço (proibição determinada pelo operador)
3GPP TS 23.011	Status do serviço suplementar (Ativo/Registrado/Provisionado/Quiescente)
3GPP TS 22.082	Serviços suplementares de Encaminhamento de Chamadas
3GPP TS 22.088	Serviços suplementares de Proibição de Chamadas

Documentos de Teste-Book Concluídos

O produto final de uma execução do OmniRoam é um **livro de testes GSMA concluído**: a planilha oficial GSMA para o livro, preenchida com os resultados da execução e todos os detalhes circundantes, pronta para ser enviada a um parceiro de roaming ou hub. O OmniRoam a produz com uma única ação de **Baixar Livro de Testes**. Não requer transcrição manual.

O Que Você Recebe

O OmniRoam pega o modelo oficial GSMA para o livro e o preenche, de modo que o resultado é o mesmo livro que um parceiro espera receber (mesmas abas, mesma numeração de casos, mesmo layout), mas populado com resultados reais em vez de campos em branco.



O Que É Preenchido

Três categorias de informações são escritas no livro.

1. Resultados por caso

Para cada caso no livro, a célula de resultado do livro é definida como o veredicto registrado (**PASS**, **FAIL** ou **NOT PERFORMED**). A célula de comentários do caso é preenchida com as evidências de suporte capturadas durante a execução.

No documento	Vem de
Resultado do caso de teste (PASS / FAIL / NOT PERFORMED)	O veredicto do caso
Comentários do caso de teste	As evidências: tempos, throughput, causas de rede, leituras de interrogação, etc.

2. Identidades e metadados

As seções de cabeçalho e informações do operador são preenchidas a partir da execução:

No documento	Vem de
IMSI	O SIM de teste
MSISDN	O SIM de teste
PLMN de origem (a) / PLMN visitado (b)	O parceiro de roaming / PLMNs escolhidos para o livro
Data dos testes	A data da execução
Nome do testador, telefone, e-mail	Os detalhes do testador no livro
APN (quando aplicável)	A configuração de dados utilizada

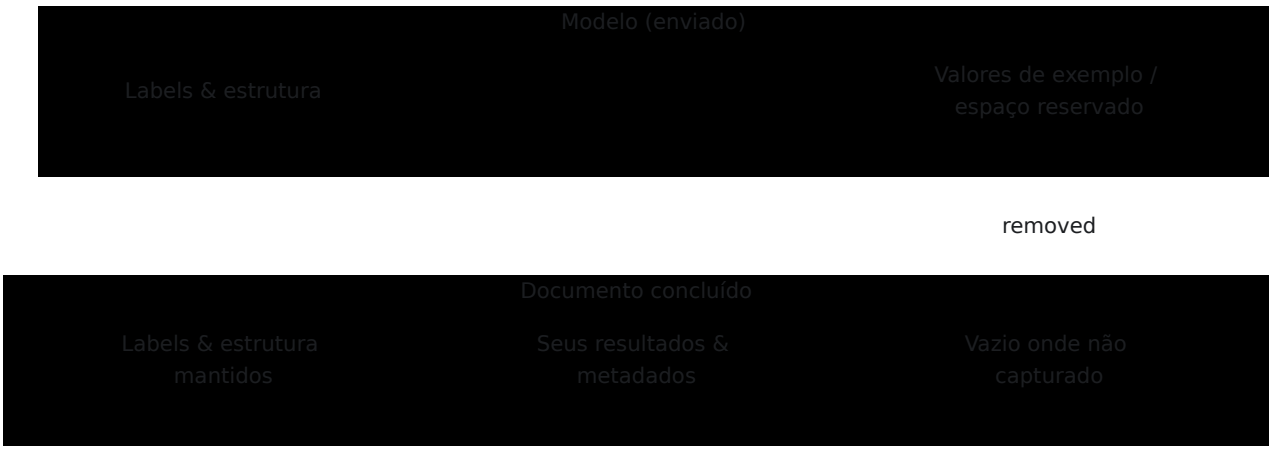
3. Valores medidos

Para os casos de dados e serviços suplementares, os valores medidos específicos que a planilha GSMA solicita são escritos em suas células dedicadas:

No documento	Vem de
Horários de início / fim da sessão de dados	A sessão de dados
Volumes de dados enviados / recebidos	Os registros de cobrança do gateway de serviço
Duração da sessão	A sessão de dados
Throughput / taxa média de dados	A medição de throughput
Indicações de sucesso do serviço (Sim/Não)	O resultado do caso

Saída Limpa e Apresentável

Os modelos GSMA em branco são enviados com conteúdo de exemplo e espaço reservado nas células a serem preenchidas: tempos de amostra e notas de referência destinadas a guiar um testador manual. O OmniRoam remove esse conteúdo de espaço reservado quando gera o documento, de modo que o livro concluído mostra apenas seus resultados reais e campos vazios onde um valor não foi capturado. Ele nunca transporta os dados de amostra do fornecedor para o seu relatório entregue, e nunca sobrescreve os rótulos, cabeçalhos ou estrutura da GSMA.



Quando Gerar

Você pode baixar o documento a qualquer momento. Ele sempre reflete o estado atual da execução. Um fluxo típico é executar o livro (ou rotina agendada), revisar os veredictos por caso, reexecutar quaisquer casos que precisem de atenção e, em seguida, baixar o livro concluído assim que os resultados parecerem corretos. Como a exportação reflete a execução ao vivo, uma nova exportação após uma reexecução simplesmente produz um documento atualizado.

Casos Manuais no Documento

Casos que o OmniRoam não pode conduzir automaticamente ainda aparecem no livro com seu número e título de caso, prontos para que o testador registre um resultado à mão. Isso mantém o documento entregue completo: os casos automatizados são preenchidos com evidências reais, e os casos manuais são apresentados no lugar certo para o testador finalizar.

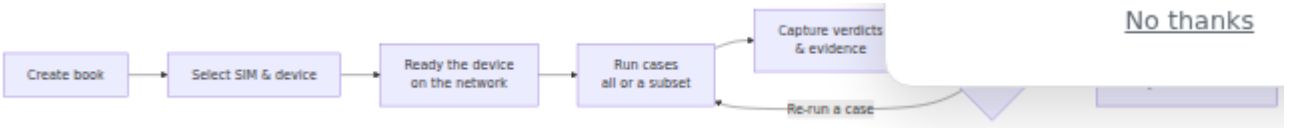
Veja Executando Testes para como os veredictos são produzidos e Explorador de Livro de Testes para o mapeamento exato célula por célula do que é preenchido.

Executando Testes do OmniRoam

Este guia cobre todo o ciclo de vida de um teste de roaming: criando um livro, executando-o, observando a execução dos casos, personalizando quais casos são executados, re-executando um único caso e agendando execuções rotineiras não supervisionadas.

- O Ciclo de Vida do Teste
- Criando um Livro de Teste
- Executando um Livro
- Como os Casos Automatizados São Executados
- Personalizando uma Execução
- Re-executando um Único Caso
- Execuções Rotineiras e Agendadas
- Lendo os Resultados

O Ciclo de Vida do Teste



Criando um Livro de Teste

A tela de Livros de Teste de Roaming lista cada livro com seu tipo, as redes de origem e visitadas, a identidade do assinante, o testador e o status atual.

Um livro de teste é criado a partir da tela **Livros de Teste de Roaming**. Ao criar um livro, você escolhe:

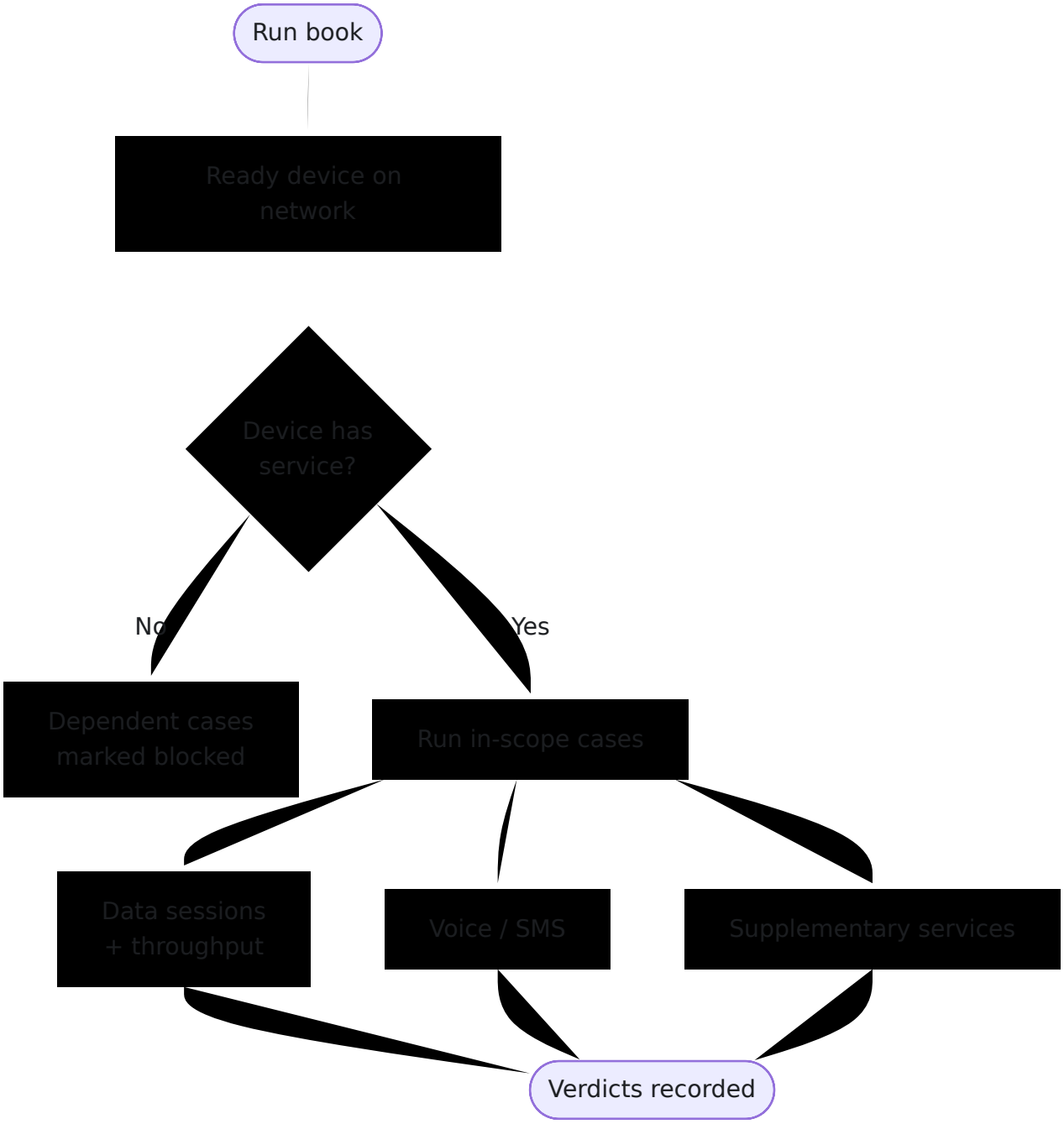
Campo	Propósito
Tipo de livro	Qual livro GSMA executar: IR.38, IR.48 ou VoLTE. Isso seleciona o conjunto de casos.
Parceiro de roaming / PLMNs	As redes de origem (PLMN a) e visitadas (PLMN b). Usado para preencher o cabeçalho do documento e para escolher o limite de throughput correto.
SIM	O SIM do assinante a ser testado. Seu IMSI e MSISDN são lidos e usados durante toda a execução e no documento final.
Detalhes do testador	Nome, telefone e e-mail da pessoa responsável, escritos no livro de trabalho concluído.

Uma vez criado, o livro lista cada caso do livro GSMA escolhido, cada um começando em um estado de "não realizado ainda".

Executando um Livro

Executar um livro realiza cada caso em escopo por sua vez. Antes que os casos de teste sejam executados, o OmniRoam prepara o dispositivo de teste na rede. Ele apresenta o SIM e confirma que o dispositivo se conectou e tem serviço. Este é um **portão pré-requisito**: se o dispositivo não conseguir obter serviço, os casos dependentes são relatados como bloqueados em vez de falhados, porque não faz sentido realizar um teste de dados ou voz sem bearer.

Como parte da preparação do dispositivo, o OmniRoam **lê a identidade do assinante do modem e preenche o livro automaticamente**: o **IMSI** é lido do SIM, a **rede de origem (HPLMN)** é derivada dele, e a **rede visitada (VPLMN)** é lida da rede na qual o dispositivo está atualmente acampado. Isso preenche o cabeçalho do livro e, portanto, o documento concluído, com o que foi realmente testado, em vez de valores digitados manualmente.



Enquanto um livro está em execução, a tela mostra cada passo à medida que acontece, com o passo atual destacado e uma indicação ao vivo de aprovação/reprovação por caso.

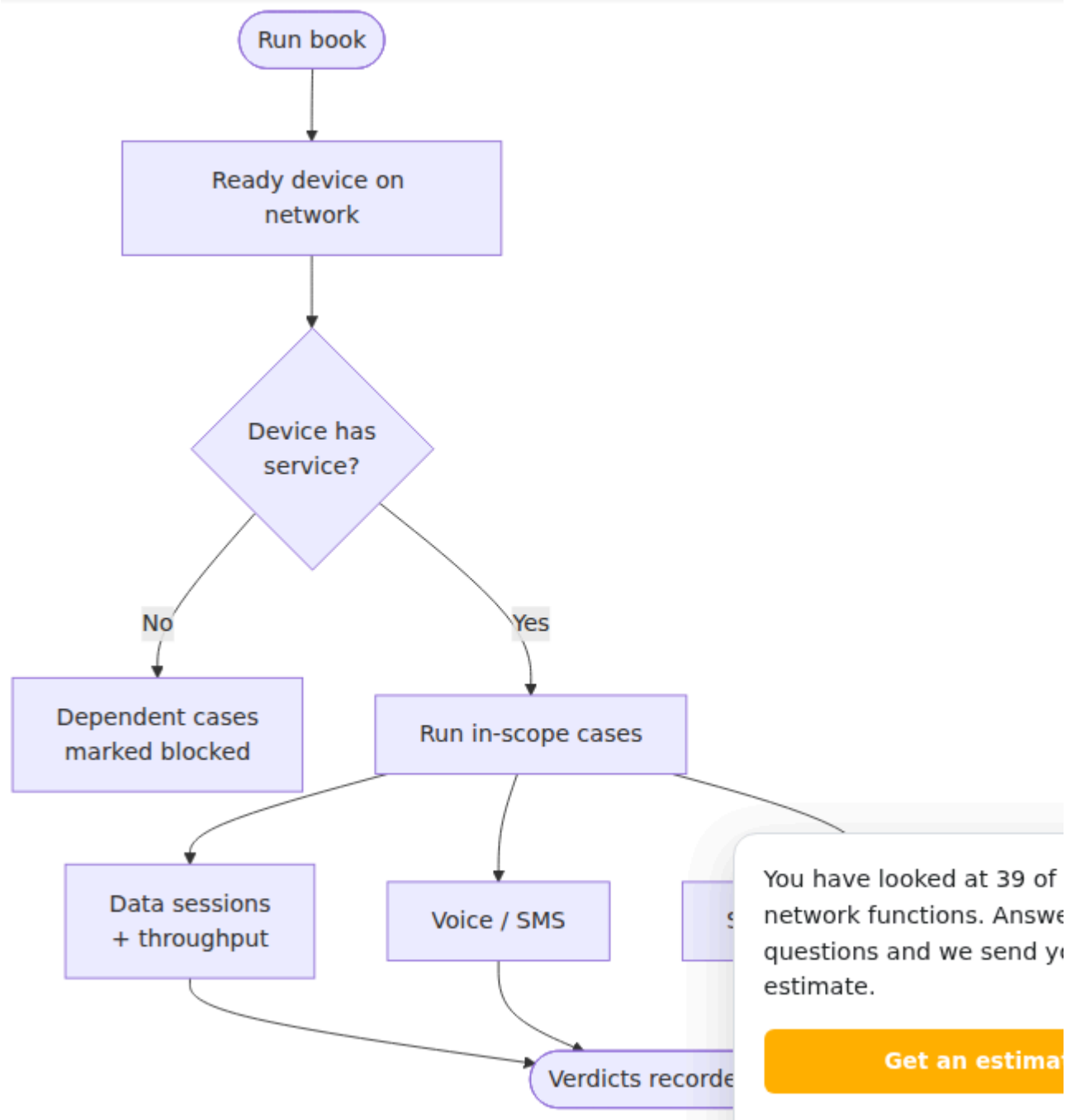
Como os Casos Automatizados São Executados

Cada caso automatizado controla o dispositivo de teste, observa o que a rede faz e compara o resultado com o resultado esperado da GSMA. Um caso só

passa com evidências positivas. Um passo que não pode ser confirmado é registrado como uma falha com a razão, nunca como uma aprovação silenciosa.

Sessões de dados e throughput

Para casos de dados, o OmniRoam estabelece uma sessão de dados de pacotes, executa tráfego para medir a taxa de download/upload alcançada e latência, e então desconecta para que a rede escreva um registro de cobrança limpo para a sessão. Os volumes de dados e os tempos são lidos dos registros de cobrança do gateway de serviço. Para o caso de velocidade IR.38, a taxa medida é afirmada em relação ao limite de throughput para a distância de origem/visitada.



Chamadas de voz

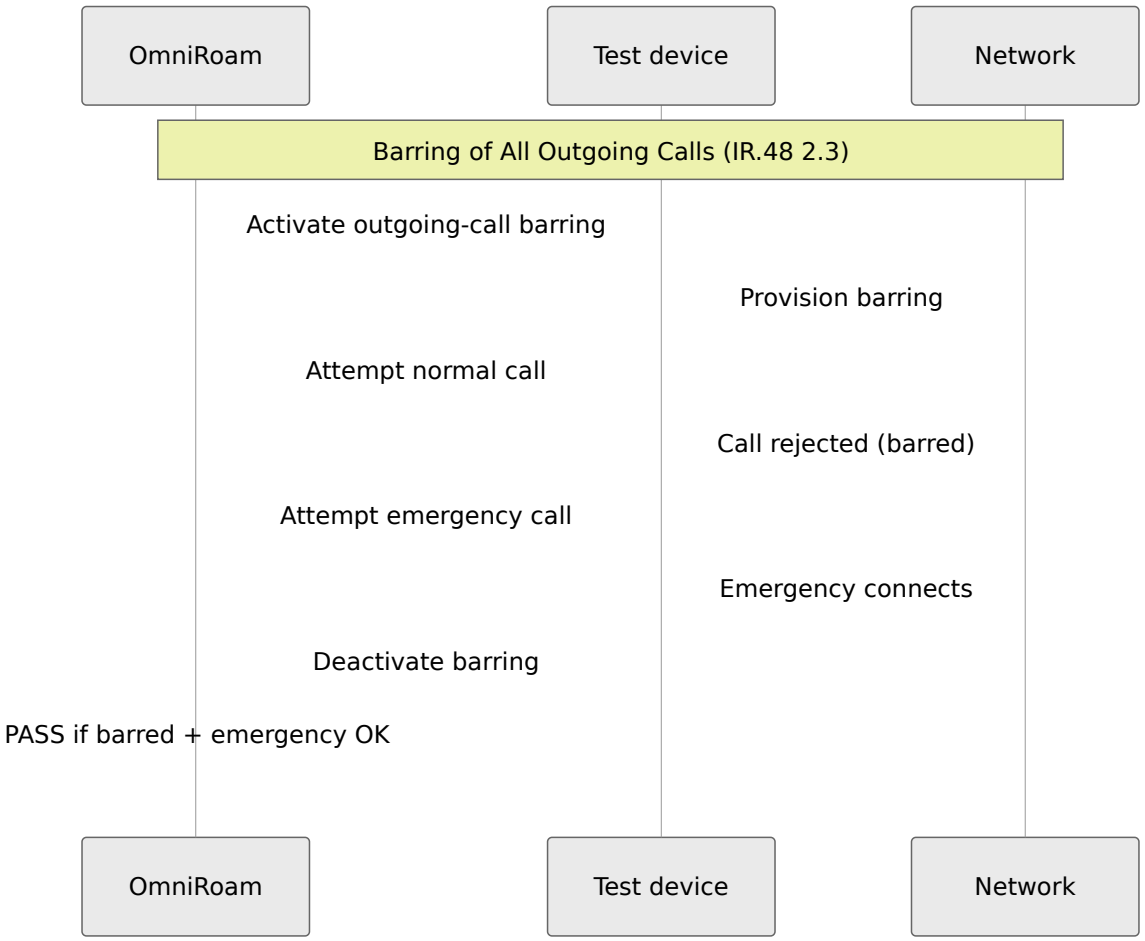
O OmniRoam realiza uma chamada do dispositivo para um serviço de atendimento em laboratório, confirma que a chamada chega ao estado ativo (atendida), opcionalmente a mantém para confirmar a estabilidade e, em seguida, a encerra. O veredicto registra o tempo para conectar e se a chamada permaneceu ativa.

SMS

O OmniRoam envia uma mensagem com um corpo único para um serviço de atendimento em laboratório e aguarda a resposta. A entrega da resposta confirma SMS originados em dispositivos móveis e SMS terminados em dispositivos móveis de ponta a ponta. Uma resposta ausente é uma falha clara com a razão, não um colapso.

Serviços suplementares (bloqueio e encaminhamento de chamadas)

O OmniRoam provisiona serviços suplementares pelo ar a partir do próprio dispositivo de teste, exatamente como um assinante faria com os códigos de controle de serviço padrão, e então os exerce:



Para **Encaminhamento de Chamadas em Caso de Não Resposta**, o OmniRoam registra o encaminhamento para um número alvo com um

temporizador de toque, e então interroga o serviço e confirma que a rede armazenou o número e o temporizador que foram registrados.

Cancelamento de Localização (IR.38 3.1.2)

Alguns casos são conduzidos do lado da rede em vez do dispositivo. Para **Cancelamento de Localização LTE**, o OmniRoam solicita ao servidor de assinantes da rede de origem para cancelar a localização do assinante na rede visitada e registra uma aprovação quando o pedido é aceito. Isso confirma que a rede de origem pode retirar um registro de roaming.

Registro IMS (VoLTE)

Para VoLTE, o OmniRoam primeiro confirma que o dispositivo está registrado no IMS. Isso condiciona os casos dependentes do IMS: se o registro não for confirmado, os casos de chamada VoLTE e SMS sobre IMS são relatados como bloqueados.

Personalizando uma Execução

Uma execução não precisa cobrir todo o livro. Usando o **seletor de teste**, o operador seleciona exatamente quais casos executar. Isso é útil para:

- Revalidar apenas os casos que falharam anteriormente.
- Executar apenas os casos de voz, ou apenas os casos de dados, durante a resolução de problemas.
- Pular casos que dependem de um arranjo ainda não implementado (por exemplo, um acordo CAMEL).

Os casos deixados de fora do escopo mantêm seu veredicto existente e não são tocados.

Re-executando um Único Caso

Cada caso tem um controle de re-execução. Selecioná-lo executa apenas aquele caso novamente, contra o mesmo dispositivo e SIM, e atualiza apenas o

veredicto daquele caso. Esta é a maneira mais rápida de confirmar uma correção (por exemplo, re-executar o caso de throughput após uma mudança de transporte) sem repetir todo o livro.

Execuções Rotineiras e Agendadas

O OmniRoam pode executar testes **não supervisionados em um cronograma** para que um relacionamento de roaming seja continuamente validado em vez de verificado uma vez.

- **Verificações rotineiras** executam um conjunto compacto de verificações de saúde contra um dispositivo (dados, velocidade, voz e SMS) e relatam uma aprovação/reprovação combinada. Estas são as mesmas execuções usadas pelos livros completos, embaladas como uma verificação rápida de confiança recorrente.
- **Agendas** executam uma rotina escolhida em um intervalo recorrente automaticamente. Cada execução agendada registra seu próprio resultado, construindo um histórico ao longo do tempo para que uma regressão (por exemplo, throughput caindo abaixo do limite, ou falha na entrega de SMS) seja detectada e visível sem que ninguém execute um teste manualmente.



Configurando uma Agenda

As agendas são gerenciadas na tela **Agendas** sob Testes de Roaming. Uma agenda define:

Configuração	Propósito
Nome	Identifica a agenda (e rotula suas métricas e histórico).
Modem(s)	O(s) dispositivo(s) de teste contra os quais a rotina é executada.
Verificações	Quais verificações a rotina realiza: dados, teste de velocidade, voz, SMS.
Intervalo	Com que frequência a rotina é executada (por exemplo, a cada hora).

Uma vez salva, a agenda é executada automaticamente em seu intervalo sem mais interação. A tela **Teste Rotineiro** mostra o histórico de execuções: a aprovação/reprovação combinada de cada execução, as velocidades medidas e os detalhes por verificação. Uma execução com falha apresenta as mesmas evidências que uma execução interativa.

Monitoramento Prometheus

Os resultados das rotinas agendadas são exportados como **métricas Prometheus**, para que a saúde do roaming possa ser alertada e monitorada ao lado do restante da rede, da mesma forma que os testes agendados em dispositivos de teste são monitorados. A exposição é servida em `/api/ir38/routine/metrics` (lê a última execução agendada por agenda e modem):

Métrica	Tipo	Signific
`omniweb_ir38_routine_pass`	gauge	Último resul rotina agend = aprovação reprovação)
`omniweb_ir38_routine_check_pass`	gauge	Resultado p verificação última execu (rótulo `chec` dados/teste velocidade/v
`omniweb_ir38_routine_download_mbps`	gauge	Taxa de dow medida na ú execução
`omniweb_ir38_routine_upload_mbps`	gauge	Taxa de uplo medida na ú execução
`omniweb_ir38_routine_latency_ms`	gauge	Latência me última execu
`omniweb_ir38_routine_last_run_timestamp_seconds`	gauge	Tempo Unix última execu agendada

Cada série carrega rótulos `schedule`, `serial`, `modem` e `imsi` (mais `check` na métrica por verificação), para que você possa alertar por agenda, por dispositivo ou por assinante de origem. O endpoint não precisa de login (scrapers não podem carregar um) e pode ser protegido com um token bearer quando necessário.

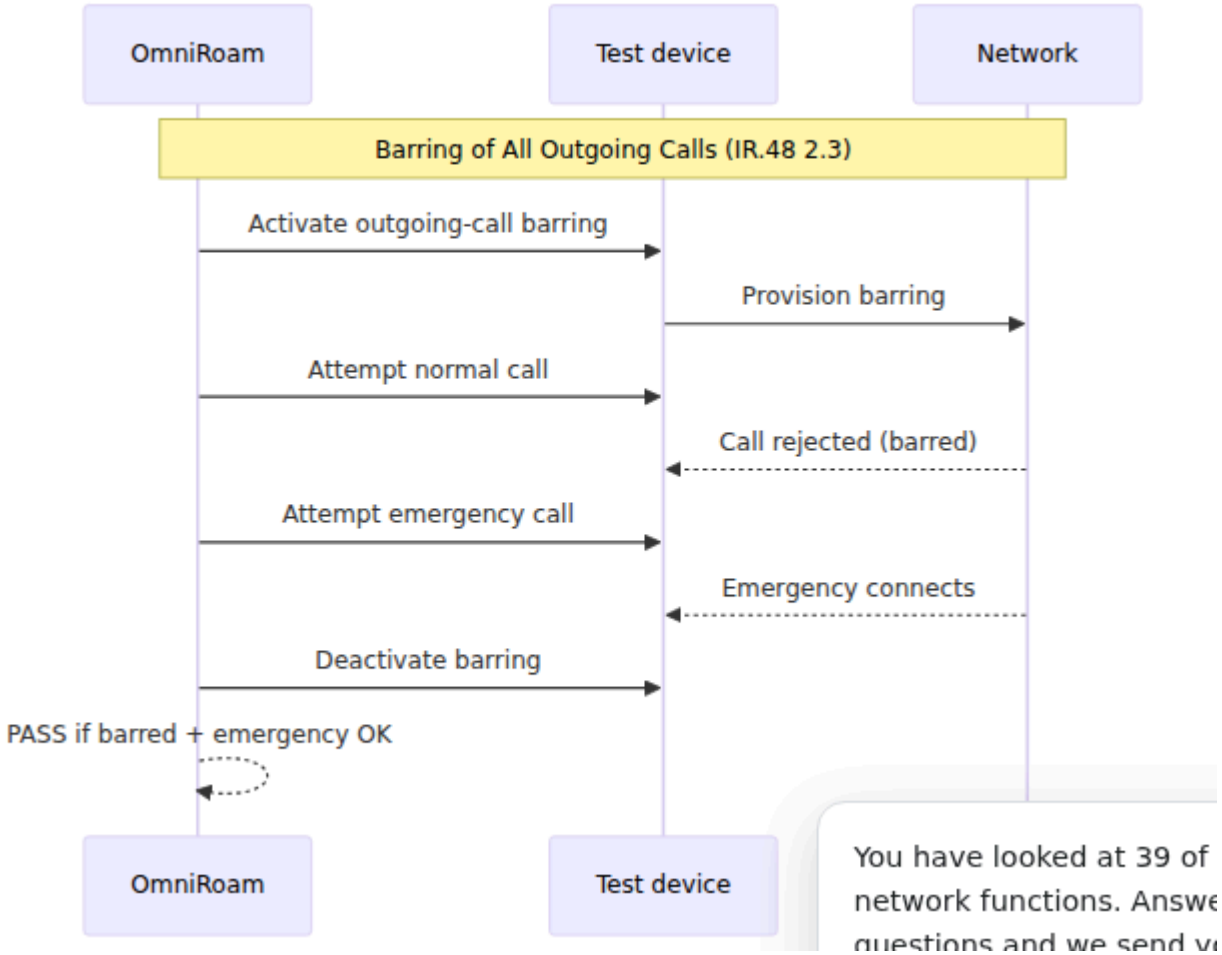
Exemplo de alerta: a voz de roaming tem falhado em um dispositivo por 15 minutos:

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

Os resultados agendados acumulam um histórico que pode ser revisado a qualquer momento, e uma execução com falha apresenta as mesmas evidências que uma execução interativa.

Lendo os Resultados

Cada caso mostra seu veredicto (**APROVADO**, **REPROVADO** ou **NÃO REALIZADO**) junto com as evidências por trás dele:



- **APROVADO**: o resultado esperado pela GSMA foi confirmado, com os números de apoio.
- **REPROVADO**: o resultado esperado não foi alcançado; a razão é registrada (por exemplo, "throughput abaixo do limite", "sem resposta de eco", ou a causa de liberação da rede para uma chamada que não se conectou).

- **NÃO REALIZADO**: o caso não foi executado, ou é um caso manual aguardando um testador.

Quando os resultados parecem corretos, gere o documento concluído. Veja Documentos de Teste de Livro Concluído.

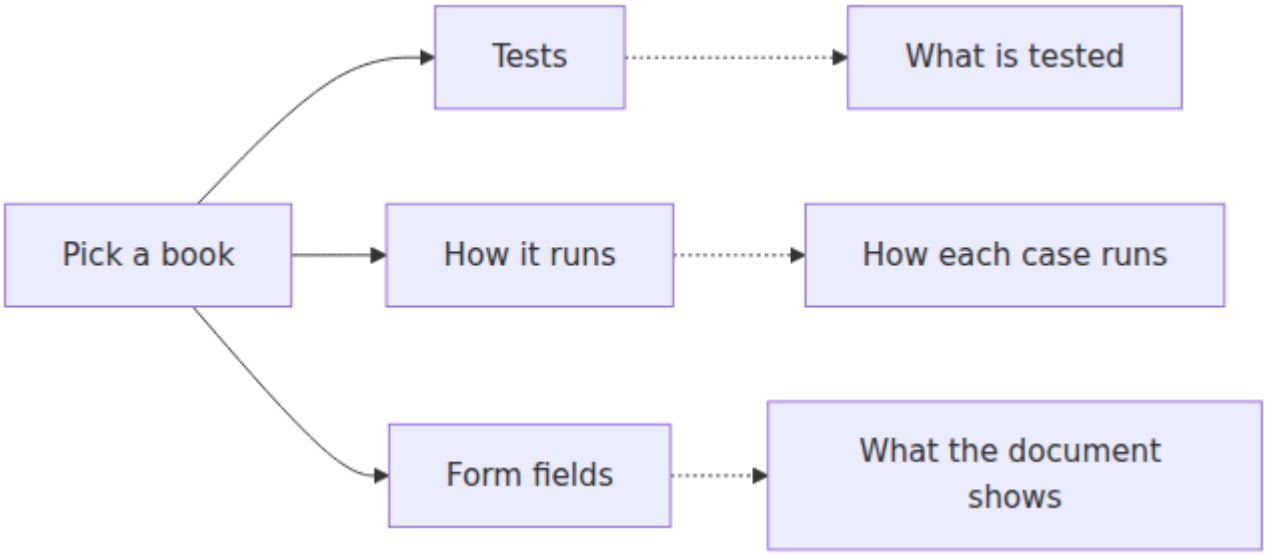
Explorador de Livros de Teste

O Explorador de Livros de Teste é uma visualização de referência somente leitura que mostra, para cada livro de teste, exatamente o que ele testa e como. Ele responde a três perguntas que um operador normalmente faz antes de confiar em uma execução automatizada:

1. **Quais casos estão neste livro e quais são automatizados?**
2. **Como cada caso é realmente executado?**
3. **O que acaba no documento finalizado e de onde vem?**

O Explorador é acessado a partir da tela de Livros de Teste em Roaming via **Explorar livros**, e permite que você mude entre IR.38, IR.48 e VoLTE.

O Explorador mostrando o livro IR.48. Cada caso é listado com se é automatizado ou manual e uma descrição de como é conduzido.



Testes

A visualização de **Testes** lista cada caso no livro com:

- o **número do caso** e **título** (correspondendo à especificação GSMA),
- se o caso é **automatizado** ou **manual**, e
- uma descrição simples de **como é conduzido**: por exemplo "sessão de dados + verificação de registro de cobrança", "chamada de voz", "ativação de bloqueio e tentativa de chamada", ou "o testador registra o resultado" para casos manuais.

Esta é a maneira mais rápida de ver, à primeira vista, quanto de um determinado livro o OmniRoam executa para você e o que permanece como verificação manual.

Como Ele Executa

A visualização de **Como ele executa** mostra a **sequência de passos** que uma execução completa do livro realizará, na ordem: preparando o dispositivo, as sessões de dados, a verificação de throughput, as execuções de voz e SMS, as execuções de serviços suplementares, e assim por diante. Ela reflete os casos atualmente em escopo, portanto é uma prévia precisa do que uma execução fará antes de você iniciá-la.

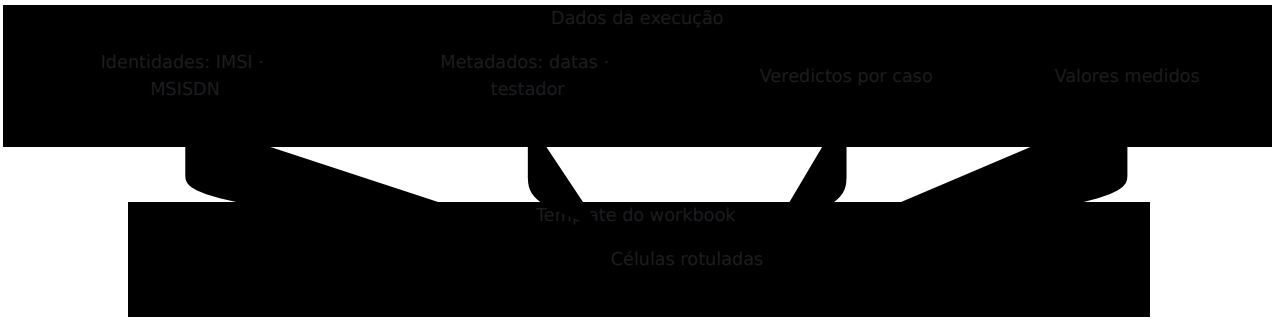
Esta visualização é útil para entender a forma de uma execução e para confirmar que um escopo personalizado realizará os passos que você espera.

Campos do Formulário

A visualização de **Campos do Formulário** lista cada célula no workbook GSMA completado que o OmniRoam preenche, cada uma anotada com:

- a **planilha e célula** no template GSMA,
- o **rótulo do campo GSMA** (lido do próprio template), e
- a **fonte** do valor: por exemplo, o MSISDN do assinante, a data do teste, um veredicto de aprovação/reprovação por caso, ou um valor medido como volume de dados.

Como esta lista é derivada da mesma lógica que produz o documento, ela não pode se desviar do que realmente é exportado: o que o Explorador diz que será preenchido é exatamente o que é preenchido. Veja Documentos de Livro de Teste Completos para o documento em si.



Baixar Template

O Explorador também oferece uma ação de **Baixar Template**, que baixa o workbook GSMA em branco para o livro selecionado: o template oficial com o conteúdo de exemplo/placeholder do fornecedor removido, pronto para ser preenchido à mão, se necessário. Este é o contraparte vazio do documento completado que uma execução produz (veja Documentos de Livro de Teste Completos).

Por Que Isso Importa

Um parceiro de roaming que aceita um livro de teste completado precisa ter confiança de que os resultados são reais e que o documento representa fielmente o que foi testado. O Explorador torna o mapeamento transparente: cada caso automatizado pode ser rastreado desde o número do caso GSMA, passando pela forma como é conduzido, até a célula exata em que ele se encontra no documento final.

Livros de Teste OmniRoam

A OmniRoam envia três livros de teste de roaming GSMA. Cada livro é o conjunto de testes oficial da GSMA, com casos identificados pelos seus números de caso GSMA, de modo que o documento concluído mapeia um para um na especificação publicada.

- IR.38: Teste de Dados de Roaming LTE
- IR.48: Roaming Bilateral (Voz / SMS / MMS / Dados)
- VoLTE: Teste de Roaming VoLTE

Para saber como cada caso automatizado é realmente conduzido e avaliado, consulte Executando Testes. Para navegar interativamente pelos casos de um livro, use o Explorador de Livros de Teste.

Nas tabelas abaixo, **Conduzido** indica se a OmniRoam executa o caso automaticamente (**Auto**) ou deixa para o testador registrar (**Manual**).

IR.38: Teste de Dados de Roaming LTE

Baseado em **GSMA IR.38 v3.0**. Prova que um assinante de roaming pode se conectar para dados na rede LTE visitada, acessar serviços através da rede doméstica e receber uma taxa de transferência aceitável. Também prova o fallback de voz e SMS por circuito comutado, e dados 2G/3G, onde estes estão em escopo.

Caso	Título	Conduzido	O que prova
`3.1.1`	Teste de velocidade LTE (dados + taxa de transferência)	Auto	Uma sessão de dados é estabelecida através do gateway doméstico, transporta tráfego e atende ao piso de taxa de transferência.
`3.1.2`	Cancelar Localização LTE	Auto	A rede doméstica pode cancelar a localização do assinante na rede visitada (acionado a partir do servidor de assinante doméstico).
`3.1.3`	Bloqueio Determinado pelo Operador LTE	Manual	O bloqueio determinado pelo operador aplicado no registro do assinante doméstico é respeitado.
`3.2.2`	Fallback CS: Chamada de Voz Originada pelo Móvel	Auto	Uma chamada de voz originada pelo assinante é bem-sucedida via fallback CS.
`3.2.3`	Fallback CS: Chamada de Voz Terminada pelo Móvel	Manual	Uma chamada para o assinante é bem-sucedida via fallback CS.
`3.2.4`	SMS sobre SGs	Auto	SMS originados e terminados por móvel funcionam sobre a interface SGs.
`3.3.1`	Acesso a Dados de 2G/3G usando PGW no HPLMN	Auto	Uma sessão de dados 2G/3G alcança serviços através do gateway doméstico.

Caso	Título	Conduzido	O que prova
`3.4`	Acesso a Dados de 4G + 5G NSA sobre S8	Auto	Dados em pacotes estão disponíveis e alcançam a internet (confirmado por uma sessão de dados com verificação de conectividade).

Cancelar Localização (3.1.2)

A OmniRoam automatiza o Cancelar Localização pedindo ao servidor de assinante doméstico para cancelar a localização do assinante na rede visitada, e então confirmando que o pedido foi aceito. Este é o cancelamento da inscrição de roaming iniciado pela rede doméstica (de acordo com o procedimento de cancelamento de localização em 3GPP TS 29.272).

O KPI de Taxa de Transferência

O caso `3.1.1` faz mais do que confirmar uma sessão de dados. Ele mede a taxa de download alcançada e a compara com o piso de taxa de transferência do IR.38. O piso depende da distância geográfica entre as redes doméstica e visitada (caminhos mais longos permitem taxas mais baixas):

Protocolo	Distância < 4000 km	Distância ≥ 4000 km
HTTP	≥ 11 Mbit/s	≥ 5 Mbit/s
FTP	≥ 13.5 Mbit/s	≥ 6 Mbit/s

A OmniRoam estima a distância a partir das identidades das redes doméstica e visitada e seleciona automaticamente o limite correto; o operador pode substituir a distância ou o protocolo quando os padrões não correspondem à configuração do teste. Registrar uma velocidade sem testá-la contra o piso nunca é tratado como um sucesso.

IR.48: Roaming Bilateral (Voz / SMS / MMS / Dados)

Baseado em **GSMA IR.48 v2.1** (internamente o conjunto de testes IR.24). O clássico livro de roaming bilateral 2G/3G: chamadas básicas, serviços suplementares, SMS e dados em pacotes, exercitados para um assinante que está em roaming na rede visitada.

Caso	Título	Conduzido	O que prova
`2.1`	MS1(a) chama MS2(a), ambos em roaming no VPLMN(b)	Auto	Uma chamada de voz básica é estabelecida e mantida.
`2.2`	Teste negativo CAMEL (MOC, pré-pago, sem acordo)	Manual	Uma chamada pré-paga é corretamente bloqueada onde não há acordo CAMEL ativo.
`2.3`	Bloqueio de Todas as Chamadas de Saída (BAOC)	Auto	Com o bloqueio de chamadas de saída ativo, chamadas normais falham enquanto chamadas de emergência ainda têm sucesso.
`2.4`	Encaminhamento de Chamadas em Caso de Não Resposta (CFNRY)	Auto	O encaminhamento de chamadas em caso de não resposta pode ser registrado e interrogado, com a configuração armazenada confirmada.
`2.5`	SMS Originados / Terminados por Móvel	Auto	Um SMS enviado do assinante em roaming é entregue e uma resposta é recebida.
`2.6`	Teste negativo CAMEL (SMS-MO, pré-pago)	Manual	Comportamento de SMS pré-pago onde não há acordo CAMEL ativo.
`2.7`	Acesso à Intranet / ISP usando gateway doméstico	Auto	Uma sessão de dados alcança a internet/intranet

Caso	Título	Conduzido	O que prova
			através do gateway doméstico.
`2.8`	MMS usando gateway doméstico e MMSC	Manual	Uma mensagem multimídia é entregue via o MMSC doméstico.

Serviços Suplementares em IR.48

Dois casos de serviços suplementares são totalmente automatizados:

- **BAOC (2.3): Bloqueio de Todas as Chamadas de Saída.** A OmniRoam ativa o bloqueio de chamadas de saída no assinante de teste, confirma que uma chamada normal de saída é rejeitada pela rede, confirma que uma chamada de emergência ainda se conecta (a exceção necessária), e então remove o bloqueio para deixar o SIM limpo.
- **CFNRY (2.4): Encaminhamento de Chamadas em Caso de Não Resposta.** A OmniRoam registra o encaminhamento de chamadas em caso de não resposta para um número alvo com um temporizador de toque, depois interroga o serviço (o equivalente a discar o código de status `*#61#`) e confirma que a rede armazenou o número e o temporizador para o qual foi registrado. Observar o desvio ativo requer uma chamada de entrada de um terceiro, então essa etapa final é deixada para uma verificação manual; o provisionamento e a interrogação são automatizados.

A OmniRoam relata o status de cada serviço suplementar usando as quatro bandeiras padrão 3GPP: **Provisionado**, **Registrado**, **Ativo**, e **Quiescente** (veja 3GPP TS 23.011).

VoLTE: Teste de Roaming VoLTE

Baseado em **GSMA BA.65 §5.3**, com comportamento VoLTE de acordo com **GSMA IR.92**. Prova que o assinante pode se registrar no IMS enquanto está

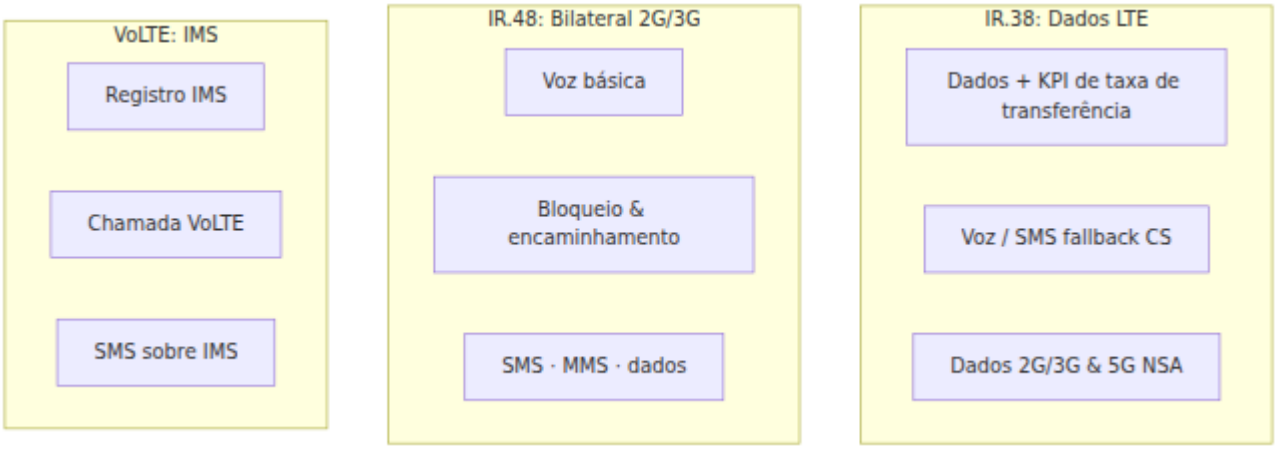
em roaming e fazer/receber chamadas VoLTE e SMS sobre IMS.

Caso	Título	Conduzido	O que prova
`ims_reg`	Registro IMS sobre roaming	Auto	O dispositivo se registra no IMS enquanto está em roaming (o pré-requisito para todos os serviços VoLTE).
`mo_call`	Chamada originada por móvel VoLTE	Auto	Uma chamada VoLTE originada pelo assinante é estabelecida e mantida.
`mt_call`	Chamada terminada por móvel VoLTE	Manual	Uma chamada para o assinante sobre VoLTE é estabelecida.
`sms_ims`	SMS sobre IMS (SMSoIP)	Auto	SMS é entregue sobre a rede IMS.
`emergency`	Chamada de emergência VoLTE	Manual	Chamadas de emergência funcionam sobre VoLTE (nunca discadas automaticamente).

O Portal de Registro IMS

Os serviços VoLTE dependem do registro IMS. A OmniRoam executa `ims_reg` primeiro como um **portal**: se o dispositivo não estiver registrado no IMS, os casos dependentes do IMS (`mo_call`, `sms_ims`) são relatados como bloqueados em vez de falhados. Não há valor em discar uma chamada VoLTE quando o IMS está fora do ar, e um resultado bloqueado informa ao operador exatamente o porquê.

Comparação dos Livros



Livro	Domínio principal	Melhor para
IR.38	Dados LTE / EPC	Validar um novo relacionamento de dados de roaming LTE e taxa de transferência
IR.48	Circuito comutado 2G/3G + pacotes	Validar voz, serviços suplementares, SMS e dados básicos
VoLTE	IMS	Validar roaming VoLTE uma vez que a interconexão IMS esteja em vigor

Gerenciamento de SIM OTA: RFM/RAM over-the-air

O módulo **OTA** gerencia SIMs **over the air**: ele lê e edita arquivos em um cartão remoto. Ele envia **pacotes seguros** (ETSI TS 102 225 / 3GPP TS 31.115, "03.48" / SCP80) que transportam comandos de Gerenciamento de Arquivos Remotos (RFM) e Gerenciamento de Aplicações Remotas (RAM). O cartão verifica e descriptografa cada pacote, executa os comandos e retorna um **Proof-of-Receipt (POR)** assinado.

Na prática, ele oferece a mesma edição em nível de arquivo que o Explorador de Sistema de Arquivos SIM: navegue pela árvore de arquivos, decodifique um EF, edite os campos, grave de volta. A diferença é que o OTA alcança o cartão **remotamente**: através de um leitor PC/SC no host central, um leitor em um agente, ou via **SMPP** para um SIM em campo.

As mesmas operações de arquivo também viajam por **HTTP (SCP81)**, onde o cartão abre uma sessão para um servidor de administração em vez de receber uma mensagem. Veja OTA over HTTP.

Ele se baseia no mesmo armazenamento de chaves por ICCID que o Armazenamento de Chaves SIM. Um perfil diz *quais conjuntos de chaves e algoritmos*, e o armazenamento de chaves contém o **KIC/KID** real para aquele cartão. O motor nunca registra ou retorna as chaves. Ele retorna apenas o texto cifrado resultante e o POR.

> **Esta página é a camada de entrega.** Ela cobre como uma alteração chega a um cartão, e as ferramentas que enviam uma manualmente. Para gerenciar um patrimônio - defina o que um cartão deve conter, emita cartões contra isso, e aplique uma alteração em todos os cartões que você emitiu - veja Ciclo de Vida do SIM. Para eSIM, veja eSIM (SGP.22).

O que é um pacote seguro

Um pacote seguro protege os comandos APDUs de ponta a ponta, independente do (básico) suporte. O motor foi validado contra cartões ISIM físicos.

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

CPL conta cada octeto após si mesmo; **CHL** conta do SPI até e incluindo o RC/CC/DS. Quando a cifra está ativada, tudo de CNTR até o final é cifrado e preenchido com zeros até o tamanho do bloco de cifra, com **PCNTR** registrando quantos octetos foram adicionados.

- **TAR** (Referência de Aplicação de Toolkit, 3 bytes) roteia o pacote para um serviço no cartão: uma aplicação RFM específica ou o RAM (gerenciador de cartão).

- **SPI** sinaliza a seleção de cifragem, a verificação de integridade, a política de contador e o que o PoR deve conter.
- **KIc / KID** indexa qual transporte (cifragem) e conjunto de chaves de autenticação o cartão usa; os **valores** vêm do armazenamento de chaves por ICCID.

Configurações de segurança em detalhes

Cada interruptor abaixo é configurável em um perfil, e cada combinação é implementada. Um fornecedor de cartões cita isso como quatro octetos hexadecimais

- MSL, PoR, KIc, KID - e um perfil os aceita dessa forma: cole `15213505` no campo **SPI** e cada interruptor é configurado a partir disso. O campo também funciona ao contrário, mostrando os quatro octetos atualizando à medida que você muda um interruptor, para que uma configuração possa ser lida de volta contra uma folha de personalização.

Octeto SPI	Configuração	Opções
MSL	Integridade	nenhum, verificação de redundância (RC), checksum criptográfico (CC)
MSL	Cifragem	ativado / desativado
MSL	Contador	sem contador; presente mas não verificado; deve ser maior; deve ser maior por um
PoR	Requisito	nunca; sempre; apenas em erro
PoR	Integridade da resposta	nenhum, RC, CC
PoR	Cifragem	ativado / desativado
PoR	Suporte	SMS-DELIVER-REPORT ou SMS-SUBMIT
KIc	Algoritmo de cifragem	DES-CBC, triple DES-CBC 2-chave, triple DES-CBC 3-chave, DES-ECB, AES-CBC
KIc	Versão da chave	1–3
KID	Algoritmo de checksum	DES-CBC, triple DES-CBC 2-chave, triple DES-CBC 3-chave, AES-CMAC
KID	Algoritmo de redundância	CRC 16, CRC 32
KID	Versão da chave	1–3

O octeto KID significa coisas diferentes em cada lado do MSL: quando a escolha de integridade é um **CC**, ele nomeia um algoritmo de checksum, e quando é um **RC**, os mesmos bits nomeiam um CRC. O editor de perfil troca as opções

para combinar, e o comprimento do RC segue - dois octetos para CRC 16, quatro para CRC 32.

As versões de chave param em 3 porque um registro de cartão contém três conjuntos de chaves; o SPI em si permite 1–15.

Parâmetros por conjunto de chaves

Um cartão é personalizado com um algoritmo **por conjunto de chaves** - o conjunto de chaves 1 pode ser triple DES com um CRC enquanto o conjunto de chaves 3 é AES com um CMAC. Isso pertence às chaves, não ao perfil que por acaso as seleciona, de modo que cada conjunto de chaves no armazenamento de chaves SIM carrega seu próprio SPI.

Quando um conjunto de chaves registra um, seus **algoritmos e versões de chave** são usados em lugar dos do perfil, porque um pacote construído com qualquer outra coisa é rejeitado pelo cartão. Tudo que é genuinamente escolha do operador - o TAR, a política de PoR, a política de contador, se deve cifrar, o formato do comando - ainda vem do perfil. A prévia relata quais configurações vieram de onde, para que um perfil que discorde de um cartão apareça antes que qualquer coisa seja enviada, em vez de como uma entrega falhada depois.

Um conjunto de chaves sem SPI registrado não muda nada: o perfil permanece como escrito.

Um **Proof of Receipt** é decodificado contra as mesmas configurações, incluindo a verificação de seu RC ou CC. O octeto de status é relatado nas próprias palavras da especificação - *PoR OK*, *RC/CC/DS falhou*, *CNTR baixo*, *CNTR alto*, *CNTR bloqueado*, *erro de cifragem*, *erro de segurança não identificado*, *memória insuficiente*, *mais tempo necessário*, *TAR desconhecido*, *nível de segurança insuficiente*.

Formato de comando remoto

Os scripts de comando têm como padrão o formato **compacto**: os C-APDUs um após o outro. Um perfil pode selecionar o formato **expandido** em vez disso (ETSI TS 102 226), que envolve cada C-APDU em um `22` TLV dentro de um template de script de comando `AA`, com codificação de comprimento indefinido

(`AE`) como uma opção. O cartão responde com um template `AB` ou `AF` contendo um `23` R-APDU por comando, de modo que um script com falha pode ser rastreado até o comando que falhou, em vez de apenas a última palavra de status. Alguns TARs não aceitam nada mais.

Os APDUs internos são um script C-APDU comum: `SELECT` + `READ BINARY` para uma leitura RFM, `SELECT` + `UPDATE BINARY` para uma gravação, GlobalPlatform `DELETE` / `INSTALL` para RAM.

Na rede (um SMS-PP), o pacote viaja nos TP-User-Data com um Identificador de Pacote de Comando UDH (IEI `0x70`), PID `0x7F` (download de dados SIM), DCS `0xF6` (8-bit, classe de mensagem 2). No shell, é entregue como um APDU CAT `ENVELOPE(SMS-PP-Download)` e o PoR retorna de forma síncrona.

Um pacote muito longo para uma mensagem curta é automaticamente dividido, seja com o cabeçalho de concatenação de 8 bits ou - via SMPP - com os parâmetros `sar_*` para que o SMSC o reassemble.

Perfis, contextos e roteamento automático

Um **perfil OTA** é uma predefinição de segurança reutilizável. Ele não contém **nenhum material de chave**:

Campo	Significado
`tar`	Referência de Aplicação de Toolkit de 3 bytes (o serviço alvo).
`kic_index` / `kid_index`	Qual conjunto de chaves (1/2/3) → `KIC{n}`/`KID{n}` da linha de armazenamento de chaves do cartão.
`cipher_algo` / `cc_algo`	Algoritmo de cifragem e checksum (`triple_des_cbc2`, `aes_cbc`, …).
`ciphering`, `rc_cc_ds`, `counter_mode`	SPI: cifrar? CC vs RC vs nenhum? política de contador de repetição.
`por`, `por_ciphered`, `por_rc_cc_ds`	PoR necessário? cifrado? assinado?

Dois perfis são semeados, correspondendo aos valores validados no sysmoISIM:

- **RFM-USIM-3DES-keyset3**: TAR `B00011`, conjunto de chaves 3, 3DES, cifragem + CC, PoR necessário + cifrado + CC. Opera dentro do **ADF.USIM**.
- **RFM-SIM-3DES-keyset2**: TAR `B00010`, conjunto de chaves 2. Opera na árvore 2G **MF-rooted** (DF.GSM / DF.TELECOM).

Aplicações diferentes precisam de serviços diferentes, então o explorador **roteia o perfil e o contexto SELECT automaticamente por arquivo**, a partir da aplicação do arquivo:

Aplicação do arquivo	Contexto	Perfil (por TAR)	Pré-SELECT antes do ENVELOPE
`ADF.USIM`	`usim`	TAR `B00011`	`SELECT ADF.USIM` (por AID)
`DF.GSM`, `DF.TELECOM`	`sim`	TAR `B00010`	nenhum (MF-rooted)
`ADF.ISIM`	`isim`	TAR `B00013`	`SELECT ADF.ISIM` (por AID)

Cada contexto mapeia para um dos seus perfis (definido por correspondência de TAR, substituível no explorador). Escolha um cartão e clique em qualquer arquivo (USIM, GSM ou TELECOM). O OmniWeb aplica o perfil, conjunto de chaves e SELECT corretos sem a necessidade de mudar nada. O ISIM funciona assim que você cria um perfil para ele (seu TAR varia por cartão).

Transportes

Um transporte entrega o pacote seguro e, onde o suporte permite, coleta o POR. Os adaptadores plugáveis compartilham uma interface:

Tipo	Atinge	POR	Notas
`local_pcsc`	um cartão em um leitor PC/SC **no host central**	síncrono	o caminho de validação diretamente conectado.
`agent_reader`	um cartão em um leitor **em um agente remoto**	síncrono	viaja pelo mesmo WebSocket do agente que Dispositivos de Teste / Banco SIM (revezamento `session_apdu`).
`smpp`	um **SIM de campo** via SMPP `submit_sm`	assíncrono	SMS MT para um SMSC; o PoR retorna mais tarde como um SMS MO, ou na mesma conexão quando vinculado como um transceptor. Veja **Parâmetros SMPP** abaixo.
`http_admin`	um **SIM de campo** via **HTTP (SCP81)**	assíncrono	um SMS de gatilho faz o cartão discar para o Servidor de Administração Remota via TLS-PSK; scripts e respostas fluem para lá. Veja OTA over HTTP.

O **Explorador** usa apenas os transportes no shell (ele precisa de um PoR síncrono); **Campanhas** podem usar qualquer um, incluindo SMPP.

Onde você configura SMPP

SMPP é configurado **por campanha**, não uma vez para o sistema. Cada campanha carrega sua própria conexão, então um patrimônio pode ser gerenciado através de mais de um SMSC.

Configure-o no editor de transporte na campanha, com o tipo `SMPP`.

Configuração	Necessária	Descrição
Host	Sim	O SMSC para se conectar.
Porta	Sim	A porta do SMSC.
ID do Sistema	Sim	A conta de vinculação.
Senha	Sim	A senha de vinculação.
Tipo de Sistema	Não	O tipo de sistema de vinculação, quando o SMSC precisa de um.
Endereço de Origem	Não	O endereço de onde a mensagem vem. O cartão envia sua resposta aqui, então configure-o para um endereço que você recebe.
Endereço de Destino	Não	Substitui o próprio MSISDN do cartão. Deixe vazio em uso normal.
TON / NPI de Origem	Não	Tipo de número e plano de numeração para o endereço de origem.
TON / NPI de Destino	Não	Tipo de número e plano de numeração para o endereço de destino.
Tempo limite do PoR	Não	Quanto tempo esperar na mesma conexão pela resposta do cartão.

Defina o endereço de origem para um lugar onde você recebe mensagens. Esses cartões enviam o Proof of Receipt para o endereço de origem do comando, então um endereço de origem que você não recebe significa que a resposta é perdida.

Um tempo limite do PoR força uma vinculação de transceptor. Uma vinculação somente de transmissor não pode receber a resposta, então o transporte muda o modo de vinculação em vez de deixá-lo esperar por uma resposta que nunca pode chegar.

Parâmetros SMPP

Uma mensagem curta OTA difere de uma comum em um punhado de parâmetros, e um SMSC aceitará uma mensagem que os tenha errados e silenciosamente nunca a entregará ao cartão. Todos eles são configuráveis:

Parâmetro	Padrão	Por que é importante
`esm_class`	`0x40`	Marca os dados do usuário como começando com um cabeçalho. Sem isso, o cartão nunca vê o Identificador de Pacote de Comando.
`protocol_id`	`0x7F`	Download de dados (U)SIM.
`data_coding`	`0xF6`	8-bit, classe de mensagem 2 - o que roteia a mensagem para o SIM em vez da caixa de entrada.
`dest_addr_subunit`	`0x02`	A subunidade de destino é o SIM. O parâmetro mais frequentemente ausente quando um pacote é aceito e nunca chega.
`user_message_reference`	não definido	Carregado para o PoR MO pela maioria dos SMSCs, que é como um PoR assíncrono é combinado de volta ao seu trabalho.
`registered_delivery`, `validity_period`, `priority_flag`, `service_type`, `schedule_delivery_time`,	Padrões do SMSC	Controles de submit_sm comuns.

Parâmetro	Padrão	Por que é importante
`replace_if_present_flag`, `sm_default_msg_id`		

Pacotes longos são segmentados de três maneiras: o cabeçalho de concatenação de 8 bits nos dados do usuário (o padrão), os parâmetros `sar_msg_ref_num` / `sar_total_segments` / `sar_segment_seqnum` para que o SMSC reassembla, ou um único `message_payload` onde o SMSC o suporta. Qualquer outro parâmetro opcional pode ser adicionado pelo nome.

Antes de enviar, um transporte relatará configurações que são válidas, mas não chegarão a um SIM - uma falta de sinalizador de cabeçalho, uma codificação de dados que vai para a caixa de entrada, uma subunidade de destino que não é o SIM.

Descobrindo os parâmetros de um cartão

Não é possível perguntar a um cartão quais TAR e configurações de segurança ele foi personalizado. Quando um lote chega com chaves, mas sem documentação, **Perfis → Descobrir parâmetros** os encontra por sondagem: ele tenta cada um dos conjuntos de chaves do cartão contra o espaço de parâmetros plausível e relata o que o cartão aceita. Um resultado pode ser transformado diretamente em um perfil com **Usar**.

Isso precisa de um transporte no shell - um suporte de armazenar e encaminhar não pode responder a cada sondagem.

Duas coisas tornam uma varredura ingênua inútil, e a execução de descoberta lida com ambas:

- **Um contador que é muito baixo é rejeitado em silêncio.** Onde o nível de segurança diz *o contador deve ser maior*, um cartão dado um contador igual ou abaixo de seu valor armazenado não retorna nada - sem erro, sem Proof of Receipt. Isso é indistinguível de chaves erradas ou um TAR errado. A descoberta portanto começa o contador alto; uma vez que um contador só aumenta, começar alto não custa nada.

- **O byte do PoR decide de onde a resposta volta.** Com o bit 6 limpo, o cartão responde na resposta do ENVELOPE; com ele definido, o cartão levanta uma mensagem curta proativa SEND SHORT MESSAGE em vez disso e a resposta do ENVELOPE fica vazia. Observe apenas um caminho e uma resposta correta é invisível, então ambos são pesquisados.

Um status de **CNTR baixo** é tratado como um sucesso em vez de uma falha: isso significa que as chaves, o TAR, os algoritmos e o nível de segurança foram todos aceitos, e apenas o contador estava errado. A descoberta para ali e resolve o contador dobrando, o que leva algumas rodadas de viagens em vez de continuar a varredura.

Se nada for aceito, isso realmente não diz qual parâmetro estava errado - o silêncio é a resposta do cartão para todo tipo de erro.

> Cada sondagem aceita avança o contador do cartão, e um contador nunca volta para baixo.

Entregando através de EF_SMS

Um pacote também pode ser escrito diretamente em um registro de `EF_SMS` (`3F00/7F10/6F3C`) em um cartão em um leitor, com o registro marcado como não lido. O cartão o processa exatamente como se tivesse chegado via over the air - sem SMSC e sem rádio. Esta é a maneira prática de exercer um script contra um cartão em uma mesa ou em um banco.

OTA over HTTP (SCP81)

Uma mensagem curta segura carrega algumas centenas de bytes. Uma alteração de qualquer tamanho se torna muitas mensagens, e cada uma delas pode ser perdida, atrasada ou reordenada pela rede no meio. **SCP81** remove esse limite.

Em vez de o OmniWeb enviar uma mensagem para o cartão, **o cartão abre uma sessão para o OmniWeb**. Ele disca para um **servidor de administração** via TLS com uma chave pré-compartilhada, pede trabalho e

executa scripts de comando inteiros um após o outro até que o servidor lhe diga que a sessão está finalizada. Não há limite de tamanho por mensagem e nenhuma segmentação. O OmniWeb executa esse servidor de administração.

As operações de arquivo são as mesmas operações de gerenciamento de arquivos remotos que via SMS.

Portas e configuração

O servidor de administração é um serviço separado. Ele escuta em duas portas.

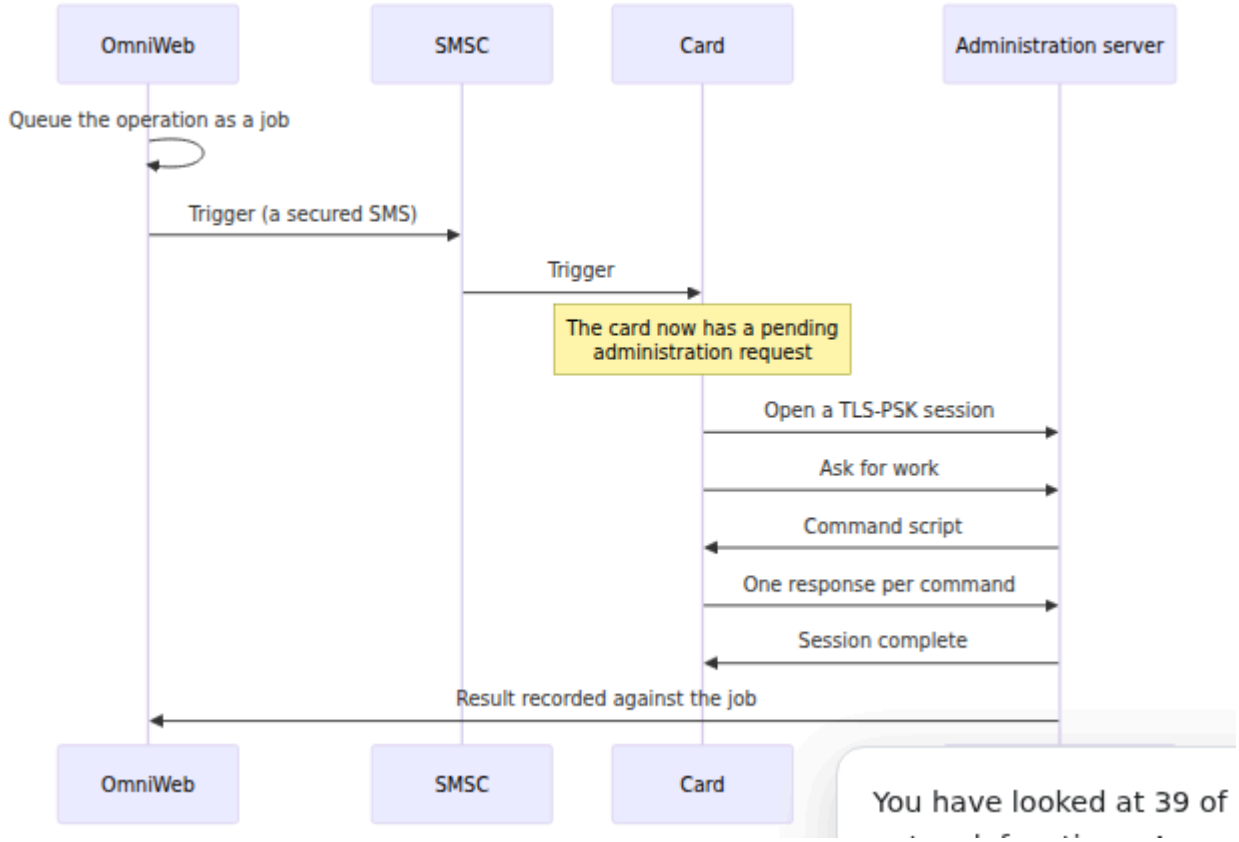
Configuração	Padrão	Alcance	Descrição
`OMNIWEB_RAS_PORT`	`8443`	público	A porta TLS à qual os cartões se conectam.
`OMNIWEB_SCP81_API_PORT`	`8090`	localhost	O plano de controle que o OmniWeb usa para enfileirar scripts e ler resultados.

Permita que seus intervalos de dados SIM alcancem a porta de administração. Um cartão só pode abrir uma sessão se puder alcançar essa porta a partir da rede à qual está conectado.

Não exponha a porta do plano de controle. Ela enfileira os scripts que são enviados para os cartões. Mantenha-a no localhost.

Sirva **TLS 1.1** bem como versões posteriores. A Emenda B da GlobalPlatform define TLS 1.1 como o mínimo, e cartões em campo o oferecem e nada mais novo. Um servidor que oferece apenas TLS 1.2 responde a tal cartão apenas com um alerta de versão de protocolo, antes que o cartão apresente sua identidade, então o log mostra uma falha de handshake e nada que identifique o cartão.

Um cartão alcança o servidor no endereço com o qual foi personalizado. Se esse endereço não for seu, veja Trasna SIMs Over The Air para como redirecionar a sessão. Somente a entrega muda.



O que um operador faz

Nada diferente. Escolha HTTP como o suporte em uma campanha, ou deixe `Auto` escolhê-lo, e o OmniWeb envia o gatilho e serve a sessão. A visualização **Admin Sessions** mostra cada sessão à medida que acontece: seu estado, quão longe está nos scripts e a escada de comando e resposta. O **trabalho** vinculado carrega o resultado final, exatamente como faz para qualquer outro transporte.

SMS ou HTTP

Propriedade	SMS (SCP80)	HTTP (SCP81)
Quem inicia	OmniWeb empurra	O cartão disca, após um gatilho
Tamanho	Algumas centenas de bytes por mensagem, segmentado além disso	Sem limite prático
Viagens de ida e volta	Um pacote, um proof of receipt	Muitos scripts em uma sessão
Necessita serviço de dados	Não	Sim. O cartão abre um canal de dados
Retorno após falha	Nenhum	Um cartão que falha sessões repetidamente para de tentar, por até 24 horas
Melhor para	Mudanças pequenas, cartões sem serviço de dados, primeiro contato com um cartão	Mudanças grandes, muitos arquivos de uma vez, uma versão inteira de perfil

Use SMS para uma mudança de um arquivo. Use HTTP quando uma campanha de convergência tiver mais de alguns arquivos para escrever.

O que esperar

- **Um cartão disca apenas enquanto tem trabalho pendente.** O gatilho é o que cria essa solicitação pendente. Um cartão que terminou sua última sessão não tem razão para chamar, e não o fará.

- **Uma sessão falhada é cara.** Um cartão que desiste de uma sessão de administração pode estacionar por até 24 horas, e nada limpa esse temporizador. O ritmo da campanha existe por esse motivo. Prove uma mudança em um cartão antes de enfileirar cinco mil.
- **Um reconhecimento não é execução.** Um cartão pode aceitar um script e não executar nenhum dele. O OmniWeb lê as respostas por comando em vez de confiar no reconhecimento, que é também por isso que uma auditoria é a única coisa que prova o conteúdo de um cartão.
- **Endereçamento difere por cartão.** Via HTTP, a aplicação alvo é nomeada por seu identificador em vez de por um TAR, e alguns cartões aceitam apenas um formato de script de comando. Isso é registrado por produto de cartão, não adivinhado por sessão.

Segurança

O servidor de administração termina o TLS com uma **chave pré-compartilhada**, não um certificado. A identidade é o ICCID do cartão, e a chave vem do armazenamento de chaves SIM para aquele cartão.

O servidor de administração de face pública **não possui material de chave próprio**. Ele pede ao OmniWeb pela chave quando um cartão apresenta uma identidade, e puxa cada script da fila de trabalhos do OmniWeb. Há uma fila para ambos os suportes, então um cartão que não convergiu tem um lugar para olhar.

A mensagem que um cartão aceita via SMS

Um pacote seguro só chega à aplicação do cartão quando a mensagem curta é endereçada ao cartão. Dois campos fazem isso, e ambos devem estar corretos.

Campo	Valor	Efeito
TP-PID	`7F`	"(U)SIM Data Download". O aparelho passa a mensagem para o cartão.
TP-DCS	`F6`	Dados de 8 bits, classe de mensagem 2. A classe marca a mensagem como específica do cartão.

Defina TP-PID como `7F`. Um aparelho aceita uma mensagem com TP-PID `00` e um esquema de codificação de dados de classe 2, e então a arquiva como armazenamento comum do cartão. A aplicação nunca é executada e o cartão não retorna nada, enquanto o relatório de entrega ainda relata sucesso. Essa falha se parece exatamente com um cartão que ignorou o comando.

Algumas plataformas de mensagens não expõem TP-PID. Uma plataforma que não pode defini-lo não pode enviar uma mensagem OTA de forma alguma, independentemente do que mais esteja correto. Confirme o valor em um rastreamento da mensagem em vez de no registro da plataforma. Veja Trasna SIMs Over The Air para o layout completo da mensagem e os códigos de status que um cartão retorna.

Cartões suportados e plataformas testadas

As plataformas abaixo foram testadas **de ponta a ponta em cartões reais**: um arquivo lido, alterado, lido novamente e confirmado de forma independente em um leitor.

Cartão	Fornecedor	OTA via SMS (SCP80)	OTA via HTTP (SCP81)	download e instalação de eSIM (SGP.22)
TF6DH01	Valid	Testado	Testado	Não aplicável
Sm@rtSIM Zeta	Giesecke+Devrient	Testado	Testado	Não aplicável
eUICC	Kigen	Testado	Testado	Testado
SIMBA	Trasna	Testado	Testado	Não aplicável

Esta é a lista de plataformas comprovadas em hardware, não uma lista de plataformas que podem funcionar. Outras são esperadas para funcionar, e a maneira de descobrir é adicioná-las.

Como uma operação de arquivo é endereçada varia por plataforma e por portadora na mesma plataforma. Um cartão roteia em um TAR via SMS e nomeia um identificador de aplicação via HTTP. Um responde a uma classe de comando GSM enquanto outro responde a uma classe UICC. Um aceita apenas a forma de comprimento definido de um script de comando expandido e nunca responde à forma indefinida. Qualquer um desses erros se apresenta de forma idêntica, como um cartão que ignorou você.

Esse endereçamento é, portanto, registrado uma vez por **produto de cartão**, e cada cartão emitido nesse produto herda isso, então **adicionar um novo tipo de cartão é configuração em vez de código**. Veja Produtos de cartão.

Explorador

O editor de arquivos SIM remoto.

1. Escolha um **ICCID alvo** (do Armazenamento de Chaves SIM) e um **transporte**.

2. Navegue pelo **catálogo de arquivos**: cada EF conhecido do modelo de arquivo offline (ADF.USIM, ADF.ISIM, DF.GSM, DF.TELECOM), agrupado por aplicação e pesquisável por código / nome / descrição.
3. Selecione um arquivo → **Ler via OTA**. A leitura RFM segura é entregue, o POR decodificado, e o EF renderizado: status do POR, último SW, hex bruto + ASCII, e um **formulário de campo tipado** (decodificado para campos nomeados).
4. Edite os **campos** (re-encodificados automaticamente) ou o **hex bruto**, então **Escreva via OTA**. O `UPDATE` RFM seguro é enviado e o arquivo é **lido novamente** automaticamente para que você veja o estado no cartão após a escrita.

As leituras/escritas são controladas pela permissão de controle `ota`; tudo é registrado como um **trabalho**.

Campanhas

Uma operação salva espalhada por um conjunto de SIMs: **consulta alvo → operação → perfil → transporte**.

- **Consulta alvo** é avaliada contra o inventário do Banco SIM em tempo de execução: lista de ICCID / prefixo, prefixo ou intervalo IMSI, agente, banco. Uma consulta vazia deliberadamente não corresponde a nada (sem fan-out acidental).
- **Operação** é o comando RFM/RAM (ler/atualizar binário ou registro, GP excluir / obter-status / instalar).
- **Executar** cria um **trabalho** por cartão correspondente. Campanhas SMPP são fire-and-forget (o POR chega mais tarde como um SMS MO).

Uma execução é limitada (`CAMPAIGN_MAX_TARGETS`) para que uma consulta com erro de digitação não possa disparar milhares de cartões em uma única solicitação.

Trabalhos

Cada entrega OTA (leituras e escritas do explorador, e execuções de campanha) com seu status e POR. O painel de detalhes mostra o **pacote de solicitação seguro** (texto cifrado), o **Comprovante de Recebimento**, e o resultado decodificado (comandos executados, último SW, dados de resposta). Segredos do cartão são **nunca** armazenados em um trabalho: apenas o texto cifrado e o POR.

API REST (`/api/ota`, JWT, tipo de

elemento RBAC `ota`)

Método	Rota	Propósito
GET	`/profiles` · POST · `/profiles/<id>` PUT/DELETE	Perfis de segurança OTA.
GET	`/campaigns` · POST · `/campaigns/<id>` GET/PUT/DELETE	Campanhas.
GET	`/campaigns/<id>/targets`	Pré-visualizar quais SIMs a consulta atualmente corresponde.
POST	`/campaigns/<id>/run`	Executar: um trabalho por cartão correspondente.
GET	`/jobs`, `/jobs/<id>`	Histórico de trabalhos (filtrar por `campaign_id` / `iccid`).
GET	`/files/catalog`	O catálogo de EF navegável (modelo de arquivo offline).
POST	`/explore/read`	Ler um EF via OTA; retorna o trabalho + EF decodificado.
POST	`/execute`	Executar uma operação (atualização RFM, RAM, bruto) contra um cartão.
POST	`/preview`	Construir o pacote seguro **sem** enviar - retorna o texto cifrado, as formatações SMS, a decomposição SPI, o contador usado e o próximo.

Método	Rota	Propósito
POST	`/spi`	Decodificar quatro octetos SPI nas configurações nomeadas, ou construir os octetos a partir das configurações. Aritmética pura; nenhum cartão ou material de chave envolvido.
POST	`/discover`	Sondar um cartão para o TAR e SPI que aceita, dado apenas suas chaves. Necessita de um transporte em shell; avança o contador do cartão.
POST	`/decode` · `/encode`	Decodificar bytes EF ↔ campos tipados (offline).
GET	`/admin/sessions`	Sessões de administração HTTP (SCP81), ao vivo.
POST	`/audit`	Quais operações um conjunto de chaves pode realizar em cada arquivo, por configuração de segurança. Uma viagem de ida e volta OTA por célula.

As rotas de convergência declarativa - `/api/ota/sync/*` - pertencem ao patrimônio em vez de a uma única entrega. Elas estão documentadas em Ciclo de Vida do SIM.

RBAC espelha `simbank`/`ir38`: administradores sempre passam; caso contrário, uma permissão JWT com `element_type == "ota"` concede visualização, e `POST` em seus métodos concede controle. Leituras são tratadas como controle (transmitem um pacote para o cartão). As rotas são auto-documentadas na Referência da API.

Esquema do banco de dados

Tabela	Linha	Colunas-chave
`ota_profiles`	um preset de segurança	`name`, `tar`, `kic_index`/`kid_index`, algoritmos, flags SPI.
`ota_campaigns`	um fan-out salvo	`name`, `profile_id`, `target_query` (JSON), `operation` (JSON), `transport` (JSON), `status`.
`ota_jobs`	uma entrega para um cartão	`iccid`, `operation`, `request_hex` (texto cifrado), `response_hex` (POR), `por_status`, `result` (JSON), `status`.

As chaves vivem na tabela existente `simbank_keys` (o Armazenamento de Chaves SIM), referenciadas por ICCID pelo índice do conjunto de chaves do perfil. Elas **não** são duplicadas aqui.

Como funciona

O mecanismo OTA lida com a criptografia, a estrutura do pacote seguro, TLVs CAT/SMS e o modelo de arquivo offline necessário para construir e decodificar pacotes RFM/RAM 03.48/SCP80. Ele roda no serviço de backend de função de agente e compartilha a conexão do agente para o transporte em shell. A entrega é plugável através do leitor local, leitor de agente remoto, SMPP e transportes de administração HTTP. O servidor de administração voltado para o público é um serviço separado que não possui material de chave próprio.

Notas de segurança

- Segredos do cartão (KIC/KID) são lidos do armazenamento de chaves para construir pacotes, mas são **nunca** escritos no log de auditoria ou

retornados em qualquer resposta. Apenas a solicitação cifrada e o POR são armazenados.

- Escrever um arquivo é destrutivo; o explorador confirma antes de cada escrita e lê o resultado de volta.
- O pacote seguro é genuíno 03.48: altere um byte e o cartão o rejeita (o CC falha); com a cifragem ativada, os APDUs em texto claro nunca aparecem no fio.

Trasna SIMs Over The Air

Esta página registra como os UICCs da Trasna se comportam via OTA. O comportamento abaixo vem de testes em cartões reais, em um leitor de bancada e em dispositivos em uma rede ao vivo. Outras plataformas de cartão se comportam de maneira diferente. Use esta página quando você integrar um tipo de cartão Trasna e quando um comando OTA chegar a um cartão, mas nada acontecer.

Para o modelo geral de OTA, veja Gerenciamento de SIM OTA. Para como um tipo de cartão é registrado uma vez e reutilizado, veja Produtos de Cartão.

Índice

- O que o cartão diz sobre si mesmo
- SMS OTA
- HTTP OTA
- Redirecionar a sessão de administração
- Tabelas de referência
- Solução de problemas

O que o cartão diz sobre si mesmo

Um cartão Trasna expõe muito pouco sem chaves. Planeje isso ao integrar um novo lote.

O cartão responde `6D00` ao INICIALIZAR ATUALIZAÇÃO na interface de contato. `6D00` é a mesma palavra de status que uma instrução que não existe retorna. Portanto, o cartão não executa nenhum canal seguro GlobalPlatform na interface de contato. O Domínio de Segurança do Emissor é acessível apenas dentro de um pacote seguro.

As aplicações carregam identificadores de aplicação curtos e imprimíveis. Elas não usam a forma ETSI de 16 octetos. Um identificador de aplicação do toolkit ETSI mantém seu TAR no deslocamento 12, para que uma ferramenta possa encontrar automaticamente a aplicação de Gerenciamento de Arquivos Remotos. Um identificador de aplicação Trasna não mantém TAR, porque o TAR é atribuído quando a aplicação é instalada. Registre o identificador da aplicação alvo contra o produto do cartão. Não espere que a descoberta o encontre.

O cartão não mantém parâmetros de administração como objetos de dados GlobalPlatform. Cada objeto de dados testado retornou `6A88`, que significa "entendido, mas não mantido". Uma instrução de controle retornou `6E00`, que significa "não este comando". As duas respostas diferentes provam que o cartão implementa GET DATA e simplesmente não mantém nada. O endereço do servidor, a porta, o nome do ponto de acesso e o slot de chave vivem todos dentro da aplicação de administração. Apenas o fornecedor do cartão pode alterá-los.

Sempre envie uma instrução de controle ao lado de uma varredura GET DATA. Sem um controle, um resultado vazio não significa nada.

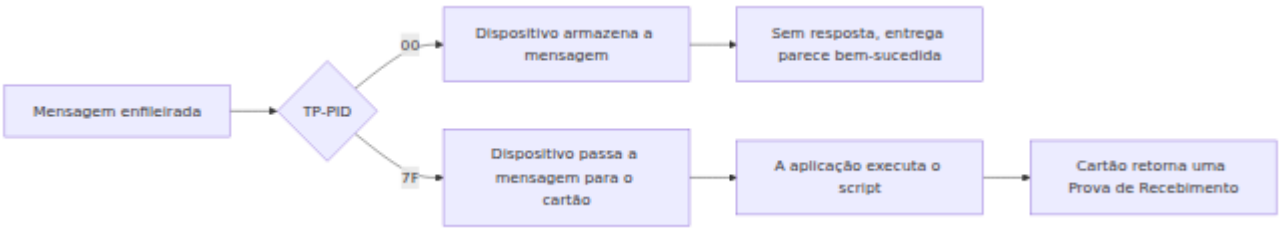
SMS OTA

A mensagem que o cartão aceita

O cartão aceita um pacote seguro padrão. Quatro propriedades devem estar corretas. Se alguma delas estiver errada, o cartão permanece em silêncio e a falha parece idêntica.

Propriedade	Valor	Por quê
TP-PID	`7F`	"(U)SIM Data Download". O dispositivo passa a mensagem para o cartão apenas para este valor. Veja 3GPP TS 23.048 §7.1.1.
TP-DCS	`F6`	Dados de 8 bits, classe de mensagem 2. A classe marca a mensagem como específica do cartão.
Cabeçalho de dados do usuário	`02 70 00`	Um elemento. O identificador `70` marca um Pacote de Comando.
Pacote seguro	TAR da aplicação alvo	O TAR seleciona qual aplicação executa o script.

Defina TP-PID como `7F`. Esta é a causa mais comum de uma mensagem entregue que não produz resposta. O dispositivo aceita uma mensagem com TP-PID `00` e um esquema de codificação de dados de classe 2. O dispositivo então arquiva a mensagem como armazenamento comum do cartão. A aplicação nunca é executada, e o cartão não retorna nada. O relatório de entrega ainda relata sucesso.



A Prova de Recebimento

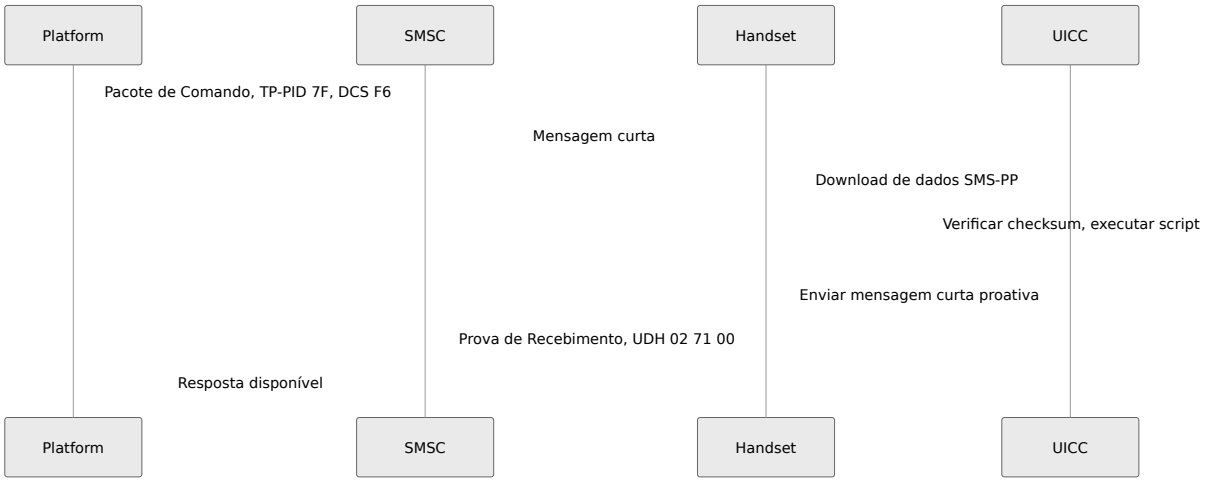
Defina o byte de Prova de Recebimento da indicação de parâmetro de segurança para que o cartão responda por mensagem originada pelo celular. O cartão então envia a resposta como uma mensagem curta normal. A resposta

chega ao SMSC que mantém o registro do assinante. Este não é sempre o SMSC que você enviou.

O cartão envia a Prova de Recebimento **para o endereço de origem do comando**. Defina o endereço de origem do comando para o endereço onde você deseja a resposta.

Uma Prova de Recebimento é reconhecível por um cabeçalho de dados do usuário de `02 71 00`. O identificador `71` marca um Pacote de Resposta.

A resposta carrega um código de status. O código de status é o diagnóstico mais valioso que o cartão fornece. Veja Códigos de status.



Contadores

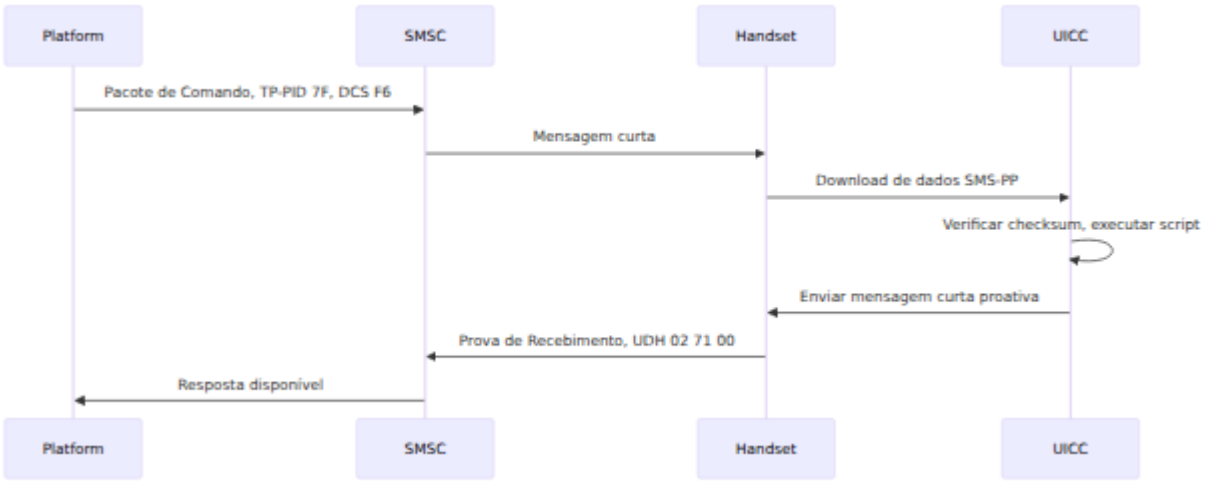
O cartão aceita qualquer valor de contador que seja maior do que o valor que ele mantém. O cartão nunca revela o valor que mantém. Abra o contador no momento atual como um número de segundos. O primeiro pacote é então aceito sem busca.

Um contador que é muito baixo retorna status `02`. Uma busca desperdiça tentativas do cartão, e falhas repetidas colocam um cartão em um atraso de nova tentativa.

HTTP OTA

O cartão abre a sessão de administração por conta própria. Você não pode acioná-la com uma mensagem curta, porque a aplicação de administração não mantém TAR.

Após a troca do perfil do terminal, o cartão inicia um temporizador de cerca de dois minutos. O cartão também se registra para os dois eventos de protocolo independente do portador. Quando o temporizador expira, o cartão pede ao dispositivo para abrir um canal.



O que o cartão pede

O comando de canal aberto nomeia tudo o que a sessão precisa.

Campo	Conteúdo
Endereço de destino dos dados	Um endereço IPv4 literal. O cartão não carrega um nome de host.
Nível de transporte	TCP, com o número da porta.
Nome de acesso à rede	O nome do ponto de acesso que o cartão usa.
Tamanho do buffer	O buffer do canal que o cartão deseja.

O cartão carrega um endereço IP, não um nome de host. O tag `3E` do ETSI TS 102 223 mantém apenas um endereço literal. O cartão nunca abre um canal para resolução de nomes. Portanto, você não pode mover o cartão para outro servidor alterando o DNS.

A sessão TLS

O cartão oferece TLS 1.1 e nenhuma versão posterior. O cartão oferece apenas suítes de cifra de chave pré-compartilhada. Ele não oferece nenhuma troca de chave efêmera.

Sirva TLS 1.1 em qualquer servidor ao qual esses cartões se conectem. A Emenda B do GlobalPlatform define TLS 1.1 como o mínimo. Bibliotecas TLS modernas deixam o TLS 1.1 de fora de sua lista de versões padrão. Um servidor que oferece apenas TLS 1.2 responde ao cartão com um alerta de versão de protocolo. O cartão nunca chega ao ponto em que apresenta sua identidade, então o log do servidor mostra uma falha na negociação e nada mais.

O cartão apresenta uma identidade na troca de chaves. A identidade é um prefixo fixo seguido pelo ICCID do cartão, em ASCII. Registre o prefixo contra o produto do cartão. Seu servidor resolve a identidade para a chave do cartão.

Executando um script

A sessão termina no domínio de segurança que mantém a chave. Um script enviado sem alvo é executado lá. Comandos de gerenciamento de conteúdo do cartão funcionam nesse domínio de segurança.

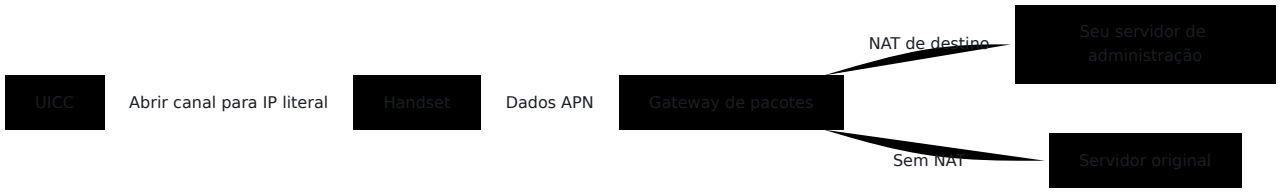
Para ler ou escrever arquivos, nomeie a aplicação de Gerenciamento de Arquivos Remotos no cabeçalho da aplicação alvo. O identificador da aplicação não é descobrível, pela razão dada em O que o cartão diz sobre si mesmo.

O cartão termina um script com uma palavra de status `61xx`. Uma resposta de get encadeada com um comprimento zero, portanto, nunca é executada. Pergunte uma vez, leia o comprimento que o cartão solicita, então pergunte novamente e nomeie esse comprimento.

Redirecionar a sessão de administração

Use este procedimento para mover a sessão de administração de um cartão para seu próprio servidor.

O cartão carrega um endereço IP literal, então você deve interceptar o tráfego no caminho de dados. Você não pode usar DNS.



Procedimento

1. Registre o endereço de destino e a porta do comando de canal aberto do cartão.
2. Registre o nome do ponto de acesso do mesmo comando. O cartão usa este APN, então aplique a regra nesse caminho de dados.
3. Adicione uma regra de tradução de endereço de destino no gateway de pacotes ou no firewall atrás dele. Traduza o endereço e a porta registrados para seu servidor de administração.
4. Configure seu servidor de administração conforme descrito em Requisitos do servidor.
5. Reinicie um cartão de teste. Aguarde o temporizador do cartão expirar.
6. Confirme a negociação no log do servidor. Confirme que o cartão apresenta a identidade esperada.

Planeje a transição antes de aplicar a regra. Após a regra estar ativa, a plataforma original não pode mais gerenciar esses cartões.

Requisitos do servidor

Requisito	Valor
Versão TLS	TLS 1.1 deve ser oferecido.
Suítes de cifra	Suítes de chave pré-compartilhada com AES-128 CBC e triple DES CBC.
Resolução de identidade	O servidor mapeia a identidade apresentada para a chave do cartão.
Aplicação alvo	Definida para gerenciamento de arquivos. Não é necessária para gerenciamento de conteúdo do cartão.
Formato de comando remoto	Expandido, comprimento definido.

Tabelas de referência

Códigos de status

O cartão retorna um desses códigos em cada Prova de Recebimento. Veja ETSI TS 102 225 para a lista completa.

Código	Significado	O que ele te diz
`00`	Prova de Recebimento OK	O script foi executado. Os dados de resposta contêm o resultado.
`01`	Falha de checksum	O cartão encontrou o conjunto de chaves e o algoritmo. O valor da chave está errado.
`02`	Contador muito baixo	Todos os outros parâmetros estão corretos. Aumente o contador.
`06`	Erro de segurança não identificado	O cartão não conseguiu resolver o conjunto de chaves ou não conseguiu ler o pacote.
`09`	TAR desconhecido	A aplicação não está instalada neste cartão.
`0A`	Nível de segurança insuficiente	O nível de segurança ou o algoritmo está abaixo do mínimo da aplicação.

Lendo os códigos

A diferença entre `01` e `06` é o sinal mais útil que o cartão fornece.

Envie uma sondagem com a cifra desligada. O cartão pode então ler o pacote, independentemente da chave de cifra que você usou. O cartão responde `01` para uma chave de checksum errada e `00` para a correta. Isso separa as duas chaves.

Não faça sondagens com a cifra ligada enquanto os parâmetros forem desconhecidos. Uma chave de cifra errada produz ruído. O cartão então responde `06`. Um conjunto de chaves errado e um algoritmo errado também produzem `06`. Uma resposta para três falhas diferentes oculta a causa.

Palavras de status dentro de um script

Palavra de status	Significado
`9000`	O comando foi bem-sucedido.
`61xx`	Dados estão disponíveis. O script para aqui.
`6A88`	O comando está implementado. O objeto não está mantido.
`6D00`	A instrução não é suportada.
`6E00`	A classe não é suportada.

Solução de problemas

Uma mensagem é entregue, mas o cartão não responde

Sintomas: O relatório de entrega relata sucesso. Nenhuma Prova de Recebimento chega. Um rastreamento do link para o dispositivo não mostra nada do cartão.

Possíveis causas:

- TP-PID não é `7F`. O dispositivo arquivou a mensagem como armazenamento do cartão.
- O esquema de codificação de dados não marca a classe da mensagem como 2.
- O cabeçalho de dados do usuário não carrega o identificador `70`.
- O byte de Prova de Recebimento não solicita uma resposta originada pelo celular.

Resolução:

1. Confirme que TP-PID é `7F` em um rastreamento da mensagem, não apenas no registro.
2. Confirme que o esquema de codificação de dados é `F6`.
3. Confirme que o cabeçalho de dados do usuário é `02 70 00`.
4. Confirme que a indicação de parâmetro de segurança solicita a resposta por mensagem originada pelo celular.

O cartão responde `06` para cada tentativa

Sintomas: Cada sondagem retorna status `06`, independentemente da chave ou conjunto de chaves que você usa.

Possíveis causas:

- A chave de cifra está errada, então o cartão lê ruído.
- A versão do conjunto de chaves não está instalada.
- O algoritmo não é o que a aplicação espera.

Resolução:

1. Envie uma sondagem com a cifra desligada.
2. Leia o novo código de status. `01` significa que o conjunto de chaves existe e a chave está errada.
3. Se o código ainda for `06`, mude a versão do conjunto de chaves e repita.

O cartão responde `0A`

Sintomas: Status `0A` para cada nível de segurança.

Possível causa: O algoritmo está abaixo do mínimo da aplicação. Um checksum de quatro octetos de uma única chave DES é um exemplo comum.

Resolução: Use triple DES, que produz um checksum de oito octetos.

A negociação TLS falha antes que o cartão apresente uma identidade

Sintomas: O log do servidor registra um alerta de versão de protocolo. O servidor não registra nenhuma identidade.

Possível causa: O servidor não oferece TLS 1.1.

Resolução: Adicione TLS 1.1 à lista de versões do servidor. Confirme que o servidor oferece uma suíte de cifra de chave pré-compartilhada que o TLS 1.1 suporta.

Um comando de arquivo retorna `6A82` ou não faz nada

Sintomas: Um select ou um read falha, ou o script para cedo.

Possíveis causas:

- O script direciona o domínio de segurança em vez da aplicação de gerenciamento de arquivos.
- O script alcançou uma palavra de status `61xx` e parou.

Resolução:

1. Defina a aplicação alvo como a aplicação de gerenciamento de arquivos.
2. Substitua uma resposta de get encadeada de comprimento zero pelo comprimento que o cartão solicita.

P-CSCF: Função de Controle de Sessão de Chamada Proxy

O **P-CSCF** (Função de Controle de Sessão de Chamada Proxy), o **OmniCSCF** da Omnitouch em seu papel de proxy, é o **primeiro ponto de contato IMS para o dispositivo de um assinante**. Cada mensagem SIP que um UE envia para o IMS entra e sai do núcleo através do P-CSCF: seu **REGISTER** inicial, cada **INVITE** de chamada e cada **SUBSCRIBE** para presença ou espera de mensagem. Ele está na borda do domínio de confiança: estabelece as **associações de segurança IPsec** que protegem a sinalização para e do dispositivo, encaminha registros para o **I-CSCF/S-CSCF** e, no caminho de mídia, autoriza recursos de portadora para cada chamada através da interface **Rx** em direção ao controle de políticas (TS 23.228). O OmniWeb exibe os contatos registrados que está ancorando, sua política e integração com o 5G-NRF, e o estado de execução do mecanismo SIP subjacente.

← Guia de Operações

O painel é uma página de elemento por instância acessada a partir da barra lateral quando um P-CSCF está em execução no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API de gerenciamento do P-CSCF, portanto, permanece atrás do único gateway autenticado. Um link de documentação no cabeçalho da página fornece ajuda em contexto. A página é organizada em abas.

Visão Geral

Uma leitura de saúde de tela única do P-CSCF: a versão do **mecanismo SIP** e o tempo de atividade, o número de **contatos** que está atualmente ancorando (UEs registrados vinculados a este proxy), a contagem de **associações de segurança IPsec** ativas e o número de **diálogos** abertos (chamadas e outras transações em andamento). É a confirmação mais rápida de que o proxy está ativo e atendendo sua parte da população de assinantes.

Contatos

Os **UEs registrados** que o P-CSCF está ancorando, retirados de seu armazenamento de localização de usuário. Cada linha é um **Endereço de Registro (AoR)**, a identidade pública de um assinante, como `sip:001001000010001@ims.mnc001.mcc001.3gppnetwork.org`, com o **contato** que o dispositivo registrou (seu IP, porta e transporte), a string do **user agent** que apresentou e a **expiração** do registro. Como o P-CSCF termina a segurança do lado de acesso, o vínculo também carrega os parâmetros de **IPsec** negociados com o dispositivo. Esta é a maneira mais rápida de confirmar que um determinado assinante está registrado e ver o dispositivo e o caminho da rede que sua sinalização está utilizando.

NRF

A integração do P-CSCF com o **Núcleo 5G**. Em uma implantação convergente, o P-CSCF se registra no **NRF** (Função de Repositório de Rede) como uma **Função de Aplicação (AF)** e usa o **BSF** (Função de Suporte de Vinculação) para descobrir qual **PCF** está atendendo um determinado UE antes de autorizar mídia pelo caminho **N5/Rx**. Esta aba mostra:

- **Registro**: se o P-CSCF está **REGISTRADO** no NRF, seu **ID de instância NF** e **tipo NF** (`AF`), o NRF com o qual se registrou, o intervalo de **heartbeat** e a idade do último heartbeat, e quaisquer **falhas de registro/heartbeat**.
- **Descoberta**: o **endpoint BSF** atualmente descoberto e por quanto tempo essa descoberta é válida; até que uma descoberta tenha sido realizada, isso lê *não descoberto*.
- **Vínculos recentes**: as últimas consultas **UE → PCF**, que mapeiam a identidade IMS de um assinante e IP para o URI do **PCF** que lidará com sua política.

Daqui você pode solicitar que o P-CSCF **re-registre no NRF** ou **descubra o BSF** sob demanda. Isso é útil após uma reinicialização do núcleo ou quando

você valida uma nova integração 5G.

Diameter

A conectividade **Diameter** do P-CSCF: seu emparelhamento **Rx** em direção ao controle de políticas (o PCRF em uma implantação EPC, ou o PCF alcançado via a interconexão Rx-para-N5 em uma implantação 5G). Cada linha mostra o **host** de um par, **domínio**, a **aplicação Diameter** em uso e o **estado de conexão**. Rx é como o P-CSCF solicita à camada de políticas que autorize e controle a portadora de mídia para cada chamada VoLTE/VoNR, portanto, um par que está inativo aqui significa que as chamadas podem se registrar, mas falham em obter recursos de mídia.

Tabelas de Hash

As **tabelas de hash em memória** do mecanismo SIP: o estado de trabalho que o P-CSCF mantém para limitação de taxa, anti-flood e contabilidade de autenticação. Cada linha é uma tabela nomeada (por exemplo, uma tabela de **banimento IP** para fontes bloqueadas, ou uma tabela de **auth** para desafios em andamento) com sua **contagem de slots**, **auto-expiração** e o número de **entradas ativas**. É uma visão diagnóstica para entender o que o proxy está rastreando atualmente e para detectar uma tabela se enchendo sob ataque ou má configuração. Tabelas individuais podem ser inspecionadas em mais detalhes a partir daqui.

Sistema

A execução de baixo nível do mecanismo SIP por trás do P-CSCF: alocação de **memória compartilhada** (total, usada e livre, com fragmentação), o pool de conexões **TCP** e sua capacidade, os **sockets de escuta** aos quais o proxy está vinculado (UDP/TCP/TLS nas portas SIP), os nós de replicação **DMQ** com os quais compartilha estado, e seus contadores de **transação** e **resposta sem estado** divididos por classe de resposta (2xx/3xx/4xx/5xx/6xx). É onde você confirma que o mecanismo está saudável sob carga e tem margem, e onde um problema de memória ou socket aparece primeiro.

Logs

A aba **Logs** exibe a saída de log ao vivo do P-CSCF. Solucione problemas de uma única instância sem sair do OmniWeb: um registro falho, um problema de negociação IPsec ou um INVITE rejeitado.

Painéis de monitoramento

As taxas de transação SIP, contagens de registro e throughput de autorização de mídia para o P-CSCF são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **I-CSCF**: o P-CSCF encaminha o REGISTER inicial de um UE para a rede doméstica, onde o I-CSCF consulta o HSS para selecionar um S-CSCF em serviço.
- **S-CSCF**: ancla o registro e aplica a lógica de serviço do assinante; o P-CSCF permanece no caminho de sinalização para cada solicitação subsequente.
- **PGW-C / PCRF / PCF**: a camada de políticas que o P-CSCF alcança através do **Rx** (e, no 5G, descobre via **NRF/BSF** na aba NRF) para autorizar a mídia da chamada.
- **ePDG** e **PGW-C**: estabelecem a portadora APN IMS pela qual a sinalização SIP protegida do UE trafega.
- Guia de Operações: voltar ao índice de elementos.

PGW-C: Gateway PDN (Plano de Controle)

O **PGW-C** é a metade do plano de controle do **Gateway PDN** do EPC. Ele é o ponto de ancoragem para cada sessão de dados de assinante: termina **S5/S8** para o SGW-C, configura e mantém cada **conexão PDN**, aloca ao UE seu endereço IP de um **pool IP** do operador e seleciona e controla o plano do usuário (**UPF**) sobre **Sx/PFCP**. Ele também executa a política e a cobrança da sessão sobre Diameter: **Gx** para o PCF/PCRF para política e QoS, e **Gy** para o OCS para cobrança online. Ele também gera **CDRs** para cobrança offline. No núcleo 5G, a função equivalente é o **SMF**. O OmniWeb exibe as sessões ativas do PGW-C, pools IP, UPF e pares Diameter, um mapa de topologia e histórico de sessões, além de ferramentas de diagnóstico. Os painéis do Grafana acessados a partir da mesma página contêm as tendências de longo prazo.

← Guia de Operações

O PGW-C é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, com uma visão de frota onde vários estão implantados. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do PGW-C, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda contextual) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status da API** do PGW-C e um resumo de seu estado ativo (contagem de sessões ativas, utilização do pool IP, pares UPF e pares Diameter). É a maneira mais rápida de confirmar que o nó está ativo e gerenciando sessões.

Sessões

Cada sessão PGW ativa, cada linha identificada pelo **IMSI** e **MSISDN** do assinante com seu **IP UE** e **APN** atribuídos. As sessões podem ser pesquisadas por IMSI, IP UE, MSISDN ou APN. Abrir uma sessão mostra seu estado completo: a conexão PDN e bearers, o SGW que está servindo e o UPF selecionado, e o contexto de política e cobrança Gx/Gy ativo. Você pode editar uma sessão aqui. Um operador pode ajustar o estado ativo, como o **AMBR** da sessão (que empurra um novo APN-AMBR para o UPF) e os **gatilhos de eventos Gx** solicitados que controlam o relatório de mudança de localização. Um operador também pode **excluir** uma sessão para liberar forçosamente um assinante preso ou com mau comportamento. Como o operador aplica edições diretamente ao estado ativo, elas têm efeito imediato.

Onde vários PGW-Cs estão implantados, a mesma aba na **visão de frota** lista cada sessão entre todos eles em uma tabela, com o PGW-C que está servindo mostrado contra cada linha. A pesquisa é passada para cada instância, então um operador pode encontrar um assinante sem saber qual PGW-C está ancorando-o; abrir uma linha vai para essa sessão em sua própria instância. Uma instância que não pode ser alcançada é nomeada acima da tabela, então uma lista curta nunca é confundida com uma rede silenciosa.

Pools IP

Os pools IP do operador dos quais o PGW-C aloca endereços UE, cada um mostrando seu **tamanho**, contagem **alocada** e **utilização**. Abrir um pool lista os endereços alocados individualmente. Aqui você confirma que um pool não está esgotado (um pool esgotado é uma causa comum de falhas na configuração de sessões) e vê qual assinante possui um dado endereço.

Pares UPF

Os pares do plano do usuário (UPF) que o PGW-C controla sobre **Sx/PFCP**, cada um mostrando seu **endereço IP** e **estado de associação** PFCP. Abrir um par mostra seus detalhes. É aqui que você confirma que as associações PFCP que transportam o plano do usuário de cada sessão estão ativas.

Diameter

Os pares Diameter com os quais o PGW-C se comunica (o **PCF/PCRF** sobre **Gx** para política e o **OCS** sobre **Gy** para cobrança online), cada um com seu **hostname** e **estado de conexão**. Abrir um par mostra seus detalhes. Quando sessões estão sendo rejeitadas ou limitadas, aqui você confirma que os caminhos de política e cobrança estão ativos.

Histórico

Um log pesquisável e paginado de **eventos** do ciclo de vida da sessão: *criado*, *modificado*, *excluído*, *transferência* e *falha*. Você pode filtrar eventos por tipo e pesquisá-los por IMSI, MSISDN, endereço IP ou TEID. Aqui você reconstrói o que aconteceu com a sessão de um assinante específico ao longo do tempo, incluindo falhas.

Topologia

Um mapa do PGW-C e os vizinhos com os quais ele trabalha: os SGWs para os quais ele ancla sessões, os UPFs que ele controla e seus pares Diameter. Ele fornece uma visão única de quais vizinhos de sinalização e plano do usuário o nó está conectado.

Seleção de UPF

As regras que decidem qual UPF uma nova sessão é colocada, juntamente com o **status de saúde** atual de cada UPF candidato e a configuração de **PCO** (Opções de Configuração de Protocolo) que o PGW-C retorna ao UE. É aqui que você confirma por que as sessões estão sendo alocadas em um UPF específico e verifica se todos os candidatos estão saudáveis.

Pesquisa de UE

Uma pesquisa direta de um único assinante por **IMSI**, **MSISDN** ou **endereço IP**, retornando as informações desse UE no PGW-C. É a maneira mais rápida de encontrar a sessão de um assinante sem rolar pela lista completa de Sessões.

Cobrança

O estado de **cobrança online (Gy/OCS)** ativo de cada sessão, cada linha identificada por **IMSI** e **MSISDN** e pesquisável por qualquer um deles. À primeira vista, cada sessão mostra se a cobrança online **Gy** está ativada (com seu **id da sessão**, e o **host OCS** e **domínio** com os quais se comunica), se a contabilidade **offline (Gz)** também está em execução, e se o OCS empurrou o assinante para um redirecionamento de **jardim murado**. Abrir uma sessão expande seu detalhe completo de cobrança: as cotas **concedidas** por URR contra o volume **utilizado** (uplink, downlink e total de octetos), a **ação de unidade final** que o OCS definiu para quando o crédito acabar, os contadores offline (Gz) e qualquer alvo de redirecionamento. É assim que você lê o estado de controle de crédito ativo de um assinante: se eles têm crédito, quanto de sua concessão consumiram e por que podem ter sido limitados ou redirecionados.

Quebrar vidro: suspender cobrança online. No topo da aba está um interruptor de nível de nó que suspende a cobrança online em todo o PGW-C. Use-o quando o OCS não puder responder e os assinantes, de outra forma, perderiam o serviço.

Enquanto o interruptor estiver armado, o PGW-C não envia CCR-I na conexão e nenhum CCR-U nas sessões ativas. Ele libera jardins murados e desbloqueia bearers bloqueados, para que o tráfego seja transportado sem a autorização do OCS. A cobrança offline não é afetada: o uso ainda é registrado em CDRs e pode ser avaliado posteriormente.

Para armar o interruptor, forneça duas coisas:

Campo	Obrigatório	Descrição
Suspender por	Sim	Quanto tempo o interruptor permanece armado. Ele se desarma quando o tempo se esgota. O nó define o maior valor que aceita.
Razão	Sim	Por que a cobrança está suspensa. É registrada contra a sobreposição.
Armado por	Não	Quem armou. O padrão é seu endereço.
Enviar um CCR-T Gy na desconexão	Não	Desligado por padrão. Ative para relatar uso que o OCS nunca autorizou.

Dê uma razão real. A razão e o operador são registrados, e eles sobrevivem ao turno que armou o interruptor.

O painel mostra o tempo restante enquanto o interruptor está armado. Pressione **Retomar cobrança** para desarmá-lo imediatamente. O interruptor também se desarma quando seu tempo se esgota, o que impede que uma sobreposição esquecida se torne um serviço gratuito permanente.

CDRs

Os **registros de cobrança** offline que o PGW-C escreve para faturamento: uma linha por evento de **início**, **intermediário** e **parada** da sessão, mais recente primeiro, e filtrável por **IMSI** ou **MSISDN**. Cada registro contém o **IMSI**, **MSISDN** e **IMEI** do assinante, o **APN** e **QCI**, o **id de cobrança** que liga os registros de uma sessão, os **octetos de uplink/downlink** contados para aquele intervalo, os endereços IP do **S-GW**, **PGW** e **UE**, e o **arquivo de origem** do qual o registro foi lido. Aqui você reconcilia o uso de dados de um assinante contra a contabilidade offline (Gz) que o operador fatura, e rastreia em qual arquivo de registro uma sessão específica foi registrada.

Teste Gy

Uma ferramenta para operadores que emite um **Gy Credit-Control-Request** contra o OCS para validar o caminho de cobrança online de ponta a ponta. Você fornece um **IMSI** (e opcionalmente um MSISDN e uma contagem de octetos solicitados/utilizados) e escolhe o tipo de solicitação. Use **Inicial (CCR-I)** para abrir uma sessão e solicitar unidades, **Atualizar (CCR-U)** para relatar uso e pedir mais, ou **Terminar (CCR-T)** para relatar o uso final e fechá-la. Em seguida, envie. O PGW-C define por padrão o grupo de classificação, Service-Context-Id e Auth-Application-Id. A **Credit-Control-Answer** analisada retorna na mesma tela. Ao contrário das outras abas, esta **não busca nada ao carregar**: é um formulário que você envia. Quando a cobrança online está com mau comportamento, é a maneira mais rápida de provar que o OCS está acessível e concedendo crédito.

Monitor P-CSCF

O status e as métricas do monitor de descoberta P-CSCF. O PGW-C retorna um endereço P-CSCF para dispositivos VoLTE durante a configuração da PDN, e esta aba confirma que a descoberta está saudável para que o registro IMS possa prosseguir.

Logs

A aba **Logs** acompanha a saída do log ativo do PGW-C para solucionar problemas de um único nó (falhas na configuração de sessões, erros PFCP e Diameter) sem sair do OmniWeb.

Monitoramento

Tendências de contagem de sessões, throughput e outras séries temporais para o PGW-C são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **SGW-C** é o par de controle sobre **S5/S8**; ele ancla os bearers do lado de acesso que o PGW-C conecta à PDN.
- O **UPF** é o plano do usuário que o PGW-C seleciona e controla sobre **Sx/PFCP**.
- O **PCF/PCRF** fornece política e QoS sobre **Gx**.
- O **CHF/OCS** realiza cobrança online sobre **Gy**; o PGW-C também gera CDRs para cobrança offline.

RAN Monitor: Nokia Rede de Acesso Rádio OSS

O **RAN Monitor** é o elemento OSS/monitoramento da Omnitouch para a **rede de acesso rádio Nokia**, as estações base que carregam a interface de ar para a rede central que o OmniWeb gerencia. Ele se comunica com as estações base **MRBTS** (AirScale) da Nokia através da interface de gerenciamento NE3S da Nokia. Ele coleta contadores de desempenho, alarmes e configurações de cada site conectado e os armazena em um banco de dados de séries temporais para análise de tendências. A partir de uma tela, um operador vê a saúde da frota, plota os sites em um mapa, trabalha com alarmes ativos, navega pelo catálogo de equipamentos, inspeciona a construção lógica e física de qualquer estação base, arquiva configurações de dispositivos, gerencia firmware em toda a frota e observa os rastros de assinantes e células sendo transmitidos. Em resumo, é a janela para a camada de rádio abaixo do núcleo de pacotes: o contraparte da visão do MME dos mesmos eNodeBs do lado do plano de controle.

← Guia de Operações

O RAN Monitor é uma página de elemento por instância acessada a partir da barra lateral quando um monitor está em execução no inventário do site. Onde vários estão implantados, ele também oferece uma visão da frota para status agregado. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do monitor, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde de tela única de toda a frota. Os cartões de status dividem as estações base por **estado de registro**: **registrado** (conectado e reportando), **pendente** (meio registro) e **não registrado** (offline ou inacessível). Um operador vê à primeira vista quanto da propriedade de rádio está ativa. Abaixo deles, um resumo de ingestão confirma que o banco de dados de séries temporais está conectado e mostra quantos pontos de **métrica de desempenho**, **configuração** e **alarme** ele atualmente possui. Um banner de aviso exibe quaisquer unidades **não provisionadas**: estações base que se conectaram, mas não possuem configuração de rádio e ainda não podem servir tráfego.

A tabela pesquisável lista cada estação base com seu nome, endereço de gerenciamento, estado de registro, status **BTS** ao vivo (`connected`, `active`, `waiting_for_pm`, `pending`), contagem de alarmes ativos e versão de software em execução. Você pode pesquisar uma estação base pelo nome, e abrir uma linha detalha o contexto completo daquela unidade: sua topologia, células, alarmes e contadores armazenados. É a confirmação mais rápida de que o monitor está ativo e de quanto da rede de rádio está sendo monitorada.

Mapa

Um mapa geográfico da frota. Cada estação base é plotada em sua localização armazenada e desenhada com **feixes de setor** espalhados nas direções das antenas, tiradas dos dados de inclinação elétrica remota (RET), coloridos pela banda de frequência que cada célula atende, para que o layout de cobertura de um site seja lido à primeira vista. A cor do marcador reflete a saúde do site: verde quando registrado e claro, âmbar quando pendente, e vermelho quando o site tem alarmes ativos.

Clicar em um site abre um popup com seu endereço, status BTS, fornecedor, versão de software, contagem acumulada de métricas de desempenho e lista de células, com um link direto para a página completa do dispositivo. As estações base **não provisionadas** são mostradas como marcadores cinzas distintos para que se destaquem da propriedade provisionada, e uma sobreposição de cobertura de sinal com uma leitura estimada de RSRP ao clicar ajuda a relacionar os setores plotados com o alcance no mundo real. É a maneira mais rápida de ver onde a rede de rádio fisicamente está e quais sites estão em problemas.

Alarmes

Todo alarme ativo levantado em toda a frota, coletado das estações base Nokia e deduplicado no banco de dados de séries temporais. Cartões de resumo contam o total e o dividem por **severidade**: **crítico**, **maior**, **menor** e **aviso**. Um resumo por site agrupa os alarmes pela estação base que os levantou, para que um operador possa imediatamente ver quais sites estão mais barulhentos e pular para os detalhes de um site a partir do agrupamento.

A tabela completa lista cada alarme ativo com seu chip de severidade, o site que levantou e o texto e identificadores do alarme que a estação base reportou. A visualização pode ser filtrada por site, por severidade e por pesquisa de texto livre para restringir uma tempestade aos alarmes que importam. Quando a frota está limpa, a aba diz isso explicitamente. É aqui que um operador triage um defeito: começa pela mistura de severidade, encontra o site ofensivo e o segue para o contexto daquela estação base.

Coleta de Rastro

O pipeline de rastreamento de assinantes e células. As estações base Nokia transmitem tráfego de rastreamento para o monitor, que termina a coleta e a correlaciona. O topo da aba mostra o **alvo de rastro** configurado (o endereço e a porta para os quais as estações base enviam, editável no local), o número de conexões de rastro ativas e as portas do ouvinte em uso. Abaixo disso, uma tabela lista cada estação base conectada com seu endereço de origem, estado de conexão, contagem de pacotes e tempo de conexão, para que um operador possa confirmar quais sites estão realmente alimentando o rastro.

O painel inferior expõe os resultados correlacionados em três visualizações: **Sessões** (trabalhos de rastreamento individuais), **UEs** (os assinantes vistos no rastreamento) e **Mensagens** (os registros de sinalização decodificados). Você pode limpar todo o armazenamento de rastros uma vez que uma investigação esteja concluída. É assim que um rastro em nível de assinante ou célula é capturado e inspecionado sem tocar na própria CLI da estação base.

Banco de Dados de Equipamentos

Um catálogo pesquisável de produtos de rádio e hardware da Nokia, dividido em dois localizadores. **Radio Finder** lista unidades de rádio (RMODs) por código de produto e nome, com sua variante, modo duplex (FDD/TDD), tecnologias suportadas (GSM/WCDMA/LTE/NR), frequência e cobertura de banda EUTRA/NR, potência de transmissão, largura de banda máxima e contagem de portadoras, e tipo de interface CPRI/eCPRI; os resultados podem ser filtrados por tipo, modo duplex, tecnologia e interface, e uma linha se expande para a ficha técnica completa do rádio. **Hardware Finder** faz o mesmo para módulos de sistema e banda base (SMODs/BBMODs) e outros hardwares, indexados por código de produto com suas tecnologias suportadas e tipo de interface.

O catálogo é dados de referência em vez de estado de frota ao vivo. Ele permite que um operador identifique o que é um código de produto, verifique o que um determinado rádio suporta antes de ser implantado e faça a referência cruzada dos módulos que aparecem na topologia e nas visualizações de encanamento de um site contra suas capacidades publicadas.

Topologia do Site

A construção lógica de uma única estação base. Depois de selecionar uma estação base, a aba desenha seu **MRBTS** como um diagrama: o armário interno com seus **módulos de sistema (SMODs)** e **módulos de banda base (BBMODs)**, os **links CPRI/eCPRI** que vão para os **módulos de rádio (RMODs)** externos, e as **células** que cada rádio atende, com estado operacional por módulo, códigos de produto e números de série. Ao lado do diagrama, ele exibe as antenas de **inclinação elétrica remota (RET)** do site (indicando qualquer desvio de inclinação entre os valores configurados e reais), os **MMEs** conectados e seu status de link S1, as interfaces **Ethernet**, endereçamento IP de transporte, fonte de relógio/sincronização, status de energia e refrigeração, e um inventário consolidado de números de série.

É a tela única para entender como um site é montado e confirmar que cada módulo está habilitado e saudável: o companheiro lógico do Diagrama de Encanamento físico.

Diagrama de Encanamento

A fiação física de uma estação base: como a fibra e RF realmente correm. Para o site selecionado, ele desenha um esquema interativo dos módulos de banda base/sistema do armário ao longo das **execuções de fibra CPRI/eCPRI** (com as portas SFP de cada execução, comprimento da fibra e velocidade do link, incluindo cadeias em série RMOD para RMOD e links de backplane do armário) para os módulos de rádio, e a partir de cada porta de **antena** de rádio (mostrando direção (TX/RX/TRX) e perda de alimentador) até as células que eles alimentam. Clicar em um rádio ou uma célula destaca toda a cadeia que a serve, e o diagrama se move e amplia.

Abaixo do diagrama, desagregações por setor e cronogramas imprimíveis apresentam as mesmas informações em forma de tabelas: um **cronograma de fibra** de cada execução CPRI com seus pontos finais, comprimento, velocidade e estado, um **cronograma de porta RF** mapeando cada porta de antena para sua direção, perda e célula atendida, e os links de backplane. Esta é a visualização que um instalador ou planejador usa para verificar se um site foi cabeado conforme projetado e para rastrear um defeito de hardware de volta a uma fibra ou alimentador específico.

Arquivo de Configuração

Um arquivo de configurações de dispositivos extraído das estações base. A tabela de dispositivos mostra cada estação base com o número de versões de configuração mantidas para ela e quando foi arquivada pela última vez. Selecionar uma estação base lista suas versões armazenadas com o timestamp, nome do arquivo e tamanho de cada versão. Você pode baixar qualquer versão, ou a mais recente para um dispositivo.

Manter um histórico da configuração de cada site dá ao operador um registro para comparar uma construção ao vivo, para ver quando uma configuração foi alterada pela última vez e para recuperar uma configuração conhecida como boa se uma mudança precisar ser revertida.

Firmware

O inventário de versões de software da Nokia disponível para a frota, além das ações de ciclo de vida que o aplicam. Cartões de resumo contam as imagens de firmware mantidas e seu tamanho total. A tabela lista cada imagem pelo nome do arquivo com seus metadados analisados (versão de software, lançamento, compilação e as unidades de hardware que ele visa), seu tamanho e tempo de modificação, e uma ação de download.

A partir de uma imagem, um operador pode **instalá-la** em uma estação base escolhida: a instalação baixa a imagem para o BTS e, se a ativação for solicitada, troca a unidade para o novo software e a reinicia (ou apenas prepara a imagem quando a ativação é deixada de fora). Uma ação de **reversão** ativa o banco de software passivo de uma estação base e a reinicia para retornar à compilação anterior. Como uma instalação ou reversão baixa, ativa e reinicia o BTS, pode levar vários minutos; o progresso e o resultado do trabalho são consultados e relatados ao vivo em um banner de status. É aqui que o ciclo de vida do software da frota de rádio é gerenciado sem sair do OmniWeb.

Não Provisionados

As estações base que o monitor viu na rede que não correspondem a um site configurado e provisionado. Estas são tipicamente unidades que se conectaram via re-registro, mas não possuem configuração de rádio porque estão em padrão de fábrica ou foram apagadas. Cada uma é listada com a identidade e o endereço que apresentou, e a aba avisa claramente que essas unidades precisam de uma configuração aplicada antes que possam servir tráfego.

Este é o apanhado que impede que uma estação base recém-conectada ou re-imaginada passe despercebida: um operador observa esta aba (e os marcadores correspondentes no Mapa) para encontrar unidades aguardando provisionamento e trazê-las para a propriedade gerenciada. Quando não há nenhuma, a aba confirma que cada BTS conectado possui configuração de rádio.

Sistema

A saúde do próprio backend do monitor: como o OSS em si está funcionando, em vez das estações base que ele observa. Ele coleta várias visualizações operacionais. **Métricas do Sistema** reporta o pipeline de ingestão: o escritor em lote alimentando o banco de dados de séries temporais (profundidade da fila, contagem de flush, total de pontos escritos, tempo desde o último flush) e estatísticas de escrita por estação base que sinalizam qualquer AirScale cujos dados se tornaram **obsoletos**, juntamente com o uso de memória e recursos de processo do próprio backend. **Banco de dados de séries temporais** mostra o estado de conexão do armazenamento, versão e as contagens de medições que ele possui para métricas de desempenho, configuração e alarmes.

Contadores PM gerencia quais **contadores de gerenciamento de desempenho** da Nokia o monitor mantém: as estações base reportam um conjunto de contadores muito grande, e este filtro seleciona os contadores que valem a pena armazenar para que o banco de dados de séries temporais não seja inundado. Você pode adicionar contadores armazenados de, ou removê-los contra, o catálogo completo disponível, pesquisável por nome e categoria. **Retenção** define quanto tempo os dados coletados são mantidos, globalmente

e por estação base, com contagens de registros por dispositivo e limpeza manual, para que o crescimento do armazenamento permaneça contido. **Gerenciamento de dados** expõe os caches em tempo de execução e arquivos temporários que o backend mantém, com controles para limpá-los ou purgar as séries armazenadas de um dispositivo. Juntas, esta aba é onde um operador confirma que o monitor está ingerindo, filtrando, retendo e armazenando dados de forma saudável.

Logs

A aba **Logs** acompanha a saída de log ao vivo do RAN Monitor para solucionar problemas de uma única instância sem sair do OmniWeb.

Painéis de Monitoramento

Tendências de contadores de desempenho, taxas de alarmes e throughput de ingestão para o RAN Monitor são apresentados como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos de séries temporais nativamente. As séries por contador que os painéis utilizam são exatamente aquelas selecionadas no filtro de contadores PM da aba Sistema.

Relacionados

- **MME**: o contraparte do plano de controle. O MME mantém a visão S1AP dos mesmos eNodeBs (estações base) que o RAN Monitor observa do lado OSS, e os MMEs conectados de cada site e seu status de link S1 aparecem na aba Topologia do Site.
- **RAN Simulator**: levanta eNodeBs e UEs virtuais para exercitar o núcleo sem hardware, complementando a visão do RAN Monitor sobre as reais estações base Nokia.
- **HSS**: mantém os dados de assinatura e autenticação para os assinantes que se conectam através dos sites de rádio, e que aparecem na visualização de UE da Coleta de Rastro do monitor.

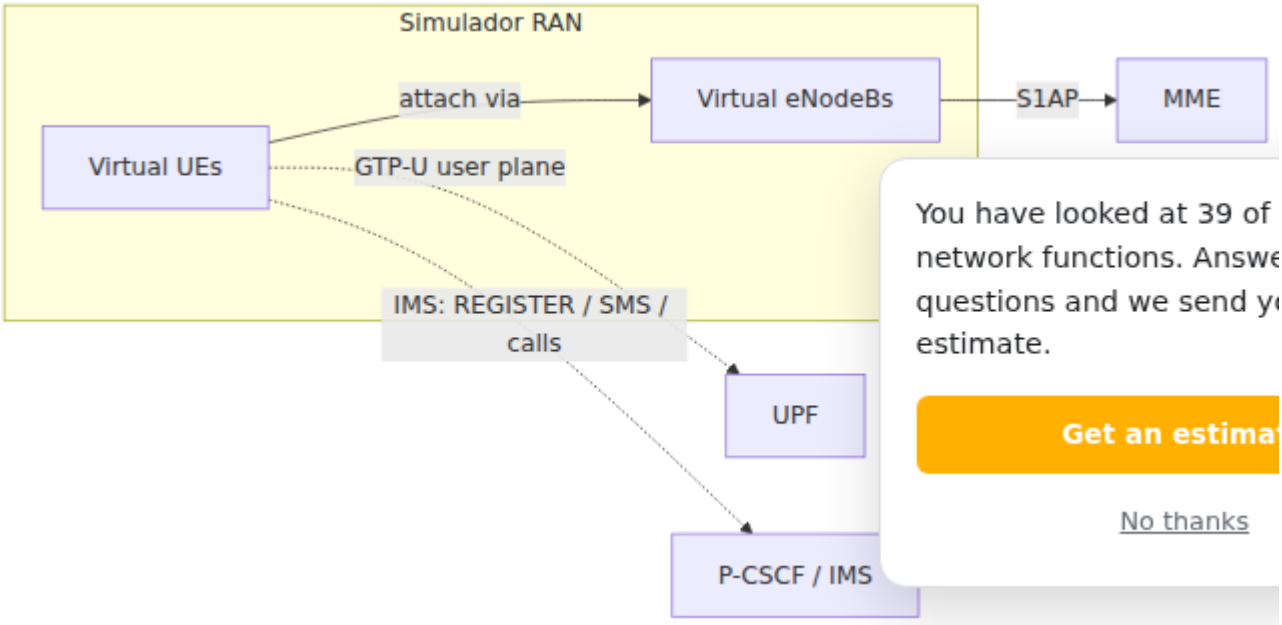
- Guia de Operações: de volta ao índice de elementos.

Simulador RAN

O **Simulador RAN** permite que você exercite uma rede central ao vivo sem rádios ou dispositivos físicos. Ele configura **eNodeBs** e **UEs** virtuais que se comunicam com o MME via S1AP/NAS e com os gateways via GTP-U, para que você possa realizar anexos, sessões de dados, registros IMS, SMS e chamadas. Use-o para testes funcionais, testes de carga ou para reproduzir cenários de campo, tudo a partir do OmniWeb.

← Guia de Operações

O Que É



O simulador roda ao lado da rede central que ele visa. No OmniWeb, ele aparece como uma área própria de **Simulador RAN** (Mapa da Rede, eNodeBs, UEs, IMS, Teste de Carga, Cronogramas de Cenário). Como um UE simulado se comporta como um dispositivo, seus UEs também aparecem em **Dispositivos de Teste** para que você possa controlá-los do mesmo lugar que os dispositivos reais.

Por padrão, ele começa com **nenhum eNodeB**. Você configura exatamente a topologia que deseja.

eNodeBs

Configurar um eNodeB o conecta ao MME (Configuração S1). Um eNB pode estar conectado a **mais de um MME** (um pool de MME). O Mapa da Rede mostra o conjunto completo de MMEs ao qual um eNB está associado.

A configuração é **fire-and-forget**: o OmniWeb pede ao simulador para ativar o eNB e retorna; o link S1 é estabelecido em segundo plano (observe o Mapa da Rede / lista de eNodeBs para confirmar que ele foi ativado).

Desconectando um eNodeB

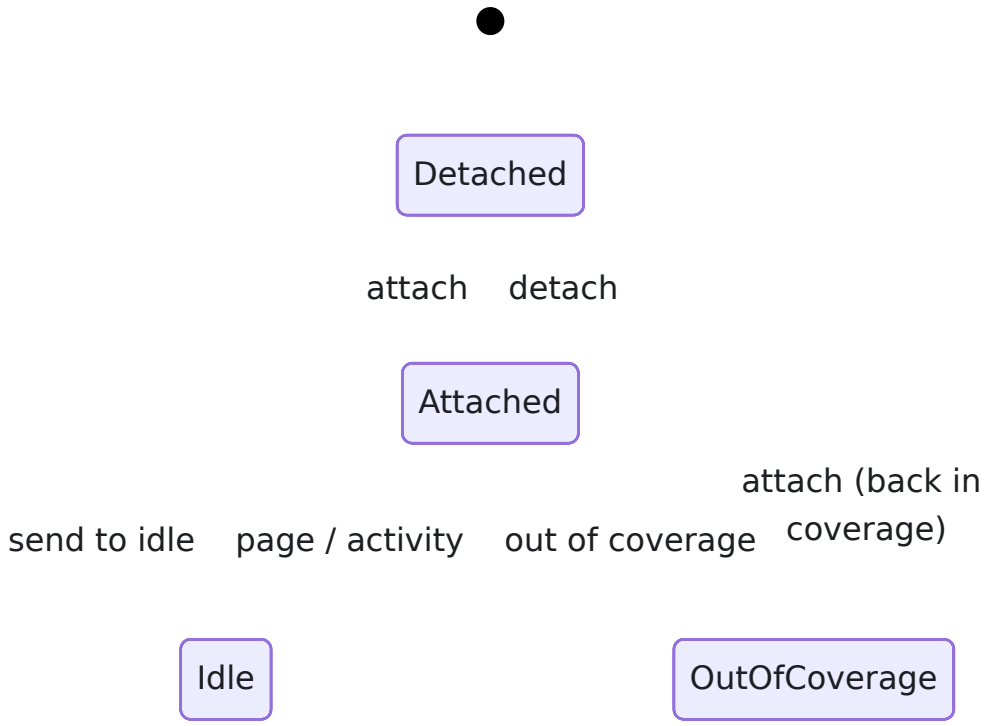
Você pode desativar um eNB de duas maneiras, que modelam diferentes eventos do mundo real:

Ação	Modelos	Efeito nos UEs
Desconexão S1 limpa	Um desligamento ordenado do eNB / redefinição S1	UEs são liberados de forma limpa e **sobrevivem**. Eles se reanexam quando um link está disponível
Queda de link	O eNB perdendo abruptamente seu S1 (corte de fibra, perda de energia)	A associação S1 é abortada; UEs **sobrevivem** à saída do eNB e se reanexam em vez de serem desconectados

Criticamente, desativar um eNB **não** destrói seus UEs. Os UEs persistem e se reanexam, permitindo que você simule interrupções de transporte sem reconstruir sua frota de assinantes.

UEs

Cada UE simulado tem um ciclo de vida que você pode controlar diretamente:

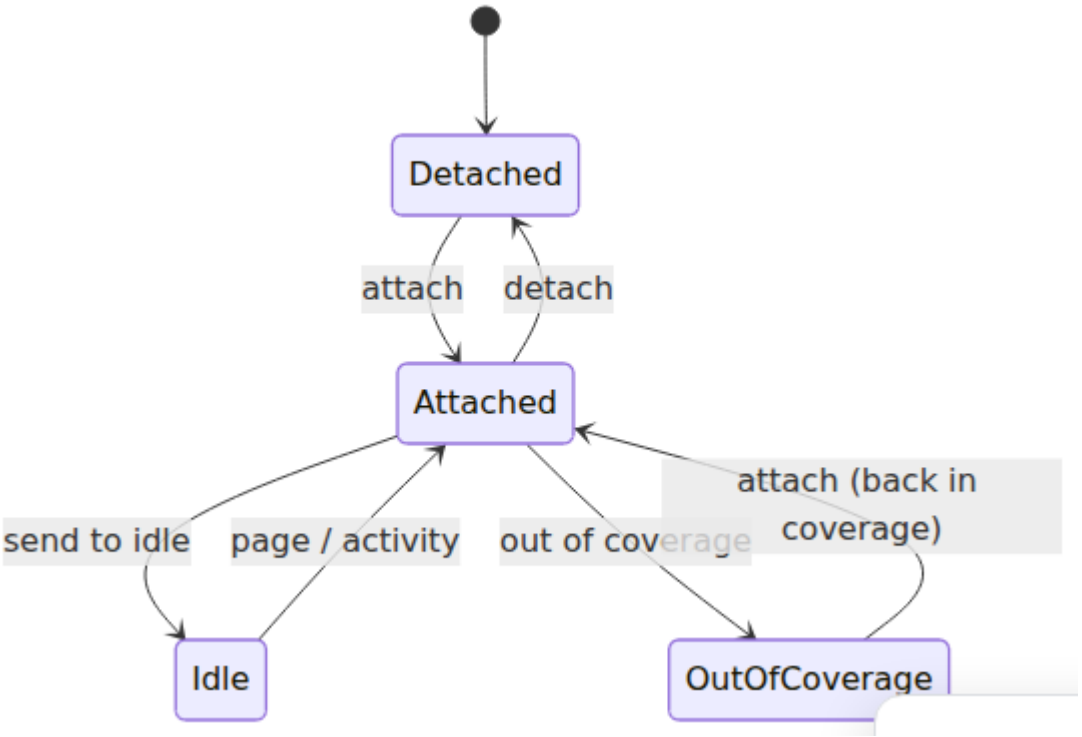


- **Anexar / Desanexar**: ingressar ou sair da rede.
- **Enviar para inativo**: mover para ECM-IDLE (como um UE real faz entre atividades). O paginamento ou nova atividade o traz de volta.
- **Fora de cobertura**: uma perda *não limpa* de rádio (o UE cai sem sinalização), para testar como a rede central lida com um UE que simplesmente desaparece. Anexar o traz de volta à cobertura.

Para cada UE, o simulador mostra o **MME de serviço** ao qual está anexado: o ID do Grupo MME e o Código MME (decodificado do GUTI do UE). Assim, em uma implantação em pool, você pode ver qual MME atendeu cada assinante.

Registro IMS e localização

Um UE simulado pode registrar-se no IMS e fazer SMS/chamadas. Quando se registra, inclui sua **localização celular** (`P-Access-Network-Info` com o `utran-cell-id-3gpp` para sua célula de serviço), exatamente como um UE real faz. Assim, o REGISTER de terceiros do S-CSCF propaga essa localização para o SMSc, TAS e outros servidores de aplicação. Isso permite que você teste o comportamento IMS dependente de localização de ponta a ponta sem rádios reais.



Controlando UEs a partir de Dispositivos

Como um UE simulado é apenas mais um dispositivo, ele aparece em **Dispositivos de Teste** marcado como um simulador e pode ser filtrado para lá. Você usa o **mesmo painel de controle de UE** quer abra um UE a partir do Mapa da Rede do Simulador RAN ou da frota de Dispositivos. É um lugar para anexar/desanexar, inativar, simular fora de cobertura, registrar-se no IMS, enviar um SMS ou fazer uma chamada, e observar o log de ações.

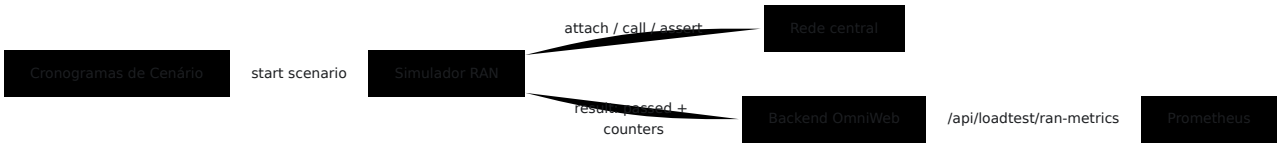
Filtre Dispositivos de Teste para os UEs do Simulador RAN para controlar assinantes emulados ao lado de dispositivos reais.

Cenários Agendados

Um **cenário** é uma receita de teste salva: uma sequência nomeada de ações de UE (anexar, inativo, acordar, registrar IMS, chamada, SMS, transferência, desanexar) que o simulador executa contra a rede central. O simulador fornece uma biblioteca de predefinições, agrupadas por categoria (por exemplo, ciclo de vida de anexação, VoLTE e casos de rejeição negativa). Execute um cenário

uma vez a partir da visualização de Teste de Carga ou execute-o em um cronograma repetido para monitorar a rede central continuamente.

A página **Cronogramas de Cenário** (barra lateral: Teste de Carga → Cronogramas de Cenário) gerencia as execuções repetidas. Para cada cronograma, você escolhe um cenário e com que frequência executá-lo. O OmniWeb registra o resultado de sucesso ou falha de cada execução e o exporta para o Prometheus, para que você possa alertar sobre isso e criar gráficos.



As execuções são **serializadas**. O OmniWeb executa um cenário agendado por vez, porque um cenário pode iniciar muitos UEs e coloca carga real na rede central. Se uma execução ainda estiver ativa quando o próximo cronograma estiver devido, o OmniWeb espera e a inicia no próximo ciclo livre. Use o botão **Executar agora** em um cronograma salvo para iniciá-lo imediatamente.

Parâmetros do Cronograma

Campo	Tipo	Obrigatório	Padrão	Descrição
Nome	String	Sim	-	Rótulo único para o cronograma. Também o rótulo `schedule` na métrica exportada.
Cenário	String	Sim	-	O cenário predefinido a ser executado. O seletor agrupa cenários por categoria.
A cada (s)	Inteiro	Não	3600	Com que frequência executar o cenário, em segundos. Mínimo 60.
Contagem de UE	Inteiro	Não	100	Número de assinantes que o cenário executa.
RPS	Número	Não	10	Número alvo de novos cenários por segundo.
Concorrência	Inteiro	Não	50	Número máximo de cenários em execução ao mesmo tempo.
APNs	Lista	Não	padrão do cenário	APNs para anexar, como uma lista separada por

Campo	Tipo	Obrigatório	Padrão	Descrição
				vírgulas. Substitui o padrão do cenário.

Testes de Velocidade

Um cronograma de **teste de velocidade** mede a largura de banda de download de um dispositivo emulado, da mesma forma que o **Teste de Largura de Banda de Dados** mede a partir de um dispositivo sob Dispositivos de Teste. Em cada execução, um UE simulado se anexa, baixa um arquivo do tamanho escolhido sobre seu portador de dados, registra a taxa em Mbps e se desanexa.

Adicione um com **Adicionar teste de velocidade** na página de Cronogramas de Cenário. A URL do arquivo padrão é o LibreSpeed no host `speedtest` do site selecionado (`/backend/garbage.php?ckSize=1024`, 1 GiB de dados aleatórios). O botão é desativado quando o site não tem um host `speedtest`. O download para quando o tamanho escolhido chega, então qualquer tamanho até 1024 MB funciona.

Campo	Tipo	Obrigatório	Padrão	Descr
URL do Arquivo	String	Sim	`http://<site speedtest host>/backend/garbage.php?ckSize=1024`	O arqu a ser baixad Deve s plain `http:/` porque UE simula não suport TLS. O OmniV resolv nome host p um endere IPv4 quand teste e execut então endere deve s acessí partir APN.
Tamanho (MB)	Número	Sim	10	Quant baixar megab (1 MB 1.000. bytes)

Campo	Tipo	Obrigatório	Padrão	Descr
				o arqu for me o teste mede arquiv inteiro
APN	String	Sim	internet	A APN qual o se ane baixa.
Timeout (s)	Inteiro	Sim	30	O máx que o downl pode levar, a 60 segun Um downl que nã termin tempo falha a execu

Conjunto de assinantes, Rede Central (MME/AMF), TAC e **Capturar pcap em caso de falha** funcionam como fazem para um cronograma de cenário. Um teste de velocidade sempre usa um UE.

A tabela **Execuções Recentes** mostra a taxa medida ao lado de cada teste de velocidade. Expanda uma execução para ver os bytes baixados e o tempo de transferência.

Passar e Falhar

Uma execução agendada **passa** quando o simulador relata que todas as afirmações passaram e nenhum cenário de assinante foi abortado. Uma execução **falha** se qualquer afirmação falhar ou qualquer cenário abortar. Um cenário sem afirmações passa desde que nenhum cenário abortar. Se o OmniWeb não conseguir iniciar a execução, ou a execução não terminar a tempo, o OmniWeb registra a execução como um **erro**.

A página mostra uma tabela **Execuções Recentes** com o resultado, a contagem de afirmações, o número de cenários abortados e a duração de cada execução.

Métricas

O OmniWeb expõe o último resultado de cada cronograma no formato Prometheus em `/api/loadtest/ran-metrics`. O Prometheus coleta isso como o trabalho `ransim_scenarios`, que o papel de monitoramento configura automaticamente.

Métrica: `ransim_scenario_pass` **Tipo**: Gauge **Descrição**: Resultado da execução agendada mais recente: `1` para sucesso, `0` para não sucesso **Rótulos**:

- `schedule`: o nome do cronograma
- `scenario`: o id do cenário que foi executado
- `category`: a categoria do cenário
- `status`: o resultado da execução (`passed`, `failed` ou `error`)

Os gauges acompanhantes compartilham os mesmos rótulos:

Métrica	Descrição
`ransim_scenario_duration_ms`	Duração da última execução, em milissegundos
`ransim_scenario_assertions_passed`	Afirmações passadas na última execução
`ransim_scenario_assertions_failed`	Afirmações falhadas na última execução
`ransim_scenario_scenarios_aborted`	Cenários de assinantes abortados na última execução
`ransim_scenario_last_run_timestamp`	Tempo Unix da última execução
`ransim_speedtest_mbps`	Taxa de download da última execução de teste de velocidade, em Mbps (apenas testes de velocidade)
`ransim_speedtest_bytes`	Bytes que a última execução de teste de velocidade baixou (apenas testes de velocidade)

Consultas de exemplo:

```
# Cenários cuja última execução não passou
ransim_scenario_pass == 0

# Total de falhas de afirmação em todos os cenários agendados
sum(ransim_scenario_assertions_failed)

# Um cronograma que não foi executado nas últimas duas horas
time() - ransim_scenario_last_run_timestamp > 7200

# Testes de velocidade abaixo de 20 Mbps
ransim_speedtest_mbps < 20
```

Dashboard do Grafana

O papel de monitoramento fornece um dashboard de **Cenários do Simulador RAN** (pasta do Grafana **RAN**). Ele lê as métricas acima e mostra uma linha do tempo de sucesso ou falha, o último resultado de cada cronograma, falhas de afirmação, frescor do cenário e duração da execução. Filtre por categoria, cenário ou cronograma na parte superior. Veja Grafana.

Usos Típicos

- **Testes funcionais**: configurar um eNB e um UE, anexar, iniciar uma sessão de dados, registrar-se no IMS, enviar um SMS e, em seguida, confirmar que cada elemento central se comporta corretamente.
- **Testes de carga**: ativar muitos UEs para gerar carga de anexação/sessão/IMS contra a rede central (veja a visualização de Teste de Carga).
- **Reprodução de cenários**: modelar interrupções (queda de link, fora de cobertura) e comportamento de MME em pool para reproduzir e diagnosticar problemas de campo.
- **Monitoramento contínuo**: agendar um cenário para ser executado em um temporizador e alertar sobre a métrica de sucesso ou falha (veja Cenários Agendados).

Relacionados

- Dispositivos de Teste: dispositivos reais e UEs simulados, controlados de um só lugar.
- Rastreamento de Sessão: correlacionar a sinalização que o simulador gera.

SIM Remota & SIM Virtual

OmniWeb pode apresentar **qualquer SIM a qualquer modem pela rede**. Ele também pode apresentar um SIM que **não existe fisicamente**: o OmniWeb o emula a partir de uma imagem de cartão salva mais as chaves do assinante mantidas no HSS. Isso transforma um rack de leitores de SIM, emuladores de cartão ("cardems") e modems em um ou mais locais em um pool compartilhado. Qualquer testador pode operar qualquer perfil de assinante contra qualquer modem sem precisar transportar um SIM plástico até um slot de cartão.

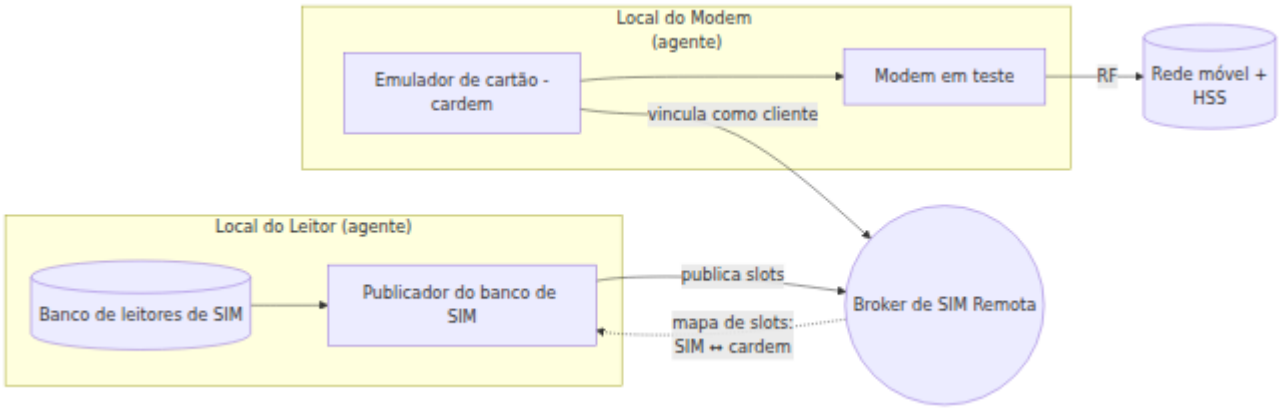
Esta página é o guia de operações para essa capacidade. A metade de **inventário** descobre quais SIMs estão em quais leitores. Banco de SIM cobre essa metade. Esta página cobre como **apresentar** um SIM (real ou virtual) a um modem e usá-lo em um teste. Imagens de SIM (Pacotes de Perfil SAIP) cobre como salvar o sistema de arquivos de um cartão como um pacote de perfil portátil e como usar um para dar suporte a um SIM virtual.

Índice

- Visão Geral da Arquitetura
- Conceitos
- O Banco de SIM: o que está onde
- SIM Remota: conectar um SIM a um cardem
- O Console do Cardem
- SIM Virtual: um assinante sem cartão físico
- Usando um SIM em um Livro de Teste de Roaming
- Solução de Problemas

Visão Geral da Arquitetura

Um banco de leitores de SIM, um ou mais emuladores de cartão e os modems em teste se conectam ao OmniWeb através de seus agentes de dispositivo. Um broker central mapeia um slot de SIM escolhido para um cardem escolhido; o cardem então apresenta esse SIM ao modem conectado a ele.



Para um SIM **virtual**, um cartão de software substitui o banco de leitores. O OmniWeb constrói esse cartão de software a partir de uma imagem de SIM salva e as chaves do assinante. Tudo mais é idêntico:



Conceitos

Termo	Significado
Banco de SIM	Um conjunto de leitores de cartões inteligentes em um agente, publicado para que seus SIMs possam ser apresentados em outro lugar. Cada leitor populado é um **slot**.
cardem	Uma placa emuladora de cartão (USB) que finge ser um SIM para um modem conectado a ele. Ele reproduz qualquer cartão ao qual está mapeado.
Mapa de slots	O vínculo "apresentar **este** slot de SIM para **aquele** cardem". Criá-lo conecta os dois pela rede; removê-lo desconecta-os.
Modem em teste	O modem atrás de um cardem. Ele se conecta à rede ao vivo usando qualquer SIM que o cardem esteja apresentando.
SIM Virtual	Um cartão de software construí́do a partir de uma imagem de SIM salva mais as chaves de um assinante. O OmniWeb o apresenta a um cardem exatamente como um SIM real. Nenhum cartão físico é necessário.

O Banco de SIM: o que está onde

A página do **Banco de SIM** lista cada slot de leitor em cada agente conectado, agrupados por agente. O layout do banco é a verdade: slots vazios, ilegíveis e em uso aparecem todos, não apenas os populados.

*Cada linha é um leitor físico. O chip de status mostra se um cartão está presente e legível. A linha então mostra a identidade do SIM (ICCID, IMSI, MCC/MNC, país, nome do operador). Leitores mantidos por uma sessão de emulação ativa aparecem como **Em uso**. SIMs persistidos cujo leitor está atualmente offline aparecem sob **Vistos anteriormente**. Eles reaparecem quando o agente se reconecta com o SIM inserido.*

Chip de status	Significado
SIM	Um cartão está presente e sua identidade foi lida.
Cartão presente	Um cartão está fisicamente inserido, mas sua identidade não pôde ser lida (por exemplo, uma combinação de leitor/cartão incompatível).
Em uso	O leitor está mantido por uma sessão de SIM remoto/emulação neste momento.
Vazio	Nenhum cartão no slot.

Ações por linha abrem o explorador do **Sistema de Arquivos de SIM** ou o **Terminal APDU** para aquele slot exato, e **Reescanear** lê novamente os

leitores de um agente sob demanda.

SIM Remota: conectar um SIM a um cardem

A página **SIM Remota** é onde você vincula um SIM a um cardem. Os vínculos funcionam **entre agentes e locais**: o SIM pode estar em um leitor em uma localização e o cardem/modem em outra.

Passos

1. **Inicie o banco de SIM** no agente que possui os leitores (**Iniciar bankd**). Isso publica seus slots de leitor.
2. **Inicie o cliente cardem** para o emulador de cartão que você deseja usar (**Iniciar cliente**). Isso vincula o cardem para que um SIM possa ser mapeado a ele.
3. Sob **Conectar um SIM**, escolha um slot publicado e escolha um cardem para vinculá-lo. O mapeamento é criado e aparece sob **Mapeamentos Ativos** como **ATIVO**.
4. O cardem agora apresenta esse SIM ao seu modem. Reinicie o modem (veja o console do cardem) para que ele leia o SIM recém-apresentado e se conecte.

Reinicialização Global desmonta todos os mapeamentos e retorna cada cardem a um estado ocioso. Use-o para se recuperar de um banco de testes confuso.

Campo (Mapeamentos Ativos)	Significado
Estado	`ATIVO` uma vez que o cardem está apresentando o SIM.
SIM (banco/slot)	Em qual banco e slot do agente o cartão reside.
ICCID	O SIM apresentado.
Cardem (cliente/slot)	Qual cardem (e qual agente) está apresentando-o.
Por	O operador que criou o mapeamento.

O Console do Cardem

Em **Dispositivos**, o OmniWeb mostra um emulador de cartão como seu próprio tipo de dispositivo (`ngff-cardem`), ao lado de modems e telefones. Ele nunca é aberto como um telefone. O OmniWeb rotula tipos de dispositivos desconhecidos de forma simples, em vez de adivinhar.

Abra o cardem para obter um console dedicado para o emulador e seu modem.

Controle	O que faz
Iniciar cliente	Vincula o cardem como um cliente de SIM remoto para que um SIM possa ser mapeado a ele.
Reiniciar modem	Reapresenta o cartão emulado, o que faz com que o modem releia o SIM e execute novamente a conexão. Esta é a maneira de "trocar o SIM" sem tocar no hardware.
SIM Remota	Conectar ou desconectar qual SIM remoto está sendo apresentado a este cardem.

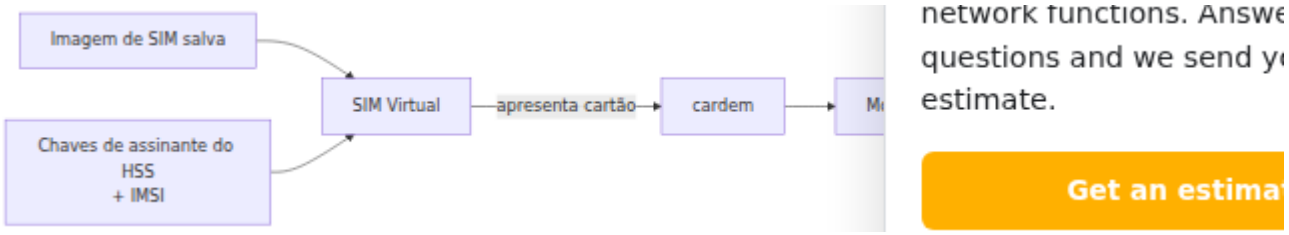
O painel **Fonte do SIM** declara honestamente o que está e não está disponível: o cardem fornece ao modem um SIM *remoto*. O console ainda não oferece a apresentação de um cartão *local* inserido na placa do emulador. O console diz isso em vez de mostrar um controle que não faz nada.

SIM Virtual: um assinante sem cartão físico

Um **SIM virtual** permite que um modem se conecte como um assinante **para o qual você não tem um SIM**. O OmniWeb o constrói a partir de duas coisas que você já possui:

1. Uma **imagem base de SIM**: um instantâneo salvo da estrutura de arquivos de um cartão real (qualquer SIM de teste compatível funciona como a base; veja **Imagens de SIM**).
2. A **identidade e chaves do assinante do HSS**: o IMSI e as chaves de autenticação de um assinante já provisionado na rede.

O OmniWeb combina-os em um cartão de software. Este cartão responde às leituras de arquivos do modem a partir da imagem e responde ao desafio de autenticação da rede com as chaves do HSS. Ele sobrepõe o IMSI do assinante escolhido. Através de um cardem, o modem não consegue diferenciá-lo de um SIM plástico: ele lê o IMSI, executa a autenticação e **se conecta à rede ao vivo**.



Quando usá-lo

- Reproduzir o comportamento de roaming ou conexão de um assinante específico sem uma fonte para seu SIM físico.
- Testar muitos assinantes provisionados contra um modem, um após o outro.
- Testar perfis que só existem no HSS (recém-provisionados, pré-envio).

O que prova. Um modem na bancada se conectou à rede ao vivo (`registrado, rede doméstica`) como um assinante do HSS para o qual não existe SIM plástico. Ele leu o IMSI desse assinante e completou a autenticação da rede inteiramente a partir do cartão virtual.

> Um elemento dedicado de **Leitor de SIM Virtual** é o próximo passo nessa capacidade. Lá você "carrega" um SIM virtual a partir de uma imagem e assinante escolhidos e o apresenta como qualquer outro slot de leitor. Hoje, o OmniWeb conecta o cartão virtual através do mesmo broker de SIM Remoto e caminho de cardem descrito acima.

Usando um SIM em um Livro de Teste de Roaming

Livros de **Teste de Roaming** (GSMA IR.38 / IR.48) podem conduzir a apresentação do SIM como parte de uma execução. No painel **Executar Testes** de um livro de teste, você pode escolher:

- um **SIM (por ICCID / IMSI)**: rastreado por identidade, seu leitor atual resolvido automaticamente em tempo de execução, e
- um **Modem Cardem**: o cardem ao qual o SIM é emulado.

Apresentar SIM ao cardem estabelece o mapeamento antes de você testar. **Ir: Executar Todos os Testes** apresenta o SIM primeiro (quando tanto um SIM quanto um cardem estão selecionados), então lê o IMSI e executa os casos de dados. Se o SIM não estiver atualmente em um leitor, ou o cliente do cardem não estiver em execução, o painel diz exatamente por quê. Ele não executa silenciosamente contra o cartão errado.

Veja Dispositivos de Teste e a documentação do livro de teste para o restante do fluxo IR.38.

Solução de Problemas

Um SIM não aparece no banco

Sintomas: um leitor está conectado, mas nenhum slot (ou um slot vazio) aparece.

Causas possíveis & resolução:

- O cartão não está inserido, ou a combinação leitor/cartão não consegue alimentar o cartão. O slot mostra **Cartão presente** ou **Vazio**. Reinsira o SIM.

- O leitor foi apenas conectado. O OmniWeb reescaneia leitores ao conectar, mas você pode forçar isso com **Reescanear** no grupo do agente.

O modem não se conecta após você conectar um SIM

Causas possíveis & resolução:

- O modem não leu novamente o SIM. Use **Reiniciar modem** no console do cardem para reapresentar o cartão.
- O mapeamento não está **ATIVO**. Confirme sob **Mapeamentos Ativos** na página de SIM Remota que o SIM está vinculado ao cardem correto.
- O assinante não está provisionado (ou está barrado) no HSS da rede servidora.

"Cartão presente (ilegível)" em um leitor

Sintomas: um cartão é detectado, mas sua identidade não pode ser lida.

Resolução: esse leitor não consegue se comunicar com esse cartão (comumente uma incompatibilidade de tensão/protocolo em leitores baratos). Mova o SIM para um leitor diferente no banco.

SIM Virtual: modem lê o cartão, mas não se conecta

Causas possíveis & resolução:

- O assinante escolhido deve estar **habilitado** e totalmente provisionado (com um perfil de dados) no HSS para a rede servidora.
- A imagem base deve vir de um tipo de cartão compatível. Se a inicialização travar, recapture a imagem base de um SIM conhecido e bom.

SCEF: Função de Exposição de Capacidade de Serviço

O **SCEF** (Função de Exposição de Capacidade de Serviço), **OmniSCEF** da Omnitouch, é o **gateway norte** da rede para a Internet das Coisas. Ele expõe as capacidades da rede central para Servidores de Aplicação externos através da API RESTful **3GPP T8** definida em TS 29.122, para que uma plataforma de máquina a máquina possa se inscrever em eventos sobre uma frota de dispositivos e trocar pequenas quantidades de dados com eles sem nunca falar Diameter ou GTP. Ele oferece duas famílias de serviços. **Eventos de Monitoramento** pedem à rede que relate quando um dispositivo se torna acessível, perde conectividade, muda de localização e assim por diante. **Entrega de Dados Não-IP (NIDD)** transporta pequenas cargas úteis não-IP para e de dispositivos NB-IoT restritos através do plano de controle. Internamente, o SCEF alcança o MME através da interface Diameter **T6a** (TS 29.128). O OmniWeb exibe seu status, os recursos T8 que um Servidor de Aplicação criou e as sessões NIDD ativas que está carregando.

← Guia de Operações

O painel é uma página de elemento por instância acessada a partir da barra lateral quando um SCEF está em execução no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API T8 do SCEF, portanto, permanece atrás do único gateway autenticado. Um link de documentação no cabeçalho da página fornece ajuda em contexto. A página é organizada em abas.

O modelo de ID SCS/AS

Cada recurso T8 (cada assinatura de monitoramento e cada configuração NIDD) é **escopado para a identidade SCS/AS** sob a qual o Servidor de Aplicação foi registrado (o *Servidor de Capacidade de Serviços / Servidor de*

Aplicação). A API T8 **não possui um endpoint que enumere os IDs SCS/AS** em uso, portanto, o OmniWeb não pode descobri-los para você: o operador **define o ID SCS/AS** na página, e o OmniWeb o lembra **através das abas do SCEF**, para que você o defina uma vez e ele carregue de Visão Geral para Eventos de Monitoramento até NIDD. Até que um ID SCS/AS seja definido, as abas escopadas solicitam um em vez de mostrar uma lista vazia. Os recursos existem sob uma identidade que você precisa nomear. Insira o ID SCS/AS com o qual um Servidor de Aplicação foi integrado (por exemplo `iot-platform-01@omnitouch`) para trabalhar com as assinaturas e configurações dessa plataforma.

Visão Geral

Uma leitura de saúde de tela única do SCEF em si: seu **status**, nome do **produto**, estado da **licença** e o **host Diameter** que usa para T6a em direção ao MME. Abaixo está o **contexto da aplicação** (o campo ID SCS/AS descrito acima) e, uma vez que um ID SCS/AS é definido, a contagem de **assinaturas de monitoramento** e **configurações NIDD** atualmente mantidas para esse Servidor de Aplicação. É a confirmação mais rápida de que o SCEF está ativo e quanto uma determinada plataforma está carregando. Painéis de

monitoramento e estatísticas são fornecidos como embeds do Grafana, acessados a partir da mesma página.

Eventos de Monitoramento

As **assinaturas de eventos de monitoramento** que um Servidor de Aplicação criou para o ID SCS/AS atual. Cada assinatura pede à rede que relate uma classe de evento e a POSTe para o Servidor de Aplicação; cada linha mostra:

- **Tipo de evento**: o tipo de monitoramento, como **Acessibilidade de UE**, **Perda de Conectividade**, **Relato de Localização**, **Disponibilidade após Falha de DDN**, **Status de Roaming** ou **Número de UEs em uma Área**.
- **Alvo**: o dispositivo ou grupo que a assinatura observa, identificado por um **ID Externo**, um **MSISDN** ou um **ID de Grupo Externo** para toda a frota.
- **Destino de notificação**: a **URL de callback** para a qual o SCEF POSTa cada relatório de evento. Deve ser um endereço `http(s)` absoluto que o Servidor de Aplicação expõe.

- **Relatórios Máximos** e, para uma assinatura de acessibilidade, o **tipo de acessibilidade** (`SMS` ou `DATA`). Juntamente com a **duração/expiração** do monitoramento, esses limitam quantos eventos são enviados e até quando a assinatura vive.

Assinaturas podem ser criadas, editadas e excluídas; excluir uma delas impede que o Servidor de Aplicação receba esses relatórios de eventos.

NIDD

As **configurações NIDD** são as ligações de Entrega de Dados Não-IP que um Servidor de Aplicação criou para o ID SCS/AS atual. Uma configuração autoriza pequenas cargas úteis não-IP a serem trocadas com um dispositivo através do plano de controle. Cada linha mostra:

- **Alvo**: o dispositivo por **ID Externo**, **MSISDN** ou **ID de Grupo Externo**.
- **DNN / APN**: o Nome da Rede de Dados (APN) que a conexão PDN NIDD usa (por exemplo `nidd.iot.omnitouch`).
- **Status**: `ATIVO`, ou terminado (`TERMINADO`, `TERMINADO_UE_NÃO_AUTORIZADO`).

- **Tamanho Máximo do Pacote**: o **tamanho máximo do pacote** em bytes que a carga útil não-IP pode alcançar.
- **RDS**: se o **Serviço de Dados Confiável** está habilitado. Ele adiciona um transporte leve reconhecido com portas de origem/destino sobre o link não-IP.

Uma configuração também carrega uma **opção de estabelecimento de PDN** que decide o que acontece quando dados de downlink chegam enquanto o dispositivo não tem uma conexão PDN NIDD ativa: **aguardar o UE** para estabelecer uma, **indicar um erro**, ou **estabelecer a conexão PDN** fazendo paging no dispositivo.

Entrega de dados de downlink

A partir de uma configuração NIDD, você pode **entregar uma carga útil de downlink** ao dispositivo. Insira a carga útil como texto. O SCEF **codifica em base64** antes de ser enviada através do NIDD, e cada entrega pode carregar uma **prioridade** e uma **latência máxima**. Entregas recentes são listadas com seu **status de entrega**: `SUCESSO`, `BUFFERIZANDO`, `ENVIANDO`, ou uma das razões de falha, como `FALHA_UE_NÃO_ACESSÍVEL`. Você pode cancelar uma

entrega em fila ou bufferizada. É assim que uma plataforma envia um comando ou um ajuste de firmware para um dispositivo restrito que não tem endereço IP.

Sessões NIDD

As **sessões NIDD T6a ativas** são as ligações de Entrega de Dados Não-IP que o SCEF mantém com o MME neste momento. Ao contrário das configurações NIDD, que são recursos T8 escopados para um ID SCS/AS, estas são **estado de tempo de execução global do servidor**: são **somente leitura** e não são escopadas por ID SCS/AS, portanto, esta aba mostra cada sessão ativa, independentemente de qual contexto de aplicaç��o você está visualizando. Cada linha mostra o **IMSI** do dispositivo, o **APN** que a conexão PDN NIDD usa, a **Identidade do Portador EPS (EBI)**, o **estado** da sessão (`ATIVO`, `OCIOSO`), o **id da sessão T6a**, o **host MME** que está servindo e o **reino MME**, e o **id de configuração** contra o qual a sessão foi configurada. É a maneira mais rápida de ver quais dispositivos realmente têm uma ligação não-IP ativa, e através de qual MME.

Logs

A aba **Logs** exibe a saída de log ao vivo do SCEF para solucionar problemas de uma única instância sem sair do OmniWeb.

Painéis de monitoramento

As taxas de solicitação T8, a taxa de throughput de relatórios de eventos e as contagens de entrega NIDD para o SCEF são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **MME**: o SCEF o alcança através de **T6a** para configurar conexões PDN NIDD e para coletar os eventos de monitoramento relatados aqui. O host MME e o reino que cada sessão usa são mostrados na aba Sessões NIDD.
- **HSS**: mantém os dados de assinatura (Identificadores Externos, autorização NIDD) dos quais os serviços de monitoramento e NIDD do SCEF dependem.
- **PGW-C / SMF** e **UPF**: transportam o plano de dados IP comum. O NIDD deliberadamente os contorna para mover pequenas cargas úteis não-IP através do plano de controle.
- Guia de Operações: voltar ao índice de elementos.

S-CSCF: Função de Controle de Sessão de Chamada

O **S-CSCF** (Função de Controle de Sessão de Chamada), o **OmniCSCF** da Omnitouch em seu papel de serviço, é o **registrador e âncora de controle de sessão do IMS**. Cada assinante doméstico é atribuído a um S-CSCF enquanto estiver registrado: ele mantém seu registro, baixa seu **perfil de serviço** do HSS através da interface **Cx** e, criticamente, avalia os **Critérios de Filtro Iniciais (iFC)** do assinante em cada solicitação. Ele roteia diálogos SIP para os **Servidores de Aplicação** (o Servidor de Aplicação de Telefonia para chamadas, o SMSc para mensagens, e assim por diante) que fornecem seus serviços (TS 23.228, TS 29.228). É o ponto fixo pelo qual cada INVITE, MESSAGE e SUBSCRIBE de um assinante registrado passa. O OmniWeb exibe os registros que está mantendo, os diálogos que está controlando e sua conectividade Diameter com o HSS.

← Guia de Operações

O painel é uma página de elemento por instância acessada a partir da barra lateral quando um S-CSCF está em execução no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API de gerenciamento do S-CSCF, portanto, permanece atrás do único gateway autenticado. Um link de documentação no cabeçalho da página fornece ajuda em contexto. A página é organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela do S-CSCF: a versão e o tempo de atividade do **motor SIP**, o número de **assinantes registrados** que está atendendo atualmente e a contagem de **diálogos** ativos. Como o ponto de ancoragem para cada assinante registrado atribuído a ele, essas duas contagens são a medida principal de quanta população e quantas sessões ativas este servidor está carregando.

Registros

Os **assinantes registrados** que o S-CSCF está atendendo, retirados de seu armazenamento de registrador. Cada linha é uma **Identidade Pública IMS (IMPU)**: por exemplo `sip:001001000010001@ims.mnc001.mcc001.3gppnetwork.org`, com o **contato** vinculando-o registrado, o **estado** de registro e **expiração**, e o agente do usuário do dispositivo. Como o S-CSCF é o registrador autoritativo, esta é a visão definitiva de quem está registrado no IMS: se um assinante aparece aqui, ele pode receber chamadas e mensagens. Você pode **desregistrar** um IMPU daqui, por exemplo, para forçar um dispositivo preso a re-registrar. O S-CSCF sinaliza isso para baixo através do I/P-CSCF para o dispositivo.

Diálogos

Os **diálogos SIP ativos** que o S-CSCF está controlando atualmente: as chamadas e sessões de longa duração em andamento. Cada linha mostra o **Call-ID** de um diálogo, as identidades **de/para** envolvidas, seu **estado** (inicial, confirmado, terminando) e o tempo. Como cada chamada para um assinante registrado está ancorada aqui e direcionada através de seus Servidores de Aplicação por iFC, esta aba é a imagem ao vivo da atividade de sessão IMS no servidor, e o lugar para confirmar que uma chamada específica está ativa e ver quais partes e rota ela envolve.

Diameter

A conectividade **Diameter** do S-CSCF: seus pares **Cx** (e, onde usado, **Sh**) em direção ao **HSS**, diretamente ou via um **DRA**. Através do Cx, o S-CSCF realiza **Atribuição de Servidor (SAR/SAA)** para reivindicar um assinante e baixar seu **perfil de serviço** e **iFC**, e **Autenticação Multimídia (MAR/MAA)** para obter os vetores de autenticação que desafiam o UE no registro. Cada linha mostra o **host** de um par, **domínio**, as **aplicações Diameter** que suporta e o **estado de conexão**. Um par Cx aqui significa que o S-CSCF não pode buscar perfis de serviço ou autenticar registros, portanto, o registro falha completamente.

Registros

A aba **Registros** exibe a saída de log ao vivo do S-CSCF. Solucione problemas de uma única instância sem sair do OmniWeb: um registro rejeitado, um iFC que não conseguiu disparar, ou uma chamada que não roteou para seu Servidor de Aplicação.

Painéis de monitoramento

Taxas de registro e chamadas, contagens de disparo de iFC e latência de transação Cx para o S-CSCF são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **HSS**: mantém os perfis de serviço e **iFC** que o S-CSCF baixa através do **Cx**, e os vetores de autenticação que usa para desafiar registros; a aba Diameter mostra esse emparelhamento.
- **I-CSCF**: seleciona este S-CSCF para um assinante no registro e encaminha chamadas de terminação para ele.
- **P-CSCF**: permanece no caminho de sinalização entre o UE e este S-CSCF para cada solicitação.
- **TAS** e **IMS SMSc / IP-SM-GW**: os Servidores de Aplicação para os quais o S-CSCF roteia diálogos quando o iFC de um assinante é acionado. Estes fornecem os serviços reais de telefonia e mensagens.
- Guia de Operações: de volta ao índice de elementos.

SGW-C: Gateway de Serviço (Plano de Controle)

O **SGW-C** é a parte do plano de controle do Gateway de Serviço EPC. Ele ancla os bearers de cada assinante entre a rede de acesso e o gateway de pacotes: termina **S11** para o MME (sinalização de sessão e bearer), **S5/S8** para o PGW-C (a conexão PDN), e programa o plano de usuário (SGW-U) que encaminha o tráfego em **S1-U** para o eNodeB. Em resumo, é o nó que mantém o estado do bearer ativo para cada assinante conectado e mantém o MME, PGW e plano de usuário em sincronia. O OmniWeb exibe as sessões ativas do SGW-C, contagens de sessões e logs; tendências de longo prazo (throughput, crescimento de sessões) estão nos painéis Grafana acessados a partir da mesma página.

← Guia de Operações

O SGW-C é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site. Onde vários estão implantados, ele também fornece uma visão de frota para o status agregado. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do SGW-C, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela: o **status da API** do SGW-C, a **contagem de sessões ativas**, e um resumo derivado das sessões ativas: o número de **MMEs** únicos (pares S11 distintos), **PGWs** únicos (pares S5/S8 distintos), e os **bearers totais** atualmente ancorados. É a maneira mais rápida de confirmar que o SGW-C está ativo, quantas sessões ele mantém e quantos MMEs e PGWs ele está utilizando.

Sessões

Cada sessão ancorada, cada linha identificada pelo **IMSI** e **MSISDN** do assinante com seu **status** de conexão. Abrir uma sessão mostra seu estado completo de bearer: os endpoints de controle **S11** (F-TEIDs do lado do MME e do lado do SGW), cada **conexão PDN** (APN, bearer padrão, e os F-TEIDs de controle S5/S8 para o PGW), e cada **bearer** (EBI, os F-TEIDs do plano de usuário S1-U e S5/S8, e sua QoS). É aqui que você confirma que os bearers de um assinante específico estão estabelecidos e vê qual MME e PGW estão atendendo-os.

Onde vários SGW-Cs estão implantados, a mesma aba na **visão de frota** lista cada sessão em todos eles em uma tabela, com o SGW-C que está servindo mostrado contra cada linha, para que um operador possa encontrar um assinante sem saber qual SGW-C está ancorando-o. Abrir uma linha leva a essa sessão em sua própria instância. Uma instância que não pode ser alcançada é nomeada acima da tabela, assim como o limite de linha por instância quando uma instância mantém mais sessões do que a visão combinada puxa.

Logs

A aba **Logs** exibe o log ao vivo do SGW-C para solucionar problemas de um único gateway sem sair do OmniWeb.

Painéis de Monitoramento

Throughput, tendências de contagem de sessões e outras séries temporais para o SGW-C são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- MME: o par de controle sobre **S11**; ele conduz a configuração de sessão e bearer no SGW-C.
- O **PGW-C** ancla a conexão PDN sobre **S5/S8**.
- O **SGW-U / UPF** é o plano de usuário que o SGW-C programa para encaminhar tráfego em S1-U.

Ferramentas de Cartão SIM: Sistema de Arquivos, APDU e eSIM

OmniWeb faz mais do que descobrir e apresentar SIMs. Ele oferece um conjunto de **ferramentas de cartão de baixo nível** que alcançam qualquer leitor em qualquer agente para se comunicar diretamente com o cartão. Você pode navegar e editar seu sistema de arquivos, enviar APDUs brutas manualmente, assistir ao rastreamento ao vivo de APDU de uma sessão de SIM remoto e gerenciar perfis de eSIM em um eUICC. Esta página é o guia de operações para essas ferramentas.

← Guia de Operações

Essas ferramentas estão ao lado dos recursos existentes do SIM e os reutilizam. Comece aqui para ter uma visão geral:

- **Banco de SIM**: o inventário: quais SIMs estão em quais leitores em todos os agentes. Cada ferramenta nesta página tem como alvo um leitor desse inventário, e as ações por slot do Banco de SIM fazem links diretos para eles.
- **Imagens de SIM (Pacotes de Perfil SAIP)**: como salvar um sistema de arquivos lido como uma imagem portátil e como navegar ou comparar imagens salvas.
- **SIM Remoto & SIM Virtual**: como apresentar um SIM (real ou virtual) a um modem pela rede através de emuladores de cartão.
- **Gerenciamento de SIM OTA**: a mesma edição em nível de arquivo, mas alcança um cartão **via aérea** com pacotes seguros (03.48 / SCP80) em vez de um leitor local.

Todas as quatro ferramentas abaixo estão na barra lateral sob o grupo **SIMs**.

Um leitor, um consumidor por vez

Apenas uma coisa por vez pode controlar um leitor físico PC/SC. Uma ferramenta nesta página pode precisar de um leitor que já está sendo utilizado por outra coisa: outro operador que o lê, ou uma sessão de banco de SIM remoto ao vivo que o apresenta a um modem. A ferramenta então mostra **quem o possui e por quê**, e oferece um **Tomar controle** explícito. Não há um desligamento silencioso: quando você assume o controle, o OmniWeb cancela a outra sessão (e, para uma sessão de banco, desconecta aquele link SIM↔cardem). Para editar ou enviar é uma ação de controle que depende da permissão de controle do banco de SIM. Sem isso, você pode visualizar leitores, mas não controlar cartões.



Explorador de Sistema de Arquivos SIM

Escolha um leitor e **leia toda a árvore de arquivos** de seu cartão: o MF, DF.GSM / DF.TELECOM, ADF.USIM e ADF.ISIM e todos os seus EFs, com cada arquivo legível decodificado em campos nomeados. Uma leitura completa toca muitos arquivos, então uma barra de progresso mostra o andamento ("leitura de X de Y arquivos: EF....").

- **Pesquise** na árvore pelo código do arquivo (FID), nome curto ou descrição. Uma pesquisa por "Códigos de Chamadas de Emergência" encontra EF.ECC, não apenas `6FB7`.
- **Arquivos protegidos por PIN são sinalizados, nunca lidos**: o explorador não queimará tentativas de PIN.
- **Edite um EF** (com a permissão de controle): o painel de detalhes oferece um formulário orientado por esquema (campos decodificados, tipados) onde disponível, e recorre ao hex bruto. Uma gravação é destrutiva e pede confirmação. Onde um EF precisa de autenticação, use **Verificar CHV/ADM** primeiro. Ele testa uma chave PIN/ADM contra o cartão (reporta

tentativas restantes e nunca queima a última tentativa). Uma vez provado, o explorador o reutiliza para a gravação. O armazenamento de chaves SIM oferece chaves salvas para o ICCID de um cartão automaticamente.

- **Salvar imagem** captura a árvore decodificada como uma Imagem SIM nomeada. **Comparar com imagem** compara o cartão ao vivo com um salvo. **Imagens salvas** abre a biblioteca de imagens. Você também pode abrir uma imagem salva *como* uma árvore (`?image=<id>`) para navegar em um cartão que você não possui mais em um leitor.

O leitor deve estar livre (não sendo mantido por uma sessão de SIM remoto), ou você pode assumir o controle como acima.

Se o explorador relatar que não pode ler um cartão

Sintomas: O explorador não oferece árvore, ou cada arquivo retorna vazio, em um host cujos leitores e cartões estão listados corretamente.

Causas possíveis:

- O serviço de leitura de cartão nesse host de agente não está em execução, ou está faltando um componente necessário para decodificar uma árvore de arquivos. O sintoma é idêntico a uma falha de cartão ou leitor, então verifique o host antes de suspeitar do cartão.
- Outro consumidor está segurando o leitor. Veja Um leitor, um consumidor por vez.

Resolução:

1. Reimplante o agente nesse host. Uma implantação instala o serviço de leitura de cartão com tudo que precisa, e a construção do pacote agora se recusa a produzir um agente que está faltando um componente necessário.
2. Confirme que o cartão ainda responde lendo um arquivo no Terminal APDU. Se uma única leitura funcionar e uma árvore completa não funcionar, a falha está no host, não no cartão.

> **Nota:** arquivos que precisam de um PIN são lidos como protegidos em vez de como conteúdo até que o PIN seja provado com **Verificar CHV/ADM**.

> Uma árvore que é principalmente protegida é o resultado esperado para um cartão cujo PIN está habilitado, não uma falha.

Terminal APDU

O Terminal APDU é um **console manual para o cartão**: digite um APDU bruto em hex, envie-o para o cartão em um leitor escolhido e veja a resposta decodificada. A decodificação mostra o nome do INS do comando, a palavra de status e seu significado, e uma interpretação expandida de quaisquer dados de resposta (uma árvore TLV FCP, campos EF decodificados ou um resultado de AUTENTICAR). Botões pré-definidos (SELECIONAR MF, STATUS, LER BINÁRIO, OBTER RESPOSTA, …) preenchem comandos comuns. A entrada é tolerante a espaços em branco/colchetes e validada (bytes inteiros, pelo menos CLA/INS/P1/P2).

Dois modos:

Modo	Comportamento	Usar para
Disparo único	Cada APDU é auto-contida; o cartão reinicia para o MF entre envios.	Probes únicas.
Sessão	Abre uma sessão de cartão persistente e exclusiva, de modo que o estado (seleção, autenticação) **persista** entre APDUs: um SELECIONAR seguido de um LER BINÁRIO funciona, e um VERIFICAR compartilha sua autenticação com uma atualização posterior. O leitor permanece mantido até que você feche a sessão.	Sequências com estado.

A ação **APDU** por slot do Banco de SIM faz um link direto aqui com aquele leitor exato pré-selecionado. As mesmas regras de um-consumidor/Tomar controle se aplicam.

Registro APDU

Onde o terminal é você controlando um cartão, o **Registro APDU** é um **rastreamento ao vivo** passivo dos APDUs de comando/resposta trocados entre um **modem e um SIM (remoto)** através da cadeia remoto-SIM / cardem. Ative a **captura** e ele acompanha a troca: cada linha emparelha um comando `modem→cartão` com sua palavra de status decodificada, além da mesma decodificação de resposta que o terminal (árvore FCP, campos EF, eventos ATR/reset). Você pode pausar a visualização (a captura continua em execução), filtrar por comando/hex/SW e rolar automaticamente.

Use-o para ver o que um modem realmente pede ao SIM durante um anexo ou uma execução de teste IR.38: quais arquivos ele seleciona, onde um VERIFICAR falha, se um AUTENTICAR é bem-sucedido. Você não precisa instrumentar o modem. Ele emparelha naturalmente com SIM Remoto, que configura o link modem↔SIM que o registro então rastreia.

---

eSIM (LPA)

A ferramenta **eSIM** gerencia um **eUICC** através do **Assistente de Perfil Local (LPA)** do agente. Um eUICC é um chip eSIM físico em um de seus leitores. Ele contém vários perfis, mas apenas um está ativo por vez.

- **Cartão eUICC**: mostra o **EID** do chip.
- **Perfis instalados**: cada perfil no cartão: seu estado (ativo/desativado), apelido, provedor, nome e ICCID. Por perfil, você pode **ativar** (torná-lo o eSIM ativo), **desativar**, **renomear** (apelido) ou **excluir**. Uma exclusão remove o perfil do eUICC e é irreversível, portanto, confirma primeiro.
- **Baixar um perfil**: puxe um novo perfil de um SM-DP+ de um operador e instale-o no cartão. Use um **código de ativação** completo (`LPA:1$smdp.example.com$MATCHING-ID`) ou um **endereço SM-DP+ dividido + ID correspondente**, com um código de confirmação opcional.

Isso é especificamente para cartões eSIM (eUICC), e controla um chip em um de seus leitores. Para edição de arquivos de SIM/UICC clássicos, use o Explorador de Sistema de Arquivos acima. Para editar um cartão

remotamente, use OTA. Para emitir perfis de eSIM e rastreá-los em uma propriedade, veja eSIM (SGP.22).

Kit de Ferramentas SIM (STK)

O cliente **Kit de Ferramentas SIM** controla applets STK em um cartão SIM. Ele envia um perfil de terminal para o cartão e, em seguida, apresenta cada comando proativo como uma tela interativa: menus, exibição de texto, entrada de tecla única e entrada de texto. Use-o para navegar pelos serviços residentes do operador, acionar fluxos de configuração OTA ou testar a lógica do applet residente no SIM.

Veja **Kit de Ferramentas SIM** para o guia completo de operações.

Relacionados

- Banco de SIM: o inventário de leitores/SIM que essas ferramentas visam.
- Imagens de SIM: salvar, navegar e comparar sistemas de arquivos lidos.
- SIM Remoto & SIM Virtual: apresentar um SIM a um modem pela rede (o link que o Registro APDU rastreia).
- Gerenciamento de SIM OTA: a mesma edição de arquivos, via aérea.
- Ciclo de Vida do SIM: perfis, lotes de emissão, a propriedade e campanhas de convergência.
- eSIM (SGP.22): solicitar e gerenciar perfis de eSIM.
- Kit de Ferramentas SIM: interagir com applets STK em um cartão em um leitor.

Imagens SIM: Pacotes de Perfil SAIP

Uma **Imagem SIM** é um instantâneo salvo de todo o sistema de arquivos de um cartão. O OmniWeb armazena cada imagem como um **Pacote de Perfil Não Protegido SAIP (UPP)** em codificação DER. Este é o mesmo formato interoperável que os perfis eUICC usam, definido pela *Especificação Técnica de Formato Interoperável de Pacote de Perfil eUICC* do TCA. Um cartão capturado se torna um único arquivo portátil `.der` que qualquer ferramenta compatível com SAIP pode ler.

Esta página é o guia de operações. Ela cobre como capturar, exportar, fazer upload, navegar e comparar imagens SIM, e como usar uma imagem salva para respaldar um SIM virtual. O Banco SIM cobre o inventário do leitor ao vivo.

Índice

- Por que SAIP UPP
- Visão Geral da Arquitetura
- O que há em uma Imagem
- Capturando uma Imagem
- Exportando uma Imagem
- Fazendo Upload de uma Imagem
- Navegando em uma Imagem no Explorador
- Comparando Duas Imagens
- Apoiando um SIM Virtual com uma Imagem
- Referência de Elementos de Perfil
- Solução de Problemas

Por que SAIP UPP

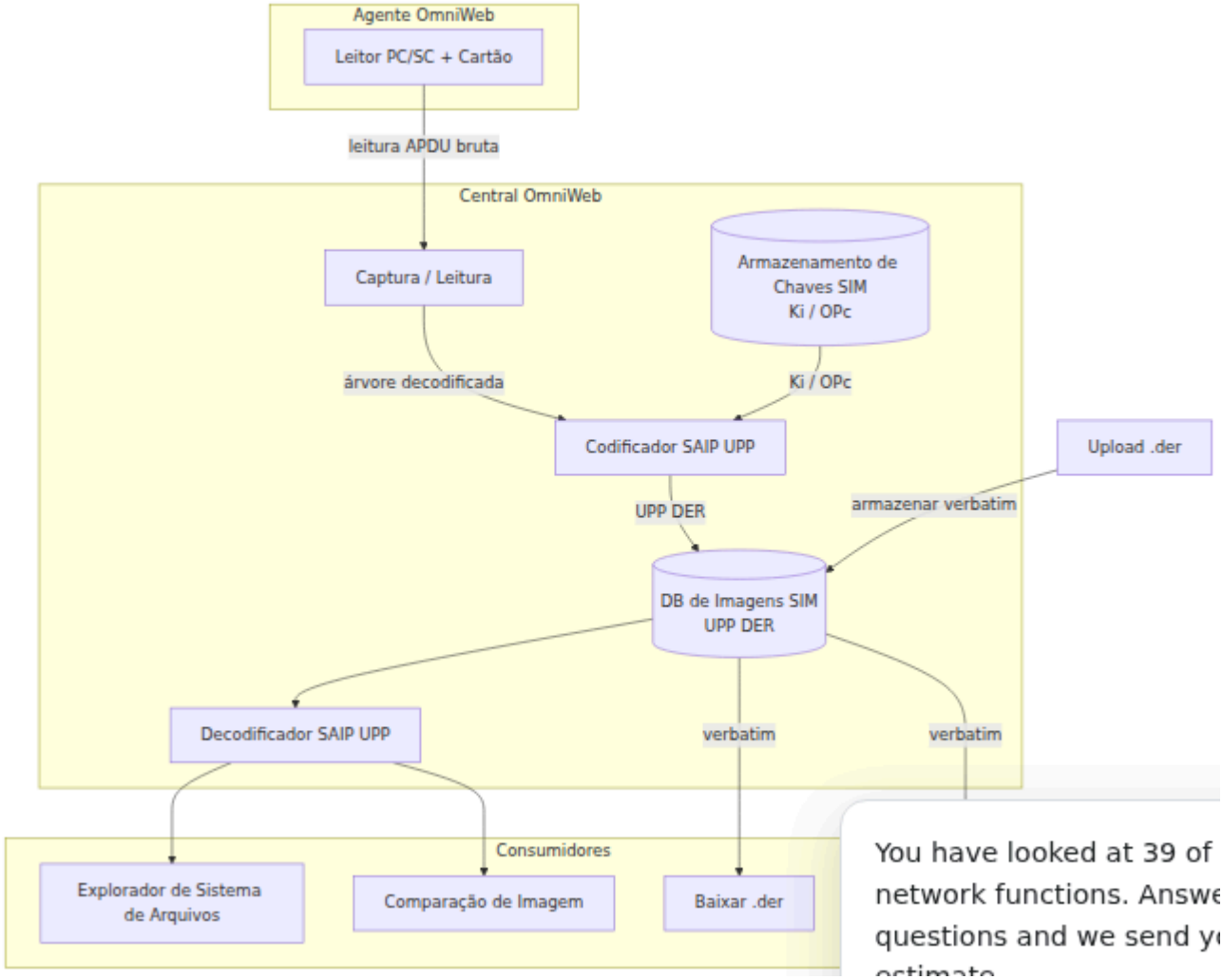
Versões anteriores armazenavam uma imagem SIM como uma árvore JSON decodificada usada apenas para comparação. Esse formato era privado do OmniWeb e nenhuma ferramenta externa poderia consumi-lo.

Quando o OmniWeb armazena a imagem como um **SAIP UPP**, você obtém:

- **Portabilidade**: o `.der` exportado é um pacote de perfil padrão. Ele carrega em validadores de perfil SAIP e qualquer cadeia de ferramentas compatível com SAIP.
- **Um formato em todos os lugares**: o mesmo `.der` que um operador baixa é o que respalda um SIM virtual e o que o explorador de sistema de arquivos renderiza. Não há uma segunda representação divergente.
- **Reprovisionamento**: quando as chaves de autenticação do cartão são conhecidas (veja Capturando uma Imagem), o UPP inclui um elemento `PE-AKAParameter` que carrega Ki e OPc. O pacote então descreve um perfil completo e instalável em vez de um despejo somente leitura.

O pacote é uma concatenação bruta de Elementos de Perfil codificados em DER. Ele **não** é criptografado (é um Pacote de Perfil *Não Protegido*). Trate um `.der` exportado com o mesmo cuidado que qualquer arquivo que contenha Ki/OPc. Veja Solução de Problemas.

Visão Geral da Arquitetura



A captura lê o cartão, o codificador produz um UPP (ele incorpora Ki/OPc do Armazenamento de Chaves SIM, se disponível), e o OmniWeb armazena o pacote. Cada consumidor lê a partir desse único pacote armazenado. O explorador e a comparação o decodificam para uma árvore sob demanda. O download e o banco SIM virtual usam os bytes verbatim.

O que há em uma Imagem

Uma imagem capturada contém, para o layout padrão MF / ADF.USIM do cartão:

Elemento	Elemento de Perfil SAIP	Conteúdos
Sistema de arquivos	`PE-GenericFileManagement`	Cada EF acessível: seus Parâmetros de Controle de Arquivo (FCP) e conteúdo bruto (EFs transparentes) ou cada registro (EFs lineares/cíclicos)
Identidade	`PE-Header`	O ICCID do cartão
Autenticação	`PE-AKAParameter`	Ki e OPc para Milenage. **Presente apenas quando as chaves do cartão estão no Armazenamento de Chaves SIM**

Os arquivos são criados com `PE-GenericFileManagement` (um grupo de operações por DF) em vez dos templates de sistema de arquivos SAIP padronizados: uma leitura de cartão recupera bytes brutos, não o template que um criador de perfil usou originalmente, então a representação genérica é sempre exata.

Capturando uma Imagem

A captura acontece a partir do Sistema de Arquivos SIM no explorador ou nas ações do slot do Banco SIM:

1. Leia o sistema de arquivos de um cartão no explorador.
2. Escolha **Salvar imagem** e dê um rótulo.

O sistema de arquivos decodificado é codificado em um UPP e armazenado. Se uma entrada de Armazenamento de Chaves SIM existir para o ICCID do cartão com **Ki** e **OPc**, essas chaves são escritas em um `PE-AKAParameter`, de modo que o pacote resultante seja totalmente instalável. Sem uma entrada no

armazenamento de chaves, o pacote ainda captura o sistema de arquivos completo; apenas o elemento de autenticação é omitido.

As **colunas de identidade** (ICCID, IMSI, tipo de cartão, contagem de arquivos) são derivadas do sistema de arquivos no momento da captura, de modo que a lista de imagens e o cabeçalho da comparação nunca precisam re-decodificar o pacote.

Exportando uma Imagem

Cada linha na lista de imagens salvas tem uma ação de **download** que serve o pacote armazenado verbatim como `UPP_<iccid>.der`.

O `.der` baixado é um padrão SAIP UPP e pode ser inspecionado com qualquer ferramenta de perfil compatível com SAIP.

Como funciona: O arquivo é exatamente os bytes armazenados na captura (ou upload), sem re-codificação no download, então um download de ida e volta é byte-idêntico ao que está armazenado.

Fazendo Upload de uma Imagem

A página de imagens salvas tem uma ação de **Upload .der** que aceita um arquivo SAIP UPP e o armazena como uma nova imagem. Use-a para trazer perfis gerados em outro lugar: por exemplo, os pacotes de *Perfil de Teste Genérico eUICC* do GSMA TS.48, ou um UPP produzido por outra ferramenta SAIP.

Ao fazer upload, o OmniWeb:

1. Valida se o arquivo começa com uma tag de Elemento de Perfil SAIP (uma tag de classe de contexto construída: `A0`, `A1` ou `B0`).
2. Armazena o pacote verbatim.
3. Decodifica o `PE-Header` para preencher a coluna ICCID onde presente.

Uma imagem carregada é uma imagem de primeira classe: pode ser baixada, navegada no explorador, comparada, editada e usada para respaldar um SIM

virtual exatamente como uma capturada.

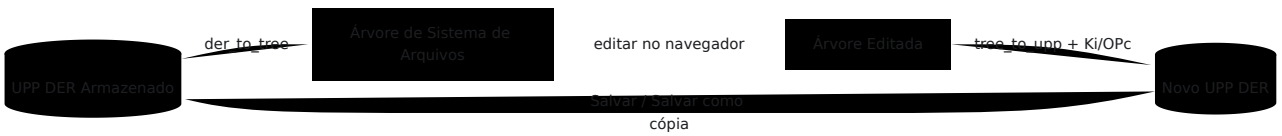
Editando uma Imagem

Uma imagem salva é um **arquivo**, não um cartão. Para editar uma, muda-se apenas o pacote de perfil armazenado e **nunca se escreve em nenhum SIM**. A partir da lista de imagens salvas, a ação **Editar sistema de arquivos** abre o Sistema de Arquivos SIM no modo de edição (`?image=<id>&edit=1`). Nenhum leitor e nenhum acesso ao cartão do agente estão envolvidos.

Você pode:

- **Editar o conteúdo de um arquivo**: mudar os bytes de qualquer EF. Assim como em um cartão ao vivo, o editor oferece um **Formulário** orientado por esquema, uma visão de **JSON** de todo o registro e uma saída de **Hexadecimal Bruto**. Não há prompt de PIN/ADM (um arquivo não tem condições de acesso a serem atendidas).
- **Adicionar um arquivo**: criar um novo EF (transparente ou estruturado em registro) ou DF sob qualquer DF/MF/ADF, e dar seu FID, estrutura e conteúdo inicial.
- **Excluir um arquivo**: remover qualquer EF ou DF (a raiz MF é a imagem inteira e não pode ser deletada).
- **Renomear** a imagem (apenas metadados) a partir da lista.

O navegador mantém as alterações até você **Salvar imagem** (sobrescrever no local) ou **Salvar como cópia** (criar uma nova imagem e deixar a original intocada). Ao salvar, o OmniWeb re-codifica a árvore do sistema de arquivos editada para um SAIP UPP. Ele incorpora Ki/OPc do Armazenamento de Chaves SIM quando conhecido. Ele preserva verbatim qualquer Elemento de Perfil que a árvore não modele (PIN, PUK, Domínio de Segurança, templates), então uma edição nunca descarta o restante do perfil.

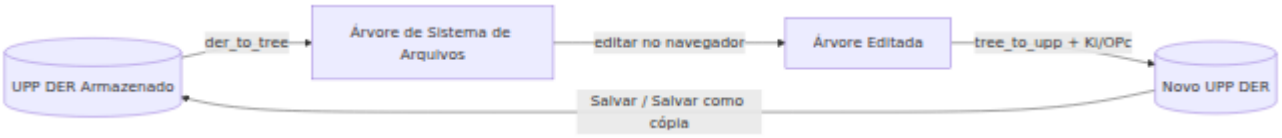


Edição de campo Formulário / JSON offline. Para decodificar um EF em campos nomeados e re-codificá-los, usa-se o mesmo modelo de arquivo que o

editor ao vivo usa, executado em qualquer agente online, mas sem **cartão**: a imagem já contém os bytes, então o agente apenas executa o codec. Se nenhum agente estiver online, a edição recai para Hexadecimal Bruto, que não precisa de nada externo.

Navegando em uma Imagem no Explorador

Cada imagem salva tem uma ação de **Navegar no explorador de sistema de arquivos**. Ela abre o Sistema de Arquivos SIM contra o pacote armazenado. **Nenhum cartão físico e nenhum leitor são necessários**. O OmniWeb decodifica o pacote de volta para a mesma árvore de sistema de arquivos que o explorador renderiza para um cartão ao vivo, para que você possa inspecionar o conteúdo bruto de cada EF offline.



Comparando Duas Imagens

A página de imagens salvas permite que você escolha duas imagens e as compare. Ambos os pacotes são decodificados em árvores de sistema de arquivos e alinhados por caminho EF, de modo que a comparação é arquivo por arquivo, independentemente da ordem de captura:

Status	Significado
`same`	EF presente em ambos com conteúdo idêntico
`changed`	EF presente em ambos, conteúdo difere
`only_a`	EF presente apenas na primeira imagem
`only_b`	EF presente apenas na segunda imagem

Para um EF **mudado**, a comparação relata os intervalos de bytes diferentes (e deltas por registro para arquivos estruturados em registro), para que você possa ver exatamente quais bytes mudaram: por exemplo, um SIM de teste antes e depois de uma mudança de personalização, ou dois SIMs de operadores lado a lado.

Apoiando um SIM Virtual com uma Imagem

Uma imagem salva pode substituir um cartão físico ao apresentar um SIM virtual. No compositor de SIM virtual, imagens salvas aparecem ao lado das imagens rspro capturadas como fontes de sistema de arquivos selecionáveis. Combine uma com uma identidade de assinante (do HSS ou do Armazenamento de Chaves SIM) e o OmniWeb lança um `bankd` virtual respaldado pelo sistema de arquivos daquela imagem, com Ki/OPc do assinante sobrepostos para autenticação.



O sistema de arquivos que o modem lê é reproduzido a partir da imagem; a identidade e as chaves são sobrepostas a partir do assinante escolhido, de modo que uma imagem pode respaldar muitos assinantes.

Referência de Elementos de Perfil

O UPP é uma sequência de Elementos de Perfil, cada um um DER TLV cuja tag de classe de contexto identifica seu tipo. O OmniWeb escreve e lê o subconjunto abaixo; outros elementos em um pacote carregado (PIN, PUK, Domínio de Segurança, templates de sistema de arquivos) são preservados no armazenamento e ignorados ao decodificar para uma árvore de sistema de arquivos.

Tag	Elemento de Perfil	Usado pelo OmniWeb
`A0`	`PE-Header`	ICCID; metadados do perfil
`A1`	`PE-GenericFileManagement`	O sistema de arquivos (FCP + conteúdo)
`A4`	`PE-AKAParameter`	Ki e OPc (Milenage)
`AA`	`PE-End`	Marcador de fim de pacote
`B0`	`PE-MF`	(MF template: lido no upload, não emitido)

Para o catálogo completo de elementos e regras de codificação, veja a Especificação Técnica de Formato Interoperável de Pacote de Perfil eUICC do TCA.

Solução de Problemas

Imagem exportada sem chaves de autenticação

Sintomas: Um `.der` baixado não possui `PE-AKAParameter`; um SIM virtual respaldado pela imagem não pode autenticar sem chaves fornecidas separadamente.

Possíveis causas:

- Nenhuma entrada no Armazenamento de Chaves SIM existia para o ICCID do cartão no momento da captura.
- A entrada do armazenamento de chaves estava faltando Ki ou OPc.

Resolução:

1. Adicione o Ki e OPc do cartão ao Armazenamento de Chaves SIM, indexado pelo seu ICCID.
2. Recapture a imagem. A nova captura incorpora as chaves em um `PE-AKAParameter`.
3. Alternativamente, forneça as chaves no momento da apresentação do SIM virtual (do HSS ou uma substituição explícita).

Upload rejeitado como "não parece um SAIP UPP"

Sintomas: Fazer upload de um arquivo retorna um erro de validação.

Possíveis causas:

- O arquivo não é um SAIP UPP: não começa com uma tag de Elemento de Perfil (`A0`, `A1` ou `B0`).
- O arquivo é um pacote de perfil *protegido* (criptografado), não um *não protegido*.

Resolução:

1. Confirme que o arquivo é um **Pacote de Perfil Não Protegido** em codificação DER.
2. Verifique se começa com um `PE-Header` (`A0`). A maioria dos UPPs bem formados faz isso.
3. Se o pacote estiver protegido/criptografado, não pode ser armazenado ou navegado; apenas pacotes não protegidos são suportados.

Navegar em uma imagem carregada mostra arquivos por FID, não por nome

Sintomas: EFs no explorador são rotulados pelo identificador de arquivo (por exemplo, `EF.6FXX`) em vez de um nome amigável.

Possíveis causas:

- Uma leitura de cartão recupera identificadores de arquivo e conteúdo bruto, não os nomes simbólicos que um criador de perfil usou. O OmniWeb mapeia os EFs USIM bem conhecidos para nomes amigáveis; qualquer EF fora desse mapeamento é mostrado pelo seu FID.

Resolução: Nenhuma ação é necessária. O FID é o identificador autoritativo e o conteúdo bruto é exato. Isso é esperado para arquivos não padronizados ou específicos de fornecedor.

Exportação recusada por não conformidade

Sintomas: Exportar uma imagem ou uma versão de perfil retorna uma recusa que nomeia um ou mais arquivos e uma regra de especificação, em vez de retornar um arquivo.

Possíveis causas: O pacote carrega uma falha que um cartão aceitaria na instalação e então se comportaria mal, então é barrado antes que possa chegar a um. As verificações cobrem as falhas que realmente chegaram ao hardware:

- Um arquivo de registro cujo tamanho não é um número inteiro de registros.
- Um arquivo de regra de acesso que não se organiza como registros inteiros, o que torna cada arquivo que o referencia ilegível no cartão.
- Uma tabela de serviços que anuncia um serviço cujo arquivo o pacote não contém. A cláusula 4.2 do 3GPP TS 31.102 torna cada um desses arquivos obrigatório exatamente quando seu serviço lê disponível.
- Material de segurança ausente ou de espaço reservado, que é coberto separadamente acima.

Resolução: Leia a recusa, que nomeia o arquivo e a regra. Para uma versão de perfil, publique uma nova versão: o codificador atual resolve essas questões e uma versão publicada é imutável, então a correção chega como uma nova versão em vez de uma edição. Se a recusa nomeia uma entrada de tabela de serviços e você deseja o serviço em vez do estreitamento, adicione o arquivo ausente ao perfil e publique novamente.

Manuseio seguro de pacotes exportados

Um UPP exportado é **não criptografado** e, quando as chaves estavam disponíveis na captura, contém Ki e OPc. Trate um `.der` baixado como material sensível de chave:

- Não o envie por canais não confiáveis.
- Exclua cópias locais quando não forem mais necessárias.
- Prefira manter imagens dentro do OmniWeb (onde o acesso é controlado pela permissão do Banco SIM) em vez de distribuir arquivos `.der`.

Ciclo de Vida do SIM: perfis, emissão e convergência

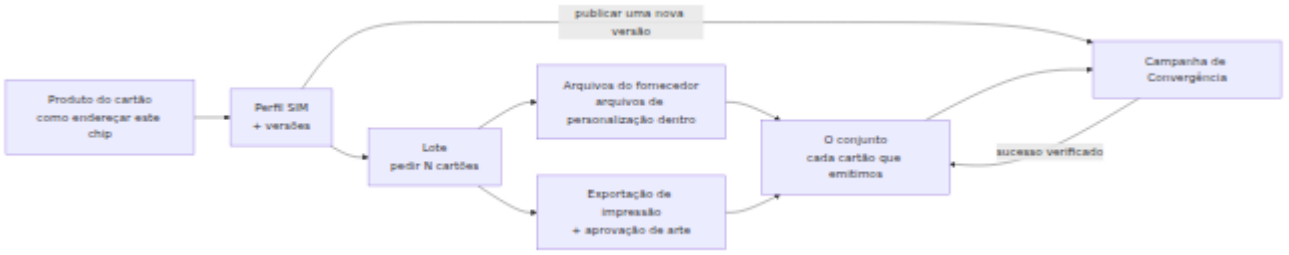
OmniWeb é o sistema de registro para um conjunto de SIMs. Você **define** um perfil, **emite** cartões contra ele, **imprime** os portadores e, em seguida, **gerencia** esses cartões via OTA pelo resto de suas vidas.

A ideia organizadora é que **o perfil de emissão é o estado desejado**. O mesmo artefato versionado que fabricou um cartão é aquele ao qual o OmniWeb converte esse cartão de volta. Duas coisas se seguem, e elas são a razão do design:

- OTA se torna um **motor de diferença**. Publique uma nova versão de perfil, e cada cartão emitido contra uma versão anterior está, por definição, atrasado. Você não escreve scripts de atualização manualmente.
- A linha de base é **conhecida, não adivinhada**. O OmniWeb não precisa ler um cartão para saber o que está nele, porque o OmniWeb o colocou lá. Ler o cartão de volta é uma **auditoria**: uma etapa de verificação que você executa quando deseja prova, não uma pré-condição para cada gravação.

Esta página cobre as etapas de definição, emissão e convergência. A etapa de entrega - os pacotes seguros que carregam uma alteração para um cartão - está documentada em Gerenciamento de SIM OTA. A emissão de eSIM está documentada em eSIM (SGP.22).

O ciclo de vida



O registro de um cartão carrega dois ponteiros de versão:

Ponteiro	Significado
Versão emitida	A versão do perfil com a qual o chip foi gravado na fabricação.
Versão aplicada	A versão que o OmniWeb acredita estar no cartão agora.
Versão alvo	A versão atual publicada do perfil. Derivada, não armazenada.

Um cartão está **atrasado** quando sua versão aplicada é inferior à versão alvo. A convergência avança a versão aplicada, e apenas após uma varredura limpa e verificada.

Onde encontrá-lo

O grupo **SIMs** na barra lateral contém as páginas do ciclo de vida. Cada página do ciclo de vida também possui uma faixa de abas na parte superior, que é a única maneira de acessar a Convergência.

Página	Caminho	Para que serve
Perfis SIM	`/sim-profiles`	Definir o que um cartão deve conter. Versioná-lo. Publicá-lo.
Produtos de Cartão	`/card-products`	Registrar como endereçar um chip em cada portador.
Lotes	`/sim-batches`	Pedir cartões, alocar identidades, trocar arquivos com o fornecedor e a impressora.
Conjunto	`/sim-estate`	Cada cartão emitido, e quais deles estão atrasados.
Convergência	`/ota/sync`	Campanhas que trazem cartões de volta em sincronia, e desvio da frota.

Produtos de cartão

Um **produto de cartão** é um tipo de cartão que você pode pedir: uma linha de produto físico ou um produto eSIM. Ele carrega o endereçamento OTA para cada cartão feito nele.

O endereçamento é importante porque **a mesma operação de arquivo precisa de endereçamento diferente em chips diferentes, e no mesmo chip em diferentes portadores**. Um SMS seguro roteia em um TAR; uma sessão de administração HTTP nomeia a aplicação pelo seu AID de instância. Uma aplicação responde a uma classe de comando GSM, outra responde a uma UICC. Um cartão aceita um script de comando expandido apenas em sua forma de comprimento definido e não responde a nada na forma indefinida. Qualquer uma dessas falhas parece idêntica da cadeira do operador: um cartão que ignorou você.

Assim, o endereçamento é registrado uma vez, por produto, e cada cartão emitido nesse produto herda isso. **Adicionar um novo tipo de cartão é configuração, não código.**

Campos do produto

Campo	Descrição
`name`	O nome do produto, como você o pede. Único.
`vendor`	O fabricante do cartão.
`form`	`physical` para um cartão plástico, `esim` para um produto eSIM.
`atr_hint`	A Resposta ao Reset que este produto deve fornecer. O Conjunto compara isso com o ATR lido do cartão.
`platform_notes`	Texto livre. Registre qualquer coisa que a plataforma faça que sua ficha técnica não menciona.

Endereçamento do portador

Um produto carrega uma linha por aplicação acessível por portador. Uma linha por portador é o padrão.

Campo	Descrição
`bearer`	`SMS (SCP80)` ou `HTTP (SCP81)`.
`label`	Um nome para esta aplicação, por exemplo `rfm-gsm`.
`is_default`	Se esta linha é a usada quando nada mais é escolhido.
`enabled`	Se esta linha pode ser usada ou não.
`tar`	O Toolkit Application Reference de 3 bytes em que um SMS seguro roteia.
`rfm_aid`	O AID de instância da aplicação RFM, que uma sessão HTTP nomeia diretamente. Quando apenas o AID é registrado, o TAR é lido dele.
`cla`	A classe de comando que a aplicação responde: `00` para UICC, `A0` para GSM. A aplicação e a classe andam juntas.
`remote_format`	`compact`, `expanded_definite` ou `expanded_indefinite`.
`keyset_index`	Qual conjunto de chaves OTA (1, 2 ou 3) no cartão esta aplicação usa.
`tls_kvn` / `tls_kid`	Qual conjunto de chaves no cartão carrega a chave pré-compartilhada TLS para sessões HTTP.
`reachable_paths`	Quais árvores de arquivos esta aplicação pode acessar, como prefixos de caminho. Vazio significa desconhecido ou irrestrito.

OmniWeb fornece endereçamento comprovado para os produtos listados em Cartões suportados e plataformas testadas. Produtos semeados nunca são

editados posteriormente, então uma correção que você faz sobrevive a uma atualização.

Perfis e versões SIM

Um **perfil SIM** é um estado desejado nomeado. Ele pertence a um cliente e a um produto de cartão, e contém uma lista ordenada de versões.

> Não confunda um perfil SIM com um **perfil OTA**. Um perfil OTA é uma pré-configuração de segurança - TAR, conjunto de chaves, algoritmos, nível de segurança - e está documentado em Gerenciamento de SIM OTA.

Status do perfil	Significado
`draft`	Sendo escrito. Ainda não usado para emissão.
`active`	Em serviço. Novos lotes pedem contra sua versão atual.
`retired`	Não mais emitido. Cartões já em campo mantêm seu perfil.

Versões

Crie uma versão a partir de uma imagem SIM salva, ou colando um pacote de perfil. Uma versão permanece como **rascunho** até que você a publique.

Publicar faz três coisas, e é unilateral:

1. Indexa cada arquivo no perfil, para que uma versão posterior possa ser comparada com ele.
2. Semeia a **política de arquivos** para essa versão.
3. Torna-se a versão atual do perfil, o que faz com que cada cartão abaixo dela esteja atrasado.

Uma versão publicada é **imutável**. Publicar a mesma versão duas vezes é recusado. Para mudar qualquer coisa, crie a próxima versão. Isso é o que torna a história de um cartão legível: um número de versão nomeia um conjunto exato de conteúdos de arquivo, para sempre.

Use **Diff** para ver o que uma campanha mudaria entre duas versões publicadas, arquivo por arquivo, antes de publicar ou enfileirar qualquer coisa.

Política de arquivos

A política de arquivos classifica cada arquivo em uma versão e decide o que uma campanha pode fazer com ele.

Tipo	Significado	Uma campanha pode escrevê-lo?
`fixed`	O mesmo em cada cartão emitido contra esta versão. Um nome de operador, uma lista PLMN, uma tabela de serviços.	Sim, quando gerenciado por OTA.
`personalized`	Diferente em cada cartão. O ICCID, o IMSI, o MSISDN, o PIN. Vem do registro de emissão.	Não.
`card_owned`	O cartão escreve isso por conta própria. Informações de localização, listas de PLMN proibidos, contadores.	Não.

Cada linha também carrega um interruptor **gerenciado por OTA**. Um arquivo é **gravável** por uma campanha apenas quando é `fixed` **e** gerenciado por OTA. Tudo o mais é somente leitura, o que impede que uma execução de convergência redefina o estado próprio de um assinante ou sobrescreva uma identidade.

A política é indexada pelo caminho do arquivo, não pelo nome do arquivo. O mesmo nome de EF pode existir em dois lugares em um cartão, e escrever a cópia errada é bem-sucedido em cada etapa e não muda nada que o telefone leia. Dois caminhos são duas linhas de política, e o autor do perfil escolhe uma ou ambas.

Duas regras merecem ser declaradas claramente:

- **Nunca deixe uma campanha escrever o ICCID do cartão.** O ICCID é como todo o sistema endereça o cartão, e é a identidade na qual uma chave pré-compartilhada TLS é correspondida. A política semeada a fixa.
- A correção de um operador a uma linha de política **sobrevive a uma re-semeadura**. Se você reclassificar um arquivo, ele permanece reclassificado.

Emissão: lotes

Um **lote** é um pedido de produção: *N* cartões fabricados contra uma versão de perfil publicada.

Pedindo um lote

Campo	Descrição
Nome do lote	Seu nome para esta execução de produção.
Versão do perfil	A versão publicada com a qual os cartões são gravados. Versões de rascunho não são oferecidas.
Cliente	Para quem os cartões são.
Fornecedor	Quem os fabrica.
Referência do pedido / Referência do PO	Suas referências comerciais, para correspondência de documentos mais tarde.
Quantidade	Quantos cartões.
Primeiro ICCID	O primeiro ICCID na série.
Primeiro IMSI	O primeiro IMSI na série.
Primeiro MSISDN	O primeiro MSISDN na série, quando o lote carrega números.
Notas	Texto livre.

A série ICCID **recomputará o dígito de verificação para cada cartão** em vez de incrementar o último dígito. Fazer isso errado numera silenciosamente todo um lote de produção, então é explícito em vez de presumido.

Status do lote	Significado
`draft`	Criado, ainda não alocado.
`allocated`	Identidades e segredos existem para cada cartão.
`sent`	O arquivo de entrada do fornecedor foi enviado ao fabricante.
`in_production`	O fornecedor está fabricando-os.
`delivered`	Os cartões chegaram.
`cancelled`	O pedido não prosseguirá.

Alocar

Alocar cria um registro de cartão por unidade e gera os próprios segredos desse cartão:

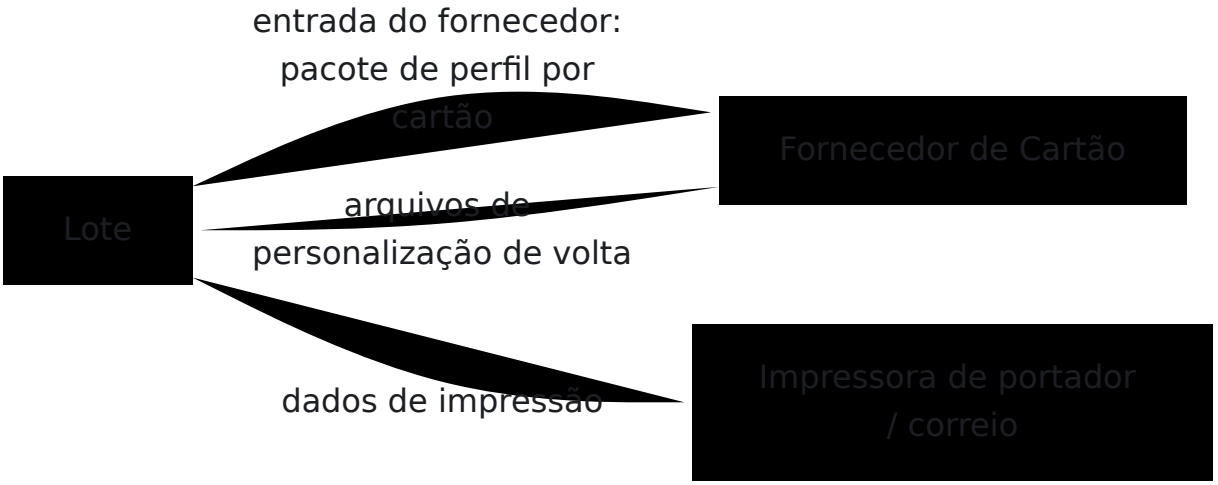
- o material da chave de autenticação,
- PIN 1, PUK 1, PIN 2, PUK 2 e a chave ADM,
- todos os três conjuntos de chaves OTA,
- uma chave pré-compartilhada TLS independente para sessões de administração HTTP.

Cada valor é gerado **por cartão**. Um lote que envia um conjunto de chaves para todos os cartões significa que qualquer um que leia um único cartão pode dirigir OTA contra todos eles, e nada a jusante notaria, porque um conjunto de chaves compartilhado funciona.

A alocação é executada **uma vez**. Uma segunda execução queimaria outro bloco de identidades e orfão o primeiro, então é recusada.

Arquivos para fora, arquivos para dentro e arquivos para a impressora

Um lote troca três tipos de arquivo com o mundo exterior.



Exportar	O que carrega	O que deliberadamente omite
Arquivo do fornecedor	ICCID, IMSI, PIN 1, PUK 1, PIN 2, PUK 2, ADM e as chaves de autenticação, no conjunto de colunas do fornecedor.	Os conjuntos de chaves OTA.
Dados de impressão	ICCID, IMSI, MSISDN, PIN 1, PUK 1, PIN 2, PUK 2, e para eSIM o EID e o código de ativação.	A chave ADM e cada chave OTA. Nada que chegue a uma impressora precisa delas.

A **entrada do fornecedor** para um chip é a versão do perfil com os próprios valores desse cartão substituídos. Esse é o artefato do qual o chip é gravado, e é o que permite que uma campanha compare contra ele com confiança mais tarde.

Importar chaves lê arquivos de personalização de volta do fornecedor para o armazenamento de chaves. Dois formatos são aceitos:

Formato	Notas
Delimitado com uma linha de cabeçalho (CSV ou TSV)	O conjunto de colunas do fornecedor comum. Esteja ciente de que um arquivo de coluna desse formato geralmente não carrega chaves OTA, e um cartão sem chaves OTA não pode ser gerenciado via OTA.
Arquivo variável do fornecedor	O formato que carrega os conjuntos de chaves OTA e a chave pré-compartilhada TLS.

O relatório de importação informa quantas linhas foram novas, atualizadas e ignoradas. Verifique o primeiro arquivo real de um fornecedor contra um pequeno lote antes que uma migração se baseie nele.

Arte e aprovação

Anexe a arte de impressão ao lote ao qual pertence e mantenha a trilha de aprovação com ele.

Tipo de arte	Uso típico
`card_face`	A face impressa do cartão.
`card_back`	O verso.
`carrier`	O portador em que o cartão é perfurado.
`qr_sheet`	A folha de código de ativação para um lote de eSIM.
`packaging`	Embalagem externa.
`other`	Qualquer outra coisa.

Cada arquivo carrega um número de versão. Um item é **pendente** ou aprovado, e um item aprovado registra quem o aprovou e quando.

Conjuntos de chaves e a imagem na qual foram construídos

Um conjunto de chaves contém os segredos de um cartão. Por si só, não diz em qual sistema de arquivos esses segredos estão, e um perfil não diz quais cartões o carregam. Vincule os dois, e ambas as perguntas têm uma resposta.

Vincule um conjunto de chaves ao seu perfil. Você pode fazer isso por cartão ou para um arquivo de fornecedor inteiro ao importá-lo. Um arquivo de fornecedor cobre uma execução de produção, e cada cartão nessa execução carrega o mesmo sistema de arquivos, então o vínculo pertence à importação.

A página do perfil então lista os cartões construídos nessa imagem:

Coluna	Significado
ICCID / IMSI	As identidades do cartão.
Lote	A execução de produção, quando o cartão está no conjunto.
Chaves mantidas	Qual material de chave está presente: chaves de autenticação, quais conjuntos de chaves OTA, e uma chave pré-compartilhada TLS.
Na versão	A revisão em que o cartão realmente está.
Estado	`in step`, `behind`, ou `keys only`.

A lista mostra qual material de chave está presente, nunca seu valor. Abra o conjunto de chaves em si para ver os valores.

`keys only` significa que o cartão tem chaves aqui, mas nenhum registro no conjunto. Isso é normal para um conjunto emitido em outro lugar, onde o arquivo de chave do fornecedor é o único registro que você possui. Esses cartões ainda podem ser alvo de uma campanha.

O vínculo é para o perfil, não para uma de suas revisões. As chaves de um cartão não mudam quando você publica uma nova revisão; o sistema de arquivos muda. A revisão em que um cartão está é rastreada por cartão, então nunca é registrada duas vezes.

O conjunto

A página **Conjunto** é cada cartão que o OmniWeb emitiu, com desvio computado por cartão.

Coluna	Significado
ICCID / IMSI / MSISDN	As identidades do cartão, conforme alocadas.
Lote	A execução de produção da qual veio.
Emitido	A versão gravada na fabricação.
No cartão	A versão que o OmniWeb acredita estar no cartão agora.
Deveria ser	A versão atual publicada do perfil.
Estado	`in step`, ou `behind` quando o cartão está abaixo da versão alvo.
Forma	`physical` ou `esim`.
ATR	A Resposta ao Reset realmente lida do cartão, ou `not seen`.
Status	`allocated`, `issued`, `active`, `suspended` ou `terminated`.
Última sincronização	Quando uma campanha tocou o cartão pela última vez, ou o último erro em vermelho.

Filtre por perfil, por prefixo ICCID, por forma, ou com **Apenas atrás de seu perfil**.

A coluna ATR é evidência, não decoração. Ela é preenchida na primeira vez que um cartão aparece em um leitor. Se não corresponder ao que o produto do cartão espera, a coluna fica vermelha. Isso significa que o chip em mãos não é a plataforma que você pediu, o que muda como o OTA deve endereçá-lo. É muito melhor ver isso aqui do que descobrir mais tarde como um cartão que ignora cada pacote.

Editar cartão corrige o registro de um cartão: seu status, seu MSISDN, e para um eSIM seu EID, endereço SM-DP+, ID de correspondência, código de confirmação e estado de download. As colunas de versão não são deliberadamente editáveis. Elas são um registro do que aconteceu, e apenas uma emissão ou uma campanha verificada as move.

Campanhas de convergência

Uma **campanha de convergência** é declarativa: *faça esses cartões corresponderem a esta versão de perfil*. O que isso significa para cada cartão é computado, não escrito à mão.

Isso é diferente de uma **campanha OTA**, que é imperativa: *execute esta operação contra esses cartões*. As campanhas OTA estão documentadas em Gerenciamento de SIM OTA. Use uma campanha de convergência para aplicar uma mudança de perfil em um conjunto. Use uma campanha OTA para uma operação única que não é uma mudança de perfil.

Criando uma campanha

Campo	Descrição
Nome	Seu nome para a execução.
Perfil	Apenas perfis com uma versão atual publicada são oferecidos.
Lotes	Quais lotes estão em escopo. **Um conjunto de destino vazio não corresponde a nada, deliberadamente.**
Cada SIM nesta imagem	Cada cartão cujo conjunto de chaves está vinculado a este perfil. Use isso para alcançar cartões emitidos em outros lugares, que têm chaves aqui, mas nenhum lote.
Portador	`Auto`, `SMS (SCP80)` ou `HTTP (SCP81)`. `Auto` escolhe entre os portadores do produto do cartão.
Conclusão	`Verificar lendo de volta`, ou `Disparar e esquecer`.
REFRESH	`Nenhum`, `reset UICC`, ou `notificação de alteração de arquivo`. O que o cartão é solicitado a fazer uma vez que os arquivos tenham mudado.
Máx por hora	Um teto de frota em entregas. `0` significa ilimitado.
Mínimo de intervalo	O espaçamento mínimo em segundos entre duas entregas para o mesmo cartão. `0` significa nenhum.
Máx tentativas	Quantas vezes um cartão é tentado antes que o trabalho falhe.
Prazo de resposta	Quantos minutos esperar pela resposta do cartão antes que a tentativa seja abandonada. `0` desativa o prazo.

Campo	Descrição
Execução a seco	Uma execução a seco planeja e enfileira, e se recusa a transmitir. Uma nova campanha é sempre uma execução a seco.

Defina o ritmo deliberadamente. Um link de sinalização que transporta tráfego OTA tem um orçamento finito, e um cartão que falha em sessões de administração repetidamente estaciona em um retrocesso de até 24 horas que nada limpa. Uma campanha que roda lentamente termina; uma campanha que inunda não.

Uma campanha é limitada a 5000 cartões-alvo. Se o filtro corresponder a mais, restrinja-o e execute o restante como uma segunda campanha.

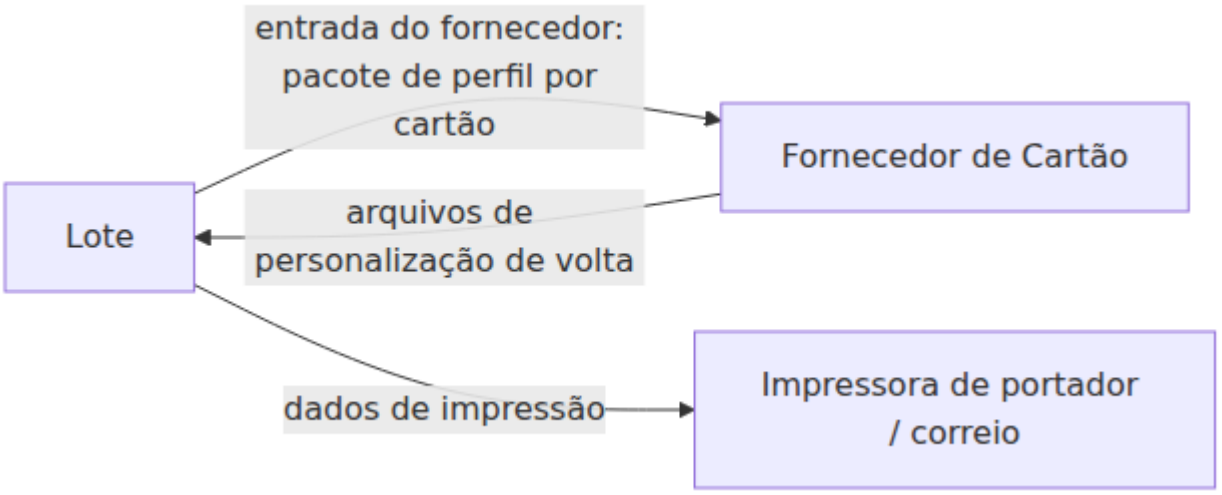
Revise a mudança antes de armá-la

Uma nova campanha é uma execução a seco. Ela computa a diferença de cada cartão e enfileira os trabalhos, e se recusa a transmitir. Armar é uma ação separada, e é a única coisa que permite que uma campanha alcance um cartão.

Use a pré-visualização na página do perfil para ver o que uma mudança envia. A pré-visualização mostra, para cada portador:

- os arquivos que diferem, e quantos comandos cada um custa
- o script de comando, exatamente como seria construído
- os caminhos que este portador não pode alcançar, que precisam de um aplicativo diferente de gerenciamento de arquivos remotos
- quantos cartões correspondem, e quantos estão atrasados em relação à versão alvo

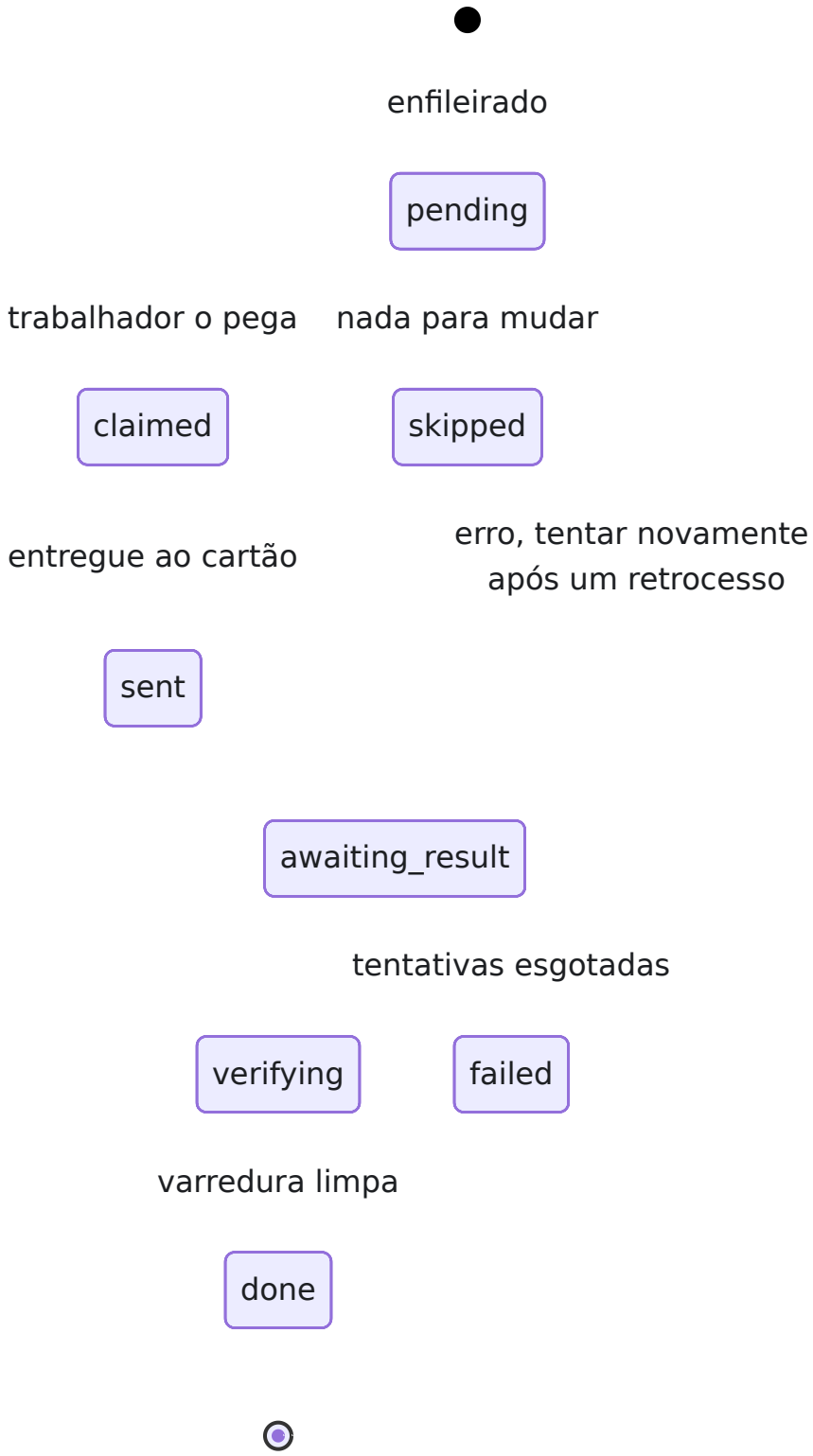
A pré-visualização não lê nenhum material de chave. Um script se torna um pacote seguro apenas no momento do envio, usando as próprias chaves do cartão, então a pré-visualização é segura para executar contra um conjunto ativo.



Arme uma campanha apenas depois de ter lido a pré-visualização. O dano que uma campanha pode causar é proporcional ao número de cartões que ela corresponde.

Enfileirar e, em seguida, executar

Enfileirar computa a diferença de cada cartão em relação à versão alvo, renderiza o script e cria um trabalho por cartão. Nada é enviado nesse ponto. Um trabalhador então pega os trabalhos e os entrega, dentro do ritmo que você definiu.


enfileirado
pending
trabalhador o pega
nada para mudar
claimed
skipped
entregue ao cartão
erro, tentar novamente
após um retrocesso
sent
awaiting_result
tentativas esgotadas
verifying
failed
varredura limpa
done

Estado do trabalho	Significado
`pending`	Enfileirado, ainda não reivindicado.
`claimed`	Um trabalhador o possui. Dois trabalhadores nunca retiram o mesmo cartão.
`sent`	O script foi enviado ao cartão.
`awaiting result`	Aguardando a resposta do cartão.
`verifying`	Verificando o que o cartão realmente fez.
`done`	Aplicado e verificado. A versão aplicada do cartão avança.
`failed`	Tentativas esgotadas. O erro está na linha.
`skipped`	Não havia nada para mudar, ou nada que pudesse ser mudado com segurança.

O controle da campanha está em cada linha: **Pausar** deixa o trabalho em fila no lugar, **Retomar** continua e **Cancelar** retira o trabalho que não começou.

Status da campanha	Significado
`draft`	Criado, nada em fila.
`running`	Trabalhos estão sendo entregues.
`paused`	A entrega está parada. Trabalhos em fila permanecem.
`complete`	Cada trabalho alcançou um estado final.
`failed`	A execução terminou com falhas.
`cancelled`	Retirado.

Quando um cartão não responde

Um cartão que está desligado, fora de cobertura ou cuja resposta foi perdida não envia nada de volta. Nada chega para finalizar o trabalho, então o prazo de resposta é o que o move adiante.

Situação	Resultado
O cartão responde	O trabalho se estabelece com o que o cartão relatou.
Sem resposta dentro do prazo, tentativas restantes	A tentativa é abandonada. O trabalho retorna para `pending` e é tentado novamente após o back-off.
Sem resposta dentro do prazo, sem tentativas restantes	O trabalho falha e registra que o cartão nunca respondeu.
Um erro de entrega que pode ser refeito	O mesmo back-off se aplica.

As esperas entre as tentativas aumentam, então um cartão que está desligado por um longo tempo não é tentado com força. A lista de trabalhos mostra o estado, o número da tentativa e quando a próxima tentativa está prevista.

Reenviar um script é seguro. Cada comando em um script de convergência é uma atualização, então executar o script inteiro novamente reaplica os arquivos que já foram entregues e então continua. Um trabalho que foi parcialmente aplicado é reencaminhado por completo.

O que uma campanha pode fazer

Um script renderizado contém **apenas** seleções de arquivos e atualizações de arquivos, sobre caminhos que a política de arquivos marca como graváveis. Essa restrição é o que torna um reencaminhamento seguro: executar o mesmo script duas vezes deixa o cartão no mesmo lugar, então um trabalho que parou no meio pode simplesmente ser tentado novamente.

Dois comportamentos seguem do cartão, não do OmniWeb, e ambos valem a pena serem esperados:

- **Um script para no primeiro erro.** Uma atualização de vinte arquivos que falha no arquivo sete deixa seis arquivos aplicados. Esse trabalho é relatado como parcial, nunca como bem-sucedido, e é tentado novamente.
- **Um reconhecimento não é execução.** Um cartão pode aceitar um script e não executar nada. Apenas as respostas por comando dizem o que foi executado, e é por isso que o veredicto de uma campanha vem dessas respostas e não apenas da entrega.

Deriva da frota

A página de Convergência abre em **Deriva da frota**: uma linha por perfil, mostrando a versão atual, quantos cartões estão nela, quantos estão atrasados e a distribuição de versões por toda a propriedade. Use-a para decidir se uma campanha é necessária antes de criar uma.

Limitações atuais

Duas opções de campanha são registradas e honradas pela fila, mas ainda não são realizadas automaticamente pelo trabalhador de entrega:

- `Verify by reading back` ainda não lê cada arquivo de volta após uma gravação. Para verificar um cartão hoje, execute uma **auditoria** (abaixo).
- `REFRESH` é armazenado na campanha, mas ainda não é enviado ao cartão.

Auditoria: corrigindo o que o OmniWeb acredita

A versão aplicada é uma **crença**. Uma auditoria é o que a corrige.

Uma auditoria lê os arquivos gerenciados de um cartão de volta pelo ar e compara cada um contra a versão que o OmniWeb espera. Ela relata, por arquivo, o valor esperado, o valor realmente no cartão e se eles correspondem. É iniciada pelo operador e nunca faz parte de uma campanha, porque cada arquivo verificado custa uma viagem OTA.

Execute uma auditoria quando a evidência e o registro discordarem: após uma migração de outra plataforma, após um lote chegar de um novo fornecedor, ou quando um cartão se comporta como se uma mudança nunca tivesse sido aplicada. Nunca corrija o registro de um cartão a partir de um palpite. Corrija-o a partir de uma auditoria.

Auditorias estão disponíveis através de `POST /api/ota/sync/audit`. A auditoria de acesso separada access audit nas páginas OTA responde a uma pergunta diferente: quais operações um conjunto de chaves está autorizado a realizar em cada arquivo.

REST API

Todas as rotas requerem um JWT. Veja a API Reference.

Produtos de cartão

Método	Rota	Propósito
GET, POST	`/api/simbank/card-products`	Listar ou criar um produto de cartão.
GET, PUT, DELETE	`/api/simbank/card-products/<id>`	Ler, atualizar ou excluir um.
POST	`/api/simbank/card-products/<id>/bearers`	Adicionar endereçamento de portador.
PUT, DELETE	`/api/simbank/card-products/<id>/bearers/<bearer_id>`	Atualizar ou remover uma linha de portador.

Perfis e versões

Método	Rota	Propó
GET, POST	`/api/simbank/profiles`	Listar o criar pe
GET, PUT, DELETE	`/api/simbank/profiles/<id>`	Detalhe perfil, incluind suas ve
GET, POST	`/api/simbank/profiles/<id>/versions`	Listar versões criar un rascunh partir d uma im ou um pacote perfil co
GET, DELETE	`/api/simbank/profiles/<id>/versions/<vid>`	Ler uma versão excluir rascunh
POST	`/api/simbank/profiles/<id>/versions/<vid>/publish`	Publica Unidire
GET, PUT	`/api/simbank/profiles/<id>/versions/<vid>/policy`	Ler ou atualiza política arquivo
GET	`/api/simbank/profiles/<id>/versions/<vid>/diff`	O que c entre d

Método	Rota	Propó
		versões

Lotes e a propriedade

Método	Rota	Propósito
GET, POST	`/api/simbank/batches`	Listar ou criar lotes.
GET, PUT, DELETE	`/api/simbank/batches/<id>`	Detalhes do lote, incluindo arte.
POST	`/api/simbank/batches/<id>/allocate`	Alocar identidades e segredos. Não repetível.
GET	`/api/simbank/batches/<id>/export`	Baixar dados de impressão ou o arquivo do fornecedor.
POST	`/api/simbank/batches/<id>/artwork`	Fazer upload de um arquivo de arte.
POST, DELETE	`/api/simbank/batches/<id>/artwork/<aid>`	Aprovar ou excluir um item de arte.
POST	`/api/simbank/keys/import`	Importar material de chave do fornecedor.
GET	`/api/simbank/issued`	A propriedade, com deriva

Método	Rota	Propósito
		computada por cartão.
GET, PUT	`/api/simbank/issued/<iccid>`	Ler ou corrigir o registro de um cartão.

Convergência

Método	Rota	Propósito
GET, POST	`/api/ota/sync/campaigns`	Listar ou criar campanhas.
GET, PUT, DELETE	`/api/ota/sync/campaigns/<id>`	Ler, atualizar ou excluir uma.
GET	`/api/ota/sync/campaigns/<id>/targets`	Quais cartões correspondem e quantos estão atrasados.
POST	`/api/ota/sync/preview`	Renderizar o que uma mudança enviaria, para um par de versões. Não lê chaves e não envia nada.
POST	`/api/ota/sync/campaigns/<id>/enqueue`	Calcular as diferenças e enfileirar os trabalhos.
POST	`/api/ota/sync/campaigns/<id>/control`	Pausar, retomar ou cancelar.
GET	`/api/ota/sync/jobs`	Lista de trabalhos.
GET	`/api/ota/sync/drift`	Deriva da frota por perfil.

Método	Rota	Propósito
POST	`/api/ota/sync/audit`	Ler um cartão de volta e compará-lo com sua versão esperada.

Controle de acesso

Páginas	Tipo de elemento RBAC
Perfis SIM, Produtos de Cartão, Lotes, Propriedade	`simbank`
Convergência	`ota`

Administradores sempre têm acesso. Caso contrário, uma permissão sobre o elemento concede visualização, e `POST` em seus métodos concede os controles de escrita. Veja Controle de Acesso Baseado em Funções.

Relacionados

- Gerenciamento de SIM OTA - como uma mudança chega a um cartão, via SMS e via HTTP, e quais plataformas são testadas.
- eSIM (SGP.22) - solicitando, entregando e gerenciando perfis de eSIM.
- Banco de SIM - o leitor e o inventário de cartões, e o armazenamento de chaves.
- Imagens de SIM - sistemas de arquivos salvos, dos quais uma versão de perfil pode ser criada.
- Ferramentas de Cartão SIM - ferramentas por cartão para um cartão em um leitor.

Banco de SIM: inventário distribuído de SIM

O **Banco de SIM** mostra cada SIM em cada leitor de smart card em todos os agentes OmniWeb. Cada agente escaneia seus leitores PC/SC locais, lê a identidade de cada SIM e reporta o inventário para o central exatamente como já reporta modems/telefones como dispositivos. O central agrega o inventário por agente e persiste um banco de dados de SIMs indexados por ICCID, para que a visão de "quais SIMs estão onde" sobreviva a desconexões de leitores e agentes.

Esta é a metade do inventário de um testbed remoto de SIM distribuído. A camada de emulação/banco de cartão remoto permite que você **conecte qualquer SIM a qualquer cardem pela rede**. Remote SIM documenta essa camada separadamente. Esta página cobre descoberta e inventário. Imagens de SIM (Pacotes de Perfil SAIP) cobre como salvar, exportar e reutilizar o sistema de arquivos de um cartão como um pacote de perfil portátil.

A página é **centrada no leitor**: uma linha por slot de leitor físico, agrupada por agente. Slots vazios, ilegíveis e em uso são todos exibidos. O layout do banco é a verdade, não apenas os slots preenchidos.

Como o agente lê um SIM

O scanner do agente espelha o scanner do modem: a enumeração é lenta, então os resultados são armazenados em cache e reescanados em um intervalo.

Para cada leitor PC/SC no host:

1. **Enumere** os leitores PC/SC conectados ao host.
2. **Prove** cada leitor com uma conexão *exclusiva*.
   - Sem cartão → `present=false`.
   - Conexão gera uma **violação de compartilhamento** → o leitor está sendo utilizado por outro processo (por exemplo, um `bankd` de SIM remoto ou uma sessão de emulação de cartão) → `present=true, in_use=true`, e **nenhuma leitura é tentada**. Um leitor ocupado nunca interrompe a varredura.
   - Cartão presente e livre → leia-o.
3. **Leia** a identidade do SIM com um conjunto autônomo de APDUs brutos:
   - Detecção de SIM UICC-vs-clássico (selecione `3F00`; `6E00` → GSM clássico, então use `CLA=A0` e modo de seleção clássico),
   - EF.ICCID (`2FE2`), EF.IMSI (`6F07`), EF.SPN (`6F46`),

- `EF.AD` (`6FAD`) para o comprimento do MNC (para que MCC/MNC sejam divididos corretamente),
- um PIN padrão **seguro** (`0000`) VERIFY em um cartão bloqueado. Ele primeiro verifica o contador de tentativas (um VERIFY vazio que não decrementa) e **recusa** se apenas uma tentativa restante, para que **nunca** queime a última tentativa ou toque no PUK (um banco de SIM não deve bloquear cartões),
- o ATR do cartão.

Cada leitor se torna um dicionário:

```
{
  "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…"
}
```

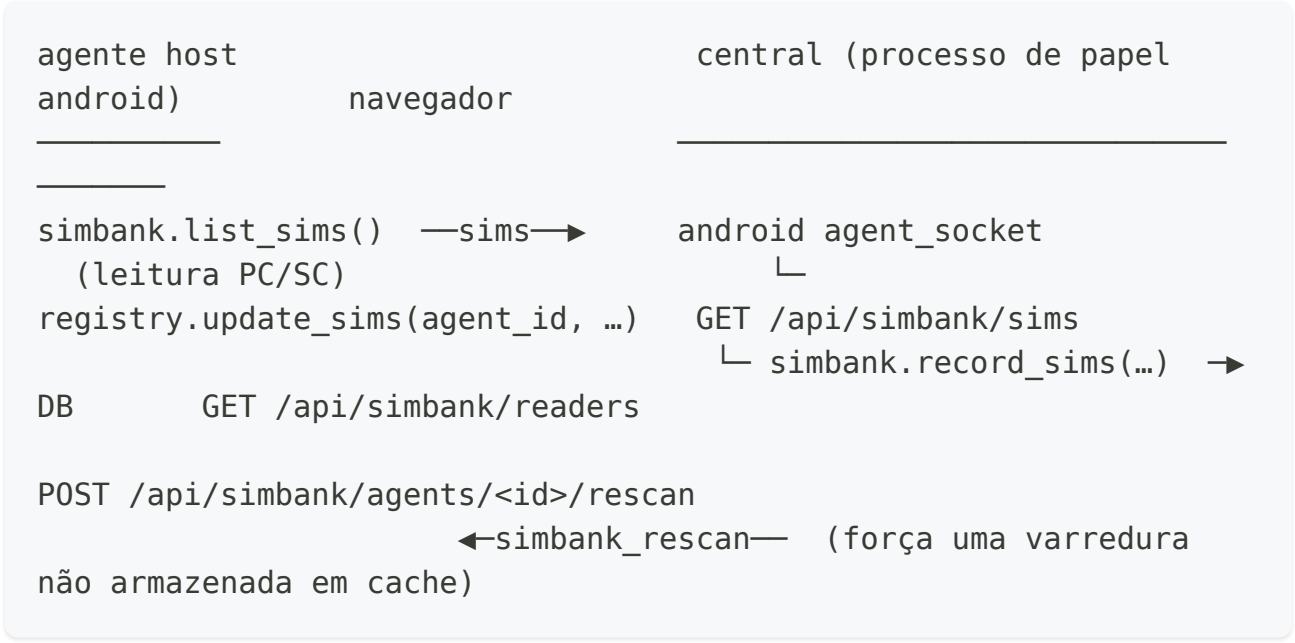
A lista é enviada para o central como uma mensagem `sims` (junto com a lista de dispositivos) no registro e sempre que muda; um comando `simbank_rescan` força uma varredura não armazenada em cache imediata.

Capacidade de leitura de cartão

Um host lê SIMs através de sua pilha de smart card PC/SC. Onde uma decodificação mais profunda do cartão é necessária, o agente usa uma biblioteca de smart card opcional, licenciada separadamente, mantida isolada do restante do agente (não é mesclada no próprio código do OmniWeb). Um host **sem** a pilha de smart card ainda executa o agente normalmente e simplesmente reporta que não há SIMs. O banco de SIM é uma capacidade opcional por host, como modems.

O leitor de referência é um SCM/Identiv SCR35xx. Vários leitores por host são suportados.

Inventário → central → fluxo de UI



- O agente se conecta **para fora** ao central através do mesmo WebSocket que usa para telefones (`/api/android/agent`). O inventário de SIM viaja por essa conexão. Não há novo transporte.
- O central mantém a **imagem ao vivo** do leitor por agente na `android.Registry` em memória (`update_sims` / `all_sims`), e espelha cada ICCID na tabela persistente `simbank_sims` via `simbank.record_sims`.
- Como isso depende do Registro de agente de processo único, a API do banco de SIM é servida **apenas pelo processo de backend de papel de agente** (mesma restrição que Dispositivos de Teste).

API REST (`/api/simbank`, JWT, tipo de elemento RBAC `simbank`)

Método	Rota	Propósito
GET	`/sims`	Cada SIM em todos os agentes (incl. offline persistido apenas), com presente/em uso ao vivo sobreposto.
GET	`/readers`	Cada leitor PC/SC em cada agente **conectado** (ao vivo), incl. leitores vazios e em uso.
GET	`/sims/<iccid>`	Um SIM.
PATCH	`/sims/<iccid>`	Editar campos atribuídos pelo operador (notas hoje). Cria a linha se o ICCID não for visto.
DELETE	`/sims/<iccid>`	Esquecer um SIM (remove o registro persistido; reaparece na próxima varredura se ainda estiver inserido).
POST	`/agents/<id>/rescan`	Forçar uma varredura PC/SC não armazenada em cache imediata em um agente e retornar seu inventário atualizado.

RBAC espelha `ir38`/`android-control`: administradores sempre passam; caso contrário, uma permissão JWT com `element_type == "simbank"` concede visualização, e `POST` em seus métodos concede controle.

Frontend

`src/pages/simbank/SimBank.tsx`: uma tabela pesquisável e filtrável de todos os SIMs: status (presente / em uso / offline), agente/site, leitor, ICCID, IMSI, MCC/MNC, país, SPN, notas editáveis, última vez visto. Botão

Reescaneamento por agente. Roteado em `/simbank` e vinculado na barra lateral sob **Testes de Roaming** › **Banco de SIM**.

Esquema do banco de dados

`simbank_sims`: uma linha por ICCID já visto:

Coluna	Notas
`iccid` (PK)	Serial do SIM.
`imsi`, `mcc`, `mnc`, `country`, `spn`, `atr`	Última identidade conhecida (substituída apenas por leituras não vazias).
`notes`	Atribuído pelo operador, editável.
`last_agent_id`, `last_site`, `last_reader_name`, `last_reader_index`	Onde foi visto pela última vez (ou está atualmente).
`first_seen`, `last_seen`	Carimbos de data/hora (UTC).
`remsim_bank_id`, `remsim_slot_nr`, `remsim_mapped_cardem`	**Reservado para a Fase 2** (nulo, não utilizado).

Leitores vazios e em uso não carregam **nenhum** ICCID, portanto, não são persistidos como SIMs. Eles aparecem apenas na imagem ao vivo `/readers`.

Futuro: SIM Remoto

A Fase 2 mapeia um leitor/SIM físico em um banco de SIM remoto para que um SIM em um site possa ser apresentado a um modem/telefone em outro (SIM

remoto). Os ganchos já estão no lugar. Pesquise o código por `# TODO remsim`:

- `simbank_sims.remsim_bank_id` / `remsim_slot_nr` / `remsim_mapped_cardem` (colunas nulas, exibidas em `to_dict` e no tipo TS `SimRow` como `null`),
- a flag `in_use` por leitor do agente já distingue um leitor mantido por uma sessão `bankd`/emulação. Esse é o leitor que a fase 2 mapeará,
- `PATCH /api/simbank/sims/<iccid>` é onde a edição do mapeamento remsim será conectada.

Nada aqui aciona remsim hoje; a forma é reservada para que o mapeamento se encaixe sem reestruturar o caminho quente do inventário.

Editor de Site: Visualizador de Configuração do Site

O **Editor de Site** mostra o arquivo de configuração bruto para o site atualmente selecionado: o arquivo YAML de host/inventário que define as funções de rede, infraestrutura e configurações daquela implantação. É uma visualização somente leitura, com destaque de sintaxe, para que você possa ver exatamente com o que o OmniWeb está trabalhando para um site, sem abrir um shell em um host.

← Guia de Operações

O que ele mostra

O OmniWeb controla cada site a partir de um arquivo de configuração por site. Esse arquivo lista os elementos do site (quais NFs estão presentes e em quais endereços), seus hosts de infraestrutura, seu papel de monitoramento, seu bloco `fivegc` (veja 5G Core), e assim por diante: tudo o que a barra lateral, a topologia, as páginas de elementos e os painéis derivam.

O Editor de Site carrega esse arquivo para o site escolhido no menu suspenso da barra superior e o exibe em um painel de editor completo (Monaco, o mesmo editor que o VS Code usa) com destaque para YAML, números de linha, dobradura e um minimapa. O cabeçalho mostra o cliente, o site e o nome do arquivo de origem.



Se nenhum site estiver selecionado, a página solicita que você escolha um primeiro no menu suspenso.

Somente leitura por design

O Editor de Site é um **visualizador**: o painel é somente leitura (marcado com um chip **somente leitura** no cabeçalho). Ele serve para *inspecionar* a configuração efetiva, não para alterá-la.

A configuração do site não é editada a partir do navegador. Como mencionado ao longo deste guia, a implantação e configuração do OmniWeb são gerenciadas via **Ansible**. Não edite arquivos de configuração diretamente nos hosts, e adicionar ou alterar um elemento é uma mudança de configuração feita através desse pipeline (veja o modelo de configuração). O Editor de Site permite que você leia o resultado desse pipeline para o site selecionado.

Quando usá-lo

- **Confirmar com o que um site está configurado**: quais elementos, hosts e NFs 5GC o OmniWeb acha que estão presentes e em quais endereços.
- **Resolver problemas da UI em relação à configuração**: se um elemento, uma entrada da barra lateral ou uma seção 5GC estiver faltando ou apontando para o host errado, o arquivo bruto é a fonte da verdade para verificar.
- **Referenciar o nome exato do arquivo e conteúdos** ao preparar uma alteração no Ansible.

Relacionado

- Arquitetura: o modelo de configuração: como a configuração do site controla o OmniWeb e como é gerenciada.
- 5G Core: o bloco `fivegc` da configuração do site e o que ele expõe.
- Topologia de Rede: as visualizações de topologia e Lista de Hosts construídas a partir da mesma configuração do site.

Gateway SMPP

O **Gateway SMPP** conecta pares SMPP externos ao núcleo de mensagens. Aplicações externas e parceiros de interconexão, os **ESMEs** (Entidades de Mensagem Curta Externas), se conectam via SMPP, seja como clientes que o gateway disca ou como servidores dos quais o gateway aceita conexões, e o gateway transporta suas mensagens curtas para e do SMSC. Cada conexão é um **bind** SMPP (transceptor, transmissor ou receptor). O gateway mantém esses binds ativos, autentica e controla-os, e encaminha o tráfego para o núcleo de mensagens. O OmniWeb exibe o status de bind ao vivo, os pares de cliente e servidor configurados, e os logs do gateway.

← Guia de Operações

O Gateway SMPP é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, com uma visão de frota onde vários estão implantados. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do gateway, portanto, permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda contextual) abre esta página. Ela está organizada em abas.

Visão Geral

Uma leitura de saúde em uma única tela das estatísticas agregadas de bind: o **total** de binds e a divisão **conectados / desconectados** dividida entre binds de **cliente** (saída) e **servidor** (entrada). É a maneira mais rápida de confirmar que o gateway está ativo e que seus pares estão conectados, e de identificar rapidamente se alguma conexão esperada caiu.

Status do Bind

Cada bind habilitado, cliente e servidor, com seu **status de conexão** atual, os **detalhes da sessão** subjacentes e as **métricas** por bind. Esta é a visão ao vivo de quem está conectado agora. A partir daqui, um operador pode agir sobre um bind:

- **Desconectar** um bind ativo. Para um bind de cliente, isso termina a conexão de saída. Para um bind de servidor, desconecta todas as conexões de cliente ativas. Use isso para limpar uma conexão travada ou com mau comportamento.
- **Reconectar** um bind de cliente. Isso força um bind de cliente (saída) a redialar seu host remoto, que é a maneira mais rápida de trazer um par de saída de volta após uma falha de rede.

Pares de Cliente

As conexões SMPP **cliente** de saída configuradas são os pares para os quais o gateway disca. Cada uma mostra seu **nome**, o **host** e **porta** remotos, o **ID do sistema** com o qual se conecta, e o **tipo de bind** (transceptor, transmissor ou receptor). Os pares de cliente são totalmente editáveis aqui: um operador pode **adicionar** um par, **editar** um existente (host, porta, credenciais, tipo de bind, intervalo de verificação de link, limite de TPS e outros parâmetros de bind), e **deletar** um que não é mais necessário. Habilitar um par coloca seu bind de saída em serviço. Desabilitá-lo retira o par sem descartar sua configuração.

Pares de Servidor

As autorizações SMPP **servidor** de entrada configuradas são as credenciais e regras para pares que se conectam *ao* gateway. Cada entrada define um **ID do sistema** e senha, os **tipos de bind permitidos**, e as regras que controlam um bind de entrada: uma **lista de permissões de IP** de endereços de origem permitidos e uma **lista de permissões de endereços de origem** de padrões de endereços de origem permitidos, além de um **limite de TPS**. Os pares de servidor são editáveis aqui da mesma forma (**adicionar**, **editar** e **deletar**), então um operador pode integrar um novo parceiro de entrada, restringir suas listas de permissões ou revogá-las. Habilitar e desabilitar uma autorização controla se esse parceiro pode se conectar.

Logs

A aba **Logs** exibe o log ao vivo do gateway para solucionar problemas de um único gateway (falhas de bind, rejeições de autenticação e conexões desconectadas) sem sair do OmniWeb.

Monitoramento

As taxas de mensagens, throughput e outras séries temporais para o Gateway SMPP são apresentadas como painéis Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **SMSC** é o núcleo de mensagens ao qual o gateway entrega mensagens curtas.
- O **IP-SM-GW** transporta SMS sobre IMS para dispositivos VoLTE e complementa o caminho SMPP para pares externos.

SMSC: Centro de Serviço de Mensagens Curtas

O **SMSC** (Centro de Serviço de Mensagens Curtas) é o coração de armazenamento e encaminhamento do SMS no núcleo. Ele **aceita** mensagens da rede (via SS7 (MAP) do lado móvel, via Diameter e via SMPP de front-ends de aplicação). Em seguida, ele **roteia**, **traduz** e **entrega** as mensagens. Ele mantém qualquer mensagem que não pode entregar imediatamente e tenta novamente até que a mensagem seja entregue, expire ou seja descartada. Ao longo do caminho, ele rastreia o estado de entrega de cada mensagem, traduz números chamadores e chamados, se federam com SMSCs pares para que uma mensagem possa ser entregue ao nó que conseguir alcançar o destinatário e impulsiona **campanhas** de SMS em massa. O OmniWeb apresenta tudo isso a partir de uma única página por instância: estado da mensagem ao vivo, localizações de assinantes, registros de front-end, saúde do Diameter e da federação, conjuntos de regras de roteamento e tradução e gerenciamento de campanhas.

← Guia de Operações

O SMSC é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, com uma visão de frota onde vários estão implantados. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do SMSC, assim permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Visão Geral

A aba de entrada é uma leitura de saúde de tela única para o nó: contagens atuais de mensagens e estado de entrega, saúde de front-end e pares à primeira vista, e uma **pesquisa por MSISDN** que busca tanto em mensagens armazenadas quanto em localizações de assinantes. É a maneira mais rápida de responder "o que está acontecendo com o SMS deste assinante agora" a partir de uma única caixa.

Mensagens

Cada mensagem que o SMSC está segurando ou processou, cada linha mostrando os números de envio e recebimento, o **estado** da mensagem (pendente, entregue, falhou, expirado, descartado ou respondido automaticamente), o número de **tentativas de entrega** e sua idade. Você pode filtrar mensagens por estado, por **SMSC**, e incluir tráfego **de carta morta** ou **não roteado**, e pesquisar por MSISDN, nome do nó ou ID da mensagem. Selecione uma mensagem para abrir seus detalhes, incluindo o texto decodificado. Um operador pode **rerotar** uma mensagem para forçá-la a passar novamente pelo roteamento, por exemplo, após corrigir uma regra de roteamento.

Frontends

Os **front-ends** de aplicação e SMPP atualmente registrados no SMSC são os clientes que enviam e recebem mensagens. Cada entrada mostra seu hostname, quando foi **visto pela última vez**, e quando seu registro **expira**, para que você possa confirmar que os front-ends de manipulação de mensagens estão conectados e seus registros estão ativos.

Localizações

As **localizações de assinantes** que o SMSC aprendeu são a última localização de serviço conhecida para cada assinante por **IMSI** e **MSISDN**. O SMSC usa essas informações para alcançar um destinatário. Você pode pesquisá-las por IMSI ou MSISDN e filtrá-las para incluir entradas expiradas. É onde você confirma que o SMSC sabe onde um assinante está antes que possa entregar a eles.

Diameter

As conexões de pares Diameter que o SMSC usa para mensagens, cada linha mostrando o **domínio** do par, **endereço IP**, **transporte**, direção de iniciação de conexão, **nome do produto** reportado, **IDs de aplicação** negociados e **estado de conexão**. É onde você confirma que o caminho Diameter do qual o SMSC depende está ativo.

Federação

A visão de **federação** mostra como este SMSC coopera com SMSCs pares para que uma mensagem possa ser entregue ao nó que conseguir alcançar o destinatário. Ela reporta **este nó**, a contagem de pares **saudáveis**, **degradados** e **insalubres**, o número de **mensagens federadas em cache** (destacado quando não é zero), o método de **descoberta** em uso (domínio DNS ou pares estáticos), e uma tabela por par com nome do nó, status, falhas recentes, última verificação de saúde bem-sucedida e os front-ends que cada par oferece. É a maneira mais rápida de ver se os SMSCs em uma federação se alcançam.

Roteamento

As **regras de roteamento de SMS** que decidem para onde cada mensagem vai, listadas por **prioridade**. Cada regra corresponde a um padrão de número **chamador** e **chamado** (e opcionalmente um SMSC de origem ou tipo de origem, como SS7 ou comutação de circuitos), e resolve para um **destino** (um SMSC de destino ou uma pesquisa **ENUM**) com uma descrição e um estado habilitado. As regras são totalmente editáveis: um operador pode adicionar, editar, habilitar, desabilitar ou excluir, e exportar e reimportar o conjunto de regras.

Traduções

As **regras de tradução de números** que reescrevem números chamadores e chamados à medida que as mensagens passam: elas normalizam formatos, aplicam prefixos e semelhantes. Cada regra é listada por **prioridade** com sua correspondência de chamador e chamado, SMSC de origem opcional, uma flag de **continuação** (para que várias regras possam se aplicar em sequência), uma descrição e um estado habilitado. Assim como no roteamento, as regras são editáveis (adicionar, editar, habilitar, desabilitar, excluir), e você pode exportá-las e reimportá-las.

Campanhas

As **campanhas** de SMS em massa são criadas e gerenciadas a partir desta aba. Uma **Nova Campanha** é definida com um nome e descrição, um número de **remetente**, o SMSC de origem, uma **lista de destinatários**, um **público** (apenas destinatários ativos ou todos na lista), uma taxa de **gotejamento** em mensagens por segundo, uma janela de **validade** da mensagem, um tempo **de entrega após** opcional e o **modelo de mensagem**. Uma vez criada, uma campanha é controlada a partir daqui (**iniciar**, **pausar**, **retomar** ou **cancelar**). Você pode inspecionar seus **alvos** para ver o estado de envio e entrega por destinatário à medida que a campanha avança.

Listas de Campanhas

As **listas** de destinatários para as quais as campanhas enviam. As listas são totalmente gerenciadas aqui: crie uma **Nova Lista de Destinatários** com um nome, descrição e um conjunto inicial de destinatários, **adicione** mais destinatários depois, edite ou exclua uma lista. Você fornece destinatários como **CSV**, para que possa importar uma lista de contatos existente diretamente em vez de digitá-la manualmente.

Teste NAPTR

A aba **Teste NAPTR** é uma ferramenta para operadores que resolve um **número E.164 (ou domínio) através de ENUM/NAPTR DNS** para ver como o SMSC irá roteá-lo. Insira o número de telefone e o **domínio ENUM** a ser consultado (`e164.arpa` por padrão) e envie. Nada é buscado até que você faça isso. O SMSC inverte os dígitos do número na zona ENUM, procura os registros **NAPTR** publicados lá e os retorna em **ordem** e **preferência**. Cada registro contém suas **flags**, **serviço**, a **regexp** de reescrita e **substituição**, e o **domínio de resultado** resolvido que o registro aponta para a mensagem. É onde você confirma que os dados ENUM por trás de uma regra de roteamento realmente resolvem um número para a URI ou rota que você espera, antes de confiar nisso em produção.

MWI

A aba **MWI** envia uma atualização de **Indicação de Mensagem à Espera** para um assinante: a notificação que define ou limpa a flag de "mensagens à espera" em um dispositivo, tipicamente após uma mensagem de voz ser deixada ou coletada. Forneça o **MSISDN de destino** a ser notificado e o **MSISDN de origem** de onde vem, escolha o **tipo de indicação** (mensagem de voz, fax, e-mail ou outro), e defina se o indicador deve estar **ativo** (ligado) ou limpo (desligado), com um **corpo de mensagem** opcional e o **SMSC** de origem. É um formulário de envio: a atualização só é enviada quando você a publica. Esta é a maneira direta de ativar ou limpar o indicador de mensagem à espera de um assinante manualmente.

Logs do Sistema

A aba **Logs do Sistema** é a própria visualização de log do SMSC com suporte à API. Você pode filtrá-la por **nível** (debug, info, warning, error) e por um **limite** no número de linhas retornadas, para que você possa puxar apenas os erros recentes ou um rastreamento mais completo ao investigar um problema específico, sem sair do OmniWeb.

Mais ferramentas

Ao lado das abas acima, a página do SMSC oferece algumas ferramentas focadas:

- **Enviar**: um formulário que envia um SMS único diretamente do OmniWeb (de, para e texto da mensagem), para testar a entrega a um destinatário específico.
- **Operações**: ações de manutenção em todo o nó, incluindo limpar os **front-ends** registrados, **mensagens** armazenadas, regras de **roteamento** e regras de **tradução**. Cada uma é uma ação destrutiva e pede confirmação primeiro.

Logs

A aba **Logs** acompanha a saída de log ao vivo do SMSC para solucionar problemas de um único nó sem sair do OmniWeb. Para uma visualização filtrada, com suporte à API do mesmo nó, use **Logs do Sistema** acima.

Monitoramento

Através deputação de mensagens, taxas de sucesso de entrega, profundidade de fila e outras séries temporais para o SMSC são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **HSS**: mantém os dados do assinante e informações de roteamento que as entregas do SMSC resolvem.
- O **DRA**: retransmite o sinalização Diameter que o SMSC usa para mensagens.
- **STP**: o caminho de sinalização SS7 pelo qual o SMSC troca mensagens MAP com a rede móvel.
- O **CSCF/TAS**: o lado IMS que origina e termina mensagens para assinantes VoLTE.

Gerenciamento e Ciclo de Vida de Software

OmniWeb fornece um único lugar para ver e gerenciar o software em execução em toda a frota: versões de pacotes, atualizações disponíveis e licenciamento. O ciclo de vida do software da rede é visível a partir do mesmo portal usado para operá-lo.

← Voltar ao Guia de Operações

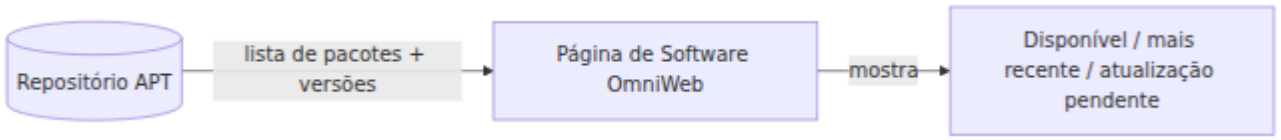
Página de Software (Repositório APT)

A página de **Software** é um navegador de repositório APT para pacotes Omnitouch. Ela se conecta ao servidor de repositório APT configurado e mostra, para os pacotes que gerencia:

- **Pacotes disponíveis** no repositório.
- **Versões** oferecidas, incluindo a mais recente disponível.
- **Status de atualização**: se existe uma versão mais nova do que a que está implantada.

Isso permite que os operadores vejam rapidamente quais componentes Omnitouch têm atualizações pendentes e quais versões estão atuais, fornecendo o lado de inventário do ciclo de vida do software. A instalação/atualização de pacotes em hosts `` realizada através das ferramentas padrão APT/`dpkg` (e é tipicamente automatizada via Ansible); o OmniWeb fornece a camada de visibilidade sobre o que está publicado e atual.

Página de Software: cada pacote Omnitouch com suas últimas versões de repositório e cache e um indicador de sincronização que sinaliza onde uma versão mais nova foi publicada do que a que está em cache/implantada (aqui `omni-upf` e `omni-msc` estão fora de sincronia).



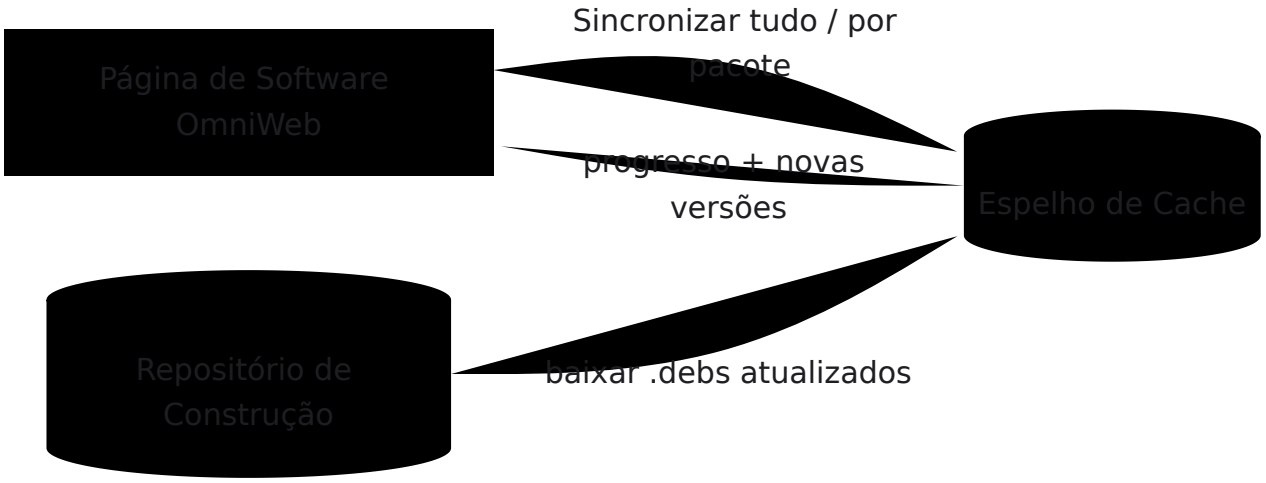
Sincronizando Pacotes para o Cache

Implantações que executam um **espelho de cache APT** local (para sites isolados ou com largura de banda limitada) mantêm uma cópia local dos pacotes publicados no repositório de construção. Com o tempo, o cache fica desatualizado. A página de Software sinaliza cada pacote que está **fora de sincronia** (uma versão mais nova foi publicada do que a que está em cache). A partir da mesma página, você pode puxar essas atualizações para o cache sem sair do OmniWeb:

- **Sincronizar tudo**: puxar todos os pacotes atualizados do repositório para o cache.
- **Sincronizar** (por linha): puxar apenas um pacote. Clique em vários e eles **ficam na fila**: eles são baixados um após o outro, e o OmniWeb regenera o índice de pacotes **uma vez** no final (não por pacote), para que o cache nunca fique meio atualizado.

Enquanto uma sincronização está em andamento, a página mostra o progresso ao vivo (qual pacote está sendo baixado, quantos estão na fila e um log de progresso em tempo real). Ela atualiza a comparação de versões quando termina.

Uma sincronização em andamento: `omni-msc` baixando com `omni-upf` na fila, o banner de fase e o log ao vivo. Quando a fila esvazia, o índice do cache é regenerado uma vez e o status de sincronização é atualizado.



A sincronização é executada no próprio espelho de cache (o OmniWeb a aciona e transmite o progresso); o espelho puxa os `.deb`s atualizados do repositório de construção e regenera seu índice. Os hosts no local então instalam os pacotes atualizados do cache como de costume.

Versionamento

O OmniWeb relata sua própria versão de construção (versão, commit e data de construção) para que os operadores possam confirmar exatamente qual versão do portal estão executando. Este é o ponto de referência ao relatar problemas ou coordenar uma atualização do próprio portal.

Gerenciamento de Licenças

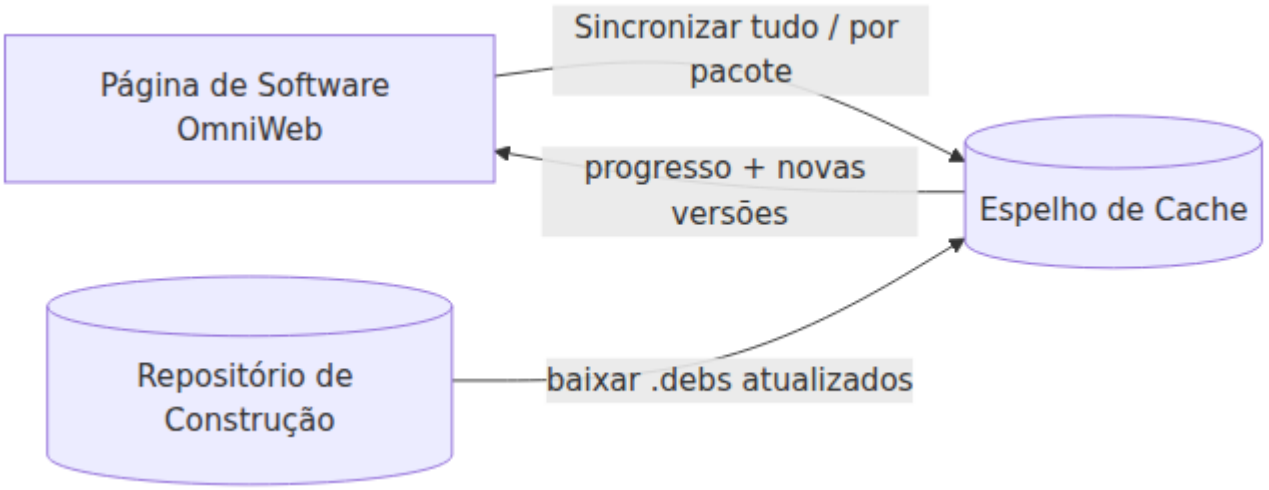
O **Servidor de Licenças** é administrado através do OmniWeb como qualquer outro elemento, usando os mesmos padrões genéricos (veja Operações Comuns). Ele exibe:

Visão geral do Servidor de Licenças: status atual da licença e validade, incluindo estado de tempo confiável.

Visualizar	Descrição
Visão Geral	Status atual da licença, datas de validade e direitos de recursos.
Registros de Solicitação	Solicitações de licença históricas, com filtragem. Isso é útil para auditar o que foi verificado e quando.
Consulta	Verificar o status da licença para um licenciado/produto específico sob demanda.

O licenciamento está ligado ao ciclo de vida do software: os direitos determinam quais produtos e recursos uma implantação está autorizada a executar, e os registros de solicitação fornecem um histórico de atividade de licença ao longo do tempo.

Ciclo de Vida em Resumo



1. **Ver o que está disponível**: a página de Software mostra atualizações pendentes.
2. **Confirmar direitos**: o Servidor de Licenças mostra para o que a implantação está licenciada.
3. **Aplicar**: atualizações são executadas via APT/Ansible nos hosts.
4. **Verificar**: confirmar versões, depois acompanhar Logs e Painéis de Elementos para confirmar um resultado saudável.

SS7: Pilha de Sinalização (STP / HLR / IP-SM-GW / CAMEL-GW)

A **pilha SS7** (OmniSS7) termina o transporte SIGTRAN (associações SCTP que transportam **M3UA**) e roteia o tráfego SS7/MAP pela rede de sinalização. Um único serviço fornece toda a pilha, e o OmniWeb a apresenta como quatro visões de elementos para seus diferentes papéis: **STP** (Ponto de Transferência de Sinalização, o roteador SS7), **HLR** (Registro de Localização do Usuário), **IP-SM-GW** (Gateway de Mensagens Curtas IP) e **CAMEL-GW** (Gateway CAMEL). Todos os quatro são suportados pelo mesmo cliente compartilhado, então o transporte e roteamento SIGTRAN que eles compartilham é a mesma pilha subjacente vista de diferentes ângulos.

← Guia de Operações

Cada visão é uma página de elemento por instância acessada a partir da barra lateral quando uma pilha SS7 está em execução no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API da pilha, então permanece atrás do único gateway autenticado. As respostas retornam em um envelope `{status, response}`. O link de documentação no cabeçalho de cada página de elemento (o botão de ajuda em contexto) abre esta página. Cada visão é organizada em abas. As taxas de mensagens e outras séries temporais são apresentadas como painéis Grafana acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

A pilha em um relance

O transporte SIGTRAN sob cada papel é o mesmo, então as abas **Peers** e **SCTP Connections** aparecem em todas as quatro visões e leem os mesmos dados.

A aba **Peers** relata o status do peer M3UA (`/api/m3ua-status`): cada peer M3UA/M2PA, com seu **estado ASP**, **estado de associação**, **endpoints** locais e remotos, **contexto de roteamento**, protocolo e modo, e estatísticas de **tempo de atividade** por peer. É aqui que você confirma que o processo de servidor de aplicação de cada vizinho de sinalização está ativo e em serviço.

A aba **SCTP Connections** lista o transporte subjacente (`/api/sctp-connections`): cada associação SCTP com seu **status**, **papel**, **IP/porta** locais e remotos, contagens de **streams** de entrada e saída, **bytes** e **mensagens** enviadas e recebidas, **última atividade**, e qualquer último erro, além de totais agregados em todas as conexões. Quando um peer mostra estar fora do ar, verifique esta camada para ver se a associação SCTP em si está estabelecida.

STP: roteamento

A visão **STP** é o roteador SS7. Junto com as abas de transporte compartilhadas, ela contém a aba **Routing**, além de **Mapa de Rede**, **Visão Geral** e um feed de **Eventos SS7**.

A aba **Routing** mostra a configuração completa de roteamento M3UA (`/api/routing`): os **peers** configurados, as **rotas de código de ponto (PC)** e as **rotas de título global (GT)**.

- **Rotas de código de ponto** direcionam o tráfego para um código de ponto de destino (`dest_pc`) via um **peer** alvo, com um **indicador de rede**, **máscara** de código de ponto e **prioridade**. Os operadores podem **adicionar** uma rota PC (`POST /api/routing/pc-routes`, fornecendo o código de ponto de destino e o peer alvo) e **deletar** uma (`DELETE /api/routing/pc-routes/{dest_pc}-{peer_id}`).
- **Rotas de título global** combinam um **prefixo** GT e encaminham para um **peer** alvo com uma **prioridade** e detalhes opcionais de SSN, tipo de tradução e natureza do endereço, além de uma descrição. Os operadores podem **adicionar** uma rota GT (`POST /api/routing/gt-routes`, fornecendo o prefixo e o peer alvo) e **deletar** uma (`DELETE /api/routing/gt-routes/{prefix}:{peer_id}`).

É aqui que você confirma e ajusta como o STP encaminha mensagens SS7 para cada destino.

HLR

A visão **HLR** exibe os assinantes ativos do registro e o link para o backend do HLR, juntamente com as abas de transporte compartilhadas, uma **Visão Geral** e uma aba **Cliente SS7**.

A aba **Subscribers** lista o registro de assinantes ativos (`/api/subscribers`): cada assinante que enviou uma **UpdateLocation** e ainda não uma **CancelLocation**, cada linha mostrando **IMSI**, **VLR**, **MSC** de serviço, hora de registro e **duração**, com contagens de VLRs e MSCs únicos. Um operador pode **limpar** todos os assinantes ativos rastreados (`DELETE /api/subscribers`) para redefinir a visão do registro.

A aba **HLR Links** verifica a conectividade com a API HLR configurada (`/api/hlr-links`): o **status** (ativo, degradado ou fora do ar), **latência** medida, **versão** reportada e o **host** alvo. É a maneira mais rápida de confirmar que a pilha pode alcançar o backend do HLR.

IP-SM-GW

A visão **IP-SM-GW** é o gateway de mensagens curtas. Ela contém o rastreador de assinantes SMSc e o link para o backend do SMSc, juntamente com as abas de transporte compartilhadas e uma **Visão Geral**.

A aba **SMSc Links** verifica a conectividade com a API SMSc configurada (`/api/smsc-links`): **status** (ativo, degradado ou fora do ar), **latência**, **versão** reportada e **host** alvo. É o equivalente ao caminho SMS da verificação de link do HLR.

A aba **SMSc Subscribers** lista os assinantes rastreados pelo rastreador de assinantes SMSc (`/api/smsc-subscribers`): cada um com **MSISDN**, **IMSI**, **HLR GT** e **VLR GT**, **mensagens enviadas** e **recebidas**, status e última atualização, além de contagens de ativos/falhados e HLRs únicos. Um operador pode **limpar** todos os assinantes SMSc rastreados (`DELETE /api/smsc-subscribers`).

CAMEL-GW

A visão **CAMEL-GW** exibe as sessões CAMEL que o gateway está executando, juntamente com as abas de transporte compartilhadas e uma **Visão Geral**.

A aba **CAMEL Sessions** lista todas as sessões CAMEL ativas gerenciadas pelo gateway (`/api/camel-sessions`): o **estado** de cada sessão, **versão CAP**, **chave de serviço**, **IMSI**, números **chamadores** e **chamados**, hora de início e **duração**, com contagens de sessões iniciadas e atendidas. É onde você acompanha o manuseio de chamadas CAMEL ao vivo em tempo real.

Status

O endpoint **Status** (`/api/status`) relata a saúde geral do nó que as abas **Visão Geral** resumem: a identidade do nó e **papel**, se o serviço está **ok**, seu **tempo de atividade**, e um resumo de peers de quantos peers de sinalização estão ativos em relação ao total. Esta é a primeira leitura para confirmar que a pilha está em execução e seus peers estão em serviço.

Relacionados

- **STP**: o elemento de roteamento SS7 (rotas de código de ponto e rotas de título global).
- **HLR**: o elemento Registro de Localização do Usuário (registro de assinantes ativos e link HLR).
- **IP-SM-GW**: o elemento Gateway de Mensagens Curtas IP (assinantes SMSc e link).
- **CAMEL-GW**: o elemento Gateway CAMEL (sessões CAMEL ao vivo).
- O **MSC/VLR** gera a UpdateLocation e sinalização CAMEL que esta pilha roteia e rastreia.
- O **SMSc** é o backend que o link SMSc do IP-SM-GW e o rastreador de assinantes resolvem.
- ← Guia de Operações

Cliente SIM Toolkit (STK)

OmniWeb inclui um cliente interativo **SIM Toolkit**. Use-o para navegar e operar applets STK em qualquer cartão SIM físico inserido em um leitor PC/SC conectado ao computador do agente. O cliente STK envia um perfil de terminal para o cartão, e então apresenta cada comando proativo como uma tela interativa. Você responde como um terminal faria, permitindo que o applet avance para seu próximo passo.

Esta ferramenta está na barra lateral sob **SIMs - SIM Toolkit**, ao lado do Terminal APDU e Explorador de Sistema de Arquivos SIM.

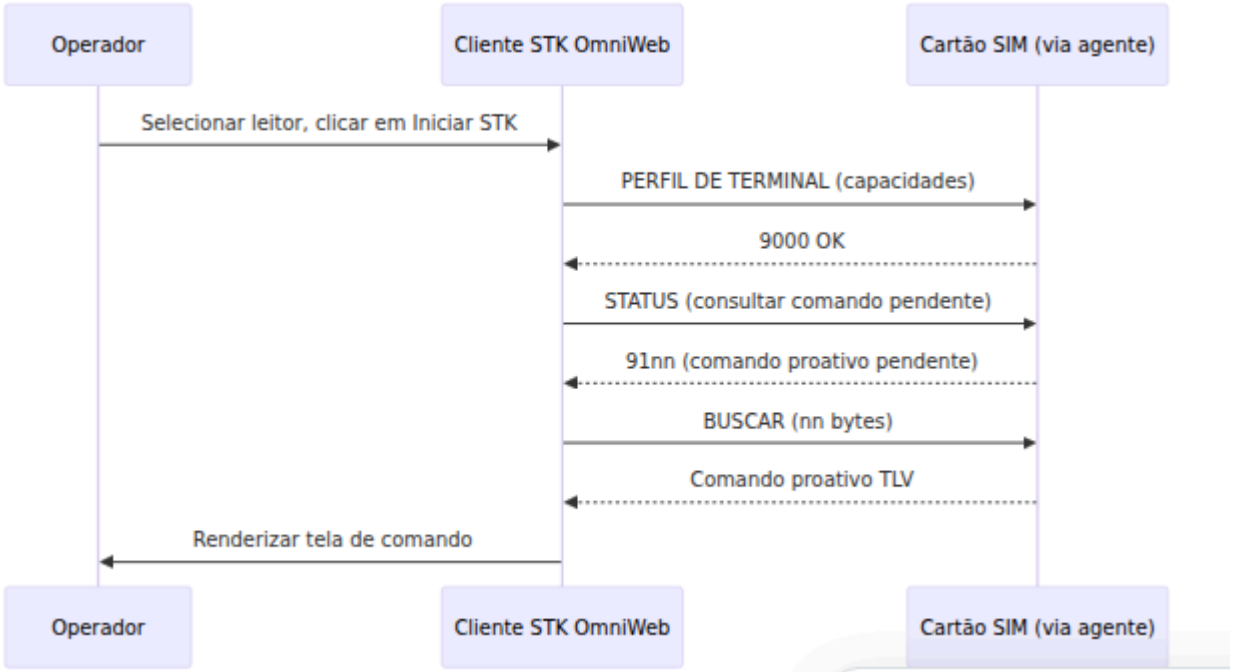
O que é SIM Toolkit?

O SIM Application Toolkit (STK) é um padrão definido na ETSI TS 102.223 que permite que um cartão SIM inicie ações no terminal. Um applet SIM emite **comandos proativos** - solicitações como "exibir este texto" ou "mostrar este menu" - e o terminal responde com a seleção ou entrada do usuário. Casos de uso comuns incluem menus de recarga de operador, consulta de saldo, gatilhos de configuração OTA e portais de serviço residentes no SIM.

Requisitos

- Um leitor com um cartão SIM que contém um applet STK.
- A permissão de **controle de banco SIM**. Sem ela, você pode ver leitores, mas não pode abrir sessões ou operar cartões.
- O leitor não deve estar sendo utilizado por outra ferramenta. Se estiver, o OmniWeb mostra quem o está utilizando e oferece uma opção de **Tomar controle**. Tomar controle cancela a outra sessão.

Abrindo uma Sessão



1. Selecione o leitor no menu suspenso **Leitor**. Apenas leitores com um cartão presente aparecem.
2. Clique em **Iniciar STK**. O OmniWeb abre uma sessão exclusiva no cartão, envia um perfil de terminal e consulta o primeiro comando proativo.
3. Interaja com cada tela à medida que ela aparece. O OmniWeb envia uma RESPOSTA DE TERMINAL após cada etapa e busca automaticamente o próximo comando.
4. A sessão termina quando o cartão emite um comando de FIM DE SESSÃO, ou quando você clica em **Encerrar sessão**.

Telas de Comando

O OmniWeb renderiza cada comando proativo como uma tela interativa. A tabela abaixo lista os tipos de comando suportados.

Comando	Descrição	Ação do usuário
EXIBIR TEXTO	O cartão mostra uma mensagem.	Clique em **OK** para reconhecer, ou **Voltar** para ir ao passo anterior.
SELECIONAR ITEM / CONFIGURAR MENU	O cartão apresenta uma lista numerada de opções.	Clique no item que deseja selecionar.
OBTER TECLA	O cartão pede um único pressionamento de tecla.	Digite um caractere e clique em **Enviar**, ou escolha **Sim** / **Não** para prompts de sim-não.
OBTER ENTRADA	O cartão pede uma string de texto de um comprimento especificado.	Digite o texto e clique em **Enviar**. O campo mostra a contagem mínima e máxima de caracteres.

Se o cartão emitir um tipo de comando que o cliente não renderiza interativamente (por exemplo, ENVIAR MENSAGEM CURTA ou CONFIGURAR CHAMADA), o OmniWeb mostra os dados brutos do comando e envia uma resposta **OK** automaticamente para que a sessão possa continuar.

Histórico da Sessão

Um painel de **Histórico da Sessão** aparece no lado direito da tela assim que você começa a interagir. Ele registra cada tipo de comando e a resposta que você deu (item selecionado, texto de entrada ou OK/Voltar). Use-o para refazer o caminho através de uma árvore de menu.

Encerrando uma Sessão

A sessão termina de uma das três maneiras:

- **Fim iniciado pelo cartão**: o applet emite um comando proativo de FIM DE SESSÃO. O OmniWeb fecha a sessão automaticamente e mostra uma mensagem de conclusão.
- **Fim iniciado pelo operador**: clique em **Encerrar sessão** a qualquer momento. O OmniWeb envia um resultado de sessão encerrada para o cartão e fecha a sessão do leitor.
- **Navegação para trás além da raiz**: clicar em **Voltar** na primeira tela envia um resultado de movimento para trás para o cartão. O cartão decide como responder - pode mostrar uma tela anterior ou encerrar a sessão.

Após o término da sessão, o leitor fica disponível novamente para outras ferramentas.

Relação com Outras Ferramentas SIM

Ferramenta	Propósito
SIM Toolkit (esta página)	Operar applets STK interativamente.
Terminal APDU	Enviar APDUs brutos manualmente, um de cada vez ou em uma sessão persistente.
Explorador de Sistema de Arquivos SIM	Navegar e editar o sistema de arquivos do cartão.
Log APDU	Rastrear passivamente comandos entre um modem e um SIM remoto.

Solução de Problemas

Falha ao Iniciar STK com "PERFIL DE TERMINAL falhou"

O cartão rejeitou o perfil de terminal ou o agente não conseguiu acessar o cartão. Verifique se:

- O cartão está corretamente encaixado no leitor.
- Nenhuma outra ferramenta está utilizando o leitor. Se estiver, use **Tomar controle**.
- O agente que possui o leitor está online (verifique a página do Banco SIM).

A sessão para após o primeiro comando

Alguns applets SIM encerram a sessão imediatamente se o perfil de terminal não declarar as capacidades que o applet precisa. O cliente declara um conjunto amplo de capacidades, mas alguns cartões verificam bits específicos. Se isso acontecer, use o Terminal APDU em modo de sessão para enviar PERFIL DE TERMINAL e BUSCAR manualmente e examinar os dados brutos do comando proativo.

Voltar retorna uma tela inesperada

A ação **Voltar** envia o código de resultado 0x11 (movimento para trás) para o cartão. O cartão controla o que isso significa. Alguns applets retornam ao menu anterior; outros reiniciam a sessão a partir do menu raiz; alguns ignoram o movimento para trás e reemitem o mesmo comando.

OBTENÇÃO DE ENTRADA rejeita meu texto

O cartão define uma contagem mínima e máxima de caracteres. O campo de entrada mostra ambos. Se o cartão também restringir apenas a dígitos, o rótulo do campo diz **apenas dígitos**. Insira um valor dentro do intervalo exigido.

TAS: Servidor de Aplicação de Telefonia

O **TAS** (Servidor de Aplicação de Telefonia) é o servidor de aplicação IMS que fornece a experiência de telefonia do assinante. Ele gerencia o **controle de chamadas** e **serviços suplementares** (encaminhamento de chamadas, bloqueio, espera, retenção e outros), realiza **conferências**, grava e reproduz **mensagens de voz**, registra **CDRs** para cada chamada, resolve **roteamento** e tradução de números, e se comunica com o **OCS** via Diameter para que as chamadas sejam cobradas em tempo real. Onde o CSCF decide *como* uma chamada é sinalizada, o TAS decide *o que* o serviço faz. O OmniWeb exibe suas chamadas ao vivo, registros de assinantes, gateways, pares Diameter e configuração em uma única página de elemento. Gráficos de volume de chamadas e tendências estão disponíveis nos painéis do Grafana acessados a partir da mesma página.

← Guia de Operações

O TAS é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API do TAS, portanto, permanece atrás do único gateway autenticado. O link da documentação no cabeçalho da página (o botão de ajuda contextual) abre esta página. Ela está organizada em abas.

Visão Geral

A aba de entrada é uma leitura de saúde de tela única para o servidor de aplicação: o número de **chamadas ativas**, **assinantes registrados**, conferências **em execução** e registros de **mensagens de voz** armazenados, a saúde dos pares **Diameter** e **gateways SIP**, e o status da **licença**. É a maneira mais rápida de confirmar que o TAS está ativo e processando tráfego.

Chamadas Ativas

Cada chamada atualmente em andamento, cada linha mostrando as partes chamadora e chamada, a **direção**, o **estado** da chamada e sua **duração**. Selecione uma chamada para abrir seus detalhes para que você possa ver como uma chamada específica está estruturada e onde ela se encontra no plano de discagem. É o primeiro lugar a ser verificado quando um assinante relata uma chamada com problemas no momento.

CDR

Os **registros de detalhes de chamadas** que o TAS registrou: uma linha por chamada concluída, com as partes, **hora de início**, **duração** e **disposição**. Abra qualquer registro para ver seus detalhes completos. Os CDRs são a trilha de contabilidade e solução de problemas após o fato: use-os para confirmar que uma chamada ocorreu, quanto tempo durou e como terminou.

Assinantes

Os **registros de assinantes** que o TAS conhece, cada um com a **identidade** do assinante, **estado** de registro e **contato** atual. Abra um assinante para ver os detalhes completos do registro. Este é o lugar onde você confirma que um assinante está registrado no servidor de aplicação antes de investigar por que um serviço não está funcionando para ele.

Diameter

Os **pares Diameter** aos quais o TAS se conecta, incluindo o caminho para o **OCS** para cobrança e o **HSS** para dados do usuário, com o nome do host de cada par e o **estado de conexão**. Abra um par para ver seus detalhes. Quando a cobrança ou as buscas de assinantes falham, esta aba é onde você confirma que os caminhos Diameter subjacentes estão ativos.

Gateways

Os **gateways SIP** que o TAS usa para alcançar outras redes e troncos, cada um mostrando seu nome e **status** atual. Abra um gateway para ver seus detalhes. Use esta aba para confirmar que os gateways de interconexão estão registrados e disponíveis antes de diagnosticar chamadas off-net com falha.

Conferências

As **conferências** ativas e seus participantes. Abra uma conferência para ver quem está nela e agir sobre ela no local: **trancar** ou **destrancar** a ponte, **expulsar** um participante, ativar ou desativar **vídeo**, ou **destruir** a conferência completamente. Este é o controle ao vivo do operador sobre uma ponte em funcionamento.

Mensagens de Voz

Os registros de **mensagens de voz** armazenadas, por assinante. Cada registro pode ser **excluído** individualmente, por exemplo, para limpar uma mensagem deixada por engano ou para liberar uma caixa de correio cheia.

Teste OCS

As **sessões OCS (Sistema de Cobrança Online)** ativas que o TAS está mantendo, para que você possa ver quais chamadas estão utilizando um saldo em tempo real. Uma sessão de cobrança individual pode ser **encerrada** a partir daqui. Isso é útil para limpar uma sessão que ficou aberta após sua chamada ter terminado.

Roteamento

Os **modelos de plano de discagem** que o TAS usa para roteamento de chamadas. A lista mostra cada modelo; abra um para ler seu conteúdo. Esta é a referência de como os números são correspondidos e para onde as chamadas são enviadas. Leia-a ao lado da ferramenta de **Tradução de Números** para confirmar que um número específico é roteado como pretendido.

Configuração

A **configuração da aplicação** que o TAS está executando, agrupada por aplicação. Abra uma entrada para ler suas configurações. Esta é a referência de leitura para confirmar que o servidor está configurado como esperado sem sair do OmniWeb.

Prompts

As **gravações de prompts de texto para fala** que o TAS reproduz para os chamadores, os anúncios e prompts de menu, com o status de cada um. Use esta aba para confirmar que os prompts esperados estão presentes e renderizados.

Ferramentas

Além das abas acima, a página do TAS possui um conjunto de ferramentas sob demanda para validar o roteamento e os dados do assinante. Cada uma delas utiliza um pequeno formulário, executa a solicitação contra o servidor de aplicação através do proxy do OmniWeb e mostra o resultado no local.

Simulador de Chamadas

Realiza uma chamada de teste através do TAS para validar o roteamento e a mídia. Insira um **destino** (e opcionalmente um número de origem, IP de origem e uma disposição forçada). O simulador percorre a chamada pelo plano de discagem **sem tocar ninguém**. Ele retorna o **tipo de chamada** resolvido (MT, MO ou emergência), a decisão de on-net/off-net, cada **variável do plano de discagem** que definiu, e uma lista passo a passo de **notas de processamento**, para que você possa ver exatamente como um número seria tratado antes de uma chamada real ser feita. A autorização do OCS e a busca HLR podem ser puladas para isolar uma etapa. Uma ação separada de **chamada de teste de eco** toca um destino e retorna o áudio da própria parte, o que confirma o caminho de voz ao vivo para um aparelho.

Consulta Sh

Consulta o HSS através da interface **Sh** para os dados do usuário de um assinante. Insira a **identidade pública** do assinante e escolha a **referência de dados** a ser buscada, desde os **dados do repositório** completos até um elemento específico, como o estado do usuário IMS, o nome do S-CSCF que está servindo, os critérios de filtro inicial, o MSISDN ou o IMSI. A ferramenta retorna os dados de serviço transparentes e do repositório que o HSS possui. Use-a para confirmar o que o servidor de aplicação vê para um assinante quando um serviço não está se comportando como esperado.

Busca HLR

Realiza uma **busca HLR** via SS7 MAP (uma solicitação de Enviar Informações de Roteamento) para resolver o estado de roteamento e roaming de um assinante. Insira o **MSISDN** no formato internacional e a ferramenta retorna a resposta HLR juntamente com as **variáveis do plano de discagem** que o resultado definiria em uma chamada. Esta é a maneira de confirmar a localização atual da rede de um número antes de diagnosticar por que chamadas para ele são roteadas da maneira que são.

Tradução de Números

Testa como um número discado é **normalizado e traduzido** pelas regras de roteamento do TAS. Insira um **código de país**, o **número de telefone** e uma **disposição** opcional. A ferramenta retorna o número traduzido que o plano de discagem usaria. Leia-a ao lado da aba de **Roteamento** para confirmar que um número espec��fico é correspondido e reescrito como pretendido.

ESL

Um **console** interativo para emitir comandos no estilo do Servidor de Mídia para o mecanismo TAS para diagnósticos. Digite um comando e pressione Enter. A saída é impressa de volta no console, e as setas para cima/baixo recuperam comandos anteriores. Comandos de exemplo como `status`, `sofia status`, `show channels` e `show registrations` são oferecidos como chips de um clique. É a visão de nível mais baixo do mecanismo em execução, para confirmar canais ao vivo, estado do gateway e registros diretamente.

Logs

A aba **Logs** acompanha a saída de log ao vivo do TAS para solucionar problemas de um único servidor de aplicação sem sair do OmniWeb.

Painéis de Monitoramento

Volumes de chamadas, contadores por serviço e outras séries temporais para o TAS são apresentados como painéis do Grafana, acessados a partir da página

do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- O **CSCF** sinaliza as chamadas às quais o TAS aplica serviços. Os dois juntos fornecem voz IMS.
- O **HSS** mantém os dados do assinante e do usuário Sh que o TAS resolve.
- O **OCS** classifica e cobra as chamadas do TAS em tempo real via Diameter.
- O **DRA** retransmite a sinalização Diameter do TAS (Sh, Gy) para esses pares.

Dispositivos de Teste

Dispositivos de Teste transforma dispositivos Android reais em locais remotos em uma fazenda de testes controlável remotamente. A partir do OmniWeb, você pode assistir à tela de um telefone ao vivo, controlá-lo (tocar, deslizar, digitar, teclas de hardware), fazer chamadas e enviar mensagens de texto, e executar verificações de saúde programadas. Essas verificações cobrem registro VoLTE, sinal e conectividade. O OmniWeb exporta seus resultados de aprovação/reprovação para o Prometheus para alertas e painéis.

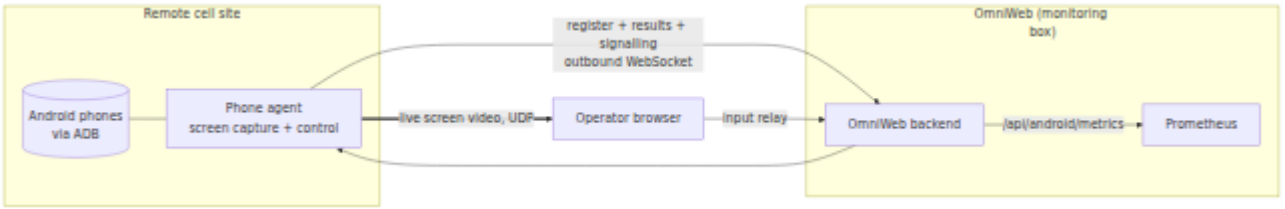
← Voltar ao Guia de Operações

Ele existe para responder à pergunta que um NOC continua fazendo sobre um site celular remoto: *"um telefone real está realmente funcionando nesta rede agora?"* O telefone deve estar registrado para VoLTE e ser capaz de fazer chamadas, enviar mensagens e acessar a internet. Ninguém precisa ir até o local.

Arquitetura

Cada host com telefones conectados via ADB executa um **agente** leve. O agente disca *para fora* para o OmniWeb central, então sites atrás de NAT não precisam de acesso de entrada. O vídeo ao vivo usa **WebRTC** (UDP), então ele sobrevive a links com perda e alta latência muito melhor do que o compartilhamento de tela TCP. O central retransmite a entrada e os resultados do teste.

> **Caminhos de rede importam.** A interface da web, a entrada e a configuração de chamadas ("sinalização") utilizam o plano de controle via HTTPS para o servidor OmniWeb. No entanto, o vídeo da tela ao vivo **flui diretamente entre o navegador do operador e o host do agente via UDP**. Ele não passa pelo servidor. Se um navegador pode alcançar o servidor, mas não o host do agente via UDP, o console fica travado em "Conectando...". Veja **Requisitos de Rede** para a regra de firewall a solicitar e como reconhecer o problema.



Componente	Função
Agente do telefone	Descobre dispositivos ADB, captura a tela, injeta entrada, executa scripts de teste do host. Um por site; instalado pelo papel Ansible `device_tester`.
OmniWeb Central	Registro de dispositivos, retransmissão de sinalização WebRTC, despacho de scripts, histórico de resultados, métricas do Prometheus.
Prometheus	Coleta resultados de testes programados de `/api/android/metrics`.

Tipos de dispositivos

A fazenda não é mais apenas de telefones. Cada dispositivo conectado é um dos três tipos, detectados automaticamente pelo agente e exibidos com seu próprio distintivo (e o logotipo do robô Android para telefones) na frota:

Tipo	O que é	Console
Telefone Android	Um dispositivo normal (Android 5.0+ / API 21+) via ADB	Tela ao vivo + controle total
Modem USB	Um módulo celular que expõe portas AT (por exemplo, Quectel EP06)	Console celular controlado por AT: status, chamadas, SMS, bloqueio de célula, VoLTE
Dongle Android Antigo	Um dongle LTE barato rodando Android antigo (API < 21, por exemplo, UZ801) muito velho para a visualização de tela ao vivo	Visualização de **screencap** baseada em polling + controle
Simulador RAN UE	Um UE virtual do Simulador RAN, sem hardware	Painel de controle UE: anexar/desanexar, ocioso, fora de cobertura, registro IMS, SMS, chamadas

Clicando em um dispositivo abre o console apropriado para seu tipo. Dentro de qualquer console, o botão **Trocar telefone** (canto superior direito) muda para outro dispositivo sem voltar para a grade da frota.

UEs simulados do Simulador RAN aparecem na frota marcados como simuladores, para que você possa controlar assinantes emulados ao lado de dispositivos reais. O filtro de Dispositivos de Teste permite que você se concentre apenas nos UEs do Simulador RAN. Eles usam o **mesmo painel de controle UE** mostrado no próprio Mapa de Rede do Simulador RAN, então há um lugar para anexar, ocioso, sair de cobertura, registrar no IMS e enviar SMS/chamadas. Veja Simulador RAN para o ciclo de vida completo do UE.

Adicionando um dispositivo a um site

Um dispositivo se junta à frota automaticamente assim que o **host do agente** naquele site pode vê-lo via ADB. Existem duas etapas. Primeiro, habilite o ADB no dispositivo. Em seguida, se o agente estiver rodando em uma VM ou contêiner, passe o dispositivo USB para ele.

1. Habilitar ADB no telefone

1. No dispositivo, abra **Configurações → Sobre o telefone** e toque em **Número da versão** sete vezes para desbloquear **Opções de desenvolvedor**.
2. Em **Configurações → Sistema → Opções de desenvolvedor**, ative **Depuração USB**.
3. Conecte o telefone ao host do agente com um cabo USB **capaz de dados**.
4. O telefone mostra um prompt *"Permitir depuração USB?"* com a chave RSA do host. Marque **Sempre permitir deste computador** e aceite. (Sem a marcação, o prompt retorna toda vez que se reconecta e o dispositivo aparece como `não autorizado`.)

Um dispositivo normal não precisa de mais nada. Os scripts de teste e a tela ao vivo usam apenas ADB padrão. Mantenha a tela desbloqueada para a primeira conexão para que o prompt possa ser aceito.

2. Passar o dispositivo USB para o host do agente

Ignore isso se o agente estiver rodando em hardware físico. Se o host do agente for uma máquina virtual ou contêiner, o hipervisor possui a porta USB, então você deve encaminhar o dispositivo:

Plataforma	Como encaminhar o dispositivo
Proxmox (VM)	`qm set <vmid> -usbN host=<bus>-<port>` para vincular uma porta física (o mapeamento sobrevive à troca de telefones nessa porta), ou `host=<vendor>:<product>` para seguir um dispositivo específico. Encontre os ids com `lsusb` no host Proxmox.
Proxmox (contêiner LXC)	Adicione a `/etc/pve/lxc/<ctid>.conf`: uma permissão de dispositivo-cgroup para USB (`lxc.cgroup2.devices.allow: c 189:* rwm`) e um bind-mount do barramento USB (`lxc.mount.entry: /dev/bus/usb/<bus> dev/bus/usb/<bus> none bind,optional,create=dir`), em seguida, reinicie o contêiner. Reconectar um dispositivo em um barramento diferente precisa do barramento correspondente montado.
VMware	Com a VM em execução, **VM → Dispositivos Removíveis → <telefone> → Conectar** (ou adicione um controlador USB e anexe o dispositivo nas configurações da VM).

> Modems USB e dongles Android antigos são encaminhados da mesma forma. Eles aparecem como a mesma classe de dispositivo USB, então um barramento que é passado carrega telefones, modems e dongles.

3. Confirmar que ele aparece

No host do agente, `adb devices` deve listar o dispositivo como `device` (não `não autorizado` ou `offline`). Dentro de alguns segundos, ele aparece na **Visualização da Frota** para aquele site. Se não aparecer, veja Solução de Problemas.

Visualização da Frota

A visualização **Dispositivos de Teste** lista cada dispositivo conectado em todos os sites, agrupados por site. Cada cartão mostra o modelo, fabricante, versão do Android, resolução da tela, operador de rede, bateria e build. À primeira vista, você pode ver quais telefones estão online e saudáveis.

A frota agrupa dispositivos por site (por exemplo, "Site Celular 12", "Laboratório Norte"). Cada cartão mostra status ao vivo, bateria e operador. Selecione telefones e um script para distribuir um teste entre eles. Clique em um cartão para abrir seu console.

Rotulando um dispositivo. O lápis em um cartão da frota abre **Editar metadados do dispositivo**, onde você pode dar um **nome** amigável a um dispositivo e registrar seu **operador**, **IMSI** e **MSISDN**. Esses são atribuídos pelo operador (Android moderno oculta o IMSI/MSISDN do ADB) e permanecem com o dispositivo mesmo quando ele está offline. O nome é o que aparece nos cabeçalhos do console e nos seletores de dispositivos.

A entrada **Dispositivos de Teste** da barra lateral se expande para mostrar cada site (com uma contagem de dispositivos), a visualização **Agentes**, a

biblioteca de scripts, o agendador e as ferramentas de dispositivos, para que você possa ir direto onde precisa.

Executando testes em dispositivos

Selecione um ou mais telefones, escolha um script e **Executar nos selecionados** distribui-o em paralelo. Os resultados são transmitidos para uma tabela, uma linha por dispositivo com um distintivo de aprovação/reprovação, código de saída, duração e saída expansível.

Agentes

A visualização **Agentes** (barra lateral → Dispositivos de Teste → Agentes) lista cada banco conectado a este servidor, uma linha por host de site, com seu status online, IP, os dispositivos que carrega, quando se registrou e sua versão de software. Ela responde "quais sites estão realmente reportando, e de onde?" à primeira vista, e é onde você confirma que um banco recém-instalado se conectou.

Console do Dispositivo

Clicando em um telefone abre seu **console**: uma visualização ao vivo da tela com controle remoto total.

*O console transmite a tela do telefone ao vivo. Clique para tocar, arraste para deslizar, digite para inserir texto. Um distintivo de **qualidade de rede** (canto superior direito da tela) mostra verde/amarelo/vermelho à primeira vista. Clique nele para ver as estatísticas de transmissão completas (resolu��ão, FPS, taxa de bits, % de perda de pacotes em 5 segundos, jitter, RTT). A barra de teclas de hardware (voltar, home, recentes, volume, energia) e ações rápidas (Avião, Discador, Mensagens, Configurações) ficam abaixo. Um painel de ferramentas em abas fica ao lado: Validação Celular, Scripts, Shell, Logcat, Arquivos e Gravar.*

> **Um visualizador por vez.** Um dispositivo transmite para um operador por vez. Se alguém já estiver visualizando, o console mostra *"Em uso por <usuário> (<IP>)"*. O IP permite que você saiba se é você em outra máquina ou um operador diferente. Um botão **Assumir** reivindica a transmissão. Um console desconectado ou recarregado se reconecta automaticamente à sua própria sessão em vez de lutar por ela.

Controle remoto

Ação	Como
Tocar	Clique em qualquer lugar na tela
Deslizar	Clique e arraste
Digitar	Clique na tela e, em seguida, digite no seu teclado
Teclas de hardware	Botões Voltar, Início, Recentes, Volume ±, Energia
Ações rápidas	Alternar Avião com um clique, ou abrir o aplicativo Discador, Mensagens ou Configurações. Essas ações são executadas em segundo plano. Elas não executam um teste ou bloqueiam o console.

A tela transmitida é o dispositivo ao vivo. Qualquer aplicativo ou página da web é renderizado e totalmente controlável a partir do console. Aqui, um telefone de teste tem uma página aberta no navegador, controlada remotamente:

Visualizando mais de um telefone

Para assistir a vários dispositivos ao mesmo tempo (ambas as extremidades de uma chamada de teste, por exemplo), abra o console de um telefone e clique em **Telefone extra** (canto superior direito). Escolha outro telefone na lista e sua tela ao vivo se abre ao lado da primeira, com seus próprios controles completos: tocar/deslizar/digitar, teclas de hardware, ações rápidas, ouvir áudio e estatísticas de transmissão. A lista permanece aberta para que você possa continuar adicionando, e as telas se organizam pela página — não há limite fixo, então adicione quantos o banco tiver.

Para abrir todo um grupo de uma só vez, marque os telefones que você deseja na lista de Dispositivos de Teste e clique em **Visualizar selecionados**: o primeiro se torna o dispositivo principal (aquele sobre o qual a coluna de ferramentas atua) e o restante se organiza ao lado dele.

Cada tela extra possui seu próprio seletor para **trocar** qual telefone ela mostra e um × para fechá-la. O arranjo é capturado no endereço da página (`?with=…`), então um layout específico de múltiplos telefones pode ser salvo como favorito ou compartilhado.

O painel de ferramentas em abas (Celular, Scripts, Shell, …) sempre atua no telefone **principal**, aquele que você abriu. O cabeçalho do painel o nomeia para que fique claro onde um script ou comando será executado.

Ferramentas do Console

Ao lado da tela, um **painel de ferramentas em abas** mantém as ferramentas por dispositivo juntas. Troque de abas sem perder o estado de cada ferramenta:

Aba	O que faz
Celular	As ferramentas de validação de chamada / texto / ping / teste de velocidade (abaixo)
Scripts	Execute um script da biblioteca neste dispositivo e veja seu histórico completo de execução, com um clique para reexecutar qualquer execução anterior
Shell	Um console interativo de comando/resposta para o dispositivo
Logcat	Transmissão de log do dispositivo ao vivo com filtragem de texto + nível
Arquivos	Navegue, baixe, faça upload, renomeie e exclua arquivos no dispositivo
Gravar	Capture uma sequência de toque/deslizamento como linhas de script reproduzíveis

Painel de Validação Celular

Ferramentas integradas para as verificações que um operador executa manualmente, cada uma recebendo as entradas que você esperaria:

Ferramenta	Entradas	O que faz
Chamada	Número, tempo de espera	Disca, confirma que a chamada foi atendida, aguarda, desliga
Texto	Número, mensagem	Envia um SMS e confirma que saiu do dispositivo
Ping	Host, contagem	Pinga um host pela conexão de dados do dispositivo
Teste de Velocidade	URL de teste	Mede a largura de banda de download pela conexão de dados do dispositivo. A URL padrão baixa do LibreSpeed no host `speedtest` do site do telefone.

A caixa **Número** lembra números que você chamou ou enviou mensagens recentemente (mantidos apenas no seu navegador, não no servidor) e os oferece como um dropdown, então rediscando um número de teste é um clique.

Scripts

A aba **Scripts** executa qualquer script da biblioteca contra este dispositivo e mantém seu histórico completo de execução sem sair do console. Você pode filtrar esse histórico por origem, status e teste. Cada execução anterior tem um botão de **reexecução**, então repetir uma verificação (ou um script que acabou de falhar) é um clique. Scripts que recebem entradas solicitam novamente.

Shell

A aba **Shell** é um console interativo de comando/resposta para o dispositivo. Digite um comando, veja sua saída e código de saída, com ↑/↓ para recordar o histórico. É o análogo do dispositivo do console AT do modem, para os momentos em que um comando rápido é mais rápido do que escrever um script.

Logcat

A aba **Logcat** transmite o log do sistema ao vivo do dispositivo. Filtre por texto livre e nível mínimo (Verbose → Fatal). Os níveis são codificados por cores. **Iniciar**/**Parar** controla a transmissão. Parar mantém o que você capturou na tela para que você possa rolar de volta.

Arquivos

A aba **Arquivos** é um gerenciador de arquivos para o dispositivo. Navegue por diretórios (começando em `/sdcard`), **baixe** um arquivo para sua máquina, **faça upload** de um arquivo para o dispositivo, e **renomeie**, **exclua** ou crie pastas. Útil para puxar um arquivo de captura ou diagnóstico de um dispositivo, ou para empurrar uma configuração para ele.

Gravação de gestos

Ative **Gravar**, execute uma sequência de toque/deslizamento na tela, e o console emite as linhas equivalentes de `adb input`. Cole-as em um script de pasta para transformar um fluxo de UI manual em um teste repetível.

Console do Modem USB

Um modem celular USB (Quectel EP06 e similares) aparece na frota como um **modem** e abre um console celular em vez de uma tela. O agente retransmite comandos AT para o modem pela sua porta serial (AT). Ele registra cada comando e resposta na aba **Terminal** como um histórico de auditoria.

Aba	O que faz
Status	Leitura única de modelo / firmware / IMEI / IMSI / SIM, sinal (CSQ + QCSQ por RAT), operador, registro EPS, anexar, IMS, IP, APN, DNS/PCO
Ações	Definir APN (pré-definido ou personalizado, com **PDP / tipo de IP**), anexar/desanexar dados, mostrar IP + DNS, pingar, enviar SMS, rádio (avião / reiniciar)
Redes	Varredura de operador (`AT+COPS=?`) e uma **medição de célula** de serviço/vizinha (`AT+QENG`) → tabela EARFCN / PCI / banda / RSRP / RSRQ / SINR
Bloqueio de célula	Bloquear para um **EARFCN específico (+PCI)** (`AT+QNWLOCK`), bloqueio de banda (`AT+QCFG="band"`), preferência de RAT, ou liberar de volta para automático
Chamadas	Discar / atender / desligar, uma tabela de chamadas `AT+CLCC`, e um controle **Habilitar / Desabilitar VoLTE** (`AT+QCFG="ims"`)
SMS	Ler a caixa de entrada (`AT+CMGL`), excluir e enviar
Eventos	Habilita os URCs relevantes e os poll para um log com timestamp (registro / chamada / sinal / novas mudanças de SMS)
Terminal	Entrada AT bruta mais o log completo de requisições/respostas

A referência completa de comandos AT, com respostas reais do EP06, está em **modem-at-commands.md**.

> **VoLTE:** o EP06 é VoLTE/IMS-only para voz. *Habilitar VoLTE* define `AT+QCFG="ims",1`; um reinício `AT+CFUN=1,1` pode ser necessário para

> (des)registrar IMS, e ele só se registra se a rede + SIM o provisionarem e o MBN do operador correto for selecionado.

Dongles Android Antigos (modo screencap)

Dongles LTE "MiFi" baratos (~$10) (por exemplo, o UZ801, Qualcomm msm8916) rodam **Android 4.4 (API 19)**, que é muito antigo para a visualização de tela ao vivo. Esses dispositivos voltam para um console de **screencap**: o agente polls `adb screencap` para quadros (alguns por segundo, porque `screencap` em si é o gargalo nesse hardware) e injeta `adb input` para controle. Você obtém uma visualização de clique-para-tocar, digitar-para-texto. Não é vídeo suave, mas é suficiente para controlá-lo.

O agente suaviza as arestas ásperas desses dongles no lado do host:

- **Desbloqueio ADB**: eles são enviados no modo RNDIS. Um serviço acionado por udev `curl` o `usbdebug.html` do dongle para mudar para o modo ADB. Veja agent/host-setup/mifi-dongle.
- **Auto-Inglês**: eles são enviados em chinês. O agente define `persist.sys.language` para `en-US` na primeira vez que vê um dispositivo API-<21 (desative com `OMNIWEB_DONGLE_AUTO_ENGLISH=0`).

Scripts

Os testes são scripts bash que rodam no **host do agente** (então ferramentas de host como `grep`/`awk` estão disponíveis) e visam um dispositivo via ADB. Existem dois tipos:

- **Scripts de pasta**: verificações de saúde que aparecem na biblioteca, no executor de distribuição e no agendador. Alguns rodam apenas com o dispositivo (Dispositivo Conectado, Registro VoLTE, Relatar Força do Sinal). Outros recebem entradas opcionais (`@param`). O Teste de Ping recebe um host e uma contagem. O Teste de Largura de Banda de Dados recebe uma URL. Nessa URL, `{SPEEDTEST}` é substituído pelo primeiro host no grupo de inventário `speedtest` do site do telefone. O site do telefone é o site de

inventário que contém o host do agente do telefone. Se o OmniWeb não conseguir encontrar o site ou seu host `speedtest`, a execução falha com um erro que nomeia o item ausente. Os testes de conectividade e voz (Ping, Largura de Banda de Dados, Enviar SMS, Fazer Chamada) são scripts de pasta, então você pode agendá-los, bem como executá-los manualmente. Dois testes de recuperação de flap de avião confirmam que um dispositivo se recupera após perder rádio. **Flap de Avião → Recuperação de Ping** ativa o modo avião, depois desativa, aguarda a reconexão de dados e, em seguida, pinga. **Flap de Avião → Recuperação de IMS** faz o mesmo, depois confirma que o VoLTE se registra novamente.

- **Ferramentas integradas**: os atalhos de abertura de aplicativo (Discador, Mensagens, Configurações) e o simples alternador de Avião nas ações rápidas do console. Cada um executa uma ação de UI com nenhum resultado de aprovação ou reprovação, então não está na biblioteca ou no agendador.

A biblioteca de scripts lista os scripts de pasta sem argumentos. Cada um mostra sua descrição e timeout. Clique em um para visualizar sua fonte (somente leitura). Execuções recentes aparecem abaixo.

Um script relata seu resultado por **código de saída**: `0` é uma aprovação, qualquer outra coisa é uma reprovação. Sua saída capturada é mostrada na tabela de resultados.

Testes Programados

Os testes programados são definidos de forma declarativa em `schedules.json` no diretório de scripts. O arquivo é lido novamente em cada ciclo, então edições entram em vigor sem uma reinicialização. Cada entrada executa um script de pasta contra seus dispositivos-alvo em um intervalo.

Configuração

```
{
  "schedules": [
    {
      "name": "Registro VoLTE",
      "script": "volte_registration.sh",
      "interval_seconds": 120,
      "serials": [],
      "enabled": true
    }
  ]
}
```

Parâmetro	Tipo	Requerido	Padrão	Descrição
`name`	String	Sim	-	Rótulo único para o agendamento. Aparece como o rótulo `schedule` na métrica exportada.
`script`	String	Sim	-	Nome do arquivo de um script em pasta no diretório de scripts a ser executado.
`interval_seconds`	Inteiro	Não	300	Com que frequência executar o script, em segundos. Mínimo 30.
`serials`	Lista	Não	`[]`	Sériais de dispositivos a serem alvo. Uma **lista vazia significa todos os dispositivos atualmente conectados**, então o agendamento segue automaticamente os telefones conectados.

Parâmetro	Tipo	Requerido	Padrão	Descrição
`params`	Objeto	Não	`{}`	Entradas para um script que declara valores `@param`. As chaves são os nomes dos parâmetros. Por exemplo, o Teste de Ping aceita `host` e `count`.
`enabled`	Booleano	Não	true	Se o agendamento está ativo. Defina `false` para pausá-lo sem remover a entrada.
`exclusive`	Booleano	Não	false	Reserve o telefone durante a duração deste teste. Enquanto um teste exclusivo está em execução, nenhum outro teste agendado começa nesse dispositivo, e o teste exclusivo em si espera que o dispositivo esteja livre antes de começar. Use-

Parâmetro	Tipo	Requerido	Padrão	Descrição
				o para testes disruptivos — uma flutuação no modo avião ou um reinício — que corromperiam outro teste (digamos uma chamada VoLTE) em execução no mesmo aparelho ao mesmo tempo.

Exemplo: Verificação VoLTE em um site

```
{
  "name": "Registro VoLTE",
  "script": "volte_registration.sh",
  "interval_seconds": 120,
  "serials": [],
  "enabled": true
}
```

Como funciona: A cada 120 segundos, o agendador executa `volte_registration.sh` em cada telefone conectado. O script verifica se o dispositivo está registrado para voz (`IN_SERVICE`) na LTE com suporte a VoPS (Voice-over-PS) e sai com `0` se o VoLTE estiver registrado. O resultado se torna um gauge do Prometheus por dispositivo.

Caso de uso: Provar continuamente que aparelhos reais em um site podem registrar para VoLTE e alertar no momento em que um não puder.

Exemplo: Ping em todos os telefones

```
{
  "name": "Teste de Ping",
  "script": "ping_test.sh",
  "interval_seconds": 120,
  "serials": [],
  "params": { "host": "8.8.8.8", "count": "5" },
  "enabled": true
}
```

Como funciona: A cada 120 segundos, o agendador executa `ping_test.sh` em cada telefone conectado. Os `params` fornecem as entradas do script. O script faz ping em `8.8.8.8` cinco vezes através do link de dados do dispositivo e sai com `0` se receber respostas. Altere `host` para testar um alvo específico.

Caso de uso: Provar que aparelhos reais em um site têm dados funcionando e alertar sobre perda de pacotes.

Pausa automática enquanto um telefone está em uso

Abrir a tela ao vivo de um telefone pausa os testes agendados **para aquele telefone**. Um teste acionado em um aparelho que alguém está assistindo e tocando lutaria por espaço na tela e registraria um resultado sem sentido de aprovação ou reprovação, então o agendador ignora qualquer telefone que tenha um visualizador ao vivo e retoma assim que a visualização é encerrada.

- A pausa é por telefone. Todos os outros telefones que um agendamento visa continuam a funcionar em seu intervalo normal.
- Uma execução ignorada não é contabilizada como concluída: o agendamento é acionado em seu próximo ciclo assim que o telefone estiver livre, em vez de esperar um intervalo completo.
- Um teste que já estava em execução quando a tela foi aberta é deixado para terminar.
- Feche a visualização do telefone (ou navegue para longe) e os testes são retomados em cerca de um minuto. Se o navegador desaparecer sem fechar corretamente, a pausa se encerra sozinha.

- **Executar agora** não é afetado — uma execução solicitada explicitamente sempre avança.

A aba Testes Agendados do telefone mostra um banner enquanto a pausa está em efeito, e a frota marca um telefone retido **em uso** com quem o possui.

Métricas

O OmniWeb central expõe o último resultado de cada teste agendado, por dispositivo, no formato Prometheus em `/api/android/metrics`. O Prometheus o coleta como o trabalho `android_device_tests` (configurado automaticamente pelo papel de monitoramento).

Métrica: `omniweb_android_test_pass` **Tipo**: Gauge **Descrição**: Resultado da execução agendada mais recente: `1` para aprovação, `0` para reprovação **Rótulos**:

- `phone`: modelo do dispositivo (por exemplo, `SM-A536E`)
- `serial`: número de série do dispositivo
- `site`: o rótulo do site do agente (por exemplo, `Cell Site 12`)
- `agent`: o host do agente ao qual o dispositivo está conectado
- `script`: o script que foi executado
- `schedule`: o nome do agendamento
- `status`: o resultado da execução (`passed`, `failed`, `timeout`, ou `error`)

Os gauges acompanhantes compartilham os mesmos rótulos:

Métrica	Descrição
`omniweb_android_test_duration_ms`	Duração da última execução, em milissegundos
`omniweb_android_test_last_run_timestamp`	Tempo Unix da última execução

Um gauge separado relata quais telefones estão atualmente retidos por um visualizador, para que um alerta de obsolescência possa distinguir um telefone deliberadamente pausado de um teste quebrado:

Métrica	Descrição	Rótulos
`omniweb_android_device_in_use`	`1` enquanto alguém tem a tela do telefone aberta (seus testes agendados estão pausados), `0` caso contrário	`serial`, `phone`, `site`, `agent`

Consultas de exemplo:

```
# Telefones que estão falhando no registro VoLTE
omniweb_android_test_pass{schedule="Registro VoLTE"} == 0

# Testes que falharam agrupados por site
count by (site) (omniweb_android_test_pass == 0)

# Um teste que não foi executado recentemente (agente obsoleto ou
dispositivo offline)
time() - omniweb_android_test_last_run_timestamp > 600

# O mesmo, ignorando telefones que alguém atualmente tem abertos
(os testes estão pausados para esses)
(time() - omniweb_android_test_last_run_timestamp > 600)
  unless on (serial) omniweb_android_device_in_use == 1

# Telefones atualmente em uso
omniweb_android_device_in_use == 1
```

Dashboard do Grafana

O papel de monitoramento envia um dashboard **Testes de Telefone / Dispositivo** (pasta do Grafana **Dispositivos**). Ele lê as métricas acima e mostra, por telefone e agendamento:

- uma linha do tempo de estado de aprovação ou reprovação,

- o resultado mais recente para cada telefone e teste,
- frescor do teste (tempo desde a última execução, para capturar um agente parado),
- duração da execução ao longo do tempo.

Filtre o dashboard por site, telefone ou teste na parte superior. O dashboard é provisionado automaticamente. Veja Grafana.

Solução de Problemas

Um telefone não aparece na frota

Sintomas: Um dispositivo está conectado em um site, mas não está listado sob Dispositivos de Teste.

Possíveis causas:

- O telefone não está autorizado para ADB no host do agente
- O agente não está em execução ou não consegue acessar o central
- O telefone está em um estado offline/não autorizado do ADB
- O serviço central de Dispositivos de Teste não está em execução (Dispositivos de Teste é servido por seu próprio serviço de backend dedicado, separado do pool de solicitações principal)

Resolução:

1. Confirme que o telefone aparece como `device` (não `unauthorized`/`offline`) no ADB no host do agente, aceitando o prompt RSA no aparelho, se necessário.
2. Verifique se o serviço do agente está em execução e se sua URL central configurada e token estão corretos.
3. No central, confirme que o serviço de Dispositivos de Teste está em execução e que o gateway roteia `/api/android/*` para ele. Se o agente se registrou, mas a frota está vazia, este serviço é a causa usual.
4. Verifique a conexão USB do telefone; reconecte o cabo se ele aparecer como offline.

A tela do console permanece em "Conectando"

Sintomas: O console do dispositivo abre, mas a tela nunca aparece, enquanto o restante da interface do usuário (lista da frota, detalhes do dispositivo, entrada) funciona normalmente e o dispositivo aparece **online**.

Possíveis causas:

- O UDP está bloqueado entre a rede do navegador e o host do agente (os streams de vídeo ao vivo **diretamente** do navegador → host do agente, não via servidor, e esta é de longe a causa mais comum)
- O agente não consegue iniciar a captura de tela naquele aparelho

Isso **não** é um problema de SSL ou MTU: o TLS está comprovadamente funcionando (a interface foi carregada), e com problemas de MTU o vídeo se conectaria e *então* se desconectaria em vez de nunca iniciar. O sinalizador indicativo é um dispositivo que aparece **online** na frota, mas cuja visualização ao vivo não começará.

Resolução:

1. Confirme que a rede do navegador pode alcançar o host do agente via **UDP** (o caminho do vídeo). Isso geralmente significa uma regra de firewall/VLAN permitindo a sub-rede do operador aos hosts de bancada via UDP. Veja **Requisitos de Rede** para a regra exata a ser solicitada e como confirmar a correção.
2. Verifique o log do agente para erros de captura de tela. Alguns aparelhos não podem ter sua tela capturada via ADB.

Verificações de VoLTE / sinal relatam "não legível"

Sintomas: Scripts de VoLTE ou sinal falham com o estado de telefonia ilegível.

Possíveis causas:

- O aparelho restringe o status de telefonia ao acesso privilegiado

Resolução:

1. Use aparelhos de teste que exponham o status de telefonia ao ADB. Dispositivos de consumo bloqueados por fornecedores podem ocultá-lo sem acesso privilegiado.

Dispositivos de Teste: Requisitos de Rede

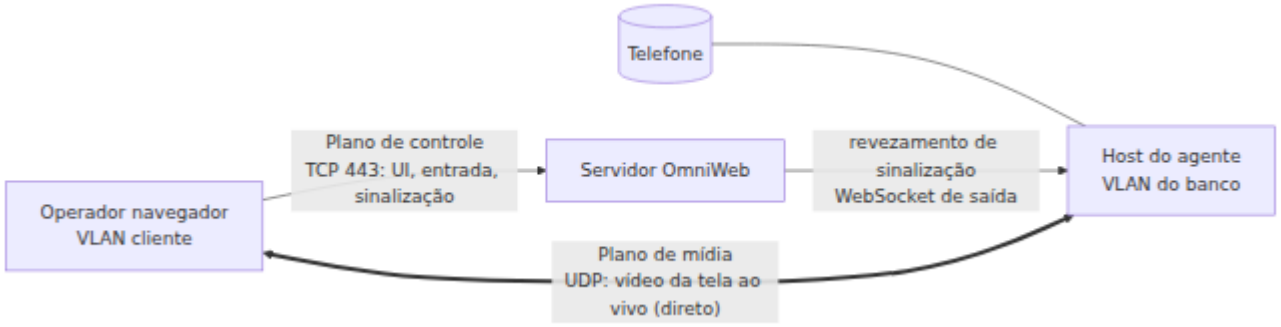
A visualização ao vivo de telefones em **Dispositivos de Teste** utiliza **dois caminhos de rede separados**. Entenda a divisão para que funcione através de firewalls e VLANs. A divisão também ajuda você a diagnosticar o sintoma mais comum, um console que fica em **"Conectando…"** para sempre.

← Voltar para Dispositivos de Teste

Os dois caminhos

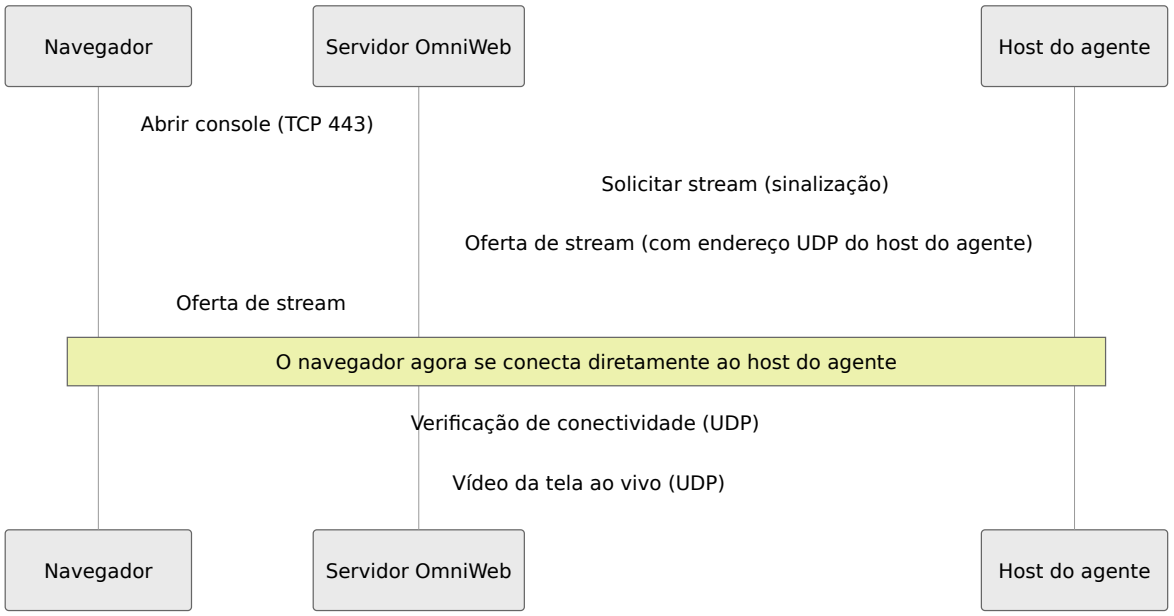
Caminho	Transporta	Direção	Transporte	Ponto final
Plano de controle	A interface web, login, a lista de dispositivos, entrada remota, resultados de teste e a configuração da chamada ("sinalização") para uma visualização ao vivo	Navegador → servidor OmniWeb	**TCP 443 (HTTPS)**	O servidor OmniWeb
Plano de mídia	O vídeo da tela ao vivo	Navegador ⇄ **host do agente** (o banco ao qual o telefone está conectado)	**UDP** (WebRTC)	O host do agente, **não** o servidor

O ponto crucial: **o vídeo ao vivo não flui através do servidor OmniWeb.** Uma vez que o servidor estabeleceu a conexão, o vídeo é transmitido **diretamente entre o navegador do operador e o host do agente** via UDP. Se uma rede permite que o navegador alcance o *servidor* mas não o *host do agente*, ela carrega a interface, mostra a lista de dispositivos e então trava em "Conectando…".



Por que o caminho de mídia é direto

O vídeo da tela ao vivo é enviado ponto a ponto com **WebRTC sobre UDP** para que sobreviva melhor aos links com perda e alta latência típicos de sites celulares remotos do que se fosse retransmitido através de um servidor central via TCP. A desvantagem é que o navegador do operador precisa de um **caminho UDP direto para o host do agente**. Não há revezamento de mídia no meio para se apoiar.



Requisitos de Firewall

Para que um operador visualize telefones em um site, **ambos** os caminhos devem ser permitidos da rede do operador para os hosts relevantes.

Plano de controle (geralmente já aberto)

Campo	Valor
Ação	Permitir (com estado)
Protocolo	TCP
Fonte	VLAN(s) do operador / cliente
Destino	Servidor OmniWeb
Porta de destino	`443`

Se a interface do OmniWeb carrega, este caminho já está aberto. Nenhuma alteração necessária.

Plano de mídia (o que geralmente está faltando)

Campo	Valor
Ação	Permitir (**com estado**, então o vídeo de retorno é permitido automaticamente)
Protocolo	**UDP**
Fonte	VLAN(s) do operador / cliente, onde os navegadores estão em execução
Destino	A **sub-rede do host do banco de dispositivos** (os hosts do agente), por exemplo, `10.0.20.0/24`
Portas de destino	**`32768–60999`** (a faixa efêmera padrão do Linux da qual o agente extrai portas de mídia)

O navegador sempre inicia a conexão de mídia, então uma permissão **com estado** em `cliente → host do agente` UDP também permite automaticamente o vídeo de retorno do agente. Nenhuma porta STUN/TURN ou outra está envolvida.

> **Não altere a porta 443 para isso.** A sinalização já utiliza o plano de controle. Apenas o caminho de mídia UDP para os hosts do agente precisa ser aberto.

Recomendado: fixar a faixa de portas de mídia

Abrir toda a faixa efêmera (`32768–60999`) é amplo. Você pode, em vez disso, configurar o agente para extrair suas portas de mídia de uma pequena faixa fixa. Isso reduz a regra do firewall para um bloco organizado:

Campo	Valor
Ação	Permitir (com estado)
Protocolo	UDP
Fonte	VLAN(s) do operador / cliente
Destino	Sub-rede do host do banco de dispositivos
Portas de destino	**`50000–50100`** (faixa fixada)

Esta é a forma preferida para entregar a uma equipe de rede. 100 portas para uma sub-rede é muito mais fácil de aprovar e auditar do que a faixa efêmera completa. A faixa fixada é definida no host do agente. Coordene a faixa exata com quem mantém os bancos para que a regra do firewall e a configuração do agente coincidam.

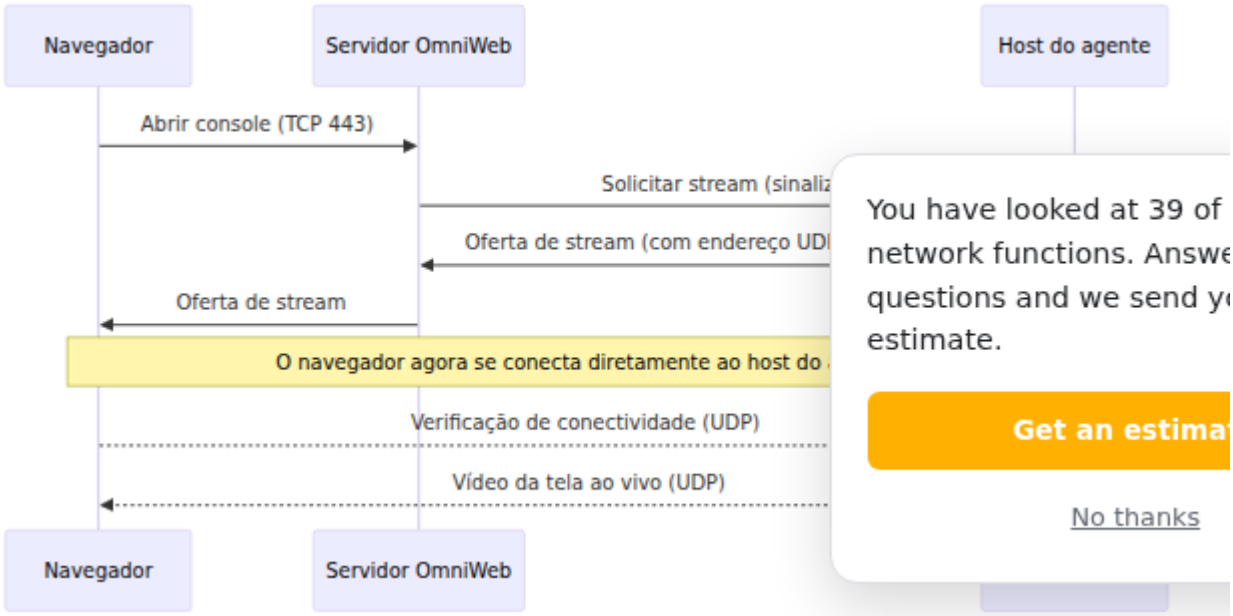
Reconhecendo o problema

Sintoma: o console do dispositivo abre, mas a tela nunca aparece. Fica em **"Conectando..."** indefinidamente. Tudo o mais funciona: a lista de frota, detalhes do dispositivo, até mesmo a configuração de entrada remota.

Isso é quase sempre o caminho UDP do plano de mídia sendo bloqueado. Não é um problema de TLS/certificado e **não** é um problema de MTU:

Causa suspeita	Por que não é isso	O que você realmente veria se fosse
SSL / certificado	A interface, login, lista de dispositivos e sinalização todos têm sucesso sobre HTTPS, então TLS está claramente funcionando	A página em si falharia ao carregar ou mostraria um aviso de certificado
MTU / fragmentação	MTU só importa uma vez que pacotes de vídeo fluem. Aqui **nenhum** pacote de vídeo nunca chega	O vídeo **conectaria**, então pararia ou rasgaria, não ficaria em "Conectando..."
Agente / telefone fora do ar	O dispositivo aparece **online** na frota com dados de bateria/operador ao vivo	O dispositivo estaria ausente da frota ou marcado como offline
Caminho UDP bloqueado ✓	O navegador pode alcançar o servidor (a interface carrega) mas não o host do agente via UDP	"Conectando..." permanente, exatamente este sintoma

Um indicativo útil: o tile do dispositivo mostra o telefone como **online** (então o agente e o telefone estão saudáveis e o servidor pode vê-los), ainda assim a visualização ao vivo não inicia. Essa combinação aponta diretamente para o caminho do firewall do plano de mídia.



Confirmando a correção

Após a regra do firewall ser aplicada, reabra o console do dispositivo. Se a tela aparecer dentro de alguns segundos e o distintivo de **qualidade da rede** (canto superior direito da visualização ao vivo) ficar verde, o caminho de mídia está funcionando. As estatísticas de stream do distintivo (resolução, FPS, bitrate, % de perda de pacotes, jitter, RTT) confirmam que o vídeo está fluindo de ponta a ponta.

Se ainda travar, verifique duas coisas com quem mantém os bancos. Primeiro, a **sub-rede e portas de destino** da regra do firewall devem corresponder aos hosts do agente e sua faixa de portas de mídia configurada. Em segundo lugar, a regra deve se aplicar à **real** VLAN de origem do operador (um laptop na Wi-Fi de convidados é uma fonte diferente da LAN corporativa).

Múltiplas localizações de operadores

Cada rede de operador que precisa visualizar telefones deve ter a regra do plano de mídia para sua própria VLAN de origem. A regra é por sub-rede de origem → sub-rede do banco, então adicionar um novo escritório, pool de VPN ou site significa adicionar sua sub-rede como uma **Fonte** adicional na mesma

permissão UDP. Sites cujos operadores visualizam telefones apenas da própria LAN do banco não precisam de regra inter-VLAN alguma.

Topologia de Rede & Painel Único

As visualizações de topologia do OmniWeb são o ponto de entrada "painel único" para toda a rede. Elas mostram como os elementos se conectam, quais estão implantados e permitem que você salte diretamente de um nó no mapa para o espaço de trabalho desse elemento.

← Voltar ao Guia de Operações

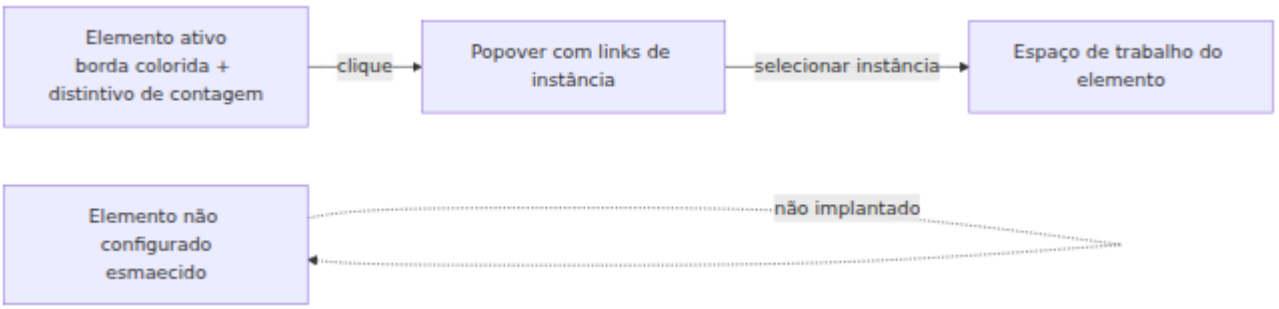
Visualizações de Topologia

A página de entrada/topologia apresenta a rede em quatro abas de domínio. Cada uma é um mapa interativo dos elementos relevantes e suas interfaces.

Topologia EPC: UE → eNB → MME → SGW-C → PGW-C → UPF, com sinalização Diameter através do DRA para o HSS. Elementos ativos mostram uma borda colorida e um distintivo de contagem de instâncias.

Aba	Elementos mostrados
Core (EPC)	UE → eNB → MME → SGW-C → PGW-C → UPF; DRA ↔ HSS; OCS; TWAG; Monitor RAN
IMS	P-CSCF → I-CSCF → S-CSCF; DRA ↔ HSS; TAS; IMS SMSc → SMSC → SMPP GW; OCS; Direito (OmniSEP)
CS Core	BTS → BSC → MSC; STP ↔ HLR / CAMEL GW / IP-SM-GW; HSS; SMSC; OCS
5G Core	gNB → AMF → SMF → UPF; NRF, SCP, AUSF, UDM, UDR, PCF; CHF → OCS; NSSF; BSF

Lendo o Mapa



- **Elementos ativos** são aqueles com instâncias declaradas em `omniweb.json`. Eles aparecem com uma borda colorida e um distintivo que mostra quantas instâncias existem. Clique em um para abrir um popover com links diretos para cada instância. Você pode então navegar da topologia diretamente para as páginas de um elemento.
- **Elementos não configurados** aparecem esmaecidos, então o mapa também serve como um inventário rápido do que está e não está implantado.
- **Conexões** indicam a interface entre elementos (por exemplo, SIP, Diameter, PFCP, GTP-C, SS7), distinguindo os tipos de sinalização.

Isso torna a página de topologia o ponto de partida natural: veja a forma da rede, identifique o que está implantado e aprofunde-se.

Topologia em Nível de Elemento

Alguns elementos também fornecem sua própria visualização de topologia focada. A aba **PGW-C → Topologia**, por exemplo, mostra os relacionamentos desse nó com seus pares SGW-C, UPF e Diameter, anotados com contagens de sessões ativas e utilização. Isso oferece uma visão de painel único localizada para a vizinhança desse elemento.

Topologia PGW-C: relacionamentos de pares SGW-C, UPF e Diameter com distribuição de sessões por par.

Lista de Hosts & Infraestrutura

Além das funções de rede em si, a página **Lista de Hosts** é o painel único para a *infraestrutura* que as executa. Ela lista todos os hosts de infraestrutura por categoria, cada um com um link direto para sua interface web:

Categoria	Exemplos
Monitoramento	Grafana, Prometheus, Loki
Captura SIP	Homer Web UI
Cobrança	OCS Web UI
DNS	Servidores DNS
Virtualização	Consoles de hipervisor Proxmox
Gerenciamento fora de banda	Gerenciamento de servidor iDRAC
Roteadores	MikroTik WebFig, Peplink
Micro-ondas	Links SAF, Ubiquiti AirFiber
NAS	Synology DSM

A Lista de Hosts: cada host de infraestrutura e elemento por categoria, cada um com um link direto para sua interface web (Grafana, Prometheus, Loki, APIs de elementos e mais).

Isso dá aos operadores um lugar para acessar todos os sistemas de suporte: monitoramento, hipervisores, gerenciamento fora de banda e transporte. Eles não precisam procurar por favoritos.

TWAG: Gateway de Acesso WLAN Confiável

O **TWAG** (Gateway de Acesso WLAN Confiável) traz acesso Wi-Fi confiável para o núcleo móvel. Ele autentica dispositivos Wi-Fi com EAP-AKA/AKA′ contra o AAA/HSS via Diameter, atribui a cada cliente autenticado um endereço IP por DHCP e ancla seus dados de volta ao núcleo de pacotes através de um túnel GTP para o PGW. Assim, um assinante no Wi-Fi recebe o mesmo APN, política e cobrança que na rede celular. Seu painel é o lugar para ver quem está conectado, se os caminhos Diameter e GTP estão saudáveis e para limpar sessões individuais.

← Guia de Operações

O painel é uma página de elemento por instância acessada a partir da barra lateral quando um TWAG está em inventário no site. Todo o tráfego passa pelo proxy de backend OmniWeb para a API do TWAG, portanto, permanece atrás do único gateway autenticado. Ele é organizado em abas.

Visão Geral

A aba de entrada é uma leitura de saúde em uma única tela: **sessões** ativas e totais, **pares Diameter** conectados/desconectados, **assinantes** aceitos, o número de **pontos de acesso**, contagem de locações **DHCP**, o status do túnel **GTP** e seu endereço PGW, o **modo de autenticação** em uso (por exemplo, EAP-AKA), **tráfego** agregado de entrada e saída, tempo de atividade e um feed **de atividade recente** ao vivo de autenticações e inícios/paradas de sessão.

Sessões

Cada sessão Wi-Fi autenticada, cada linha mostrando a **identidade** do assinante (o identificador de acesso à rede), **status**, **IP** atribuído, **MAC** do cliente, **SSID**, **IP NAS** servidora, **duração** da sessão e **bytes de entrada/saída**. Um operador pode **deletar** uma sessão para desconectar forçadamente um cliente, por exemplo, para limpar um dispositivo preso ou com mau funcionamento.

Pontos de Acesso

Os pontos de acesso WLAN (dispositivos NAS) atualmente conectados ao gateway. Cada um pode ser **removido** individualmente quando um ponto de acesso é desativado ou precisa ser limpo.

Contabilidade

As sessões de contabilidade que o TWAG registrou: os registros de uso gerados para clientes autenticados. Sessões de contabilidade individuais podem ser **deletadas**.

Diameter

As conexões de pares Diameter para o AAA/HSS que transportam autenticação, com contagens conectadas e desconectadas. Esta aba também oferece um **teste Diameter**. Ele envia um teste de Multimedia-Auth-Request (MAR) para confirmar que o caminho de autenticação para o AAA/HSS está ativo, que é a maneira mais rápida de provar a conectividade Diameter quando as autenticações estão falhando.

DHCP

As locações DHCP que o TWAG emitiu para clientes Wi-Fi, com o endereço, cliente e estado da locação para cada um, para que você possa confirmar que os clientes estão sendo endereçados e ver quanto do pool está em uso.

Logs

A aba **Logs** exibe a saída de log ao vivo do TWAG para solucionar problemas de um gateway individual sem sair do OmniWeb.

Ações

Cada ação pede confirmação primeiro:

- **Deletar uma sessão**: desconectar forçadamente uma sessão Wi-Fi autenticada (aba Sessões, por linha).
- **Deletar um ponto de acesso**: limpar uma única entrada de ponto de acesso / NAS (aba Pontos de Acesso, por linha).

- **Deletar uma sessão de contabilidade**: remover um único registro de contabilidade (aba Contabilidade, por linha).
- **Teste Diameter**: enviar um MAR de teste para validar o caminho Diameter para o AAA/HSS (aba Diameter).

Relacionados

- O **PGW** ancla o plano de usuário do TWAG sobre GTP. Veja os elementos do núcleo de pacotes.
- O **HSS** mantém os dados de autenticação do assinante que as solicitações Diameter do TWAG resolvem.
- ePDG: o contraparte de Wi-Fi não confiável para chamadas Wi-Fi.

UPF: Função do Plano do Usuário

A **UPF** (Função do Plano do Usuário) é o nó de encaminhamento de pacotes do núcleo móvel. Ela transporta o tráfego real de cada assinante: recebe túneis GTP-U da rede de acesso na **N3** (S1-U no EPC), encaminha pacotes para e da rede de dados, aplica QoS por fluxo e contabilidade de volume, e armazena pacotes de downlink quando um dispositivo está ocioso. Ela não possui lógica própria. O plano de controle (um **SGW-C** no EPC sobre **Sxa**, ou um **SMF** em um núcleo 5G sobre **N4**) a programa completamente via **PFCP**. O plano de controle instala as regras de detecção de pacotes, encaminhamento, QoS e relatórios de uso que descrevem como a UPF lida com o tráfego de cada sessão. O **OmniUPF** da Omnitouch implementa o caminho de encaminhamento como um **dataplane eBPF/XDP** no kernel, de modo que as regras instaladas pelo plano de controle se tornam entradas em mapas eBPF que o programa XDP consulta para cada pacote. O OmniWeb exibe as associações e sessões PFCP da UPF, o conteúdo dos mapas eBPF ao vivo, estatísticas do dataplane, roteamento, buffers de downlink, estado de jardim murado e configuração. Ele acessa os gráficos de throughput e tendência nos painéis do Grafana a partir da mesma página.

← Guia de Operações

A UPF é uma página de elemento por instância acessada a partir da barra lateral quando se está no inventário do site, com um seletor de instância onde várias estão implantadas e uma visão de frota para status agregado. Todo o tráfego passa pelo proxy de backend do OmniWeb para a API da UPF, de modo que permanece atrás do único gateway autenticado. O link de documentação no cabeçalho da página (o botão de ajuda em contexto) abre esta página. Ela está organizada em abas.

Seleção de frota e instância

Onde um site executa mais de uma UPF, a **visão da frota** lista cada instância com sua saúde à primeira vista. Esta é a maneira mais rápida de confirmar que todo o plano do usuário está ativo antes de você investigar um nó.

De qualquer aba, o **seletor de instância** no cabeçalho da página alterna qual UPF a página lê. Tudo abaixo (sessões, associações, mapas eBPF, estatísticas) é escopo da instância selecionada, então você escolhe o nó uma vez e toda a página o segue.

Visão Geral

Uma leitura de saúde em uma única tela da UPF: seu status de **saúde**, o número de **associações PFCP** que mantém com pares do plano de controle, o total de **sessões ativas** entre esses pares, e os **contadores de ação XDP**: quantos pacotes o dataplane passou, descartou, redirecionou, transmitiu ou abortou, que é a confirmação mais rápida de que o tráfego está realmente fluindo. Abaixo, cada **par PFCP** é listado com seu estado de associação, contagem de sessões e quaisquer batimentos perdidos, e os **tamanhos dos mapas eBPF** mostram a capacidade dos mapas PDR, FAR, QER e URR e a contagem máxima de sessões. Uma caixa de pesquisa salta diretamente para uma sessão por **IP UE** ou **TEID**, e uma ação de **Relatório de Nó** envia um Pedido de Relatório de Nó PFCP para o primeiro par ativo do plano de controle.

Sessões

Cada **sessão PFCP**: o estado do plano do usuário por portadora / por sessão PDU que o plano de controle instalou. Cada linha é identificada por seu **SEID local e remoto** e mostra o **IMSI** da sessão, **APN/DNN**, a **associação** (qual par do plano de controle a possui), e a contagem de regras de **detecção de pacotes**, **ação de encaminhamento**, **aplicação de QoS** e **relatórios de uso** que carrega. Pesquise **por IP UE ou TEID** para encontrar a sessão que atende a um dispositivo ou túnel específico.

Onde várias UPFs estão implantadas, a mesma aba na **visão da frota** lista cada sessão PFCP em todas elas em uma tabela, com a UPF responsável mostrada contra cada linha. IP UE e TEID são pesquisados em cada UPF; IMSI e APN/DNN são correspondidos na lista combinada. Abrir uma linha vai para os detalhes daquela sessão em sua própria instância. Uma UPF que não pode ser alcançada é nomeada acima da tabela, então uma lista curta nunca é confundida com um plano do usuário ocioso.

Detalhe da Sessão

Abrir uma sessão mostra seu estado completo de regras. Um **mapa de regras de sessão** ilustra como cada **Regra de Detecção de Pacote (PDR)** referencia a **Regra de Ação de Encaminhamento (FAR)**, **Regra de Aplicação de QoS (QER)** e **Regras de Relatório de Uso (URR)** que aplica. Clique em qualquer nó para destacar apenas as regras conectadas a ele, para que você possa rastrear o caminho de um único fluxo através do dataplane. Abaixo do mapa, quatro tabelas fornecem os detalhes:

- **Regras de Detecção de Pacotes (PDR)**: como a UPF classifica pacotes de entrada. Isso cobre direção (uplink / downlink), o IP UE ou TEID de entrada que eles correspondem, os filtros SDF (protocolos e intervalos de portas), e quais FAR, QER e URRs eles resolvem.
- **Regras de Ação de Encaminhamento (FAR)**: o que acontece com pacotes correspondidos. A ação é **Encaminhar**, **Descartar**, **Armazenar** ou **Notificar CP**, com os detalhes do túnel GTP-U de saída (IP remoto e TEID) e a instância da rede. Você pode editar FARs no local.
- **Regras de Aplicação de QoS (QER)**: a QoS por fluxo. Isso cobre o **QFI**, o status do **gate** de uplink e downlink (aberto / fechado) e as **taxas de bits máxima** e **garantida**. Você pode editar QERs no local.

- **Regras de Relatório de Uso (URR)**: os contadores de volume. Estes são os bytes de uplink e downlink atuais e últimos relatados e o número da sequência do relatório, que é o que a UPF retroalimenta ao plano de controle para cobrança e cota.

A partir do cabeçalho da sessão, você também pode **ativar ou remover um redirecionamento de jardim murado** para essa sessão específica (veja Jardim Murado abaixo).

Associações

As **associações PFCP**: as relações Sxa/N4 que a UPF mantém com seus pares do plano de controle (o SGW-C ou SMF). Cada linha mostra o **IP remoto e porta** do par, sua **contagem de sessões**, se está atualmente **associado**, o número de **batimentos perdidos**, e quando se **conectou** ou **desconectou** pela última vez. Aqui você confirma que o plano do usuário e o plano de controle estão em sincronia. Aqui você também identifica um par cujos batimentos estão falhando.

Estatísticas

Os números em tempo real do dataplane. **Uso de Mapas eBPF** mostra quão cheios cada mapa está (sessões, PDR, FAR, QER e URR) como barras de usado versus capacidade que se tornam âmbar e vermelhas à medida que se aproximam de seu limite, para que você possa ver uma UPF se aproximando de sua capacidade dimensionada antes de começar a rejeitar sessões. **Estatísticas XDP** detalham os contadores de pacotes passados / descartados / redirecionados / TX / abortados, e a seção **Métricas** exibe os contadores Prometheus da UPF como figuras individuais.

Uma verificação de capacidade lê o mesmo modelo de usado versus capacidade. À primeira vista, você pode dizer se o recurso limitante é a tabela de sessões ou um dos mapas de regras.

Roteamento

As rotas que direcionam o tráfego do assinante para dentro e para fora da UPF. A tabela **Rotas IP UE Ativas** lista as rotas que a UPF atualmente mantém para pools de IP UE alocados, e uma ação **Sincronizar Rotas** as reconcilia com o dataplane. Abaixo, um **console FRR** fornece um terminal vtysh em contexto contra o daemon de roteamento da UPF. Para inspecionar o estado de roteamento, digite um comando `show` (por exemplo, `show ip route` ou `show ip ospf neighbor`), com conclusão de tabulação e histórico de comandos. Para fazer uma alteração, mude para **modo de configuração**. É assim que a UPF anuncia seus pools de UE na rede circundante sem deixar o OmniWeb.

Buffers

Os **buffers de pacotes de downlink**. Quando dados de downlink chegam para um dispositivo que está ocioso (sem túnel ativo), o dataplane retém esses pacotes contra o FAR relevante e pede ao plano de controle para localizar o dispositivo. Uma vez que o túnel é restabelecido, a UPF esvazia os pacotes armazenados (este é o lado do plano do usuário da **Notificação de Dados de Downlink**). A aba mostra o **total de pacotes armazenados** e **total de FARs** retendo pacotes, os limites de buffer **por FAR** e **total**, e uma **pesquisa por ID de FAR** para ver quantos pacotes um FAR específico está retendo. Os buffers podem ser **esvaziados** individualmente ou **limpos** em massa.

Mapas eBPF

Um navegador direto para os **mapas eBPF** que são o dataplane da UPF. Estas são as entradas brutas do lado do kernel que o programa XDP consulta para cada pacote, divididas em abas:

- **PDR de Uplink**: identificado por TEID de entrada, que mapeia um túnel para seu PDR e FAR.
- **PDR de Downlink**: identificado por IP UE, que mapeia o downlink de um assinante para seu PDR e FAR.
- **FAR**: as ações de encaminhamento, com ação decodificada, IP remoto, TEID de saída e criação de cabeçalho externo.
- **QER**: as entradas de QoS, com QFI, status do gate e limites de taxa de bits.
- **URR**: os contadores de uso, com volumes de uplink/downlink atuais e últimos relatados.

Clique em qualquer linha para **editar a entrada do mapa bruto**, que é uma ferramenta de solução de problemas e reparo de baixo nível. O PFCP normalmente controla os mapas completamente, então você edita manualmente uma entrada para diagnóstico em vez de operação rotineira.

Configuração

Uma visão somente leitura de como a UPF está configurada: sua identidade de **rede** (ID do nó, endereço e porta PFCP, porta API, endereços N3 e N9), os **recursos** que ela tem habilitados (FTUP, UEIP, o gerenciador de rotas e seu tipo, e o modo de anexação XDP: nativo, genérico ou descarregado), o intervalo de **batimento PFCP**, configurações de tempo limite e repetição, e os endereços **dataplane** N3/N9. Um alternador **JSON Bruto** mostra o documento de configuração completo para suporte. É aqui que você confirma que uma UPF está dimensionada e endereçada como esperado.

Diagnósticos

Executa um **ping do nó UPF** para um host de destino. Insira um destino e uma contagem de pacotes, e a saída bruta do ping retorna com um veredicto de sucesso/falha. É uma maneira rápida de confirmar que a UPF tem acessibilidade à rede de dados (por exemplo, para um servidor DNS ou gateway upstream) de onde os pacotes realmente saem, sem acessar o nó.

Jardim Murado

O **jardim murado**: encaminhamento restrito para sessões que devem alcançar apenas um portal cativo antes de serem autenticadas ou autorizadas. Quando você ativa um redirecionamento no SEID de uma sessão, ele reescreve o downlink para que o dispositivo vá para um **URL de redirecionamento / IP do portal** em vez da internet aberta. A aba lista cada **redirecionamento ativo** com o IP UE, IP do portal, URL de redirecionamento, IP do gNB e os TEIDs envolvidos. Para liberar a sessão para o encaminhamento normal, remova o redirecionamento. Uma **lista de permissões** de IPs ou CIDRs nomeia os destinos que uma sessão de jardim murado ainda pode alcançar diretamente (por exemplo, o portal e seus ativos). Você também pode ativar e remover redirecionamentos por sessão a partir da página de detalhes da sessão.

Logs

A aba **Logs** acompanha a saída de log ao vivo da UPF para solução de problemas de uma única instância sem deixar o OmniWeb.

Painéis de Monitoramento

Throughput, taxas de pacotes por interface, tendências de contagem de sessões e outras séries temporais para a UPF são apresentadas como painéis do Grafana, acessados a partir da página do elemento. O OmniWeb não duplica esses gráficos nativamente.

Relacionados

- **SGW-C**: o par de controle do EPC que programa esta UPF (como o SGW-U) sobre **Sxa/PFCP** e encaminha tráfego em **S1-U / N3**.
- **PGW-C / SMF**: ancla a conexão PDN e, como o SMF, programa o plano do usuário 5G sobre **N4/PFCP**.

- **MME**: conduz a configuração de portadora que, em última análise, instala as sessões vistas aqui.
- **SCEF**: transporta pequenos payloads não-IP pelo plano de controle e deliberadamente contorna este plano do usuário.
- Guia de Operações: de volta ao índice do elemento.

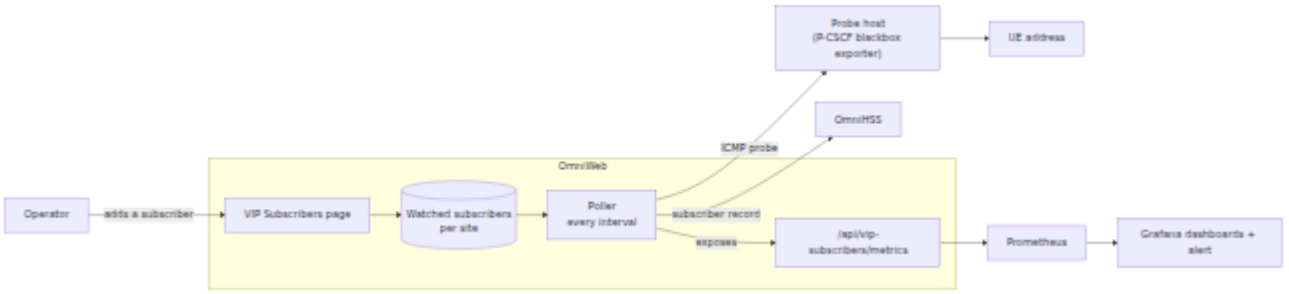
Assinantes VIP: Saúde dos Assinantes Monitorados

Assinantes VIP monitora uma lista escolhida de assinantes continuamente e informa, para cada um, se seu serviço está ativo: registrado no IMS, anexado ao EPC e acessível em seu endereço UE. A lista é gerenciada na página, por site, e cada verificação é exportada para o Prometheus, de modo que gráficos e alertas do Grafana sejam gerados exatamente sobre os assinantes que a equipe de operações escolheu.

← Guia de Operações

O que é

Alguns assinantes são mais importantes do que a média: serviços de emergência, hospitais, o roteador do site de um cliente, os telefones IP de uma conta chave. Quando um deles perde o serviço, os gráficos da frota não se movem, e o primeiro relatório vem do cliente. Esta página transforma essa lista de nomes em uma verificação contínua.



Tudo funciona **dentro do serviço OmniWeb**. Não há exportador para instalar, nenhuma lista YAML no inventário de implantação e nenhuma necessidade de reimplantação para adicionar um nome.

Tipos de serviço

Um assinante é monitorado pelo que se espera que ele faça. O tipo decide a regra de saúde; as outras verificações ainda são mostradas, mas não decidem o veredicto.

Tipo	Saudável quando	Uso típico
Voz + dados	Um S-CSCF está atribuído **e** um MME mantém o assinante	Um aparelho
Apenas dados	Um MME mantém o assinante	Um roteador, um dispositivo IoT, um sensor
Apenas voz	Um S-CSCF está atribuído	Uma conta VoIP sem SIM, um telefone IP

Um assinante que está desativado no HSS, ou cujo HSS não pode ser alcançado, é considerado não saudável, independentemente de seu tipo.

Anexação ao EPC vem do MME. O poller pergunta a cada MME do site sobre o contexto UE; o assinante está anexado quando um deles o mantém em `emm_registered`. O HSS mantém `last_seen_mme` até que esse MME envie sua purga, muitas vezes dias após o UE ter saído, então o veredicto do HSS é mostrado ao lado da linha quando os dois discordam, e decide por conta própria apenas em um site sem MME no inventário. **Registro IMS** é o S-CSCF atribuído do HSS. Para uma entrada apenas de voz, o identificador pode ser o nome de assinatura IMS (o nome de usuário SIP) de uma conta que não tem SIM; o HSS é consultado por um assinante por esse valor primeiro, e depois por uma assinatura IMS desse nome.

Os PGW-Cs também são consultados, e suas sessões são comparadas com o que o MME diz que está ativo. Uma sessão em um PGW-C que o MME não aponta para aquele APN foi deixada para trás quando o bearer se moveu, e a linha diz isso. Essas sessões obsoletas não transportam tráfego; seus endereços nunca respondem a um ping.

Acessibilidade do UE

O contexto UE no MME também carrega o endereço de cada PDN que o UE mantém. O poller pega o endereço do APN `internet`, já que esse é o bearer que um ping prova, ou qualquer outro endereço que o UE tenha. A sessão ativa do PGW-C fornece isso quando nenhum MME pode ser consultado, e o registro do HSS apenas depois disso. O endereço é pingado, e a perda e o tempo de ida e volta são relatados ao lado do veredicto de saúde, como um smokeping faria.

O ping tem que vir de algum lugar que roteie para o pool de UEs. O host OAM geralmente não faz isso, então o painel **Probing** escolhe um host de sondagem do inventário do site: qualquer host em que a implantação execute o exportador blackbox (P-CSCF, PGW-C, SGW-C, o host de monitoramento). *Este host OmniWeb* pinga diretamente, para uma implantação onde o próprio OmniWeb tem a rota. *Não pingar* ignora completamente o teste. Até que um host de sondagem seja escolhido, o endereço UE é mostrado, mas não testado.

A acessibilidade nunca muda o veredicto de saúde. Um UE que descarta ICMP ainda está em serviço.

Usando a página

Assinantes VIP está na barra lateral sob Monitoramento. A lista pertence ao site selecionado; troque de site para ver outra lista.

- **Monitorar um assinante**: insira o IMSI (ou nome de usuário SIP para voz apenas), um rótulo que as pessoas reconhecerão em um alerta, o tipo de serviço e, quando o site tiver mais de um, o HSS a ser consultado. A entrada é verificada assim que é adicionada, então a linha retorna com um veredicto.
- **Saúde** é o veredicto para o tipo. **IMS** e **EPC** mostram o registro, com o nome do S-CSCF ou MME e há quanto tempo. **Endereço UE** mostra o endereço e o resultado do ping.
- **Verificar agora** executa uma verificação de um assinante sem esperar pela próxima sondagem.

- **Pausar** suspende uma entrada. Um assinante pausado é mantido, mostrado em tom mais claro, e excluído das métricas, para que uma interrupção conhecida não mantenha um alerta ativo.
- **Abrir em…** salta para o mesmo assinante na página que possui cada fato: o registro do HSS, o contexto UE do MME, a sessão do PGW-C, os registros SIP capturados e o Rastro de Chamadas por MSISDN.
- **Editar** altera qualquer campo de uma entrada: rótulo, identificador, tipo de serviço, HSS, notas, link do ticket e expiração.
- **Link do ticket** é uma URL http ou https, geralmente o ticket de suporte que solicitou a monitorização. A linha mostra isso como seu número de ticket (a última parte do endereço) e o abre em uma nova aba.
- **Expira** remove a entrada automaticamente naquele horário. Está vazio por padrão, o que monitora o assinante até que alguém o remova. Uma entrada expirada sai das métricas imediatamente e é excluída em cerca de dez segundos. O horário é definido e mostrado no próprio fuso horário do navegador.
- **Histórico de registro** (ícone de relógio, serviços de voz) lista o que o sniffer VoIPmonitor viu para o assinante na última hora, 6 horas, dia ou semana: cada mudança de estado de registro com o endereço UE, o sensor que a viu e a perna, além de explosões de REGISTER falhadas. As contagens somam as mudanças de estado e o distintivo indica se está registrado agora. Ele procura o assinante pelo identificador, depois pelo MSISDN quando o identificador não encontra nada.
- **Parar de monitorar** remove a entrada.
- **Probing** define o host de sondagem, quantos pings cada verificação envia, seu tempo limite e com que frequência o site é rechecado.

Ver a página requer acesso de leitura ao elemento HSS; adicionar, alterar e remover entradas, e mudar as configurações de sondagem, requerem acesso de gravação a ele. O acesso ao site se aplica como em qualquer outro lugar: um usuário restrito a um site vê apenas a lista desse site.

Grafana

A exposição mantém os nomes das métricas do exportador anterior por site, então os painéis **Assinantes VIP** e **Assinantes IMS VIP**, e o alerta *Serviço de*

Assinante VIP Não Saudável, funcionam sem alterações. Dois rótulos são novos, `customer` e `site`, porque um OmniWeb pode monitorar vários sites.

Métrica	Significado
`vip_subscriber_service_healthy`	O veredicto para o tipo de serviço, 1 ou 0. Alerta sobre este.
`vip_subscriber_ims_registered`	Um S-CSCF está atribuído.
`vip_subscriber_epc_registered`	Um MME mantém o assinante.
`vip_subscriber_hss_reachable`	O HSS respondeu.
`vip_subscriber_enabled`	A conta está habilitada no HSS.
`vip_subscriber_ims_registration_age_seconds`, `vip_subscriber_epc_registration_age_seconds`	Tempo desde o último registro ou Atualização de Localização; -1 quando nenhum.
`vip_subscriber_ue_ip_reachable`, `vip_subscriber_ping_loss_percent`, `vip_subscriber_ping_rtt_avg_ms`, `_min_ms`, `_max_ms`, `vip_subscriber_ping_packets_sent`, `_received`	O resultado do ping. Presente apenas quando um host de sondagem está definido e o UE tem um endereço.

Métrica	Significado
`vip_subscriber_info`	Sempre 1; carrega o S-CSCF, MME, endereço UE, APN e qualquer erro como rótulos.
`vip_subscriber_last_check_timestamp_seconds`	Quando a linha foi verificada pela última vez.

Cada série carrega `customer`, `site`, `hss`, `imsi`, `label`, `msisdn` (do HSS) e `type`.

Scraping

`GET /api/vip-subscribers/metrics` retorna a exposição de texto do Prometheus. Ele nomeia assinantes, portanto não é acessível pela rede: o nginx admite apenas chamadores de loopback para esse caminho, e o Prometheus coleta o serviço OmniWeb no mesmo host.

```
  - job_name: vip_subscribers
    metrics_path: /api/vip-subscribers/metrics
    static_configs:
      - targets: ["127.0.0.1:5001"]
```

API

Endpoint	Propósito
`GET /api/vip-subscribers/`	A lista do site selecionado, cada uma com sua última verificação.
`POST /api/vip-subscribers/`	Adiciona um; é verificado antes da resposta.
`PATCH /api/vip-subscribers/<id>`	Altera qualquer campo: rótulo, identificador, tipo, HSS, notas, `ticket_url`, `expires_at` (null = nunca) ou a flag habilitada.
`DELETE /api/vip-subscribers/<id>`	Remove um.
`POST /api/vip-subscribers/<id>/check`	Verifica um agora.
`GET /api/vip-subscribers/options`	As instâncias HSS do site, hosts de sondagem e configurações.
`GET`, `PUT /api/vip-subscribers/settings`	As configurações de sondagem do site.

Endpoint	Propósito
`GET /api/sip-trace/registrations/subscriber/<identity>?range=1h|6h|24h|7d`	O histórico de registro que a página mostra.
`GET /api/vip-subscribers/metrics`	Exposição do Prometheus, apenas loopback.

O site viaja no cabeçalho `X-Omniweb-Site`, como para cada endpoint por site.