UZ801 LTE MiFi dongle — Activación automática de ADB (lado del host)

Los dongles Qualcomm LTE MiFi baratos de ~$10 (`05c6:90b6`, "Android"/UZ801, msm8916) inician en **modo RNDIS** con una interfaz web en `http://192.168.100.1`. Al hacer un GET a `http://192.168.100.1/usbdebug.html`, se cambian a **modo ADB** (y ya vienen root). Ref: https://nickvsnetworking.com/adventures-with-a-10-lte-mifi-dongle/

El paso de habilitación debe ejecutarse en el **host USB** (el hipervisor Proxmox), porque solo el host tiene el enlace RNDIS a `192.168.100.1` — el agente de teléfono OmniWeb se ejecuta en el LXC sin privilegios (CT 102) y alcanza el dongle solo como un dispositivo USB una vez que está en modo ADB. Así que esta automatización es udev + systemd del lado del host, no código del agente.

Archivos

- `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
```

Flujo: dongle conectado (RNDIS) → udev se activa → `mifi-adb-enable.service` → script activa la interfaz RNDIS, hace curl a `usbdebug.html` → dongle reinicia en modo ADB → reenumeración con la interfaz ADB → la regla udev CT-102 (a continuación) entrega el nodo al contenedor → el `adb` del agente lo ve. En la reenumeración en modo adb, el script se ejecuta nuevamente, detecta la interfaz ADB (`ff/42/01`) y sale — sin bucle.

Cambio de udev de paso USB CT-102 (REQUERIDO)

El VID Qualcomm del dongle `05c6` debe ser entregado al contenedor, y el grupo **debe ser plugdev (gid del host 100046)**, no root del contenedor, o el adb del agente (usuario `omniweb-agent`, un miembro de plugdev) no puede abrir el nodo. Lo mismo se aplica a las reglas del teléfono Android: eran `GROUP="100000"` (root del contenedor) a las que el agente no puede acceder — los dispositivos solo funcionaban mientras adb mantenía el fd desde el tiempo de enumeración y se caían en cada reenumeración. Corregido a `GROUP="100046"`.

En `/etc/udev/rules.d/99-ct102-android.rules`, todas las reglas de teléfonos usan `OWNER="100000", GROUP="100046", MODE="0660"`, además del VID del 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"
```

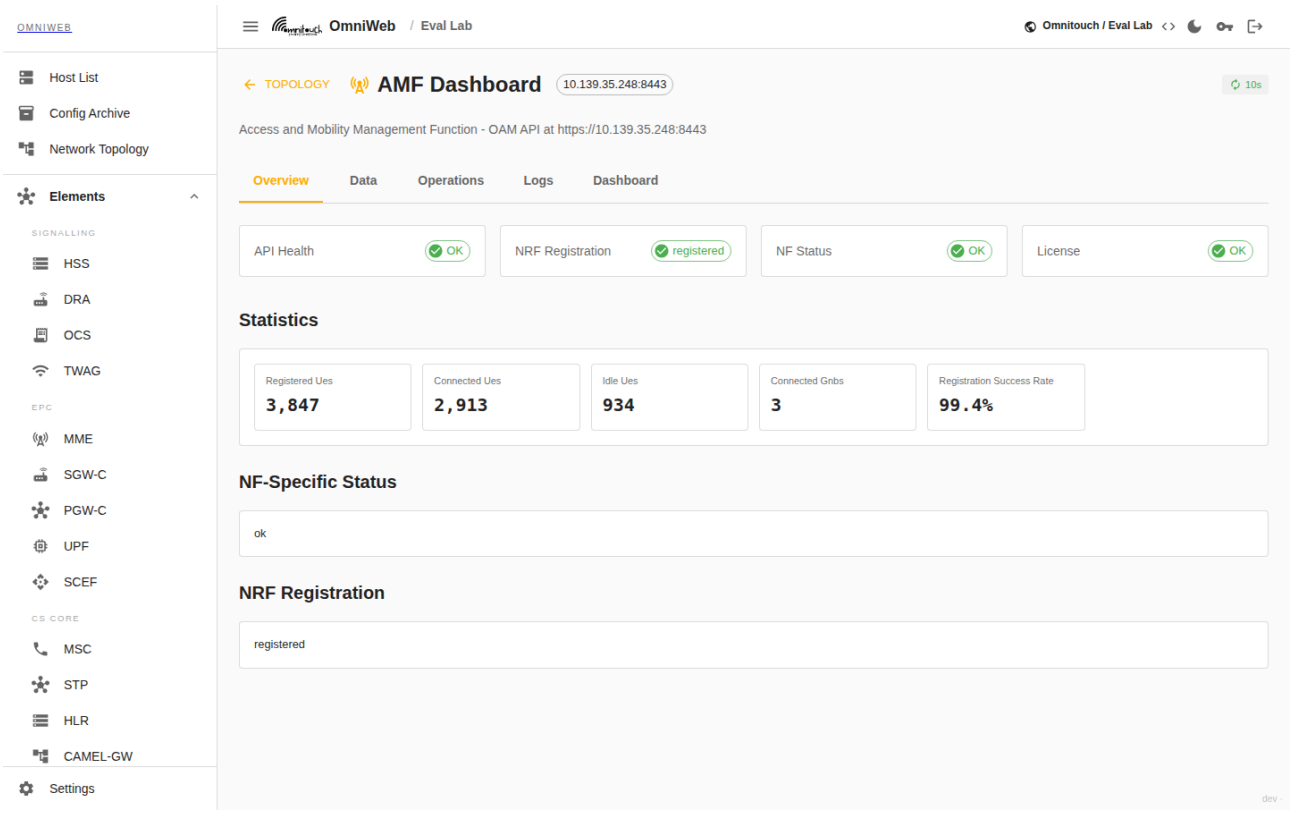
> Estos cambios en el host se aplican en vivo en el laboratorio, pero deben ser codificados en el ansible de OmniCore (rol de monitoreo/host) para que sobrevivan a una reconstrucción del host.

AMF: Función de Gestión de Acceso y Movilidad

El **AMF** es el ancla del plano de control del núcleo 5G. Termina la señalización **N1** hacia el UE y la asociación **N2** (NGAP) a cada gNodeB. Maneja la gestión de registro y conexión: adjunta UEs, los mantiene accesibles y los busca cuando están inactivos. Posee los **contextos de UE** (uno por suscriptor registrado, identificado por SUPI) y las **asociaciones de gNB** (una por radio conectada, identificada por la asociación SCTP). Selecciona el SMF para cada sesión PDU y retransmite solicitudes de sesión entre el UE y el SMF. Cuando un suscriptor está en la red, el AMF es el NF que sabe dónde se encuentra y cómo contactarlo.

← Núcleo 5G

En el panel de control



El panel de control del AMF se abre con las cuatro tarjetas de salud estándar: **Salud de API**, **Registro de NRF** (si el AMF est�? actualmente registrado con el NRF), **Estado de NF**, y **Licencia**. Cada una consulta en un intervalo. Debajo de ellas, muestra los datos que posee el AMF:

- **Lista de UE**: cada contexto de UE que posee el AMF, identificado por SUPI, con su estado de registro y conexión. Esta es la vista de "quién está adjunto en este momento". Seleccione un UE para abrir su contexto detallado. El AMF también puede listar las sesiones PDU activas de un UE por SUPI.
- **gNodeBs**: las radios conectadas, una fila por asociación SCTP. La tabla decodifica los valores NGAP en **gNB-ID**, **TAC** (área de seguimiento), **PLMN**, y **SST** (tipo de corte/servicio) legibles. Un operador puede, por lo tanto, confirmar qué celdas están activas y qué áreas de seguimiento y cortes sirven sin decodificar identificadores manualmente. Seleccione una fila para abrir el gNB detallado por su ID de asociación SCTP.
- **Estadísticas**: los contadores en vivo del AMF (UEs registrados, gNBs conectados y volúmenes de señalización), para una lectura rápida sobre

carga y actividad.

- **Modo de Mantenimiento**: si el AMF está en mantenimiento. Úselo para drenar o mantener un nodo durante trabajos planificados.
- **Configuración**: la configuración en tiempo de ejecución que el servicio está utilizando actualmente.

Acciones

El panel de control expone acciones para recuperarse de un estado atascado. El panel de control confirma cada una antes de ejecutarla, ya que limpian el estado en vivo:

- **Limpiar Todos los Contextos de UE** (masivo): elimina cada contexto de UE del AMF. Úselo como último recurso para recuperar un nodo que tiene contextos obsoletos o corruptos. Cada UE afectado debe volver a registrarse.
- **Limpiar Caché** (masivo): limpia la caché de descubrimiento de NF del AMF y las cachés de UE. Úselo cuando el AMF actúe sobre datos de pares o de búsqueda obsoletos, por ejemplo, después de que un NF se haya movido o re-registrado.
- **Darse de Baja** (por UE): da de baja un solo UE y limpia su estado. Úselo para eliminar el contexto de un suscriptor que no se limpiará por sí solo, en lugar de reiniciar todo el nodo.

Más allá de los botones del panel de control, la API OAM del AMF expone controles de recuperación más detallados que un operador puede alcanzar a través del proxy de backend:

- **Desconectar forzosamente un gNB**: desmantela un solo gNB por su ID de asociación SCTP. Úselo para limpiar una asociación de radio atascada o que no funciona sin afectar a las demás.
- **Liberar forzosamente una sesión PDU**: libera una sesión PDU por su identificador `supi:psi`. Úselo para eliminar una sesión que está atascada del lado del AMF mientras el UE permanece registrado.
- **Darse de baja o buscar un UE**: obliga a un UE a darse de baja, o busca un UE inactivo para volver a conectarlo. Use la búsqueda para probar la

accesibilidad. Use la baja forzada para desalojar un UE de manera limpia.

Operaciones

- **Diagnósticos en tiempo de ejecución** (`/api/oam/diagnostics`): muestra diagnósticos de bajo nivel para el servicio en ejecución.
- **Uso de recursos** (`/api/oam/resources`): informa sobre el uso de memoria, procesos y programador en tiempo de ejecución para una verificación de salud del nodo.
- **Pares** (`/api/oam/peers`): lista las URIs de pares NF configurados y descubiertos y las asociaciones SCTP actuales, para que un operador pueda ver con quién habla el AMF.
- **Caché de descubrimiento de NRF** (`/api/oam/nrf_discovery`): muestra el contenido de la caché de descubrimiento: qué instancias de NF ha aprendido el AMF del NRF.
- **Establecer nivel de registro** (`/api/oam/log_level`): cambia el nivel de registro en tiempo de ejecución (uno de `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar el detalle mientras soluciona problemas.
- **Forzar re-registro de NRF** (`/api/oam/nrf/reregister`): re-registra el AMF con el NRF. Úselo para recuperar un registro caído u obsoleto.

Relacionados

- SMF: Función de Gestión de Sesiones: el AMF selecciona el SMF y retransmite solicitudes de sesión PDU a él.
- UDM: Gestión de Datos Unificada: los datos del suscriptor que el AMF utiliza durante el registro.
- AUSF: Función de Servidor de Autenticación: autentica el UE durante el registro en nombre del AMF.
- NSSF: Función de Selección de Cortes de Red: resuelve la selección de cortes para el AMF.
- ← Núcleo 5G: la visión general de todos los paneles de control de NF.

AUSF: Función del Servidor de Autenticación

El **AUSF** autentica a los suscriptores en nombre del AMF. Cuando un UE se conecta, el AMF pide al AUSF que ejecute 5G-AKA (o EAP-AKA') para ese suscriptor. El AUSF trabaja con el **UDM** para obtener el material clave, deriva la clave de anclaje que devuelve al AMF y confirma el resultado de la autenticación. Mantiene una sesión de autenticación activa para cada autenticación en curso o establecida, de modo que un operador pueda rastrear su progreso y resultado y, si es necesario, finalizarla.

← 5G Core

En el panel de control

El panel de control del AUSF se abre con las tarjetas de salud estándar en la parte superior (**Salud de la API**, **Registro de NRF** (¿está el AUSF registrado con el NRF?), **Estado del NF**, y **Licencia**), cada una sondeando en un intervalo. Debajo de ellas están las secciones de datos del AUSF, leídas en vivo desde su API de OAM a través del proxy de OmniWeb:

- **Estadísticas**: los propios contadores del AUSF (`AUSF Statistics`), que ofrecen una vista en tiempo real de la actividad de autenticación.
- **Sesiones de autenticación activas del AUSF**: la lista de sesiones de autenticación que el AUSF mantiene actualmente (`List Active AUSF Authentication Sessions`). Cada fila está identificada por su identificador de sesión, para que un operador pueda ver de un vistazo qué autenticaciones están en curso o establecidas.

Acciones

Ambas acciones limpian el estado de autenticación y piden confirmación primero, ya que son destructivas:

- **Limpiar una sesión de autenticación específica** (por fila): elimina una única sesión de autenticación por su identificador. Utiliza esto para eliminar una sesión atascada o obsoleta sin perturbar la autenticación de otros suscriptores.
- **Limpiar todas las sesiones de autenticación**: elimina todas las sesiones de autenticación que el AUSF mantiene. Utiliza esto para recuperar el AUSF de un estado atascado generalizado. Cada suscriptor afectado se vuelve a autenticar en su próximo intento.

Operaciones

Controles estándar de OAM disponibles en el AUSF:

- **Diagnósticos** (`/api/oam/diagnostics`): diagnósticos en tiempo de ejecución para el servicio.
- **Recursos** (`/api/oam/resources`): el uso de recursos del servicio.

- **Forzar re-registro de NRF** (`/api/oam/nrf/reregister`): hace que el AUSF se vuelva a registrar con el NRF, para recuperarse si su registro ha quedado obsoleto.

Relacionado

- AMF: Gestión de Acceso y Movilidad: solicita autenticación al AUSF para cada UE que se conecta.
- UDM: Gestión Unificada de Datos: suministra el material clave que el AUSF utiliza para autenticar a un suscriptor.
- ← 5G Core: la visión general del panel de 5GC y los otros NF.

BSF: Función de Soporte de Vinculación

El **BSF** registra y resuelve la vinculación entre la sesión PDU de un UE y el PCF que la atiende. Cuando se establece una sesión, el BSF registra qué PCF está manejando la política para esa sesión, utilizando como clave los identificadores de la sesión: la dirección IP del UE, el DNN y el S-NSSAI. Otros NFs y funciones de aplicación consultan al BSF para descubrir el PCF correcto para una sesión de UE dada, de modo que las solicitudes de política lleguen al PCF que ya tiene el contexto de esa sesión en lugar de a uno arbitrario. El BSF mantiene una vinculación por cada sesión PDU activa y las expone, junto con estadísticas resumidas, para su monitoreo.

← 5G Core

En el panel de control

El panel de control del BSF se abre con las tarjetas de salud estándar en la parte superior (**Salud de API**, **Registro de NRF** (¿está registrado el BSF con el NRF?), **Estado de NF**, y **Licencia**), cada una sondeando en un intervalo. Debajo de ellas están las secciones de datos del BSF, leídas en vivo desde su API de OAM a través del proxy de OmniWeb:

- **Vinculaciones de PCF**: la lista de vinculaciones activas que el BSF mantiene actualmente (`List all PCF bindings with binding ID, UE IP, DNN, S-NSSAI, PCF FQDN/IP`). Cada fila está indexada por su ID de vinculación y muestra la dirección IP del UE, el DNN y el S-NSSAI que identifican la sesión, junto con el FQDN o IP del PCF que la atiende. Esto responde a "¿qué PCF está manejando la política para esta sesión de UE?" de un vistazo. Seleccione una vinculación para abrir su detalle completo (`Get detailed PCF binding by binding ID`).
- **Estadísticas**: los propios contadores del BSF (`BSF statistics: total bindings, bindings by DNN`), que ofrecen una vista continua de cuántas vinculaciones están activas en total y cómo se desglosan por DNN.

Acciones

El panel de control del BSF está orientado a la lectura y monitoreo. Superficies vinculaciones y estadísticas para inspección y no expone acciones destructivas por fila o a nivel de NF.

Operaciones

Controles de OAM estándar disponibles en el BSF:

- **Forzar re-registro de NRF** (`/api/oam/nrf/reregister`): hace que el BSF se re-registre con el NRF, para recuperarse si su registro ha caducado.

Relacionado

- PCF: Control de Políticas: el NF al que apunta cada vinculación. El BSF es cómo los consumidores encuentran el PCF correcto para una sesión de UE.

- SMF: Gestión de Sesiones y funciones de aplicación: consumidores de Nbsf que registran y buscan vinculaciones a medida que las sesiones van y vienen.
- ← 5G Core: la visión general del panel de control de 5GC y los otros NFs.

CHF: Función de Carga

La **CHF** (Función de Carga) proporciona carga convergente en línea y fuera de línea para el núcleo 5G. El SMF la consume a través de la interfaz N40: a medida que las sesiones PDU transportan tráfico, la CHF gestiona las cuotas de uso, tasa ese uso a través del motor de calificación/carga y genera los CDR (Registros de Datos de Carga) que alimentan la facturación y la conciliación. Su panel muestra las sesiones de carga en vivo, la salud del enlace al motor de calificación y el historial de CDR completados. Un operador puede entonces responder "¿se está cobrando correctamente a un suscriptor y es accesible el motor de calificación?" sin salir de OmniWeb.

← Núcleo 5G

En el panel

En la parte superior se encuentran las **tarjetas de salud** estándar (**Salud de API**, **Registro de NRF** (¿está registrada la CHF con el NRF?), **Estado de NF** y

Licencia), cada una sondeando en un intervalo. Debajo de ellas, las secciones de datos específicas de CHF se actualizan automáticamente:

- **Sesiones de carga activas**: las sesiones en vivo que la CHF está midiendo, cada una mostrando su referencia de carga (`chargingDataRef`), el suscriptor (SUPI), el DNN, el uso acumulado y las marcas de tiempo de inicio/actualización. Este es el conjunto de trabajo de "quién se está cobrando en este momento".
- **Estadísticas**: una vista resumida del total de sesiones, conectividad al motor de calificación/carga y volumen total cobrado.
- **Salud de conectividad del motor de calificación**: una verificación de salud dedicada que confirma que la CHF puede alcanzar el motor de calificación/carga que realiza la calificación real. Si esto no es saludable, la CHF no puede calificar sesiones y la carga está en riesgo.
- **Búsqueda de CDR completados**: una vista buscable sobre los CDR finalizados, filtrable por SUPI, DNN y rango de fechas, para confirmar lo que la CHF registró después de que una sesión se cierra.
- **Configuración**: la configuración en tiempo de ejecución de la CHF tal como el servicio la ve actualmente.

Selecciona una sesión para abrir su detalle completo por referencia de datos de carga, que muestra el estado completo de uso y medición para esa sesión.

Acciones

- **Abortar una sesión de carga**: termina una sesión de carga en progreso por su `chargingDataRef`. Usa esto para limpiar una sesión atascada u huérfana que el SMF ya no mantiene, para que deje de consumir cuota y estado de medición.
- **Buscar CDRs**: consulta el historial de CDR completados por SUPI, DNN y rango de fechas. Usa esto después de que una sesión termine para confirmar qué uso la CHF calificó y registró. Soporta consultas de facturación, investigación de disputas o una verificación puntual de que la CHF escribe la carga correctamente.

Operaciones

- **Establecer nivel de registro**: cambia la verbosidad del registro de la CHF en tiempo de ejecución (emergencia, alerta, crítica, error, advertencia, aviso, información, depuración) para recopilar más detalles mientras investigas un problema de carga, luego regresa a la normalidad.
- **Forzar re-registro de NRF**: hace que la CHF se re-registre con el NRF. Úsalo para recuperarte si la CHF ha caído fuera del registro y el SMF ya no puede descubrirla.

Relacionado

- SMF: el consumidor N40 que impulsa la carga a medida que las sesiones PDU transportan tráfico.
- PCF: el lado de políticas del control de políticas y carga que gobierna contra lo que la CHF mide.
- El motor de calificación/carga (OCS): el sistema aguas abajo a través del cual la CHF califica. La tarjeta de salud de conectividad del motor de calificación refleja el enlace a él.
- ← Núcleo 5G: la visión general de todos los paneles de NF.

NRF: Función de Repositorio de Red

Todo el núcleo 5G está construido alrededor del registro **NRF**. Al iniciar, cada NF registra su **perfil NF** con el NRF: su tipo, direcciones, PLMNs, los **servicios** que ofrece, y su capacidad y prioridad. Luego descubre a sus pares preguntando al NRF quién está disponible. El NRF rastrea el **estado** de cada instancia registrada. Mantiene **suscripciones de cambio de estado**, por lo que puede informar a un NF cuando un par del que depende llega o se va. Observa los **latidos** para expirar instancias que dejan de registrarse. Cuando cualquier NF necesita encontrar otro, el NRF es la fuente de verdad sobre lo que está activo y cómo alcanzarlo.

← Núcleo 5G

En el panel de control

El NRF tiene su propio panel de control dedicado, más rico que la página estándar de NF porque posee el registro a través del cual el resto del núcleo descubre. Se abre con las tarjetas de salud estándar: **Salud de API**, **Registro NRF** (si el NRF mismo está registrado), **Estado NF**, y **Licencia**. Cada una consulta en un intervalo.

Sobre los datos, muestra cuatro **tarjetas métricas** que resumen el registro: **Tipos de NF**, **Total de instancias**, **Registradas** (con una barra de porcentaje del total), y **Servicios** (con el conteo de suscripciones). Debajo de ellas están las vistas principales del NRF:

- **Instancias NF registradas**: cada instancia registrada, agrupada por **tipo de NF** (AMF, SMF, UDM, PCF, etc.). El panel codifica por colores cada tarjeta de instancia por tipo. La tarjeta muestra su estado de registro, temporizador de latido, conteo de servicios y PLMN. Selecciona una instancia para abrir su **perfil NF** completo: el registro detallado que mantiene el NRF, con un enlace de **Abrir Panel** a la propia página de ese NF y un botón de **Darse de baja**. Esta es la vista de "¿qué NFs están activos y están todos registrados?".
- **Servicios registrados**: una tabla plana de cada servicio que cada instancia publicita, con sus versiones y estado. Un operador puede ver, por lo tanto, qué capacidades ofrece actualmente el núcleo a través de todos los NFs.
- **Suscripciones**: las suscripciones de cambio de estado NF actualmente mantenidas. Cada una es una solicitud permanente de un NF para ser notificado cuando cambia el estado de un par.
- **Estadísticas**: los contadores en vivo del NRF: total de NFs por tipo, suscripciones y solicitudes de descubrimiento, para una lectura rápida sobre el tamaño del registro y la actividad de búsqueda.

Acciones

El panel de control expone acciones para gestionar el registro. El panel confirma cada una antes de ejecutarla, ya que cambia el estado de registro en vivo:

- **Darse de baja de una instancia NF** (por fila): elimina el registro de una instancia del NRF. Úsalo para limpiar un registro obsoleto o atascado de un solo NF. Ese NF debe volver a registrarse antes de que otros NFs puedan descubrirlo nuevamente.
- **Darse de baja de todos los NFs** (por lotes): elimina todos los registros del NRF a la vez. Úsalo como último recurso para restablecer un registro que contiene entradas obsoletas. Cada NF debe volver a registrarse.
- **Eliminar una suscripción**: elimina una suscripción de cambio de estado. Úsalo para limpiar una suscripción obsoleta u huérfana dejada por un NF que ya no la necesita.
- **Actualizar un perfil NF**: parchea el perfil de una instancia registrada (por ejemplo, su capacidad, prioridad o estado). Los operadores pueden, por lo tanto, ajustar cómo el NRF dirige el descubrimiento hacia o desde una instancia sin necesidad de una baja.

Operaciones

La API OAM del NRF expone controles adicionales a los que un operador puede acceder a través del proxy de backend:

- **Diagnósticos en tiempo de ejecución** (`/api/oam/diagnostics`): muestra diagnósticos de bajo nivel para el servicio en ejecución.
- **Uso de recursos** (`/api/oam/resources`): informa sobre el uso de memoria, procesos y programador del tiempo de ejecución para una verificación de salud del nodo.
- **Verificación manual de latido** (`/api/oam/heartbeat`): activa una verificación de latido a demanda para una instancia NF. Confirma si el NF sigue vivo en lugar de esperar a su temporizador.
- **Tiempo de actividad NF** (`/api/oam/nf_uptime/{id}`): muestra el tiempo de registro de una instancia y cuánto tiempo ha estado registrada, para confirmar cuánto tiempo ha estado activo un NF.
- **Establecer nivel de registro** (`/api/oam/log_level`): cambia el nivel de registro en tiempo de ejecución (uno de `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar el detalle mientras solucionas problemas.

- **Forzar re-registro del NRF** (`/api/oam/nrf/reregister`): vuelve a registrar el NRF. Úsalo para recuperar un registro automático perdido o obsoleto.

Relacionados

- AMF: Función de Gestión de Acceso y Movilidad: se registra con el NRF y descubre a sus pares a través de él, como cada NF a continuación.
- SMF: Función de Gestión de Sesiones: descubierto a través del NRF para la gestión de sesiones.
- UDM: Gestión Unificada de Datos: uno de los NFs de datos de suscriptores para los que el NRF mantiene registros.
- PCF: Función de Control de Políticas: registrado con el NRF para el descubrimiento de políticas.
- SCP: Proxy de Comunicación de Servicios: enruta la señalización entre NFs utilizando los registros y datos de descubrimiento que mantiene el NRF.
- ← Núcleo 5G: la visión general de todos los paneles de control de NF.

NSSF: Función de Selección de Slice de Red

El **NSSF** selecciona la(s) instancia(s) de slice de red y el NSSAI permitido para un UE. Cuando el AMF maneja un registro o una solicitud de slice, solicita al NSSF que resuelva los S-NSSAIs solicitados por el UE en relación con los slices configurados para ese PLMN. El NSSF mapea cada uno a su instancia de slice de red (NSI) y al conjunto de AMF que lo atiende, y devuelve el NSSAI permitido que el UE puede usar. Mantiene las definiciones de slice configuradas y rastrea la disponibilidad de NSSAI por AMF para que un operador pueda razonar y monitorear la selección de slices.

← 5G Core

En el panel de control

El panel de control del NSSF se abre con las tarjetas de salud estándar en la parte superior (**Salud de API**, **Registro de NRF** (¿está el NSSF registrado con el NRF?), **Estado de NF**, y **Licencia**), cada una sondeando en un intervalo. Debajo de ellas están las secciones de datos del NSSF, leídas en vivo desde su API de OAM a través del proxy OmniWeb:

- **Slices**: cada S-NSSAI configurado, listado con sus mapeos de NSI, los conjuntos de AMF que lo atienden, y el NSSAI permitido por PLMN (`List all configured S-NSSAIs with NSI mappings, AMF sets, and allowed NSSAI per PLMN`). Esta es la vista autoritativa de cómo los slices solicitados se resuelven en instancias de slice y conjuntos de AMF para cada PLMN.
- **Disponibilidad de NSSAI**: el estado de disponibilidad de NSSAI por AMF (`Per-AMF NSSAI availability state`), que muestra qué slices cada AMF ha informado que puede atender actualmente.
- **Estadísticas**: los propios contadores del NSSF (`NSSF statistics: total slices, NS selection request counts`), que dan una vista continua del número de slices configurados y del volumen de solicitudes de selección de slices.

Una vista de **configuración de slice** separada (`Query Slice Configuration`) muestra la configuración de slice en tiempo de ejecución del NSSF para referencia.

Acciones

El panel de control del NSSF está orientado a la lectura y monitoreo. Muestra slices, disponibilidad de NSSAI y estadísticas sin acciones de control por ítem.

Operaciones

Los controles de OAM que expone el NSSF son:

- **Ver configuración en tiempo de ejecución** (`/api/oam/config`): la configuración en vivo del NSSF en tiempo de ejecución.
- **Forzar re-registro de NRF** (`/api/oam/nrf/reregister`): hace que el NSSF se re-registre con el NRF, para recuperarse si su registro ha

caducado.

Relacionados

- AMF: Gestión de Acceso y Movilidad: consulta al NSSF para resolver S-NSSAIs solicitados en el NSSAI permitido y el conjunto de AMF que atiende a un UE.
- NRF: Función de Repositorio de Red: donde el NSSF se registra para que otros NFs puedan descubrirlo.
- ← 5G Core: la visión general del panel de control de 5GC y los otros NFs.

PCF: Función de Control de Políticas

El **PCF** toma las decisiones de políticas que el resto del núcleo 5G aplica. Responde al AMF a través de N15 para la **política de acceso y movilidad (AM)**: las restricciones de movilidad y RFSP que un UE recibe al registrarse. Responde al SMF a través de N7 para la **política de gestión de sesiones (SM)**: las reglas PCC que establecen la QoS de cada sesión, control de acceso, control de cobro y monitoreo de uso. El PCF vincula las asociaciones de políticas SM de un UE de vuelta a sí mismo a través del BSF, de modo que cualquier NF pueda encontrar el PCF adecuado para una sesión. El panel de control del PCF es el lugar para responder "¿qué políticas están activas, para qué UEs y sesiones, y son lo que espero?" sin salir de OmniWeb. Cada respuesta de OAM está envuelta en `{status, response}`, y el panel de control la desenrolla por ti.

← Núcleo 5G

En el panel de control

En la parte superior se encuentran las cuatro tarjetas de salud estándar (**Salud de API**, **Registro de NRF** (¿está el PCF registrado con el NRF?), **Estado de NF**, y **Licencia**), cada una sondeando en un intervalo. Usa el indicador de sondeo en el encabezado para pausar la actualización o leer la hora de la última actualización. Debajo de las tarjetas está la barra de **Acciones** (ver más abajo), luego las secciones de datos del PCF, cada una actualizándose automáticamente.

Estadísticas: los contadores en vivo del PCF (`GET /api/statistics`), los totales de asociación de políticas y los conteos actuales. Esta es la lectura más rápida sobre si el PCF está sirviendo activamente políticas AM y SM.

Políticas AM: cada asociación de política AM activa (`GET /api/am_policy`), una fila por UE para el que el AMF tiene una política AM. Esta es la vista del PCF de la política de movilidad actualmente aplicada a cada UE registrado.

Políticas SM: cada asociación de política SM activa (`GET /api/sm_policy`), una fila por sesión PDU para la que el SMF tiene una política. Selecciona una fila para abrir su detalle (`GET /api/sm_policy/{id}`), que devuelve las reglas

PCC completas sobre esa sesión: las decisiones de QoS, control de acceso, cobro y monitoreo de uso que el SMF aplica.

Contexto de Políticas: la vista de contextos de políticas activas (`GET /api/policy_context`), los contextos que el PCF mantiene a través de sus asociaciones AM y SM. Es útil para reconciliar lo que el PCF cree que está activo frente al AMF y SMF.

Configuración: la configuración de tiempo de ejecución del PCF (`GET /api/oam/config`), los ajustes con los que el servicio se está ejecutando actualmente.

Acciones

Cada acción por fila solicita confirmación primero, ya que eliminar una asociación activa es disruptivo para el UE o la sesión que afecta.

Eliminar una política AM: en cualquier fila de Políticas AM, **Eliminar** borra esa asociación de política AM (`DELETE /api/am_policy/{id}`). Úsalo para limpiar una política de movilidad atascada o obsoleta para un UE.

Eliminar una política SM: en cualquier fila de Políticas SM, **Eliminar** borra esa asociación de política SM (`DELETE /api/sm_policy/{id}`). Úsalo para eliminar la política de una sesión que no se despejará por sí sola.

Actualizar una política SM: también puedes editar una asociación de política SM. Envía `PATCH` o `PUT /api/oam/sm_policy/{id}` para actualizar las reglas PCC en una política SM activa, de modo que puedas ajustar las decisiones de QoS o cobro de una sesión sin deshacer la asociación. Úsalo para reimpulsar la política en una sesión existente en lugar de eliminarla y recrearla.

Operaciones

La sección de Operaciones lleva los controles comunes a cada NF:

- **Diagnósticos** (`GET /api/oam/diagnostics`): diagnósticos en tiempo de ejecución para el servicio.

- **Uso de recursos** (`GET /api/oam/resources`): memoria, procesos y programadores del servicio en ejecución.
- **Pares** (`GET /api/oam/peers`): los URIs de pares NF configurados con los que el PCF se comunica y su estado de alcanzabilidad.
- **Cache de descubrimiento de NRF** (`GET /api/oam/nrf_discovery`): la caché de descubrimiento de NRF, o los URIs de NF configurados a través de los cuales el PCF resuelve pares.
- **Nivel de registro** (`POST /api/oam/log_level`): cambiar el nivel de registro en tiempo de ejecución. Elige uno de emergencia, alerta, crítico, error, advertencia, aviso, información o depuración.
- **Re-registro de NRF** (`POST /api/oam/nrf/reregister`): forzar al PCF a re-registrarse con el NRF, por ejemplo, después de que un reinicio de NRF lo dejó obsoleto.

Relacionados

- SMF: solicita política SM del PCF a través de N7 y aplica las reglas PCC que el PCF devuelve.
- AMF: solicita política AM del PCF a través de N15.
- BSF: la función de vinculación con la que el PCF registra asociaciones de políticas SM para que cualquier NF pueda encontrar el PCF que sirve.
- CHF: la función de cobro. Las decisiones de control de cobro del PCF impulsan lo que el SMF informa a través de N40.
- ← visión general del Núcleo 5G

SCP: Proxy de Comunicación de Servicio

El **SCP** se sitúa entre las funciones de red del núcleo 5G y transporta su tráfico basado en servicios. En lugar de que cada NF consumidor se conecte directamente a cada productor, las solicitudes pueden ser enrutadas a través del SCP, que reenvía cada mensaje a una instancia saludable del tipo de NF objetivo, equilibrando la carga entre instancias y reintentando en caso de fallos. Puede realizar descubrimiento en nombre de un consumidor (descubrimiento delegado) y almacena en caché la accesibilidad de NF para que, una vez que conoce un tipo objetivo, dirija solicitudes posteriores sin una nueva búsqueda. El resultado es comunicación indirecta: los productores y consumidores no necesitan conocerse ni mantener conexiones entre sí, y el SCP maneja el enrutamiento, el equilibrio y la frescura de la caché en medio.

← Núcleo 5G

En el panel de control

El panel de control del SCP sigue el mismo diseño que cada página de NF del 5GC. Cuatro **tarjetas de salud** se encuentran en la parte superior (**Salud de API**, **Registro de NRF** (¿está el SCP registrado con el NRF?), **Estado de NF**, y **Licencia**), cada una sondeando en un intervalo.

Debajo de las tarjetas, el SCP muestra sus propios datos operativos:

- **Salud de NF**: la vista del equilibrador de carga de los NFs a los que hace proxy, con conteos de salud y fallos por instancia, para que un operador pueda ver qué instancias de productores el SCP considera alcanzables y cuáles están fallando.
- **Caché de Descubrimiento**: el contenido de la caché de descubrimiento del SCP, qué tipos de NF están en caché, sus TTLs, y las tasas de aciertos/fallos de la caché. Esto es lo que permite al SCP dirigir solicitudes repetidas sin un redescubrimiento.
- **Estadísticas**: rendimiento del SCP, total de solicitudes proxy, un desglose de solicitudes por tipo de NF objetivo, y la tasa de aciertos de la caché en general.

- **Configuración**: la configuración de tiempo de ejecución actual del SCP.

Cada sección se actualiza automáticamente, y los valores de tipo de NF están interconectados con el propio panel de control de ese NF.

Acciones

El panel de control del SCP no expone botones de acción destructivos a nivel de NF o por fila. Hace proxy del tráfico en lugar de poseer el estado de sesión o suscriptor que un operador podría limpiar. Sin embargo, su caché es manejable: la API OAM permite a un operador ver la caché de descubrimiento y expulsar una única entrada obsoleta para que el SCP redescubra ese objetivo en la siguiente solicitud (ver **Operaciones**). Para recuperarse de un productor que se ha movido o ha sido reemplazado pero que aún está en caché como alcanzable, limpie su entrada.

Operaciones

La API OAM del SCP expone los siguientes controles:

- **Ver / gestionar caché de descubrimiento**: leer la caché de descubrimiento actual y eliminar una entrada de caché individual por id para forzar el redescubrimiento de ese objetivo.
- **Ver configuración de tiempo de ejecución**: leer la configuración en vivo del SCP.
- **Establecer nivel de registro**: cambiar la verbosidad del registro en tiempo de ejecución. Elija uno de `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, o `debug`.
- **Forzar re-registro de NRF**: hacer que el SCP se re-registre con el NRF. Esto es útil después de que el NRF o el SCP se haya reiniciado y el registro se haya vuelto obsoleto.

Relacionados

- NRF: el registro a través del cual el SCP descubre y se re-registra.

- AMF, SMF, UDM, AUSF, PCF, CHF, NSSF, BSF: los NFs cuyo tráfico basado en servicios el SCP puede hacer proxy y cuya accesibilidad almacena en caché.
- ← Núcleo 5G: la visión general de la sección 5GC y el diseño de panel de control compartido.

SMF: Función de Gestión de Sesiones

El **SMF** posee la sesión PDU. Establece, modifica y libera la sesión de datos de cada UE, asigna a la UE su dirección IP de un grupo local y gestiona el plano de usuario a través de N4/PFCP. Programa el UPF con las reglas de detección de paquetes, reenvío y QoS para cada sesión. También se comunica con el PCF (N7) para la política de sesión y con el CHF (N40) para la facturación. Utiliza el panel de SMF para responder "¿están surgiendo sesiones, está el SMF todavía asociado con su UPF y se está quedando sin direcciones?" sin salir de OmniWeb. El SMF envuelve cada respuesta de OAM `{status, response}`. El panel lo desenrolla por ti.

← Núcleo 5G

En el panel

En la parte superior se encuentran las cuatro tarjetas de salud estándar: **Salud de API**, **Registro de NRF** (¿está el SMF registrado con el NRF?), **Estado de NF** y **Licencia**. Cada una consulta en un intervalo. Utiliza el indicador de sondeo en el encabezado para pausar la actualización o leer la hora de la última actualización. Debajo de las tarjetas se encuentra la barra de **Acciones** (ver más abajo). Luego vienen las secciones de datos del SMF, cada una actualizándose automáticamente.

Estadísticas: los contadores en vivo del SMF (`GET /api/statistics`): totales de establecimiento / modificación / liberación de sesiones y conteos de sesiones actuales. Esta es la lectura más rápida para saber si el SMF realmente establece sesiones.

Sesiones PDU: cada sesión PDU activa (`GET /api/pdu_session`), devuelta como `{ pdu_sessions: [...], total }`. Cada fila lleva tanto un `sm_context_ref` (un UUID que identifica de manera única el contexto SM) como un `pdu_session_id` (el PSI de 3GPP, un pequeño entero que **no** es único entre UEs, ya que cada UE numera sus propias sesiones desde una base baja). Cada operación por sesión (búsqueda de detalles y liberación) se basa, por lo tanto, en `sm_context_ref`. La acción de **Liberar** por fila del panel pasa ese UUID en lugar del PSI. Junto a los identificadores, una fila muestra el DNN de la sesión, la IP de UE asignada y el estado.

Grupo de IP: el grupo de direcciones del que el SMF asigna IPs a las UEs (`GET /api/ip_pool/detail`): el resumen del grupo (subred, total, conteos asignados y disponibles) más la lista de IPs actualmente asignadas. Aquí puedes ver si el SMF está cerca de agotar su espacio de direcciones.

Asociación de UPF: el estado del enlace N4/PFCP al plano de usuario (`GET /api/upf`): si el SMF está actualmente asociado con su UPF. Si las sesiones no logran establecerse, verifica esto primero.

Pares PFCP: el estado de asociación del par PFCP (UPF) (`GET /api/oam/pfcp_peers`): la vista del SMF de cada UPF con el que se asocia a través de N4, incluyendo el estado de asociación.

Acciones

Cada acción solicita confirmación primero. Varias son destructivas para sesiones activas.

Liberar Todas las Sesiones PDU: desmantela cada sesión PDU y su estado PFCP en el UPF. Utilízalo para limpiar el SMF y volver a un estado limpio, por ejemplo, después de un intercambio de UPF o cuando drenas un nodo para mantenimiento.

Limpiar Caché: limpia las cachés de sesión del SMF sin liberar una sesión. Utilízalo cuando el panel o la vista interna del SMF parezcan obsoletos o inconsistentes con la realidad.

Reasociar PFCP: restablece la asociación PFCP con el UPF (iniciado por el SMF). Utilízalo cuando la asociación de UPF se haya perdido y no se puedan establecer nuevas sesiones.

Re-asociar UPF: fuerza una reasociación PFCP con el UPF **configurado**. La dirección del UPF está impulsada por la configuración. No hay acción de agregar-UPF o inyectar-UPF aquí. Esto vuelve a dirigir la asociación al UPF ya en la configuración del SMF. En la práctica, sirve al mismo propósito de recuperación que Reasociar PFCP.

Liberar por DNN: escribe un DNN en el campo editable **DNN** (por ejemplo, `internet`). Esto libera **todas** las sesiones en ese DNN. Utilízalo para drenar o restablecer una única red de datos, por ejemplo, para forzar a las UEs a salir de un APN/DNN, sin afectar las sesiones en otros DNNs.

Liberación por fila: en cualquier fila de Sesiones PDU, **Liberar** desmantela esa sesión y su contexto PFCP en el UPF. Libera por `sm_context_ref`, por lo que siempre apunta exactamente a la sesión en esa fila, aunque varias UEs puedan compartir el mismo `pdu_session_id`. Utilízalo para eliminar una única sesión atascada.

Operaciones

La sección de Operaciones lleva los controles comunes a cada NF:

- **Diagnósticos** (`GET /api/oam/diagnostics`): diagnósticos en tiempo de ejecución para el servicio.
- **Uso de recursos** (`GET /api/oam/resources`): memoria, procesos y programadores del servicio en ejecución.
- **Pares** (`GET /api/oam/peers`): las URIs de pares NF configuradas con las que el SMF se comunica (AMF, PCF, CHF, NRF y sus pares UPF PFCP a través de los Pares PFCP arriba).
- **Nivel de registro** (`POST /api/oam/log_level`): cambia el nivel de registro en tiempo de ejecución. Elige uno de emergencia, alerta, crítico, error, advertencia, aviso, información o depuración.
- **Re-registro de NRF** (`POST /api/oam/nrf/reregister`): fuerza al SMF a re-registrarse con el NRF, por ejemplo, después de que un reinicio del NRF lo dejó obsoleto.

Relacionados

- AMF: solicita la configuración de sesión al SMF a través de Nsmf.
- PCF: suministra la política de sesión al SMF a través de N7.
- CHF: la función de facturación a la que el SMF reporta el uso a través de N40.
- UPF: el par N4/PFCP del SMF. Es el plano de usuario que el SMF programa y asocia.
- ← visión general del Núcleo 5G

UDM: Gestión Unificada de Datos

El **UDM** es la autoridad de datos de suscripción del núcleo 5G. Gestiona los perfiles de suscripción de cada suscriptor. Realiza un seguimiento de qué NFs de servicio manejan cada UE y registra el AMF y SMF contra un suscriptor. Proporciona los datos de autenticación utilizados para desafiar a la UE. Lee los registros subyacentes de suscripción del **UDR**, su almacenamiento de respaldo, y los almacena en caché para una búsqueda rápida. El **AMF** lo consulta durante el registro. El **SMF** lo consulta durante la configuración de la sesión. El **AUSF** obtiene su material de autenticación de él. Cuando otro NF necesita conocer el perfil de un suscriptor o dónde la red lo atiende, el UDM es el NF que responde.

← Núcleo 5G

En el panel de control

El panel de control del UDM se abre con las cuatro tarjetas de salud estándar: **Salud de API**, **Registro de NRF** (si el UDM está actualmente registrado con el NRF), **Estado de NF**, y **Licencia**. Cada una consulta en un intervalo. Debajo de ellas, muestra los datos que posee el UDM:

- **Lista de UE**: cada contexto de UE que el UDM tiene, indexado por SUPI. Esta es la vista de "qué suscriptores está atendiendo actualmente el UDM". El UDM también puede devolver un contexto detallado para un solo suscriptor por SUPI. Muestra las registraciones de NF de servicio de ese suscriptor y los datos de suscripción en caché.
- **Estadísticas**: los contadores en vivo del UDM, para una lectura rápida sobre carga y actividad.
- **Configuración**: la configuración en tiempo de ejecución que el servicio está utilizando actualmente.

Acciones

El panel de control expone acciones para limpiar los datos de suscriptores en caché. El panel de control confirma cada una antes de ejecutarla, ya que elimina el estado en vivo:

- **Limpiar Caché de Suscriptor** (por lotes): limpia toda la caché de datos de suscriptores. Úselo cuando el UDM atienda perfiles obsoletos, por ejemplo, después de que los registros de suscripción hayan cambiado en el UDR y el UDM deba volver a leerlos en lugar de servir sus copias en caché.

Más allá del botón del panel de control, la API OAM del UDM expone un control más detallado al que un operador puede acceder a través del proxy de backend:

- **Purgar la caché de un UE** (`/api/oam/ue_cache/{id}`): elimina los datos de suscripción en caché para un solo suscriptor por SUPI. Úselo para forzar una nueva lectura para un suscriptor cuyo perfil ha cambiado, en lugar de limpiar la caché para todos.

Operaciones

- **Diagnósticos en tiempo de ejecución** (`/api/oam/diagnostics`): muestra diagnósticos de bajo nivel para el servicio en ejecución.
- **Uso de recursos** (`/api/oam/resources`): informa el uso de memoria, procesos y programador en tiempo de ejecución para una verificación de salud en el nodo.
- **Establecer nivel de registro** (`/api/oam/log_level`): cambia el nivel de registro en tiempo de ejecución (uno de `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) para aumentar el detalle mientras soluciona problemas.
- **Forzar re-registro de NRF** (`/api/oam/nrf/reregister`): vuelve a registrar el UDM con el NRF. Úselo para recuperar un registro caído u obsoleto.

Relacionados

- UDR: Repositorio de Datos Unificado: el almacenamiento de respaldo del que el UDM lee los registros de suscriptores.
- AUSF: Función de Servidor de Autenticación: obtiene su material de autenticación del UDM.
- AMF: Función de Gestión de Acceso y Movilidad: consulta al UDM durante el registro y se registra como un NF de servicio.
- SMF: Función de Gestión de Sesiones: consulta al UDM durante la configuración de la sesión y se registra como un NF de servicio.
- ← Núcleo 5G: la visión general de todos los paneles de control de NF.

UDR: Repositorio de Datos Unificado

El **UDR** es el almacenamiento persistente de datos de suscripción, políticas y aplicaciones que se encuentra detrás del UDM y PCF. Donde el UDM y PCF son las funciones de red de front-end con las que se comunican otras NFs, el UDR es la base de datos que leen y escriben. Es la única fuente de verdad sobre quién es un suscriptor y a qué tiene derecho. En el núcleo de Omnitouch, el UDR comparte su almacenamiento de suscriptores con el **HSS**, por lo que un repositorio unificado alberga suscriptores de 4G y 5G en lugar de dos bases de datos paralelas.

← Núcleo 5G

En el panel de control

El panel de control del UDR se abre con las tarjetas de salud de NF estándar en la parte superior (**Salud de API**, **Registro de NRF** (¿está el UDR registrado con el NRF?), **Estado de NF**, y **Licencia**), cada una sondeando en un intervalo.

Debajo de las tarjetas están las dos secciones de datos específicas del UDR:

- **Salud del HSS**: una verificación de salud de conectividad que confirma que el UDR puede alcanzar el almacenamiento de suscriptores compartido del HSS que representa. Esto responde a "¿es la base de datos de suscriptores accesible y saludable?" de un vistazo.
- **Suscriptores**: la lista de suscriptores extraída del HSS, paginada y buscable por **IMSI**. Seleccione un suscriptor para devolver el detalle completo del suscriptor para ese IMSI, de modo que un operador pueda confirmar la provisión de un suscriptor sin salir de OmniWeb.

Acciones

El panel de control del UDR no expone acciones destructivas a nivel de NF o por fila. Es una vista de lectura y búsqueda sobre el almacenamiento de suscriptores compartido. Su valor radica en la interrogación: verifique que el almacenamiento sea accesible a través de la sección de salud del HSS, liste suscriptores y profundice en el detalle completo de cualquier suscriptor por IMSI.

Operaciones

Junto a las secciones de datos, el UDR lleva las operaciones comunes a cada función de red 5GC:

- **Establecer nivel de registro**: aumentar o disminuir la verbosidad del registro en tiempo de ejecución (`emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) a través de `/api/oam/log_level`, para aumentar el detalle mientras diagnostica un problema.
- **Forzar re-registro de NRF**: empujar al UDR a re-registrarse con el NRF (`/api/oam/nrf/reregister`) si su registro ha caducado.

- **Ver configuración en tiempo de ejecución**: inspeccionar la configuración en vivo del UDR a través del endpoint de configuración OAM.

Relacionados

- UDM: Gestión de Datos Unificada: la función de red de front-end que sirve datos de suscripción desde este almacenamiento.
- PCF: Función de Control de Políticas: lee los datos de políticas almacenados en el UDR.
- HSS: la base de datos de suscriptores compartida con la que se unifica el UDR, por lo que los suscriptores de 4G y 5G viven en un solo repositorio.
- ← Núcleo 5G: la visión general completa del panel de control 5GC.

Referencia de API (OpenAPI / Swagger)

El controlador de OmniWeb (backend central) expone una única API REST detrás del mismo inicio de sesión JWT que rige el resto del portal. Esa API es autocomunicante:

- **Swagger UI:** `/api/docs`. Navega por cada endpoint. Expande una ruta para ver su método, parámetros de ruta/query, si necesita un token y su resumen. Haz clic en **Authorize** y pega un JWT de portador para probar llamadas en vivo contra la instancia en ejecución.
- **Especificación OpenAPI 3:** `/api/openapi.json`. Este es el documento legible por máquina. Úsalo para importar en Postman/Insomnia o para generar clientes.

← Volver a la Guía de Operaciones

Qué está documentado

La especificación es **generada en tiempo de ejecución** al introspectar el mapa de rutas en vivo, por lo que siempre coincide con los endpoints que la instancia en ejecución realmente sirve. Ningún archivo mantenido a mano puede desviarse. Para cada ruta captura:

- el método HTTP y la ruta (con parámetros de ruta/query),
- un resumen y descripción tomados del código,
- si se requiere un **JWT de portador**, y
- donde sea aplicable, el permiso **view/control** por elemento que la ruta impone.

Los endpoints están agrupados por área (Auth, Admin, SIM Bank, Remote SIM, APDU, Test Devices, IR.38, RAEX, TAP, etc.) para que puedas encontrar rápidamente las rutas de una función.

Obtención de un token

La mayoría de los endpoints requieren un token de portador. Obtén uno con `POST /api/auth/login` (las mismas credenciales que usas para el portal), luego envíalo como `Authorization: Bearer <token>`. En Swagger UI, usa el botón **Authorize** para que cada llamada "Try it out" lleve automáticamente el token.

Alcance

Esto documenta solo la API del **controlador**. El agente del dispositivo que se ejecuta en sitios remotos no es parte de esta API: se conecta *saliente* al controlador a través de un WebSocket y no expone ningún endpoint REST entrante, por lo que no hay nada que llamar en él directamente.

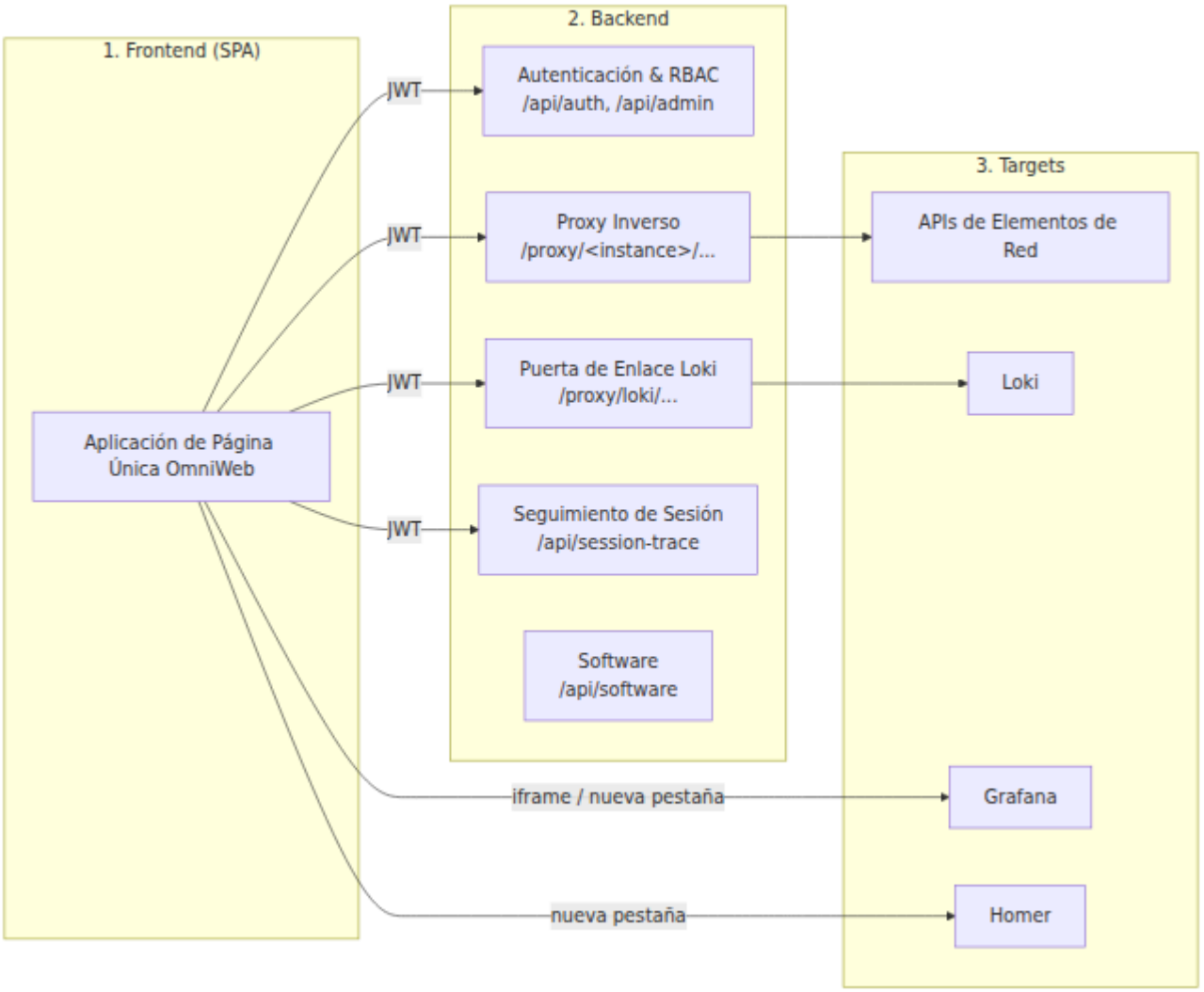
Arquitectura de OmniWeb

Esta página explica cómo está compuesto OmniWeb y cómo una única sesión de navegador alcanza cada función de red, Grafana y Loki. Si solo lees una página para entender el sistema, lee esta.

← Volver a la Guía de Operaciones

Componentes

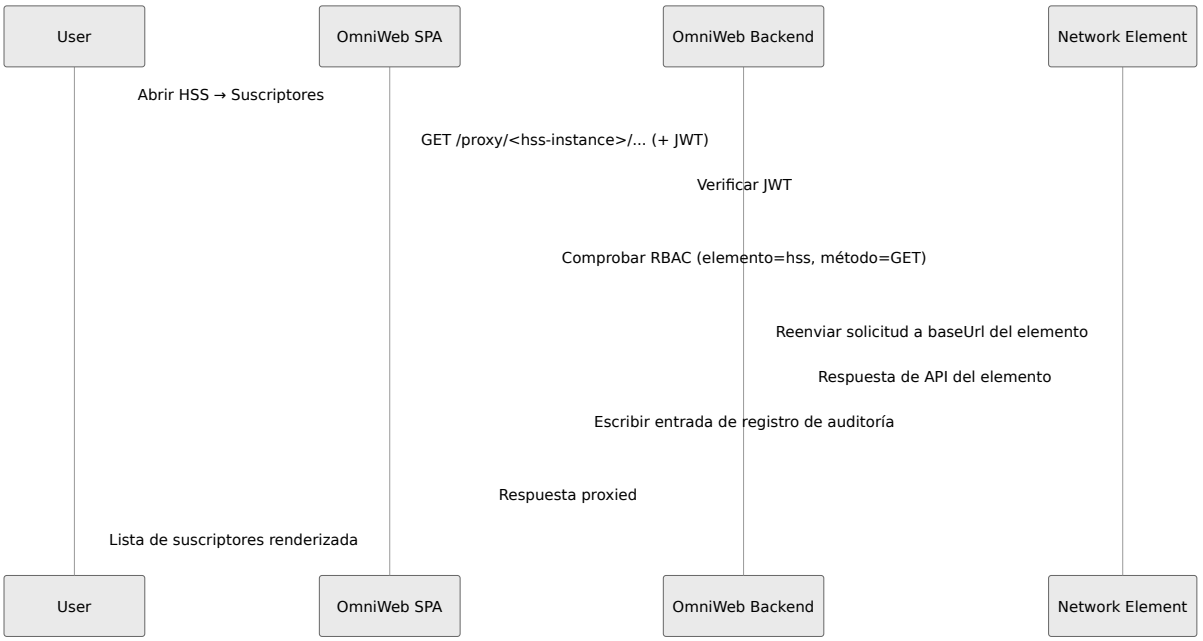
OmniWeb tiene tres partes móviles:



Componente	Rol
Frontend SPA	La interfaz de usuario. Una aplicación web de una sola página que renderiza páginas de elementos, topología, registros, trazas y paneles integrados.
Backend	La capa de seguridad e integración. Autentica a los usuarios, aplica RBAC y hace proxy inverso a cada solicitud al API de elemento correcto, Loki o Grafana.
Targets	Las cosas que se gestionan y observan: las propias APIs de gestión de los elementos de red, además de Grafana, Loki y Homer.

Flujo de Solicitudes

Cada solicitud operativa sigue el mismo camino. Nada en el navegador habla directamente con un elemento. Siempre pasa por el backend para que la autenticación, autorización y auditoría se apliquen de manera centralizada.



El camino del proxy codifica el **ID de instancia**, por lo que OmniWeb puede gestionar muchas instancias del mismo tipo de elemento (por ejemplo, varios nodos HSS) y dirigir cada solicitud al backend correcto.

El Modelo de Configuración

OmniWeb es **impulsado por configuración**. El conjunto de elementos, sus instancias y dónde viven sus APIs se declara en un único archivo: `public/config/omniweb.json`. El backend lo carga al inicio y el frontend lo utiliza para construir la barra lateral, la topología y los objetivos de proxy.

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

Parámetro	Tipo	Requerido	Predeterminado	D
`type`	String	Sí	-	Tip ele De mó ren ele tip
`displayName`	String	Sí	-	No por se bar top
`description`	String	No	-	De lar mu too de
`instances`	Lista	Sí	-	Un no de par ins cor
`defaults.pollIntervalMs`	Entero	No	5000	Co fre act aut las ope mil

Parámetro	Tipo	Requerido	Predeterminado	D
`defaults.timeoutMs`	Entero	No	10000	Tie esp par ele API eje util ma

Parámetros de instancia:

Parámetro	Tipo	Requerido	Predeterminado	Descripción
`id`	String	Sí	-	Identificador único de la instancia. Se utiliza en URLs (`/hss/<id>`) y en l ruta del proxy (`/proxy/<id>/...`
`name`	String	Sí	-	Nombre de visualización para la instancia.
`baseUrl`	String	Sí	-	La URL base de la API de gestión del elemento. El proxy reenvía solicitudes aquí. Se acepta TL autofirmado.
`tags`	Lista	No	`[]`	Etiquetas de forma libre (por ejemplo, `primary`, `geo-redundant`) mostradas como chips.

Tipos de Elementos Soportados

`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 se mapea a un módulo de UI con su propio conjunto de pestañas, pero todos se operan a través de los mismos patrones genéricos. Ver Operaciones Comunes.

Cómo OmniWeb Habla con Cada NF

El proxy del backend es agnóstico al elemento. Reenvía lo que el módulo de frontend solicita a la `baseUrl` del elemento. La *forma* de esas llamadas depende de la API nativa del elemento:

Estilo de API	Elementos	Notas
API de Elemento	Todas las funciones de red	La propia API de gestión del elemento, proxied literalmente bajo `/proxy/<instance-id>/...`. OmniWeb reenvía `GET`/`POST`/`PUT`/`PATCH`/`DELETE` como el elemento espera; la forma de solicitud/respuesta es la que ese elemento define.
Consulta de registro (LogQL)	Todos (pestaña de Registros)	Enrutado a través de `/proxy/loki/...` a Loki. Ver Registros & Trazado.

Debido a que todo está proxied, agregar una instancia es puramente un cambio de configuración en `omniweb.json`. No se requiere ningún cambio de código para gestionar otro nodo.

Referencia de API (OpenAPI)

Un documento consolidado de OpenAPI/Swagger (`swagger-doc.json`) se envía con OmniWeb y describe los esquemas de backend y de elementos (por ejemplo, registros de frontend de SMSC y ubicaciones de suscriptores IMS). Es un artefacto de referencia en lugar de un servidor API en vivo.

Tiempos de Espera del Proxy

Cada tipo de elemento tiene un tiempo de espera de proxy configurable (`defaults.timeoutMs`). La mayoría de los elementos responden bien dentro del predeterminado de 10 segundos. Los elementos con consultas más pesadas tienen más margen:

Elemento	Tiempo de Espera Predeterminado	Por Qué
La mayoría de los elementos	10 segundos	Tiempo de respuesta estándar de API
OCS	180 segundos	Consultas de calificación/CDR sobre grandes conjuntos de datos

Integración de Monitoreo

OmniWeb no reimplementa Grafana, Loki o Homer. Los integra para que un solo inicio de sesión abarque toda la pila:

- **Grafana** se sirve detrás de la puerta de enlace autenticada y se incrusta como un iframe. Cada solicitud se autoriza contra tu inicio de sesión de OmniWeb, por lo que no hay una segunda contraseña. Ver Grafana.
- **Loki** se accede a través de la puerta de enlace `/proxy/loki/*` del backend, que ejecuta consultas LogQL en nombre del operador. Ver Registros & Trazado.
- **Homer** (captura SIP) se detecta automáticamente al inicio (`/api/homer/status`) y, cuando está presente, se abre en una nueva pestaña. También se autoriza contra tu inicio de sesión de OmniWeb.

Referencia de Entorno

Los puntos finales de integración del backend se configuran a través de variables de entorno:

Variable	Predeterminado	Descripción
`GRAFANA_URL`	`http://localhost:3000`	URL base de la instancia de Grafana a la que OmniWeb hace proxy.
`LOKI_URL`	`http://localhost:3100`	URL base de la instancia de Loki utilizada para registros y trazado.
`LDAP_URI`	`ldap://localhost:389`	Servidor OpenLDAP para sincronización de usuario/clave SSH (opcional).
`LDAP_BASE_DN`	`dc=omniweb,dc=local`	DN base de LDAP.
`LDAP_ADMIN_DN`	`cn=admin,dc=omniweb,dc=local`	DN de enlace para escrituras LDAP.
`LDAP_ADMIN_PASSWORD`	`omniweb-admin`	Contraseña de enlace LDAP (cambia esto).
`AUDIT_API_KEY`	`omniweb-audit-key`	Secreto compartido para callbacks de auditoría de inicio de sesión

Variable	Predeterminado	Descripción
		SSH (cambia esto).

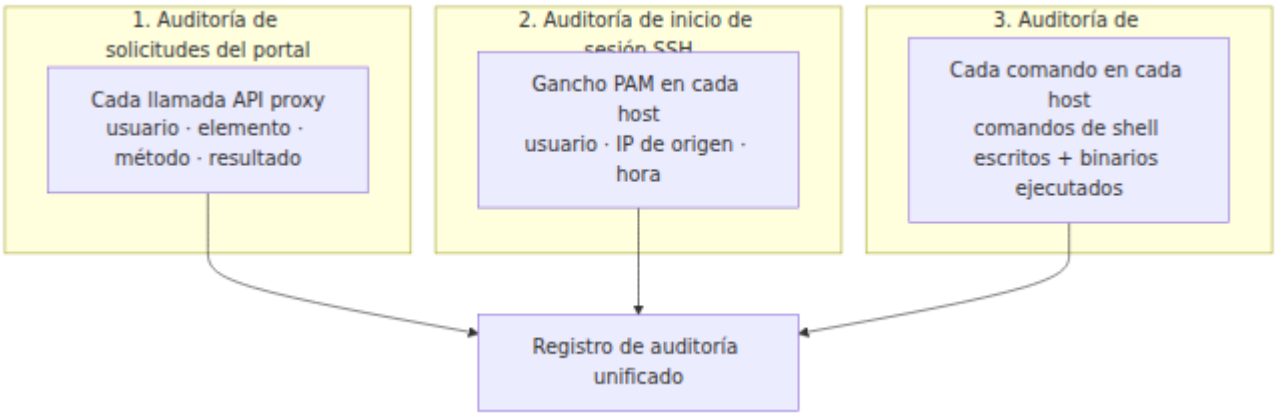
Ver Autenticación & Control de Acceso para los detalles de LDAP/SSH y auditoría.

Registro de Auditoría

Debido a que OmniWeb es la única puerta de enlace a la red, también es el único lugar donde se puede registrar la actividad. La auditoría en OmniWeb tiene **tres capas** que juntas responden "quién hizo qué, dónde" tanto en el portal como en los hosts que gestiona.

← Autenticación y Control de Acceso · ← Guía de Operaciones

Las Tres Capas



Capa	Captura	Dónde aparece
Auditoría de solicitudes del portal	Cada acción realizada *a través* de OmniWeb	Configuración → Auditoría
Auditoría de inicio de sesión SSH	Cada inicio de sesión SSH *en un host gestionado*	Configuración → Auditoría (a través de la devolución de llamada del host)
Auditoría de comandos	Cada comando *ejecutado en un host* (escritos + ejecutados)	Configuración → Comandos

Auditoría de Solicitudes del Portal

Cada solicitud que pasa a través del proxy de OmniWeb se registra, independientemente de si tuvo éxito, falló o fue rechazada por RBAC. Cada entrada captura:

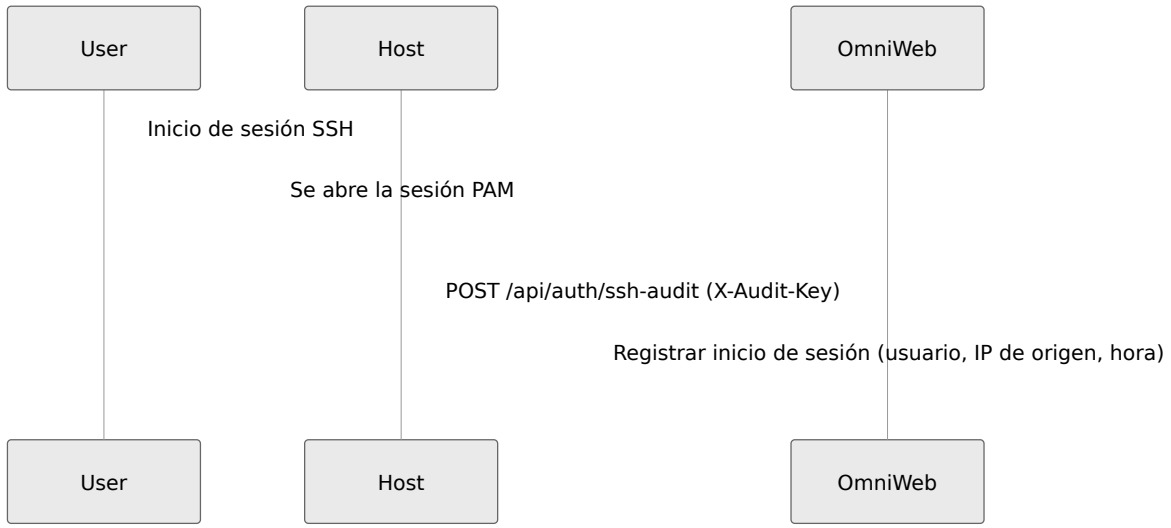
- El **usuario** que realizó la solicitud.
- El **tipo de elemento y la instancia** objetivo.
- El **método HTTP** (que indica si fue una vista, un cambio o una eliminación).
- El **resultado** (código de estado).
- La **marca de tiempo**.

Esto proporciona un registro completo de quién cambió qué, dónde y cuándo, dentro del portal. Se encuentra bajo **Configuración → Auditoría**. Dado que las lecturas (`GET`), escrituras (`POST`/`PUT`/`PATCH`) y eliminaciones son todas distinguibles por método, el registro de auditoría también funciona como un historial de cambios para la red.

El Registro de Auditoría (Configuración → Auditoría): cada acción con el usuario, tipo de evento, elemento/instancia, método HTTP, resultado y IP de origen. Nota el `DELETE` denegado (403), los eventos `permission_changed` y `ssh_login` junto a las solicitudes API ordinarias. Filtra por tipo de evento, usuario, elemento o rango de fechas.

Auditoría de Inicio de Sesión SSH

Los hosts pueden informar inicios de sesión SSH de vuelta a OmniWeb para que el acceso al host aparezca en la misma vista de auditoría que la actividad del portal. Un pequeño gancho PAM en cada host llama a OmniWeb cuando se abre una sesión, informando el nombre de usuario, IP de origen y detalle del servicio.



La devolución de llamada se autentica con un secreto compartido para que solo los hosts de confianza puedan escribir entradas de auditoría:

Variable	Predeterminado	Descripción
`AUDIT_API_KEY`	`omniweb-audit-key`	Secreto compartido que el gancho PAM del host presenta (como `X-Audit-Key`) al informar un inicio de sesión. **Cambia esto**, y establece el valor correspondiente en cada host.

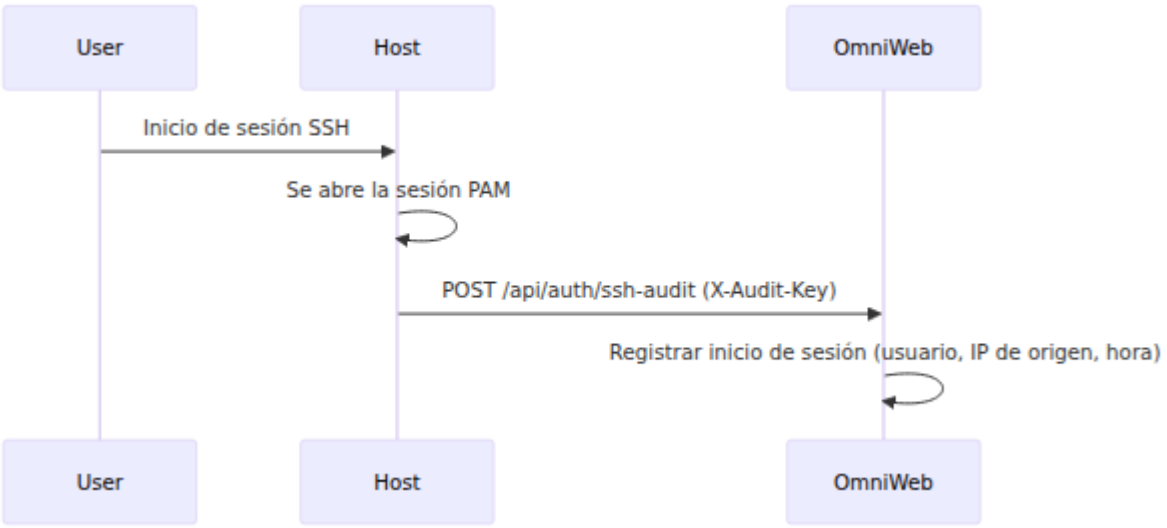
Con esto en su lugar, cada inicio de sesión SSH en un host gestionado aparece bajo **Configuración → Auditoría** junto a las acciones del portal, uniendo la actividad de una persona en el portal y en el host.

Auditoría de Comandos

Para la visibilidad a nivel de comandos en los hosts, OmniWeb recopila **dos flujos complementarios**, ambos enviados a Loki y navegables bajo **Configuración → Comandos** con un interruptor de origen:

Origen	Captura	Flujo de Loki
Comandos escritos	Las líneas de comandos exactas que un usuario escribe en un shell interactivo, **incluyendo comandos internos de shell** como `echo`, `cd`, `export`	`job="cmdaudit"`
Ejecuciones de binarios	Cada binario que realmente se ejecutó en el host (scripts, herramientas, automatización)	`job="auditd"`

Ninguno reemplaza al otro: los internos nunca ejecutan un binario separado, por lo que solo el flujo de comandos escritos los ve; y la automatización/scripts que nunca están en un aviso interactivo solo aparecen en el flujo de ejecución de binarios. Juntos cubren *lo que una persona escribió* y *lo que realmente se ejecutó*.



Comandos escritos son capturados por un gancho de shell interactivo ligero que registra cada comando que un usuario ejecuta (con usuario, directorio de trabajo y TTY). Esta es la capa que captura los internos que un rastreador de binarios no puede ver estructuralmente.

Ejecuciones de binarios provienen de un agente ligero del host que registra cada binario ejecutado en el host. Debido a que funciona en espacio de usuario, funciona dentro de contenedores LXC sin soporte de auditoría del kernel. Cada entrada captura:

Campo	Significado
`login`	El usuario que originalmente inició sesión; **sobrevive a** `sudo`/`su`, por lo que los cambios de privilegio no ocultan quién está actuando
`uid`	UID efectivo con el que realmente se ejecutó el comando
`filename`	El binario que fue ejecutado
`cwd`	Directorio de trabajo en el momento de la ejecución
(después de `]:`)	La línea de comando completa

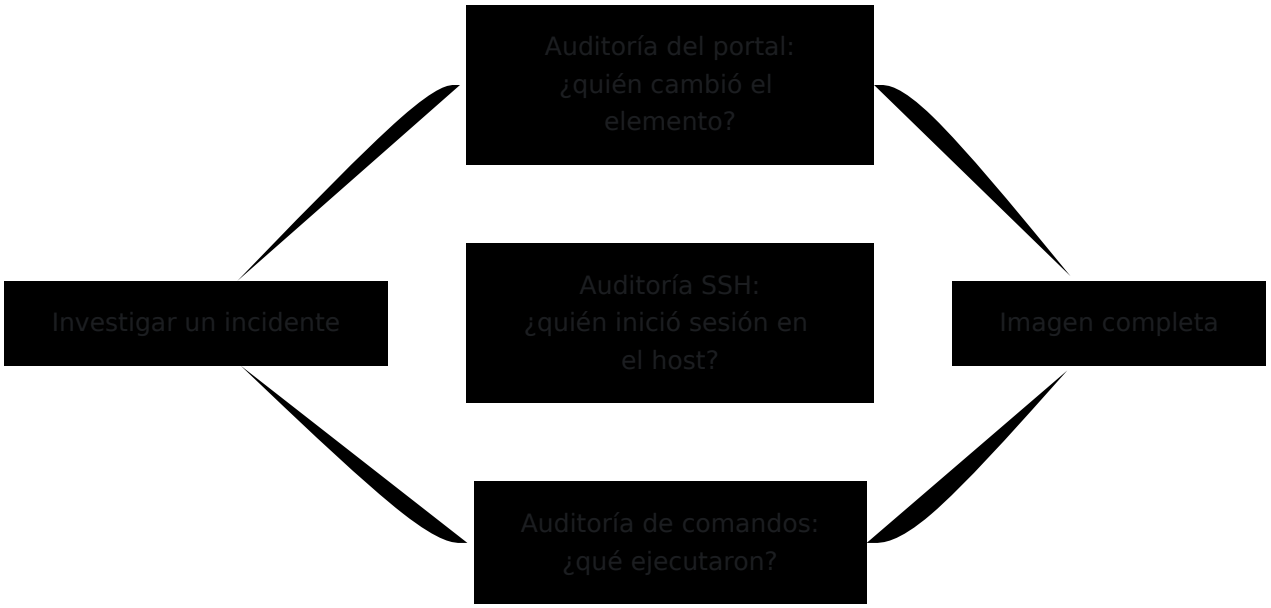
Una entrada de ejecución representativa:

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

La vista de **Configuración → Comandos** se predetermina al flujo de comandos escritos y te permite filtrar por host, buscar por usuario o comando, y seguir la actividad en tiempo real a través de la flota, con el interruptor de origen para cambiar a la vista de ejecución de binarios en bruto cuando quieras ver exactamente qué se ejecutó.

> **Nota:** los flujos de comandos son una ayuda de visibilidad para el operador capturada en espacio de usuario. Un usuario root decidido puede eludirlos; la auditoría a nivel de kernel es el paso de endurecimiento si necesitas una captura no eludible. Para el registro estructurado relevante para la seguridad (inicios de sesión, cambios de permisos, denegaciones), confía en la **Auditoría del Portal** y **Auditoría de inicio de sesión SSH** arriba, que se escriben en la propia base de datos de OmniWeb.

Cómo se Integran las Capas



- Un cambio de configuración realizado **a través de OmniWeb** → auditoría de solicitudes del portal.
- Un cambio realizado **manualmente en un host** → auditoría de inicio de sesión SSH (quién entró) + auditoría de comandos (qué hicieron).

Juntos no dejan ningún punto ciego entre "lo cambié en la interfaz" y "lo cambié en la máquina".

Relacionado

- Registros y Seguimiento de Suscriptores: el explorador de registros general detrás de los flujos de comandos.
- Inicio de Sesión con Clave SSH: el lado de acceso de la actividad del host.
- RBAC: los permisos cuyo uso registra la auditoría del portal.

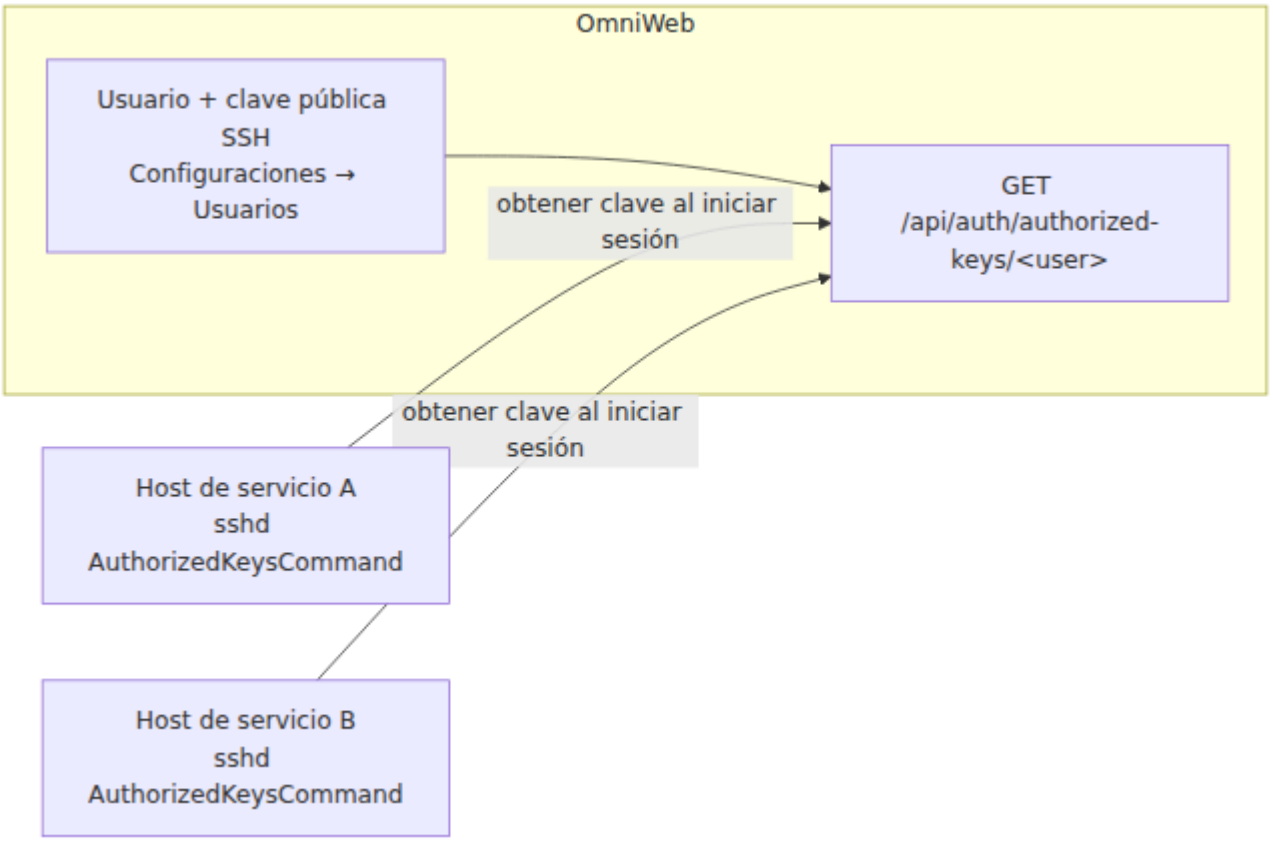
Inicio de Sesión con Clave SSH (Acceso al Host)

El control de acceso de OmniWeb se extiende más allá del portal a los **hosts** que ejecutan la red. Cada usuario puede llevar una **clave pública SSH**, y los hosts gestionados obtienen esas claves **en vivo desde OmniWeb** en el momento del inicio de sesión. Así que OmniWeb es el único lugar para gestionar *quién puede SSH dónde*, y, combinado con registro de auditoría, quién realmente lo hizo.

No hay un servidor de directorio que ejecutar ni archivos `authorized_keys` por host que mantener. (Esto reemplaza un diseño anterior de sincronización de OpenLDAP; el directorio ha desaparecido y las claves se sirven bajo demanda a través de HTTPS.)

← Autenticación y Control de Acceso · ← Guía de Operaciones

Qué Hace



Le das a un usuario una clave pública SSH en OmniWeb una vez. El `sshd` de cada host gestionado está configurado para pedir a OmniWeb la clave de ese usuario **en el momento del inicio de sesión** (a través del `AuthorizedKeysCommand` de OpenSSH). Agrega una clave en OmniWeb y el usuario puede SSH a cada host inscrito; desactiva al usuario y ese acceso se pierde en todas partes en su **siguiente** intento de inicio de sesión, sin sincronización, sin desvío y sin archivos de claves que limpiar.

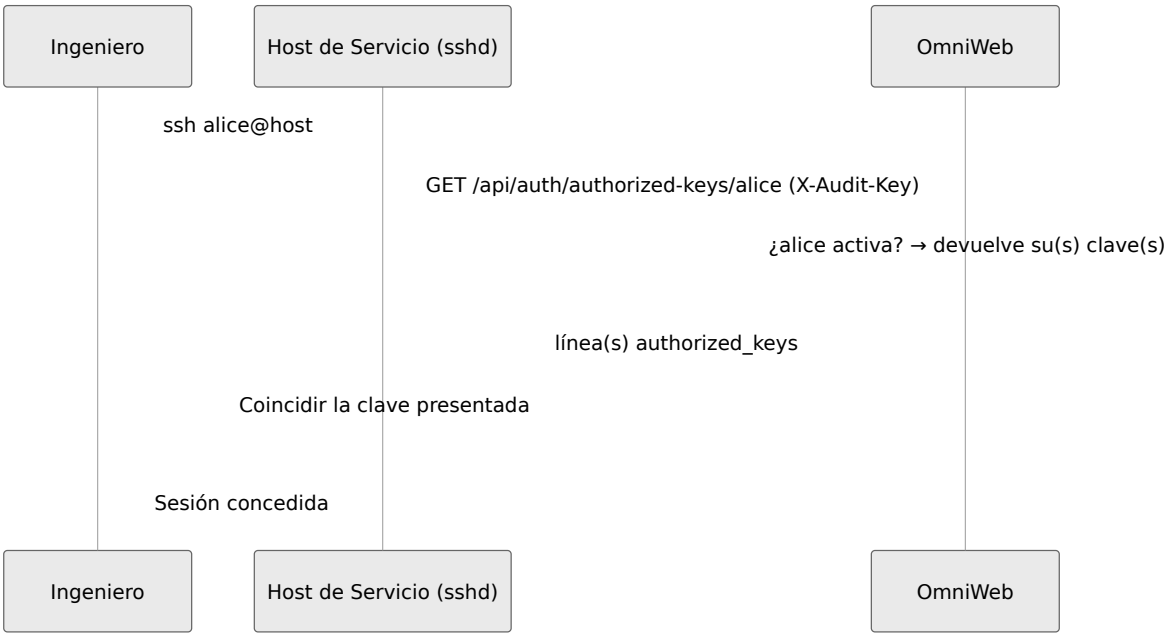
Estableciendo la Clave de un Usuario

Las claves se gestionan en **Configuraciones → Usuarios**, la misma pantalla que gestiona las cuentas del portal, RBAC y el estado activo/desactivado. Cada fila de usuario muestra si se ha configurado una clave SSH; crea o edita un usuario para pegar una.

Configuraciones → Usuarios: cada usuario con si se ha configurado una clave pública SSH. La clave que pegas aquí es la que otorga acceso al host; no hay otro lugar para mantenerla.

Cómo los Hosts la Consumen

Cada host gestionado ejecuta un pequeño ayudante conectado a `sshd` como su `AuthorizedKeysCommand`. Cuando alguien se conecta, `sshd` ejecuta el ayudante, que obtiene las claves autorizadas de ese usuario desde OmniWeb a través de HTTPS y las devuelve para la coincidencia:



Propiedades clave de este flujo:

- **En vivo**: la clave se obtiene por inicio de sesión, por lo que los cambios tienen efecto inmediato.
- **Solo usuarios activos**: OmniWeb solo devuelve claves para usuarios **activos**. Cuando desactivas o eliminas un usuario en OmniWeb, eso niega su siguiente inicio de sesión en cada host a la vez. Este es el botón de revocación.
- **Sin enumeración**: un usuario desconocido o desactivado, o uno sin clave, devuelve un resultado vacío. El inicio de sesión simplemente no encuentra ninguna clave y es denegado, por lo que el endpoint no filtra qué nombres de usuario existen.
- **Sobrevive a una interrupción de OmniWeb**: el ayudante almacena en caché el último resultado bueno por usuario en el host, por lo que una breve interrupción de OmniWeb no bloquea a todos.

La cuenta en sí (el usuario de Unix, el directorio personal, el shell) se provisiona mediante la gestión de configuración junto con el ayudante `sshd`. OmniWeb posee la **identidad y las claves**, y la automatización de la flota posee **la existencia de la cuenta** en cada host.

Configuración

El endpoint que sirve claves está protegido por el mismo secreto compartido que el callback de auditoría:

Variable	Predeterminado	Descripción
`AUDIT_API_KEY`	`omniweb-audit-key`	Secreto compartido que presenta el ayudante `AuthorizedKeysCommand` de cada host (como `X-Audit-Key`) al obtener claves. **Cambia esto**, y establece el valor correspondiente en cada host.

Debido a que OmniWeb es lo único que debe ser consultado y el ayudante se ejecuta en hosts de confianza, el endpoint se sirve a través de HTTPS y el secreto es una segunda puerta sobre la ruta de red.

Por Qué Esto Importa

- **Un lugar para otorgar/revocar acceso SSH** en toda la flota: el estado activo del usuario *es* su acceso al host.
- **Sin archivos de claves dispersos** que se desincronizan en hosts individuales, y sin servidor de directorio que operar y respaldar.
- **Una única identidad** que une el acceso al portal de una persona, su acceso SSH y, a través del registro de auditoría, su actividad registrada.

Relacionado

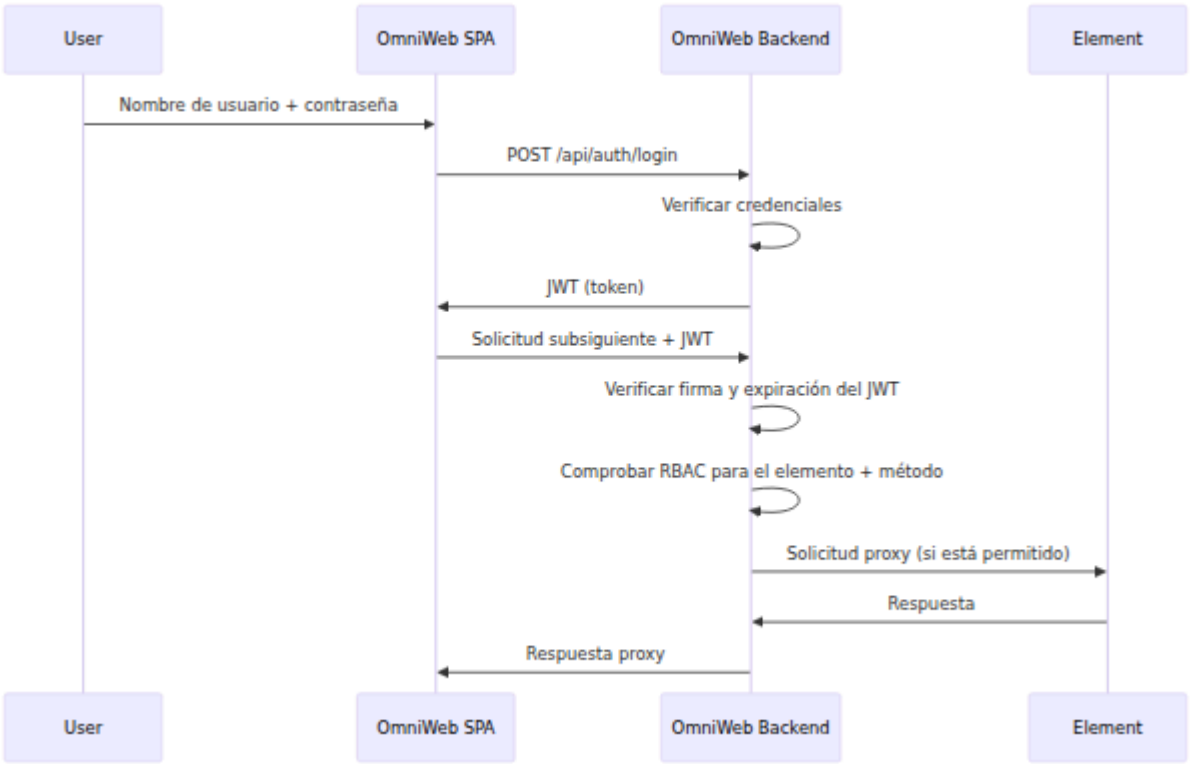
- Registro de Auditoría: registrar inicios de sesión SSH y cada comando ejecutado en los hosts.
- RBAC: controlar lo que los mismos usuarios pueden hacer *dentro* de OmniWeb.

Inicio de sesión y sesiones JWT

OmniWeb autentica a los operadores con un nombre de usuario y una contraseña y emite un JSON Web Token (JWT). Ese token prueba quién eres en cada solicitud subsiguiente. Crucialmente, es la *misma* credencial que autoriza el Grafana, Loki y Homer integrados. Un inicio de sesión abarca toda la pila.

← Autenticación y control de acceso · ← Guía de operaciones

Flujo de inicio de sesión



El token se emite mediante `POST /api/auth/login`. Una vez obtenido, la SPA lo presenta en cada llamada a la API, y el backend verifica la firma y la expiración antes de hacer cualquier otra cosa.

La pantalla de inicio de sesión. Autenticarse aquí genera el JWT que rige toda la pila: APIs de elementos, Loki, Grafana y Homer.

Cómo se transporta el token

El backend acepta el JWT en tres ubicaciones, lo que permite que el mismo token funcione para llamadas a la API XHR, navegaciones por el navegador y iframes incrustados:

Ubicación	Usado para
Encabezado de autorización	Solicitudes estándar de API (XHR/fetch) desde la SPA
Cookie (`access_token`, HttpOnly)	Navegaciones por el navegador y contenido incrustado (iframe de Grafana, pestaña de Homer)
Cadena de consulta	Casos en los que no se puede establecer ni un encabezado ni una cookie

La cookie es **HttpOnly** (no legible por JavaScript) y utiliza `SameSite=Lax`, lo que protege el token del robo a través del acceso a scripts de sitios cruzados, mientras que aún permite navegaciones de nivel superior a las herramientas integradas.

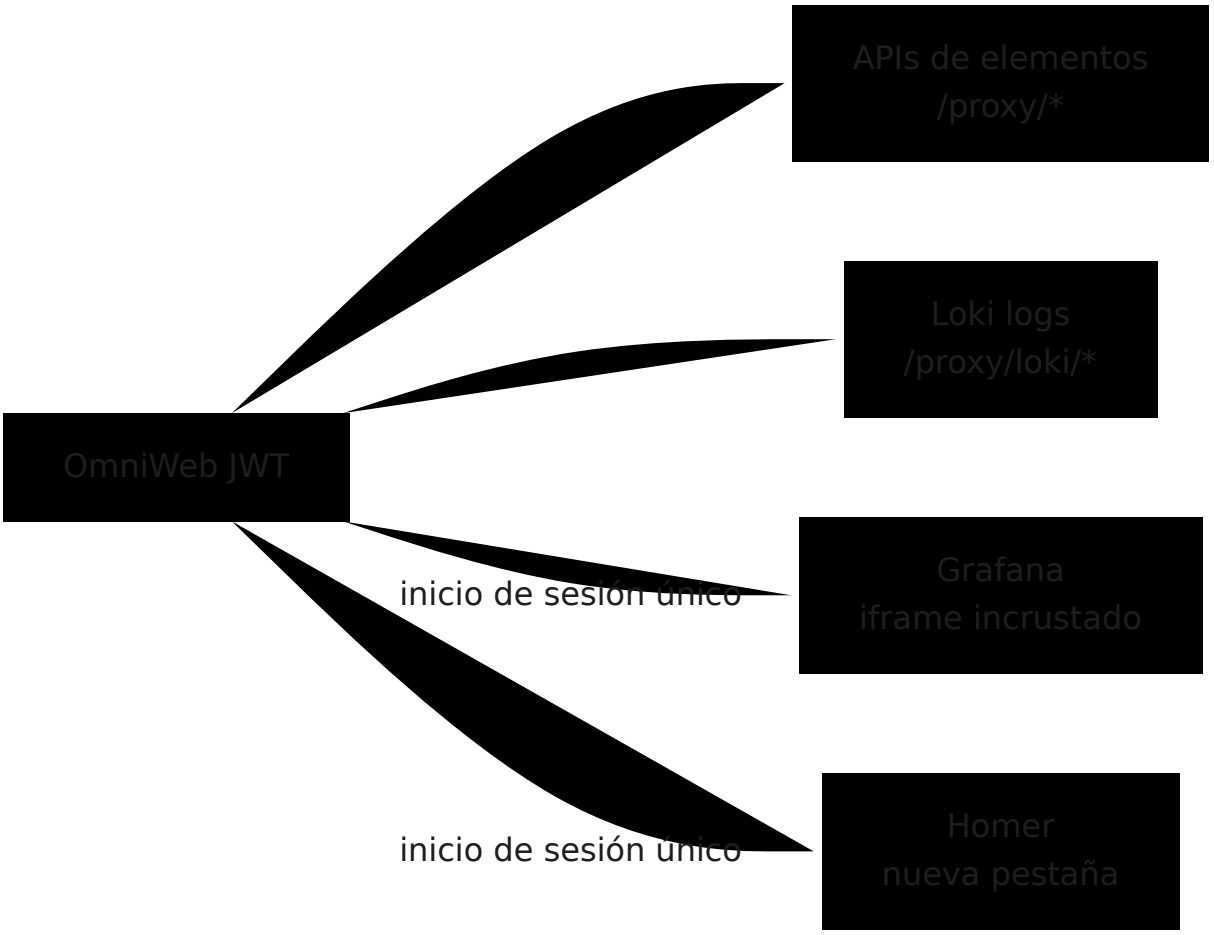
Tiempo de vida del token

El token de acceso tiene una expiración configurable, **24 horas por defecto** (`JWT_ACCESS_TOKEN_EXPIRES`, en segundos). Cuando expira, el operador es devuelto a la pantalla de inicio de sesión y se vuelve a autenticar. No hay una sesión silenciosa indefinida; la duración es un límite de seguridad deliberado.

Configuración	Predeterminado	Descripción
`JWT_ACCESS_TOKEN_EXPIRES`	`86400` (24 h)	Tiempo de vida del token de acceso en segundos. Redúzcalo para sesiones más ajustadas; aumente para menos reingresos.
`JWT_SECRET_KEY`	*(generado)*	Secreto utilizado para firmar y verificar tokens. Establecer explícitamente en producción para que los tokens sobrevivan a un reinicio del backend y sean consistentes entre instancias.

Un inicio de sesión, toda la pila

El mismo JWT autoriza las herramientas de monitoreo integradas, por lo que los operadores nunca inician sesión dos veces:



- **APIs de elementos y Loki** se acceden a través del proxy del backend, que verifica el JWT directamente.
- **Grafana y Homer** se acceden a través de la puerta de enlace autenticada, que verifica tu inicio de sesión en OmniWeb antes de hacer el proxy, sin una segunda contraseña. Consulta Grafana y Homer.

Esta es la razón por la que una sola sesión de OmniWeb rige toda la superficie operativa: paneles, registros, trazas y gestión de elementos se basan en un solo token.

Primer inicio de sesión y cambio de credenciales

Una implementación nueva se envía con una cuenta de administrador predeterminada (`admin` / `admin`). **Cambia esto inmediatamente** después del primer inicio de sesión, a través de Configuración. El predeterminado existe solo para iniciar el sistema y no debe sobrevivir en producción.

Cierre de sesión y expiración

Cerrar sesión descarta el token. Un token expirado o inválido provoca que la siguiente solicitud sea rechazada y la SPA regrese a la pantalla de inicio de sesión. Dado que las acciones de los elementos solo se realizan a través de una llamada proxy autenticada y verificada por RBAC, una sesión expirada nunca puede realizar una acción privilegiada.

Relacionado

- Control de acceso basado en roles: lo que se permite hacer a un usuario autenticado.
- Registro de auditoría: cada acción autenticada se registra.

Control de Acceso Basado en Roles (RBAC)

Estar autenticado le dice a OmniWeb *quién* eres. RBAC decide *qué puedes hacer*. El acceso se concede con un grano fino, **por tipo de elemento, por método HTTP**, que se mapea directamente a las operaciones reales que un operador realiza: ver, modificar o eliminar. Además, dos ámbitos deciden *dónde*: qué **sitios** puede alcanzar un operador y qué **dispositivos de prueba** puede usar. Cada solicitud debe pasar todos ellos.

← Autenticación y Control de Acceso · ← Guía de Operaciones

Niveles de Permiso

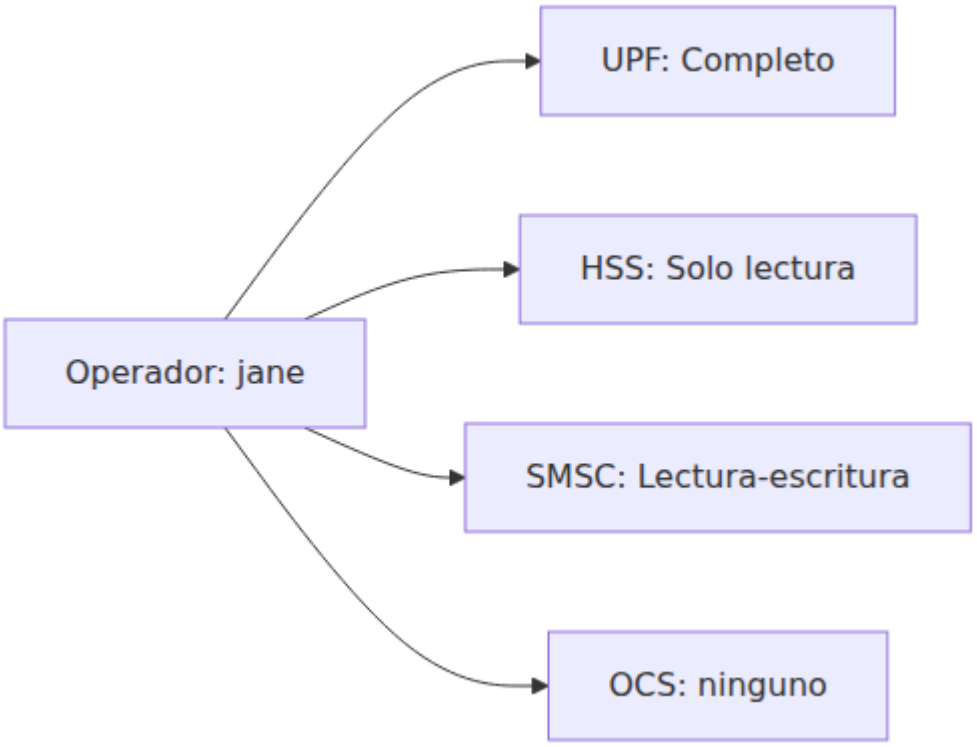
Cada tipo de elemento puede ser concedido a un usuario en uno de tres niveles. El nivel se expresa como el conjunto de métodos HTTP que el usuario puede usar contra ese elemento a través del proxy:

Permiso	Métodos permitidos	Lo que el operador puede hacer
Solo lectura	`GET`	Ver datos solamente, sin cambios
Lectura-escritura	`GET`, `POST`, `PUT`, `PATCH`	Ver y modificar: por ejemplo, agregar un suscriptor, editar una ruta, cambiar una regla de QoS
Completo	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	Todo, incluyendo eliminación y limpieza de sesiones

Debido a que los permisos están vinculados a métodos HTTP, se alinean exactamente con el modelo de edición genérico: un formulario de "Agregar" es un `POST`, un "Editar" es un `PUT`/`PATCH`, y un "Eliminar"/"limpiar" es un `DELETE`.

Granularidad por Elemento

Los permisos se asignan **independientemente por tipo de elemento**. Un usuario puede tener diferentes niveles en diferentes elementos:

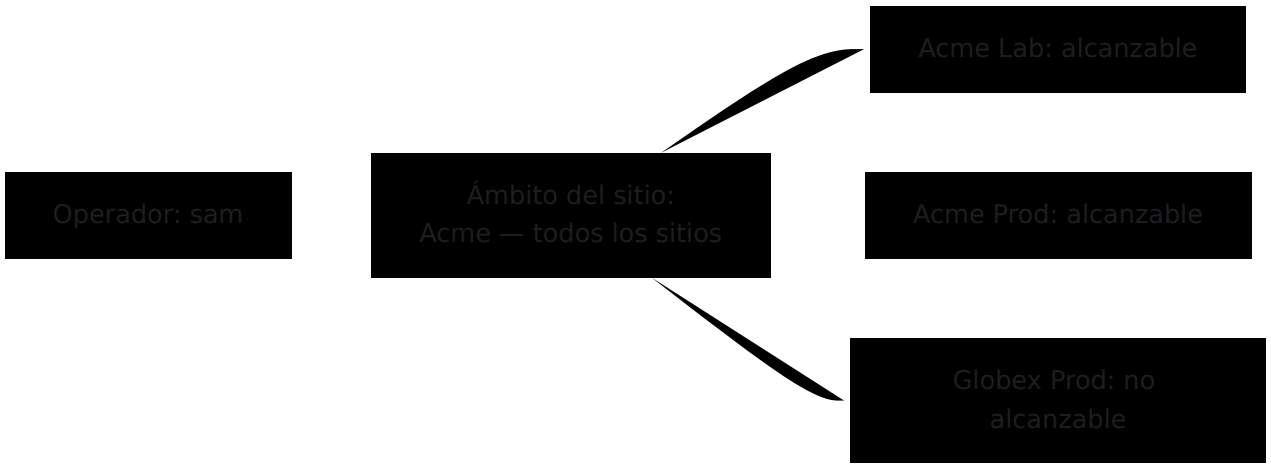


En este ejemplo, Jane puede limpiar sesiones de UPF, puede ver pero no cambiar el HSS, puede agregar rutas SMSC y no puede ver el OCS en absoluto. Esto te permite dar, por ejemplo, a un ingeniero de plano de datos control total del UPF mientras mantienes los datos de suscriptores como solo lectura.

Ámbito del Sitio (Despliegues Multi-Sitio)

Los permisos de elemento responden *qué* puede hacer un operador. En una flota con más de un sitio, un segundo eje independiente responde *dónde*: el conjunto de sitios que pueden alcanzar. Una solicitud debe satisfacer ambos.

Por defecto, un usuario es **sin restricciones**: puede alcanzar todos los sitios, incluidos los sitios añadidos más tarde. Limitar a un usuario a uno o más sitios los restringe exactamente a esos, y a un cliente completo se le puede conceder de una sola vez para que los nuevos sitios de ese cliente se incluyan automáticamente.



Un operador con ámbito limitado ve solo sus propios sitios en el selector de sitios; los demás no están listados, y los elementos, registros, métricas, inventario de software y trazas de llamadas detrás de ellos son rechazados del lado del servidor. Los administradores alcanzan todos los sitios independientemente del ámbito.

El ámbito del sitio se gestiona en **Configuración → Usuarios**, desde la acción del globo en la fila de un usuario. Marca los sitios que pueden alcanzar, o deja todo sin marcar para dejarlos sin restricciones.

Ámbito del Dispositivo de Prueba (Granja de Teléfonos)

La granja de teléfonos es un único tipo de elemento — **Dispositivos de Prueba** — que cubre cada banco, teléfono y módem, sus herramientas y sus pruebas programadas. Concederlo sigue la misma regla por método que cualquier otro elemento:

Permiso	Lo que el operador puede hacer con los teléfonos
Solo lectura	Listar los bancos y dispositivos, ver la pantalla de un teléfono, leer registros, descargar archivos y ver resultados de pruebas
Lectura-escritura	También escribir en un teléfono, enviar comandos AT y SMS, subir archivos y ejecutar un script de prueba
Completo	También eliminar un registro de dispositivo y limpiar sus metadatos asignados

Ver la pantalla de un teléfono se trata como una **lectura**, no un cambio: un operador que solo puede observar aún puede ver lo que está haciendo un banco. Escribir en el teléfono es una acción de nivel de escritura separada.

Debido a que toda la granja es un tipo de elemento, una concesión es, de otro modo, todo o nada. Para dar a alguien solo *algunos* de los teléfonos, establece un **ámbito de dispositivo**: marca los dispositivos individuales que pueden usar, agrupados por banco. No marcar nada los deja sin restricciones: cada dispositivo, incluidos los que se añadan más tarde.

Un operador con ámbito de dispositivo ve solo sus propios dispositivos en la lista de flota, ve cada banco restringido a esos dispositivos (y bancos sin ninguno de ellos no en absoluto), y se le niega si nombra otro dispositivo directamente. Ejecutar un script en varios teléfonos es rechazado de inmediato si alguno de ellos está fuera de su ámbito, en lugar de ejecutarse silenciosamente en el subconjunto: una ejecución parcial se leería como un pase completo. Editar la lista de horarios reemplaza todo el conjunto, por lo que eso se queda con los operadores que tienen cada dispositivo.

El ámbito del sitio y el ámbito del dispositivo son independientes: la granja de teléfonos es deliberadamente independiente del sitio, ya que un banco no es parte de un despliegue de red.

Ambos se establecen en **Configuración → Usuarios**, desde la acción del globo en la fila de un usuario.

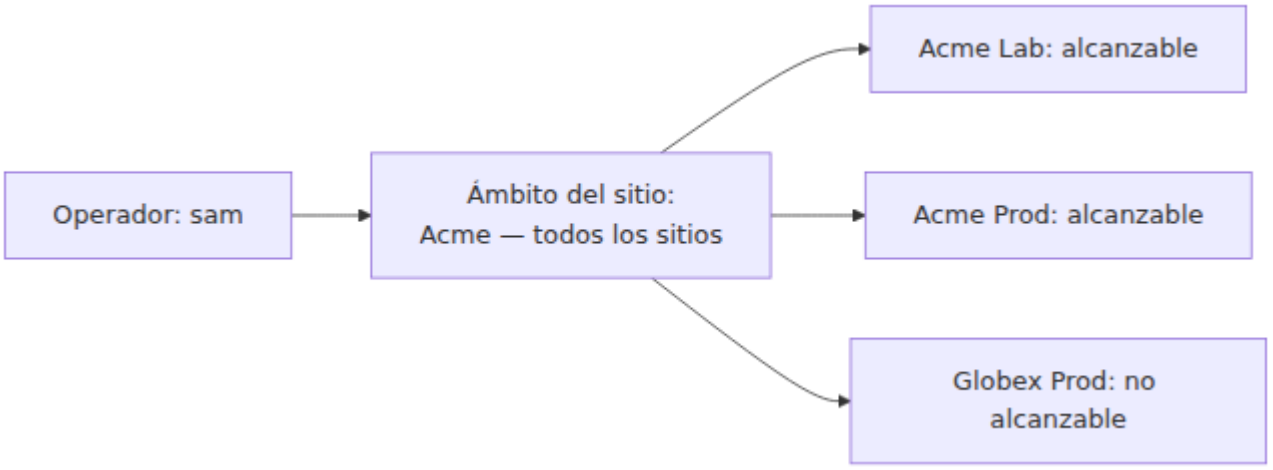
> **Al actualizar:** la granja de teléfonos anteriormente solo necesitaba un inicio de sesión, por lo que cada cuenta que existía antes de este cambio mantiene acceso completo a Dispositivos de Prueba, registrado como una concesión normal. Restringe de la misma manera que cualquier otro elemento: revoca **Dispositivos de Prueba** de quien no debería tener los teléfonos, y establece un ámbito de dispositivo para quien solo debería tener algunos. Las cuentas creadas después comienzan sin acceso hasta que se les conceda.

Administradores

Los administradores tienen acceso completo a todos los tipos de elementos automáticamente. El rol de administrador también es lo que concede acceso a la gestión de usuarios y permisos. Mantén el número de administradores pequeño y prefiere concesiones específicas por elemento para todos los demás.

Gestión de Roles y Permisos

Los permisos se gestionan en **Configuración → Permisos**. Para cada usuario que elijas, por tipo de elemento, si tienen acceso solo lectura, lectura-escritura, o completo (o ninguno).

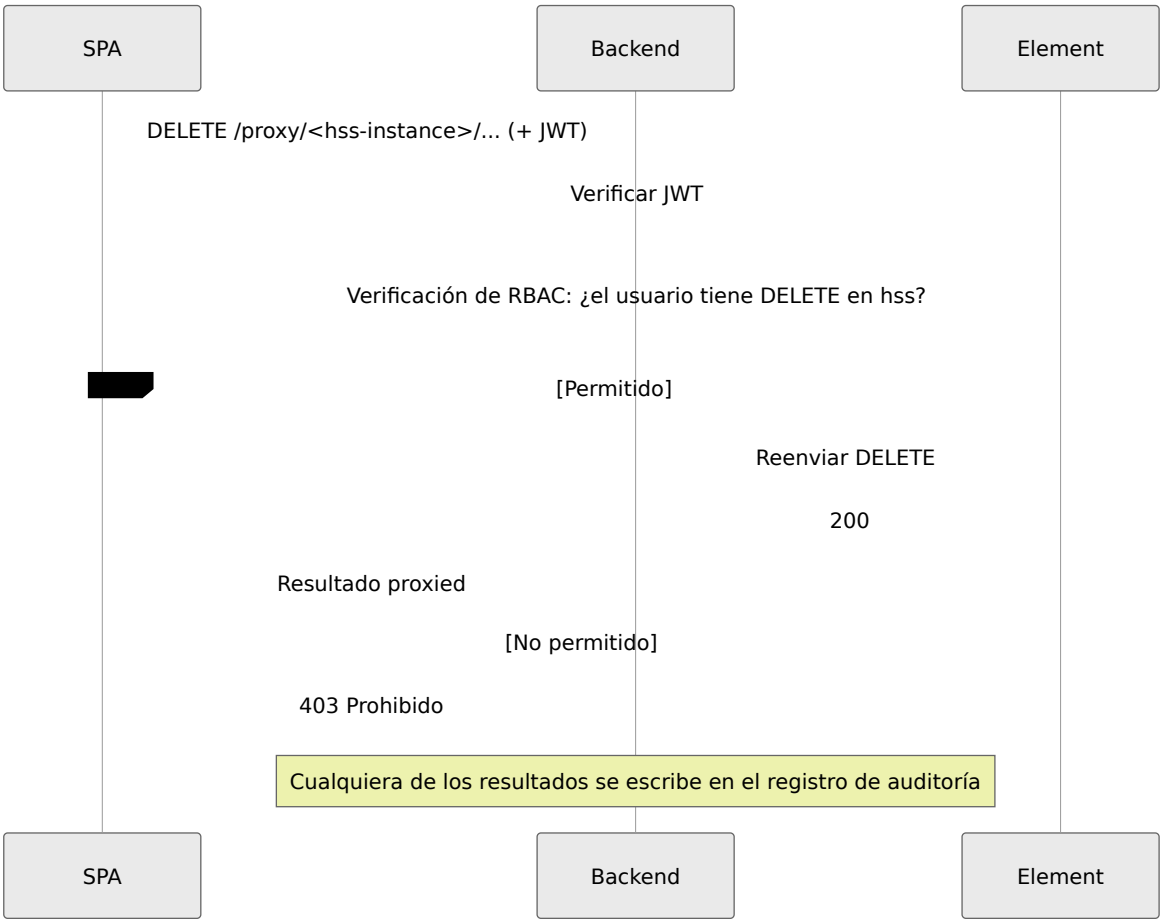


Cómo Funciona la Aplicación

RBAC se aplica en dos lugares complementarios:

1. **En la UI**: los controles para acciones que no puedes realizar no se muestran. Si solo tienes acceso de lectura al HSS, no verás botones de Agregar/Editar/Eliminar allí.
2. **En el backend**: cada solicitud proxy se verifica nuevamente contra tus permisos *del lado del servidor*. Incluso una solicitud diseñada para eludir la UI es rechazada si tu rol no permite ese elemento/método, o si nombra un elemento en un sitio fuera de tu ámbito de sitio. El sitio en el que actúa una solicitud se toma de la propia solicitud, por lo que se verifica en lugar de confiar en él.

Esta "defensa en profundidad" significa que la UI es una conveniencia, no el límite de seguridad. El proxy del backend es el límite.



Configuración → Permisos: selecciona un usuario, luego concede un nivel (solo lectura, lectura-escritura o completo) por tipo de elemento.

Buenas Prácticas

- **Menos privilegios**: concede el nivel más bajo que permita a alguien hacer su trabajo; amplía solo cuando sea necesario.
- **Solo lectura por defecto** para elementos que un operador solo necesita observar.
- **Reserva Completo (DELETE)** para aquellos que realmente necesitan limpiar sesiones o eliminar registros.
- **Pocos administradores**: usa concesiones específicas por elemento en lugar de otorgar acceso de administrador.
- **Ámbito por sitio** en una flota multi-sitio: da a los operadores de un cliente sus propios sitios, para que un error no pueda alcanzar otro despliegue.
- **Ámbito de dispositivos de prueba** a los teléfonos de los que alguien es responsable, para que una ejecución de script no pueda perturbar el banco de otro equipo.

- **Fijar credenciales de servicio**: una clave API puede restringirse a menos sitios que su propietario, por lo que una clave emitida para un despliegue no puede actuar en otro. Una clave solo puede ser más estrecha que la cuenta a la que pertenece, nunca más amplia.

Relacionado

- Inicio de sesión y sesiones JWT: autenticación en la que se basa RBAC.
- Operaciones Comunes: cómo los permisos dan forma a la UI cotidiana.
- Registro de Auditoría: tanto las acciones permitidas como las denegadas se registran.

Autenticación y Control de Acceso

OmniWeb es la única puerta de entrada a toda la red, por lo que el control de acceso es una de sus responsabilidades más importantes. Utiliza inicio de sesión basado en JWT, control de acceso basado en roles (RBAC) de forma granular sobre cada elemento, inicio de sesión con clave SSH para acceso a hosts y un registro de auditoría unificado que abarca el portal y los hosts que gestiona.

Esta área se divide en páginas enfocadas:

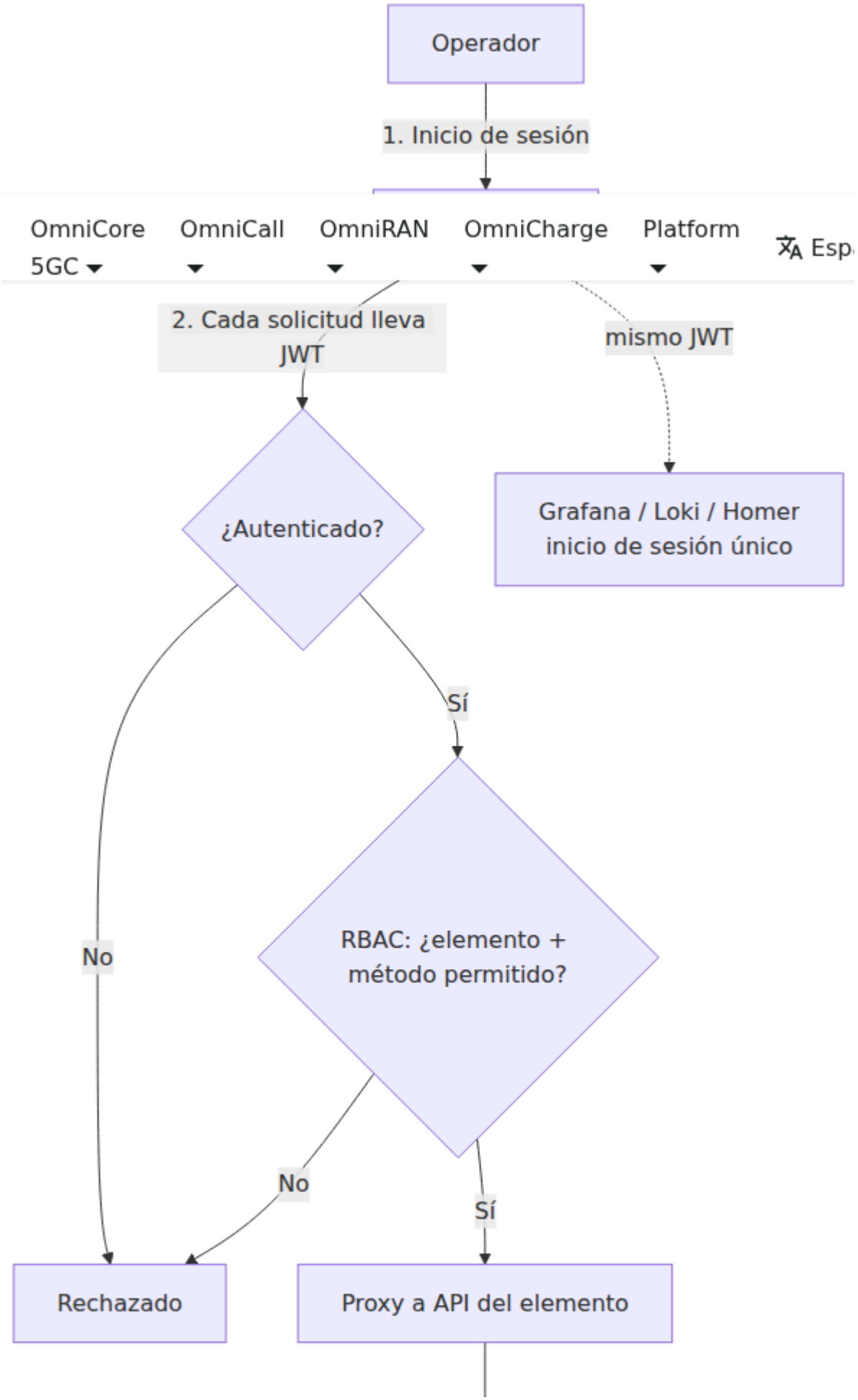
← Volver a la Guía de Operaciones

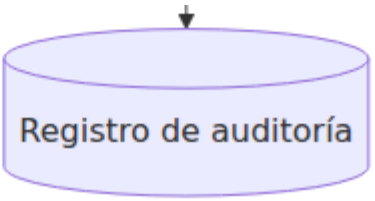
En Esta Sección

- **Inicio de Sesión y Sesiones JWT**: Cómo inician sesión los operadores, cómo funciona el JWT, la duración del token y cómo un único inicio de sesión abarca Grafana, Loki y Homer.
- **Control de Acceso Basado en Roles (RBAC)**: Permisos por elemento y por método; cómo otorgarlos; y cómo se hacen cumplir.
- **Inicio de Sesión con Clave SSH**: Los hosts gestionados obtienen la clave pública SSH de cada usuario en tiempo real desde OmniWeb (AuthorizedKeysCommand), por lo que el acceso a los hosts se otorga/revoca de manera centralizada.
- **Registro de Auditoría**: Las tres capas de auditoría: auditoría de solicitudes del portal, auditoría de inicio de sesión SSH y auditoría de comandos.

El Modelo de Control de Acceso

OmniWeb superpone cuatro controles. Una solicitud debe pasar por cada uno antes de llegar a un elemento, y toda la cadena se registra.


Operador
1. Inicio de sesión
OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platform
Esp
2. Cada solicitud lleva JWT
mismo JWT
¿Autenticado?
Grafana / Loki / Homer
inicio de sesión único
Sí
No
RBAC: ¿elemento + método permitido?
No
Sí
Rechazado
Proxy a API del elemento



Capa	Qué controla	Página
Autenticación	Quién eres, probado por un JWT firmado	Inicio de Sesión y JWT
Autorización (RBAC)	Qué puedes hacer, por tipo de elemento y método HTTP	RBAC
Acceso a Hosts	Quién puede SSH dónde; claves servidas en vivo desde OmniWeb	Inicio de Sesión con Clave SSH
Auditoría	Lo que realmente sucedió, a través del portal y los hosts	Registro de Auditoría

Por Qué Es Importante

Debido a que OmniWeb actúa como proxy para cada elemento, panel de Grafana, consulta de Loki y sesión de Homer, esta única cadena de control de acceso gobierna la *superficie* operativa *entera* de la red. Hay un lugar para otorgar acceso, un lugar para revocarlo y un registro que documenta quién hizo qué, en el portal y en los hosts subyacentes.

Un registro para todo: solicitudes de API, inicios de sesión, inicios de sesión SSH y cambios de permisos, con usuario, elemento, método, resultado y IP de origen. Ver Registro de Auditoría.

Comienza con Inicio de Sesión y Sesiones JWT.

Trazado de Llamadas (SIP Trace)

Trazado de Llamadas es la herramienta de OmniWeb para la solución de problemas de llamadas de voz. Registra la señalización SIP y el medio RTP de las llamadas que cruzan el IMS. Luego te permite buscar esas llamadas, abrir un informe completo por llamada, seguir la llamada como una escalera de señalización a través de la red, medir la calidad de voz, escuchar el audio y descargar la captura de paquetes en bruto (PCAP).

Trazado de Llamadas es una herramienta a nivel de sitio. Aparece en la barra lateral bajo **Trazado de Sesiones** como **SIP Trace**. La herramienta solo aparece cuando el servicio de captura está configurado y es accesible para el sitio seleccionado.

← Guía de Operaciones

Contenidos

- Qué es
- Arquitectura
- Buscar
- Detalle de la llamada
- Escalera (Trazado de Sesiones)
- Pestaña de QoS
- Escuchar
- Descarga de PCAP
- Llamadas Activas
- Sniffer en Vivo
- Agentes de Captura Remota
- Reglas de Grabación y Retención
- Privacidad e interceptación legal

- Cómo se compara Trazado de Llamadas con Homer y Trazado de Sesiones

Qué es

Trazado de Llamadas responde a una pregunta en profundidad: **¿qué pasó con esta llamada?** Para cualquier llamada grabada, te proporciona:

- Las dos partes, sus números, sus dominios SIP y el nombre para mostrar.
- La dirección IP SIP de cada parte, vinculada a su elemento de red OmniWeb.
- La respuesta SIP final y la razón de desconexión (SIP y Q.850).
- La calidad de voz de cada dirección de medio: MOS, jitter, pérdida de paquetes y retraso de ida y vuelta.
- El flujo completo de mensajes SIP (escalera) a través de cada elemento IMS que tocó la llamada.
- El audio grabado y el PCAP en bruto.

Trazado de Llamadas registra las llamadas de primera mano. Debido a que captura el SIP Call-ID y el medio en la red, una llamada se mapea a su captura de paquetes sin conjeturas.

La calidad de voz se informa como **MOS** (Mean Opinion Score). MOS es una puntuación de 1 a 5. Una puntuación de 4.0 o más es buena, de 3.0 a 4.0 es regular, y por debajo de 3.0 es mala. OmniWeb colorea los valores de MOS: verde para bueno, ámbar para regular y rojo para malo. Las llamadas AMR-WB (banda ancha) en una red saludable puntúan alrededor de 4.5.

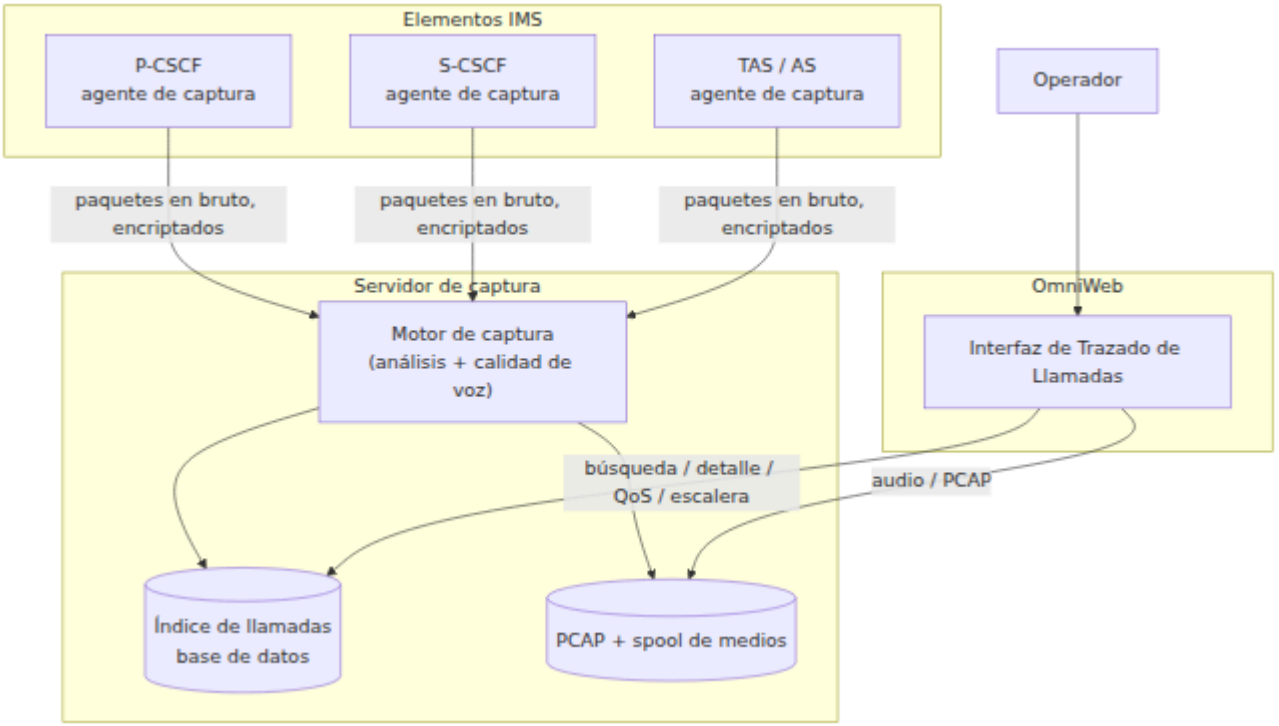
Arquitectura

Trazado de Llamadas utiliza dos partes:

1. **Agentes de captura** que se ejecutan en los elementos IMS (P-CSCF, S-CSCF y TAS). Cada agente captura los paquetes SIP y RTP que ve en su host. Los agentes no almacenan ni analizan paquetes localmente. Reenvían los paquetes en bruto al servidor de captura central a través de un canal encriptado.

2. El **servidor de captura central** analiza cada paquete, calcula la calidad de voz y escribe un índice en su base de datos. Mantiene el spool de captura de paquetes y los medios grabados. OmniWeb lee este único servidor para búsqueda, detalle de llamada, escalera, QoS, audio y PCAP.

Este diseño mantiene todos los datos grabados en un solo servidor central. Los elementos IMS no mantienen datos de captura propios.



Los agentes de captura le dan a Trazado de Llamadas una vista desde muchos puntos en la red. Una sola llamada se ensambla a partir de cada agente que la vio. Esto es lo que permite que la escalera muestre el flujo SIP de múltiples saltos a través del P-CSCF, el S-CSCF y el TAS.

Buscar

Abre Trazado de Llamadas para acceder a la vista de **Buscar**. La búsqueda encuentra llamadas completadas en el índice de llamadas central.

La vista de búsqueda. Cada fila apila al llamador y la parte llamada (número, dominio, nombre, IP SIP y agente de usuario) junto a celdas RTP por dirección que muestran IP de origen, códec, tres estimaciones de MOS, jitter y pérdida.

Filtros

Establece uno o más filtros, luego selecciona **Buscar**. Todos los filtros se combinan con AND.

Filtro	Qué coincide
Número	El número del llamador O el número del llamado.
Rango de Tiempo	Una ventana preestablecida (Últimos 15m a Últimos 7d) o un inicio y fin personalizados.
Dirección	Entrante, Saliente o Interna. La dirección proviene del rol de la IP del llamador y del llamado.
Min MOS	Mantener solo las llamadas cuyo MOS en la peor dirección esté en o por encima de este valor. Usa esto para encontrar buenas llamadas, o invierte tu lectura para encontrar malas.
Max pérdida	Mantener solo las llamadas cuya pérdida de paquetes en la peor dirección esté en o por debajo de este valor.

Cuadrícula de resultados

Cada fila de resultado muestra:

- **Tiempo**: el inicio y fin de la llamada.
- **Llamador** y **Llamado**: una celda apilada con el número y dominio (`num@domain`), el nombre para mostrar, la IP SIP (un enlace a ese elemento en OmniWeb) y el agente de usuario. Un chip de **colgó** marca a la parte que envió el BYE.
- **Resultado**: el código y texto de respuesta SIP final.
- **RTP A** y **RTP B**: una celda por dirección de medio. Cada celda muestra la IP de origen, el códec, tres estimaciones de MOS (fijo 50 | fijo 200 | adaptativo), el jitter y el conteo de paquetes perdidos. Los tres valores de MOS están codificados por colores.
- **Dur (s)**: la duración de la llamada en segundos.
- **PCAP**: un botón de descarga por fila para la captura de paquetes de esa llamada.

Selecciona una fila para abrir el detalle de la llamada.

Detalle de la llamada

La vista de detalle de la llamada es el informe completo para una llamada. Se abre cuando seleccionas un resultado de búsqueda. La URL lleva el identificador de la llamada, por lo que puedes marcar o compartir una llamada.

La vista de detalle de la llamada. El encabezado muestra el Call-ID y el contexto. La franja de resumen muestra Inicio, Duración, PDD, Timbre, Conectado, la última respuesta SIP y las razones de desconexión. La tabla de dos columnas muestra Identidad y calidad de voz para las piernas del Llamador (A) y el Llamado (B).

Encabezado y contexto

El encabezado muestra el **Call-ID** en la red. Un bloque de contexto debajo muestra la **Dirección** de la llamada, el **Sensor** propietario (el agente de captura), qué parte **Colgó**, el tiempo **Finalizado** y el **Nombre del Llamador**.

Franja de resumen

La franja de resumen es una visión general de una línea de la llamada:

Campo	Significado
Inicio	Cuándo comenzó la llamada.
Duración	Longitud total de la llamada.
PDD	Retraso post-marcado: el tiempo desde INVITE hasta la primera indicación de timbre.
Timbre	Cuánto tiempo sonó el teléfono antes de responder.
Conectado	Cuánto tiempo estuvo conectada la llamada (fluyendo medios).
Última respuesta SIP	El código y texto de respuesta SIP final.
Razón SIP	La causa de desconexión SIP, cuando el motor de captura registra una.
Razón Q.850	La causa y texto de desconexión Q.850, cuando está presente.
Llamador y **Llamado**	Las dos partes como `num@domain`.

Tabla de Identidad y calidad de voz

La tabla principal tiene dos columnas: **Llamador (A)** y **Llamado (B)**. Cada IP se vincula a su elemento de red OmniWeb cuando se conoce el elemento. La tabla tiene tres grupos.

Identidad:

Fila	Significado
IP SIP	La IP de señalización SIP de la parte.
IP RTP	La IP de medios RTP de la parte.
Puerto RTP	El puerto de medios RTP.
Agente de Usuario	El agente de usuario SIP de la parte.
Códec	El códec de audio, por ejemplo AMR-WB.
Paquetes recibidos	El conteo de paquetes RTP recibidos.
Paquetes perdidos	El conteo de paquetes RTP perdidos.

MOS: tres estimadores de MOS, cada uno mostrado como `promedio | mínimo`:

Fila	Significado
MOS fijo 50	MOS sobre una ventana fija de 50 paquetes.
MOS fijo 200	MOS sobre una ventana fija de 200 paquetes.
MOS adaptativo 500	MOS sobre una ventana adaptativa de hasta 500 paquetes.

Jitter y RTCP: el jitter RTP (máximo y promedio), el jitter RTCP, el conteo de pérdida y fracción perdida de RTCP, y el retraso de ida y vuelta de RTCP (máximo y promedio).

Escalera (Trazado de Sesiones)

La pestaña **Escalera** dibuja la llamada como un flujo de señalización ordenado por tiempo. Trazado de Llamadas ensambla los mensajes SIP de cada agente

de captura que vio la llamada. El resultado es una escalera de múltiples saltos a través de los elementos IMS: por ejemplo, de P-CSCF a S-CSCF a TAS.

La pestaña de Escalera. Las columnas son los elementos IMS que cruzó la llamada. Cada peldaño es un mensaje SIP. La escalera muestra el flujo de INVITE a 100 a 180 a 200 a ACK a BYE, con deltas de tiempo por mensaje y el ida y vuelta de solicitud a respuesta.

Cada columna es un elemento IMS, etiquetado con su rol y nombre de host. Cada peldaño es un mensaje SIP extraído de origen a destino. La escalera muestra:

- El **delta de tiempo por mensaje** (el intervalo desde el mensaje anterior).
- El **ida y vuelta de solicitud a respuesta** para cada respuesta, emparejado de vuelta a su solicitud.
- Modos de tiempo **absoluto**, **relativo** y **hace** para la columna de tiempo.
- **Decodificación de paquetes en línea**: selecciona un peldaño para ver el texto completo del mensaje SIP y una vista en hex.

Un panel de **Detalles de Sesión** lista las sesiones en la escalera. Para una sola llamada hay una sesión, por lo que el panel permanece colapsado.

La escalera utiliza el mismo renderizado que los Flujos en Vivo de Trazado de Sesiones a nivel de red. Consulta Registros y Trazado de Suscriptores para la herramienta de Trazado de Sesiones más amplia.

Pestaña de QoS

La pestaña **QoS** muestra la calidad de voz a lo largo de la vida de la llamada.

La pestaña de QoS. Las tablas muestran los cubos de distribución de PDV (retraso) y el desglose de pérdida en fila para cada dirección. Se dibuja un gráfico interactivo de calidad de retraso y MOS sobre la duración de la llamada debajo de las tablas.

La pestaña de QoS tiene tres partes:

- Un **gráfico interactivo de retraso / jitter y calidad de MOS** a lo largo de la llamada. El gráfico es por dirección de medio. Puedes leer el retraso y el MOS en cualquier punto de la llamada, lo que muestra dónde cayó la calidad.

- La **distribución de PDV (retraso)**: cuántos paquetes cayeron en cada cubo de retraso (por ejemplo, 50 a 70 ms, 70 a 90 ms, y así sucesivamente hasta más de 300 ms). Una distribución que se mantiene en los cubos bajos es saludable.
- El desglose de **pérdida en fila**: cuántas veces se perdieron 1, 2, 3 y hasta 10 paquetes uno tras otro. Las pérdidas aisladas son mucho menos audibles que las largas rachas de pérdida.

Ambos desglose se muestran por dirección (Llamador y Llamado), por lo que puedes identificar qué pierna tuvo el problema.

Escuchar

El panel **Escuchar** reproduce la llamada grabada en el navegador. El audio se decodifica de los RTP capturados. El llamador es el canal izquierdo y el llamado es el canal derecho, por lo que puedes escuchar cada lado por separado.

Escuchar solo funciona cuando el medio de la llamada fue grabado y su códec puede ser decodificado. Consulta Reglas de Grabación y Retención para saber cómo se arma la captura de medios.

Descarga de PCAP

Cada llamada tiene un botón de **Descargar PCAP**, tanto en la cuadrícula de búsqueda como en el encabezado de detalle de la llamada. La descarga es la captura de paquetes en bruto (SIP y, cuando se graba, RTP) para esa única llamada. Usa el PCAP para inspeccionar la llamada en una herramienta externa como Wireshark.

Llamadas Activas

La vista de **Llamadas Activas** muestra llamadas que están en progreso en este momento. Lee la lista de llamadas en vivo de los agentes de captura y se actualiza en un intervalo corto, por lo que las filas aparecen y desaparecen a medida que se establecen y se desmantelan las llamadas.

La vista de Llamadas Activas. Cada fila es una llamada en vivo con su estado (Conectado o Configuración), las dos partes y sus direcciones IP, la dirección, la duración creciente, el códec, el MOS en vivo y el agente de captura propietario.

Cada fila muestra el **Estado** de la llamada (Conectado, Configuración o Fallando), las dos partes, la ruta de IP del llamador al llamado, la **Dirección**, la **Duración** creciente, el **Códec**, el **MOS** en vivo, la última respuesta SIP y el **Sensor** propietario (agente de captura). Desactiva **Auto-refrescar** para mantener la lista actual.

Sniffer en Vivo

La vista de **Sniffer en Vivo** muestra la salud del servidor de captura central y sus agentes de captura.

La vista de Sniffer en Vivo. El panel del Servidor Central muestra versión, tiempo de actividad, conteo de llamadas activas, rendimiento, caídas de paquetes y carga promedio. La tabla de Agentes de Captura Remota lista cada agente. El panel de I/O de Disco de Spool muestra utilización y rendimiento.

La vista muestra:

- **Servidor Central**: versión y compilación, tiempo de actividad, conteo de llamadas activas, rendimiento de captura, caídas de paquetes, carga promedio y la última vez que se escribió un registro de llamada.
- **Agentes de Captura Remota**: los agentes por elemento y su estado (consulta Agentes de Captura Remota).
- **I/O de Disco de Spool**: la utilización, rendimiento de lectura y escritura, IOPS, latencia, capacidad utilizada y nivel de búfer del disco de spool de captura.
- Un feed de actividad en vivo de las llamadas en progreso.

Observa esta vista para confirmar que el motor de captura está saludable, no está perdiendo paquetes y tiene margen en el disco de spool.

Agentes de Captura Remota

La tabla de **Agentes de Captura Remota** (en la vista de Sniffer en Vivo) lista los agentes de captura que se ejecutan en los elementos IMS. Cada fila muestra:

Columna	Significado
Agente	El nombre de host del agente. Selecciónalo para abrir ese host en la Lista de Hosts.
ID de Sensor	El identificador numérico del agente en el índice de captura.
Estado	Activo, Inactivo o Desconocido, derivado de llamadas en vivo y registros de llamadas recientes.
Llamadas activas	Cuántas llamadas está capturando el agente en este momento.
CDRs	Cuántos registros de llamadas ha producido el agente.
Última vez visto	Cuándo fue la última vez que el agente produjo un registro de llamada.

Usa esta tabla para confirmar que cada elemento IMS que debería capturar está capturando. Un agente que está inesperadamente Inactivo o ausente significa que el tráfico de ese elemento no se está registrando.

Reglas de Grabación y Retención

La vista de **Reglas de Grabación** controla qué llamadas tienen su **medio** grabado y muestra la retención del spool de captura y la base de datos de índices.

La vista de Reglas de Grabación. Las reglas están agrupadas por tipo de coincidencia: Por IP, Por número y Por dominio SIP (también existe un grupo Por encabezado SIP). Cada regla arma la captura de medios RTP, salta un objetivo o guarda los datos del gráfico de QoS.

Reglas de grabación

Por defecto, el motor de captura graba la señalización SIP para cada llamada, pero **no** graba el medio RTP. Una regla de grabación arma la captura de medios para un objetivo específico. El motor de captura vuelve a leer las reglas en vivo, sin necesidad de reiniciar.

Las reglas están agrupadas según cómo coinciden con una llamada:

Grupo	Coincide con
Por IP	Una IP de origen o destino y máscara.
Por número	Un prefijo de número de llamador o llamado.
Por dominio SIP	Un dominio SIP.
Por encabezado SIP	Un valor de encabezado SIP arbitrario.

Cada regla lleva un conjunto de banderas:

Bandera	Efecto
RTP	Arma la captura de medios RTP para el objetivo coincidente. Esto es lo que te permite escuchar la llamada y obtener el PCAP completo de medios. Mantén RTP desactivado globalmente y ármalo por objetivo.
Saltar	Elimina completamente el objetivo coincidente: sin registro de llamada y sin captura. Usa esto para tráfico de prueba conocido.
Gráfico	Guarda los datos del gráfico de QoS de alta resolución para el objetivo coincidente, que impulsa el gráfico de QoS.
rtcp	Registra los informes de calidad RTCP para el objetivo coincidente.
habilitado	Activa o desactiva la regla sin eliminarla.

Para armar la captura para un objetivo, agrega una regla en el grupo de coincidencia, completa el valor de coincidencia y activa **RTP**. Para dejar de grabar tráfico de prueba conocido, agrega una regla con **Saltar** activado.

Retención

El panel de Retención muestra cuánto tiempo se mantienen los datos grabados. La retención se establece centralmente en el servidor de captura. El panel es de solo lectura en OmniWeb.

Los ajustes de retención controlan dos cosas: los límites de tamaño y edad del spool en disco (dividido por SIP, RTP y datos de gráfico), y el límite de edad del índice de llamadas y las filas de calidad por flujo en la base de datos. La tabla a continuación enumera los ajustes que informa el panel:

Ajuste	Significado
`maxpoolsize_gb`	Tamaño máximo total del spool, en GB. Los datos más antiguos se eliminan cuando se alcanza este límite.
`maxpooldays`	Edad máxima de cualquier dato de spool, en días.
`maxpoolsipsize_gb`	Tamaño máximo del spool SIP, en GB.
`maxpoolsipdays`	Edad máxima del spool SIP, en días.
`maxpoolrtpsize_gb`	Tamaño máximo del spool RTP (medios), en GB.
`maxpoolrtpdays`	Edad máxima del spool RTP, en días.
`maxpoolgraphsize_gb`	Tamaño máximo del spool de gráfico de QoS, en GB.
`maxpoolgraphdays`	Edad máxima del spool de gráfico de QoS, en días.
`cleandatabase_cdr_days`	Edad máxima de los registros de llamadas en la base de datos de índices, en días.
`cleandatabase_rtp_stat_days`	Edad máxima de las filas de calidad por flujo en la base de datos, en días.

Los datos de medios (RTP) son grandes. Mantén la retención de RTP más corta que la retención de SIP, y arma la captura de RTP solo para los objetivos que necesitas.

Privacidad e interceptación legal

Grabar el **medio** de la llamada es una decisión de interceptación legal. La captura de señalización registra quién llamó a quién y cuándo. La captura de medios registra el **contenido** de la llamada: el audio de voz. Arma la captura de medios (una regla de grabación **RTP**) solo para los objetivos que estás autorizado a grabar, y solo por el tiempo que estás autorizado.

Mantén la captura de RTP desactivada por defecto y ármala por objetivo. Establece la retención de RTP al período más corto que permita tu política. Sigue tu legislación local de privacidad y reglas de consentimiento tanto para la captura de señalización como de medios.

Cómo se compara Trazado de Llamadas con Homer y Trazado de Sesiones

OmniWeb tiene tres formas de ver la señalización. Alcánzala correcta:

	Trazado de Llamadas (SIP Trace)	Homer (SIP Capture)	Trazado de Sesiones
Alcance	SIP y medios RTP para llamadas IMS	Solo SIP	Toda la red: Diameter, GTP-C, PFCP, SIP, MAP
Pregunta que responde	"¿Qué hizo esta llamada y cuán buena fue la voz?"	"¿Qué hizo el flujo SIP de esta llamada?"	"¿Qué pasó con este suscriptor a través de cada elemento?"
Calidad de voz (MOS)	Sí	No	No
Audio grabado	Sí	No	No
Descarga de PCAP	Sí, por llamada	No	No
Mejor para	Diagnosticar la calidad, medios y flujo de una llamada VoLTE	Una rápida mirada a un flujo SIP	Seguir a un suscriptor de extremo a extremo

Alcanza Trazado de Llamadas cuando debes juzgar la **calidad de voz** de una llamada, escuchar el audio o obtener el PCAP de medios. Alcanza Trazado de Sesiones cuando sigues a un suscriptor a través de toda la pila.

Relacionado

- Registros y Trazado de Suscriptores: el Trazado de Sesiones a nivel de red y la escalera compartida.
- Homer: Captura SIP: la herramienta de captura solo SIP.

- Topología de Red: la Lista de Hosts a la que se vinculan los agentes de captura.

Operaciones Comunes

Cada elemento de red en OmniWeb es diferente por dentro, pero la forma en que *trabajas* con ellos es deliberadamente la misma. Esta página documenta los patrones compartidos por todos los elementos: visualización de datos, edición y cambio de configuraciones de NF, lectura de configuraciones, ejecución de acciones, visualización de registros y comprensión de sondeos y permisos. Aprende estos una vez y se aplican al HSS, al UPF, al SMSC, al MSC y a cada otro NF.

Las capturas de pantalla a continuación provienen de elementos específicos, pero ilustran el patrón *genérico*: los mismos controles aparecen, con diferentes campos, en cada elemento.

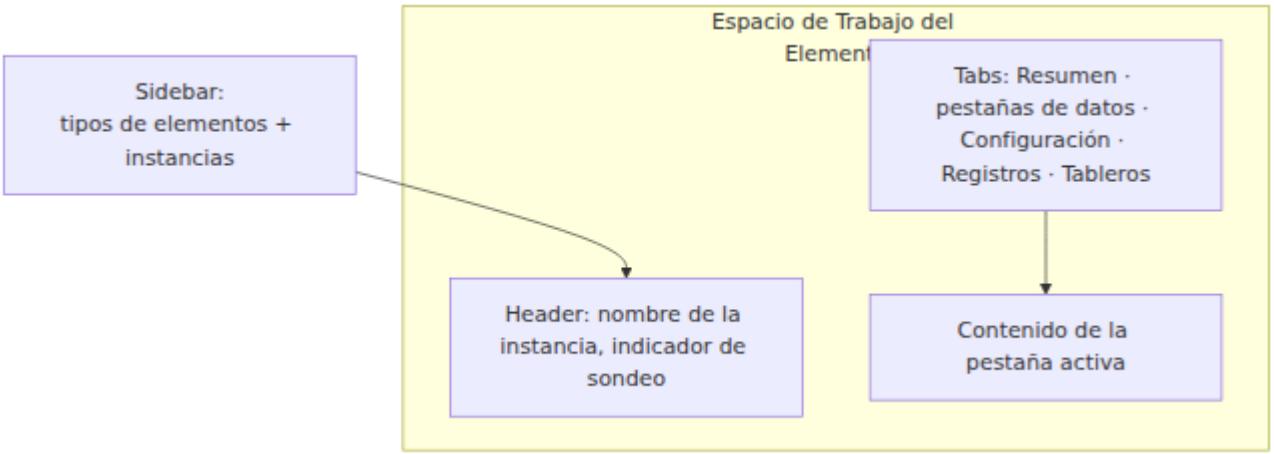
← Volver a la Guía de Operaciones

Tabla de Contenidos

- Anatomía de la Página
- Visualización de Datos
- Vistas Detalladas
- Edición y Cambio de Configuraciones de NF
- Ejecución de Acciones (limpiar, liberar, probar, hacer ping)
- Visualización de Configuración
- Registros en Cada Elemento
- Tableros en Cada Elemento
- Sondeo en Tiempo Real
- Permisos y Qué Puedes Cambiar
- Vistas de Múltiples Instancias y Flota

Anatomía de la Página

Seleccionar una instancia de elemento en la barra lateral abre su espacio de trabajo. Cada espacio de trabajo de elemento comparte el mismo diseño:



- **Resumen**: la pestaña de inicio: salud, conteos clave y estado de componentes para esa instancia.
- **Pestañas de datos**: las vistas específicas del elemento (sesiones, suscriptores, pares, enrutamiento, etc.).
- **Configuración**: una vista estructurada de la configuración en tiempo de ejecución del elemento (donde se expone).
- **Registros**: un visor de registros en vivo de Loki limitado a ese elemento.
- **Tableros**: tableros de Grafana incrustados para ese elemento (cuando las etiquetas de Grafana coinciden).

Las entradas de la barra lateral son enlaces ordinarios, por lo que puedes **Ctrl/Cmd-click** (o clic del medio, o clic derecho → *Abrir en nueva pestaña*) cualquiera de ellos para abrir ese espacio de trabajo en una nueva pestaña del navegador. Esto es útil para observar dos elementos a la vez.

Visualización de Datos

Los datos operacionales se presentan en una tabla consistente y ordenable en todo OmniWeb. Las tablas proporcionan:

- **Ordenación** por columna.
- **Paginación** para conjuntos de resultados grandes.

- **Búsqueda / filtrado** donde la API del elemento lo soporta (por ejemplo, búsqueda por IMSI/MSISDN o IP de UE).
- **Carga esquelética** mientras se obtienen los datos, y un **estado vacío** claro cuando no hay nada que mostrar.
- **Clic en fila** para una vista detallada donde exista.

Los valores están formateados para legibilidad: marcas de tiempo como hora local, duraciones como `h m s`, conteos de bytes como KB/MB/GB, y números grandes con separadores de miles.

El patrón de lista genérico (aquí, una lista de suscriptores): buscable, ordenable, paginada, con clic a través y edición en línea. La misma tabla impulsa sesiones, pares, rutas y cada otro listado.

Las tablas pueden renderizar celdas más ricas: aquí, barras de utilización por fila. El patrón es el mismo; solo difieren las columnas.

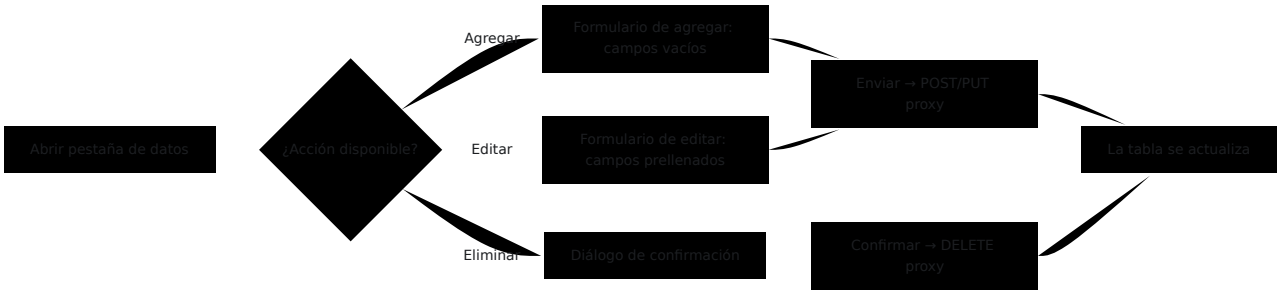
Vistas Detalladas

Donde una fila tiene más que mostrar, haz clic en ella para abrir una vista detallada. Estas reutilizan el mismo diseño (encabezado, sondeo, acciones) pero presentan el registro único en profundidad, por ejemplo, un mapa de relaciones interactivo para un objeto complejo:

Una vista detallada abierta desde una fila de tabla: aquí, un mapa interactivo de las reglas internas de una sesión. Las vistas detalladas se alcanzan de la misma manera en todas partes: haz clic en la fila.

Edición y Cambio de Configuraciones de NF

Dondequiera que la API de un elemento soporte modificación, OmniWeb lo expone a través de un **formulario de acción** consistente. El mismo componente de formulario impulsa "agregar un suscriptor", "agregar una ruta", "editar una regla de QoS" y "cambiar un perfil". Solo difieren los campos.



Los formularios de acción soportan estos tipos de campos: **texto**, **número**, **seleccionar** (desplegable), **booleano** (interruptor), **contraseña** (enmascarada, con un interruptor de mostrar/ocultar), y **texto de varias líneas**. Cada campo puede ser marcado como requerido, llevar un marcador de posición y mostrar texto de ayuda. El formulario muestra un estado de carga mientras se envía y reporta éxito o fracaso a través de una notificación en pantalla.

El método HTTP detrás de cada acción se asigna a un nivel de permiso. Consulta Permisos.

El mismo patrón, tres elementos

Estos ilustran la *misma* mecánica aplicada a diferentes NFs:

Tarea	Dónde	Qué sucede
Agregar/editar un suscriptor	HSS → Suscriptores → Agregar	Completar el formulario (IMSI, MSISDN, perfil, claves) → `POST`/`PUT` proxy → la lista se actualiza
Agregar/cambiar una ruta	SMSC → Enrutamiento → Agregar (o MSC → Enrutamiento)	Completar la regla (patrón, destino, prioridad) → escritura proxy → la tabla se actualiza
Limpiar/liberar una sesión	UPF → Sesiones (o MSC → Llamadas)	Seleccionar el registro → confirmar → `DELETE` proxy → la lista se actualiza

La mecánica es idéntica: formulario o diálogo de confirmación, escritura proxy, actualización de tabla. Solo cambian el elemento y los campos.

Cambiar el enrutamiento es el mismo patrón de edición: la tabla de enrutamiento es una lista que agregas y editas; algunos elementos además analizan destinos en chips legibles y ofrecen un simulador para probar un cambio antes de que entre en funcionamiento.

Ejecución de Acciones

Más allá de CRUD, muchos elementos exponen **acciones operativas** que no encajan en un formulario simple. Estas se presentan como botones que desencadenan una llamada proxy y muestran el resultado en línea. Ejemplos del mismo patrón de botón-acción:

Acción de ejemplo	Elemento	Efecto
Forzar la liberación de una llamada	MSC → Llamadas	Destruye una llamada activa
Hacer ping OPTIONS a un par SIP	MSC → Pares SIP	Prueba la conectividad de un tronco SIP
Probar MAR a un par Diameter	TWAG → Diameter	Envía una Multimedia-Auth-Request de prueba
Activar/desactivar un redireccionamiento	UPF → Jardín Cerrado	Redirige o restaura un suscriptor
Hacer ping desde el nodo	UPF → Diagnósticos	Ejecuta un ping desde el propio elemento
Desconectar una sesión	TWAG → Sesiones	Cierra una sesión WiFi autenticada
Paginación manual	MSC → Paginación	Desencadena una solicitud de paginación

Las acciones destructivas (liberar, eliminar, desactivar) siempre requieren confirmación explícita antes de ejecutarse.

Las acciones operativas aparecen como botones junto a los datos que afectan: aquí, activando/desactivando redireccionamientos de suscriptores y gestionando IPs en la lista blanca. Las acciones destructivas piden confirmación primero.

Visualización de Configuración

Los elementos que exponen su configuración en tiempo de ejecución tienen una pestaña de **Configuración**. OmniWeb la renderiza en un diseño estructurado y legible con un interruptor de **JSON Crudo** para el documento subyacente completo.

Dos comportamientos son dignos de conocer:

- **Los formatos de configuración mixtos se normalizan.** Algunos elementos devuelven la configuración como diccionarios al estilo de Python (`'key': True`, `None`) en lugar de JSON estricto. OmniWeb los analiza en una vista limpia automáticamente y retrocede de manera elegante si no puede analizar un valor.

- **Los secretos están enmascarados.** Cualquier campo cuyo nombre parezca sensible (coincidiendo con `password`, `secret`, `token` o `credential`) se muestra como `***` en lugar de su valor real, tanto en vistas de configuración como en campos de formulario.

La vista de configuración genérica: configuraciones en un diseño estructurado, con un interruptor de JSON Crudo y valores sensibles enmascarados. Los elementos que exponen configuración (UPF, TAS, ePDG, frontends de SMSC, OCS, RAN Monitor) utilizan todos este patrón.

Registros en Cada Elemento

Cada elemento tiene una pestaña de **Registros** respaldada por Loki. Consulta los registros del servicio de ese elemento por host/etiqueta, soporta filtrado estructurado y transmite nuevas líneas a medida que llegan. Debido a que el modelo de registro es idéntico en todos los elementos, se documenta en su totalidad en su propia página:

➡ **Registros y Trazado de Suscriptores**

La pestaña de Registros de cada elemento utiliza el mismo visor: registros estructurados, codificados por colores, transmitidos en vivo de Loki con filtrado de servicio y severidad.

Tableros en Cada Elemento

Los elementos etiquetados para Grafana muestran una pestaña de **Tableros**. OmniWeb descubre tableros coincidentes por etiqueta y los renderiza en línea, para que puedas ver las estadísticas de un elemento sin salir de su espacio de trabajo. Consulta:

➡ **Tableros y Estadísticas de Grafana**

Sondeo en Tiempo Real

Las páginas operativas se actualizan automáticamente. El **Indicador de Sondeo** en el encabezado de cada página muestra:

- **Activo (punto verde)** o **pausado**.

- El **intervalo** (5 segundos por defecto, establecido por elemento a través de `pollIntervalMs`).
- Un **spinner** mientras se está realizando una obtención.
- La **marca de tiempo** de la última actualización exitosa.

El sondeo se puede alternar por página. Las páginas construidas alrededor de acciones interactivas o de una sola vez (consolas, diagnósticos, ejecutores JSON) no son sondeadas por defecto y se actualizan manualmente. Pausa el sondeo cuando desees una vista estable mientras lees una tabla grande o mientras se está realizando un trazado.

Permisos y Qué Puedes Cambiar

Lo que puedes *hacer* en un elemento depende de tu rol. El acceso se concede **por tipo de elemento, por método HTTP**:

Permiso	Métodos permitidos	Uso típico
Solo lectura	`GET`	Ver datos, sin cambios
Lectura-escritura	`GET`, `POST`, `PUT`, `PATCH`	Ver y modificar (agregar suscriptor, editar ruta)
Completo	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	Todo, incluida la eliminación / limpieza

Los permisos se asignan de manera independiente por elemento: podrías tener acceso completo al UPF pero solo lectura en el HSS. Si una acción no está permitida para tu rol, su control no está disponible. Los administradores tienen acceso completo a todos los elementos. Consulta Autenticación y Control de Acceso para gestionar roles, y ten en cuenta que **cada solicitud proxy se registra en auditoría** independientemente del rol.

Vistas de Múltiples Instancias y Flota

Muchos tipos de elementos funcionan como múltiples instancias: varios UPFs detrás de un PGW-C, un par de SMSCs, STPs redundantes. OmniWeb maneja esto a nivel de tipo de elemento: un tipo con más de una instancia configurada obtiene dos modos de navegación.

Selección de Barra Lateral e Instancia

Cuando un tipo tiene múltiples instancias, la entrada de la barra lateral se expande para listar cada una por nombre. Haz clic en una instancia nombrada para abrir directamente el espacio de trabajo de esa instancia. También aparece un desplegable de instancia en el encabezado del espacio de trabajo. Te permite cambiar entre instancias sin volver a la barra lateral, lo cual es útil cuando comparas el comportamiento entre nodos sin perder tu posición en una pestaña particular.

El selector de instancia en la parte superior derecha del encabezado del espacio de trabajo. Abrirlo muestra cada instancia configurada más "Todas las

Instancias" para volver a la vista de flota, sin salir de tu pestaña actual.

Vista de Flota

Haz clic en el nombre del tipo de elemento en la barra lateral (en lugar de una instancia específica), o selecciona **Todas las Instancias** desde el desplegable, para abrir la **vista de flota** para ese tipo. La vista de flota muestra una tarjeta de resumen por instancia con estado de salud y métricas clave, para que puedas evaluar toda la flota de un vistazo antes de profundizar en un nodo específico.

Vista de flota de UPF: una tarjeta por instancia, todas sondeadas en paralelo. Haz clic en cualquier tarjeta de instancia o usa el desplegable para profundizar.

Cuándo Usar Cada Vista

Situación	Uso
Comprobando la salud general de la flota	Vista de flota: todas las instancias de un vistazo
Investigando un nodo específico	Desplegable de instancia o subelemento de barra lateral
Comparando los conteos de sesiones de dos UPFs	Abre cada uno en el desplegable de instancia por turno
Limpiando una sesión en un UPF específico	Navega a esa instancia, luego a Sesiones

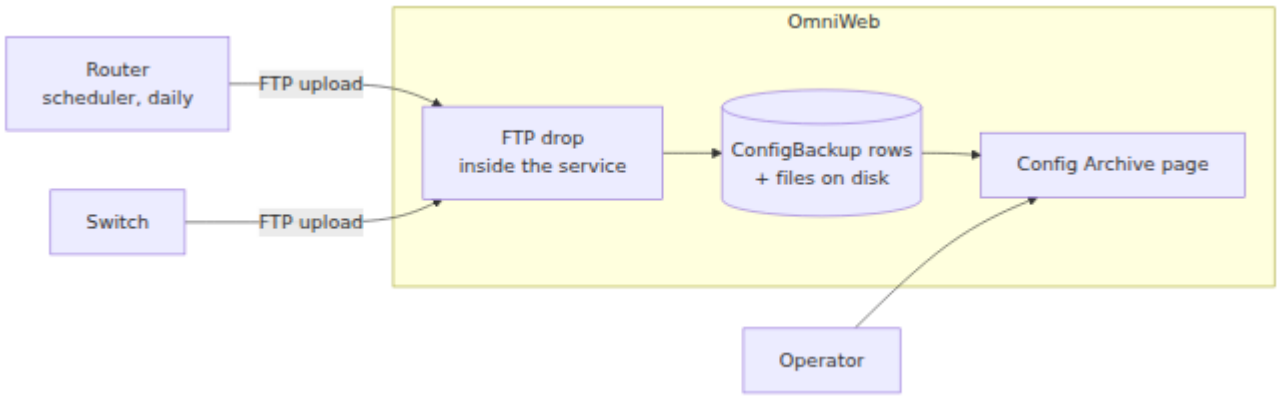
Archivo de Configuración: Copias de Seguridad de Configuración del Dispositivo

Archivo de Configuración mantiene la configuración de cada dispositivo de red que la sube y hace que la colección sea buscable, ordenable y comparable. Un enrutador exporta su propia configuración en su propio horario y la envía a OmniWeb; la página muestra lo que llegó, qué hay dentro y qué cambió desde la última vez.

← Guía de Operaciones

Qué es

Los enrutadores y conmutadores no pueden ejecutar un agente de registro o un cliente de copia de seguridad, pero todos pueden subir un archivo. Así que el archivo convierte esa única capacidad en un registro de cada configuración que ha ejecutado el patrimonio.



La entrega se realiza **dentro del servicio OmniWeb**. No hay un proceso adicional, ningún paquete extra y nada que instalar en el host: el oyente es parte de la aplicación, escrita contra la biblioteca estándar de Python.

Por qué FTP

RouterOS `/tool fetch` sube un archivo a través de FTP o SFTP. También puede enviar un HTTP POST, pero el cuerpo proviene de una variable de RouterOS, y una variable tiene como máximo 4 KB, muy por debajo de una exportación de configuración. Por lo tanto, FTP es el único transporte que tanto los dispositivos como OmniWeb hablan para un archivo de este tamaño.

FTP transporta la contraseña y la configuración en texto claro. Ejecútalo en una red de gestión y restringe las direcciones de origen en el firewall.

Qué acepta la entrega

El oyente implementa la parte de FTP que un dispositivo necesita para entregar un archivo y rechaza el resto.

Acción	Resultado
`STOR` un archivo	Aceptado, donde sea que el dispositivo lo coloque.
`RETR`, `LIST`, `NLST`, `MLSD`	Rechazado. La entrega es solo de escritura: nada puede ser leído de ella a través de FTP.
`DELE`, `RMD`, `RNFR`, `RNTO`	Rechazado. Un dispositivo puede agregar una copia de seguridad y nunca puede eliminar o renombrar una.
`CWD` en un directorio que no existe	Aceptado. El árbol es virtual y la ruta se convierte en el nombre del dispositivo.
`MKD`	Aceptado y no crea nada. Los directorios son implícitos por las subidas.
Una ruta con `..` en ella	Normalizada antes de que cualquier cosa toque el disco. La subida aterriza dentro del archivo.
Una subida que excede el límite de tamaño	Rechazada con `552`, y nada se escribe.

Ambos tipos de archivo son compatibles, y el archivo los trata de manera diferente:

- **Texto**, como un `/export` de RouterOS (`.rsc`), o cualquier `.txt`, `.conf` o `.cfg`. El texto se indexa, por lo que puede ser buscado y comparado.
- **Binario**, como un `/system backup` de RouterOS. El archivo se mantiene byte por byte para restaurar y se marca como binario en la lista.

Identidad: la dirección, no el nombre

La dirección de origen es la identidad. Todo se basa en la dirección de la que realmente provienen los bytes: a qué serie se une una subida, con qué se compara y de quién cuenta la retención. Esto es TCP, por lo que un remitente no puede falsificar la dirección sin tenerla: el apretón de manos debe completarse.

El nombre es solo una afirmación. RouterOS `dst-path=<identity>/<file>` proporciona el primer elemento de la ruta, y un simple `edge-rtr09-20260910.rsc` da `edge-rtr09`. Cualquier remitente puede reclamar cualquier nombre, por lo que el archivo lo almacena, lo muestra y lo busca, y no se basa en él.

Eso es lo que hace que una entrega abierta sea segura de ejecutar:

Alguien sube	Qué sucede
Desde la propia dirección de un enrutador	Se une a la serie de ese enrutador, como su próxima copia de seguridad.
Desde una dirección diferente, reclamando el nombre de un enrutador	Comienza su propia serie al lado de la real. No puede falsificar un cambio en el enrutador real, y no puede inundar la historia del enrutador real hasta que la retención envejezca las copias de seguridad genuinas.
Desde una nueva dirección	Una nueva serie, anunciada una vez en Slack, por lo que un remitente inesperado es visible en lugar de silencioso.

La etiqueta de un origen comienza como lo que sus subidas se llaman a sí mismas, lo cual es conveniente y no confiable. Asigna un nombre veraz al origen para detener las subidas que lo mueven.

El costo de este modelo: un dispositivo que realmente cambia de dirección comienza una nueva serie, por lo que su historia se divide. Asigna etiquetas a ambas, o trata la serie antigua como cerrada.

Configuración

No hay nada que configurar. La entrega se ejecuta en el puerto 2121, abierto, tan pronto como OmniWeb comienza. Apunta un dispositivo hacia él y sube.

Eso es deliberado, no un atajo. Una contraseña no es lo que protege el archivo: FTP la envía en claro, y los enrutadores la mantienen en las mismas configuraciones que suben, por lo que cualquiera que pueda leer el archivo o espiar la red de gestión ya la tiene. Lo que protege el archivo es que un remitente solo escribe en la serie para la dirección que tiene, lo que TCP hace que realmente mantenga. El firewall es el control que importa; restringe el puerto a tus dispositivos.

Establece una contraseña para exigir una además de la verificación de dirección, o `OMNIWEB_CONFIG_ARCHIVE_FTP=0` para mantener la página del archivo sin oyente en absoluto. El resto de la tabla está allí para el sitio inusual, y cada valor a continuación es un valor predeterminado sensato que no necesita ser configurado.

Variable de entorno	Predeterminado	De
`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD`	(vacío)	Establ exigir contra de la v direcci la form ejecut
`OMNIWEB_CONFIG_ARCHIVE_FTP_OPEN`	`1`	Acepta una co Establ contra requer
`OMNIWEB_CONFIG_ARCHIVE_FTP_USER`	`devbackup`	Nombr con el dispos autent
`OMNIWEB_CONFIG_ARCHIVE_FTP_PORT`	`2121`	Puerto Usa 21 servici enlaza privile
`OMNIWEB_CONFIG_ARCHIVE_FTP_HOST`	`0.0.0.0`	Direcc escuch
`OMNIWEB_CONFIG_ARCHIVE_PASV_MIN`	`40000`	Primer datos este ra dispos
`OMNIWEB_CONFIG_ARCHIVE_PASV_MAX`	`40100`	Último datos

Variable de entorno	Predeterminado	De
`OMNIWEB_CONFIG_ARCHIVE_ROOT`	`backend/data/config-archive`	Donde los arc directo dispos
`OMNIWEB_CONFIG_ARCHIVE_MAX_BYTES`	`33554432`	Una su grande rechaz
`OMNIWEB_CONFIG_ARCHIVE_MAX_TEXT_BYTES`	`4194304`	Texto h tamañ para b diferen más gr mantie solame
`OMNIWEB_CONFIG_ARCHIVE_RETENTION_DAYS`	`365`	Una co seguri de est elimin
`OMNIWEB_CONFIG_ARCHIVE_KEEP_MINIMUM`	`10`	Copias más re dispos perma indepe de su
`OMNIWEB_CONFIG_ARCHIVE_FTP`	`1`	Establ para m página pero n oyente

Variable de entorno	Predeterminado	De
`OMNIWEB_CONFIG_ARCHIVE_TIMEOUT`	`120`	Segun que ur de con una tra estanc descar
`OMNIWEB_CONFIG_ARCHIVE_RETRY_SECONDS`	`20`	Con qu un trab perdió intenta nueva también tiempo sin ser entreg que el que la recicla
`OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK`	(vacío)	Webho de Sla signifi notific
`OMNIWEB_PUBLIC_URL`	(vacío)	URL ba este O utiliza vincula de Sla al arch
`OMNIWEB_CONFIG_ARCHIVE_MAX_DIFF_BYTES`	`262144`	La dife grande Un car

Variable de entorno	Predeterminado	De
		grande la fila.
`OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN`	(vacío)	Token Prome preser raspar Vacío l abierta

OmniWeb ejecuta varios trabajadores de gunicorn, y cada trabajador inicia la entrega. Exactamente uno gana el enlace y sirve; los demás esperan y reintentan, por lo que el oyente sobrevive a un reciclaje de trabajador. La página informa `listening_here` por proceso, por lo que un `false` en una solicitud no es un error.

Seguimiento de cambios y Slack

Cada subida se compara con la subida anterior **desde la misma fuente**, del mismo tipo, a medida que llega. El mismo tipo significa la misma extensión, por lo que un dispositivo que envía una exportación de texto y una copia de seguridad binaria cada noche compara cada una contra su propio predecesor en lugar de alternar entre ellas y llamar a todo un cambio. Bytes idénticos significan ningún cambio, sea cual sea el archivo. Bytes diferentes en un archivo de texto producen una diferencia unificada y un conteo de líneas, ambos almacenados en la fila, por lo que la página y la notificación nunca los recalculan. Un archivo binario que difiere se registra como cambiado sin diferencia, porque no hay nada legible para mostrar.

Qué no cuenta como un cambio

Un dispositivo sella su exportación con la hora en que se ejecutó. RouterOS abre cada `/export` con

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

por lo que dos exportaciones de un enrutador sin tocar difieren por esa línea y nada más, y escribe el archivo bajo un nuevo nombre en cada ejecución. Comparado en bruto, cada dispositivo informaría un cambio cada noche, lo publicaría en Slack y enterraría la única señal que vale la pena tener bajo un falso positivo diario por dispositivo.

Así que estas líneas se eliminan antes de que se compare cualquier cosa, y solo para comparar: el archivo almacenado y el texto buscable mantienen exactamente lo que el dispositivo envió.

Ignorado	Por qué
`# <date> <time> by RouterOS <version>`	El encabezado de exportación de RouterOS. Cambia en cada ejecución. RouterOS 7 escribe una fecha ISO (`2026-09-10 11:39:35`), RouterOS 6 escribe `sep/10/2026`; el patrón coincide con la forma que comparten en lugar de con cualquiera de las representaciones.
`# software id = ...`	Presente en algunas exportaciones de RouterOS.
`! Last configuration change at ...`	Cisco IOS. Cambia cuando se escribe algo, incluso por el dispositivo.
`! NVRAM config last updated at ...`	Cisco IOS.
`ntp clock-period ...`	Cisco IOS. Se desvía por sí solo, sin intervención del operador.

El nombre del archivo no es parte de la comparación en absoluto: una subida se empareja con la subida anterior de la misma fuente con la misma extensión,

por lo que un nombre con una marca de tiempo en él no cambia nada.

Establece `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS` a una lista de expresiones regulares separadas por `|||` para reemplazar esta lista para un proveedor que sella algo diferente.

Después de cambiar los patrones, rehace el archivo. Cada copia de seguridad almacena un hash de su configuración normalizada, por lo que un nuevo patrón deja obsoleto cada hash almacenado: la próxima subida de cada dispositivo ya no coincidiría con su propia historia, almacenando un archivo duplicado e informando un cambio que nunca ocurrió.

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

Esa comparación impulsa dos cosas:

- **La página.** Cada fila muestra `+N/-N` cuando la configuración se mueve, o una marca cuando el dispositivo envió el mismo archivo nuevamente. **Cambios solo** reduce la lista a subidas que realmente cambiaron algo.
- **Slack.** Un cambio se publica en un webhook entrante, con la fuente, los conteos de líneas, las primeras 40 líneas de la diferencia y un enlace de regreso al archivo. Una dirección escuchada por primera vez se publica una vez también, nombrando primero la dirección y lo que afirma ser en segundo lugar.

Una copia de seguridad nocturna sin cambios no publica nada. Un patrimonio que realiza copias de seguridad cada noche, de otro modo, llenaría un canal con "no pasó nada", y todos lo silenciarían. Lo que llega en su lugar es solo lo que un operador querría que se interrumpiera.

```
*core-rtr01 (10.64.10.1)* configuración cambiada (+3/-1)
`core-rtr01-2026-09-10-0215.rsc` recibido 2026-09-10 02:15
Copia de seguridad anterior: 2026-09-09 02:15
```

seguido de la diferencia y un enlace al archivo.

Establece `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` a un webhook entrante de Slack para activar esto, y `OMNIWEB_PUBLIC_URL` para que el mensaje se vincule de regreso a este OmniWeb. Sin un webhook establecido, el archivo aún rastrea cambios y la página aún los muestra; nada se publica.

El POST se envía y se olvida en un hilo en segundo plano, por lo que un Slack lento o inalcanzable nunca puede detener una subida o perder una copia de seguridad.

Registro y métricas

Dos hechos, y el monitoreo necesita ambos:

Hecho	Campo	Qué significa el silencio
Escuchamos de él	`last_upload_at`, incrementado en **cada** subida, cambiada o no	Una falla. El dispositivo, su horario o la ruta aquí han dejado de funcionar.
Su configuración se movió	`last_change_at`, incrementado solo en un cambio	Nada. Un dispositivo cuya configuración nunca cambia es un dispositivo saludable.

Alerta sobre el primero y nunca sobre el segundo, o un enrutador estable te enviará un mensaje cada noche.

Contadores (`upload_count`, `change_count`) viven en la fuente en lugar de ser contados desde filas, por lo que la retención de copias de seguridad antiguas no puede hacer que caigan. Un archivo que precede a estos campos se completa a partir de las copias de seguridad que ya tiene cuando se ejecuta la migración.

Raspeo

`GET /api/config-archive/metrics` devuelve la exposición de texto de Prometheus. Es un endpoint simple sin dependencia, y no utiliza la sesión: establece `OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN` y Prometheus lo presenta como un portador. No establecerlo lo deja abierto, y la exposición nombra dispositivos y direcciones, así que configúralo en cualquier cosa alcanzable.

```
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	Descripción
`config_archive_last_upload_timestamp_seconds`	Gauge	Última subida desde esta fuente, cambiada o no. **Esta es la que hay que alertar.** `0` cuando nunca ha subido, por lo que la misma alerta captura un dispositivo que nunca comenzó.
`config_archive_last_change_timestamp_seconds`	Gauge	Última subida cuya configuración difería. `0` cuando nunca ha cambiado.
`config_archive_uploads_total`	Counter	Subidas recibidas desde que se vio la fuente por primera vez. La retención no la reduce.
`config_archive_changes_total`	Counter	Subidas que cambiaron la configuración

Métrica	Tipo	Descripción
`config_archive_retained_backups`	Gauge	Copias de seguridad mantenidas después de la retención.
`config_archive_retained_bytes`	Gauge	Bytes mantenidos después de la retención.
`config_archive_sources`	Gauge	Fuentes de las que el archivo ha escuchado alguna vez.
`config_archive_ftp_enabled`	Gauge	Si la entrega está configurada para ejecutarse.
`config_archive_ftp_bound`	Gauge	Si el socket de entrega está aceptando conexiones en el host. **Alerta sobre este.** Cualquier trabajador puede responder a

Métrica	Tipo	Descripción
		esto, porque se mide con una conexión local.
`config_archive_ftp_listening_here`	Gauge	Si el trabajador que respondió a este raspado es el que sostiene el socket. Solo para depuración: un raspado a través de nginx aterriza en un trabajador arbitrario del grupo, por lo que esto es un lanzamiento de moneda. Nunca alertes sobre esto.

Cada serie lleva `source` (la dirección, la identidad) y `label` (el nombre de visualización, que es solo lo que las subidas afirman hasta que un operador lo fija).

Alertas que valen la pena tener

```
# Un dispositivo dejó de hacer copias de seguridad, o nunca
comenzó. Horario diario más slack.
(time() - config_archive_last_upload_timestamp_seconds) > 172800

# Nadie está sirviendo la entrega.
config_archive_ftp_bound == 0 and config_archive_ftp_enabled == 1

# Un dispositivo que de repente cambia en cada ejecución, lo que
generalmente significa que su exportación
# lleva una marca de tiempo en lugar de que alguien lo esté
editando.
increase(config_archive_changes_total[1d]) > 3
```

Retención

La retención se ejecuta **por fuente**, que es el punto: un remitente llenando su propia serie nunca puede hacer que las copias de seguridad de otro remitente envejezcan. Una copia de seguridad más antigua que la ventana de retención se elimina, excepto que las más recientes de cada fuente siempre permanecen. Un dispositivo que deja de subir, por lo tanto, mantiene su última configuración buena conocida para siempre, y la edad por sí sola nunca vacía la historia de un dispositivo.

Las subidas de la misma **configuración** comparten un archivo en disco, comparadas de la misma manera que los cambios: con la propia marca de tiempo de la exportación y otras líneas volátiles eliminadas. Esto importa más de lo que parece. Una exportación de RouterOS sella la hora en que se ejecutó en su primera línea, por lo que los bytes en bruto difieren cada noche; basar el almacenamiento en ellos escribiría una nueva copia de la configuración de un enrutador sin tocar cada noche para siempre.

Un enrutador que sube una configuración sin cambios cada noche, por lo tanto, aún obtiene una fila cada noche, que es lo que hace visible "escuchamos de él", mientras que los bytes se almacenan una vez.

Configurando un MikroTik

Dos comandos, ejecutados en el enrutador. Establece `<omniweb-host>` a tu dirección de OmniWeb. No se necesita contraseña, y las credenciales a continuación se ignoran: la entrega identifica un dispositivo por la dirección desde la que sube.

```
/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="Exportación de configuración
nocturna al Archivo de Configuración de OmniWeb"
```

Ejecuta una vez a mano para probar la ruta antes de confiar en el horario:

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

Una ejecución exitosa imprime `status: finished` con el tamaño subido, y el dispositivo aparece en el archivo en segundos.

Por qué está escrito así

Detalle	Razón
Todo el script es **una línea**	La CLI de RouterOS rechaza las continuaciones de barra invertida cuando un comando llega a través de SSH. Un script escrito en varias líneas se pega bien en un terminal y falla desde la automatización, con un simple `syntax error (line 1 column N)`.
`policy=read,write,ftp,test`	`fetch` necesita `ftp` y `test`. Sin ellos, la ejecución falla con un error de política y nada se sube.
`port=2121`	El predeterminado de la entrega. `/tool fetch` toma el puerto por separado de la dirección.
`user=omniweb password=x`	Marcadores de posición. La entrega acepta cualquier credencial, porque la dirección de origen es la identidad. `fetch` aún quiere que los argumentos estén presentes.
`[find name=...]` en `/file remove`	`/file remove` toma un id interno, no un nombre. Pasar el nombre directamente falla y la exportación se deja en el enrutador, llenando su almacenamiento con el tiempo.
`:delay 5s` después de `/export`	La exportación se escribe de forma asíncrona. Subir inmediatamente puede capturar un archivo parcial.

Detalle	Razón
`$d` en el nombre del archivo	RouterOS 7 representa la fecha como `2026-09-10`, por lo que el archivo se ordena de forma natural. El nombre cambia en cada ejecución y eso está bien: el archivo coincide una subida contra la anterior de la misma fuente, nunca por el nombre del archivo.

Escalonar `start-time` entre enrutadores para que no todos suban a la vez.

Para mantener una copia de seguridad binaria también, agrega `/system backup save name=$base` y sube `$base.backup` de la misma manera. La exportación de texto es la que se debe diferenciar; el binario es el que se debe restaurar en hardware idéntico.

Cualquier dispositivo que pueda subir a través de FTP funciona de la misma manera: apúntalo al host y puerto y deja que nombre su propio archivo.

Usando la página

Archivo de Configuración está en la barra lateral, bajo Lista de Hosts.

Control	Qué hace
Banner silencioso	Nombra cada fuente que no ha subido en 48 horas, con cuánto tiempo ha pasado. Esta es la verificación, por lo que se activa para un dispositivo que envía copias de seguridad sin cambios solo si deja de enviarlas.
Fuente	Filtra a una dirección de fuente. Cada entrada muestra cuándo fue la última vez que empujó, y marca una silenciosa.
Nombre, dirección o archivo	Búsqueda de subcadena en el nombre reclamado, la etiqueta de origen, la dirección y el nombre del archivo.
Texto dentro de la configuración	Busca las configuraciones mismas, por ejemplo, una dirección IP, `ospf` o un nombre de usuario. Esta es la forma más rápida de encontrar qué dispositivos llevan una configuración.
Encabezados de columna	Ordenar por dispositivo, archivo, hora recibida o tamaño.
Cambios solo	Reduce la lista a subidas que cambiaron la configuración, ocultando las nocturnas sin cambios.
Columna de cambio	`+N/-N` cuando la configuración se movió, una marca cuando el dispositivo volvió a enviar el mismo archivo.
Una fila	Abre la configuración, con una diferencia contra la copia de seguridad anterior de ese dispositivo.
Descargar	El archivo exactamente como lo envió el dispositivo.
Agregar un archivo	Subir una configuración manualmente, para un dispositivo que no puede empujar.

El diff es la parte que se gana su lugar: responde "qué cambió en este router, y cuándo" sin necesidad de iniciar sesión en el dispositivo.

API

Todos los endpoints necesitan una sesión autenticada.

Método y ruta	Descripción
`GET /api/config-archive/backups`	Lista, con `source`, `address`, `q`, `content`, `changed`, `ordering`, `limit` y `offset`.
`POST /api/config-archive/backups`	Agregar una copia de seguridad manualmente: `file` multipart, `device` opcional.
`GET /api/config-archive/backups/<id>`	Una copia de seguridad, con su texto.
`GET /api/config-archive/backups/<id>/download`	El archivo almacenado.
`GET /api/config-archive/backups/<id>/diff`	Diff unificado contra la copia de seguridad anterior, o `?against=<id>`.
`GET /api/config-archive/sources`	Una fila por dirección de origen: conteo de copias de seguridad, cambios, última carga, tamaño, y cada nombre que sus cargas han reclamado.
`PATCH /api/config-archive/sources/<id>/label`	Fijar un nombre veraz a una fuente, para que las cargas dejen de moverlo.
`GET /api/config-archive/status`	Estado de la caída y totales del archivo.
`GET /api/config-archive/metrics`	Exposición de texto de Prometheus. Ver Check-in y métricas.

`changed=1` devuelve el feed de cambios: cargas que difieren de la copia de seguridad anterior del dispositivo.

`ordering` acepta `received_at`, `claimed_name`, `filename` y `size_bytes`, con un `-` al principio para invertir. Cualquier otro valor vuelve a lo más nuevo primero.

Solución de problemas

Síntoma	Verificación
La página advierte que la caída está apagada	`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD` no está configurado. Configúralo y reinicia OmniWeb.
El dispositivo informa un fallo de inicio de sesión	Confirma el nombre de usuario y la contraseña, luego busca `config archive ftp: login failed` en el registro de OmniWeb.
La transferencia comienza y se detiene	El rango pasivo no es accesible. Abre `OMNIWEB_CONFIG_ARCHIVE_PASV_MIN` a `..._MAX` desde el dispositivo.
Las cargas llegan con un nombre reclamado extraño	El dispositivo envió un nombre de archivo simple que no comienza con su identidad. Establece `dst-path` a `<identity>/<file>`, o fija una etiqueta en la fuente.
Un dispositivo aparece como dos fuentes	Su dirección cambió, por lo que comenzó una nueva serie. Fija etiquetas en ambas para hacer obvia la relación.
Aparece una dirección inesperada	Alguien o algo más puede alcanzar el puerto. Verifica el mensaje de Slack "ahora respaldando" para saber cuándo comenzó, y restringe el puerto.
Falta un dispositivo de la lista	Nunca ha completado una carga. Ejecuta el script manualmente en el dispositivo y observa su registro.

Síntoma	Verificación
No llega nada a Slack	Confirma que `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` está configurado, luego verifica si las cargas son cambios: una copia de seguridad sin cambios es silenciosa por diseño. Los fallos se registran como `Slack post failed`.
Slack publica en cada copia de seguridad	El dispositivo estampa algo en cada exportación que no está cubierto por la lista de ignorados. Compara dos copias de seguridad para ver qué se mueve, luego agrega un patrón a `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS`.

DRA: Agente de Enrutamiento Diameter

El **DRA** es el centro de enrutamiento Diameter del núcleo. En lugar de que cada nodo mantenga una malla completa de conexiones Diameter, las funciones EPC e IMS se conectan al DRA y este reenvía y enruta su señalización: **S6a** entre el MME y el HSS, **Gx/Gy** al PCF/PCRF y OCS, **Cx/Dx** y **Sh** para el IMS, y así sucesivamente. Elige a dónde va cada mensaje a partir de las **reglas de enrutamiento** (coincidencia en la aplicación Diameter, dominio o AVP) y un algoritmo de selección de pares, y puede reescribir mensajes con **reglas de transformación**. Es el contraparte Diameter de un STP SS7. OmniWeb muestra los pares del DRA, las reglas de enrutamiento, el estado en vivo y un mapa de conexiones. Los gráficos de rendimiento y tendencias están en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

El DRA es una página de elemento por instancia que se alcanza desde la barra lateral cuando se ejecuta en el inventario del sitio, con una vista de flota (el mapa de la red) donde se despliegan varios. Todo el tráfico pasa a través del proxy backend de OmniWeb hacia la API del DRA, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Mapa de Red

Una vista de hub y radio del DRA y de cada par Diameter que conoce, con el recuento de conexiones de un vistazo (por ejemplo, *5/6 conectados*). Los pares conectados están vinculados al DRA en verde. Un par **deshabilitado** o **desconectado** se muestra en gris y con líneas discontinuas. Es la forma más rápida de ver, en una imagen, qué vecinos de señalización están activos.

Estado

La pestaña de **Estado** informa sobre la propia identidad y configuración del DRA: su **Origin-Host**, **dominio**, la **IP y puerto de escucha** (Diameter suele ser 3868), el **nombre del producto** reportado y el **algoritmo de selección de pares** en uso (por ejemplo, round-robin). Aquí es donde confirmas que el DRA está funcionando y configurado como se esperaba.

Pares

Cada par Diameter, cada fila muestra el **Origin-Host** del par, **IP y puerto**, **producto** reportado, **transporte** (SCTP o TCP), **dominio**, las **aplicaciones Diameter** negociadas y su **estado de conexión**. Los pares se pueden filtrar por nombre, aplicación, dominio o estado. Cada par tiene un interruptor de **habilitar/deshabilitar**. Deshabilitar un par administrativamente lo saca del enrutamiento sin desmantelar su configuración, que es cómo se drena un vecino para mantenimiento.

Reglas

Las **reglas de enrutamiento** y **reglas de transformación** activas, y el **algoritmo de enrutamiento** bajo el cual se ejecutan. Cada regla de enrutamiento coincide con un filtro (una aplicación Diameter, un AVP, o todo el tráfico) y se resuelve a un destino: ya sea un conjunto explícito de pares o una estrategia nombrada como *destination-host* o *destination-realm*. Aquí es donde confirmas, por ejemplo, que S6a se enruta al HSS y Gx al PCF.

Registros

La pestaña de **Registros** muestra en tiempo real la salida del registro del DRA para solucionar problemas de un solo agente de enrutamiento sin salir de OmniWeb.

Paneles de monitoreo

Las tasas de mensajes, el rendimiento por interfaz y otras series temporales para el DRA se presentan como paneles de Grafana, accesibles desde la página

del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- **MME** y el **HSS**: el DRA retransmite **S6a** entre ellos.
- El **PCF/PCRF** (**Gx**) y **OCS** (**Gy**): pares de políticas y cobro enrutados a través del DRA.
- El **CSCF** y **HSS**: señalización IMS **Cx/Dx**.
- **STP**: el contraparte de enrutamiento SS7 del DRA en el plano de señalización.

Servidor de Derechos: OmniSEP

El **Servidor de Derechos** (**OmniSEP**) decide qué servicios puede usar un suscriptor y su dispositivo. Cuando un teléfono solicita si puede activar **VoWiFi**, **VoLTE** o **Wi-Fi Calling**, o realiza la provisión de dispositivo **ODSA** para agregar o activar un dispositivo, consulta al servidor de derechos. El servidor autoriza la solicitud a través de la interfaz de **derechos (TS.43)**, resuelve los datos del suscriptor a través de **Diameter**, y aplica los perfiles de servicio **XCAP** del suscriptor. OmniWeb presenta sus derechos en vivo, actividad, sesiones, tokens, pares de Diameter y perfiles XCAP en una página de elemento; los gráficos de volumen y tendencias se encuentran en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

OmniSEP es una página de elemento por instancia que se accede desde la barra lateral cuando se opera en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del servidor de derechos, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda contextual) abre esta página. Está organizada en pestañas.

Resumen

La pestaña de aterrizaje es una lectura de salud de pantalla única para el servidor de derechos: su **estado del sistema**, el conteo de **sesiones** y **tokens** activos, suscriptores con **derechos** personalizados, y la salud de sus pares de **Diameter**. Es la forma más rápida de confirmar que el servidor está activo y autorizando dispositivos.

Derechos

Los suscriptores que tienen **derechos personalizados**: sobrescrituras del conjunto de servicios predeterminado, por suscriptor. Abre un suscriptor para ver qué servicios están habilitados para ellos. Un operador puede **eliminar todos los derechos** de un suscriptor para devolverlos al valor predeterminado de la red. Esto es útil para limpiar una mala sobrescritura durante un fallo.

Actividad

Los registros de **actividad** recientes: un feed de las solicitudes de derechos que el servidor ha manejado, cada una mostrando el suscriptor o dispositivo, el servicio solicitado y el resultado. Abre un registro para ver su detalle. Esta es la pista de auditoría para confirmar si un teléfono realmente solicitó VoWiFi/VoLTE y qué respuesta se le dio.

Sesiones

Las **sesiones EAP-AKA** activas que el servidor está manteniendo para la autenticación del dispositivo, cada una con su identidad de suscriptor y estado. Una sesión individual puede ser **expirada** desde aquí para forzar a un dispositivo a re-autenticarse. Esta es la forma más rápida de limpiar una sesión que se ha quedado atascada.

Tokens

Los **tokens de autenticación** activos que el servidor ha emitido a dispositivos después de que se autenticaron. Cada token puede ser **revocado** individualmente, lo que retira la autorización de un dispositivo y requiere que se autentique nuevamente. Esto es el equivalente de derechos de forzar un re-login.

Diameter

Los **pares de Diameter** a los que el servidor de derechos se conecta para los datos del suscriptor, con el **estado de conexión** de cada par. Cuando las decisiones de derechos comienzan a fallar por razones que parecen datos de suscriptor faltantes, esta pestaña es donde confirmas que la ruta de Diameter está activa.

Perfiles XCAP

Los **perfiles XCAP**: la configuración de servicio por suscriptor (como la configuración de servicios suplementarios) que el servidor de derechos aplica. Abre un perfil para leerlo. Un perfil puede ser **eliminado** para limpiar la configuración almacenada de un suscriptor y volver al valor predeterminado.

Registros

La pestaña de **Registros** muestra la salida de registro en vivo del servidor de derechos para solucionar problemas de un solo servidor sin salir de OmniWeb.

Paneles de monitoreo

Las tasas de solicitud, contadores por servicio y otras series temporales para el servidor de derechos se presentan como paneles de Grafana, accesibles desde la página de elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- El **HSS** contiene los datos del suscriptor contra los que se resuelven las solicitudes de Diameter del servidor de derechos.
- El **CSCF** y **TAS** entregan los servicios VoLTE/VoWiFi que el servidor de derechos autoriza.
- El **ePDG** y **TWAG** llevan el acceso a Wi-Fi Calling que el servidor de derechos habilita.
- El **DRA** retransmite la señalización de Diameter del servidor de derechos a sus pares.

ePDG: Puerta de Datos de Paquete Evolucionada

El **ePDG** es la puerta de enlace segura para el **acceso Wi-Fi no confiable**: el nodo detrás de la Llamada Wi-Fi (VoWiFi) y los datos de WLAN no confiables. Un dispositivo construye un túnel IPsec/IKEv2 hacia el ePDG a través de cualquier conexión a internet; el ePDG autentica al suscriptor contra el AAA/HSS a través de Diameter (SWm/SWx), ancla la sesión al núcleo de paquetes (S2b al PGW) y aplica límites de tasa por suscriptor y políticas de geo-IP. OmniWeb muestra los túneles activos del ePDG, sus pares de Diameter, la configuración de limitación de tasa y geo-IP, y los ajustes de tiempo de ejecución; las tendencias a largo plazo están en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

El ePDG es una página de elemento por instancia que se alcanza desde la barra lateral cuando se ejecuta en el inventario del sitio. Todo el tráfico pasa a través del proxy backend de OmniWeb, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Resumen

Una lectura de salud en una sola pantalla: el **estado** del ePDG, el número de **sesiones activas** (túneles IPsec) y un resumen del estado operativo de la puerta de enlace. Esta es la confirmación más rápida de que el ePDG está activo y transportando túneles de llamadas Wi-Fi.

Sesiones

Cada sesión activa: los túneles IPsec/IKEv2 actualmente establecidos, clasificados por suscriptor, con el estado del túnel y del portador. Puedes inspeccionar una sesión para ver sus detalles. Aquí es donde confirmas que el túnel de llamada Wi-Fi de un suscriptor específico está activo.

Diameter

Las conexiones de pares Diameter al AAA/HSS que llevan la autenticación (SWm/SWx), con el estado de conexión de cada par. Este es el primer lugar al que mirar cuando las autenticaciones de llamadas Wi-Fi están fallando.

Limitador de Tasa

El ePDG termina túneles IPsec/IKEv2 de Wi-Fi no confiable (SWu) y los conecta al EPC a través de S2b, lo que lo hace expuesto a cualquier dispositivo (o cualquier fuente) en internet abierto. El **Limitador de Tasa** es la defensa contra un cliente que abusa de la configuración del túnel: limita la inundación de IKE para que un solo dispositivo mal comportado o fuente atacante no pueda agotar la puerta de enlace. La pestaña muestra los **umbrales** aplicados junto con un conteo en vivo de cuántas **IPs** y **IMSIs** están **actualmente bloqueados**. Los umbrales son los límites de solicitud **por IP** y **por IMSI**, cada uno expresado como un número de intentos de autenticación dentro de una **ventana** móvil, y la **duración del bloqueo** aplicada una vez que se supera un límite.

Debajo de los umbrales, puedes **buscar** cualquier dirección IP o IMSI para ver si está bloqueada y cuántas fallas ha acumulado, y **limpiar** ese bloqueo para que se permitan futuros intentos de autenticación desde él; una única acción de **Limpiar Todo** elimina todos los bloqueos y restablece todos los contadores de fallas a la vez. Aquí es donde un operador confirma por qué se está rechazando el túnel de llamada Wi-Fi de un suscriptor y libera un bloqueo una vez que la fuente ofensiva se ha estabilizado.

GeoIP

GeoIP es el control de admisión basado en país del ePDG: cómo un operador restringe el establecimiento de túneles VoWiFi a países permitidos al comparar la IP de origen de cada túnel entrante con una base de datos GeoIP. La pestaña muestra si el filtrado está **habilitado** y si la base de datos está **lista** (cargada y utilizable), el **modo**, y la **lista de países** a la que se aplica el modo. El modo es **lista blanca** (solo los países enumerados pueden conectarse) o **lista negra** (los países enumerados son rechazados). También muestra la **base de datos GeoIP en uso** y si se permiten o bloquean **IPs de países desconocidos**. Estas son direcciones de origen que la base de datos no puede resolver a un país.

Una vez que el archivo de la base de datos GeoIP se ha actualizado en el disco, la pestaña puede **recargarlo** para que el nuevo mapeo entre en efecto sin perturbar los túneles establecidos. Este es el control que mantiene la configuración del túnel VoWiFi confinada a las regiones que un operador sirve.

Configuración

La **configuración** de tiempo de ejecución del ePDG, las reglas de **limitación de tasa** (límites por suscriptor / por fuente que protegen la puerta de enlace), y la política de **geo-IP** (qué regiones de origen están permitidas para establecer túneles). Estos son los controles que determinan quién puede conectarse y cuán agresivamente.

Registros

La pestaña de **Registros** muestra la salida de registro en vivo del ePDG para solucionar problemas de una única puerta de enlace sin salir de OmniWeb.

Paneles de monitoreo

Las tasas de túnel, el rendimiento y otras series temporales para el ePDG se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- El **PGW** ancla el plano de usuario del ePDG sobre **S2b**.
- El **AAA/HSS** contiene los datos de autenticación del suscriptor contra los que se resuelven las solicitudes de Diameter del ePDG.
- TWAG: el contraparte de Wi-Fi *confiable*.

Núcleo 5G

La sección **Núcleo 5G** proporciona a cada función de red 5GC (NF) su propio panel en vivo. Cada panel muestra la salud, el registro y los datos operativos que posee la NF (contextos de UE, sesiones PDU, grupos de IP, registros de NRF, políticas, sesiones de carga). También ofrece acciones por NF y por elemento para limpiar el estado. Es el equivalente 5GC de las páginas por elemento para funciones EPC/IMS. Lee la API OAM de cada NF a través del proxy de backend de OmniWeb.

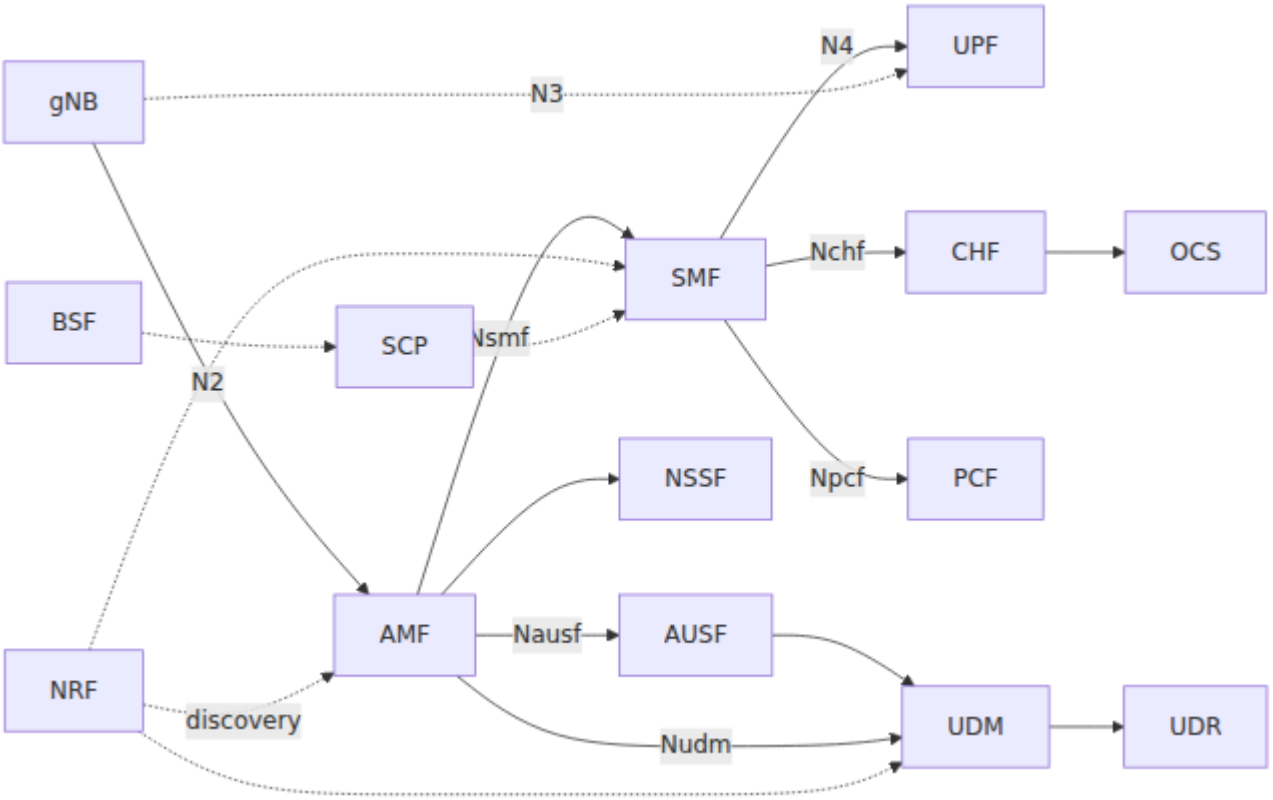
← Guía de Operaciones

Cuándo aparece

El grupo **Núcleo 5G** solo se muestra en la barra lateral cuando el sitio seleccionado realmente ejecuta un plano de control 5GC. OmniWeb basa esto en la presencia de un **AMF y/o SMF** en el inventario del sitio. Un UPF o CHF aislado compartido con el EPC no es un 5GC y no muestra esta sección.

OmniWeb deriva qué NFs aparecen, y la dirección de la API OAM de cada NF, **directamente del inventario de Ansible del sitio**: los grupos de NF 5GC definidos en el archivo de host. Por lo tanto, agregar o mover una NF es un cambio de inventario sin nada que plantillar manualmente. Cada NF se resuelve a una etiqueta, descripción, IP y puerto. OmniWeb sirve el registro resuelto a través de `/api/5gc/nf-registry`. Los paneles luego consultan la API OAM de cada NF a través del proxy (`/api/5gc/nf/<id>/…`), por lo que todo el tráfico permanece detrás de la única puerta de enlace autenticada. Consulta el modelo de configuración. Las implementaciones que no ejecutan inventario (por ejemplo, el servicio alojado) regresan a un bloque estático `fivegc` en la configuración de OmniWeb.

Las NFs



Cada NF tiene su propio panel:

NF	Función	Datos clave expuestos
NRF	Función de Repositorio de Red	Instancias de NF registradas (agrupadas por tipo), servicios registrados, suscripciones: ver abajo
AMF	Gestión de Acceso y Movilidad	Lista de UE, gNodeBs conectados (con gNB-ID / TAC / PLMN / SST decodificados), estadísticas, modo de mantenimiento
SMF	Gestión de Sesiones	Sesiones PDU, **Grupos de IP**, asociación de UPF, estadísticas
UDM	Gestión Unificada de Datos	Lista de UE, estadísticas
UDR	Repositorio Unificado de Datos	Salud de HSS, suscriptores
AUSF	Servidor de Autenticación	Sesiones AUSF (auth), estadísticas
PCF	Control de Políticas	Políticas AM, políticas SM, estadísticas
CHF	Función de Carga	Sesiones de carga, salud de CGrateS, registros CDR
NSSF	Selección de Cortes de Red	Cortes, disponibilidad de NSSAI, estadísticas
BSF	Soporte de Vinculación	Vínculos de PCF, estadísticas
SCP	Proxy de Comunicación de Servicio	Salud de NF, caché de descubrimiento, estadísticas

No todas las implementaciones ejecutan cada NF. Solo aparecen las NFs definidas en el inventario del sitio. Cada NF tiene su propia página de referencia. Sigue los enlaces arriba.

La pestaña de Grupos de IP del SMF

Como un ejemplo de los datos de propiedad de la NF que estos paneles exponen: el panel del SMF tiene una pestaña de **Grupos de IP** que muestra los grupos de direcciones de los cuales el SMF asigna IPs a las UE, junto con sus **Sesiones PDU** en vivo y su **Asociación de UPF** (el estado del enlace N4/PFCP al plano de usuario). Juntos responden a "¿está el SMF conectado a su UPF, qué sesiones están activas y se está quedando sin direcciones?" sin salir de OmniWeb.

Un panel de un vistazo

Cada panel de NF sigue el mismo diseño:

1. **Tarjetas de salud** en la parte superior: Salud de API, Registro de NRF (¿está registrada esta NF con el NRF?), Estado de NF y Licencia. Cada una consulta en un intervalo. Usa el **Indicador de Consulta** en el encabezado para pausar o ver la hora de la última actualización (la consulta es un patrón compartido: consulta Operaciones Comunes).
2. **Acciones**: operaciones a nivel de NF (ver abajo).
3. **Secciones de datos**: el detalle del estado de la API, el detalle del registro de NRF y las tablas específicas de NF de la tabla anterior, cada una actualizándose automáticamente. Las tablas decodifican automáticamente lo que pueden: PLMN/TAC/SST de términos S1AP codificados en Erlang, marcas de tiempo a tiempo relativo, estados a fichas coloreadas y enlaces cruzados (un valor de tipo NF se vincula al panel de esa NF).

Acciones

Los paneles exponen acciones para limpiar el estado de la NF. Cada una pide confirmación primero, ya que son destructivas:

NF	Acciones a nivel de NF	Acciones por fila
AMF	Limpiar todos los contextos de UE · Limpiar caché	Desregistrar una UE
SMF	Liberar todas las sesiones PDU · Limpiar caché · Reasociar PFCP (restablecer la asociación de UPF)	Liberar una sesión PDU
NRF	Desregistrar todas las NFs	Desregistrar una NF · Eliminar una suscripción
AUSF	Limpiar todas las sesiones de autenticación	Limpiar una sesión
UDM	Limpiar caché de suscriptores	-
PCF	-	Eliminar una política AM o SM

Estas permiten a un operador recuperarse de un estado atascado. Por ejemplo, forzar a un SMF que perdió su UPF a reasociarse, eliminar un contexto de UE que no se puede limpiar o desregistrar una NF obsoleta del NRF.

El panel de NRF

El NRF obtiene una vista más rica porque es el registro que todo el 5GC descubre a través de:

- **Tarjetas de métricas**: tipos de NF, total de instancias, registradas (con una barra de porcentaje del total) y servicios/suscripciones.
- **Instancias de NF registradas**: agrupadas por tipo de NF. El panel codifica por colores cada tarjeta de instancia. La tarjeta muestra el estado de registro, el temporizador de latido, el conteo de servicios y PLMN. Haz

clic en una instancia para ver su perfil completo (con un enlace de **Abrir Panel** a esa NF y un botón de **Desregistrar**).
- **Servicios registrados**: una tabla plana de cada servicio que cada instancia publicita, sus versiones y estado.
- **Desregistrar Todas las NFs**: limpia cada registro (cada NF debe luego volver a registrarse).

Esto hace que el NRF sea el lugar para responder "¿qué NFs están activas, todas están registradas y qué servicios están ofreciendo?"

Relacionado

- Topología de Red: las vistas de topología que se vinculan a estos paneles.
- Operaciones Comunes: los patrones de consulta, configuración y RBAC compartidos con cada página de elemento.
- PGW-C / SMF y UPF: las páginas de sesión/plano de usuario del lado EPC para un EPC+5GC convergente.

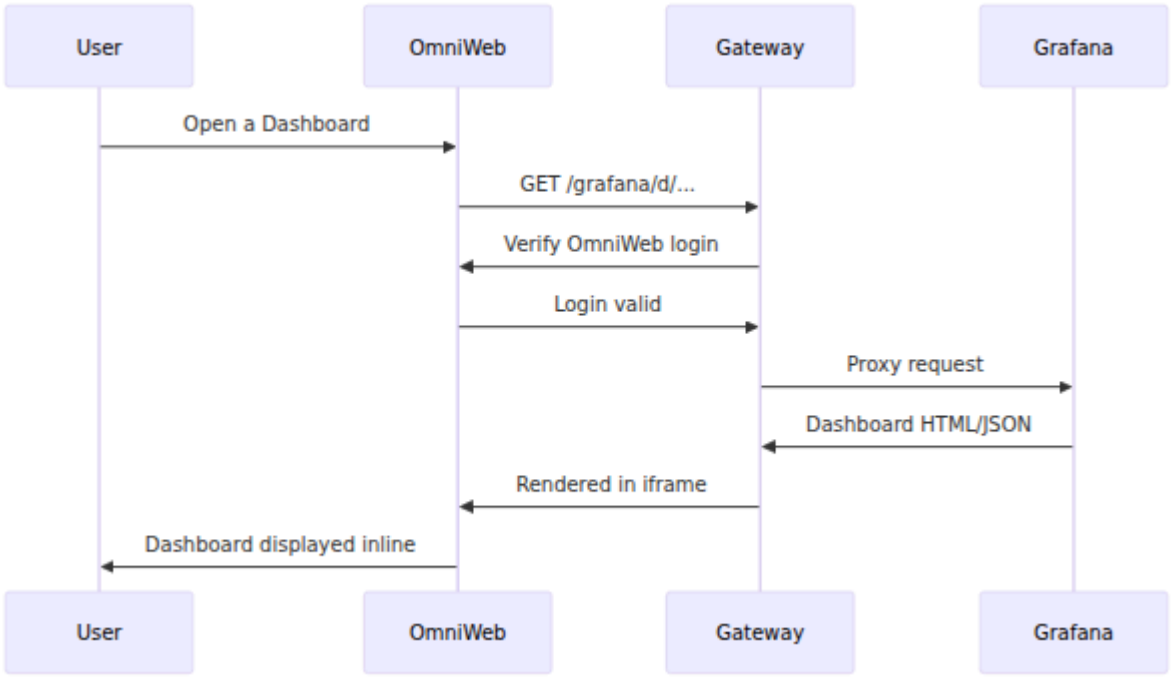
Grafana Dashboards y Estadísticas

OmniWeb integra Grafana directamente en el portal. Los operadores pueden ver dashboards y estadísticas para cualquier elemento y para la red en su conjunto, sin necesidad de un inicio de sesión o pestaña de navegador separada.

← Volver a la Guía de Operaciones

Cómo Funciona

Grafana se sirve detrás del gateway autenticado en la ruta `/grafana/` y se incrusta como un iframe dentro de OmniWeb. La autenticación es transparente: cuando estás conectado a OmniWeb, el acceso a Grafana se autoriza automáticamente contra tu inicio de sesión de OmniWeb. No hay una segunda contraseña.



La instancia de Grafana a la que OmniWeb hace proxy está configurada por la variable de entorno `GRAFANA_URL` (por defecto `http://localhost:3000`). El

gateway maneja el proxy y la verificación de inicio de sesión único de manera transparente.

Dos Maneras de Acceder a los Dashboards

1. Pestaña de Dashboards por elemento

Los elementos que están etiquetados para Grafana muestran una pestaña de **Dashboards** en su espacio de trabajo. OmniWeb consulta a Grafana para obtener dashboards que coincidan con las etiquetas de ese elemento y renderiza el relevante en línea. Esto mantiene las estadísticas de un elemento junto a sus datos operativos.

La coincidencia de etiquetas no distingue entre mayúsculas y minúsculas. Conjuntos de etiquetas representativas:

Elemento	Etiquetas de Grafana coincidentes
UPF	`upf`
P-CSCF	`pcscf`, `cscf`
I-CSCF	`icscf`, `cscf`
S-CSCF	`scscf`, `cscf`
PGW-C, MME, SMSC, DRA, OCS, TAS	etiquetas específicas del elemento

Para hacer que un dashboard aparezca bajo un elemento, etiquétalo en Grafana con la etiqueta de ese elemento (por ejemplo, etiqueta un dashboard de UPF como `upf`).

2. Barra lateral de Grafana

La entrada **Grafana → Dashboards** de la barra lateral lista todos los dashboards disponibles. Seleccionar uno lo abre en línea dentro de OmniWeb, y la URL se actualiza para reflejar la ruta del dashboard, de modo que puedas enlazar a un dashboard específico.

Estadísticas

Los dashboards incrustados son donde viven las **estadísticas** de toda la red y por elemento: conteos y tasas de sesiones, rendimiento, latencia, tasas de caída, salud de pares Diameter/PFCP a lo largo del tiempo, volúmenes de CDR, conteos de registro y tendencias de capacidad. Las propias páginas de elementos de OmniWeb te dan el estado *actual* (y te permiten actuar sobre él); Grafana te da la imagen y las tendencias *históricas*. Están diseñados para ser utilizados juntos. Investiga una alerta de Grafana saltando a las páginas operativas del elemento, registros y trazas.

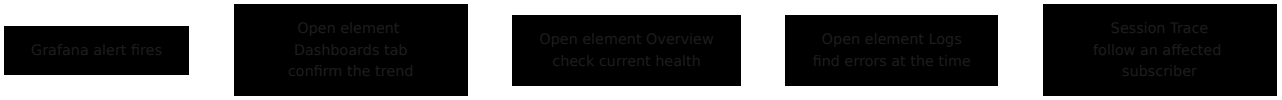
Alertas

El motor de alertas integrado de Grafana maneja todas las alertas basadas en umbrales. Las reglas de alerta se definen en Grafana y pueden notificar a través de correo electrónico, Slack, PagerDuty o webhook. OmniWeb no duplica las alertas. Proporciona el contexto operativo (páginas de elementos, registros, trazas) necesario para investigar cuando se activa una alerta.

Categorías comunes de alertas:

Categoría	Ejemplos
Disponibilidad	Elemento inalcanzable, par Diameter caído, asociación PFCP perdida
Capacidad	Agotamiento de pool de IP, utilización de mapa eBPF > 80%, umbral de conteo de suscriptores de VLR
Rendimiento	Latencia de configuración de sesión, tasa de caída de XDP, fallos de latido
Tráfico	Volumen anormal de CDR, tasa de caída de llamadas, fallos de entrega de SMS

Investigando una Alerta: Flujo Recomendado



1. Confirma la tendencia en Grafana (Dashboards).
2. Verifica el estado actual en la Vista General del elemento.
3. Lee los Registros del elemento alrededor del tiempo de la alerta.
4. Si es específico del suscriptor, ejecuta una Trazabilidad de Sesión. Consulta Registros y Trazabilidad de Suscriptores.

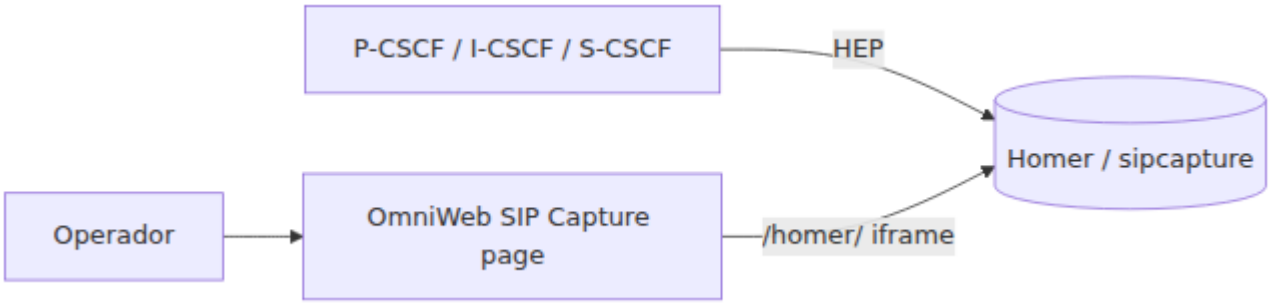
Homer: Captura de SIP y Análisis de Flujo de Llamadas

Homer es un sistema de captura y búsqueda de SIP (HEP / sipcapture). OmniWeb incrusta la interfaz web de Homer directamente, por lo que puedes buscar el tráfico SIP capturado y reconstruir la escalera de señalización de una llamada sin salir del portal o iniciar sesión por separado.

← Guía de Operaciones

Qué es

Homer recopila mensajes SIP del IMS (a través del protocolo HEP) y los almacena de manera que se puedan buscar por call-id, número de origen/destino, tiempo y más. Su interfaz web te permite encontrar una llamada y dibujar su **diagrama de flujo** completo: cada mensaje SIP entre los puntos finales y los CSCFs, con tiempos y cualquier causa de fallo/colgado. OmniWeb no reimplementa nada de esto. **Incrusta la aplicación Homer** en un iframe bajo **Captura de SIP** (anidado bajo Trazado de Sesiones en la barra lateral).



Inicio de sesión único

No inicias sesión en Homer por separado. OmniWeb actúa como proxy de la aplicación Homer en `/homer/` e inyecta los encabezados de auth-proxy en el camino, por lo que la interfaz incrustada ya está **autenticada**, sin un aviso de inicio de sesión de Homer. Se accede a través de la misma puerta de enlace autenticada de OmniWeb que Grafana y Loki, por lo que un inicio de sesión en OmniWeb también lo rige.

La entrada de **Captura de SIP** solo aparece en la barra lateral cuando Homer está **configurado y accesible** para la implementación. OmniWeb lo sondea y oculta la entrada si no está presente, por lo que nunca haces clic en una página muerta.

Homer vs Trazado de Sesiones

OmniWeb tiene dos formas complementarias de ver la señalización, y es útil saber cuál elegir:

	Homer (Captura de SIP)	**Trazado de Sesiones**
Alcance	Solo SIP, en profundidad	Toda la red: Diameter, GTP-C, PFCP, SIP, MAP
Pregunta que responde	"¿Qué hizo el flujo SIP de esta *llamada*, mensaje por mensaje, con tiempo y causa de colgado?"	"¿Qué le sucedió a este *suscriptor* a través de cada elemento?"
Mejor para	Diagnosticar una llamada VoIP/VoLTE, un registro fallido, un colgado específico	Seguir un IMSI/MSISDN de extremo a extremo a través del núcleo

Recurre a Homer cuando tengas una llamada que diseccionar; recurre a Trazado de Sesiones cuando estés siguiendo a un suscriptor a través de toda la

pila. Homer también está vinculado desde la guía de Registros y Trazado de Suscriptores.

Relacionado

- Registros y Trazado de Suscriptores: trazado de sesiones a través de la red y dónde encaja Homer.
- Dashboards y Estadísticas de Grafana: la otra herramienta de monitoreo incrustada, alcanzada de la misma manera autenticada.

HSS: Servidor de Suscriptores en el Hogar

El **HSS** (Servidor de Suscriptores en el Hogar) es la base de datos maestra de suscriptores para el núcleo móvil. Contiene las identidades de cada suscriptor (IMSI, MSISDN y SIM/ICCID), el material de clave de autenticación que prueba quiénes son, y los perfiles de servicio de EPC, IMS, PCRF y roaming que indican lo que cada suscriptor puede hacer en la red. El MME lo lee a través de S6a para autenticar y localizar un dispositivo y para conocer su suscripción a EPC. El CSCF lo lee a través de Cx para el registro IMS y los disparadores de servicio iFC. El PCRF extrae sus políticas y reglas de carga de él. Un operador utiliza su panel de control para aprovisionar y buscar suscriptores, curar los perfiles de servicio compartidos y verificar la salud del HSS.

← Guía de Operaciones

El panel de control es una página de elemento por instancia. Se abre desde la barra lateral cuando un HSS está en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del HSS, por lo que permanece detrás de la única puerta de enlace autenticada. Las respuestas regresan en un sobre `{status, response}`. Un enlace de documentación en el encabezado de la página proporciona ayuda en contexto. La página tiene pestañas.

Suscriptores

La pestaña de inicio es el directorio de suscriptores. Busque **por IMSI, MSISDN o ICCID** para encontrar un registro. La búsqueda también resuelve un suscriptor **por dirección IP** cuando rastrea una sesión activa hasta su propietario. Abra un registro para mostrar la vista general del suscriptor: un diagrama de relación que une al suscriptor con su **identidad** (IMSI), su **estado** (habilitado, y si IMS está habilitado), y los perfiles de **EPC**, **IMS** y **roaming** asignados a él. La página muestra los APNs del perfil debajo del perfil de EPC. El HSS contiene valores clave sensibles pero no los muestra. Puede actualizarlos, pero se leen como redactados.

Aprovisionamiento

Cree o edite un suscriptor desde el formulario de aprovisionamiento. El formulario reúne la identidad, credenciales, SIM y perfiles en un solo lugar:

- **Identidad del suscriptor**: IMSI, un nombre de suscriptor, y los interruptores de **habilitado** y **habilitado IMS**.
- **Conjunto de claves de autenticación**: el algoritmo de autenticación, **Ki** y **OPc** (o **OP**), **AMF**, **SQN**, y la contraseña SIP utilizada para IMS.
- **Tarjeta SIM**: el **ICCID**, si es una eSIM, los valores PIN/PUK y los detalles del lote y proveedor.
- **Números de teléfono**: asigne uno o más **MSISDNs**. Busque números existentes mientras escribe para que no cree un número dos veces.
- **Asignar perfiles**: adjunte los perfiles de **EPC**, **IMS** y **roaming** que le dan al suscriptor su servicio.

Puede actualizar suscriptores existentes de la misma manera. Puede eliminar un suscriptor desde su registro.

SIMs

El inventario de SIM contiene cada **SIM** que el HSS conoce. Búsquelo **por ICCID**. Cada SIM lleva su **ICCID**, bandera de eSIM, nombre del lote y proveedor, sus valores de clave de transporte (**KIC**, **KID**) y eSIM **LPA**, y el conjunto completo de **claves ADM**. Puede crear, editar y eliminar SIMs. Los conjuntos de claves de autenticación con los que se emparejan los registros de SIM se gestionan en su propia pestaña.

MSISDNs

El directorio de MSISDN contiene el grupo de números de teléfono aprovisionados. Busque **por dígitos** para una coincidencia parcial para encontrar o verificar un número antes de asignarlo. Puede crear, editar y eliminar números. Adjunta números a suscriptores durante el aprovisionamiento.

Conjuntos de Claves

El directorio de conjuntos de claves es el almacén de credenciales de autenticación al que apunta cada registro de suscriptor. Cada entrada contiene el **algoritmo** (Milenage o Digest-MD5), el material clave, el **AMF** y el contador de secuencia **SQN**, y el contador opcional de SIM OTA. Filtre la página **por ID, algoritmo o AMF**. Puede crear, editar y eliminar conjuntos de claves.

El material clave es solo de escritura. **Ki**, **OPc**, **OP** y la contraseña SIP nunca se muestran; se leen como redactados, y una edición que deje uno en blanco mantiene el valor almacenado en lugar de borrarlo. Eliminar un conjunto de claves que un suscriptor aún referencia detiene la autenticación de ese suscriptor, así que verifique antes de eliminar uno.

Perfiles de Servicio

Los perfiles de servicio son los bloques de construcción reutilizables que indican lo que un suscriptor puede hacer. Un suscriptor los referencia en lugar de llevar su propia copia. Por lo tanto, un cambio en un perfil se aplica a todos los que lo utilizan.

Perfiles de EPC

La suscripción de núcleo de paquetes que el MME aplica. Un **perfil de EPC** establece el **modo de acceso a la red**, el ancho de banda agregado **downlink/uplink** de UE-AMBR, el **intervalo de TAU**, y la lista de **perfiles APN** que el suscriptor puede utilizar. Un APN es el **APN predeterminado**. Cada **perfil APN** une un **identificador APN** a un **perfil QoS APN** y un **perfil PCRF**. Puede marcar un perfil APN como predeterminado. Un perfil de EPC debe hacer referencia a al menos un perfil APN. El APN predeterminado debe ser uno de los APNs asignados.

Expanda un perfil de EPC para listar sus perfiles APN. **Agregar APN** adjunta un APN al perfil. La acción de desvincular en cada fila **lo elimina solo de este perfil de EPC**. El HSS mantiene el perfil APN en sí. Puede volver a agregarlo más tarde, o otros perfiles de EPC pueden reutilizarlo. Un perfil debe mantener al menos un APN, por lo que no puede eliminar el último. El HSS borra automáticamente el APN predeterminado si elimina el APN al que apuntaba.

Perfiles APN

La pestaña de Perfiles APN lista cada perfil APN independientemente de los perfiles EPC que lo utilizan. Muestra su **identificador APN**, **perfil QoS APN** y **perfil PCRF**. La columna **Usado Por** nombra cada perfil EPC que referencia el APN. Marca el APN como **Huérfano** cuando ningún perfil EPC lo referencia. Un APN alcanza este estado una vez que lo elimina del último perfil EPC que lo utilizó. El conmutador **Solo Huérfano** filtra la lista solo a esos, para que pueda encontrar y limpiar APNs no utilizados.

Puede crear perfiles aquí, editarlos y eliminarlos. Un nuevo perfil comienza sin adjuntar. Para vincularlo al servicio de un suscriptor, agréguelo a un perfil de EPC. No puede eliminar un perfil APN que aún esté vinculado a uno o más perfiles EPC. Primero, elimínelo de esos perfiles, luego elimínelo de esta pestaña.

Perfiles QoS APN

La pestaña de Perfiles QoS APN gestiona las plantillas QoS reutilizables a nivel de APN a las que apuntan los perfiles EPC y APN. Cada suscriptor cuyo APN

referencia una plantilla recibe la misma calidad de servicio en su portadora predeterminada. Cada plantilla lleva un **nombre** y un **QCI** (el Identificador de Clase QoS que mapea la portadora a un comportamiento de retraso y pérdida estandarizado). También lleva un **ARP** (la prioridad de asignación/retenencia), con banderas de **capacidad de pre-empción** y **vulnerabilidad a la pre-empción**. Estas banderas deciden si la portadora puede sobresalir, o ser sobresalida por, otras cuando los recursos son escasos. Cada plantilla también lleva las tasas agregadas de **APN-AMBR** de subida y bajada, y si se habilitan la **carga en línea** y la **carga fuera de línea**.

Puede crear, editar y eliminar plantillas. También puede clonar una plantilla para derivar una nueva variante. Un perfil APN referencia una plantilla QoS en lugar de llevar su propia copia. Si edita una plantilla, remodela la QoS de cada APN que la utiliza. No puede eliminar una plantilla que aún esté referenciada por un perfil APN. Primero, reasigne esos APNs.

Perfiles QoS APN

La configuración de calidad de servicio por APN a la que apunta un perfil APN: el **QCI**, **ARP** y capacidad/vulnerabilidad de pre-empción, el ancho de banda **downlink/uplink** de APN-AMBR, y si se aplican la carga **en línea (Gy)** y **fuera de línea (Rf)**. Puede clonar un perfil para derivar una nueva variante de uno existente.

Perfiles IMS

La suscripción IMS que el CSCF lee a través de Cx. Un **perfil IMS** lleva una **plantilla iFC**: los Criterios de Filtro Inicial que deciden qué servidores de aplicaciones reciben el tráfico SIP de un suscriptor. Puede crear, editar y eliminar perfiles.

IPs Estáticas

Asignaciones de IP fijas para suscriptores que deben recibir siempre la misma dirección, gestionadas junto con los datos de suscripción de EPC.

PCRF

La capa de políticas que aplica el PCRF. Una vista de relación vincula las tres partes:

- **Perfiles PCRF**: la política nombrada a la que referencia el APN de un suscriptor, compuesta por un conjunto de reglas de carga.
- **Reglas de carga**: cada una con un **tipo de regla** y **precedencia**, un **QCI** y **ARP**, límites de MBR/GBR **downlink/uplink**, y un **grupo de calificación** y **identificador de servicio** para la carga. Una portadora dedicada lleva una regla con un MBR o GBR.
- **Reglas de información de flujo**: las plantillas de flujo de tráfico adjuntas a una regla de carga que definen qué paquetes coincide.

Puede crear, editar y eliminar las tres. Si edita una regla de carga, afecta a cada perfil que la utiliza.

Roaming

La política de roaming que el HSS aplica a suscriptores entrantes y salientes. Un **perfil de roaming** establece una **acción de datos predeterminada**, una **acción IMS predeterminada**, y una lista de **reglas de roaming**. Cada regla se basa en un **MCC/MNC** y establece la **acción de datos** y **acción IMS** para esa red. Por lo tanto, puede permitir o bloquear redes visitadas específicas mientras que la acción predeterminada del perfil cubre el resto. Para agregar una regla, use la búsqueda de operadores para encontrar el MCC/MNC de una red a partir de un nombre de operador (de IR.21). Las reglas son compartidas. Si edita una regla, afecta a cada perfil que la utiliza.

EIR

El Registro de Identidad de Equipos. Cada **regla EIR** coincide un **IMEI** por expresión regular y establece una **acción**: permitir o bloquear. Por lo tanto, puede prohibir un modelo de dispositivo o un teléfono específico en la red. Una búsqueda de modelo de dispositivo ayuda a construir el patrón de IMEI. Puede crear, editar y eliminar reglas.

Estado

Una lectura de salud de una sola pantalla del HSS en sí: la salud de la **API**, **base de datos** y **licencia**, y los **conteos de entidades** para total de **suscriptores**, **perfiles EPC**, **perfiles IMS**, **SIMs**, **MSISDNs** y **perfiles de roaming**. Es la confirmación más rápida de que el HSS está activo y cuánto lleva. Las incrustaciones de Grafana proporcionan los paneles de monitoreo y estadísticas.

La pestaña de **Replicación** muestra el estado de la replicación de la base de datos a cualquier instancia HSS par. La pestaña de **Registros** muestra la salida del registro en vivo del HSS. Úselo para solucionar problemas de una sola instancia sin salir de OmniWeb.

Replicación

La pestaña de Replicación lee la salud de replicación de PostgreSQL de la base de datos de suscriptores del nodo HSS y la dibuja como una topología en vivo. Cada nodo muestra si su base de datos es **primaria** o **de respaldo**. Un respaldo es un nodo que está en recuperación. Reproduce los cambios del primario en lugar de aceptar escrituras propias. Para un primario, la pestaña dibuja cada respaldo conectado como un enlace descendente. El enlace muestra la **dirección del cliente** del respaldo, el **slot de replicación** a través del cual transmite, su **estado de transmisión**, y el **retraso de replicación** medido contra la posición WAL actual del primario. La pestaña muestra el retraso en bytes, por lo que un réplica que se retrasa destaca de un vistazo. Si cada slot de replicación está actualmente **activo** determina si su enlace se lee como saludable o roto.

Un operador utiliza esta pestaña para confirmar que la base de datos de suscriptores se replica a través del clúster HSS: que un cambio aprovisionado en un nodo llegará a los demás, y que existe un respaldo al que fallar. Un réplica que se retrasa muestra una cifra de retraso creciente. Un réplica roto o desconectado pierde su enlace. Si dos o más instancias HSS están en funcionamiento pero ninguna de ellas se replica, la pestaña marca todo el

clúster como un vacío de replicación. Corrija esto antes de que se convierta en un riesgo de pérdida de datos.

Operaciones

Dos operaciones a nivel de suscriptor actúan sobre una sesión activa en lugar de sobre el registro almacenado:

- **Cancelar-Ubicación (CLR)**: envía una Solicitud de Cancelación de Ubicación S6a a un MME que sirve a un suscriptor. Esto desata al suscriptor, por lo que se vuelve a conectar y recoge datos de suscripción cambiados.
- **Re-Autenticación PCRF**: solicita que el PCRF reautentique a un suscriptor para una sesión PDN dada. Esto empuja políticas o reglas de carga actualizadas a una sesión activa.

Relacionados

- **MME**: lee los datos de autenticación de suscriptores y de suscripción a EPC a través de **S6a**. Es el objetivo de una Cancelación de Ubicación.
- **CSCF**: lee el perfil IMS y iFC a través de **Cx** para el registro IMS y el disparo de servicio.
- **PCRF / PCF**: aplica los perfiles PCRF, reglas de carga y reglas de flujo mantenidas aquí. Es el objetivo de una Re-Autenticación.
- **UDR**: el almacén de datos de suscriptores compartido que el HSS presenta en un núcleo 5G.
- Guía de Operaciones: volver al índice de elementos.

LCS: Servicios de Localización (OmniLCS)

La función **LCS** proporciona **servicios de localización** para el núcleo. Responde a "¿dónde está este suscriptor?" y activa advertencias de difusión celular. Resuelve la posición de un UE desde la celda de servicio (y la geometría de celda configurada), atiende solicitudes de localización de la red (inmediatas y diferidas), y envía advertencias de **Alertas Móviles Comerciales / difusión celular** a un área. OmniWeb muestra el inventario de celdas del LCS, las fijaciones de ubicación en vivo y recientes, solicitudes de ubicación diferida, alertas y transmisiones CAP; las tendencias a largo plazo están en los tableros de Grafana accesibles desde la misma página.

← Guía de Operaciones

El LCS es una página de elemento por instancia que se accede desde la barra lateral cuando se ejecuta en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Descripción General

Una lectura de salud de pantalla única: el **estado** del LCS, las sesiones de localización **activas** y **completadas**, el número de **celdas cargadas**, y el resultado de **sincronización de celdas**. Esta es la confirmación más rápida de que el LCS está activo y tiene la geometría de celda actual.

La descripción general también muestra cada conexión que el LCS mantiene con el resto del núcleo, cada una con su estado (**Conectado** o **Desconectado**), dirección y, para asociaciones SCTP, el id de asociación y el tiempo en que se activó:

- **Pares SBc-AP**: la asociación de **difusión celular** 4G a cada MME. Una difusión de advertencia 4G solo puede alcanzar las celdas de un MME cuya asociación SBc-AP esté conectada, por lo que esto es lo primero que se debe verificar cuando una difusión no llega a los dispositivos.
- **Pares SLs**: la asociación **LCS-AP** a cada MME, que transporta posicionamiento (E-CID, OTDOA, A-GNSS) entre el LCS y el MME de servicio.
- **Pares Diameter**: las conexiones Diameter SLg/SLh (por ejemplo, al DRA), con el producto del par y los ids de aplicación.

- **Flujos CAP**: cada conexión a una fuente de alerta (ver Flujos CAP), con el tiempo de su último latido o sondeo.

Los cuadros en la parte superior cuentan los pares conectados de cada tipo contra el total configurado, volviéndose rojos cuando alguno está caído.

Celdas

El **inventario de celdas** contra el que el LCS posiciona: el id de cada celda, latitud/longitud, radio, altura, TAC/LAC, PCI, EARFCN, azimut y RAT. Puedes agregar, editar y eliminar celdas aquí. Esta geometría es lo que convierte un id de celda de servicio en una posición.

Agregar o editar una celda

1. Selecciona el **radio** (2G, 3G, 4G o 5G). El diálogo muestra los campos que utiliza ese radio: LAC para 2G/3G, TAC para 4G/5G, y el número de canal correspondiente (ARFCN, UARFCN, EARFCN o NR-ARFCN) y la identidad física de la celda.
2. Ingresa el **ID de Celda** exactamente como lo reporta la red. Para 4G, **Construir ECI desde el ID de eNB** calcula el ECI a partir del ID de eNB y el número de celda.
3. Ingresa el **TAC** o **LAC**. Las difusiones de celdas para esta celda van a este código de área.
4. Coloca la celda: haz clic en el mapa, arrastra el marcador, o escribe o pega la latitud y longitud (`lat, lon` pegado en cualquiera de los cuadros llena ambos). Establece el **radio** de cobertura y, para una antena sectorizada, el **azimut**; el mapa muestra la cobertura resultante.

Cada valor se verifica contra su rango válido antes de que la celda pueda ser guardada. Una alerta CAP llega a una celda cuando la posición de la celda está dentro del área de alerta, por lo que una celda sin posición, o con el TAC o LAC incorrecto, no recibe alertas.

Ubicación

Fijaciones de **ubicación recientes**: el suscriptor de cada fijación, la celda resolvente, la posición calculada, la precisión y el método. Se puede **solicitar** una ubicación para un suscriptor desde aquí, y abrir una fijación muestra su posición autoritativa conocida más reciente. Aquí es donde un operador confirma un resultado de posicionamiento.

Diferido

Las **solicitudes de ubicación diferida pendientes** que el LCS está manteniendo. Donde la pestaña Ubicación responde "¿dónde está este suscriptor *ahora*", una **MT-LR diferida** (solicitud de ubicación móvil terminada diferida) pide a la red que informe la posición de un suscriptor **más tarde, cuando se active un disparador**, en lugar de inmediato: el GMLC arma la solicitud y el informe regresa cuando se cumple la condición. Los disparadores comunes son **disponibilidad de UE** (informa la próxima vez que el dispositivo se vuelva accesible, habiendo estado inactivo o inaccesible cuando se hizo la solicitud), ubicación **periódica** (informa a un **intervalo** fijo por un **número** establecido de reportes), y eventos de área/movimiento (informa cuando el UE entra, sale o se mueve dentro de un área designada). Así es como un operador programa el posicionamiento para un suscriptor que no se puede encontrar en ese momento o que necesita ser rastreado a lo largo del tiempo.

Cada fila lista el suscriptor de la sesión diferida por **IMSI**, su **tipo** (periódico o activado), el **método** de posicionamiento, su programación (el intervalo de reporte para una sesión periódica; el evento de área y el intervalo de sondeo para una activada), los **reportes restantes** del total, su **estado**, el cliente

solicitante, cuándo **comenzó** y el tiempo de la **última fijación**. Una sesión activada sin límite de reportes muestra *infinito* reportes restantes.

Un operador puede **crear** una nueva solicitud diferida desde aquí, nombrando el IMSI objetivo, el tipo y el método de posicionamiento (celda, E-CID, GNSS u OTDOA):

- **Periódico**: el intervalo de reporte en segundos y el número de reportes a enviar.
- **Activado**: el evento de área (**entrando**, **saliendo** o **estando dentro**), el área en sí (un círculo dado por su centro y radio en metros, o un polígono de al menos tres puntos de latitud/longitud), el número máximo de reportes (0 para ilimitado) y con qué frecuencia el LCS sondea la posición del suscriptor.

Un operador también puede **cancelar** una sesión pendiente en cualquier momento, lo que desarma la solicitud armada para que no se produzcan más reportes. La lista se sondea para que el estado de una sesión se actualice a medida que la red la arma y se activa el disparador.

Alertas CAP

Las alertas del **Protocolo Común de Alertas (CAP)** que el LCS ha aceptado para difusión celular, en tres grupos:

- **Aprobación pendiente**: alertas esperando a un operador. **Aprobar** difunde la alerta a las celdas dentro de su área de advertencia; **Rechazar** la elimina.
- **Activas**: alertas que se están transmitiendo. **Detener Difusión** quita una alerta del aire en cada red en la que se envió.
- **Historial**: alertas que fueron enviadas, rechazadas, **canceladas** (por la autoridad emisora o un operador) o **expiradas**.

Cada alerta muestra de dónde proviene (un flujo CAP o una presentación manual), el identificador CAP y el remitente, y una línea por **idioma**: el idioma, el **identificador de mensaje** de difusión celular por el que se envía y el texto enviado a los dispositivos. Cuando se ha enviado una alerta, cada línea también muestra el número de serie y el resultado por red. El pie de página proporciona el código de red, los TACs/LACs objetivo, cuántas celdas coincidieron con el área de advertencia, y cuándo se recibió, envió, aprobó, expiró y finalizó la alerta.

Las alertas llegan automáticamente de los flujos CAP, o un operador puede **Enviar Alerta** con XML CAP. No todos los mensajes CAP son para dispositivos. El LCS aplica las reglas de alerta a continuación, y una presentación que no califica se informa en lugar de ser encolada:

- solo se difunden alertas **Actuales** con alcance **Público**. Los mensajes de prueba que no están destinados a la difusión son ignorados;
- para alertas canadienses (CAP-CP), solo se difunden bloques de información marcados para distribución inalámbrica, utilizando su texto inalámbrico;
- cada idioma se envía como su propia difusión: el idioma principal en el identificador de mensaje configurado (4370 por defecto) y cada otro idioma en el identificador de idioma adicional correspondiente (4383);
- una **Cancelar** o **Actualizar** de la autoridad emisora detiene la difusión de la alerta anterior, y una alerta deja de difundirse cuando **expira**;
- la misma alerta (mismo remitente e identificador) solo se procesa una vez.

Flujos CAP

Los **flujos CAP** de los que el LCS recibe alertas. Se admiten dos tipos:

- **Flujo NAAD (Canadá)**: el Sistema Nacional de Agregación y Difusión de Alertas de Pelmorex (NAAD). El LCS se conecta a cada sitio de transmisión a la vez (los dos sitios brindan redundancia) y espera un latido de cada uno cada minuto; un sitio que queda en silencio se vuelve a conectar. Cada latido lista las alertas más recientes, y cualquier alerta que no llegó por el flujo se obtiene del archivo NAAD, por lo que una alerta emitida mientras una conexión estaba caída aún se recibe.
- **Flujo Atom CAP**: un flujo CAP en formato Atom, sondeado a un intervalo establecido.

Cada flujo muestra si está habilitado, su configuración de aprobación y, para cada sitio o URL, el **estado de conexión**, el tiempo del último latido (o sondeo) y contadores: alertas y latidos recibidos, alertas **enviadas** para difusión, **ignoradas** (no para dispositivos), **canceladas**, **duplicadas** (la misma alerta del otro sitio) y alertas **rellenadas** desde el archivo.

Agregar Flujo crea un flujo. El botón **Canadá — Pelmorex NAAD** completa ambos sitios de transmisión NAAD y ambas direcciones de archivo. Para cada flujo, estableces su nombre, tipo, URLs, si está habilitado y su comportamiento de **aprobación**: usar la configuración a nivel de LCS, requerir que un operador apruebe cada alerta, o difundir sin aprobación. Los flujos agregados aquí pueden ser editados, habilitados o deshabilitados, y eliminados. Los flujos definidos en la configuración del LCS están marcados como **Desde configuración** y son de solo lectura aquí.

Difusiones

La pestaña **Difusiones** muestra los mensajes de **difusión celular** que el LCS está enviando, una fila por red: el identificador de mensaje y su nombre (los identificadores de prueba y ejercicio están marcados como **prueba**), el número de serie, la red (2G sobre CBSP, 3G sobre SABP, 4G sobre SBc-AP), el texto del mensaje, su estado y cuándo fue enviado. La vista de **Historial** lista las difusiones pasadas, incluyendo su tipo de advertencia.

El número de serie se muestra en hexadecimal con su **código de mensaje** y **número de actualización**; pasa el cursor sobre él para ver el alcance geográfico. Un dispositivo muestra un mensaje solo una vez para cada identificador de mensaje y número de serie. Una fila donde se enviaron el mismo identificador y número de serie más de una vez se marca como **duplicado – los dispositivos ignoran**: los dispositivos que recibieron el primer envío no mostraron los posteriores.

Un operador puede **detener** una difusión activa desde su fila; la detención se aplica solo a la red de esa fila, por lo que un mensaje enviado tanto en 3G como en 4G se detiene en cada uno por separado.

Enviar Difusión inicia una nueva:

- **ID de Mensaje**: selecciona de la lista 3GPP (ETWS terremoto/tsunami, CMAS/WEA presidencial, extremo, severo, AMBER, prueba mensual, ejercicio, definido por el operador, seguridad pública, prueba estatal/local) o ingresa un valor personalizado. Para identificadores ETWS, elige el **tipo de advertencia** ETWS.
- **Idiomas**: el texto del mensaje, más cualquier número de **idiomas adicionales**. Cada idioma adicional se envía en el identificador de idioma adicional que coincide con el elegido (por ejemplo, 4370 → 4383), con el mismo número de serie, y se informa el resultado de cada idioma. Los identificadores ETWS y personalizados no tienen identificador de idioma adicional. Debajo de cada texto, un contador muestra la codificación (GSM de 7 bits, o UCS-2 cuando el texto tiene caracteres como algunas letras acentuadas) y las páginas utilizadas, hasta 15.
- **Número de serie**: construido a partir del **alcance geográfico**, un **código de mensaje** (0–1023) y un **número de actualización** (0–15). Una nueva alerta obtiene el siguiente código de mensaje que aún no se ha utilizado para ese identificador. **Enviar como actualización de…** selecciona una difusión anterior y mantiene su código con el número de actualización incrementado en uno, por lo que los dispositivos reemplazan el mensaje

anterior. Aparece una advertencia cuando el identificador y el número de serie ya fueron enviados, porque los dispositivos ignorarían el mensaje.
- **MCC y MNC** de la red a la que se está transmitiendo (siempre requerido, para que una difusión nunca se envíe bajo el código de red incorrecto), las redes a enviar, y los **TACs** (4G), **LACs** (2G/3G) y **SACs** (3G) objetivo para las redes seleccionadas.
- Con qué frecuencia y cuántas veces se repite el mensaje (0 repeticiones hasta que se detenga).

Registros

La pestaña **Registros** muestra en tiempo real la salida de registro del LCS para solucionar problemas sin salir de OmniWeb.

Tableros de monitoreo

Las tasas de solicitudes de ubicación y otras series temporales se presentan como tableros de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- El **MME** solicita posicionamiento a través de las interfaces de ubicación y es el par Diameter del LCS.
- Las **alertas CAP** y las **difusiones** alimentan el sistema de advertencia de difusión celular.

Servidor de Licencias: Licenciamiento de Omnitouch

El **Servidor de Licencias** es la autoridad de licencias de Omnitouch contra la que los funciones de la red verifican. Cada producto de Omnitouch (el MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF y el resto) valida su derecho contra el Servidor de Licencias antes de ejecutarse, preguntando si un **licenciatario** dado está autorizado para ese **producto** y si la licencia sigue dentro de su ventana de validez. El servidor mantiene **licencias firmadas** criptográficamente, cada una otorgando a un licenciatario un conjunto de productos con un período de validez y metadatos, y responde a consultas de derechos y registra cada solicitud que se le hace. Debido a que una licencia solo tiene sentido contra un reloj confiable, el servidor también rastrea una fuente de **tiempo confiable** para que una licencia no pueda ser revivida retrocediendo el reloj de un nodo. OmniWeb muestra lo que está licenciado y su estado, el registro de solicitudes de derechos que han hecho las funciones de la red, una herramienta de consulta bajo demanda y los registros en vivo del servidor.

← Guía de Operaciones

El Servidor de Licencias es una página de elemento por instancia que se accede desde la barra lateral cuando se ejecuta en el inventario del sitio, con una vista de flota donde varios están desplegados. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del Servidor de Licencias, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Resumen / Estado

Una lectura de pantalla única de lo que el servidor está licenciando y si está saludable. Las tarjetas de resumen dan el conteo de **productos totales**, cuántos son **válidos** e **inválidos**, y el número de **licenciatarios** distintos. Un panel de **tiempo confiable** muestra el estado de la fuente de reloj del servidor: **válido**, **período de gracia** o **inválido**. Cuando el tiempo confiable no está disponible, el servidor no puede validar licencias de manera segura, y eso eleva la salud de la página a una advertencia o error.

La tabla de **Productos Licenciados** lista una fila por cada producto licenciado, cada una mostrando el **producto**, el **licenciatario** al que se le otorga, cuándo fue **emitido**, sus fechas de **inicio** y **expiración** (con un indicador de "días restantes" o "expirado hace N días" que se vuelve ámbar dentro de los 30 días antes de la expiración y rojo una vez pasado), y su estado **válido/inválido**. Abrir una fila expande el detalle completo: las marcas de tiempo exactas de validez, si la **firma criptográfica** es válida, cualquier metadato del producto y la firma misma. Esta es la confirmación más rápida de que las funciones de la red están todas licenciadas y que nada está a punto de caducar.

Registros de Solicitudes

La pista de auditoría de las **solicitudes de derecho** que las funciones de la red han realizado contra el servidor. Cada fila registra la **marca de tiempo**, la **IP de origen** de la que provino la solicitud (qué host de función de red preguntó), el **licenciatario** y el **producto** sobre el que preguntó, la **decisión** (**permitido** o **rechazado**), y, para un rechazo, la **razón**. La lista se puede filtrar por decisión, por producto y por una búsqueda parcial de **IP de origen** o **licenciatario**, y está paginada. Aquí es donde puedes ver, por ejemplo, que una función recién desplegada está siendo rechazada porque su producto nunca fue licenciado, o confirmar que una función está verificando correctamente.

Consulta de Licencia

Una **verificación de derecho** bajo demanda. Ingresa un **licenciatario** y un **producto** y la herramienta pregunta al servidor la misma pregunta que haría una función de red (¿está este licenciatario autorizado para este producto en este momento?) y devuelve el veredicto: **válido** o **inválido**, la fecha **válido hasta** de la licencia, la **marca de tiempo** de respuesta, cualquier **metadato**, y la **firma**. Es la forma directa de confirmar un derecho específico sin esperar a que la función propietaria verifique, y lista los identificadores de producto conocidos (por ejemplo `omnihss`, `omniupf`, `omnimme`) para que puedas consultar el exacto.

Registros

La pestaña de **Registros** muestra la salida de registro en vivo del Servidor de Licencias para solucionar problemas de una sola instancia sin salir de OmniWeb.

Relacionado

- **Cada función de red de Omnitouch**: el MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF y el resto validan su derecho aquí; la propia pestaña de **Resumen / Estado** de cada producto muestra una insignia de salud de licencia derivada de esta verificación.
- Guía de Operaciones: volver al índice de elementos.

Registros y Trazado de Suscriptores

OmniWeb ofrece a los operadores varias vistas complementarias y en tiempo real sobre lo que está haciendo la red:

1. **Registros**: registros de servicio estructurados y en vivo para cualquier elemento, impulsados por Loki.
2. **Trazado de Sesiones**: una vista a través de la red que sigue a un suscriptor a través de cada protocolo y elemento (Diameter, GTP-C, PFCP, SIP, MAP).
3. **Homer**: captura profunda de paquetes SIP/VoIP y análisis de flujo de llamadas.

← Volver a la Guía de Operaciones

Saltar a un Suscriptor desde un NF

Muchas funciones de red muestran un suscriptor, UE o sesión por IMSI. Estos incluyen el **MME** (UEs), **SGW-C**, **PGW-C** y **ePDG** (Sesiones), **MSC** y **TAS** (Suscriptores), y **SMSC** (Ubicación). En cada caso, una fila de botones de enlace rápido te permite pivotar directamente a ese suscriptor en otro lugar, sin necesidad de copiar el IMSI:

- **Ir al Registro HSS** abre el registro de aprovisionamiento del suscriptor en el HSS (resuelto por IMSI a través de las instancias de HSS configuradas).
- **Ver Trazado de Sesión** abre la escalera de señalización en vivo del suscriptor en Trazado de Sesión, limitado a ese IMSI.
- **Ver Registros** abre la pestaña de Registros de *este* elemento prefiltrada a ese IMSI, por lo que solo ves las líneas de registro para ese suscriptor.

Cada botón solo aparece cuando aplica: el IMSI es conocido y se ha configurado un HSS o Trazado de Sesión para el sitio. Por lo tanto, el conjunto se adapta al

despliegue.

Los enlaces rápidos de suscriptor (aquí en un MME UE): un clic al registro HSS, la escalera de señalización en vivo, o los registros de este elemento filtrados al suscriptor.

Registros en Tiempo Real (Loki)

Cada elemento tiene una pestaña de **Registros**. Consulta los registros de servicio del elemento desde Loki y transmite nuevas líneas a medida que llegan, para que puedas ver un elemento en vivo mientras realizas un cambio o reproduces un problema.

La pestaña de Registros (aquí en un UPF): líneas de registro estructuradas y codificadas por colores transmitidas desde Loki, con filtros de servicio, severidad, protocolo y suscriptor (IMSI). Cada elemento expone el mismo visor.

Cómo funcionan las consultas de registro

El frontend construye una consulta LogQL y la envía a través de la puerta de enlace Loki del backend. Nada consulta a Loki directamente desde el navegador. Se proxied (y, por lo tanto, autenticado y auditado) como cualquier otra solicitud.



El objetivo de Loki del backend se establece mediante la variable de entorno `LOKI_URL` (por defecto `http://localhost:3100`). Las consultas utilizan la API de consulta de rango de Loki con una expresión LogQL, una ventana de tiempo, un límite de resultados y una dirección (nuevo primero o más antiguo primero).

Selectores vs. filtros de canalización

OmniWeb construye consultas estructuradas a partir de dos tipos de filtros:

Ubicación del filtro	Posición de LogQL	Ejemplo	Uso
Selector	Dentro del selector de flujo `{ … }`	`{hostname="omni-eval-upf01"}`	Elegir qué flujos (qué host/servicio) leer. Indexado y rápido.
Pipeline	Después de un `|`	`| level="error"`	Filtrar las líneas coincidentes por un campo estructurado.

Una pestaña típica de Registros de elemento fija el host/servicio como selector y te permite agregar filtros de canalización (severidad, componente, identificadores de suscriptor) encima. Debido a que los servicios de Omnitouch emiten líneas de registro **estructuradas**, puedes filtrar en campos reales en lugar de buscar texto libre.

Datos de registro estructurados

Los hosts envían registros estructurados a Loki (configurados por el rol común de Ansible). Dos fuentes estructuradas especialmente útiles:

- **Registros de servicio**: la propia salida estructurada de cada NF, etiquetada por `hostname`/servicio, disponible en la pestaña de Registros de ese elemento.
- **Auditoría de comandos**: cada comando ejecutado en un host, incluyendo quién inició sesión (sobreviviendo a `sudo`/`su`), el UID efectivo, el binario, el directorio de trabajo y la línea de comandos completa. Enviado a Loki. Consulta Registro de Auditoría para la referencia de campos.

Uso de la pestaña de Registros

1. Abre cualquier elemento y selecciona **Registros**.
2. El visor carga líneas recientes para ese elemento y comienza a consultar nuevas.
3. Reduce la vista con filtros de canalización (por ejemplo, severidad, o un IMSI/MSISDN si los registros de servicio lo incluyen).
4. Ajusta la ventana de tiempo para mirar un evento pasado.
5. Pausa la consulta (indicador de encabezado) para mantener una vista estable mientras lees.

> **Consejo:** Al investigar un suscriptor, filtrar los registros de elementos por su IMSI/MSISDN es el primer paso rápido; para ver al suscriptor a través de *múltiples* elementos a la vez, utiliza el Trazado de Sesión a continuación.

Trazado de Sesiones: Seguir a un Suscriptor a Través de la Red

El motor de **Trazado de Sesiones** correlaciona la señalización para un solo suscriptor a través de múltiples elementos y protocolos, proporcionando una línea de tiempo unificada desde el adjunto de radio a través de la autenticación, establecimiento de sesión y entrega de llamadas/SMS. Esta es la herramienta para responder "¿qué le pasó a este suscriptor?" sin saltar entre las CLIs de los elementos.

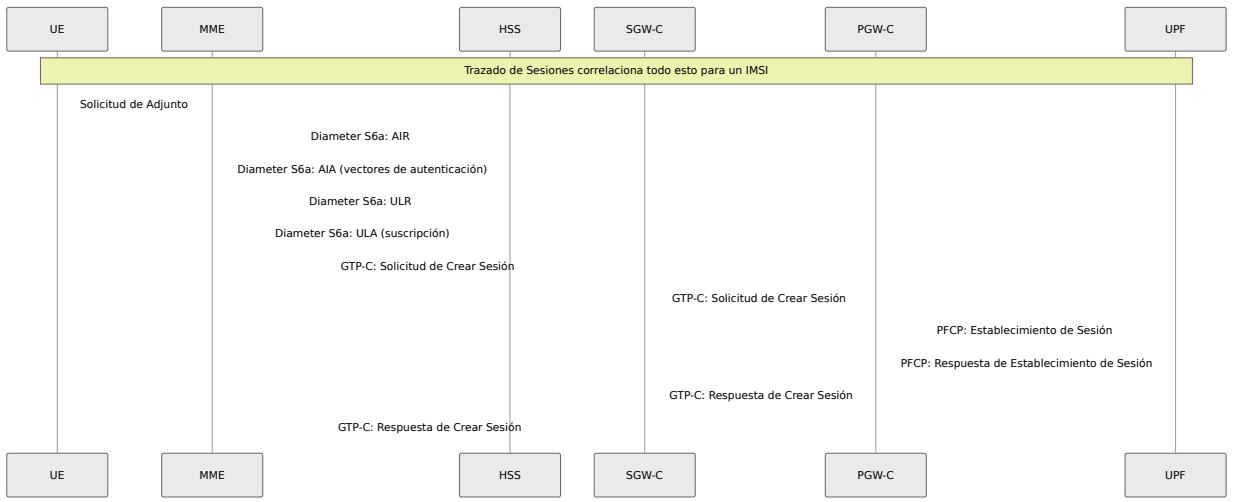
Trazado de Sesiones: busca por IMSI o MSISDN y correlaciona la actividad de un suscriptor a través de Diameter, GTP-C, PFCP, SIP y MAP, con pestañas por protocolo en la parte superior.

Protocolos soportados

Protocolo	Lo que muestra	Elementos involucrados
Diameter	Autenticación, política, cobro	HSS, DRA, PGW-C, PCRF, OCS, CSCF (Cx/Dx/Rx)
GTP-C	Gestión de sesiones (S5/S8, S11)	SGW-C, PGW-C, MME
PFCP	Reglas de sesión de plano de usuario (N4)	PGW-C/SMF ↔ UPF
SIP	Control de llamadas IMS	P-CSCF, I-CSCF, S-CSCF, TAS
MAP	Ubicación SS7, autenticación, SMS	MSC, HLR, CAMEL GW, IP-SM-GW

Trazado de Usuario

La vista de **Trazado de Usuario** te permite buscar por **IMSI** o **MSISDN** y ver cada interacción de protocolo correlacionada para ese suscriptor a través de la red. Un único adjunto, por ejemplo, revela la autenticación Diameter, la creación de sesión GTP-C y la instalación de la regla PFCP como una secuencia coherente:



Pestañas específicas de protocolo

Cada protocolo tiene su propia pestaña (**Diameter, GTP-C, PFCP, SIP, MAP**), además de una visión general de **Todos los Protocolos**. Las pestañas por protocolo son vistas filtradas. Ayudan cuando persigues un problema específico de protocolo (por ejemplo, solo el intercambio SIP de una llamada VoLTE) en lugar de seguir a un solo suscriptor a través de todo.

Escalera PCAP

La pestaña de **Escalera PCAP** convierte una captura de paquetes en una escalera: un diagrama de secuencia ordenado por tiempo de la señalización. Sube una captura PCAP o PCAPNG (por ejemplo, de un tap de red o un trazado a nivel de elemento) y OmniWeb analiza los paquetes, identifica los nodos de señalización por dirección IP y rol inferido (MSC/VLR, HSS, S-CSCF, etc.), y correlaciona solicitudes con sus respuestas en sesiones. El resultado se dibuja como una escalera de mensajes a través de esos nodos, ordenada en el tiempo, para que puedas leer todo un intercambio de arriba a abajo de un vistazo.

Escalera PCAP: una captura subida renderizada como una escalera a través de los nodos detectados. Haz clic en cualquier mensaje para ver su marco decodificado y hex.

Haz clic en un mensaje en la escalera para abrir su decodificación completa y hex, el mismo detalle que obtendrías de un analizador de protocolos. La herramienta reconoce las familias de señalización que encuentras a través de un núcleo móvil: MAP, CAMEL, TCAP, Diameter, SIP, GTP-C, PFCP y GSM SMS. Cada captura que subas se lista en la pestaña para que pueda ser reabierta o compartida con un colega en lugar de pasar el archivo.

Flujos en Vivo

La pestaña de **Flujos en Vivo** muestra la misma vista de escalera, pero proveniente en vivo de los registros de señalización estructurados de la red (a través de Loki) en lugar de un archivo subido. A medida que los elementos de la red emiten telemetría de señalización, los flujos de llamadas recientes por suscriptor aparecen aquí automáticamente, agrupados por IMSI, sin necesidad de captura para subir. Selecciona un flujo para reconstruirlo en la misma escalera que un PCAP, por lo que un flujo en vivo es tan rico como uno leído de un archivo, hasta la decodificación por mensaje y hex.

Flujos en Vivo: flujos de llamadas recientes extraídos directamente de la telemetría de señalización de la red. Filtra por IMSI, nodo o protocolo, luego abre un flujo para renderizar su escalera en vivo.

Abre un flujo y OmniWeb lo reconstruye en la misma escalera que un PCAP, pero desde la propia telemetría de la red, sin nada que capturar o subir. El ejemplo a continuación es un adjunto LTE de un solo suscriptor, correlacionado a través de cada elemento que lo tocó: el intercambio S1AP/NAS con el **eNodeB**, la autenticación Diameter S6a y la actualización de ubicación contra el **HSS**, y la configuración de sesión GTP-C a través del **SGW-C** y **PGW-C**. Todo esto aparece en una única escalera ordenada por tiempo, con tiempos de ida y vuelta de solicitud/respuesta por mensaje y decodificación completa a un clic de distancia.

Un flujo en vivo abierto en su escalera: el adjunto LTE de un suscriptor a través del eNodeB, MME, HSS, SGW-C y PGW-C, correlacionando S1AP, Diameter S6a y GTP-C. Haz clic en cualquier mensaje para su decodificación y hex, o en cualquier nodo para centrarte en sus intercambios.

Si aún no fluye telemetría de señalización, la pestaña muestra un estado vacío; los flujos se poblarán por sí mismos a medida que los elementos de la red

comiencen a emitir telemetría.

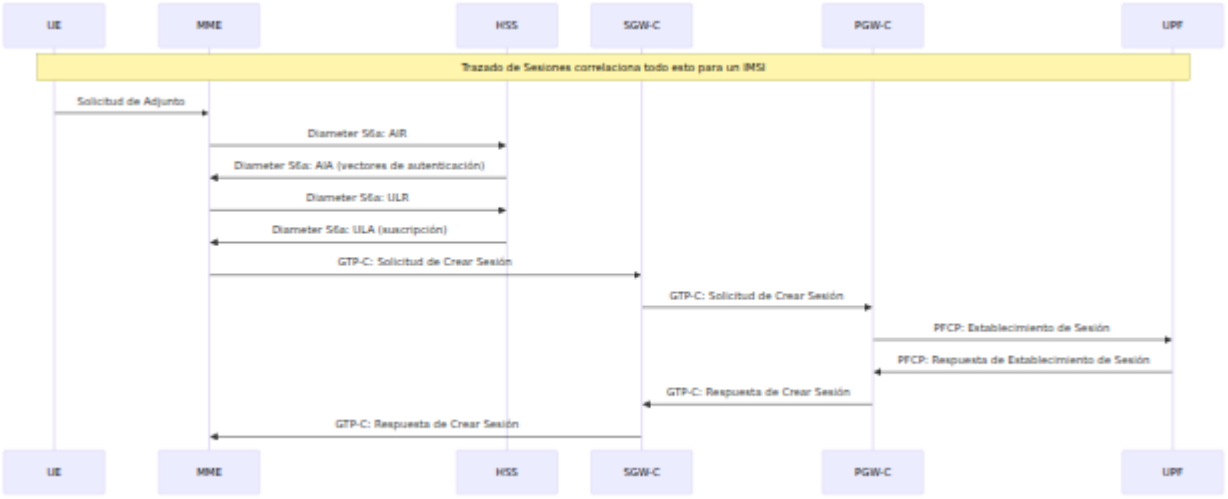
Homer: Captura SIP y Análisis de Flujo de Llamadas

OmniWeb se integra con Homer, la plataforma de captura SIP de código abierto y solución de problemas de VoIP, para visualización profunda de flujo de llamadas, decodificación de protocolos y búsqueda a través de la señalización SIP capturada. Mientras que el Trazado de Sesiones proporciona un *resumen* de múltiples protocolos para un suscriptor, Homer ofrece el detalle completo de paquetes SIP, mensaje por mensaje.

Disponibilidad y acceso

Homer es **opcional** y se detecta automáticamente. Al iniciar, OmniWeb verifica `/api/homer/status`:

- Si Homer está configurado (`HOMER_URL` establecido en el backend) y es accesible, aparece una entrada de **Homer** en la barra lateral.
- Si Homer no está desplegado, la entrada simplemente está oculta, y nada más cambia.



Hacer clic en **Homer** abre la interfaz web de Homer en una nueva pestaña del navegador. La autenticación es transparente: la puerta de enlace verifica tu inicio de sesión de OmniWeb a través del mismo inicio de sesión único utilizado

para Grafana, por lo que no hay un segundo inicio de sesión. La `HOMER_URL` del backend (y `HOMER_PROXY_SECRET`, cuando se establece) configuran la integración.

Casos de uso

Homer es la herramienta a la que recurrir cuando un problema está en la capa SIP misma:

- **Análisis de flujo de llamadas VoLTE**: rastrear secuencias SIP `INVITE`/`BYE` a través de P-CSCF, I-CSCF, S-CSCF y TAS.
- **Solución de problemas de VoWiFi**: analizar interacciones SIP entre ePDG ↔ P-CSCF.
- **Depuración de registro IMS**: inspeccionar intercambios `REGISTER` / `401` / `REGISTER` / `200 OK`.
- **Problemas de interconexión**: capturar señalización de tronco SIP entre el MSC y pares SIP.

Trazado de Sesiones vs. Homer

Ambos ayudan con la solución de problemas, pero responden a diferentes preguntas. Son complementarios, no alternativas:

Herramienta	Mejor para	Alcance	Dónde se abre
Trazado de Sesiones	"Sigue a este suscriptor a través de toda la red"	Diameter, GTP-C, PFCP, SIP, MAP correlacionados por IMSI/MSISDN	En línea en OmniWeb
Homer	"Muéstrame los mensajes SIP exactos para esta llamada"	Señalización SIP/VoIP, decodificación completa de paquetes (VoLTE/VoWiFi/IMS)	Nueva pestaña (detectada automáticamente)

Un flujo común es detectar una anomalía relacionada con SIP en el Trazado de Sesiones, luego saltar a Homer para el flujo de llamada detallado.

Solución de Problemas

No aparecen registros en la pestaña de Registros de un elemento

Síntomas: La pestaña de Registros está vacía o muestra "sin resultados".

Causas posibles:

- Loki no es accesible desde el backend (`LOKI_URL` mal configurado).
- El host no está enviando registros a Loki (envío de registros no funcionando / mal configurado).
- La ventana de tiempo seleccionada es anterior a los registros disponibles, o la etiqueta del host no coincide.

Resolución:

1. Confirma que `LOKI_URL` apunta a una instancia de Loki accesible.
2. Verifica que el host del elemento esté enviando registros (verifica el agente de envío de registros en ese host).
3. Amplía la ventana de tiempo y elimina filtros de canalización para confirmar que lleguen líneas.

El Trazado de Sesiones no devuelve nada para un suscriptor

Síntomas: Un Trazado de Usuario por IMSI/MSISDN no muestra eventos.

Causas posibles:

- El suscriptor estuvo inactivo en la ventana seleccionada.
- El identificador está mal escrito (IMSI vs. MSISDN).

- Las fuentes de trazado para el protocolo relevante no están alimentando el motor.

Resolución:

1. Revisa el identificador y prueba el alternativo (IMSI ↔ MSISDN).
2. Amplía la ventana de tiempo.
3. Confirma con la pestaña de Registros del elemento que el suscriptor estuvo activo.

La entrada de Homer falta en la barra lateral

Síntomas: No aparece ningún enlace de **Homer**.

Causas posibles:

- Homer no está desplegado, o `HOMER_URL` no está configurado en el backend.
- Homer no es accesible, por lo que `/api/homer/status` lo informa como no disponible.

Resolución:

1. Confirma que Homer está desplegado y que `HOMER_URL` está configurado en el backend de OmniWeb.
2. Verifica que el backend pueda alcanzar a Homer, luego recarga OmniWeb (la detección se realiza al inicio).

MME: Entidad de Gestión de Movilidad

La **MME** es el ancla del plano de control del EPC. Termina **S1AP** hacia los eNodeBs, ejecuta los procedimientos de conexión, autenticación y movilidad para cada UE, y mantiene un **contexto de UE** para cada suscriptor conectado. Obtiene datos de suscripción y autenticación del HSS a través de **S6a** (Diameter), establece portadores en el Gateway de Servicio a través de **S11**, y coordina las transferencias inter-MME y entre sistemas a través de **S10/N26**. En resumen, es el nodo que decide dónde y cómo se conecta cada suscriptor, es paginado y se mueve a través de la red. OmniWeb muestra los eNodeBs activos de la MME, contextos de UE, SGW y pares de Diameter, estados de interfaz y estado de transferencia. Las tendencias a largo plazo están en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

La MME es una página de elemento por instancia que se alcanza desde la barra lateral cuando se navega en el inventario del sitio, y, donde se despliegan varias, una vista de flota para el estado agregado. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API de la MME, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Resumen

Una lectura de salud en una sola pantalla: el **estado de la API** de la MME y un resumen de su carga activa, incluyendo **eNodeBs** conectados, **UEs** adjuntos, **pares de SGW** y el estado de sus pares de **Diameter** (S6a). Es la forma más rápida de confirmar que la MME está activa y ver cuánto de la red de acceso está sirviendo.

eNodeBs

Cada eNodeB con el que la MME tiene una asociación S1AP, cada fila muestra el **ID global de eNB**, nombre y **estado** de conexión. Abre un eNodeB para mostrar su contexto: las celdas servidas y TACs y las UEs en él. Un operador puede **actualizar la capacidad de la MME** anunciada a un eNodeB, lo que ajusta cómo el eNodeB distribuye la carga de UEs a través de la piscina de MME (utilizado para drenar o ponderar una MME para mantenimiento o reequilibrio).

UEs

El **contexto de UE** de cada suscriptor adjunto, cada fila identificada por **IMSI** y **GUTI** con su estado de conexión y movilidad y el eNodeB que lo sirve. Abrir una UE muestra su contexto completo. Hay una gama de acciones por UE disponibles:

- **Pagar** la UE.
- **Enviar a inactivo**: liberar la conexión de radio mientras se mantiene el contexto.
- **Descargar** la UE a otra MME.
- **Solicitar re-conexión**: forzar a la UE a reconectarse.
- **Enviar SMS** a la UE.
- **Eliminar** el contexto de la UE: limpiar un suscriptor obsoleto o atascado.

También puedes **buscar el operador / PLMN** para un IMSI para identificar suscriptores de hogar frente a suscriptores en roaming.

Pares de S-GW

Los Gateways de Servicio con los que la MME se comunica a través de **S11** (GTP-C), cada fila muestra la **IP** del par, su **actividad / alcanzabilidad**, el **contador de reinicio (recuperación)** de GTP y el **conteo de sesiones** ancladas en ese gateway. El contador se incrementa cuando el S-GW se reinicia, lo que indica a la MME que restablezca las sesiones que estaba manteniendo. Se muestra si un par fue aprendido por **DNS** o es una entrada **estática** junto con el **método de selección** de S-GW que la MME aplica para suscriptores de hogar y roaming. Abre un par para listar las **sesiones** que lleva, cada una identificada por **IMSI** con sus **TEIDs de S11** (los puntos finales de túnel del lado de la MME y del S-GW). Es donde un operador confirma cuáles S-GWs están activos y ve cómo se distribuyen las sesiones de UE entre ellos. Esto ayuda cuando se balancea la carga o se diagnostica por qué los portadores para un grupo de suscriptores fallaron con un solo gateway.

Reasignación de GUTI y descarga S10

Dos acciones de movilidad se impulsan por IMSI en lugar de por fila:

- **Reasignación de GUTI**: reasignar el **GUTI** de un suscriptor conectado para refrescar la identidad temporal que la UE presenta (utilizado al rotar identificadores o limpiar un desajuste de identidad).
- **Descarga S10**: forzar la descarga de un suscriptor a **otra MME**. Esto mueve el contexto de un suscriptor específico fuera de esta MME a través de S10, y complementa el control de capacidad del eNodeB cuando se drena una MME.

S10

La interfaz **S10/N26 inter-MME** es el camino a través del cual se reubica el contexto de una UE cuando se mueve entre MMEs en una piscina durante un **TAU** o **transferencia** (y, a través de **N26**, entre la MME y un AMF para la interoperabilidad de EPC a 5GC). La pestaña tiene dos partes. **Transferencias**

activas lista las reubicaciones en curso, cada una mostrando la MME **de origen** y **destino** y el **IMSI** que se está moviendo, para que un operador pueda observar cómo avanza un evento de movilidad o detectar uno que está atascado. **Descubrimiento de pares MME** muestra cómo la MME encuentra a sus pares en la piscina: las búsquedas de **DNS / NAPTR** que ejecuta y cualquier par **estático** configurado, con el FQDN y la dirección de cada par. Es donde confirmas que la movilidad inter-MME es saludable y que la MME puede alcanzar efectivamente a los vecinos a los que necesita entregar contextos. Complementa la acción de **descarga S10** por suscriptor impulsada desde la pestaña de UEs.

Diameter

Los pares de Diameter de la MME, principalmente el HSS a través de **S6a**, cada fila muestra el **host** del par, **dominio** y **estado** de conexión. Abre un par para mostrar su detalle. Aquí es donde confirmas que la ruta de autenticación y suscripción al HSS está activa cuando las conexiones están fallando.

Interfaces

La vista de **Interfaces** informa el estado de cada interfaz de la MME en un solo lugar: **S1AP** hacia los eNodeBs, **GTP-C** (S11) hacia el SGW, **Diameter** para **S6a** (HSS) y **SLg** (servicios de localización), **SGsAP** (hacia el MSC para retroceso de CS y SMS), **LCS-AP / SLs** (servicios de localización), y **S10/N26** (transferencia inter-MME y transferencia de EPC a 5GC). Es la pantalla única para confirmar cuáles de las rutas de señalización de la MME están activas y cuáles están inactivas.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo de la MME para solucionar problemas de una sola MME sin salir de OmniWeb.

Paneles de monitoreo

Las tasas de conexión, conteos de UE, tasas de transferencia y otras series temporales para la MME se presentan como paneles de Grafana, accesibles

desde la página del elemento. OmniWeb no duplica esos gráficos de manera nativa.

Relacionados

- El **HSS** mantiene los datos de suscripción y autenticación que la MME obtiene a través de **S6a**.
- El **SGW-C** es el par de control a través de **S11**. La MME impulsa la configuración de sesión y portador en él.
- El **MSC** se alcanza a través de **SGsAP** para retroceso de CS y SMS.
- Otras **MMEs** se alcanzan a través de **S10** para movilidad inter-MME, y el **AMF** a través de **N26** para transferencia de EPC a 5GC.

Quectel EP06 Referencia de Comandos AT (pruebas de red celular)

Referencia para la consola del módem de los Dispositivos de Prueba. Está dirigida al **Quectel EP06** (firmware `EP06ELAR04A05M4G`, IMEI `868186042000040`) en el contenedor de laboratorio, pero se aplica a la familia EC25 / EG06 / EG06 / EM06. Cada comando a continuación fue probado contra el EP06 en vivo; las respuestas de ejemplo son las **respuestas reales capturadas de ese módem** (estaba en un estado de `NO SERVICE / SEARCH` en ese momento, por lo que los campos de señal se leen vacíos, y los analizadores deben manejar eso).

El relé es solicitud/respuesta: `sendModemAt(serial, command, readMs, timeoutMs)` → backend `modem_at` → agente `modem.run_at(serial, command, min_read, timeout)`. `min_read` sigue leyendo el puerto durante al menos ese tiempo para que se capturen los URCs asíncronos antes de que la llamada regrese. No hay **flujo de URC persistente**. Ver "Registro de eventos" a continuación.

Información del dispositivo / SIM

Comando	Propósito	Respuesta en vivo
`ATI`	Fabricante / modelo / firmware	`Quectel` / `EP06` / `Revisión: EP06ELAR04A05M4G`
`AT+CGMM`	Modelo	`EP06`
`AT+CGMR`	Revisión del firmware	`EP06ELAR04A05M4G`
`AT+CGSN`	IMEI	`868186042000040`
`AT+CIMI`	IMSI	(IMSI de SIM)
`AT+QCCID`	ICCID	(ICCID de SIM)
`AT+CPIN?`	Estado del PIN de SIM	`+CPIN: READY`

Señal / medición

Comando	Propósito	Respuesta en vivo
`AT+CSQ`	RSSI/BER (legado)	`+CSQ: 99,99` (99 = sin señal). dBm = `-113 + 2*rssi`.
`AT+QCSQ`	Señal por RAT	`+QCSQ: "NOSERVICE"`. Cuando está conectado: `+QCSQ: "LTE",<rssi>,<rsrp>,<sinr>,<rsrq>`.
`AT+QNWINFO`	RAT / banda / canal actual	`+QNWINFO: No Service`. Cuando está conectado: `+QNWINFO: "FDD LTE","<mccmnc>","LTE BAND 3",1850`.
`AT+QENG="servingcell"`	Mediciones completas de la celda de servicio	`+QENG: "servingcell","SEARCH"` (inactivo). Ver formato a continuación.
`AT+QENG="neighbourcell"`	Celdas vecinas	`OK` (ninguna cuando no está acampado).

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 enteros con signo).

- `SINR` es un valor **convertido**: dB real = `(1/5)*SINR - 20` (rango 0..250 → -20..+30 dB).
- `cellID`/`PCI`/`EARFCN` suelen ser hexadecimales/decimales por campo; `band` es el indicador de 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 / conexión

Comando	Propósito	Respuesta en vivo
`AT+CFUN?`	Funcionalidad de radio	`+CFUN: 1` (completo). `0` = mínimo/avión.
`AT+CEREG?`	Registro EPS	`+CEREG: 2,2` (2 = buscando).
`AT+CEREG=2`	Habilitar URC de registro **con ubicación** (TAC/cellID)	`OK`
`AT+CGATT?` / `AT+CGATT=1` / `=0`	Estado de conexión PS / conectar / desconectar	`+CGATT: 0`
`AT+COPS?`	Selección de operador actual	`+COPS: 0` (automático, no registrado).
`AT+COPS=?`	**Escaneo de red** (búsqueda de operador, lento)	lista de tuplas `(stat,"long","short","numeric",AcT)`.
`AT+COPS=0`	Selección automática de operador	`OK`

Comando	Propósito	Respuesta en vivo
`AT+COPS=1,2,"<mccmnc>"[,<AcT>]`	Selección manual por ID numérico	`OK`

Bloqueo de celda / banda / RAT

Comando	Propósito	Respuesta en vivo
`AT+QNWLOCK=?`	Capacidades	`+QNWLOCK: "common/4g",<num de celdas>,[[<freq>,<pci>],...]` y `+QNWLOCK: "common/lte"[,<action>[,<EARFCN>,<PCI>[,<status>]]]`
`AT+QNWLOCK="common/4g"`	Consultar bloqueo de celda	`+QNWLOCK: "common/4g",0` (0 celdas = sin bloqueo); después del bloqueo `+QNWLOCK: "common/4g",1,1850,0`.
`AT+QNWLOCK="common/4g",<n>,<EARFCN>,<PCI>[,<EARFCN>,<PCI>...]`	**Bloquear** en n celdas (funciona en este firmware)	`OK`
`AT+QNWLOCK="common/4g",0`	**Desbloquear**	`OK` (elimina el bloqueo).
`AT+QNWLOCK="common/lte"`	Consultar bloqueo de LTE de celda única (solo lectura)	`+QNWLOCK: "common/lte",0,0,0,0`.

> **Comportamiento del firmware (verificado en vivo en `EP06ELAR04A05M4G`):** la forma `common/4g` es la que acepta una *acción* de bloqueo en esta unidad. `AT+QNWLOCK="common/4g",1,<EARFCN>,<PCI>` bloquea (devuelve `OK`, el bloqueo persiste) y `AT+QNWLOCK="common/4g",0` lo elimina. Las formas de *conjunto* de `common/lte` (`...,1,<EARFCN>,<PCI>` y `...,0`) todas devuelven `ERROR` en este firmware, por lo que `common/lte` es solo consulta aquí. La interfaz de usuario, por lo tanto, utiliza `common/4g` tanto para bloquear como 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` | **Bloqueo de banda** (LTE). `0x0` máscara LTE = todas las bandas. | `OK` | | `AT+QCFG="nwscanmode"` | Modo de escaneo RAT | `+QCFG: "nwscanmode",0` (0 = automático, 1 = GSM, 2 = WCDMA, 3 = LTE). | | `AT+QCFG="nwscanmode",<m>[,1]` | Establecer preferencia de RAT (`,1` = efectivo inmediatamente) | `OK` | | `AT+QCAINFO` | Información de agregación de portadora | `OK` (ninguna agregada cuando está inactivo). |

Máscara de banda LTE: bit `(band-1)`, es decir, banda N → `1 << (N-1)`. por ejemplo, B3 = `0x4`, B7 = `0x40`, B28 = `0x8000000`. `0x0` (o todos unos) = todas las bandas habilitadas.

> **Nota del firmware:** `AT+QCFG="nwscanseq"` devuelve `ERROR` en este firmware EP06 (`EP06ELAR04A05M4G`). La interfaz de usuario **no** lo muestra. `AT+QSCAN` tampoco es compatible con este firmware EP06 (es un comando de la serie RG/RM 5G). El escaneo de red utiliza `AT+COPS=?` más `AT+QENG` en su lugar.

Llamadas de voz (VoLTE / IMS)

La voz del EP06 es **solo VoLTE**: necesita IMS registrado sobre LTE. `AT+QCFG="ims"` en esta unidad devuelve `+QCFG: "ims",1,0` (IMS habilitado por configuración, estado actual 0).

Comando	Propósito
`AT+QCFG="ims"`	Consultar/habilitar IMS. `AT+QCFG="ims",1` para forzar la habilitación.
`ATD<number>;`	Marcar una llamada de voz (el `;` final = voz, no datos).
`ATA`	Contestar una llamada entrante.
`ATH` / `AT+CHUP`	Colgar.
`AT+CLCC`	Listar llamadas actuales: `+CLCC: <id>,<dir>,<state>,<mode>,<mpty>,"<number>",<type>`. Vacío `OK` = sin llamadas.
`AT+CLIP=1`	Habilitar URC de identificación de línea de llamada (`+CLIP:`) en `RING`.

Estados de llamada de `AT+CLCC`: 0 activo, 1 en espera, 2 marcando, 3 alertando, 4 entrante, 5 esperando.

SMS (modo texto)

Comando	Propósito	Respuesta en vivo
`AT+CMGF=1`	Modo texto (vs PDU)	`OK`
`AT+CPMS?`	Áreas de almacenamiento / conteos	`+CPMS: "ME",0,255,"ME",0,255,"ME",0,25`
`AT+CMGL="ALL"`	Listar mensajes (modo texto)	por mensaje: `+CMGL: <index>,"<stat>","<sender>",,"<timestamp>"` luego línea del cuerpo.
`AT+CMGR=<index>`	Leer un mensaje	`+CMGR: "<stat>","<sender>",,"<timestamp>"` + cuerpo.
`AT+CMGS="<number>"` luego cuerpo + Ctrl-Z	Enviar (manejado por agente `send_sms`).	`+CMGS: <mr>`
`AT+CMGD=<index>[,<delflag>]`	Eliminar mensaje (`delflag` 4 = todos).	`OK`
`AT+CNMI?` / `AT+CNMI=2,1,0,0,0`	Configuración de indicación de nuevo mensaje	`+CNMI: 2,1,0,0,0`

PDP / datos

Comando	Propósito	Respuesta en vivo
`AT+CGDCONT?`	Listar contextos PDP (APNs)	`+CGDCONT: 1,"IPV4V6","ims",...`
`AT+CGDCONT=<cid>,"<type>","<apn>"`	Establecer contexto. tipos: IP, IPV6, IPV4V6, Non-IP.	`OK`
`AT+CGACT=1,<cid>` / `=0,<cid>`	Activar / desactivar contexto.	`OK`
`AT+CGPADDR[=<cid>]`	Mostrar IP asignada.	`+CGPADDR: 1,"<ip>"`
`AT+CGCONTRDP=<cid>`	DNS / puerta de enlace / PCO.	`+CGCONTRDP: ...`
`AT+QPING=1,"<host>"`	Hacer ping desde el módem (respuestas URC; necesita `min_read`).	`+QPING: ...`

Registro de eventos (URCs): y la limitación del relé

El relé del agente es **solicitud/respuesta con un puerto abierto por llamada**. Abre el puerto serie, envía un comando, lee hasta OK/ERROR (o se agota `min_read`), luego cierra. No **mantiene** el puerto abierto para transmitir códigos de resultado no solicitados (URCs) de vuelta al navegador. Por lo tanto, un verdadero flujo de eventos en vivo no es posible a través de este camino sin cambios en el agente.

URCs que vale la pena habilitar (cada uno es un comando `OK` de un solo uso):

Comando	Habilita URC
`AT+CEREG=2`	`+CEREG:` cambios de registro (con TAC/cellID).
`AT+CGEREP=2,1`	`+CGEV:` eventos de PS/bearer.
`AT+CLIP=1`	`+CLIP:` ID de llamada en `RING` entrante.
`AT+CNMI=2,1,0,0,0`	`+CMTI:` indicación de nuevo SMS.
`AT+QINDCFG="all",1`	`+QIND:` indicaciones de Quectel.

Enfoque pragmático utilizado en la interfaz de usuario: la pestaña de Eventos habilita los URCs anteriores, luego **sondea** el módem en un intervalo (`AT+CEREG?`, `AT+CLCC`, `AT+QENG`, `AT+CSQ`, `AT+CMGL`) y renderiza cambios de estado en un registro con marcas de tiempo. Cada sondeo también utiliza una ventana corta de `min_read` para que cualquier URC que llegue durante la lectura se capture oportunamente. Esto captura transiciones de estado (registro adquirido/perdido, llamada iniciada/terminada, nuevo SMS, cambio de señal) a la cadencia de sondeo, lo cual es suficiente para pruebas de laboratorio. La limitación está documentada en la interfaz de usuario.

MSC: Centro de Conmutación Móvil

El **MSC** es el corazón del control de llamadas del núcleo conmutado por circuitos. Mantiene el registro de ubicación de visitantes (VLR) para los suscriptores que actualmente se encuentran en su área de servicio, establece y finaliza **llamadas de voz**, transporta **SMS** y gestiona la **movilidad** (actualizaciones de ubicación, búsqueda y transferencias) para esos suscriptores. Se conecta al lado de radio a través de conexiones **RAN/BSC** (interfaz A, impulsada por M3UA/SS7), conecta la voz al IMS e interconecta a través de **pares SIP**, y dirige los medios reales a través de uno o más **puentes de medios**. OmniWeb presenta los suscriptores activos del MSC, llamadas, transacciones de SMS, RAN y pares SIP, tabla de enrutamiento y páginas pendientes. Las tendencias a largo plazo se encuentran en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

El MSC es una página de elemento por instancia que se accede desde la barra lateral cuando se navega en el inventario del sitio, y, donde se despliegan varios, una vista de flota para el estado agregado. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del MSC, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Visión General

Una lectura de salud de una sola pantalla: el **estado de la API** del MSC y un resumen de lo que está manejando actualmente, incluyendo **suscriptores** registrados en el VLR, **llamadas activas**, transacciones de **SMS** en curso, **conexiones RAN** activas y el estado de los **pares SIP** y enlaces de señalización **STP**. Es la forma más rápida de confirmar que el MSC está operativo y ver, de un vistazo, su carga activa.

Suscriptores

Cada suscriptor que actualmente mantiene el VLR, cada fila identificada por **IMSI** y **MSISDN** con su estado de registro y ubicación. Abre un suscriptor para mostrar su contexto completo en el VLR. Desde aquí, un operador puede:

- **Eliminar** un suscriptor del VLR para limpiar un registro obsoleto o atascado para que el suscriptor se registre nuevamente de manera limpia.
- Ejecutar una **acción de suscriptor** contra un suscriptor específico.
- Gestionar **servicios suplementarios**: inspeccionar y cambiar el desvío de llamadas, bloqueo y servicios relacionados activos para el suscriptor.
- Enviar **Aviso de Carga (AoC)** al suscriptor.
- Enviar un **SMS silencioso (Tipo 0)** o iniciar una **llamada silenciosa**: una sonda de ubicación/alcance que no alerta al dispositivo.

Llamadas

Cada llamada activa, cada fila mostrando las partes **que llaman** y **llamadas**, el **estado** de la llamada y su **duración**. Abre una llamada para mostrar su detalle completo: las patas, la conexión RAN que la sirve y la ruta de medios. Un operador puede **forzar la liberación** de una llamada para despejar una llamada atascada o no deseada.

SMS

Las transacciones de SMS que el MSC está manejando actualmente, cada una mostrando el **originador**, **destinatario** y **estado de entrega**, para que puedas confirmar que los mensajes están siendo transportados y detectar aquellos que están atascados.

RAN

El lado de radio del MSC. Lista las **conexiones RAN** activas (las asociaciones de interfaz A en vivo que transportan la señalización de suscriptores) y los **BSC** conocidos, aprendidos de los intercambios RESET en los enlaces SS7/M3UA. Aquí es donde confirmas que los controladores de estación base están conectados y ves qué suscriptores están en qué conexión.

Pares SIP

Los pares SIP a través de los cuales el MSC conecta la voz son el IMS, conmutadores suaves y troncos de interconexión, cada fila muestra la **dirección** del par y su **estado** de alcance. Abre un par para mostrar su detalle. Un operador puede **activar un ping OPTIONS** en un par para probar activamente el alcance, que es la forma más rápida de probar que una ruta SIP está activa cuando las llamadas a ella están fallando.

Puentes de Medios

Los puentes de medios a través de los cuales el MSC dirige los portadores de voz, cada fila muestra el puente y su **estado**, para que puedas confirmar que el plano de medios está disponible para el establecimiento de llamadas.

Enrutamiento

La tabla de enrutamiento de números del MSC contiene las reglas que deciden, por prefijo de número marcado, a dónde se envía una llamada. Cada regla muestra su **prefijo** y **destino**. Un operador puede:

- **Agregar una ruta**: un nuevo prefijo y su destino.
- **Eliminar una ruta** por prefijo.
- **Probar una búsqueda de ruta** para un número: ingresa un número y ve a qué ruta se resuelve, para confirmar planes de marcado antes o después de un cambio.

Páginas

Las solicitudes de páginas pendientes son los suscriptores que el MSC está tratando de localizar a través de la red de radio para una llamada entrante o SMS. Un operador también puede **pagar a un suscriptor** directamente desde aquí.

Registros

La pestaña de **Registros** muestra la salida de registro en vivo del MSC para solucionar problemas de un solo conmutador sin salir de OmniWeb.

Paneles de Monitoreo

Las tasas de llamadas, volúmenes de SMS, conteos de suscriptores y otras series temporales para el MSC se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de manera nativa.

Relacionados

- El **HSS** contiene los datos de suscriptores contra los que el VLR resuelve y donde el MSC se registra como el nodo de servicio.
- El **CSCF / IMS** se conecta a través de los **pares SIP** del MSC para voz.
- Los **BSC** se conectan en el lado de radio a través de la interfaz A, transportada en los enlaces de señalización SS7/M3UA.

Pruebas de Red (Prueba de Carga)

Pruebas de Red genera carga de señalización sintética en un núcleo en vivo para que puedas medir cómo se comporta bajo estrés. Está impulsado por el Simulador RAN: eNodeBs y UEs virtuales que ejercen todo el camino radio→núcleo (S1AP/NAS, GTP-U, IMS) en lugar de una sola interfaz.

← Guía de Operaciones

El grupo de **Pruebas de Red** en la barra lateral recopila las herramientas de prueba de carga del Simulador RAN:

Sub-pestaña	Qué hace
Prueba de Carga RAN	Trabajos recientes de prueba de carga — adjuntos, sesiones de datos y registros IMS ejecutados contra el núcleo, con sus resultados y un pcap descargable.
Programaciones de Escenarios	Define ejecuciones de escenarios recurrentes (por ejemplo, un lote de adjuntos por hora), ejecuta uno ahora y navega por el historial de ejecuciones. Los resultados se exportan a Prometheus para alertas.
Simulador RAN	Configura eNodeBs/gNodeBs y UEs virtuales y dirígelos directamente.
Radio RAN	Control de radio Multi-RAT (5G NR / 2G GERAN / 3G UTRAN).
RANsimware — IMS	Registro IMS y carga de VoLTE a través de la flota simulada.

Todo esto está documentado en profundidad en **Simulador RAN**.

Apuntando una ejecución a un núcleo

Cuando activas una celda, OmniWeb ofrece un menú desplegable de los nodos del núcleo que puede marcar — cada **MME**, **AMF** y **STP** que encuentra en los inventarios de tu sitio — para que apuntas la ejecución al núcleo correcto (`mme_ip` / `amf_ip` / `stp_ip`) en lugar de escribir una IP. Sin un inventario configurado, el campo vuelve a texto libre.

Uso Típico

1. Abre **Simulador RAN**, activa un eNodeB/gNodeB y apúntalo al núcleo para probar.
2. Adjunta un lote de UEs y ejecuta un escenario (adjunto, datos, registro IMS, VoLTE o un escenario de interrupción).
3. Observa los resultados y, para detalles de señalización, descarga el pcap de la ejecución.
4. Para cobertura de rutina, guarda el escenario como una **Programación de Escenario** para que se ejecute en un intervalo y exporte el resultado de aprobado/reprobado a Prometheus.

Relacionado

- Simulador RAN: eNodeBs/UEs virtuales para pruebas funcionales y de carga a través de todo el camino radio→núcleo.
- Dashboards y Estadísticas de Grafana: el resultado de aprobado/reprobado y el tiempo se exportan a Prometheus; usa Grafana para tener una visión completa durante una prueba.

OmniRoam: Acuerdos de Roaming y Automatización de Correos Electrónicos

La parte de **acuerdos** de OmniRoam convierte el papeleo de establecer un socio de roaming (los correos electrónicos, los formularios AA.12/AA.13, las tarifas IOT, los cambios de SIM y el trabajo de aprovisionamiento) en un único registro rastreado por socio. Automatiza las partes que solían ser copiar y pegar. Su truco principal: **reenvía un correo electrónico de un socio a OmniRoam y lee el hilo, extrae los hechos y actualiza el acuerdo por ti**. Luego genera y firma electrónicamente los contratos, los archiva y crea las órdenes de trabajo para poner en marcha al socio.

← Volver a la Guía de Operaciones

> **Dos "OmniRoam" diferentes.** Este documento trata sobre la parte de **acuerdos / correo / documentos** de OmniRoam (el ciclo de vida comercial y de aprovisionamiento con un socio de roaming). **No** es lo mismo que los **libros de pruebas de roaming** (IR.38 / IR.48 / pruebas de conformidad VoLTE). Esos se cubren por separado en OmniRoam: Automatización de Pruebas de Roaming. Un producto, dos trabajos: *obtener el acuerdo firmado* (aquí) y *demostrar que el roaming funciona* (allí).

Tabla de Contenidos

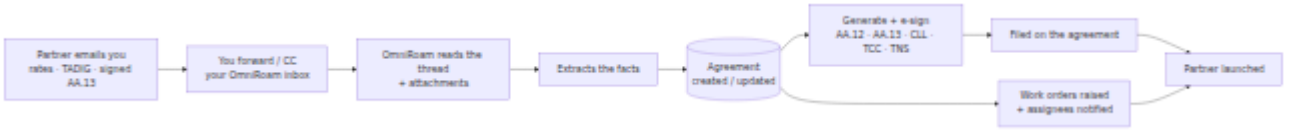
- La Gran Imagen
- 1. Ingesta de Correos Electrónicos Entrantes: "extrayendo los datos"
- 2. Acuerdos y Socios
- 3. Generación y Firma Automática de Documentos

- 4. Archivo y Almacenamiento
- 5. Órdenes de Trabajo y Notificaciones a Asignados
- El Ciclo de Vida Completo, de Principio a Fin
- Lo Que Configuras Una Vez

La Gran Imagen

Todo en OmniRoam se basa en un registro: el **Acuerdo**, uno por socio de roaming. Un acuerdo lleva el nombre del socio, país, TADIG(s)/PLMN, su **estado** de ciclo de vida, sus contactos, las **tarifas** comerciales acordadas, las SIM intercambiadas, los **documentos** generados y recibidos, una **línea de tiempo** de actividades, y las **órdenes de trabajo** que ponen al socio en funcionamiento.

Puedes construir todo eso manualmente en la interfaz de usuario. Pero el objetivo de OmniRoam es que la mayor parte llega *por correo electrónico*, y OmniRoam lo archiva por ti.



El inquilino en el que estás trabajando es un **Operador** (tu propia red, el lado "local"). Todo está limitado a él: tu membrete y firmante llenan los documentos generados, tu dirección de entrada impulsa la automatización del correo electrónico, y tus equipos son los asignados a las órdenes de trabajo.

---

1. Ingesta de Correos Electrónicos Entrantes: "extrayendo los datos"

Lo que haces

Negociar con un socio es una conversación por correo electrónico. Para llevarlo a OmniRoam haces una cosa: **reenviar el correo electrónico, o CC la**

dirección de entrada de OmniRoam en el hilo. Eso es todo. Tu dirección de entrada dedicada (por ejemplo `roaming@yourdomain`) está configurada una vez por operador (Configuraciones → detalles del papeleo, `Correo electrónico entrante`).

- **Reenvía todo un hilo** una vez y OmniRoam construye el acuerdo a partir de la historia enterrada en los mensajes citados.
- **CC la dirección en una negociación en curso** y cada nuevo correo mantiene el registro actualizado. El estado avanza, los contactos y TADIGs se completan, las tarifas llegan y el papeleo adjunto se archiva, correo por correo.

Nunca llenas un formulario para hacer esto. El correo electrónico *es* la entrada.

Lo que hace OmniRoam

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

Intente de nuevo

Paso a paso, una vez que un correo llega a OmniRoam:

1. **Determina para qué operador (inquilino) es el correo** al hacer coincidir una dirección To/Cc con la dirección de entrada configurada de un operador. Si no hay coincidencias, el correo se registra como `no-operator` y *no se cambia nada*: un no-op seguro.
2. **Lee los adjuntos, no solo el cuerpo.** Las tarifas acordadas o los términos firmados a menudo están dentro de un **AA.13** adjunto, una **hoja de tarifas IOT**, o una hoja de cálculo. Así que OmniRoam extrae el texto de archivos PDF, Word, Excel y CSV y también lo alimenta al extractor. Los logotipos de bloque de firma (PNG/JPG) se ignoran.
3. **Extrae los hechos** utilizando la API de ChatGPT. Al extractor se le indica específicamente que el remitente externo generalmente solo está *reenviando* el hilo (a menudo tu propio gerente de roaming) y que lea **toda la historia citada**. Atribuye tarifas, contactos, direcciones y SIMs a quien realmente los declaró, nunca al reenviante. Devuelve un registro estructurado: nombre del socio, país, dirección, TADIG(s)/PLMN, estado de

ciclo de vida mejor ajustado, tarifas acordadas (solo si *ambas* partes acordaron explícitamente), contactos del socio, SIMs intercambiadas/solicitadas, si hay un acuerdo firmado adjunto, y un resumen de una línea.

4. **Encuentra el acuerdo correcto, o crea uno.** La coincidencia es deliberadamente indulgente para que un hilo nunca genere un duplicado: nombre exacto del socio, luego una coincidencia de "nombre normalizado" (así *AT&T Mobility* se une a *AT&T*), luego una coincidencia de **PLMN compartido** (MCC+MNC). Esta es una señal de alta precisión, ya que un PLMN identifica de manera única una red. Sin coincidencia → un nuevo acuerdo.
5. **Fusiona solo lo que es nuevo.** Para acuerdos nuevos y existentes, OmniRoam aplica lo que *este* correo revela de nuevo y **nunca sobrescribe** los valores existentes:
    - **Estado** solo avanza *hacia adelante* a lo largo del ciclo de vida (nunca hacia atrás).
    - **País / dirección** se establece si está en blanco o cambiado.
    - **TADIGs** añadidos, pero solo códigos que existen en el catálogo IR.21 (por lo que la IA no puede inventar uno), y nunca los códigos de tu propia red local.
    - **Contactos** añadidos, o los existentes *enriquecidos* (campos en blanco completados).
    - **SIMs** registradas (SIMs de prueba que compartió el socio) y **solicitudes de SIM** (lotes que alguien pidió que se enviaran a una dirección).
    - **Tarifas acordadas** se convierten en un nivel de tarifas, solo cuando ambas partes acordaron explícitamente, y nunca un duplicado de un nivel existente.
    - Un **AA.12/AA.13 firmado** (adjunto, o declarado en el correo) avanza el estado a *IRA Firmado*.
6. **Escribe dos registros.** Una amigable **entrada de registro de actividad** en la línea de tiempo del acuerdo ("Correo electrónico de *Jane en Partner* (reenviado): tarifa de datos acordada; estado → rates_agreed, contacto añadido Jane, tarifas acordadas registradas"), y una **fila de auditoría entrante** en bruto (ver más abajo).

El procesamiento es **idempotente**: el mismo correo (por Message-ID) solo se procesa una vez, por lo que CC'ing a múltiples personas o reenviar un hilo nunca cuenta dos veces.

Tres formas en que llega el correo electrónico

Solo necesitas una. Las tres terminan llamando a la misma lógica de procesamiento:

Ruta	Cómo funciona	Cuándo usarlo
Cloudflare Email Worker	Cloudflare Email Routing reenvía el mensaje en bruto a un pequeño Worker que transmite el `.eml` directamente al webhook de OmniRoam.	Dominios que ya utilizan Cloudflare; sin buzón que sondear.
IMAP poller	OmniRoam inicia sesión en un buzón real cada ~60 s, procesa mensajes no leídos y los marca como leídos.	Cualquier buzón estándar (TLS implícito, STARTTLS o plano).
Provider inbound-parse	Un proveedor de correo (Mailjet/SendGrid) envía por POST el mensaje analizado + adjuntos al webhook.	Si ya ejecutas inbound-parse.

El webhook (`/api/roaming/inbound-email`) está protegido por un **secreto compartido**, por lo que solo tu ruta de correo configurada puede publicar en él.

El Registro de Correos Electrónicos Entrantes: tu rastro de auditoría

Cada correo electrónico procesado, éxito *o* fallo, escribe una fila en el **Registro de Correos Electrónicos Entrantes** (en la interfaz de usuario bajo la vista de

Correos del operador). Cada fila muestra el remitente, destinatarios, asunto, adjuntos, si la **extracción de IA tuvo éxito**, exactamente lo que extrajo y qué **cambió** el correo electrónico (o por qué no hizo nada: `no-operator`, `no-partner`). Esta es tu ventana a la automatización: si una tarifa no fue capturada, el registro te dice lo que el extractor realmente vio.

El Registro de Correos Electrónicos Entrantes: una fila por correo electrónico procesado, con el resultado de la extracción y los cambios que realizó. Este es el rastro de auditoría para toda la automatización de correo→acuerdo.

---

2. Acuerdos y Socios

La lista de **Acuerdos** es tu libro de socios de roaming para el operador actual. Cada fila es un socio, con su **estado** de ciclo de vida, TADIG/país, prioridad, y a quién está esperando la siguiente acción ("Nosotros" o "Ellos").

La lista de Acuerdos. Los estados se extienden de izquierda a derecha a lo largo del ciclo de vida; la barra de filtro se reduce por estado. Creas acuerdos aquí a mano, o llegan automáticamente de un correo electrónico entrante.

El ciclo de vida (estado)

Un acuerdo avanza a través de estas etapas. La automatización del correo electrónico solo avanza el estado, por lo que el registro refleja el punto más lejano que ha alcanzado la conversación:

`Consultado → Negociación IOT → IOT Pendiente de Firma → IRA Negociando → Esperando Firmas IRA → IRA Firmado → Tarifas Acordadas → Intercambio de SIM → Pruebas → Lanzado` (más `Lanzamiento por Defecto`, `Suspendido`, `Terminado`).

Abrir un socio

Haz clic en un socio para abrir su página de **detalles**: un conjunto de pestañas/secciones que cubren todo sobre la relación:

- **Resumen y línea de tiempo**: estado, prioridad, notas y el registro de actividad (cada correo electrónico, documento generado, firma y nota manual en orden de fecha).
- **TADIGs**: los códigos de red del socio (con MCC/MNC, tipo de conexión y dirección). Una acción de **"encontrar candidatos"** puede extraer los otros TADIGs del operador socio del catálogo IR.21 para que los revises y añadas.
- **Contactos**: personas de roaming/comerciales/técnicas en el socio.
- **Tarifas**: los niveles de tarifas comerciales acordadas (datos/SMS/voz, moneda, unidad).
- **SIMs y solicitudes de SIM**: SIMs de prueba intercambiadas y lotes solicitados para envío.
- **Documentos**: papeleo generado y recibido (ver más abajo).
- **Enrutamiento**: rutas DRA, títulos globales SS7, rangos de DNS e IP para aprovisionamiento (gran parte de ello pre-poblado del IR.21 del socio).

Todo en la página de detalles es **editable**. La automatización te da una ventaja inicial, y puedes corregir o añadir a mano según sea necesario.

El catálogo IR.21

Las búsquedas de TADIG se basan en un **catálogo global de operadores IR.21** indexado por TADIG (organización, red, MCC/MNC, DNS, rangos de IP, nodos SS7, contactos). Así es como OmniRoam valida un TADIG que la IA extrajo, descubre los TADIGs hermanos de un socio y pre-puebla los datos de enrutamiento.

---

3. Generación y Firma Automática de Documentos

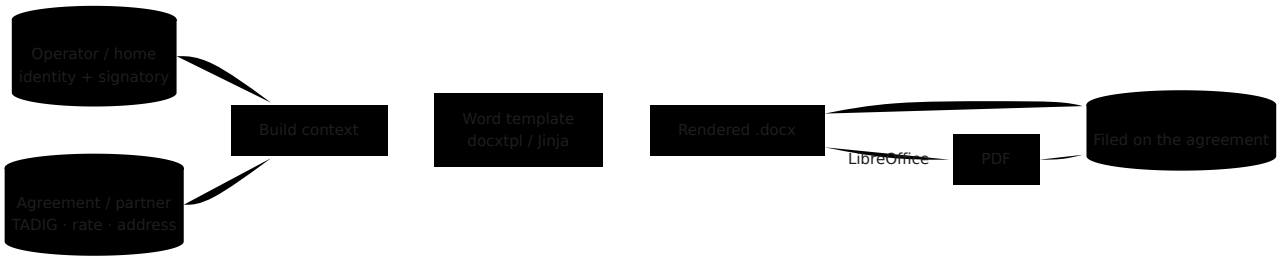
Generando un documento

En la sección de **Documentos** de un acuerdo, eliges un tipo de documento y haces clic en **Generar**. OmniRoam renderiza el verdadero formulario de Word, lleno con los detalles de ambas partes, listo para firmar:

Tipo	Qué es	Formato
AA.12	Acuerdo de roaming GSMA AA.12 IREG (el formulario real, pre-llenado por ambas partes)	.docx / PDF
AA.13	Anexos comunes GSMA AA.13, incluyendo el anexo de facturación/ajuste (ver opciones de ajuste AA.13)	.docx / PDF
CLL	Carta de Lanzamiento Comercial (genérica)	.docx / PDF
CLL (Bilateral / Unilateral, después de pruebas)	Carta de lanzamiento que confirma la fecha de inicio **después de pruebas exitosas de IREG y TADIG**	.docx / PDF
CLL (Bilateral / Unilateral, por defecto)	Carta de lanzamiento para un lanzamiento **por defecto, sin completar pruebas de IREG/TADIG**	.docx / PDF
TCC (VoLTE)	Finalización de Llamadas de Prueba VoLTE	.docx / PDF
Finalización de TADIG	Formulario de finalización de TADIG	.docx / PDF
Formulario de Acuerdo de Roaming TNS	Solicitud de clearing-house TNS (entregada como .doc legado)	.doc
Solicitud TNS 3G-4G	Solicitud de clearing-house TNS	.docx

Cómo se llenan los campos. Cada documento es una plantilla de Word con marcadores de posición (docxtpl / Jinja). OmniRoam los llena de:

- **El lado local**: de tu registro de **Operador**: tu nombre, nombre legal, TADIG, PLMN, país, **firmante y título**, lugar y dirección. Debido a que esto proviene del inquilino, cada operador alojado obtiene su *propio* membrete y firmante automáticamente.
- **El lado del socio**: del **Acuerdo**: nombre del socio, su abreviatura de forma corta utilizada en el cuerpo del contrato, TADIG(s), PLMN(s), país y dirección. El propio firmante/título del socio queda en blanco, por lo que esa línea se deja lista para que ellos firmen.
- **Valores derivados**: fecha efectiva, dirección (bilateral/entrante/saliente), empresa central, dominios Diameter, moneda y la tarifa IOT confirmada.



Formato de salida: Word por defecto, PDF para firmar

La generación produce un **Word** `.docx` editable por defecto. Esa es la copia de trabajo que revisas y editas a mano si es necesario. Obtienes un PDF solo cuando realmente necesitas un renderizado fijo y final:

- Marca la casilla de **salida PDF** antes de hacer clic en Generar para renderizar un PDF en lugar del `.docx`.
- El flujo de **firma electrónica** siempre utiliza PDF (el artefacto firmado no debe cambiar).
- **Descargar / previsualizar** un documento archivado *como PDF* bajo demanda.

Un correo electrónico de **Paquete de Roaming** adjunta el AA.12/AA.13 como `.docx` editable para que el socio pueda revisar y comentar. No es el paso de firma, por lo que no se envía como PDF.

Opciones de ajuste AA.13 (Anexo C.3.2)

El Anexo C.3.2 de GSMA AA.13 (facturación y ajuste) es un **menú de opciones** que cada socio negocia: qué modelo de factura, qué método de pago, el umbral y período de ajuste, términos de pago e interés. En lugar de bloquear un conjunto de opciones en la plantilla, OmniRoam las expone como un panel de opciones de ajuste en la sección de **Documentos**: expande **opciones de ajuste AA.13**, establece los valores para este socio y luego haz clic en **Generar AA.13**. El anexo generado contiene solo las opciones que elegiste. Las alternativas (y la estructura de "eliminar aquellas que no aplican" de GSMA) se eliminan automáticamente.

Cada campo tiene un valor predeterminado sensato, por lo que generar sin tocar el panel produce los términos estándar; cambia solo lo que difiere para un socio dado.

Opción	Predeterminado	Descripción
Tipo de factura	Factura de red única (SNI)	Selecciona el anexo de ajuste: **Red única (SNI)** → Anexo C.3.2 H, o **Red múltiple (MNI)** → Anexo C.3.2 I. El anexo no utilizado se elimina.
Método de pago	Ajuste neto	El mecanismo de ajuste: **Ajuste neto**, **Pago completo directo (sin conversión)**, **Pago completo directo (con conversión)**, o **Ajuste sin conversión**. Solo se mantiene la cláusula del método elegido.
Ajuste de umbral	Opción 1 (Ajuste)	**Opción 1 (Ajuste)** aplica un único umbral de saldo bajo acordado; **Opción 2 (Pago directo)** utiliza umbrales por parte (Parte A / Parte B).
Umbral	50	Monto del umbral de ajuste de saldo bajo, en la moneda de ajuste del acuerdo (por ejemplo, SDR). Por debajo de este agregado mensual, el ajuste puede ser diferido.
Inicio del período / **Fin del período**	Enero / Diciembre	El período no de ajuste para saldos por debajo del umbral, típicamente el año financiero.
Días de pago	60	Días desde la fecha de la factura dentro de los cuales el deudor debe pagar.
Interés hogar %	8	Interés anual que el acreedor puede cobrar sobre saldos vencidos cuando el operador **local** es el acreedor.

Opción	Predeterminado	Descripción
Interés socio %	8	Interés anual cuando el operador **socio** es el acreedor.
Enviar facturas de valor cero	Apagado	Cuando está apagado, el anexo indica que cada parte **no enviará** facturas mensuales con un monto cero (0.00).
BCE en factura TAP	Apagado	Cuando está apagado, el anexo indica que el uso de BCE **no se incluirá** en la Factura de Roaming TAP.

Cómo funciona. Las elecciones se pasan a la generación como sobrescrituras sobre los valores predeterminados incorporados. La plantilla AA.13 las resuelve en el anexo terminado: selecciona los bloques de opción correctos, llena los montos/períodos/tarifas y formula los toggles. La moneda de ajuste en sí proviene de la moneda configurada del acuerdo, no de este panel.

Caso de uso. Un socio insiste en términos de 90 días, un umbral de 100 SDR y un año financiero de abril a marzo: abre el panel, establece **Días de pago** 90, **Umbral** 100, **Inicio del período** abril, **Fin del período** marzo y genera. Cada otra cláusula se mantiene en los términos estándar.

> **Los formularios de clearing-house TNS son especiales.** Las dos solicitudes TNS *no* son plantillas docxtpl. Son los formularios TNS genuinos del operador con solo los campos rellenables cambiados y las casillas de verificación correctas marcadas, para que TNS reciba exactamente el diseño que espera. Son **IOT-gated**: OmniRoam no los genera hasta que el acuerdo tenga una **tarifa confirmada (acordada)**. Intentar antes devuelve un claro mensaje de "se requiere un IOT confirmado". Los estados de las casillas de verificación (tipo de acuerdo, dirección, servicios, interfaces LTE, GRX) se derivan automáticamente del acuerdo, y todos los campos son sobrescribibles en el momento de la generación.

LibreOffice sin cabeza en el servidor realiza la generación de PDF (y el legado `.doc` para TNS). Solo obtienes el archivo terminado.

La sección de Documentos de un acuerdo. Genera un contrato a la izquierda; documentos generados y recibidos (con estado de firma) listados abajo, cada uno descargable.

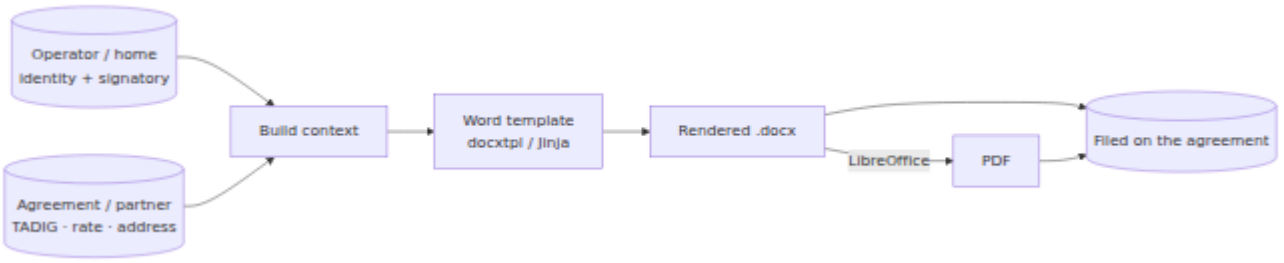
Firma: en línea o fuera de línea

OmniRoam admite dos rutas de firma:

Firma electrónica en línea (el socio firma en el navegador, sin inicio de sesión). Desde un AA.12/AA.13 generado, haces clic en **Enviar para firma**, nombras al firmante y su correo electrónico, y OmniRoam:

1. Crea una solicitud de firma con un token opaco y envía un **enlace seguro** por correo electrónico al socio (no se necesita cuenta).
2. Cuando lo abren, OmniRoam marca la solicitud como *vista* y la registra en la línea de tiempo. Revisan el documento, corrigen opcionalmente su nombre/título/empresa del firmante, y **firman** escribiendo su nombre y/o dibujando una firma.
3. OmniRoam produce el **PDF firmado** y lo envía por correo electrónico a **ambas partes** (firmante + el buzón de retorno de tu operador), lo archiva en el acuerdo y registra "Firmado por … el …".

4. El socio también puede **rechazar** (con un motivo), lo cual también se registra.



Firma fuera de línea. ¿Prefieres firmar de la manera tradicional? Descarga el documento generado, fírmalo externamente y vuelve a subir la copia firmada al acuerdo. Un nombre de archivo que contenga *firmado*/*ejecutado*/*contrafirmado* se reconoce como una copia firmada. Un correo electrónico entrante que adjunte uno avanza el estado a *IRA Firmado* automáticamente.

El Paquete de Roaming: primer contacto con un clic

En lugar de generar cada formulario por separado, **Enviar paquete de roaming** envía a un contacto del socio el **AA.12 + AA.13 + oferta IOT** juntos en un solo mensaje. Genera los contratos como PDFs sobre la marcha y adjunta tu oferta IOT más reciente. Elige un contacto (o escribe un nombre + correo electrónico, que se completa como un contacto), y OmniRoam envía el paquete con tu redacción de plantilla guardada. Este es el correo electrónico de apertura "hagamos un acuerdo de roaming", enviado desde dentro de OmniRoam.

Plantillas de correo electrónico editables

Los tres correos electrónicos automatizados (**solicitud de firma**, **copia firmada** y **paquete de roaming**) utilizan plantillas editables (sobrescritura por operador, de lo contrario un predeterminado global), con marcadores de posición como `{{ signer_name }}`, `{{ partner }}`, `{{ operator }}`, `{{ sign_url }}` y `{{ document_name }}`. Ajusta la redacción una vez en Configuraciones y cada envío la utiliza.

> **Cómo sale realmente el correo electrónico de OmniRoam.** Todo el correo saliente pasa a través de la **API de Envío HTTPS de Mailjet**, no

> SMTP. Las plataformas de alojamiento (Railway) bloquean los puertos SMTP salientes, por lo que OmniRoam envía por POST a Mailjet a través de HTTPS en su lugar. Los envíos son **mejor esfuerzo y no bloqueantes**: el botón de la interfaz de usuario devuelve inmediatamente y el correo se envía en un hilo en segundo plano, por lo que un servidor de correo lento nunca detiene la aplicación.

---

4. Archivo y Almacenamiento

Cada documento se archiva **directamente en el acuerdo** al que pertenece. Esto cubre documentos **generados** (AA.12, AA.13, CLL, TCC, TNS…) y documentos **recibidos** (una copia firmada adjunta a un correo electrónico, un IR.21 subido, una hoja IOT). No hay un almacén de documentos separado que gestionar:

- Los documentos se almacenan como blobs **en la base de datos**, etiquetados con un **tipo** (`aa12`, `aa13`, `aa12_signed`, `iot`, `ir21`, `cll`, `other`, …), nombre de archivo, tipo de contenido, tamaño y si OmniRoam **lo generó**.
- Las copias firmadas se etiquetan de manera distinta (por ejemplo, `aa12_signed`) para que el conjunto firmado siempre sea distinguible de los borradores.
- **Los adjuntos entrantes se deduplican**: una copia idéntica (mismo nombre de archivo + longitud de bytes) que llega nuevamente no se vuelve a archivar.
- Cada generación, carga, firma y exportación de IOT escribe una **entrada de línea de tiempo**, por lo que el registro de actividad del acuerdo es un rastro completo de lo que se produjo y recibió, y cuándo.

Para recuperar un documento, abre la sección de **Documentos** del acuerdo y descárgalo (Word/PDF generado, o el original recibido). Los PDFs firmados producidos por el flujo de firma en línea se almacenan en la solicitud de firma y también se envían por correo electrónico a ambas partes.

También puedes **exportar la tarifa acordada como un archivo XML GSMA RAEX IOT 5.0** desde el acuerdo. Esta es la misma selección de tarifas que

utilizan los formularios TNS, por lo que el IOT exportado y los formularios generados siempre concuerdan.

---

5. Órdenes de Trabajo y Notificaciones a Asignados

Poner en marcha a un socio es *trabajo*: enviar SIMs, cambiar enrutamiento, realizar pruebas IREG/TADIG, auditorías, resolver problemas. En OmniRoam ese trabajo se rastrea como **Órdenes de Trabajo**: la única unidad rastreada de trabajo de roaming. Una orden de trabajo puede depender de un acuerdo (un socio) o ser independiente.

La vista de Órdenes de Trabajo. Cada orden tiene un tipo, prioridad, estado, enlace opcional al socio y un asignado: la parte notificada cuando se le asigna.

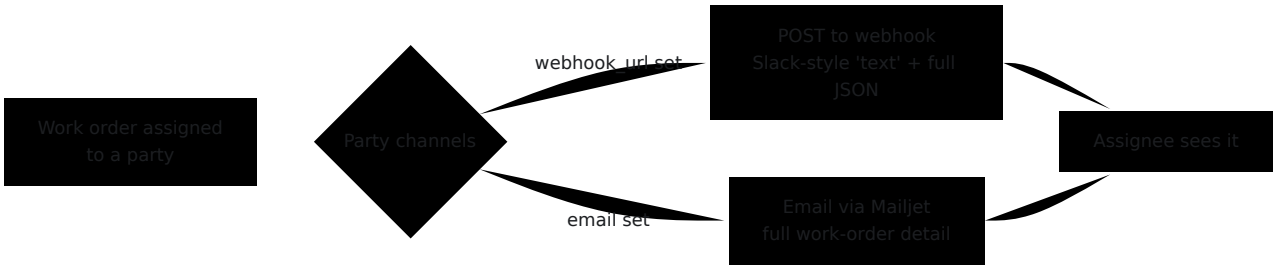
Creando y asignando

Una orden de trabajo tiene un **tipo** (Envío de SIM, Enrutamiento, Pruebas IREG, Pruebas TADIG, Auditoría, Problema), un título, prioridad, estado (Abierto / En Progreso / Bloqueado / Hecho / Cancelado), un enlace opcional al socio (acuerdo), detalles de texto libre, una fecha de vencimiento y campos estructurados específicos del tipo (por ejemplo, un Envío de SIM lleva cantidad, dirección postal, transportista y seguimiento).

Asignas una orden de trabajo a una **parte**: un equipo interno nombrado o contacto externo (por ejemplo, "Roaming NOC", "administrador de TADIG") gestionado por operador en **Configuraciones**. Puedes establecer un **asignado predeterminado por tipo de orden de trabajo**, por lo que un nuevo Envío de SIM se asigna automáticamente a quien maneja el envío a menos que lo sobrescribas.

La notificación: webhook + correo electrónico

Cuando una orden de trabajo es **asignada** (creada con un asignado, o reasignada a una nueva parte), OmniRoam **notifica a ese asignado** a través de los canales que la parte ha configurado:



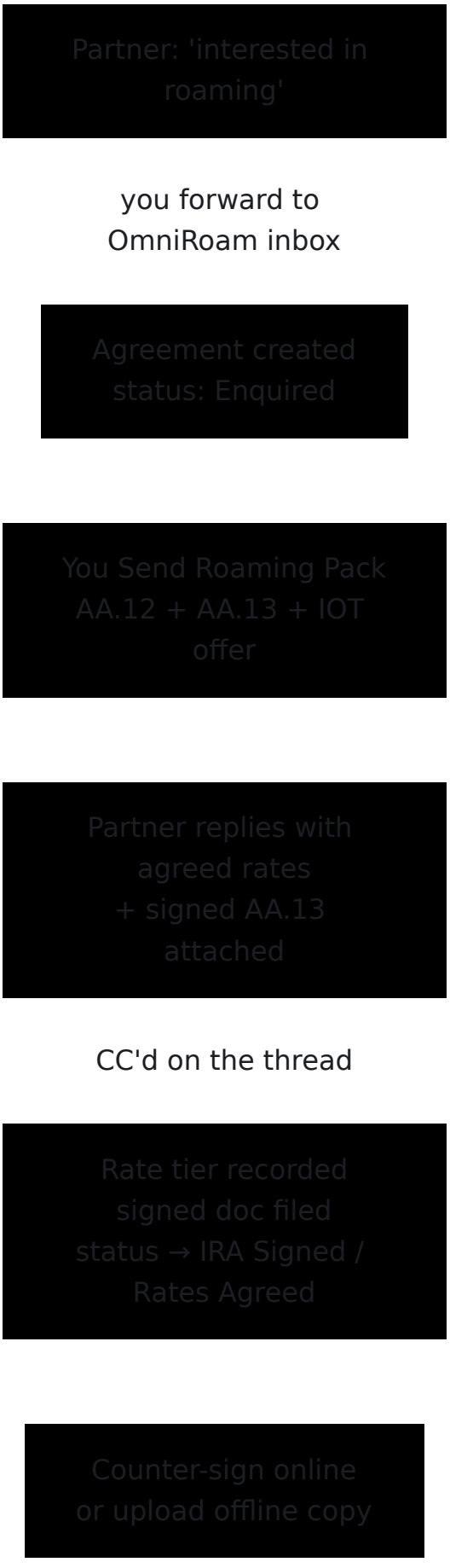
- **Webhook**: si la parte tiene una URL de webhook (por ejemplo, un **webhook entrante de Slack**), OmniRoam envía un mensaje con un bloque `text` legible por humanos *y* la orden de trabajo completa como JSON estructurado (tipo, prioridad, estado, socio, la carga útil específica del tipo, un enlace de regreso a la página de Órdenes de Trabajo).
- **Correo electrónico**: si la parte tiene una dirección de correo electrónico, OmniRoam envía el mismo detalle como un correo electrónico (a través de Mailjet), asunto `[Orden de Trabajo] <título> asignada a ti`.

Una parte con **ninguno** de los canales configurados es simplemente un asignado silencioso (no-op). Ambas notificaciones son de mejor esfuerzo y no bloqueantes, por lo que un webhook o servidor de correo lento nunca puede detener la aplicación. La reasignación solo notifica cuando el asignado realmente **cambia** a una nueva parte (por lo que editar otros campos no vuelve a notificar a las personas).

> **Desde la silla del asignado:** recibes un mensaje de Slack (o correo electrónico) en el momento en que un trabajo llega a tu equipo, con todo lo que necesitas: qué hacer, para qué socio, la cantidad de SIM y dirección de envío (o el cambio de enrutamiento, o el alcance de la prueba), la prioridad y la fecha de vencimiento, y un enlace directo a la orden de trabajo.

El Ciclo de Vida Completo, de Principio a Fin

Poniéndolo todo junto, este es el viaje desde "un socio nos envió un correo" hasta "el socio está en funcionamiento":


Partner: 'interested in roaming'
you forward to OmniRoam inbox
Agreement created status: Enquired
You Send Roaming Pack AA.12 + AA.13 + IOT offer
Partner replies with agreed rates + signed AA.13 attached
CC'd on the thread
Rate tier recorded signed doc filed status → IRA Signed / Rates Agreed
Counter-sign online or upload offline copy



En cada paso, la **línea de tiempo** del acuerdo registra lo que sucedió, y el **registro de correos electrónicos entrantes** mantiene la evidencia en bruto de lo que cada correo electrónico contribuyó.

Lo Que Configuras Una Vez

La mayor parte de la automatización solo necesita una pequeña configuración única por operador (en **Configuraciones**):

Configuración	Por qué	Dónde se utiliza
Detalles del papeleo (nombre legal, TADIG, PLMN, país, **firmante y título**, lugar, dirección)	Llena el lado local de cada documento generado	Generación de documentos
Dirección de correo electrónico entrante	La dirección a la que reenvías/CC el correo del socio	Ingesta de correos electrónicos
Buzón de retorno firmado	Donde van los correos electrónicos de copia firmada y firmados fuera de línea	Firma
Plantillas de correo electrónico (solicitud de firma, copia firmada, paquete de roaming)	Tu redacción para los correos electrónicos automatizados	Correo electrónico saliente
Partes de órdenes de trabajo + asignados predeterminados por tipo	Quién recibe notificaciones para cada tipo de trabajo	Órdenes de trabajo

Con eso en su lugar, reenviar un correo electrónico de un socio realmente se convierte en: *correo electrónico entrante → acuerdo saliente → contratos generados y firmados → órdenes de trabajo creadas y tu equipo notificado.*

Ver También

- OmniRoam: Automatización de Pruebas de Roaming: el *otro* OmniRoam. Ejecuta los libros de pruebas de roaming GSMA (IR.38 / IR.48 / VoLTE) contra una red en vivo. Esto es complementario: firma el acuerdo aquí, demuestra que funciona allí.
- Operaciones Comunes: los patrones de visualización/edición compartidos en toda OmniWeb.

OmniRoam: Automatización de Pruebas de Roaming

OmniRoam es la función de automatización de libros de pruebas de roaming de OmniWeb. Ejecuta los libros de pruebas de cumplimiento de roaming de GSMA contra una red en vivo. Conduce los casos de prueba individuales automáticamente desde un dispositivo de prueba. Registra un veredicto de aprobado/reprobado con evidencia de apoyo para cada caso. Luego produce un libro de trabajo de GSMA completado listo para enviar a un socio de roaming o hub.

En resumen: OmniRoam convierte un ejercicio manual de cumplimiento de roaming de varias horas en una pulsación de botón (o un trabajo programado). Devuelve la misma hoja de cálculo oficial de GSMA que un evaluador llenaría a mano.

> **OmniRoam tiene dos lados.** Este documento cubre los **libros de pruebas de roaming** (IR.38 / IR.48 / pruebas de conformidad de VoLTE: *¿funciona realmente el roaming?*). El otro lado es la **automatización de acuerdos de roaming y correos electrónicos**. Convierte un correo electrónico de socio en un acuerdo firmado, generando la documentación AA.12/AA.13/CLL/TCC/TNS y las órdenes de trabajo para poner al socio en vivo. Eso está documentado por separado en **Acuerdos de Roaming y Automatización de Correos Electrónicos**. Un producto, dos trabajos: *obtener el acuerdo firmado* (allí) y *probar que el roaming funciona* (aquí).

La pantalla de Libros de Pruebas de Roaming. Cada fila es un libro ejecutado contra un socio de roaming, con su estado actual.

Enlaces Rápidos

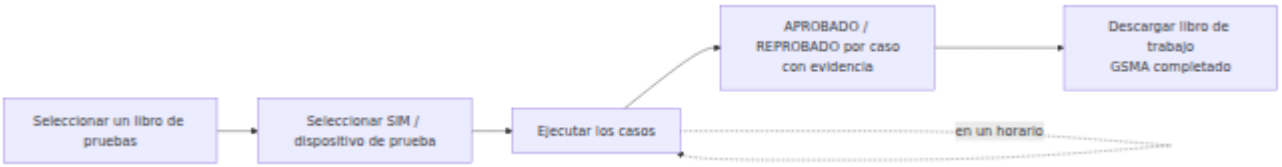
- **Libros de Pruebas**: los libros disponibles (IR.38, IR.48, VoLTE) y cada caso de prueba que contienen
- **Ejecutando Pruebas**: cómo crear un libro, ejecutarlo, personalizar el conjunto de casos y programar ejecuciones rutinarias
- **Explorador de Libros de Pruebas**: cómo inspeccionar qué prueba cada libro y cómo se ejecuta cada caso
- **Documentos de Libros de Pruebas Completados**: cómo OmniRoam genera el libro de trabajo de GSMA completado
- **Acuerdos de Roaming y Automatización de Correos Electrónicos**: el *otro* lado de OmniRoam. Reenviar un correo electrónico de socio → acuerdo creado, contratos generados y firmados electrónicamente, archivados y órdenes de trabajo levantadas

Qué Hace OmniRoam

Un libro de pruebas de roaming es una lista de verificación definida por la GSMA: una lista de casos de prueba que demuestran que un suscriptor de una red (el **PLMN de Origen**, "PLMN(a)") recibe los servicios esperados mientras está en roaming en otra red (el **PLMN Visitado**, "PLMN(b)"). Históricamente, cada caso se realiza a mano y el resultado se escribe en una hoja de cálculo.

OmniRoam automatiza tres cosas:

1. **Conducción de la prueba**: realiza la llamada, envía el SMS, ejecuta la sesión de datos o provisiona el servicio suplementario en un dispositivo de prueba.
2. **Juicio del resultado**: compara lo que sucedió con el resultado esperado de GSMA. Registra **APROBADO**, **REPROBADO** o **NO REALIZADO**, con la evidencia de apoyo (tiempos, rendimiento, causas de liberación de red, etc.).
3. **Producción del documento**: llena el libro de trabajo oficial de GSMA con los resultados y todos los metadatos circundantes (identidades, fechas, detalles del evaluador).



Dónde Encaja

OmniRoam ejerce un suscriptor real en la red real utilizando un dispositivo de prueba gestionado. Cada caso automatizado conduce el dispositivo, luego lee el resultado de vuelta del dispositivo y, cuando es aplicable, de los propios registros de la red (por ejemplo, los registros de carga del gateway de servicio para una sesión de datos). Nada es simulado: una llamada que se informa como conectada realmente se conectó.


OmniWeb
Motor de libro de pruebas OmniRoam
conduce pruebas
Dispositivo de prueba gestionado + SIM de suscriptor
Generador de documentos
se conecta / llama / envía
lee resultados y registros
libro de trabajo GSMA completado
Red Móvil bajo prueba
Acceso Radio 2G / 3G / 4G / 5G
Red Central voz · SMS · datos · IMS
Operador / Socio de roaming

Conceptos Clave

Término	Significado
Libro de pruebas	Un conjunto de casos de prueba definido por GSMA (por ejemplo, IR.38, IR.48, VoLTE). Ver Libros de Pruebas.
Caso de prueba	Una verificación única dentro de un libro, identificada por su número de GSMA (por ejemplo, caso `2.3` de IR.48, "Prohibición de Todas las Llamadas Salientes").
Ejecución	Una ejecución de un libro (o un subconjunto elegido de sus casos) contra un dispositivo y SIM.
Veredicto	El resultado registrado de un caso: `APROBADO`, `REPROBADO` o `NO REALIZADO`.
Evidencia	El detalle de apoyo capturado para un veredicto: tiempos, cifras de rendimiento, causas de red, lecturas de interrogación, etc.
PLMN de Origen (a)	La red que posee el suscriptor que se está probando.
PLMN Visitado (b)	La red en la que el suscriptor está en roaming.

Casos Automatizados vs. Manuales

La mayoría de los casos en cada libro son **auto-conducidos**: OmniRoam los realiza de extremo a extremo y registra el veredicto sin interacción del operador. Algunos casos dependen de condiciones de red que no se pueden inducir desde un dispositivo de prueba solo (por ejemplo, las pruebas negativas opcionales de CAMEL prepago, o la entrega de mensajes multimedia). Estos

permanecen **manuales**. OmniRoam aún los lista en el libro y el operador registra el resultado a mano, por lo que el documento final está completo.

El Explorador de Libros de Pruebas muestra exactamente qué casos en un libro son automatizados y cómo se ejecuta cada uno.

Normas Referenciadas

OmniRoam sigue los Documentos de Referencia Permanentes de GSMA y las especificaciones subyacentes de 3GPP:

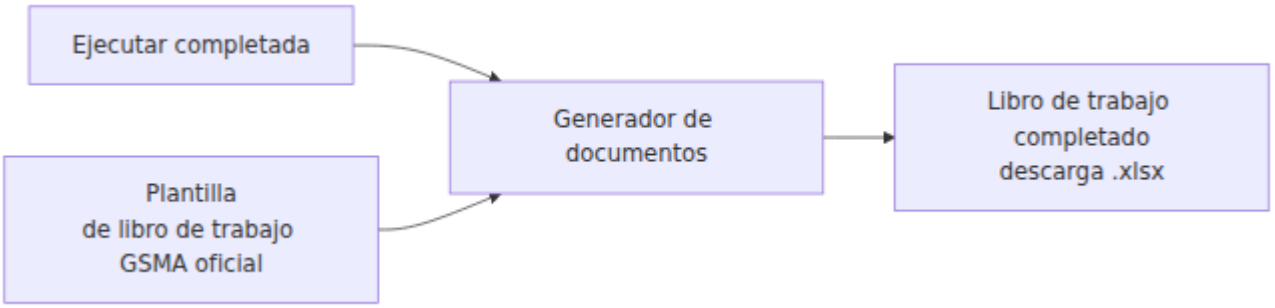
Referencia	Aplica a
GSMA IR.38	Libro de pruebas de datos de roaming LTE
GSMA IR.48 / IR.24	Libro de pruebas de roaming bilateral (voz / SMS / MMS / datos)
GSMA BA.65	Pruebas de VoLTE en roaming
GSMA IR.92	Perfil IMS para voz y SMS (comportamiento de VoLTE)
GSMA IR.88	Directrices de roaming LTE (causas de rechazo de conexión)
3GPP TS 22.011	Accesibilidad del servicio (prohibición determinada por el operador)
3GPP TS 23.011	Estado del servicio suplementario (Activo/Registrado/Provisionado/En reposo)
3GPP TS 22.082	Servicios suplementarios de desvío de llamadas
3GPP TS 22.088	Servicios suplementarios de prohibición de llamadas

Documentos de Test-Book Completados

El producto final de una ejecución de OmniRoam es un **libro de pruebas GSMA completado**: la hoja de cálculo oficial de GSMA para el libro, llena con los resultados de la ejecución y todos los detalles circundantes, lista para enviar a un socio de roaming o hub. OmniRoam lo produce con una única acción de **Descargar Libro de Pruebas**. No necesita transcripción manual.

Lo Que Obtienes

OmniRoam toma la plantilla oficial de GSMA para el libro y la completa en su lugar, por lo que el resultado es el mismo libro que un socio espera recibir (mismas hojas, misma numeración de casos, mismo diseño), pero poblado con resultados reales en lugar de campos en blanco.



Qué Se Rellena

Tres categorías de información se escriben en el libro de trabajo.

1. Resultados por caso

Para cada caso en el libro, la celda de resultado del libro de trabajo se establece en el veredicto registrado (**APROBADO**, **RECHAZADO** o **NO REALIZADO**). La celda de comentarios del caso se llena con la evidencia de apoyo capturada durante la ejecución.

En el documento	Proviene de
Resultado del caso de prueba (APROBADO / RECHAZADO / NO REALIZADO)	El veredicto del caso
Comentarios del caso de prueba	La evidencia: tiempos, rendimiento, causas de red, lecturas de interrogación, etc.

2. Identidades y metadatos

Las secciones de encabezado e información del operador se llenan a partir de la ejecución:

En el documento	Proviene de
IMSI	La SIM de prueba
MSISDN	La SIM de prueba
PLMN de origen (a) / PLMN visitado (b)	El socio de roaming / PLMNs elegidos para el libro
Fecha de las pruebas	La fecha de la ejecución
Nombre del probador, teléfono, correo electrónico	Los detalles del probador en el libro
APN (donde sea aplicable)	La configuración de datos utilizada

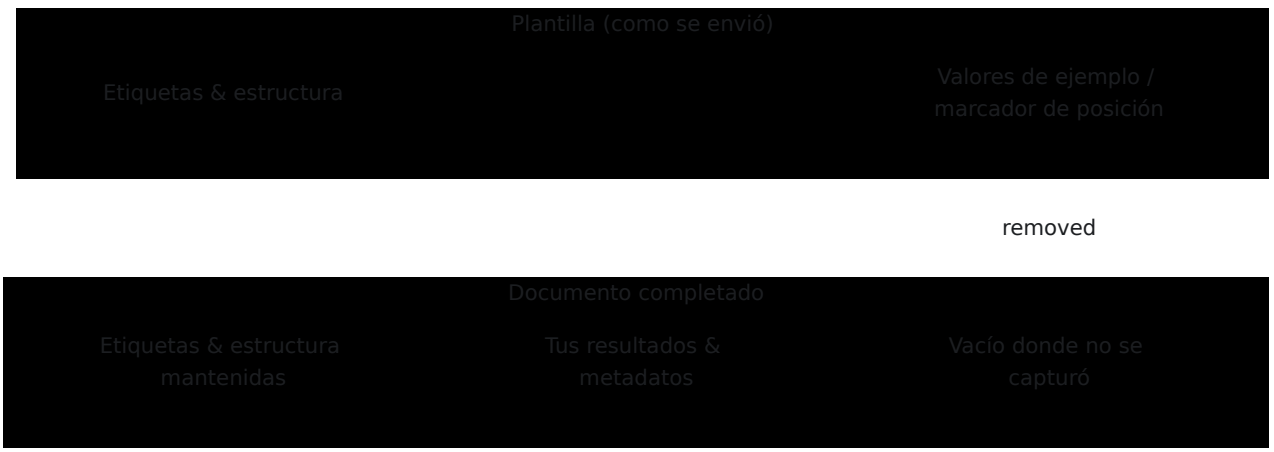
3. Valores medidos

Para los casos de datos y servicios suplementarios, los valores medidos específicos que la hoja de GSMA solicita se escriben en sus celdas dedicadas:

En el documento	Proviene de
Tiempos de inicio / fin de la sesión de datos	La sesión de datos
Volúmenes de datos enviados / recibidos	Los registros de carga del gateway de servicio
Duración de la sesión	La sesión de datos
Rendimiento / tasa de datos media	La medición de rendimiento
Indicaciones de éxito del servicio (Sí/No)	El resultado del caso

Salida Limpia y Presentable

Las plantillas GSMA en blanco se envían con contenido de ejemplo y marcador de posición en las celdas de llenado: tiempos de muestra y notas de referencia destinadas a guiar a un probador manual. OmniRoam elimina ese contenido de marcador de posición cuando genera el documento, por lo que el libro de trabajo completado muestra solo tus resultados reales y campos vacíos donde no se capturó un valor. Nunca lleva los datos de muestra del proveedor a tu informe entregado, y nunca sobrescribe las etiquetas, encabezados o estructura de GSMA.



Cuándo Generar

Puedes descargar el documento en cualquier momento. Siempre refleja el estado actual de la ejecución. Un flujo típico es ejecutar el libro (o rutina programada), revisar los veredictos por caso, volver a ejecutar cualquier caso que necesite atención, y luego descargar el libro de trabajo terminado una vez que los resultados se vean correctos. Dado que la exportación refleja la ejecución en vivo, una re-exportación después de una re-ejecución simplemente produce un documento actualizado.

Casos Manuales en el Documento

Los casos que OmniRoam no puede manejar automáticamente aún aparecen en el libro de trabajo con su número de caso y título, listos para que el probador registre un resultado a mano. Esto mantiene el documento entregado completo: los casos automatizados están llenos de evidencia real, y los casos manuales se presentan en el lugar correcto para que el probador termine.

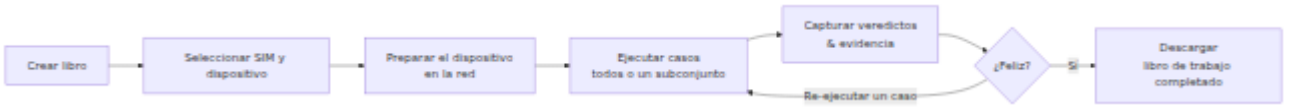
Consulta Ejecutando Pruebas para ver cómo se producen los veredictos y Explorador de Libro de Pruebas para el mapeo exacto celda por celda de lo que se llena.

Ejecución de Pruebas de OmniRoam

Esta guía cubre todo el ciclo de vida de una prueba de roaming: crear un libro, ejecutarlo, observar la ejecución de los casos, personalizar qué casos se ejecutan, volver a ejecutar un solo caso y programar ejecuciones rutinarias no atendidas.

- El Ciclo de Vida de la Prueba
- Creando un Libro de Pruebas
- Ejecutando un Libro
- Cómo se Controlan los Casos Automatizados
- Personalizando una Ejecución
- Volviendo a Ejecutar un Solo Caso
- Ejecuciones Rutinarias y Programadas
- Leyendo los Resultados

El Ciclo de Vida de la Prueba



Creando un Libro de Pruebas

La pantalla de Libros de Pruebas de Roaming lista cada libro con su tipo, las redes de origen y visitadas, la identidad del suscriptor, el probador y el estado actual.

Un libro de pruebas se crea desde la pantalla de **Libros de Pruebas de Roaming**. Al crear un libro, eliges:

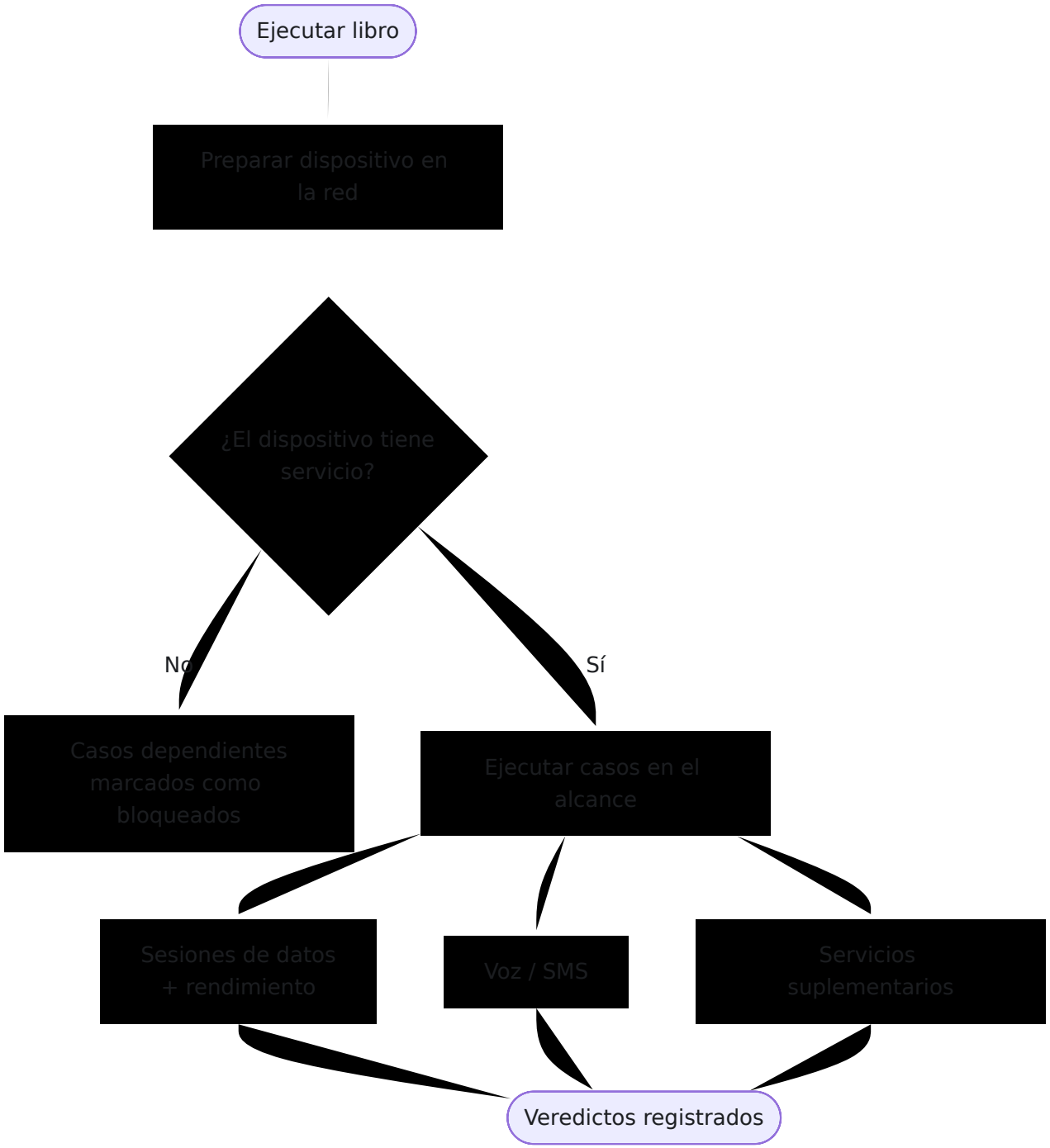
Campo	Propósito
Tipo de libro	Qué libro GSMA ejecutar: IR.38, IR.48 o VoLTE. Esto selecciona el conjunto de casos.
Socio de roaming / PLMNs	Las redes de origen (PLMN a) y visitadas (PLMN b). Se utilizan para completar el encabezado del documento y para elegir el umbral de rendimiento correcto.
SIM	La SIM del suscriptor con la que se va a probar. Su IMSI y MSISDN se leen y utilizan durante toda la ejecución y en el documento final.
Detalles del probador	Nombre, teléfono y correo electrónico de la persona responsable, escritos en el libro de trabajo completado.

Una vez creado, el libro lista cada caso del libro GSMA elegido, cada uno comenzando en un estado de "no realizado aún".

Ejecutando un Libro

Ejecutar un libro realiza cada caso en el alcance por turno. Antes de que se ejecuten los casos de prueba, OmniRoam prepara el dispositivo de prueba en la red. Presenta la SIM y confirma que el dispositivo se ha conectado y tiene servicio. Esta es una **puerta de requisito**: si el dispositivo no puede obtener servicio, los casos dependientes se informan como bloqueados en lugar de fallidos, porque no tiene sentido realizar una prueba de datos o voz sin portadora.

Como parte de la preparación del dispositivo, OmniRoam **lee la identidad del suscriptor del módem y llena el libro automáticamente**: el **IMSI** se lee de la SIM, la **red de origen (HPLMN)** se deriva de ella, y la **red visitada (VPLMN)** se lee de la red en la que el dispositivo está actualmente acampado. Estos completan el encabezado del libro, y por lo tanto el documento completado, con lo que realmente se probó, en lugar de con valores escritos a mano.



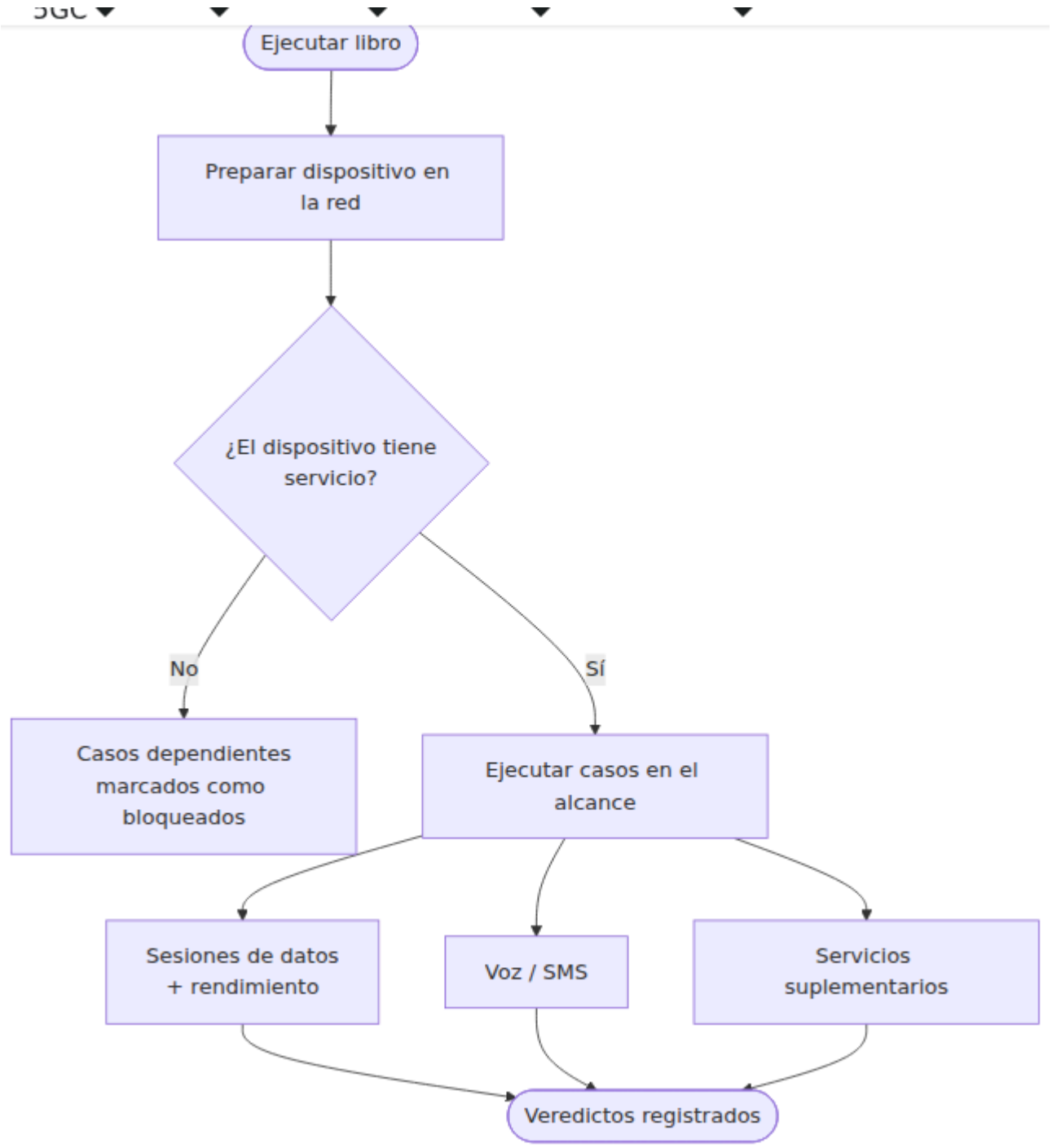
Mientras un libro se ejecuta, la pantalla muestra cada paso a medida que ocurre, con el paso actual resaltado y una indicación en vivo de aprobación/reprobación por caso.

Cómo se Controlan los Casos Automatizados

Cada caso automatizado controla el dispositivo de prueba, observa lo que hace la red y compara el resultado con el resultado esperado de GSMA. Un caso solo pasa con evidencia positiva. Un paso que no puede ser confirmado se registra como un fallo con la razón, nunca como un pase silencioso.

Sesiones de datos y rendimiento

Para los casos de datos, OmniRoam establece una sesión de datos por paquetes, ejecuta tráfico para medir la tasa de descarga/subida lograda y la latencia, luego se desconecta para que la red escriba un registro de carga limpio para la sesión. Los volúmenes de datos y los tiempos se leen de los registros de carga del gateway de servicio. Para el caso de velocidad IR.38, la tasa medida se afirma contra el umbral de rendimiento para la distancia de origen/visitada.



Llamadas de voz

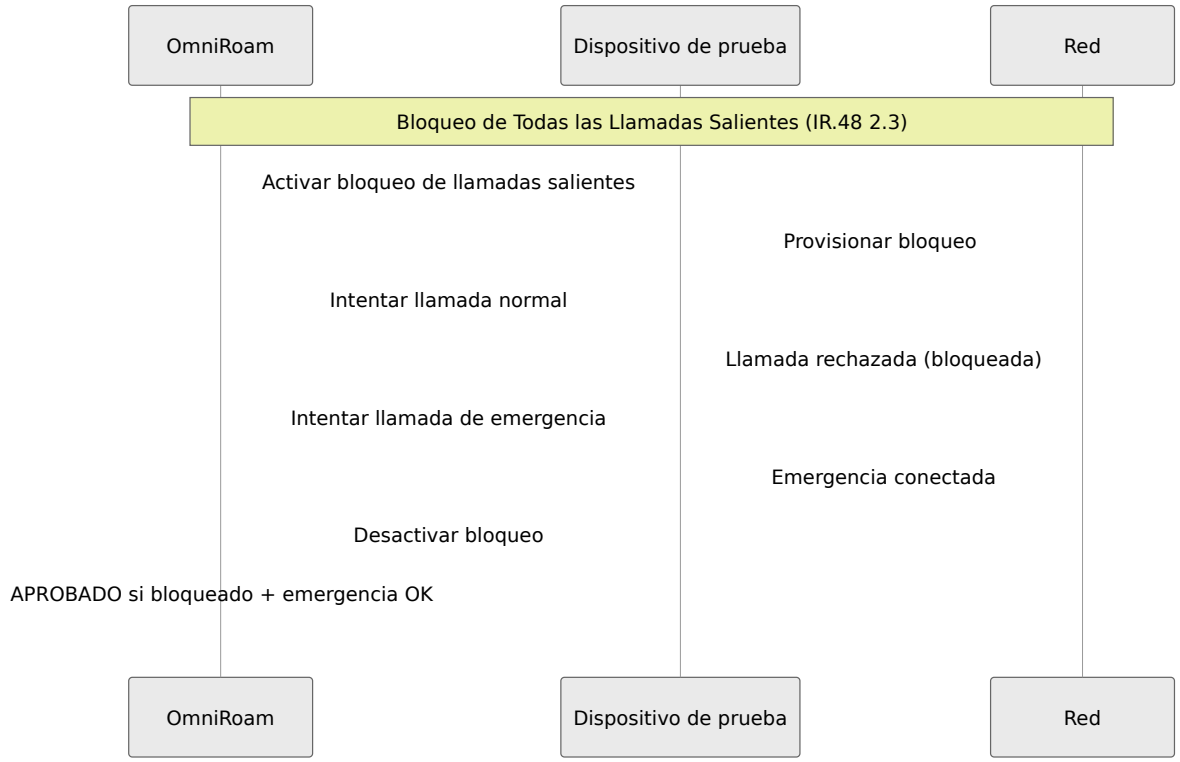
OmniRoam realiza una llamada desde el dispositivo a un servicio de respuesta de laboratorio, confirma que la llamada alcanza el estado activo (respondido), opcionalmente la mantiene para confirmar estabilidad, y luego la finaliza. El veredicto registra el tiempo de conexión y si la llamada se mantuvo.

SMS

OmniRoam envía un mensaje con un cuerpo único a un servicio de respuesta de laboratorio y espera la respuesta. La entrega de la respuesta confirma SMS de origen móvil y SMS de terminación móvil de extremo a extremo. Una respuesta faltante es un claro fallo con la razón, no un colapso.

Servicios suplementarios (bloqueo y reenvío de llamadas)

OmniRoam provisiona servicios suplementarios por aire desde el propio dispositivo de prueba, exactamente como lo haría un suscriptor con los códigos de control de servicio estándar, y luego los ejercita:



Para **Reenvío de Llamadas en Caso de No Respuesta**, OmniRoam registra el reenvío a un número objetivo con un temporizador de timbre, luego interroga el servicio y confirma que la red almacenó el número de reenvío y el temporizador que fueron registrados.

Cancelar Ubicación (IR.38 3.1.2)

Algunos casos se controlan desde el lado de la red en lugar del dispositivo. Para **Cancelar Ubicación LTE**, OmniRoam pide al servidor de suscriptores de origen que cancele la ubicación del suscriptor en la red visitada, y registra un pase cuando se acepta la solicitud. Esto confirma que la red de origen puede retirar un registro de roaming.

Registro IMS (VoLTE)

Para VoLTE, OmniRoam primero confirma que el dispositivo está registrado en IMS. Esto condiciona los casos dependientes de IMS: si no se confirma el registro, los casos de llamada VoLTE y SMS sobre IMS se informan como bloqueados.

Personalizando una Ejecución

Una ejecución no tiene que cubrir todo el libro. Usando el **selector de pruebas**, el operador selecciona exactamente qué casos ejecutar. Esto es útil para:

- Revalidar solo los casos que fallaron anteriormente.
- Ejecutar solo los casos de voz, o solo los casos de datos, durante la resolución de fallos.
- Omitir casos que dependen de un acuerdo que aún no está en su lugar (por ejemplo, un acuerdo CAMEL).

Los casos omitidos del alcance mantienen su veredicto existente y no se tocan.

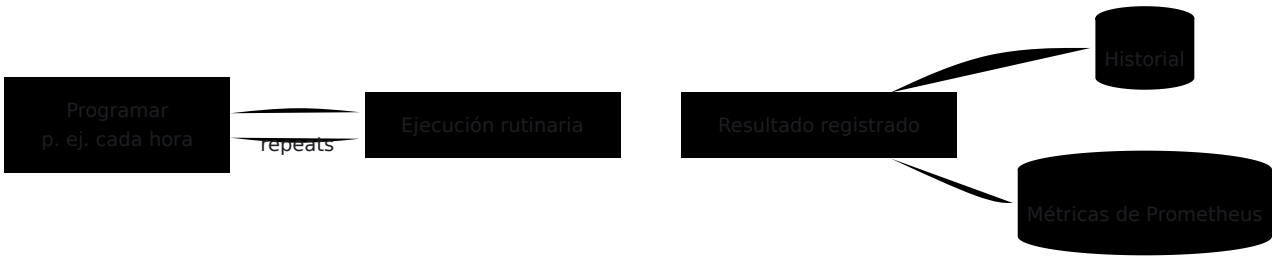
Volviendo a Ejecutar un Solo Caso

Cada caso tiene un control de re-ejecución. Seleccionarlo ejecuta solo ese caso nuevamente, contra el mismo dispositivo y SIM, y actualiza solo el veredicto de ese caso. Esta es la forma más rápida de confirmar una solución (por ejemplo, volver a ejecutar el caso de rendimiento después de un cambio de transporte) sin repetir todo el libro.

Ejecuciones Rutinarias y Programadas

OmniRoam puede ejecutar pruebas **no atendidas en un horario** para que una relación de roaming se valide continuamente en lugar de ser verificada una vez.

- **Verificaciones rutinarias** ejecutan un conjunto compacto de verificaciones de salud contra un dispositivo (datos, velocidad, voz y SMS) e informan un pase/reprueba combinado. Estos son los mismos impulsos utilizados por los libros completos, empaquetados como una verificación de confianza rápida y recurrente.
- **Horarios** ejecutan una rutina elegida en un intervalo recurrente automáticamente. Cada ejecución programada registra su propio resultado, construyendo un historial a lo largo del tiempo para que una regresión (por ejemplo, rendimiento cayendo por debajo del umbral, o fallo en la entrega de SMS) sea detectada y visible sin que nadie ejecute una prueba manualmente.



Configurando un Horario

Los horarios se gestionan en la pantalla de **Horarios** bajo Pruebas de Roaming. Un horario define:

Configuración	Propósito
Nombre	Identifica el horario (y etiqueta sus métricas e historial).
Módem(s)	El/los dispositivo(s) de prueba contra los que se ejecuta la rutina.
Verificaciones	Qué verificaciones realiza la rutina: datos, prueba de velocidad, voz, SMS.
Intervalo	Con qué frecuencia se ejecuta la rutina (por ejemplo, cada hora).

Una vez guardado, el horario se ejecuta automáticamente en su intervalo sin más interacción. La pantalla de **Prueba Rutinaria** muestra el historial de ejecuciones: la aprobación/reprueba combinada de cada ejecución, las velocidades medidas y el detalle por verificación. Una ejecución fallida presenta la misma evidencia que una ejecución interactiva.

Monitoreo de Prometheus

Los resultados de rutina programados se exportan como **métricas de Prometheus**, para que la salud del roaming pueda ser alertada y visualizada junto con el resto de la red, de la misma manera que se monitorean las pruebas programadas en dispositivos de prueba. La exposición se sirve en `/api/ir38/routine/metrics` (lee la última ejecución programada por horario y módem):

Métrica	Tipo	Signific
`omniweb_ir38_routine_pass`	gauge	Último resul de rutina programada pase, 0 = fa
`omniweb_ir38_routine_check_pass`	gauge	Resultado p verificación última ejecu (etiqueta `ch` datos/prueb velocidad/v
`omniweb_ir38_routine_download_mbps`	gauge	Tasa de des medida en l última ejecu
`omniweb_ir38_routine_upload_mbps`	gauge	Tasa de sub medida en l última ejecu
`omniweb_ir38_routine_latency_ms`	gauge	Latencia me en la última ejecución
`omniweb_ir38_routine_last_run_timestamp_seconds`	gauge	Tiempo Unix última ejecu programada

Cada serie lleva etiquetas `schedule`, `serial`, `modem` y `imsi` (más `check` en la métrica por verificación), por lo que puedes alertar por horario, por dispositivo o por suscriptor de origen. El punto final no necesita inicio de sesión (los scrapers no pueden llevar uno) y puede estar protegido con un token de portadora cuando sea necesario.

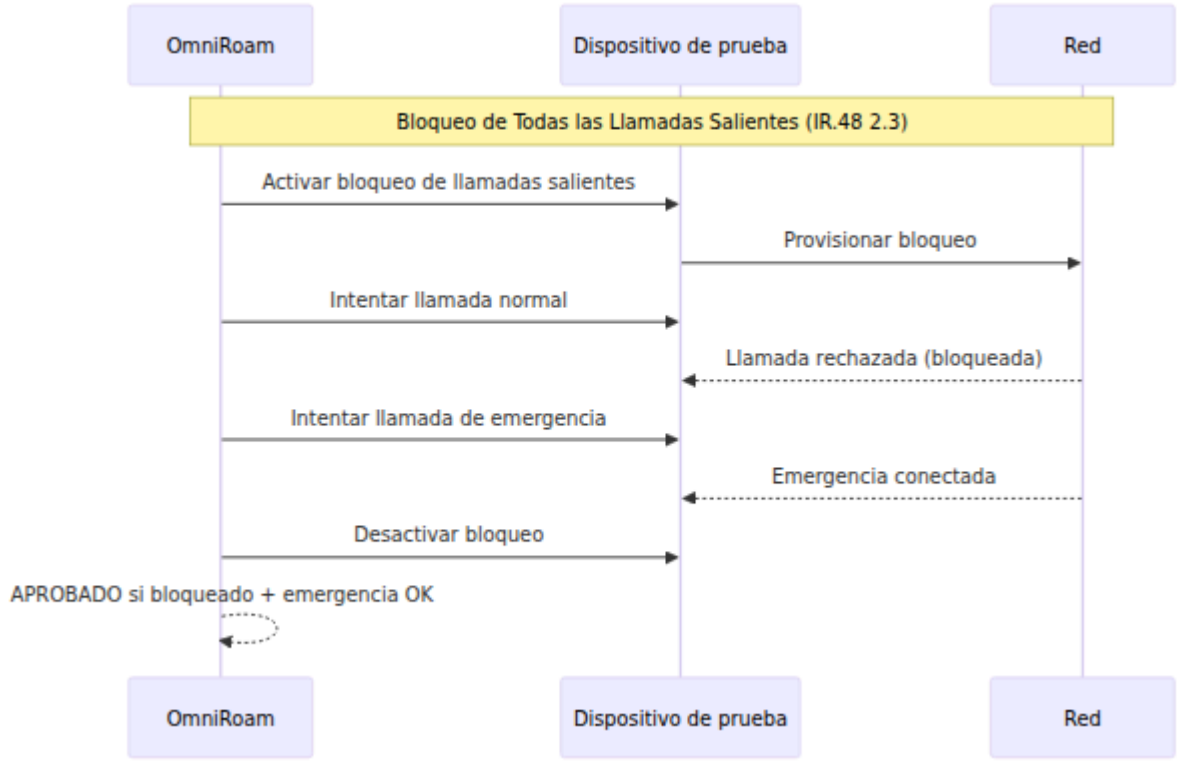
Ejemplo de alerta: la voz de roaming ha estado fallando en un dispositivo durante 15 minutos:

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

Los resultados programados se acumulan en un historial que se puede revisar en cualquier momento, y una ejecución fallida presenta la misma evidencia que una ejecución interactiva.

Leyendo los Resultados

Cada caso muestra su veredicto (**APROBADO**, **REPROBADO** o **NO REALIZADO**) junto con la evidencia detrás de él:



- **APROBADO**: se confirmó el resultado esperado de GSMA, con las cifras de apoyo.
- **REPROBADO**: no se cumplió el resultado esperado; se registra la razón (por ejemplo, "rendimiento por debajo del umbral", "sin respuesta de eco", o la causa de liberación de la red para una llamada que no se conectó).

- **NO REALIZADO**: el caso no se ejecutó, o es un caso manual que espera a un probador.

Cuando los resultados parecen correctos, genera el documento completado. Consulta Documentos de Libros de Pruebas Completados.

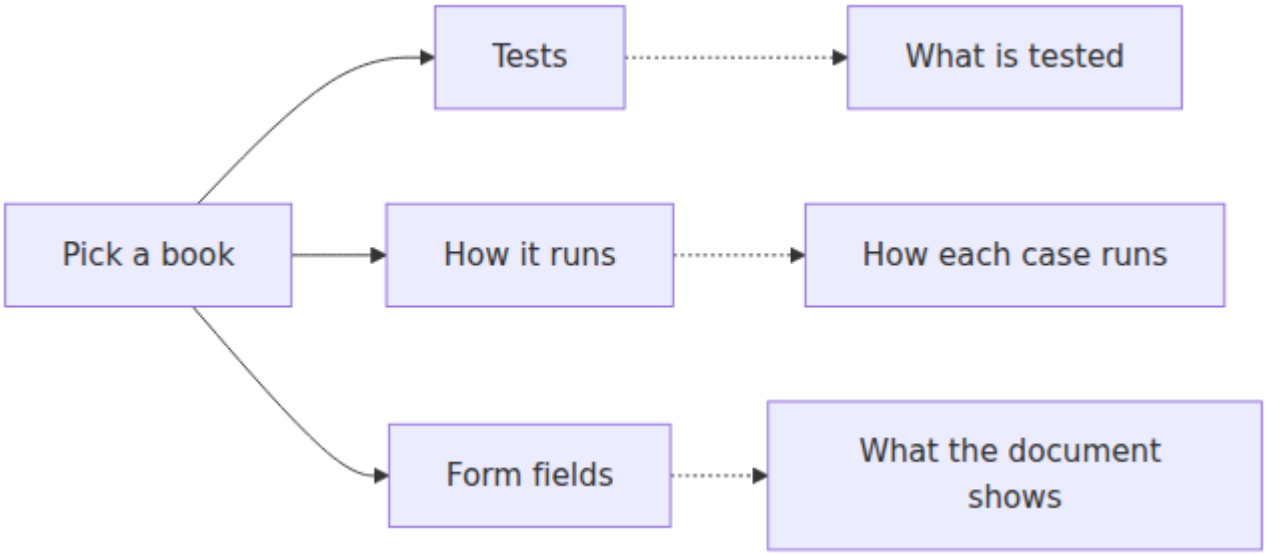
Explorador de Libros de Prueba

El Explorador de Libros de Prueba es una vista de referencia de solo lectura que muestra, para cada libro de prueba, exactamente qué prueba y cómo. Responde a tres preguntas que un operador típicamente hace antes de confiar en una ejecución automatizada:

1. **¿Qué casos hay en este libro y cuáles son automatizados?**
2. **¿Cómo se realiza cada caso en realidad?**
3. **¿Qué termina en el documento completado y de dónde proviene?**

El Explorador se accede desde la pantalla de Libros de Prueba en Movimiento a través de **Explorar libros**, y te permite alternar entre IR.38, IR.48 y VoLTE.

El Explorador mostrando el libro IR.48. Cada caso está listado con si es automatizado o manual y una descripción de cómo se ejecuta.



Pruebas

La vista de **Pruebas** lista cada caso en el libro con:

- el **número de caso** y **título** (que coincide con la especificación de GSMA),
- si el caso es **automatizado** o **manual**, y
- una descripción simple de **cómo se ejecuta**: por ejemplo "sesión de datos + verificación de registro de carga", "llamada de voz", "activación de barrera e intento de llamada", o "el probador registra el resultado" para casos manuales.

Esta es la forma más rápida de ver, de un vistazo, cuánto de un libro dado OmniRoam realiza por ti y qué queda como verificación manual.

Cómo Se Ejecuta

La vista de **Cómo se ejecuta** muestra la **secuencia de pasos** que una ejecución completa del libro realizará, en orden: preparando el dispositivo, las sesiones de datos, la verificación de rendimiento, las pruebas de voz y SMS, las pruebas de servicios suplementarios, y así sucesivamente. Refleja los casos actualmente en alcance, por lo que es una vista previa precisa de lo que hará una ejecución antes de que la inicies.

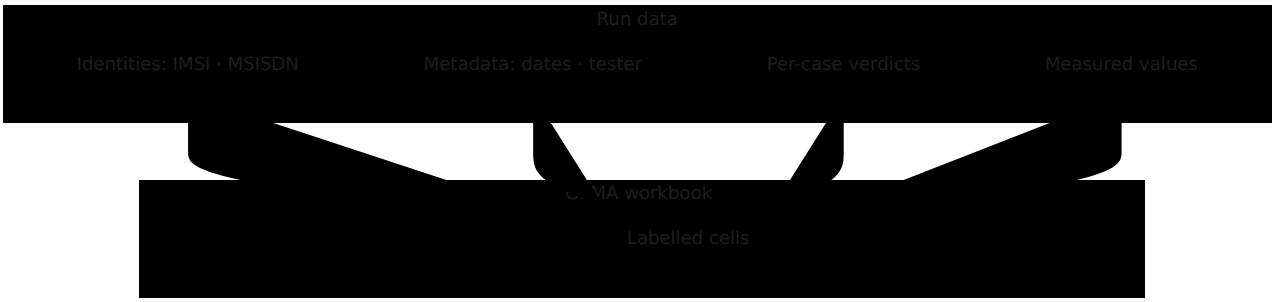
Esta vista es útil para entender la forma de una ejecución y para confirmar que un alcance personalizado realizará los pasos que esperas.

Campos del Formulario

La vista de **Campos del Formulario** lista cada celda en el libro de trabajo GSMA completado que OmniRoam llena, cada una anotada con:

- la **hoja y celda** en la plantilla GSMA,
- la **etiqueta de campo GSMA** (leída de la plantilla misma), y
- la **fuente** del valor: por ejemplo el MSISDN del suscriptor, la fecha de prueba, un veredicto de aprobado/reprobado por caso, o un valor medido como volumen de datos.

Debido a que esta lista se deriva de la misma lógica que produce el documento, no puede desviarse del paso con la exportación real: lo que dice el Explorador que se llenará es exactamente lo que se llena. Consulta Documentos de Libros de Prueba Completados para el documento en sí.



Descargar Plantilla

El Explorador también ofrece una acción de **Descargar Plantilla**, que descarga el libro de trabajo GSMA en blanco para el libro seleccionado: la plantilla oficial con el contenido de ejemplo/espacio reservado del proveedor eliminado, lista para completar a mano si es necesario. Este es el contraparte vacío del documento completado que produce una ejecución (ver Documentos de Libros de Prueba Completados).

Por Qué Es Importante

Un socio de roaming que acepta un libro de prueba completado necesita confianza en que los resultados son reales y que el documento representa fielmente lo que se probó. El Explorador hace que el mapeo sea transparente: cada caso automatizado puede ser rastreado desde el número de caso GSMA, a través de la forma en que se ejecuta, hasta la celda exacta en la que termina en el documento final.

Libros de Prueba de OmniRoam

OmniRoam envía tres libros de prueba de roaming GSMA. Cada libro es el conjunto de pruebas oficial de GSMA, con casos identificados por sus números de caso GSMA, por lo que el documento completado se mapea uno a uno con la especificación publicada.

- IR.38: Prueba de Datos de Roaming LTE
- IR.48: Roaming Bilateral (Voz / SMS / MMS / Datos)
- VoLTE: Pruebas de Roaming VoLTE

Para saber cómo se ejecuta y evalúa cada caso automatizado, consulte Ejecutar Pruebas. Para explorar los casos de un libro de manera interactiva, use el Explorador de Libros de Prueba.

En las tablas a continuación, **Automatizado** indica si OmniRoam realiza el caso automáticamente (**Auto**) o lo deja para que el probador lo registre (**Manual**).

IR.38: Prueba de Datos de Roaming LTE

Basado en **GSMA IR.38 v3.0**. Demuestra que un suscriptor de roaming puede conectarse para datos en la red LTE visitada, acceder a servicios a través de la red de origen y recibir un rendimiento aceptable. También demuestra la caída de voz y SMS por conmutación de circuitos, y datos 2G/3G, donde estos están en el alcance.

Caso	Título	Automatizado	Lo que prueba
`3.1.1`	Prueba de velocidad LTE (datos + rendimiento)	Auto	Se establece una sesión de datos a través de la puerta de enlace de origen, transporta tráfico y cumple con el umbral de rendimiento.
`3.1.2`	Cancelar Ubicación LTE	Auto	La red de origen puede cancelar la ubicación del suscriptor en la red visitada (activado desde el servidor de suscriptores de origen).
`3.1.3`	Prohibición Determinada por el Operador LTE	Manual	La prohibición determinada por el operador aplicada en el registro del suscriptor de origen es respetada.
`3.2.2`	CS Fallback: Llamada de Voz de Origen Móvil	Auto	Una llamada de voz originada por el suscriptor tiene éxito a través de la caída de CS.
`3.2.3`	CS Fallback: Llamada de Voz Terminada Móvil	Manual	Una llamada al suscriptor tiene éxito a través de la caída de CS.
`3.2.4`	SMS sobre SGs	Auto	SMS originados y terminados desde móviles funcionan a través de la interfaz SGs.
`3.3.1`	Acceso a Datos desde 2G/3G	Auto	Una sesión de datos 2G/3G accede a servicios a través

Caso	Título	Automatizado	Lo que prueba
	usando PGW en HPLMN		de la puerta de enlace de origen.
`3.4`	Acceso a Datos desde 4G + 5G NSA sobre S8	Auto	Los datos por paquete están disponibles y alcanzan Internet (confirmado por una sesión de datos con verificación de conectividad).

Cancelar Ubicación (3.1.2)

OmniRoam automatiza la Cancelación de Ubicación pidiendo al servidor de suscriptores de origen que cancele la ubicación del suscriptor en la red visitada, luego confirma que la solicitud fue aceptada. Esta es la eliminación iniciada por la red de origen del registro de roaming (de acuerdo con el procedimiento de cancelación de ubicación en 3GPP TS 29.272).

El KPI de Rendimiento

El caso `3.1.1` hace más que confirmar una sesión de datos. Mide la tasa de descarga alcanzada y la compara con el umbral de rendimiento de IR.38. El umbral depende de la distancia geográfica entre las redes de origen y visitada (caminos más largos permiten tasas más bajas):

Protocolo	Distancia < 4000 km	Distancia ≥ 4000 km
HTTP	≥ 11 Mbit/s	≥ 5 Mbit/s
FTP	≥ 13.5 Mbit/s	≥ 6 Mbit/s

OmniRoam estima la distancia a partir de las identidades de las redes de origen y visitada y selecciona automáticamente el umbral correcto; el operador puede anular la distancia o el protocolo cuando los valores predeterminados no

coinciden con la configuración de la prueba. Registrar una velocidad sin probarla contra el umbral nunca se considera un pase.

IR.48: Roaming Bilateral (Voz / SMS / MMS / Datos)

Basado en **GSMA IR.48 v2.1** (internamente el conjunto de pruebas IR.24). El clásico libro de roaming bilateral 2G/3G: llamadas básicas, servicios suplementarios, SMS y datos por paquete, ejercidos para un suscriptor que ha hecho roaming en la red visitada.

Caso	Título	Automatizado	Lo que prueba
`2.1`	MS1(a) llama a MS2(a), ambos en roaming en VPLMN(b)	Auto	Se establece y mantiene una llamada de voz básica.
`2.2`	Prueba negativa CAMEL (MOC, prepago, sin acuerdo)	Manual	Una llamada de prepago es correctamente prohibida donde no hay un acuerdo CAMEL activo.
`2.3`	Prohibición de Todas las Llamadas Salientes (BAOC)	Auto	Con la prohibición de llamadas salientes activa, las llamadas normales fallan mientras que las llamadas de emergencia aún tienen éxito.
`2.4`	Desvío de Llamada en Caso de No Respuesta (CFNRY)	Auto	El desvío de llamada en caso de no respuesta puede ser registrado e interrogado, con la configuración almacenada confirmada.
`2.5`	SMS de Origen / Terminados Móvil	Auto	Un SMS enviado desde el suscriptor en roaming es entregado y se recibe una respuesta.
`2.6`	Prueba negativa CAMEL (SMS-MO, prepago)	Manual	Comportamiento de SMS de prepago donde no hay un acuerdo CAMEL activo.
`2.7`	Acceso a Intranet / ISP usando puerta	Auto	Una sesión de datos alcanza Internet/intranet a través de la puerta de enlace de origen.

Caso	Título	Automatizado	Lo que prueba
	de enlace de origen		
`2.8`	MMS usando puerta de enlace de origen y MMSC	Manual	Un mensaje multimedia es entregado a través del MMSC de origen.

Servicios Suplementarios en IR.48

Dos casos de servicios suplementarios están completamente automatizados:

- **BAOC (2.3): Prohibición de Todas las Llamadas Salientes.** OmniRoam activa la prohibición de llamadas salientes en el suscriptor de prueba, confirma que una llamada saliente normal es rechazada por la red, confirma que una llamada de emergencia aún se conecta (la excepción requerida), luego elimina la prohibición para dejar la SIM limpia.
- **CFNRY (2.4): Desvío de Llamada en Caso de No Respuesta.** OmniRoam registra el desvío de llamada en caso de no respuesta a un número objetivo con un temporizador de timbre, luego interroga el servicio (el equivalente a marcar el código de estado `*#61#`) y confirma que la red almacenó el número y el temporizador de desvío que fueron registrados. Observar el desvío en vivo requiere una llamada entrante de un tercero, por lo que ese último paso se deja para una verificación manual; la provisión y la interrogación son automatizadas.

OmniRoam informa el estado de cada servicio suplementario utilizando las cuatro banderas estándar de 3GPP: **Provisionado**, **Registrado**, **Activo** y **En reposo** (ver 3GPP TS 23.011).

VoLTE: Pruebas de Roaming VoLTE

Basado en **GSMA BA.65 §5.3**, con comportamiento de VoLTE según **GSMA IR.92**. Demuestra que el suscriptor puede registrarse en IMS mientras hace roaming y realizar/recibir llamadas VoLTE y SMS sobre IMS.

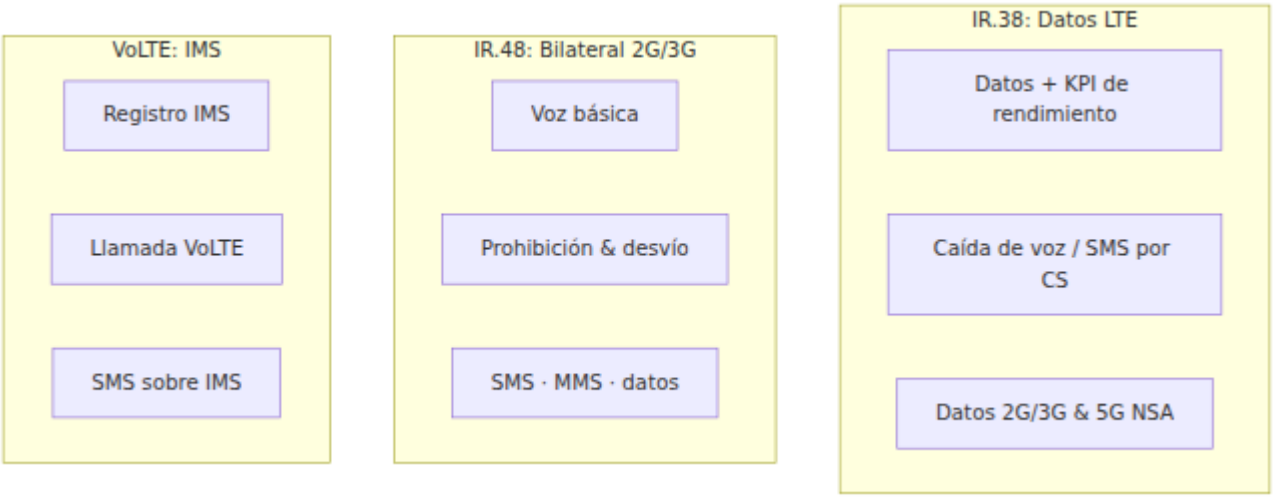
Caso	Título	Automatizado	Lo que prueba
`ims_reg`	Registro IMS sobre roaming	Auto	El dispositivo se registra en IMS mientras hace roaming (el requisito previo para todos los servicios VoLTE).
`mo_call`	Llamada VoLTE de origen móvil	Auto	Se establece y mantiene una llamada VoLTE originada por el suscriptor.
`mt_call`	Llamada VoLTE de terminación móvil	Manual	Una llamada al suscriptor a través de VoLTE se establece.
`sms_ims`	SMS sobre IMS (SMSoIP)	Auto	El SMS se entrega a través de la red IMS.
`emergency`	Llamada de emergencia VoLTE	Manual	La llamada de emergencia funciona a través de VoLTE (nunca se marca automáticamente).

La Puerta de Registro IMS

Los servicios VoLTE dependen del registro IMS. OmniRoam ejecuta `ims_reg` primero como una **puerta**: si el dispositivo no está registrado en IMS, los casos dependientes de IMS (`mo_call`, `sms_ims`) se informan como bloqueados en

lugar de fallidos. No tiene sentido marcar una llamada VoLTE cuando IMS está inactivo, y un resultado bloqueado le dice al operador exactamente por qué.

Comparación de los Libros



Libro	Dominio principal	Mejor para
IR.38	Datos LTE / EPC	Validar una nueva relación de datos de roaming LTE y rendimiento
IR.48	Circuito 2G/3G + paquete	Validar voz, servicios suplementarios, SMS y datos básicos
VoLTE	IMS	Validar el roaming VoLTE una vez que la interconexión IMS esté en su lugar

Gestión de SIM OTA: RFM/RAM por aire

El módulo **OTA** gestiona SIMs **por aire**: lee y edita archivos en una tarjeta remota. Envía **paquetes seguros** (ETSI TS 102 225 / 3GPP TS 31.115, "03.48" / SCP80) que transportan comandos de Gestión de Archivos Remotos (RFM) y Gestión de Aplicaciones Remotas (RAM). La tarjeta verifica y descifra cada paquete, ejecuta los comandos y devuelve una **Prueba de Recepción (POR)** firmada.

En la práctica, te ofrece la misma edición a nivel de archivo que el Explorador de Sistema de Archivos SIM: navega por el árbol de archivos, decodifica un EF, edita los campos y lo escribe de nuevo. La diferencia es que OTA llega a la tarjeta **remotamente**: a través de un lector PC/SC en el host central, un lector en un agente, o a través de **SMPP** a una SIM en el campo.

Se basa en el mismo almacén de claves por ICCID que el Almacén de Claves SIM. Un perfil indica *qué conjunto de claves y algoritmos*, y el almacén de claves contiene el **KIC/KID** real para esa tarjeta. El motor nunca registra ni devuelve las claves. Solo devuelve el texto cifrado resultante y el POR.

Qué es un paquete seguro

Un paquete seguro protege los comandos APDUs de extremo a extremo, independientemente del (portador) (plano). El motor ha sido validado contra tarjetas ISIM físicas.

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

CPL cuenta cada octeto después de sí mismo; **CHL** cuenta desde SPI hasta e incluir el RC/CC/DS. Cuando el cifrado está activado, todo desde CNTR hasta el final es cifrado y rellenado con ceros hasta el tamaño del bloque de cifrado, con **PCNTR** registrando cuántos octetos se añadieron.

- **TAR** (Referencia de Aplicación de Toolkit, 3 bytes) dirige el paquete a un servicio en la tarjeta: una aplicación RFM específica o el RAM (gestor de tarjeta).

- **SPI** indica el cifrado, la verificación de integridad, la política de contadores y lo que debe contener el PoR.
- **KIc / KID** indexan qué transporte (cifrado) y conjunto de claves de autenticación utiliza la tarjeta; los **valores** provienen del almacén de claves por ICCID.

Configuraciones de seguridad en su totalidad

Cada interruptor a continuación se puede configurar en un perfil, y cada combinación está implementada. Un proveedor de tarjetas cita estos como cuatro octetos hexadecimales — MSL, PoR, KIc, KID — y un perfil los acepta de esa manera: pega `15213505` en el campo **SPI** y cada interruptor se configura a partir de él. El campo también funciona al revés, mostrando los cuatro octetos actualizándose a medida que cambias un interruptor, de modo que una configuración se puede leer de nuevo contra una hoja de personalización.

Octeto SPI	Configuración	Opciones
MSL	Integridad	ninguno, verificación de redundancia (RC), suma de verificación criptográfica (CC)
MSL	Cifrado	activado / desactivado
MSL	Contador	sin contador; presente pero no verificado; debe ser mayor; debe ser mayor en uno
PoR	Requisito	nunca; siempre; solo en caso de error
PoR	Integridad de respuesta	ninguno, RC, CC
PoR	Cifrado	activado / desactivado
PoR	Portador	SMS-DELIVER-REPORT o SMS-SUBMIT
KIc	Algoritmo de cifrado	DES-CBC, triple DES-CBC 2-clave, triple DES-CBC 3-clave, DES-ECB, AES-CBC
KIc	Versión de clave	1–3
KID	Algoritmo de suma de verificación	DES-CBC, triple DES-CBC 2-clave, triple DES-CBC 3-clave, AES-CMAC
KID	Algoritmo de redundancia	CRC 16, CRC 32
KID	Versión de clave	1–3

El octeto KID significa cosas diferentes a cada lado del MSL: cuando la opción de integridad es un **CC** nombra un algoritmo de suma de verificación, y cuando es un **RC** los mismos bits nombran un CRC. El editor de perfil intercambia las opciones para que coincidan, y la longitud de RC sigue — dos octetos para CRC 16, cuatro para CRC 32.

Las versiones de clave se detienen en 3 porque un registro de tarjeta contiene tres conjuntos de claves; el SPI en sí permite 1–15.

Parámetros por conjunto de claves

Una tarjeta se personaliza con un algoritmo **por conjunto de claves** — el conjunto de claves 1 podría ser triple DES con un CRC mientras que el conjunto de claves 3 es AES con un CMAC. Eso pertenece a las claves, no al perfil que las selecciona, por lo que cada conjunto de claves en el almacén de claves SIM lleva su propio SPI.

Cuando un conjunto de claves registra uno, sus **algoritmos y versiones de clave** se utilizan en lugar de los del perfil, porque un paquete construido con cualquier otra cosa es rechazado por la tarjeta. Todo lo que es genuinamente elección del operador — el TAR, la política de PoR, la política de contadores, si cifrar o no, el formato del comando — sigue viniendo del perfil. La vista previa informa qué configuraciones vinieron de dónde, de modo que un perfil que no coincide con una tarjeta se muestra antes de que se envíe algo en lugar de como una entrega fallida después.

Un conjunto de claves sin SPI registrado no cambia nada: el perfil se mantiene como está.

Una **Prueba de Recepción** se decodifica contra las mismas configuraciones, incluyendo la verificación de su RC o CC. El octeto de estado se informa en las propias palabras de la especificación — *PoR OK*, *RC/CC/DS falló*, *CNTR bajo*, *CNTR alto*, *CNTR bloqueado*, *error de cifrado*, *error de seguridad no identificado*, *memoria insuficiente*, *más tiempo necesario*, *TAR desconocido*, *nivel de seguridad insuficiente*.

Formato de comando remoto

Los scripts de comando se configuran por defecto en el formato **compacto**: los C-APDUs uno tras otro. Un perfil puede seleccionar el formato **expandido** en su lugar (ETSI TS 102 226), que envuelve cada C-APDU en un `22` TLV dentro de una plantilla de scripting de comando `AA`, con codificación de longitud indefinida (`AE`) como opción. La tarjeta responde con una plantilla `AB` o `AF` que contiene un `23` R-APDU por comando, por lo que un script fallido puede ser rastreado hasta el comando que falló en lugar de solo la última palabra de estado. Algunos TARs no aceptan nada más.

Los APDUs dentro son un script C-APDU ordinario: `SELECT` + `READ BINARY` para una lectura RFM, `SELECT` + `UPDATE BINARY` para una escritura, `DELETE` / `INSTALL` de GlobalPlatform para RAM.

En la red (un SMS-PP) el paquete viaja en el TP-User-Data con un Identificador de Paquete de Comando UDH (IEI `0x70`), PID `0x7F` (descarga de datos SIM), DCS `0xF6` (8-bit, clase de mensaje 2). En el shell se entrega como un APDU de CAT `ENVELOPE(SMS-PP-Download)` y la PoR regresa de manera sincrónica.

Un paquete demasiado largo para un solo mensaje corto se divide automáticamente, ya sea con el encabezado de concatenación de 8 bits o — a través de SMPP — con los parámetros `sar_*` para que el SMSC lo reensamble.

Perfiles, contextos y enrutamiento automático

Un **perfil OTA** es un ajuste de seguridad reutilizable. No contiene **material de clave**:

Campo	Significado
`tar`	Referencia de Aplicación de Toolkit de 3 bytes (el servicio objetivo).
`kic_index` / `kid_index`	Qué conjunto de claves (1/2/3) → `KIC{n}`/`KID{n}` de la fila del almacén de claves de la tarjeta.
`cipher_algo` / `cc_algo`	Algoritmo de cifrado y suma de verificación (`triple_des_cbc2`, `aes_cbc`, …).
`ciphering`, `rc_cc_ds`, `counter_mode`	SPI: ¿cifrar? ¿CC vs RC vs ninguno? política de contador de repetición.
`por`, `por_ciphered`, `por_rc_cc_ds`	¿PoR requerido? ¿cifrado? ¿firmado?

Se han sembrado dos perfiles, coincidiendo con los valores validados en sysmoISIM:

- **RFM-USIM-3DES-keyset3**: TAR `B00011`, conjunto de claves 3, 3DES, cifrado + CC, PoR requerido + cifrado + CC. Opera dentro de **ADF.USIM**.
- **RFM-SIM-3DES-keyset2**: TAR `B00010`, conjunto de claves 2. Opera en el árbol 2G **MF-rooted** (DF.GSM / DF.TELECOM).

Diferentes aplicaciones necesitan diferentes servicios, por lo que el explorador **enruta el perfil y el contexto SELECT automáticamente por archivo**, desde la aplicación del archivo:

Aplicación de archivo	Contexto	Perfil (por TAR)	Pre-SELECT antes del ENVELOPE
`ADF.USIM`	`usim`	TAR `B00011`	`SELECT ADF.USIM` (por AID)
`DF.GSM`, `DF.TELECOM`	`sim`	TAR `B00010`	ninguno (MF-rooted)
`ADF.ISIM`	`isim`	TAR `B00013`	`SELECT ADF.ISIM` (por AID)

Cada contexto se asigna a uno de tus perfiles (predeterminado por coincidencia de TAR, sobreescribible en el explorador). Elige una tarjeta y haz clic en cualquier archivo (USIM, GSM o TELECOM). OmniWeb aplica el perfil, conjunto de claves y SELECT correctos sin necesidad de cambiar nada. ISIM funciona tan pronto como creas un perfil para él (su TAR varía según la tarjeta).

Transportes

Un transporte entrega el paquete seguro y, donde el portador lo permite, recoge el POR. Los adaptadores enchufables comparten una interfaz:

Tipo	Alcance	POR	Notas
`local_pcsc`	una tarjeta en un lector PC/SC **en el host central**	sincrónico	la ruta de validación directamente conectada.
`agent_reader`	una tarjeta en un lector **en un agente remoto**	sincrónico	viaja por el mismo WebSocket de agente que Dispositivos de Prueba / Banco SIM (`session_apdu` relay).
`smpp`	una **SIM de campo** a través de SMPP `submit_sm`	asincrónico	SMS MT a un SMSC; el PoR regresa más tarde como un SMS MO, o en la misma conexión cuando se vincula como un transceptor. Ver **Parámetros SMPP** a continuación.
`http_admin`	una **SIM de campo** a través de **HTTP (SCP81)**	asincrónico	un SMS de activación hace que la tarjeta marque el Servidor de Administración Remota a través de TLS-PSK; scripts + respuestas fluyen allí. Ver **HTTP OTA** a continuación.

El **Explorador** utiliza solo los transportes en-shell (necesita un PoR sincrónico); **Campañas** pueden usar cualquiera, incluyendo SMPP.

Parámetros SMPP

Un mensaje corto OTA difiere de uno ordinario en un puñado de parámetros, y un SMSC aceptará un mensaje que los tenga incorrectos y silenciosamente nunca lo entregará a la tarjeta. Todos ellos son configurables:

Parámetro	Predeterminado	Por qué es importante
`esm_class`	`0x40`	Marca los datos del usuario como comenzando con un encabezado. Sin él, la tarjeta nunca ve el Identificador de Paquete de Comando.
`protocol_id`	`0x7F`	Descarga de datos (U)SIM.
`data_coding`	`0xF6`	8-bit, clase de mensaje 2 — lo que dirige el mensaje a la SIM en lugar de a la bandeja de entrada.
`dest_addr_subunit`	`0x02`	La subunidad de destino es la SIM. El parámetro que más a menudo falta cuando un paquete es aceptado y nunca llega.
`user_message_reference`	no establecido	Transportado al PoR MO por la mayoría de los SMSCs, que es

Parámetro	Predeterminado	Por qué es importante
		cómo se empareja un PoR asincrónico con su trabajo.
`registered_delivery`, `validity_period`, `priority_flag`, `service_type`, `schedule_delivery_time`, `replace_if_present_flag`, `sm_default_msg_id`	Predeterminados del SMSC	Controles de submit_sm ordinarios.

Los paquetes largos se segmentan de tres maneras: el encabezado de concatenación de 8 bits en los datos de usuario (el predeterminado), los parámetros `sar_msg_ref_num` / `sar_total_segments` / `sar_segment_seqnum` para que el SMSC los reensamble, o un único `message_payload` donde el SMSC lo soporte. Cualquier otro parámetro opcional puede ser añadido por nombre.

Antes de enviar, un transporte informará sobre configuraciones que son válidas pero que no alcanzarán una SIM — una bandera de encabezado faltante, una codificación de datos que aterriza en la bandeja de entrada, una subunidad de destino que no es la SIM.

Descubriendo los parámetros de una tarjeta

No se puede preguntar a una tarjeta qué TAR y configuraciones de seguridad se utilizó para personalizarla. Cuando llega un lote con claves pero sin documentación, **Perfiles → Descubrir parámetros** los encuentra mediante sondeo: intenta cada uno de los conjuntos de claves de la tarjeta contra el espacio de parámetros plausible y reporta lo que la tarjeta acepta. Un resultado puede convertirse directamente en un perfil con **Usar**.

Esto necesita un transporte en-shell — un portador de almacenamiento y reenvío no puede responder cada sondeo.

Dos cosas hacen que un barrido ingenuo sea inútil, y la ejecución de descubrimiento maneja ambas:

- **Un contador que es demasiado bajo es rechazado en silencio.** Donde el nivel de seguridad dice *el contador debe ser mayor*, una tarjeta dada un contador en o por debajo de su valor almacenado no devuelve nada en absoluto — sin error, sin Prueba de Recepción. Eso es indistinguible de claves incorrectas o un TAR incorrecto. Por lo tanto, el descubrimiento comienza el contador alto; dado que un contador solo aumenta, comenzar alto no cuesta nada.
- **El byte de PoR decide de dónde regresa la respuesta.** Con el bit 6 claro, la tarjeta responde en la respuesta ENVELOPE; con él establecido, la tarjeta eleva un proactivo ENVIAR MENSAJE CORTO en su lugar y la respuesta ENVELOPE está vacía. Observa solo un camino y una respuesta correcta es invisible, por lo que ambos son buscados.

Un estado de **CNTR bajo** se trata como un éxito en lugar de un fracaso: significa que las claves, el TAR, los algoritmos y el nivel de seguridad fueron todos aceptados, y solo el contador estaba mal. El descubrimiento se detiene allí y resuelve el contador duplicándolo, lo que toma un puñado de viajes de ida y vuelta en lugar de continuar el barrido.

Si nada es aceptado, eso realmente no te dice qué parámetro estaba mal — el silencio es la respuesta de la tarjeta a cada tipo de error.

> Cada sondeo aceptado avanza el contador de la tarjeta, y un contador nunca vuelve hacia abajo.

Entregando a través de EF_SMS

Un paquete también se puede escribir directamente en un registro de `EF_SMS` (`3F00/7F10/6F3C`) en una tarjeta en un lector, con el registro marcado como no leído. La tarjeta lo procesa exactamente como si hubiera llegado por aire — sin SMSC y sin radio. Esta es la forma práctica de ejercitar un script contra una tarjeta en un escritorio o en un banco.

Explorador

`src/pages/ota/OtaExplorer.tsx`: el editor de archivos SIM remoto.

1. Elige un **ICCID objetivo** (del Almacén de Claves SIM) y un **transporte**.
2. Navega por el **catálogo de archivos**: cada EF conocido del modelo de archivo offline (ADF.USIM, ADF.ISIM, DF.GSM, DF.TELECOM), agrupados por aplicación y buscables por código / nombre / descripción.
3. Selecciona un archivo → **Leer por OTA**. La lectura RFM segura se entrega, el POR se decodifica y el EF se renderiza: estado de POR, último SW, hex crudo + ASCII, y un **formulario de campo tipado** (decodificado a campos nombrados).
4. Edita los **campos** (re-codificados automáticamente) o el **hex crudo**, luego **Escribir por OTA**. El `UPDATE` RFM seguro se envía y el archivo se **lee de nuevo** automáticamente para que veas el estado en la tarjeta después de la escritura.

Las lecturas/escrituras están controladas por el permiso de control `ota`; todo se registra como un **trabajo**.

Campañas

`src/pages/ota/OtaCampaigns.tsx`: una operación guardada distribuida a un conjunto de SIMs: **consulta objetivo → operación → perfil → transporte**.

- **Consulta objetivo** se evalúa contra el inventario del Banco SIM en tiempo de ejecución: lista de ICCID / prefijo, prefijo o rango IMSI, agente, banco. Una consulta vacía coincide deliberadamente con nada (sin distribución accidental).
- **Operación** es el comando RFM/RAM (leer/actualizar binario o registro, GP eliminar / obtener estado / instalar).
- **Ejecutar** crea un **trabajo** por cada tarjeta coincidente. Las campañas SMPP son de disparo y olvido (el POR llega más tarde como un SMS MO).

Una ejecución está limitada (`CAMPAIGN_MAX_TARGETS`) para que una consulta con errores no pueda disparar miles de tarjetas en una sola solicitud.

Trabajos

`src/pages/ota/OtaJobs.tsx`: cada entrega OTA (lecturas/escrituras del explorador y ejecuciones de campañas) con su estado y POR. El panel de detalles muestra el **paquete de solicitud seguro** (texto cifrado), la **Prueba de Recepción**, y el resultado decodificado (comandos ejecutados, último SW,

datos de respuesta). Los secretos de la tarjeta **nunca** se almacenan en un trabajo: solo el texto cifrado y el POR.

API REST (`/api/ota`, JWT, tipo de

elemento RBAC `ota`)

Método	Ruta	Propósito
GET	`/profiles` · POST · `/profiles/<id>` PUT/DELETE	Perfiles de seguridad OTA.
GET	`/campaigns` · POST · `/campaigns/<id>` GET/PUT/DELETE	Campañas.
GET	`/campaigns/<id>/targets`	Vista previa de qué SIMs coincide actualmente la consulta.
POST	`/campaigns/<id>/run`	Ejecutar: un trabajo por tarjeta coincidente.
GET	`/jobs`, `/jobs/<id>`	Historial de trabajos (filtrar por `campaign_id` / `iccid`).
GET	`/files/catalog`	El catálogo de EF navegable (modelo de archivo offline).
POST	`/explore/read`	Leer un EF por OTA; devuelve el trabajo + EF decodificado.
POST	`/execute`	Ejecutar una operación (actualización RFM, RAM, crudo) contra una tarjeta.
POST	`/preview`	Construir el paquete seguro **sin** enviar — devuelve el texto cifrado, los enmarcados SMS, el desglose del SPI, el contador utilizado y el siguiente.

Método	Ruta	Propósito
POST	`/spi`	Decodificar cuatro octetos SPI en las configuraciones nombradas, o construir los octetos a partir de configuraciones. Aritmética pura; no se involucra ninguna tarjeta o material de clave.
POST	`/discover`	Sondear una tarjeta para el TAR y SPI que acepta, dado solo sus claves. Necesita un transporte en-shell; avanza el contador de la tarjeta.
POST	`/decode` · `/encode`	Decodificar bytes EF ↔ campos tipados (offline).

RBAC refleja `simbank`/`ir38`: los administradores siempre pasan; de lo contrario, un permiso JWT con `element_type == "ota"` otorga vista, y `POST` en sus métodos otorga control. Las lecturas se tratan como control (transmiten un paquete a la tarjeta). Las rutas se documentan automáticamente en la Referencia API.

Esquema de base de datos

Tabla	Fila	Columnas clave
`ota_profiles`	un ajuste de seguridad	`name`, `tar`, `kic_index`/`kid_index`, algoritmos, banderas SPI.
`ota_campaigns`	un fan-out guardado	`name`, `profile_id`, `target_query` (JSON), `operation` (JSON), `transport` (JSON), `status`.
`ota_jobs`	una entrega a una tarjeta	`iccid`, `operation`, `request_hex` (texto cifrado), `response_hex` (POR), `por_status`, `result` (JSON), `status`.

Las claves viven en la tabla existente `simbank_keys` (el Almacén de Claves SIM), referenciadas por ICCID por el índice de conjunto de claves del perfil. **No** se duplican aquí.

Cómo funciona

El motor OTA maneja la criptografía, la estructura del paquete seguro, los TLVs de CAT/SMS y el modelo de archivo offline necesario para construir y decodificar paquetes RFM/RAM 03.48/SCP80. Funciona en el servicio de backend de rol de agente y comparte la conexión del agente para el transporte en-shell. La entrega es enchufable a través de los transportes de lector local, lector de agente remoto y SMPP.

Notas de seguridad

- Los secretos de la tarjeta (KIC/KID) se leen del almacén de claves para construir paquetes pero **nunca** se escriben en el registro de auditoría ni se

devuelven en ninguna respuesta. Solo el texto cifrado de la solicitud y el POR se almacenan.
- Escribir un archivo es destructivo; el explorador confirma antes de cada escritura y lee de nuevo el resultado.
- El paquete seguro es genuino 03.48: manipula un byte y la tarjeta lo rechaza (el CC falla); con el cifrado activado, los APDUs en texto plano nunca aparecen en la red.

HTTP OTA (SCP81 / RAM-a-través-de-HTTP)

Junto con SCP80 sobre SMS/lector, OmniWeb habla **SCP81** — OTA basado en HTTP según **GlobalPlatform Card Spec v2.3 Amendment B**. En lugar de un SMS seguro, la tarjeta abre una **sesión de administración HTTP sobre TLS-PSK** y ejecuta un script completo.

```
 SMS de activación (SCP80) ─► tarjeta ─BIP ABRIR CANAL─► TLS-PSK
─► Servidor de Administración Remota
                         RAS sirve scripts de comando, recopila
respuestas, termina con 204
```

- **Activador** — una operación `http_admin` envía un SMS seguro que lleva el *activador de sesión de administración* de la Enmienda B (host/URI de RAS, `psk_id`, política de reintento) a través del mismo portador SMPP, luego encola una **sesión de administración**.
- **TLS-PSK** — una clave precompartida **derivada del KIC/KID** del conjunto de claves OTA de la tarjeta; sin certificados. Perfil TLS según **GlobalPlatform Amendment B §3.3.2** (la especificación ETSI TS 102 226 se remite a): TLS 1.2 con `TLS_PSK_WITH_AES_128_CBC_SHA256` / `TLS_PSK_WITH_NULL_SHA256`, retrocediendo a los conjuntos RFC 4279 para tarjetas TLS 1.0/1.1. Los conjuntos `NULL` (solo integridad) son válidos aquí — el script ya está asegurado por SCP80 por debajo.
- **Bucle de administración** — la tarjeta POSTea al RAS, que sirve el script de comando encolado y recopila cada respuesta hasta que la sesión se

completa.

- La vista de **Sesiones de Administración** (`/ota/admin-sessions`) muestra cada sesión en vivo: estado, progreso del script y la escalera de comando→respuesta. El **trabajo** vinculado lleva el resultado final, exactamente como los otros transportes.

La criptografía (derivación de PSK, activador seguro) permanece en el sidecar OTA; el **RAS** de cara al público (`omniweb-ota-scp81`, un servicio Elixir/OTP) no tiene claves — termina TLS-PSK y extrae scripts del backend a través de localhost. Funciona para RFM/RAM UICC clásico y eUICC (SGP.02). Ver `docs/ota-specs/HTTP_OTA_PLAN.md`.

PGW-C: Puerta de Acceso de PDN (Plano de Control)

El **PGW-C** es la mitad del plano de control de la **Puerta de Acceso de PDN** del EPC. Es el punto de anclaje para cada sesión de datos de suscriptor: termina **S5/S8** hacia el SGW-C, establece y mantiene cada **conexión de PDN**, asigna al UE su dirección IP de un **grupo de IP** del operador, y selecciona y controla el plano de usuario (**UPF**) a través de **Sx/PFCP**. También ejecuta la política y el cobro de la sesión a través de Diameter: **Gx** hacia el PCF/PCRF para política y QoS, y **Gy** hacia el OCS para cobro en línea. También genera **CDRs** para cobro fuera de línea. En el núcleo 5G, la función equivalente es el **SMF**. OmniWeb presenta las sesiones activas del PGW-C, grupos de IP, UPF y pares de Diameter, un mapa de topología e historial de sesiones, y herramientas de diagnóstico. Los paneles de Grafana accesibles desde la misma página contienen las tendencias a largo plazo.

← Guía de Operaciones

El PGW-C es una página de elemento por instancia que se alcanza desde la barra lateral cuando se navega en el inventario del sitio, con una vista de flota donde se despliegan varios. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del PGW-C, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda contextual) abre esta página. Está organizada en pestañas.

Descripción General

Una lectura de salud de pantalla única: el **estado de la API** del PGW-C y un resumen de su estado en vivo (número de sesiones activas, utilización del grupo de IP, pares de UPF y pares de Diameter). Es la forma más rápida de confirmar que el nodo está activo y manejando sesiones.

Sesiones

Cada sesión PGW activa, cada fila identificada por el **IMSI** y **MSISDN** del suscriptor con su **IP de UE** y **APN** asignados. Las sesiones se pueden buscar por IMSI, IP de UE, MSISDN o APN. Abrir una sesión muestra su estado completo: la conexión de PDN y portadoras, el SGW que sirve y el UPF seleccionado, y el contexto de política y cobro Gx/Gy en vivo. Puedes editar una sesión aquí. Un operador puede ajustar el estado en vivo, como el **AMBR** de la sesión (que envía un nuevo APN-AMBR al UPF) y los **disparadores de eventos Gx** solicitados que controlan el reporte de cambio de ubicación. Un operador también puede **eliminar** una sesión para liberar forzosamente a un suscriptor atascado o que se comporta mal. Dado que el operador aplica ediciones directamente al estado en vivo, tienen efecto inmediato.

Donde se despliegan varios PGW-Cs, la misma pestaña en la **vista de flota** lista cada sesión a través de todos ellos en una tabla, con el PGW-C que sirve mostrado contra cada fila. La búsqueda se pasa a cada instancia, por lo que un operador puede encontrar un suscriptor sin saber qué PGW-C lo está anclando; abrir una fila va a esa sesión en su propia instancia. Una instancia que no se puede alcanzar se nombra sobre la tabla, por lo que una lista corta nunca se confunde con una red silenciosa.

Grupos de IP

Los grupos de IP del operador de los que el PGW-C asigna direcciones a los UE, cada uno mostrando su **tamaño**, conteo **asignado** y **utilización**. Abrir un grupo lista las direcciones individuales asignadas. Aquí confirmas que un grupo no está agotado (un grupo agotado es una causa común de fallos en la configuración de sesiones) y ves qué suscriptor tiene una dirección dada.

Pares de UPF

Los pares del plano de usuario (UPF) que el PGW-C controla a través de **Sx/PFCP**, cada uno mostrando su **dirección IP** y **estado de asociación** PFCP. Abrir un par muestra sus detalles. Aquí confirmas que las asociaciones PFCP que llevan el plano de usuario de cada sesión están activas.

Diameter

Los pares de Diameter con los que el PGW-C se comunica (el **PCF/PCRF** a través de **Gx** para política y el **OCS** a través de **Gy** para cobro en línea), cada uno con su **nombre de host** y **estado de conexión**. Abrir un par muestra sus detalles. Cuando las sesiones son rechazadas o limitadas, aquí confirmas que las rutas de política y cobro están activas.

Historial

Un registro paginado y buscable de **eventos** del ciclo de vida de la sesión: *creada*, *modificada*, *eliminada*, *transferencia* y *fallida*. Puedes filtrar eventos por tipo y buscarlos por IMSI, MSISDN, dirección IP o TEID. Aquí reconstruyes lo que le sucedió a la sesión de un suscriptor específico a lo largo del tiempo, incluidos los fallos.

Topología

Un mapa del PGW-C y los vecinos con los que trabaja: los SGWs para los que ancla sesiones, los UPFs que controla y sus pares de Diameter. Proporciona una vista de una imagen de qué vecinos de señalización y plano de usuario están conectados al nodo.

Selección de UPF

Las reglas que deciden en qué UPF se coloca una nueva sesión, junto con el **estado de salud** actual de cada UPF candidato y la configuración de **PCO** (Opciones de Configuración de Protocolo) que el PGW-C devuelve al UE. Aquí confirmas por qué las sesiones están aterrizando en un UPF particular y verificas que todos los candidatos están saludables.

Búsqueda de UE

Una búsqueda directa de un solo suscriptor por **IMSI**, **MSISDN** o **dirección IP**, devolviendo la información de ese UE en el PGW-C. Es la forma más rápida de encontrar la sesión de un suscriptor sin desplazarse por toda la lista de Sesiones.

Cobro

El estado de **cobro en línea (Gy/OCS)** en vivo de cada sesión activa, cada fila identificada por **IMSI** y **MSISDN** y buscable por cualquiera de los dos. A simple vista, cada sesión muestra si el cobro en línea **Gy** está activado (con su **id de sesión**, y el **host de OCS** y **dominio** con el que se comunica), si la contabilidad **fuera de línea (Gz)** también está activa, y si el OCS ha empujado al suscriptor a una redirección de **jardín amurallado**. Abrir una sesión expande su detalle completo de cobro: las cuotas **concedidas** por URR contra el volumen **utilizado** (octetos de subida, bajada y totales), la **acción de unidad final** que el OCS estableció para cuando se agote el crédito, los contadores fuera de línea (Gz), y cualquier objetivo de redirección. Así es como lees el estado de control de crédito en vivo de un suscriptor: si tiene crédito, cuánto de su concesión ha consumido, y por qué puede haber sido limitado o redirigido.

Romper el cristal: suspender el cobro en línea. En la parte superior de la pestaña hay un interruptor a nivel de nodo que suspende el cobro en línea en todo el PGW-C. Úsalo cuando el OCS no pueda responder y los suscriptores de otro modo perderían el servicio.

Mientras el interruptor esté armado, el PGW-C no envía CCR-I al adjuntar y no envía CCR-U en sesiones en vivo. Libera jardines amurallados y desactiva portadoras restringidas, por lo que el tráfico se transporta sin la autorización del OCS. El cobro fuera de línea no se ve afectado: el uso todavía se escribe en CDRs y puede ser facturado más tarde.

Para armar el interruptor, dale dos cosas:

Campo	Requerido	Descripción
Suspender por	Sí	Cuánto tiempo permanece armado el interruptor. Se desarma solo cuando se agota el tiempo. El nodo establece el valor más largo que acepta.
Razón	Sí	Por qué se suspende el cobro. Se registra contra la anulación.
Armado por	No	Quién lo armó. Por defecto, es tu dirección.
Enviar un CCR-T de Gy al desanexar	No	Desactivado por defecto. Actívalo para informar el uso que el OCS nunca autorizó.

Da una razón real. La razón y el operador se registran, y sobreviven al turno que armó el interruptor.

El panel muestra el tiempo restante mientras el interruptor está armado. Presiona **Reanudar cobro** para desarmarlo de inmediato. El interruptor también se desarma solo cuando se agota su tiempo, lo que evita que una anulación olvidada se convierta en un servicio gratuito permanente.

CDRs

Los **registros de cobro** fuera de línea que el PGW-C escribe para facturación: una fila por evento de **inicio**, **intermedio** y **detención** de sesión, el más reciente primero, y filtrable por **IMSI** o **MSISDN**. Cada registro lleva el **IMSI**, **MSISDN** y **IMEI** del suscriptor, el **APN** y **QCI**, el **id de cobro** que une los registros de una sesión, los **octetos de subida/bajada** contados para ese intervalo, las direcciones IP de **S-GW**, **PGW** y **UE**, y el **archivo fuente** del que se leyó el registro. Aquí concilias el uso de datos de un suscriptor contra la contabilidad fuera de línea (Gz) que el operador factura, y rastreas en qué archivo de registro aterrizó una sesión dada.

Prueba de Gy

Una herramienta para operadores que emite una **Solicitud de Control de Crédito Gy** contra el OCS para validar el camino de cobro en línea de extremo a extremo. Proporcionas un **IMSI** (y opcionalmente un MSISDN y un conteo de octetos solicitados/utilizados) y eliges el tipo de solicitud. Usa **Inicial (CCR-I)** para abrir una sesión y solicitar unidades, **Actualizar (CCR-U)** para informar el uso y pedir más, o **Terminar (CCR-T)** para informar el uso final y cerrarla. Luego envíala. El PGW-C establece por defecto el grupo de tarifas, el Id de Contexto de Servicio y el Id de Aplicación de Autenticación. La **Respuesta de Control de Crédito** analizada regresa en la misma pantalla. A diferencia de las otras pestañas, esta **no recupera nada al cargar**: es un formulario que envías. Cuando el cobro en línea se comporta mal, es la forma más rápida de probar que el OCS es accesible y está otorgando crédito.

Monitor de P-CSCF

El estado y las métricas del monitor de descubrimiento de P-CSCF. El PGW-C devuelve una dirección de P-CSCF a dispositivos VoLTE durante la configuración de PDN, y esta pestaña confirma que el descubrimiento está saludable para que el registro IMS pueda proceder.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo del PGW-C para solucionar problemas de un solo nodo (fallos en la configuración de sesiones, errores de PFCP y Diameter) sin salir de OmniWeb.

Monitoreo

Las tendencias del conteo de sesiones, el rendimiento y otras series temporales para el PGW-C se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionados

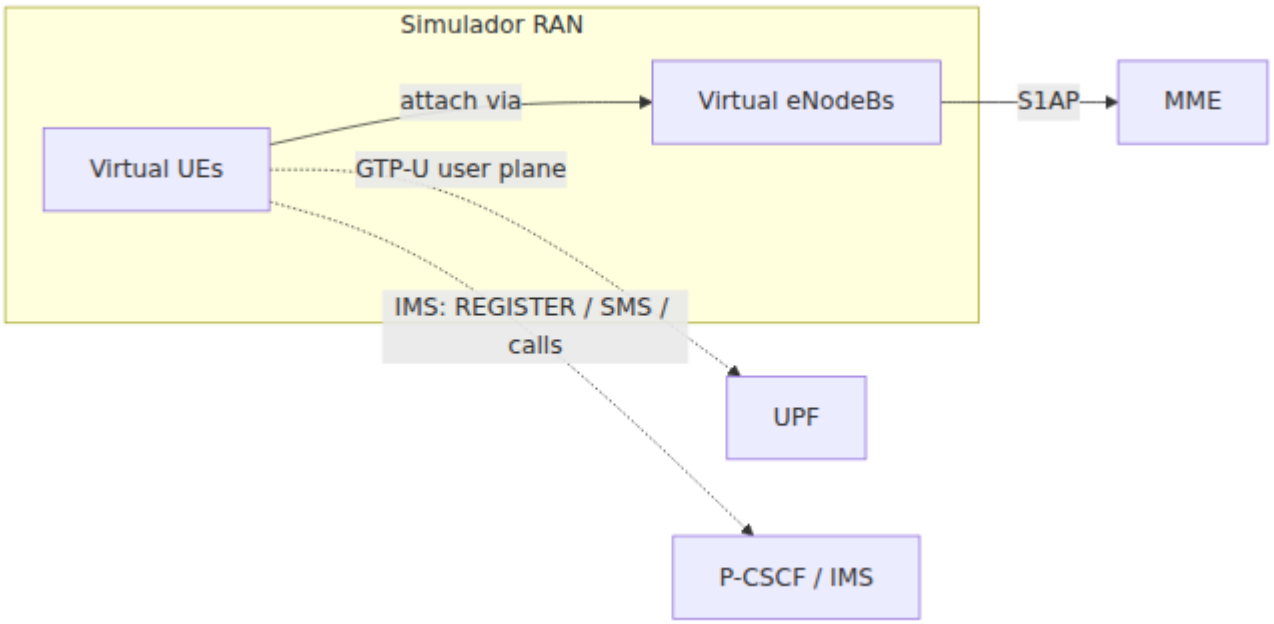
- El **SGW-C** es el par de control sobre **S5/S8**; ancla las portadoras del lado de acceso a las que el PGW-C se conecta a la PDN.
- El **UPF** es el plano de usuario que el PGW-C selecciona y controla a través de **Sx/PFCP**.
- El **PCF/PCRF** proporciona política y QoS a través de **Gx**.
- El **CHF/OCS** realiza el cobro en línea a través de **Gy**; el PGW-C también genera CDRs para el cobro fuera de línea.

Simulador RAN

El **Simulador RAN** te permite ejercitar una red central en vivo sin radios o dispositivos físicos. Establece **eNodeBs** y **UEs** virtuales que hablan S1AP/NAS reales al MME y GTP-U a las puertas de enlace, para que puedas realizar adjuntos, sesiones de datos, registros IMS, SMS y llamadas. Úsalo para pruebas funcionales, pruebas de carga o para reproducir escenarios de campo, todo desde OmniWeb.

← Guía de Operaciones

Qué Es



El simulador funciona junto a la red central que apunta. En OmniWeb aparece como su propia área de **Simulador RAN** (Mapa de Red, eNodeBs, UEs, IMS, Prueba de Carga, Programas de Escenarios). Debido a que un UE simulado se comporta como un dispositivo, sus UEs también aparecen en **Dispositivos de Prueba** para que puedas controlarlos desde el mismo lugar que los dispositivos reales.

Por defecto, comienza con **sin eNodeBs**. Configuras exactamente la topología que deseas.

eNodeBs

Activar un eNodeB lo conecta al MME (Configuración S1). Un eNB puede estar conectado a **más de un MME** (un grupo de MME). El Mapa de Red muestra el conjunto completo de MMEs a los que está asignado un eNB.

La activación es **fire-and-forget**: OmniWeb solicita al simulador que active el eNB y regresa; el enlace S1 se establece en segundo plano (observa el Mapa de Red / lista de eNodeBs para confirmar que se activó).

Desconectando un eNodeB

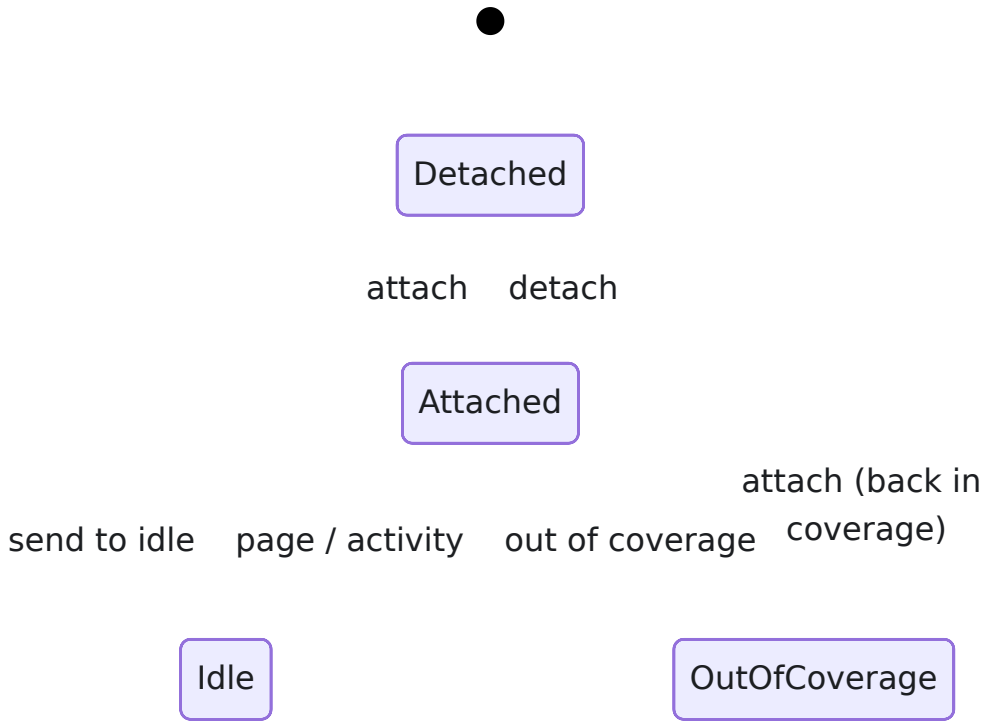
Puedes desactivar un eNB de dos maneras, que modelan diferentes eventos del mundo real:

Acción	Modelos	Efecto en UEs
Desconexión S1 limpia	Un apagado ordenado del eNB / reinicio S1	Los UEs se liberan limpiamente y **sobreviven**. Se vuelven a adjuntar cuando hay un enlace disponible
Caída de enlace	El eNB pierde abruptamente su S1 (corte de fibra, pérdida de energía)	La asociación S1 se aborta; los UEs **sobreviven** a la desaparición del eNB y se vuelven a adjuntar en lugar de ser desactivados

Críticamente, desactivar un eNB **no** destruye sus UEs. Los UEs persisten y se vuelven a adjuntar, por lo que puedes simular interrupciones de transporte sin reconstruir tu flota de suscriptores.

UEs

Cada UE simulado tiene un ciclo de vida que puedes controlar directamente:

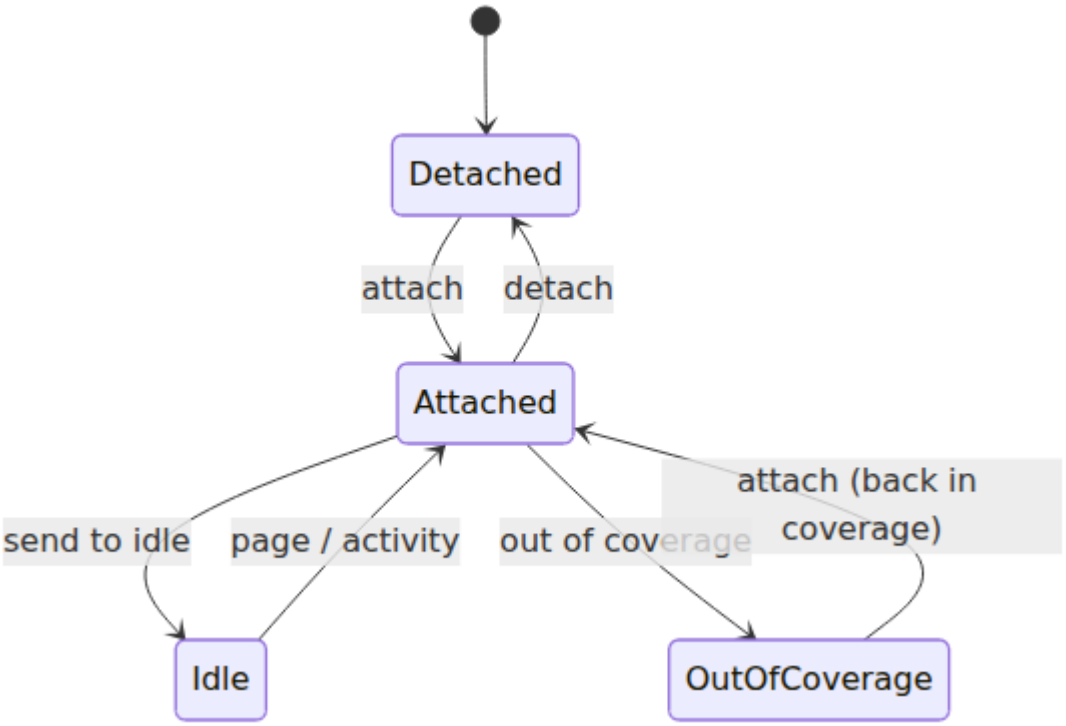


- **Adjuntar / Desadjuntar**: unirse o abandonar la red.
- **Enviar a inactivo**: moverse a ECM-IDLE (como lo hace un UE real entre actividades). La paginación o nueva actividad lo devuelve.
- **Fuera de cobertura**: una pérdida *no limpia* de radio (el UE se desconecta sin señalizar), para probar cómo maneja el núcleo un UE que simplemente desaparece. Adjuntarse lo devuelve a la cobertura.

Para cada UE, el simulador muestra el **MME que lo atiende**: el ID de grupo MME y el código MME (decodificado del GUTI del UE). Así que en un despliegue agrupado puedes ver qué MME recogió a cada suscriptor.

Registro IMS y ubicación

Un UE simulado puede registrarse en IMS y realizar SMS/llamadas. Cuando se registra, incluye su **ubicación celular** (`P-Access-Network-Info` con el `utran-cell-id-3gpp` para su celda de servicio), exactamente como lo hace un UE real. Así, el REGISTER de terceros del S-CSCF propaga esa ubicación al SMSc, TAS y otros servidores de aplicaciones. Esto te permite probar el comportamiento IMS dependiente de la ubicación de extremo a extremo sin radios reales.



Controlando UEs desde Dispositivos

Debido a que un UE simulado es solo otro dispositivo, aparece en **Dispositivos de Prueba** etiquetado como un simulador, y puede ser filtrado allí. Usas el **mismo panel de control de UE** ya sea que abras un UE desde el Mapa de Red del Simulador RAN o desde la flota de Dispositivos. Es un solo lugar para adjuntar/desadjuntar, inactivo, simular fuera de cobertura, registrarse en IMS, enviar un SMS o realizar una llamada, y ver el registro de acciones.

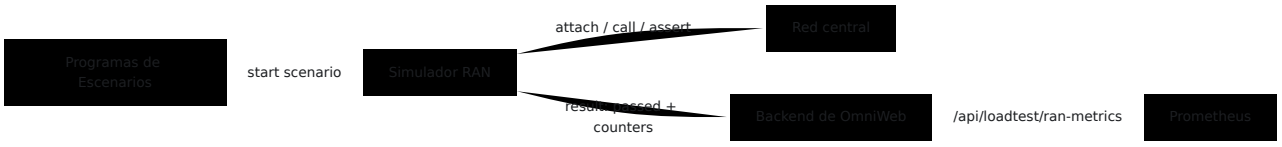
Filtra los Dispositivos de Prueba a los UEs del Simulador RAN para controlar suscriptores emulados junto a dispositivos reales.

Escenarios Programados

Un **escenario** es una receta de prueba guardada: una secuencia nombrada de acciones de UE (adjuntar, inactivo, despertar, registro IMS, llamada, SMS, transferencia, desadjuntar) que el simulador ejecuta contra el núcleo. El simulador incluye una biblioteca de preajustes, agrupados por categoría (por ejemplo, ciclo de vida de adjunto, VoLTE y casos de rechazo negativo). Ejecuta

un escenario una vez desde la vista de Prueba de Carga, o ejecútalo en un horario repetido para monitorear el núcleo continuamente.

La página de **Programas de Escenarios** (barra lateral: Prueba de Carga → Programas de Escenarios) gestiona las ejecuciones repetidas. Para cada programa eliges un escenario y con qué frecuencia ejecutarlo. OmniWeb registra el resultado de aprobado o fallido de cada ejecución y lo exporta a Prometheus, para que puedas alertar sobre ello y graficarlo.



Las ejecuciones son **serializadas**. OmniWeb ejecuta un escenario programado a la vez, porque un escenario puede iniciar muchos UEs y genera una carga real en el núcleo. Si una ejecución sigue activa cuando se debe la siguiente programación, OmniWeb espera y la inicia en el siguiente ciclo libre. Usa el botón **Ejecutar ahora** en un programa guardado para iniciarlo de inmediato.

Parámetros del programa

Campo	Tipo	Requerido	Predeterminado	Descripción
Nombre	Cadena	Sí	-	Etiqueta única para el programa. También la etiqueta `schedule` en la métrica exportada.
Escenario	Cadena	Sí	-	El escenario preestablecido a ejecutar. El selector agrupa escenarios por categoría.
Cada (s)	Entero	No	3600	Con qué frecuencia ejecutar el escenario, en segundos. Mínimo 60.
Conteo de UE	Entero	No	100	Número de suscriptores que ejecuta el escenario.
RPS	Número	No	10	Número objetivo de nuevos escenarios por segundo.

Campo	Tipo	Requerido	Predeterminado	Descripción
Concurrencia	Entero	No	50	Número máximo de escenarios en vuelo a la vez.
APNs	Lista	No	predeterminado del escenario	APNs a adjuntar, como una lista separada por comas. Anula e predeterminado del escenario.

Aprobación y fallo

Una ejecución programada **aprueba** cuando el simulador informa que todas las afirmaciones pasaron y ningún escenario de suscriptor fue abortado. Una ejecución **falla** si alguna afirmación falla o algún escenario es abortado. Un escenario sin afirmaciones aprueba siempre que ningún escenario sea abortado. Si OmniWeb no puede iniciar la ejecución, o la ejecución no termina a tiempo, OmniWeb registra la ejecución como un **error**.

La página muestra una tabla de **Ejecuciones Recientes** con el resultado, el conteo de afirmaciones, el número de escenarios abortados y la duración de cada ejecución.

Métricas

OmniWeb expone el último resultado de cada programa en formato Prometheus en `/api/loadtest/ran-metrics`. Prometheus lo extrae como el trabajo `ransim_scenarios`, que el rol de monitoreo configura automáticamente.

Métrica: `ransim_scenario_pass` **Tipo**: Gauge **Descripción**: Resultado de la ejecución programada más reciente: `1` para aprobado, `0` para no aprobado **Etiquetas**:

- `schedule`: el nombre del programa
- `scenario`: el id del escenario que se ejecutó
- `category`: la categoría del escenario
- `status`: el resultado de la ejecución (`passed`, `failed`, o `error`)

Los medidores complementarios comparten las mismas etiquetas:

Métrica	Descripción
`ransim_scenario_duration_ms`	Duración de la última ejecución, en milisegundos
`ransim_scenario_assertions_passed`	Afirmaciones aprobadas en la última ejecución
`ransim_scenario_assertions_failed`	Afirmaciones fallidas en la última ejecución
`ransim_scenario_scenarios_aborted`	Escenarios de suscriptores abortados en la última ejecución
`ransim_scenario_last_run_timestamp`	Tiempo Unix de la última ejecución

Consultas de ejemplo:

```
# Escenarios cuya última ejecución no aprobó
ransim_scenario_pass == 0

# Total de fallos de afirmaciones en todos los escenarios
programados
sum(ransim_scenario_assertions_failed)

# Un programa que no se ha ejecutado en las últimas dos horas
time() - ransim_scenario_last_run_timestamp > 7200
```

Dashboard de Grafana

El rol de monitoreo incluye un dashboard de **Escenarios del Simulador RAN** (carpeta de Grafana **RAN**). Lee las métricas anteriores y muestra una línea de tiempo de aprobado o fallido, el último resultado para cada programa, fallos de afirmaciones, frescura de escenarios y duración de ejecuciones. Filtra por categoría, escenario o programa en la parte superior. Ver Grafana.

Usos Típicos

- **Pruebas funcionales**: activa un eNB y un UE, adjunta, inicia una sesión de datos, regístrate en IMS, envía un SMS, luego confirma que cada elemento del núcleo se comporta.
- **Pruebas de carga**: activa muchos UEs para generar carga de adjunto/sesión/IMS contra el núcleo (ver la vista de Prueba de Carga).
- **Reproducción de escenarios**: modela interrupciones (caída de enlace, fuera de cobertura) y comportamiento de MME agrupados para reproducir y diagnosticar problemas de campo.
- **Monitoreo continuo**: programa un escenario para ejecutarse en un temporizador y alerta sobre la métrica de aprobado o fallido (ver Escenarios Programados).

Relacionados

- Dispositivos de Prueba: dispositivos reales y UEs simulados, controlados desde un solo lugar.
- Trazado de Sesiones: correlaciona la señalización que genera el simulador.

SIM Remota y SIM Virtual

OmniWeb puede presentar **cualquier SIM a cualquier módem a través de la red**. También puede presentar una SIM que **no existe físicamente**: OmniWeb la emula a partir de una imagen de tarjeta guardada más las claves del suscriptor almacenadas en el HSS. Esto convierte un rack de lectores de SIM, emuladores de tarjetas ("cardems") y módems en uno o más sitios en un pool compartido. Cualquier probador puede utilizar cualquier perfil de suscriptor contra cualquier módem sin necesidad de llevar una SIM de plástico a una ranura de tarjeta.

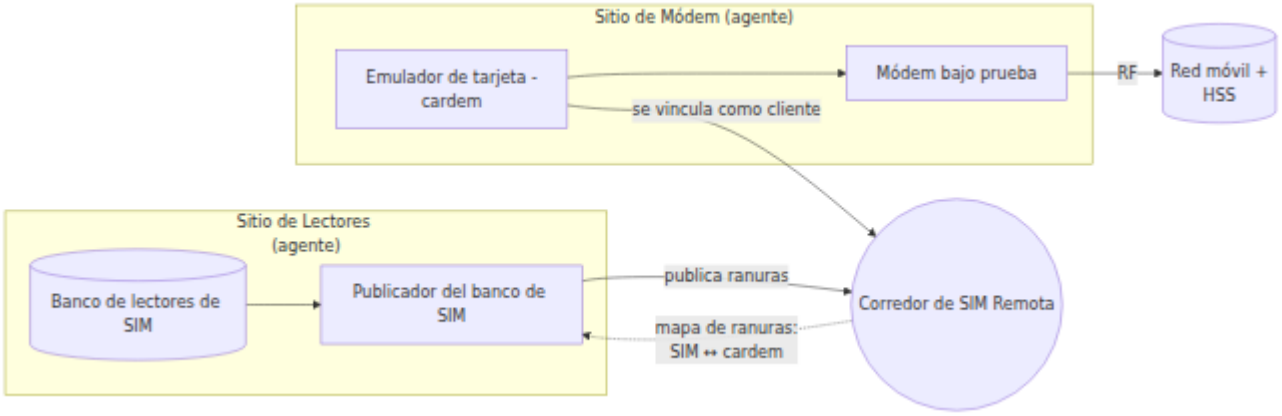
Esta página es la guía de operaciones para esa capacidad. La mitad de **inventario** descubre qué SIMs están en qué lectores. Banco de SIM cubre esa mitad. Esta página cubre cómo **presentar** una SIM (real o virtual) a un módem y usarla en una prueba. Imágenes de SIM (Paquetes de Perfil SAIP) cubre cómo guardar el sistema de archivos de una tarjeta como un paquete de perfil portátil y cómo usar uno para respaldar una SIM virtual.

Tabla de Contenidos

- Descripción General de la Arquitectura
- Conceptos
- El Banco de SIM: qué hay donde
- SIM Remota: conectar una SIM a un cardem
- La Consola Cardem
- SIM Virtual: un suscriptor sin tarjeta física
- Usando una SIM en un Libro de Pruebas de Roaming
- Solución de Problemas

Descripción General de la Arquitectura

Un banco de lectores de SIM, uno o más emuladores de tarjetas y los módems bajo prueba se conectan a OmniWeb a través de sus agentes de dispositivo. Un corredor central asigna una ranura de SIM elegida a un cardem elegido; el cardem luego presenta esa SIM al módem conectado a él.



Para una SIM **virtual**, una tarjeta de software reemplaza al banco de lectores. OmniWeb construye esta tarjeta de software a partir de una imagen de SIM guardada y las claves del suscriptor. Todo lo demás es idéntico:



Conceptos

Término	Significado
Banco de SIM	Un conjunto de lectores de tarjetas inteligentes en un agente, publicado para que sus SIMs puedan ser presentadas en otros lugares. Cada lector poblado es una **ranura**.
cardem	Una placa emuladora de tarjetas (USB) que finge ser una SIM hacia un módem conectado a ella. Reproduce cualquier tarjeta a la que esté asignada.
Mapa de ranuras	La vinculación "presentar **esta** ranura SIM a **ese** cardem". Crearla conecta los dos a través de la red; eliminarla los desconecta.
Módem bajo prueba	El módem detrás de un cardem. Se conecta a la red en vivo utilizando la SIM que el cardem está presentando.
SIM Virtual	Una tarjeta de software construida a partir de una imagen de SIM guardada más las claves de un suscriptor. OmniWeb la presenta a un cardem exactamente como una SIM real. No se requiere tarjeta física.

El Banco de SIM: qué hay donde

La página del **Banco de SIM** lista cada ranura de lector en cada agente conectado, agrupadas por agente. El diseño del banco es la verdad: ranuras vacías, ilegibles y en uso se muestran, no solo las pobladas.

*Cada fila es un lector físico. El chip de estado muestra si una tarjeta está presente y es legible. La fila luego muestra la identidad de la SIM (ICCID, IMSI, MCC/MNC, país, nombre del operador). Los lectores mantenidos por una sesión de emulación activa se muestran como **En uso**. Las SIMs persistidas cuyo lector está actualmente fuera de línea aparecen bajo **Vistos previamente**. Vuelven a aparecer cuando el agente se reconecta con la SIM insertada.*

Chip de estado	Significado
SIM	Una tarjeta está presente y su identidad fue leída.
Tarjeta presente	Una tarjeta está físicamente colocada pero su identidad no pudo ser leída (por ejemplo, una combinación de lector/tarjeta incompatible).
En uso	El lector está siendo utilizado por una sesión de SIM remota/emulación en este momento.
Vacío	No hay tarjeta en la ranura.

Las acciones por fila abren el explorador del **Sistema de Archivos de SIM** o el **Terminal APDU** para esa ranura exacta, y **Volver a escanear** vuelve a leer

los lectores de un agente a demanda.

SIM Remota: conectar una SIM a un cardem

La página de **SIM Remota** es donde vinculas una SIM a un cardem. Las vinculaciones funcionan **a través de agentes y sitios**: la SIM puede estar en un lector en una ubicación y el cardem/módem en otra.

Pasos

1. **Inicia el banco de SIM** en el agente que tiene los lectores (**Iniciar bankd**). Esto publica sus ranuras de lector.
2. **Inicia el cliente cardem** para el emulador de tarjeta que deseas usar (**Iniciar cliente**). Esto vincula el cardem para que una SIM pueda ser asignada a él.
3. Bajo **Conectar una SIM**, elige una ranura publicada y selecciona un cardem para vincularlo. La asignación se crea y se muestra bajo **Asignaciones activas** como **ACTIVA**.
4. El cardem ahora presenta esa SIM a su módem. Reinicia el módem (consulta la consola cardem) para que lea la SIM recién presentada y se conecte.

Reinicio Global desmantela todas las asignaciones y devuelve cada cardem a un estado inactivo. Úsalo para recuperarte de un banco de pruebas confundido.

Campo (Asignaciones activas)	Significado
Estado	`ACTIVA` una vez que el cardem está presentando la SIM.
SIM (banco/ranura)	En qué banco y ranura del agente vive la tarjeta.
ICCID	La SIM presentada.
Cardem (cliente/ranura)	Qué cardem (y qué agente) la está presentando.
Por	El operador que creó la asignación.

La Consola Cardem

En **Dispositivos**, OmniWeb muestra un emulador de tarjeta como su propio tipo de dispositivo (`ngff-cardem`), junto a módems y teléfonos. Nunca se abre como un teléfono. OmniWeb etiqueta los tipos de dispositivos desconocidos de manera simple en lugar de adivinar.

Abre el cardem para obtener una consola dedicada para el emulador y su módem.

Control	Qué hace
Iniciar cliente	Vincula el cardem como un cliente de SIM remota para que una SIM pueda ser asignada a él.
Reiniciar módem	Re-presenta la tarjeta emulada, lo que hace que el módem vuelva a leer la SIM y vuelva a ejecutar la conexión. Esta es la forma de "intercambiar la SIM" sin tocar el hardware.
SIM Remota	Conectar o desconectar qué SIM remota se presenta a este cardem.

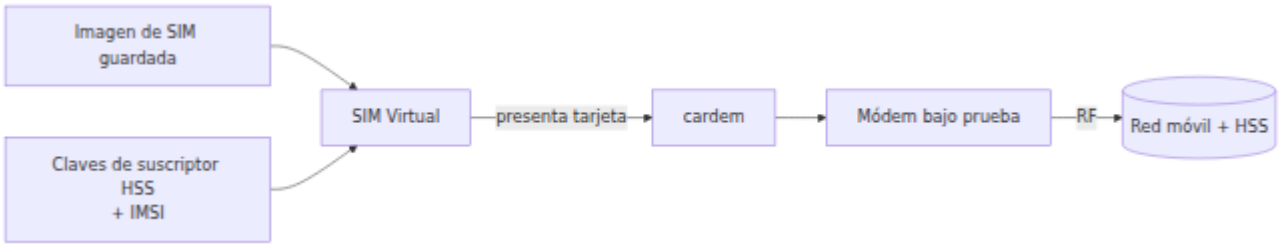
El panel de **Fuente de SIM** indica honestamente qué está y no está disponible: el cardem alimenta al módem una SIM *remota*. La consola aún no ofrece presentar una tarjeta *local* colocada en la placa del emulador. La consola lo dice en lugar de mostrar un control que no hace nada.

SIM Virtual: un suscriptor sin tarjeta física

Una **SIM virtual** permite que un módem se conecte como un suscriptor **para el cual no tienes una SIM**. OmniWeb la construye a partir de dos cosas que ya tienes:

1. Una **imagen base de SIM**: una instantánea guardada de la estructura de archivos de una tarjeta real (cualquier SIM de prueba compatible funciona como base; consulta **Imágenes de SIM**).
2. La **identidad y claves del suscriptor del HSS**: el IMSI y las claves de autenticación de un suscriptor ya provisionado en la red.

OmniWeb las combina en una tarjeta de software. Esta tarjeta responde a las lecturas de archivos del módem a partir de la imagen y responde al desafío de autenticación de la red con las claves del HSS. Superpone el IMSI del suscriptor elegido. A través de un cardem, el módem no puede distinguirla de una SIM de plástico: lee el IMSI, realiza la autenticación y **se conecta a la red en vivo**.



Cuándo usarlo

- Reproducir el comportamiento de roaming o conexión de un suscriptor específico sin una fuente para su SIM física.
- Probar muchos suscriptores provisionados contra un módem, uno tras otro.
- Probar perfiles que solo existen en el HSS (nuevamente provisionados, pre-envío).

Qué prueba. Un módem en el banco se ha conectado a la red en vivo (`registrado, red local`) como un suscriptor HSS para el cual no existe una SIM de plástico. Leyó el IMSI de ese suscriptor y completó la autenticación de la red completamente a partir de la tarjeta virtual.

> Un elemento dedicado de **Lector de SIM Virtual** es el siguiente paso en esta capacidad. Allí "cargas" una SIM virtual a partir de una imagen y suscriptor elegidos y la presentas como cualquier otra ranura de lector. Hoy, OmniWeb conecta la tarjeta virtual a través del mismo corredor de SIM remota y ruta de cardem descrita anteriormente.

Usando una SIM en un Libro de Pruebas de Roaming

Los **Libros de Pruebas** de roaming (GSMA IR.38 / IR.48) pueden impulsar la presentación de SIM como parte de una ejecución. En el panel de **Ejecutar Pruebas** de un libro de pruebas puedes elegir:

- una **SIM (por ICCID / IMSI)**: rastreada por identidad, su lector actual resuelto automáticamente en tiempo de ejecución, y
- un **Módem Cardem**: el cardem al que se emula la SIM.

Presentar SIM al cardem establece la asignación antes de que pruebes. **Ir: Ejecutar Todas las Pruebas** presenta primero la SIM (cuando se seleccionan tanto una SIM como un cardem), luego lee el IMSI y ejecuta los casos de datos. Si la SIM no está actualmente en un lector, o el cliente del cardem no está en ejecución, el panel dice exactamente por qué. No se ejecuta contra el cardem incorrecto en silencio.

Consulta Dispositivos de Prueba y la documentación del libro de pruebas para el resto del flujo IR.38.

Solución de Problemas

Una SIM no aparece en el banco

Síntomas: un lector está conectado pero no se muestra ninguna ranura (o una ranura vacía).

Causas posibles y resolución:

- La tarjeta no está colocada, o la combinación lector/tarjeta no puede alimentar la tarjeta. La ranura muestra **Tarjeta presente** o **Vacío**. Vuelve a colocar la SIM.

- El lector acaba de ser conectado. OmniWeb vuelve a escanear lectores al conectarse, pero puedes forzarlo con **Volver a escanear** en el grupo del agente.

El módem no se conecta después de conectar una SIM

Causas posibles y resolución:

- El módem no ha vuelto a leer la SIM. Usa **Reiniciar módem** en la consola cardem para volver a presentar la tarjeta.
- La asignación no está **ACTIVA**. Confirma bajo **Asignaciones activas** en la página de SIM Remota que la SIM está vinculada al cardem correcto.
- El suscriptor no está provisionado (o está bloqueado) en el HSS de la red que sirve.

"Tarjeta presente (ilegible)" en un lector

Síntomas: se detecta una tarjeta pero no se puede leer su identidad.

Resolución: ese lector no puede comunicarse con esa tarjeta (comúnmente una incompatibilidad de voltaje/protocolo en lectores económicos). Mueve la SIM a un lector diferente en el banco.

SIM Virtual: el módem lee la tarjeta pero no se conecta

Causas posibles y resolución:

- El suscriptor elegido debe estar **habilitado** y completamente provisionado (con un perfil de datos) en el HSS para la red que sirve.
- La imagen base debe provenir de un tipo de tarjeta compatible. Si la inicialización se detiene, vuelve a capturar la imagen base de una SIM conocida como buena.

SCEF: Función de Exposición de Capacidades de Servicio

El **SCEF** (Función de Exposición de Capacidades de Servicio), **OmniSCEF** de Omnitouch, es la **puerta de enlace norte** de la red para el Internet de las Cosas. Expone las capacidades de la red central a los Servidores de Aplicaciones externos a través de la API RESTful **3GPP T8** definida en TS 29.122, de modo que una plataforma de máquina a máquina pueda suscribirse a eventos sobre una flota de dispositivos e intercambiar pequeñas cantidades de datos con ellos sin necesidad de hablar Diameter o GTP. Se presenta frente a dos familias de servicio. Los **Eventos de Monitoreo** piden a la red que informe cuando un dispositivo se vuelve accesible, pierde conectividad, cambia de ubicación, etc. La **Entrega de Datos No IP (NIDD)** transporta pequeñas cargas útiles no IP hacia y desde dispositivos NB-IoT restringidos a través del plano de control. Internamente, el SCEF se conecta al MME a través de la interfaz Diameter **T6a** (TS 29.128). OmniWeb muestra su estado, los recursos T8 que un Servidor de Aplicaciones ha creado y las sesiones NIDD activas que está llevando.

← Guía de Operaciones

El panel es una página de elemento por instancia que se alcanza desde la barra lateral cuando un SCEF se ejecuta en el inventario del sitio. Todo el tráfico pasa a través del proxy backend de OmniWeb hacia la API T8 del SCEF, por lo que permanece detrás de la única puerta de enlace autenticada. Un enlace de documentación en el encabezado de la página proporciona ayuda contextual. La página está organizada en pestañas.

El modelo de ID SCS/AS

Cada recurso T8 (cada suscripción de monitoreo y cada configuración de NIDD) está **asociado a la identidad SCS/AS** bajo la cual el Servidor de Aplicaciones se registró (el *Servidor de Capacidades de Servicios / Servidor de Aplicaciones*). La API T8 **no tiene un punto final que enumere los IDs SCS/AS** en uso, por lo que OmniWeb no puede descubrirlos por ti: el operador **establece el ID SCS/AS** en la página, y OmniWeb lo recuerda **a través de las pestañas del SCEF**, de modo que lo estableces una vez y se lleva de Resumen a Eventos de Monitoreo a NIDD. Hasta que se establezca un ID SCS/AS, las pestañas asociadas solicitan uno en lugar de mostrar una lista vacía. Los recursos existen bajo una identidad que debes nombrar. Ingresa el ID SCS/AS con el que se incorporó un Servidor de Aplicaciones (por ejemplo `iot-platform-01@omnitouch`) para trabajar con las suscripciones y configuraciones de esa plataforma.

Resumen

Una lectura de salud de pantalla única del SCEF en sí: su **estado**, nombre del **producto**, estado de la **licencia** y el **host Diameter** que utiliza para T6a

hacia el MME. Debajo se encuentra el **contexto de aplicación** (el campo ID SCS/AS descrito anteriormente) y, una vez que se establece un ID SCS/AS, el recuento de **suscripciones de monitoreo** y **configuraciones NIDD** actualmente mantenidas para ese Servidor de Aplicaciones. Es la confirmación más rápida de que el SCEF está activo y cuánto está llevando una plataforma dada. Se proporcionan paneles de monitoreo y estadísticas como incrustaciones de Grafana, accesibles desde la misma página.

Eventos de Monitoreo

Las **suscripciones de eventos de monitoreo** que un Servidor de Aplicaciones ha creado para el ID SCS/AS actual. Cada suscripción pide a la red que informe una clase de evento y lo envíe por POST al Servidor de Aplicaciones; cada fila muestra:

- **Tipo de evento**: el tipo de monitoreo, como **Accesibilidad UE**, **Pérdida de Conectividad**, **Informe de Ubicación**, **Disponibilidad después de Fallo DDN**, **Estado de Roaming** o **Número de UEs en un Área**.
- **Objetivo**: el dispositivo o grupo que la suscripción monitorea, identificado por un **ID Externo**, un **MSISDN** o un **ID de Grupo Externo** para toda una

flota.

- **Destino de notificación**: la **URL de callback** a la que el SCEF envía por POST cada informe de evento. Debe ser una dirección `http(s)` absoluta que el Servidor de Aplicaciones exponga.
- **Máx. Informes** y, para una suscripción de accesibilidad, el **tipo de accesibilidad** (`SMS` o `DATA`). Junto con la **duración/expiración** de monitoreo, estos limitan cuántos eventos se envían y hasta cuándo vive la suscripción.

Las suscripciones pueden ser creadas, editadas y eliminadas; eliminar una detiene al Servidor de Aplicaciones de recibir esos informes de eventos.

NIDD

Las **configuraciones NIDD** son las vinculaciones de Entrega de Datos No IP que un Servidor de Aplicaciones ha creado para el ID SCS/AS actual. Una configuración autoriza el intercambio de pequeñas cargas útiles no IP con un dispositivo a través del plano de control. Cada fila muestra:

- **Objetivo**: el dispositivo por **ID Externo**, **MSISDN** o **ID de Grupo Externo**.
- **DNN / APN**: el Nombre de Red de Datos (APN) que utiliza la conexión PDN NIDD (por ejemplo `nidd.iot.omnitouch`).
- **Estado**: `ACTIVO`, o terminado (`TERMINADO`, `TERMINADO_UE_NO_AUTORIZADO`).
- **Máx. Paquete**: el **tamaño máximo de paquete** en bytes que puede alcanzar la carga útil no IP.
- **RDS**: si el **Servicio de Datos Confiable** está habilitado. Agrega un transporte ligero con acuse de recibo con puertos de origen/destino a través del enlace no IP.

Una configuración también lleva una **opción de establecimiento de PDN** que decide qué sucede cuando llegan datos de bajada mientras el dispositivo no tiene una conexión PDN NIDD activa: **esperar a que el UE** establezca una, **indicar un error**, o **establecer la conexión PDN** al paginar el dispositivo.

Entrega de datos de bajada

Desde una configuración NIDD puedes **entregar una carga útil de bajada** al dispositivo. Ingresa la carga útil como texto. El SCEF **la codifica en base64**

antes de enviarla a través de NIDD, y cada entrega puede llevar una **prioridad** y una **latencia máxima**. Las entregas recientes se enumeran con su **estado de entrega**: `ÉXITO`, `BUFFERING`, `ENVIANDO`, o una de las razones de fallo como `FALLO_UE_NO_ACCESIBLE`. Puedes cancelar una entrega en cola o en búfer. Así es como una plataforma envía un comando o un ajuste de firmware a un dispositivo restringido que no tiene dirección IP.

Sesiones NIDD

Las **sesiones NIDD T6a activas** son las vinculaciones de Entrega de Datos No IP que el SCEF mantiene con el MME en este momento. A diferencia de las configuraciones NIDD, que son recursos T8 asociados a un ID SCS/AS, estas son **estado de ejecución global del servidor**: son **solo lectura** y no están asociadas por ID SCS/AS, por lo que esta pestaña muestra cada sesión activa independientemente del contexto de aplicación que estés visualizando. Cada fila muestra el **IMSI** del dispositivo, el **APN** que utiliza la conexión PDN NIDD, la **Identidad de Portadora EPS (EBI)**, el **estado** de la sesión (`ACTIVO`, `INACTIVO`), el **id de sesión T6a**, el **host MME** que sirve y el **reino MME**, y el **id de configuración** contra el cual se configuró la sesión. Es la forma más

rápida de ver qué dispositivos tienen realmente una vinculación no IP activa, y a través de qué MME.

Registros

La pestaña de **Registros** muestra la salida de registro en vivo del SCEF para solucionar problemas de una sola instancia sin salir de OmniWeb.

Paneles de monitoreo

Las tasas de solicitud T8, el rendimiento de informes de eventos y los recuentos de entrega NIDD para el SCEF se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- **MME**: el SCEF se conecta a él a través de **T6a** para establecer conexiones PDN NIDD y para recopilar los eventos de monitoreo informados aquí. El host MME y el reino que utiliza cada sesión se muestran en la pestaña de Sesiones NIDD.
- **HSS**: contiene los datos de suscripción (Identificadores Externos, autorización NIDD) de los que dependen los servicios de monitoreo y NIDD del SCEF.
- **PGW-C / SMF** y **UPF**: transportan el plano de datos IP ordinario. NIDD deliberadamente los elude para mover pequeñas cargas útiles no IP a través del plano de control en su lugar.
- Guía de Operaciones: de vuelta al índice de elementos.

SGW-C: Puerta de enlace de servicio (Plano de control)

El **SGW-C** es la mitad del plano de control de la Puerta de enlace de servicio EPC. Ancla los portadores de cada suscriptor entre la red de acceso y la puerta de enlace de paquetes: termina **S11** hacia el MME (señalización de sesión y portador), **S5/S8** hacia el PGW-C (la conexión PDN), y programa el plano de usuario (SGW-U) que reenvía el tráfico en **S1-U** hacia el eNodeB. En resumen, es el nodo que mantiene el estado del portador activo para cada suscriptor conectado y mantiene sincronizados el MME, PGW y el plano de usuario. OmniWeb muestra las sesiones activas del SGW-C, el conteo de sesiones y los registros; las tendencias a largo plazo (rendimiento, crecimiento de sesiones) están en los paneles de Grafana accesibles desde la misma página.

← Guía de operaciones

El SGW-C es una página de elemento por instancia que se accede desde la barra lateral cuando se opera en el inventario del sitio. Donde se despliegan varios, también proporciona una vista de flota para el estado agregado. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del SGW-C, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda contextual) abre esta página. Está organizada en pestañas.

Visión general

Una lectura de salud en una sola pantalla: el **estado de la API** del SGW-C, el **conteo de sesiones activas**, y un resumen derivado de las sesiones activas: el número de **MMEs** únicos (pares S11 distintos), **PGWs** únicos (pares S5/S8 distintos), y los **portadores totales** actualmente anclados. Es la forma más rápida de confirmar que el SGW-C está activo, cuántas sesiones tiene y cuántos MMEs y PGWs está utilizando.

Sesiones

Cada sesión anclada, cada fila identificada por el **IMSI** y **MSISDN** del suscriptor con su **estado** de conexión. Abrir una sesión muestra su estado completo del portador: los puntos finales de control **S11** (F-TEIDs del lado del MME y del lado del SGW), cada **conexión PDN** (APN, portador por defecto, y los F-TEIDs de control S5/S8 hacia el PGW), y cada **portador** (EBI, los F-TEIDs del plano de usuario S1-U y S5/S8, y su QoS). Aquí es donde confirmas que los portadores de un suscriptor específico están establecidos y ves qué MME y PGW los están sirviendo.

Donde se despliegan varios SGW-Cs, la misma pestaña en la **vista de flota** lista cada sesión a través de todos ellos en una tabla, con el SGW-C que sirve mostrado contra cada fila, para que un operador pueda encontrar un suscriptor sin saber qué SGW-C lo está anclando. Abrir una fila va a esa sesión en su propia instancia. Una instancia que no se puede alcanzar se nombra sobre la tabla, y también se indica el límite de filas por instancia cuando una instancia tiene más sesiones de las que la vista combinada puede mostrar.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo del SGW-C para solucionar problemas de una sola puerta de enlace sin salir de OmniWeb.

Paneles de monitoreo

El rendimiento, las tendencias de conteo de sesiones y otras series temporales para el SGW-C se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- MME: el par de control sobre **S11**; impulsa la configuración de sesión y portador en el SGW-C.
- El **PGW-C** ancla la conexión PDN sobre **S5/S8**.
- El **SGW-U / UPF** es el plano de usuario que el SGW-C programa para reenviar tráfico en S1-U.

Herramientas de tarjeta SIM: Sistema de archivos, APDU y eSIM

OmniWeb hace más que descubrir y presentar SIMs. Te proporciona un conjunto de **herramientas de tarjeta de bajo nivel** que se comunican directamente con la tarjeta a través de cualquier lector en cualquier agente. Puedes explorar y editar su sistema de archivos, enviar APDUs en bruto manualmente, observar el seguimiento en vivo de APDU de una sesión de SIM remota y gestionar perfiles de eSIM en un eUICC. Esta página es la guía de operaciones para esas herramientas.

← Guía de Operaciones

Estas herramientas se encuentran junto a las características existentes de SIM y las reutilizan. Comienza aquí para tener una visión general:

- **Banco de SIM**: el inventario: qué SIMs están en qué lectores a través de cada agente. Cada herramienta en esta página apunta a un lector de ese inventario, y las acciones por ranura del Banco de SIM enlazan directamente a ellas.
- **Imágenes de SIM (Paquetes de Perfil SAIP)**: cómo guardar un sistema de archivos leído como una imagen portátil, y cómo explorar o diferenciar imágenes guardadas.
- **SIM Remota y SIM Virtual**: cómo presentar una SIM (real o virtual) a un módem a través de emuladores de tarjeta.
- **Gestión de SIM OTA**: la misma edición a nivel de archivo, pero llega a una tarjeta **a través del aire** con paquetes asegurados (03.48 / SCP80) en lugar de un lector local.

Las cuatro herramientas a continuación se encuentran en la barra lateral bajo el grupo **SIMs**.

Un lector, un consumidor a la vez

Solo una cosa a la vez puede controlar un lector físico PC/SC. Una herramienta en esta página puede necesitar un lector que ya esté en uso por otra cosa: otro operador que lo lea, o una sesión de banca de SIM remota activa que lo presente a un módem. La herramienta entonces muestra **quién lo tiene y por qué**, y ofrece una opción explícita de **Tomar control**. No hay un desalojo silencioso: cuando tomas el control, OmniWeb cancela la otra sesión (y, para una sesión de banca, desconecta ese enlace SIM↔cardem). Para editar o enviar es una acción de control que requiere el permiso de control del banco de SIM. Sin él, puedes ver lectores pero no controlar tarjetas.



Explorador del Sistema de Archivos SIM

Elige un lector y **lee todo el árbol de archivos** de su tarjeta: el MF, DF.GSM / DF.TELECOM, ADF.USIM y ADF.ISIM y todos sus EFs, con cada archivo legible decodificado en campos nombrados. Una lectura completa toca muchos archivos, por lo que una barra de progreso muestra el avance ("leído X de Y archivos: EF....").

- **Buscar** en el árbol por código de archivo (FID), nombre corto o descripción. Una búsqueda de "Códigos de Llamada de Emergencia" encuentra EF.ECC, no solo `6FB7`.
- **Los archivos protegidos por PIN están marcados, nunca leídos**: el explorador no agotará los reintentos de PIN.
- **Editar un EF** (con el permiso de control): el panel de detalles ofrece un formulario guiado por esquema (campos decodificados, tipados) donde esté disponible, y recurre a hex en bruto. Una escritura es destructiva y solicita confirmación. Donde un EF necesita autenticación, usa **Verificar CHV/ADM** primero. Esto prueba un PIN/clave ADM contra la tarjeta (informa los intentos restantes y nunca agota el último reintento). Una vez

probado, el explorador lo reutiliza para la escritura. El almacén de claves SIM ofrece claves guardadas para el ICCID de una tarjeta automáticamente.

- **Guardar imagen** toma una instantánea del árbol decodificado como una Imagen SIM nombrada. **Comparar con imagen** diferencia la tarjeta en vivo contra una guardada. **Imágenes guardadas** abre la biblioteca de imágenes. También puedes abrir una imagen guardada *como* un árbol (`?image=<id>`) para explorar una tarjeta que ya no tienes en un lector.

El lector debe estar libre (no sostenido por una sesión de SIM remota), o puedes tomar el control como se mencionó anteriormente.

Terminal APDU

El Terminal APDU es una **consola manual para la tarjeta**: escribe un APDU en bruto en hex, envíalo a la tarjeta en un lector elegido y ve la respuesta decodificada. La decodificación muestra el nombre INS del comando, la palabra de estado y su significado, y una interpretación ampliada de cualquier dato de respuesta (un árbol TLV FCP, campos EF decodificados, o un resultado de AUTENTICAR). Botones predefinidos (SELECCIONAR MF, ESTADO, LEER BINARIO, OBTENER RESPUESTA, …) llenan comandos comunes. La entrada es tolerante a espacios en blanco/dos puntos y validada (bytes completos, al menos CLA/INS/P1/P2).

Dos modos:

Modo	Comportamiento	Usar para
Disparo único	Cada APDU es autónomo; la tarjeta se reinicia al MF entre envíos.	Sondeos únicos.
Sesión	Abre una sesión de tarjeta persistente y exclusiva, por lo que el estado (selección, autenticación) **persiste** entre APDUs: un SELECCIONAR seguido de un LEER BINARIO funciona, y un VERIFICAR comparte su autenticación con una posterior ACTUALIZAR. El lector permanece ocupado hasta que cierras la sesión.	Secuencias con estado.

La acción **APDU** por ranura del Banco de SIM enlaza aquí con ese lector exacto preseleccionado. Se aplican las mismas reglas de un consumidor/Tomar control.

Registro APDU

Donde el terminal eres tú controlando una tarjeta, el **Registro APDU** es un **seguimiento pasivo en vivo** de los APDUs de comando/respuesta intercambiados entre un **módem y una SIM (remota)** a través de la cadena de SIM remota / cardem. Activa la **captura** y sigue el intercambio: cada fila empareja un comando `módem→tarjeta` con su palabra de estado decodificada, además de la misma decodificación de respuesta que el terminal (árbol FCP, campos EF, eventos ATR/reset). Puedes pausar la vista (la captura sigue en ejecución), filtrar por comando/hex/SW y desplazarte automáticamente.

Úsalo para ver lo que un módem realmente le pregunta a la SIM durante un attach o una ejecución de prueba IR.38: qué archivos selecciona, dónde falla un VERIFICAR, si un AUTENTICAR tiene éxito. No tienes que instrumentar el módem. Se empareja naturalmente con SIM Remota, que establece el enlace módem↔SIM que luego rastrea el registro.

---

eSIM (LPA)

La herramienta **eSIM** gestiona un **eUICC** a través del **Asistente de Perfil Local (LPA)** del agente. Un eUICC es un chip eSIM físico en uno de tus lectores. Contiene varios perfiles, pero solo uno está activo a la vez.

- **Tarjeta eUICC**: muestra el **EID** del chip.
- **Perfiles instalados**: cada perfil en la tarjeta: su estado (activo/deshabilitado), apodo, proveedor, nombre e ICCID. Por perfil puedes **habilitar** (hacerlo el eSIM activo), **deshabilitar**, **renombrar** (apodo) o **eliminar**. Una eliminación quita el perfil del eUICC y es irreversible, por lo que primero solicita confirmación.
- **Descargar un perfil**: extraer un nuevo perfil de un SM-DP+ de un operador e instalarlo en la tarjeta. Usa un **código de activación** completo (`LPA:1$smdp.example.com$MATCHING-ID`) o una **dirección SM-DP+ dividida + ID de coincidencia**, con un código de confirmación opcional.

Esto es específicamente para tarjetas eSIM (eUICC). Para la edición de archivos de SIM/UICC clásica, utiliza el Explorador de Sistema de Archivos anterior. Para editar una tarjeta **de forma remota**, utiliza OTA.

Kit de Herramientas SIM (STK)

El cliente **Kit de Herramientas SIM** controla applets STK en una tarjeta SIM. Envía un perfil de terminal a la tarjeta, luego presenta cada comando proactivo como una pantalla interactiva: menús, visualización de texto, entrada de una tecla y entrada de texto. Úsalo para navegar por servicios residenciales del operador, activar flujos de configuración OTA o probar la lógica de applets residentes en la SIM.

Consulta **Kit de Herramientas SIM** para la guía completa de operaciones.

Relacionados

- Banco de SIM: el inventario de lector/SIM que estas herramientas apuntan.

- Imágenes de SIM: guardar, explorar y diferenciar sistemas de archivos leídos.
- SIM Remota y SIM Virtual: presentar una SIM a un módem a través de la red (el enlace que rastrea el Registro APDU).
- Gestión de SIM OTA: la misma edición de archivos, a través del aire.
- Kit de Herramientas SIM: interactuar con applets STK en una tarjeta en un lector.

Imágenes SIM: Paquetes de Perfil SAIP

Una **Imagen SIM** es una instantánea guardada de todo el sistema de archivos de una tarjeta. OmniWeb almacena cada imagen como un **Paquete de Perfil No Protegido SAIP (UPP)** en codificación DER. Este es el mismo formato interoperable que utilizan los perfiles eUICC, definido por la *Especificación Técnica de Formato Interoperable de Paquete de Perfil eUICC* del TCA. Una tarjeta capturada se convierte en un archivo portátil `.der` que cualquier herramienta compatible con SAIP puede leer.

Esta página es la guía de operaciones. Cubre cómo capturar, exportar, cargar, navegar y diferenciar imágenes SIM, y cómo usar una imagen guardada para respaldar un SIM virtual. SIM Bank cubre el inventario del lector en vivo.

Tabla de Contenidos

- Por qué SAIP UPP
- Descripción General de la Arquitectura
- Qué hay en una Imagen
- Capturando una Imagen
- Exportando una Imagen
- Cargando una Imagen
- Navegando una Imagen en el Explorador
- Diferenciando Dos Imágenes
- Respaldando un SIM Virtual con una Imagen
- Referencia de Elementos de Perfil
- Solución de Problemas

Por qué SAIP UPP

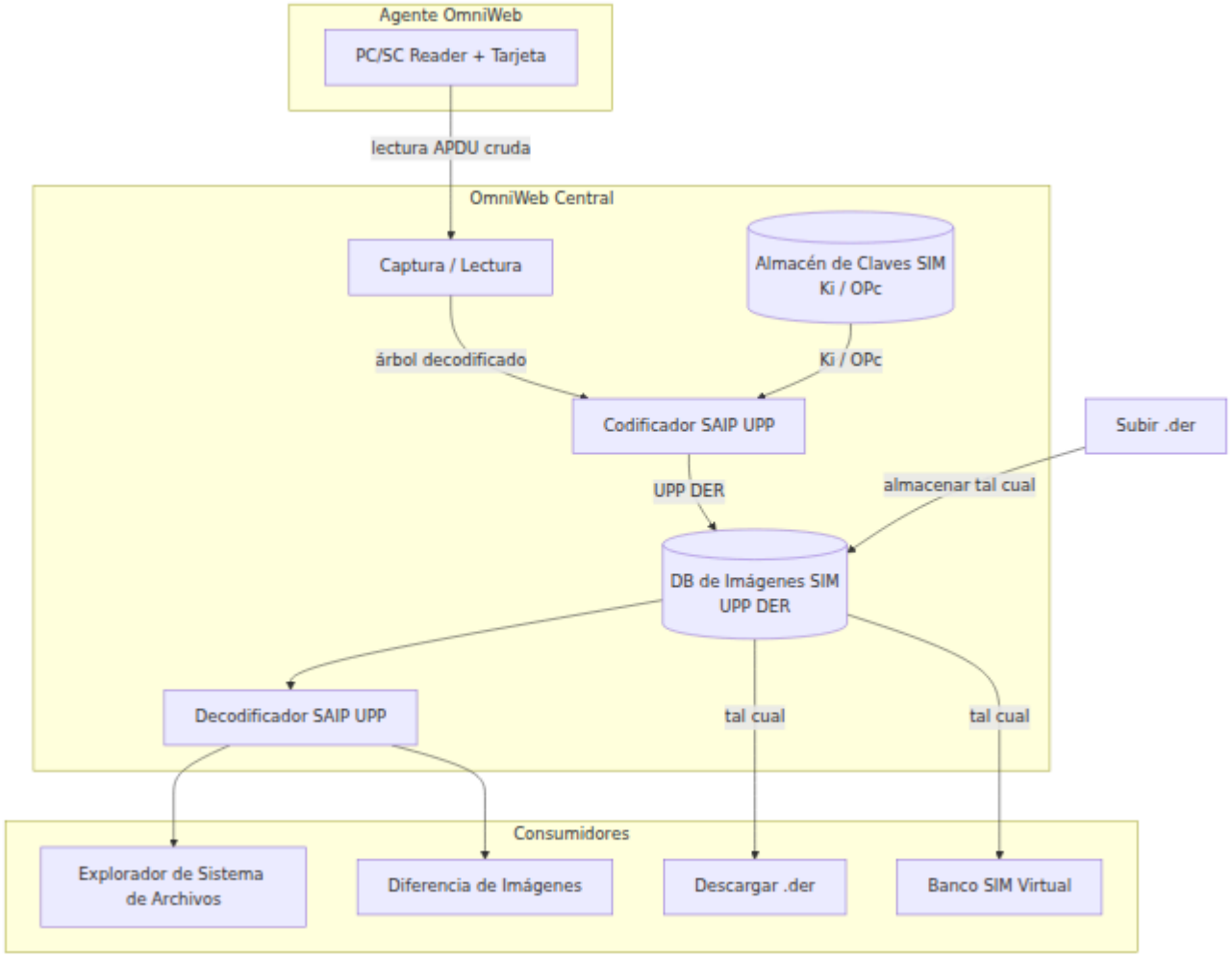
Las versiones anteriores almacenaban una imagen SIM como un árbol JSON decodificado utilizado solo para diferenciar. Ese formato era privado de OmniWeb y ninguna herramienta externa podía consumirlo.

Cuando OmniWeb almacena la imagen como un **SAIP UPP**, obtienes:

- **Portabilidad**: el `.der` exportado es un paquete de perfil estándar. Se carga en validadores de perfil SAIP y en cualquier cadena de herramientas compatible con SAIP.
- **Un formato en todas partes**: el mismo `.der` que un operador descarga es lo que respalda un SIM virtual y lo que el explorador de archivos representa. No hay una segunda representación divergente.
- **Reaprovisionamiento**: cuando se conocen las claves de autenticación de la tarjeta (ver Capturando una Imagen), el UPP incluye un elemento `PE-AKAParameter` que lleva Ki y OPc. El paquete describe entonces un perfil completo e instalable en lugar de un volcado de solo lectura.

El paquete es una concatenación cruda de Elementos de Perfil codificados en DER. **No está** cifrado (es un *Paquete de Perfil No Protegido*). Trata un `.der` exportado con el mismo cuidado que cualquier archivo que contenga Ki/OPc. Ver Solución de Problemas.

Descripción General de la Arquitectura



La captura lee la tarjeta, el codificador produce un UPP (incorpora Ki/OPc del Almacén de Claves SIM si está disponible), y OmniWeb almacena el paquete. Cada consumidor lee de ese único paquete almacenado. El explorador y la diferencia lo decodifican a un árbol bajo demanda. La descarga y el banco SIM virtual utilizan los bytes tal cual.

Qué hay en una Imagen

Una imagen capturada contiene, para el diseño estándar MF / ADF.USIM de la tarjeta:

Elemento	Elemento de Perfil SAIP	Contenido
Sistema de archivos	`PE-GenericFileManagement`	Cada EF accesible: sus Parámetros de Control de Archivo (FCP) y contenido crudo (EFs transparentes) o cada registro (EFs lineales/cíclicos)
Identidad	`PE-Header`	El ICCID de la tarjeta
Autenticación	`PE-AKAParameter`	Ki y OPc para Milenage. **Presente solo cuando las claves de la tarjeta están en el Almacén de Claves SIM**

Los archivos se crean con `PE-GenericFileManagement` (un grupo de operaciones por DF) en lugar de las plantillas de sistema de archivos SAIP estandarizadas: una lectura de tarjeta recupera bytes crudos, no la plantilla que un creador de perfil utilizó originalmente, por lo que la representación genérica siempre es exacta.

Capturando una Imagen

La captura se realiza desde el Sistema de Archivos SIM en el explorador o las acciones del slot del SIM Bank:

1. Leer el sistema de archivos de una tarjeta en el explorador.
2. Elegir **Guardar imagen** y darle una etiqueta.

El sistema de archivos decodificado se codifica en un UPP y se almacena. Si existe una entrada en el Almacén de Claves SIM para el ICCID de la tarjeta con **Ki** y **OPc**, esas claves se escriben en un `PE-AKAParameter` para que el paquete resultante sea completamente instalable. Sin una entrada en el almacén de

claves, el paquete aún captura el sistema de archivos completo; solo se omite el elemento de autenticación.

Las **columnas de identidad** (ICCID, IMSI, tipo de tarjeta, conteo de archivos) se derivan del sistema de archivos en el momento de la captura, por lo que la lista de imágenes y el encabezado de diferencia nunca tienen que volver a decodificar el paquete.

Exportando una Imagen

Cada fila en la lista de imágenes guardadas tiene una acción de **descarga** que sirve el paquete almacenado tal cual como `UPP_<iccid>.der`.

El `.der` descargado es un UPP SAIP estándar y se puede inspeccionar con cualquier herramienta de perfil compatible con SAIP.

Cómo funciona: El archivo son los bytes exactos almacenados en la captura (o carga), sin recodificación en la descarga, por lo que una descarga de ida y vuelta es byte por byte idéntica a lo que se almacenó.

Cargando una Imagen

La página de imágenes guardadas tiene una acción de **Cargar .der** que acepta un archivo SAIP UPP y lo almacena como una nueva imagen. Úsalo para traer perfiles generados en otros lugares: por ejemplo, los paquetes de *Perfil de Prueba Genérico eUICC* del GSMA TS.48, o un UPP producido por otra herramienta SAIP.

Al cargar, OmniWeb:

1. Valida que el archivo comience con una etiqueta de Elemento de Perfil SAIP (una etiqueta construida de clase de contexto: `A0`, `A1` o `B0`).
2. Almacena el paquete tal cual.
3. Decodifica el `PE-Header` para poblar la columna ICCID donde esté presente.

Una imagen cargada es una imagen de primera clase: se puede descargar, navegar en el explorador, diferenciar, editar y usar para respaldar un SIM virtual exactamente como una capturada.

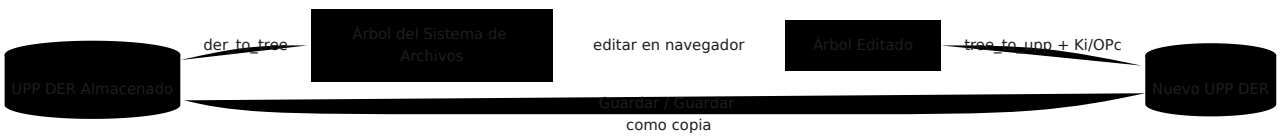
Editando una Imagen

Una imagen guardada es un **archivo**, no una tarjeta. Para editar una, se cambia solo el paquete de perfil almacenado y **nunca se escribe en ningún SIM**. Desde la lista de imágenes guardadas, la acción **Editar sistema de archivos** abre el Sistema de Archivos SIM en modo de edición (`?image=<id>&edit=1`). No se involucran lectores ni acceso a tarjetas de agente.

Puedes:

- **Editar el contenido de un archivo**: cambiar los bytes de cualquier EF. Al igual que con una tarjeta en vivo, el editor ofrece un **Formulario** impulsado por esquema, una vista de **JSON** de todo el registro y un acceso de **Hex crudo**. No hay un aviso de PIN/ADM (un archivo no tiene condiciones de acceso que satisfacer).
- **Agregar un archivo**: crear un nuevo EF (transparente o estructurado por registro) o DF bajo cualquier DF/MF/ADF, y dar su FID, estructura y contenido inicial.
- **Eliminar un archivo**: eliminar cualquier EF o DF (la raíz MF es toda la imagen y no se puede eliminar).
- **Renombrar** la imagen (solo metadatos) desde la lista.

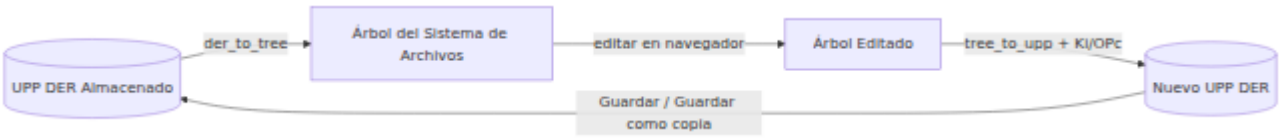
El navegador mantiene los cambios hasta que **Guardar imagen** (sobrescribir en su lugar) o **Guardar como copia** (dividir una nueva imagen y dejar la original intacta). Al guardar, OmniWeb recodifica el árbol del sistema de archivos editado a un SAIP UPP. Incorpora Ki/OPc del Almacén de Claves SIM cuando se conoce. Preserva tal cual cualquier Elemento de Perfil que el árbol no modele (PIN, PUK, Dominio de Seguridad, plantillas), por lo que una edición nunca elimina el resto del perfil.



Edición de campos de Formulario / JSON sin conexión. Para decodificar un EF en campos nombrados y recodificarlos, utiliza el mismo modelo de archivo que usa el editor en vivo, ejecutado en cualquier agente en línea, pero sin **tarjeta**: la imagen ya contiene los bytes, por lo que el agente solo ejecuta el códec. Si no hay un agente en línea, la edición vuelve a Hex crudo, que no necesita nada externo.

Navegando una Imagen en el Explorador

Cada imagen guardada tiene una acción de **Navegar en el explorador de sistema de archivos**. Abre el Sistema de Archivos SIM contra el paquete almacenado. **No se necesita tarjeta física ni lector**. OmniWeb decodifica el paquete de vuelta al mismo árbol del sistema de archivos que el explorador representa para una tarjeta en vivo, por lo que puedes inspeccionar el contenido crudo de cada EF sin conexión.



Diferenciando Dos Imágenes

La página de imágenes guardadas te permite seleccionar dos imágenes y diferenciarlas. Ambos paquetes se decodifican en árboles de sistema de archivos y se alinean por la ruta de EF, por lo que la comparación es archivo por archivo sin importar el orden de captura:

Estado	Significado
`same`	EF presente en ambos con contenido idéntico
`changed`	EF presente en ambos, el contenido difiere
`only_a`	EF presente solo en la primera imagen
`only_b`	EF presente solo en la segunda imagen

Para un EF **cambiado**, la diferencia informa los rangos de bytes que difieren (y deltas por registro para archivos estructurados por registro), por lo que puedes ver exactamente qué bytes se movieron: por ejemplo, un SIM de prueba antes y después de un cambio de personalización, o dos SIM de operadores uno al lado del otro.

Respaldando un SIM Virtual con una Imagen

Una imagen guardada puede sustituir a una tarjeta física al presentar un SIM virtual. En el compositor de SIM virtual, las imágenes guardadas aparecen junto a las imágenes rspro capturadas como fuentes de sistema de archivos seleccionables. Combina una con una identidad de suscriptor (del HSS o del Almacén de Claves SIM) y OmniWeb lanza un `bankd` virtual respaldado por el sistema de archivos de esa imagen, con el Ki/OPc del suscriptor superpuesto para autenticación.



El sistema de archivos que lee el módem se reproduce desde la imagen; la identidad y las claves se superponen desde el suscriptor elegido, por lo que una imagen puede respaldar a muchos suscriptores.

Referencia de Elementos de Perfil

El UPP es una secuencia de Elementos de Perfil, cada uno un DER TLV cuya etiqueta de clase de contexto identifica su tipo. OmniWeb escribe y lee el subconjunto a continuación; otros elementos en un paquete cargado (PIN, PUK, Dominio de Seguridad, plantillas de sistema de archivos) se preservan en el almacenamiento y se omiten al decodificar a un árbol de sistema de archivos.

Etiqueta	Elemento de Perfil	Usado por OmniWeb
`A0`	`PE-Header`	ICCID; metadatos del perfil
`A1`	`PE-GenericFileManagement`	El sistema de archivos (FCP + contenido)
`A4`	`PE-AKAParameter`	Ki y OPc (Milenage)
`AA`	`PE-End`	Marcador de fin de paquete
`B0`	`PE-MF`	(MF con plantilla: leído en carga, no emitido)

Para el catálogo completo de elementos y reglas de codificación, consulta la Especificación Técnica de Formato Interoperable de Paquete de Perfil eUICC del TCA.

Solución de Problemas

La imagen exportada no tiene claves de autenticación

Síntomas: Un `.der` descargado no tiene `PE-AKAParameter`; un SIM virtual respaldado por la imagen no puede autenticarse sin claves suministradas por separado.

Causas posibles:

- No existía una entrada en el Almacén de Claves SIM para el ICCID de la tarjeta en el momento de la captura.
- La entrada en el almacén de claves carecía de Ki u OPc.

Resolución:

1. Agrega el Ki y OPc de la tarjeta al Almacén de Claves SIM, indexado por su ICCID.
2. Vuelve a capturar la imagen. La nueva captura incorpora las claves en un `PE-AKAParameter`.
3. Alternativamente, suministra las claves en el momento de presentación del SIM virtual (desde el HSS o un anulación explícita).

Carga rechazada como "no parece un SAIP UPP"

Síntomas: Cargar un archivo devuelve un error de validación.

Causas posibles:

- El archivo no es un SAIP UPP: no comienza con una etiqueta de Elemento de Perfil (`A0`, `A1` o `B0`).
- El archivo es un paquete de perfil *protegido* (cifrado), no uno *no protegido*.

Resolución:

1. Confirma que el archivo es un **Paquete de Perfil No Protegido** en codificación DER.
2. Verifica que comience con un `PE-Header` (`A0`). La mayoría de los UPP bien formados lo hacen.
3. Si el paquete está protegido/cifrado, no se puede almacenar ni navegar; solo se admiten paquetes no protegidos.

Navegar una imagen cargada muestra archivos por FID, no por nombre

Síntomas: Los EFs en el explorador están etiquetados por identificador de archivo (por ejemplo, `EF.6FXX`) en lugar de un nombre amigable.

Causas posibles:

- Una lectura de tarjeta recupera identificadores de archivo y contenido crudo, no los nombres simbólicos que utilizó un creador de perfil. OmniWeb mapea los EFs USIM bien conocidos a nombres amigables; cualquier EF fuera de ese mapa se muestra por su FID.

Resolución: No se necesita ninguna acción. El FID es el identificador autoritativo y el contenido crudo es exacto. Esto es esperado para archivos no estándar o específicos de proveedores.

Manejo seguro de paquetes exportados

Un UPP exportado es **no cifrado** y, cuando las claves estaban disponibles en la captura, contiene Ki y OPc. Trata un `.der` descargado como material clave sensible:

- No lo envíes a través de canales no confiables.
- Elimina copias locales cuando ya no sean necesarias.
- Prefiere mantener imágenes dentro de OmniWeb (donde el acceso está restringido por el permiso del SIM Bank) sobre distribuir archivos `.der`.

Banco de SIM: inventario de SIM distribuido

El **Banco de SIM** muestra cada SIM en cada lector de tarjeta inteligente a través de cada agente de OmniWeb. Cada agente escanea sus lectores locales de PC/SC, lee la identidad de cada SIM y reporta el inventario a central exactamente como ya reporta módems/teléfonos como dispositivos. Central agrega el inventario por agente y persiste una base de datos de SIMs indexada por ICCID, por lo que la vista de "qué SIMs están dónde" sobrevive a las desconexiones del lector y del agente.

Esta es la mitad del inventario de un banco de pruebas de SIM remota distribuida. La capa de emulación/banco de tarjetas de SIM remota te permite **conectar cualquier SIM a cualquier cardem a través de la red**. SIM Remota documenta esa capa por separado. Esta página cubre el descubrimiento y el inventario. Imágenes de SIM (Paquetes de Perfil SAIP) cubre cómo guardar, exportar y reutilizar el sistema de archivos de una tarjeta como un paquete de perfil portátil.

La página es **centrada en el lector**: una fila por cada ranura de lector físico, agrupada por agente. Se muestran ranuras vacías, ilegibles y en uso. El diseño del banco es la verdad, no solo las ranuras pobladas.

Cómo el agente lee una SIM

El escáner del agente refleja el escáner del módem: la enumeración es lenta, por lo que los resultados se almacenan en caché y se vuelven a escanear en un intervalo.

Para cada lector de PC/SC en el host:

1. **Enumerar** los lectores de PC/SC conectados al host.
2. **Sondear** cada lector con una conexión *exclusiva*.
   - Sin tarjeta → `present=false`.
   - La conexión genera una **violación de uso compartido** → el lector está ocupado por otro proceso (por ejemplo, un `bankd` de SIM remota o una sesión de emulación de tarjeta) → `present=true, in_use=true`, y **no se intenta leer**. Un lector ocupado nunca provoca un fallo en el escaneo.
   - Tarjeta presente y libre → leerla.
3. **Leer** la identidad de la SIM con un conjunto autónomo de APDUs en bruto:
   - Detección de SIM UICC vs clásica (seleccionar `3F00`; `6E00` → GSM clásico, por lo que usar `CLA=A0` y modo de selección clásica),
   - EF.ICCID (`2FE2`), EF.IMSI (`6F07`), EF.SPN (`6F46`),

- `EF.AD` (`6FAD`) para la longitud de MNC (para que MCC/MNC se dividan correctamente),
- un PIN predeterminado **seguro** (`0000`) VERIFICAR en una tarjeta bloqueada. Primero sondea el contador de reintentos (una VERIFICACIÓN vacía que no decrementa) y **se niega** si solo queda un reintento, por lo que **nunca** quema el último reintento ni toca el PUK (un banco de SIM no debe bloquear tarjetas),
- el ATR de la tarjeta.

Cada lector se convierte en un diccionario:

```
{
  "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…"
}
```

La lista se envía a central como un mensaje `sims` (junto con la lista de dispositivos) al registrarse y cada vez que cambia; un comando `simbank_rescan` fuerza un escaneo no almacenado en caché inmediato.

Capacidad de lectura de tarjetas

Un host lee SIMs a través de su pila de tarjetas inteligentes PC/SC. Donde se necesita una decodificación más profunda de la tarjeta, el agente utiliza una biblioteca de tarjeta inteligente opcional y licenciada por separado, mantenida aislada del resto del agente (no se fusiona en el propio código de OmniWeb). Un host **sin** la pila de tarjetas inteligentes aún ejecuta el agente correctamente y simplemente informa que no hay SIMs. El banco de SIM es una capacidad opcional por host, como los módems.

El lector de referencia es un SCM/Identiv SCR35xx. Se admiten múltiples lectores por host.

Flujo de inventario → central → UI

```
agente host                          central (proceso de rol
android)         navegador
──────────                          ──────────────────────────────
────────
simbank.list_sims()  ──sims──▶     android agent_socket
  (lectura de PC/SC)                       └─
registry.update_sims(agent_id, …)   GET /api/simbank/sims
                                      └─ simbank.record_sims(…)  ─▶
DB       GET /api/simbank/readers

POST /api/simbank/agents/<id>/rescan
                       ◀─simbank_rescan──  (fuerza un escaneo no
almacenado en caché)
```

- El agente marca **hacia afuera** a central a través del mismo WebSocket que usa para teléfonos (`/api/android/agent`). El inventario de SIM viaja por esa conexión. No hay nuevo transporte.
- Central mantiene la instantánea **en vivo** por agente de lectores en la memoria `android.Registry` (`update_sims` / `all_sims`), y refleja cada ICCID en la tabla persistente `simbank_sims` a través de `simbank.record_sims`.
- Debido a que esto depende del Registro de agente de un solo proceso, la API del banco de SIM se sirve **solo por el proceso de backend de rol de agente** (la misma restricción que los Dispositivos de Prueba).

API REST (`/api/simbank`, JWT, tipo de elemento RBAC `simbank`)

Método	Ruta	Propósito
GET	`/sims`	Cada SIM a través de todos los agentes (incl. solo persistidos fuera de línea), con presencia/en uso en vivo superpuestos.
GET	`/readers`	Cada lector de PC/SC en cada agente **conectado** (en vivo), incl. lectores vacíos y en uso.
GET	`/sims/<iccid>`	Una SIM.
PATCH	`/sims/<iccid>`	Editar campos asignados por el operador (notas hoy). Crea la fila si el ICCID no se ha visto.
DELETE	`/sims/<iccid>`	Olvidar una SIM (elimina el registro persistido; reaparece en el siguiente escaneo si sigue insertada).
POST	`/agents/<id>/rescan`	Forzar un escaneo PC/SC no almacenado en caché inmediato en un agente y devolver su inventario fresco.

RBAC refleja `ir38`/`android-control`: los administradores siempre pasan; de lo contrario, un permiso JWT con `element_type == "simbank"` otorga vista, y `POST` en sus métodos otorga control.

Frontend

`src/pages/simbank/SimBank.tsx`: una tabla filtrable y buscable de todas las SIMs: estado (presente / en uso / fuera de línea), agente/sitio, lector, ICCID, IMSI, MCC/MNC, país, SPN, notas editables, última vez visto. Botón de

Reescaneo por agente. Enrutado en `/simbank` y vinculado desde la barra lateral bajo **Pruebas de Roaming › Banco de SIM**.

Esquema de base de datos

`simbank_sims`: una fila por cada ICCID visto alguna vez:

Columna	Notas
`iccid` (PK)	Serial de SIM.
`imsi`, `mcc`, `mnc`, `country`, `spn`, `atr`	Última identidad conocida (solo sobrescrita por lecturas no vacías).
`notes`	Asignadas por el operador, editables.
`last_agent_id`, `last_site`, `last_reader_name`, `last_reader_index`	Dónde fue visto por última vez (o se encuentra actualmente).
`first_seen`, `last_seen`	Timestamps (UTC).
`remsim_bank_id`, `remsim_slot_nr`, `remsim_mapped_cardem`	**Reservado para la Fase 2** (nullable, no utilizado).

Los lectores vacíos y en uso no llevan **ningún** ICCID, por lo que no se persisten como SIMs. Solo aparecen en la instantánea en vivo `/readers`.

Futuro: SIM Remota

La fase 2 mapea un lector/SIM físico en un banco de SIM remota para que una SIM en un sitio pueda presentarse a un módem/teléfono en otro (SIM remota).

Los ganchos ya están en su lugar. Busca en el código `# TODO remsim`:

- `simbank_sims.remsim_bank_id` / `remsim_slot_nr` / `remsim_mapped_cardem` (columnas nullable, expuestas en `to_dict` y el tipo TS `SimRow` como `null`),
- la bandera `in_use` por lector del agente ya distingue un lector mantenido por una sesión de `bankd`/emulación. Ese es el lector que la fase 2 mapeará,
- `PATCH /api/simbank/sims/<iccid>` es donde se conectará la edición del mapeo de remsim.

Nada aquí impulsa remsim hoy; la forma está reservada para que el mapeo se inserte sin reestructurar la ruta caliente del inventario.

Editor de Sitios: Visor de Configuración del Sitio

El **Editor de Sitios** muestra el archivo de configuración en bruto para el sitio seleccionado actualmente: el archivo YAML de host/inventario que define las funciones de red, infraestructura y configuraciones de ese despliegue. Es una vista de solo lectura, con resaltado de sintaxis, por lo que puedes ver exactamente con qué está trabajando OmniWeb para un sitio sin abrir una terminal en un host.

← Guía de Operaciones

Lo que muestra

OmniWeb gestiona cada sitio a partir de un archivo de configuración por sitio. Ese archivo enumera los elementos del sitio (qué NFs están presentes y en qué direcciones), sus hosts de infraestructura, su rol de monitoreo, su bloque `fivegc` (ver 5G Core), y así sucesivamente: todo lo que la barra lateral, la topología, las páginas de elementos y los paneles derivan.

El Editor de Sitios carga ese archivo para el sitio elegido en el menú desplegable de la barra superior y lo muestra en un panel de editor completo (Monaco, el mismo editor que usa VS Code) con resaltado de YAML, números de línea, plegado y un minimapa. El encabezado muestra el cliente, el sitio y el nombre del archivo fuente.

Parse error on line 3: ... SE -->|/api/sites/{customer}/{site}/ra ----------
--^ Expecting 'SQE', 'DOUBLECIRCLEEND', 'PE', '-)', 'STADIUMEND', 'SUBROUTINEEND', 'PIPE', 'CYLINDEREND', 'DIAMOND_STOP', 'TAGEND', 'TRAPEND', 'INVTRAPEND', 'UNICODE_TEXT', 'TEXT', 'TAGSTART', got 'DIAMOND_START'

Intente de nuevo

Si no se selecciona ningún sitio, la página te pide que elijas uno del menú desplegable primero.

Solo lectura por diseño

El Editor de Sitios es un **visor**: el panel es de solo lectura (marcado con un chip de **solo lectura** en el encabezado). Está ahí para *inspeccionar* la configuración efectiva, no para cambiarla.

La configuración del sitio no se edita desde el navegador. Como se menciona a lo largo de esta guía, el despliegue y la configuración de OmniWeb se gestionan a través de **Ansible**. No edites archivos de configuración directamente en los hosts, y agregar o cambiar un elemento es un cambio de configuración realizado a través de ese pipeline (ver el modelo de configuración). El Editor de Sitios te permite leer el resultado de ese pipeline para el sitio seleccionado.

Cuándo usarlo

- **Confirmar con qué está configurado un sitio**: qué elementos, hosts y NFs de 5GC OmniWeb cree que están presentes, y en qué direcciones.
- **Solucionar problemas de la interfaz de usuario contra la configuración**: si falta un elemento, una entrada en la barra lateral o una sección de 5GC, el archivo en bruto es la fuente de verdad para verificar.
- **Referenciar el nombre de archivo exacto y su contenido** al preparar un cambio de Ansible.

Relacionado

- Arquitectura: el modelo de configuración: cómo la configuración del sitio impulsa OmniWeb y cómo se gestiona.
- 5G Core: el bloque `fivegc` de la configuración del sitio y lo que presenta.

- Topología de Red: las vistas de topología y lista de hosts construidas a partir de la misma configuración del sitio.

Puerta de Enlace SMPP

La **Puerta de Enlace SMPP** conecta pares SMPP externos con el núcleo de mensajería. Las aplicaciones externas y los socios de interconexión, los **ESMEs** (Entidades de Mensaje Corto Externas), se conectan a través de SMPP ya sea como clientes a los que la puerta de enlace llama o como servidores de los que la puerta de enlace acepta enlaces, y la puerta de enlace transporta sus mensajes cortos hacia y desde el SMSC. Cada conexión es un **enlace** SMPP (transceptor, transmisor o receptor). La puerta de enlace mantiene esos enlaces activos, los autentica y los supervisa, y transfiere el tráfico al núcleo de mensajería. OmniWeb muestra el estado de enlace en vivo, los pares de clientes y servidores configurados, y los registros de la puerta de enlace.

← Guía de Operaciones

La Puerta de Enlace SMPP es una página de elemento por instancia que se alcanza desde la barra lateral cuando se ejecuta en el inventario del sitio, con una vista de flota donde se despliegan varios. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API de la puerta de enlace, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Resumen

Una lectura de salud de pantalla única de las estadísticas de enlace agregadas: el **número total** de enlaces y el desglose de **conectados / desconectados** dividido entre enlaces de **cliente** (saliente) y **servidor** (entrante). Es la forma más rápida de confirmar que la puerta de enlace está activa y que sus pares están enlazados, y de detectar de un vistazo si alguna conexión esperada se ha caído.

Estado del Enlace

Cada enlace habilitado, cliente y servidor, con su **estado de conexión** actual, los **detalles de sesión** subyacentes y las **métricas** por enlace. Esta es la vista en vivo de quién está enlazado en este momento. Desde aquí, un operador puede actuar sobre un enlace:

- **Eliminar** un enlace activo. Para un enlace de cliente, esto termina la conexión saliente. Para un enlace de servidor, desconecta todas las conexiones de cliente activas. Úselo para despejar una conexión atascada o que no funciona correctamente.
- **Reconectar** un enlace de cliente. Esto obliga a un enlace de cliente (saliente) a volver a marcar su host remoto, que es la forma más rápida de recuperar un par saliente después de un pequeño problema de red.

Pares de Cliente

Las conexiones SMPP **cliente** salientes configuradas son los pares a los que la puerta de enlace llama. Cada uno muestra su **nombre**, el **host** y **puerto** remotos, el **ID del sistema** con el que se enlaza, y el **tipo de enlace** (transceptor, transmisor o receptor). Los pares de cliente son completamente editables aquí: un operador puede **agregar** un par, **editar** uno existente (host, puerto, credenciales, tipo de enlace, intervalo de consulta, límite de TPS y otros parámetros de enlace), y **eliminar** uno que ya no se necesita. Habilitar un par pone su enlace saliente en servicio. Deshabilitarlo retira al par sin descartar su configuración.

Pares de Servidor

Las autorizaciones SMPP **servidor** entrantes configuradas son las credenciales y reglas para los pares que se enlazan *dentro* de la puerta de enlace. Cada entrada define un **ID del sistema** y contraseña, los **tipos de enlace permitidos**, y las medidas de seguridad que supervisan un enlace entrante: una **lista blanca de IP** de direcciones de origen permitidas y una **lista blanca de direcciones de origen** de patrones de direcciones de origen permitidos, además de un **límite de TPS**. Los pares de servidor son editables aquí de la misma manera (**agregar**, **editar** y **eliminar**), por lo que un operador puede incorporar un nuevo socio entrante, ajustar sus listas blancas, o revocarlo. Habilitar y deshabilitar una autorización controla si ese socio puede enlazarse.

Registros

La pestaña **Registros** muestra la salida de registro en vivo de la puerta de enlace para solucionar problemas de una sola puerta de enlace (fallos de enlace, rechazos de autenticación y conexiones caídas) sin salir de OmniWeb.

Monitoreo

Las tasas de mensajes, el rendimiento y otras series temporales para la Puerta de Enlace SMPP se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- El **SMSC** es el núcleo de mensajería al que la puerta de enlace entrega mensajes cortos.
- El **IP-SM-GW** transporta SMS sobre IMS para dispositivos VoLTE y complementa el camino SMPP hacia pares externos.

SMSC: Centro de Servicio de Mensajes Cortos

El **SMSC** (Centro de Servicio de Mensajes Cortos) es el corazón de almacenamiento y reenvío de SMS en el núcleo. **Acepta** mensajes de la red (a través de SS7 (MAP) desde el lado móvil, a través de Diameter y a través de SMPP desde las interfaces de aplicación). Luego **rutea**, **traduce** y **entrega** los mensajes. Retiene cualquier mensaje que no puede entregar de inmediato y vuelve a intentar hasta que el mensaje sea entregado, expire o sea descartado. A lo largo del camino, rastrea el estado de entrega de cada mensaje, traduce los números de llamada y llamados, se federan con SMSCs pares para que un mensaje pueda ser entregado al nodo que pueda alcanzar al destinatario, y gestiona campañas de SMS en **masa**. OmniWeb presenta todo esto desde una única página por instancia: estado de mensajes en vivo, ubicaciones de suscriptores, registros de front-end, salud de Diameter y federación, conjuntos de reglas de enrutamiento y traducción, y gestión de campañas.

← Guía de Operaciones

El SMSC es una página de elemento por instancia que se alcanza desde la barra lateral cuando se ejecuta en el inventario del sitio, con una vista de flota donde se despliegan varios. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del SMSC, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Visión general

La pestaña de aterrizaje es una lectura de salud de pantalla única para el nodo: conteos de mensajes actuales y estado de entrega, salud de front-end y pares de un vistazo, y una **búsqueda por MSISDN** que busca tanto en mensajes almacenados como en ubicaciones de suscriptores. Es la forma más rápida de responder "¿qué está sucediendo con el SMS de este suscriptor en este momento?" desde una sola caja.

Mensajes

Cada mensaje que el SMSC está reteniendo o ha procesado, cada fila muestra los números de envío y recepción, el **estado** del mensaje (pendiente, entregado, fallido, expirado, descartado o auto-respondido), el número de **intentos de entrega**, y su antigüedad. Puedes filtrar mensajes por estado, por **SMSC**, e incluir tráfico **de cartas muertas** o **no enrutado**, y buscar por MSISDN, nombre de nodo o ID de mensaje. Selecciona un mensaje para abrir su detalle, incluyendo el texto plano decodificado. Un operador puede **reencaminar** un mensaje para forzarlo a pasar nuevamente por el enrutamiento, por ejemplo, después de corregir una regla de enrutamiento.

Frontends

Los **front-ends** de aplicación y SMPP actualmente registrados con el SMSC son los clientes que envían y reciben mensajes. Cada entrada muestra su nombre de host, cuándo fue **última vez visto**, y cuándo **expira** su registro, para que puedas confirmar que los front-ends de manejo de mensajes están conectados y sus registros están activos.

Ubicaciones

Las **ubicaciones de suscriptores** que el SMSC ha aprendido son la última ubicación de servicio conocida para cada suscriptor por **IMSI** y **MSISDN**. El SMSC utiliza esta información para alcanzar a un destinatario. Puedes buscarlo por IMSI o MSISDN y filtrarlo para incluir entradas expiradas. Es donde confirmas que el SMSC sabe dónde está un suscriptor antes de poder entregarle.

Diameter

Las conexiones de pares de Diameter que el SMSC utiliza para mensajería, cada fila muestra el **dominio** del par, **dirección IP**, **transporte**, dirección de iniciación de conexión, **nombre del producto** reportado, **IDs de aplicación** negociados y **estado de conexión**. Aquí es donde confirmas que la ruta de Diameter de la que depende el SMSC está activa.

Federación

La vista de **federación** muestra cómo este SMSC coopera con SMSCs pares para que un mensaje pueda ser entregado al nodo que pueda alcanzar al destinatario. Informa sobre **este nodo**, el conteo de pares **saludables**, **degradados** y **no saludables**, el número de **mensajes federados en caché** (destacados cuando no son cero), el método de **descubrimiento** en uso (dominio DNS o pares estáticos), y una tabla por par de nombre de nodo, estado, fallos recientes, última verificación de salud exitosa y los front-ends que cada par ofrece. Es la forma más rápida de ver si los SMSCs en una federación se alcanzan entre sí.

Enrutamiento

Las **reglas de enrutamiento de SMS** que deciden a dónde va cada mensaje, listadas por **prioridad**. Cada regla coincide con un patrón de número **llamante** y **llamado** (y opcionalmente un SMSC de origen o tipo de origen como SS7 o conmutación de circuitos), y se resuelve a un **destino** (un SMSC objetivo o una búsqueda **ENUM**) con una descripción y un estado habilitado. Las reglas son completamente editables: un operador puede agregar, editar, habilitar, deshabilitar o eliminar, y exportar e importar nuevamente el conjunto de reglas.

Traducciones

Las **reglas de traducción de números** que reescriben los números de llamada y llamados a medida que los mensajes pasan: normalizan formatos, aplican prefijos y similares. Cada regla está listada por **prioridad** con su coincidencia de llamada y llamada, SMSC de origen opcional, una bandera de **continuar** (para que varias reglas puedan aplicarse en secuencia), una descripción y un estado habilitado. Al igual que con el enrutamiento, las reglas son editables (agregar, editar, habilitar, deshabilitar, eliminar), y puedes exportarlas e importarlas nuevamente.

Campañas

Las **campañas** de SMS en masa se crean y gestionan desde esta pestaña. Una **Nueva Campaña** se define con un nombre y descripción, un número de **remitente**, el SMSC de origen, una **lista de destinatarios**, una **audiencia** (solo destinatarios activos o todos en la lista), una tasa de **goteo** en mensajes por segundo, una ventana de **validez** del mensaje, un tiempo **de entrega posterior** opcional y la **plantilla de mensaje**. Una vez creada, una campaña se controla desde aquí (**iniciar**, **pausar**, **reanudar** o **cancelar**). Puedes inspeccionar sus **objetivos** para ver el estado de envío y entrega por destinatario a medida que avanza la campaña.

Listas de Campañas

Las **listas** de destinatarios a las que las campañas envían. Las listas se gestionan completamente aquí: crea una **Nueva Lista de Destinatarios** con un nombre, descripción y un conjunto inicial de destinatarios, **agrega** más destinatarios más tarde, edita o elimina una lista. Proporcionas destinatarios como **CSV**, por lo que puedes importar una lista de contactos existente directamente en lugar de ingresarla manualmente.

Prueba NAPTR

La pestaña de **Prueba NAPTR** es una herramienta para operadores que resuelve un **número E.164 (o dominio) a través de ENUM/NAPTR DNS** para ver cómo el SMSC enrutará un mensaje hacia él. Ingresa el número de teléfono y el **dominio ENUM** a consultar (`e164.arpa` por defecto) y envía. No se recupera nada hasta que lo hagas. El SMSC invierte los dígitos del número en la zona ENUM, busca los registros **NAPTR** publicados allí, y los devuelve en **orden** y **preferencia**. Cada registro lleva sus **banderas**, **servicio**, el **regexp** de reescritura y **reemplazo**, y el **dominio de resultado** resuelto al que el registro apunta el mensaje. Es donde confirmas que los datos ENUM detrás de una regla de enrutamiento realmente resuelven un número al URI o ruta que esperas, antes de confiar en ello en producción.

MWI

La pestaña de **MWI** envía una actualización de **Indicación de Mensaje en Espera** para un suscriptor: la notificación que establece o borra la bandera de "mensajes en espera" en un dispositivo, típicamente después de que se deja o se recoge un correo de voz. Proporciona el **MSISDN de destino** a notificar y el **MSISDN de origen** de donde proviene, selecciona el **tipo de indicación** (correo de voz, fax, correo electrónico u otro), y establece si el indicador debe estar **activo** (encendido) o borrado (apagado), con un **cuerpo de mensaje** opcional y el **SMSC** de origen. Es un formulario de envío: la actualización solo se envía cuando lo publicas. Esta es la forma directa de activar o borrar el indicador de mensaje en espera de un suscriptor manualmente.

Registros del Sistema

La pestaña de **Registros del Sistema** es la propia vista de registro respaldada por API del SMSC. Puedes filtrarla por **nivel** (depuración, información, advertencia, error) y por un **límite** en el número de líneas devueltas, para que puedas obtener solo los errores recientes o un rastro más completo cuando investigas un problema específico, sin salir de OmniWeb.

Más herramientas

Junto a las pestañas anteriores, la página del SMSC ofrece algunas herramientas enfocadas:

- **Enviar**: un formulario que envía un SMS único directamente desde OmniWeb (de, a y texto del mensaje), para probar la entrega a un destinatario específico.
- **Operaciones**: acciones de mantenimiento a nivel de nodo, incluyendo limpiar los **front-ends** registrados, **mensajes** almacenados, reglas de **enrutamiento** y reglas de **traducción**. Cada una es una acción destructiva y solicita confirmación primero.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo del SMSC para solucionar problemas de un solo nodo sin salir de OmniWeb. Para una vista filtrada, respaldada por API del mismo nodo, utiliza **Registros del Sistema** arriba.

Monitoreo

El rendimiento de mensajes, tasas de éxito de entrega, profundidad de cola y otras series temporales para el SMSC se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- **HSS**: contiene los datos de suscriptores e información de enrutamiento contra la que se resuelven las entregas del SMSC.
- El **DRA**: retransmite la señalización de Diameter que el SMSC utiliza para mensajería.
- **STP**: la ruta de señalización SS7 a través de la cual el SMSC intercambia mensajes MAP con la red móvil.
- El **CSCF/TAS**: el lado de IMS que origina y termina la mensajería para suscriptores de VoLTE.

Gestión de Software y Ciclo de Vida

OmniWeb proporciona un solo lugar para ver y gestionar el software que se ejecuta en toda la flota: versiones de paquetes, actualizaciones disponibles y licencias. El ciclo de vida del software de la red es visible desde el mismo portal utilizado para operarlo.

← Volver a la Guía de Operaciones

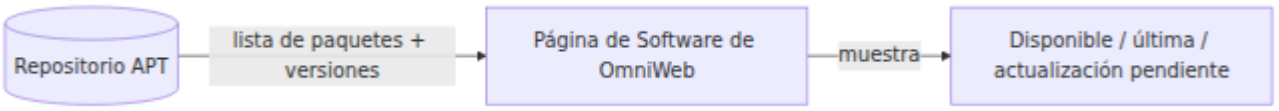
Página de Software (Repositorio APT)

La página de **Software** es un navegador de repositorios APT para paquetes de Omnitouch. Se conecta al servidor de repositorio APT configurado y muestra, para los paquetes que gestiona:

- **Paquetes disponibles** en el repositorio.
- **Versiones** ofrecidas, incluyendo la última disponible.
- **Estado de actualización**: si existe una versión más nueva que la que está desplegada.

Esto permite a los operadores ver de un vistazo qué componentes de Omnitouch tienen actualizaciones pendientes y qué versiones son actuales, proporcionando el lado de inventario del ciclo de vida del software. La instalación/actualización de paquetes en los hosts se realiza a través de las herramientas estándar APT/`dpkg` (y generalmente se automatiza a través de Ansible); OmniWeb proporciona la capa de visibilidad sobre lo que está publicado y es actual.

La página de Software: cada paquete de Omnitouch con sus últimas versiones de repositorio y caché y un indicador de sincronización que señala dónde se ha publicado una versión más nueva que la que está en caché/desplegada (aquí `omni-upf` y `omni-msc` están fuera de sincronización).



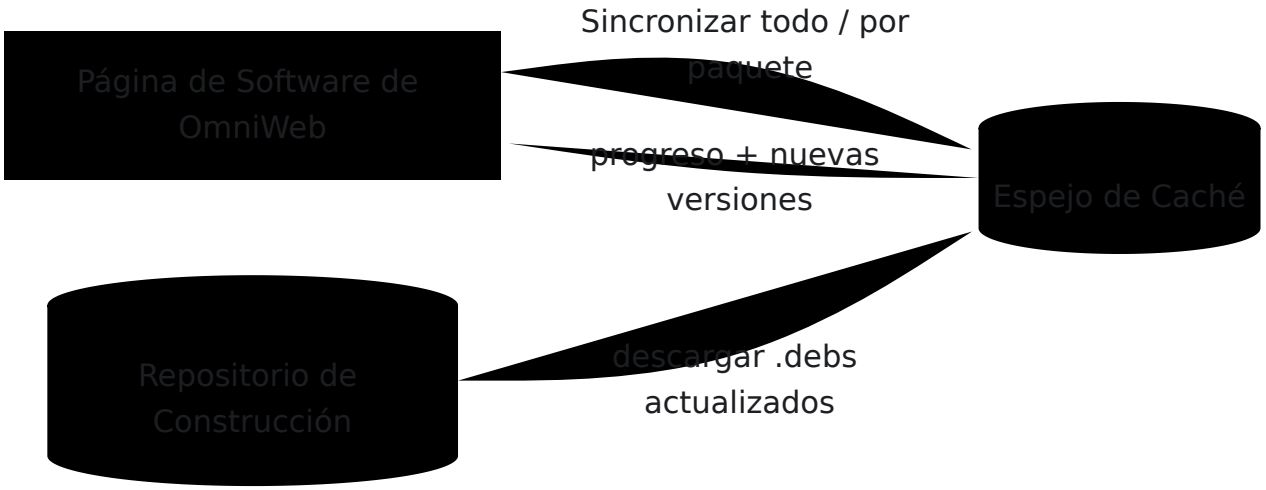
Sincronizando Paquetes en la Caché

Las implementaciones que ejecutan un **espejo de caché APT** en el sitio (para sitios sin conexión o con ancho de banda limitado) mantienen una copia local de los paquetes publicados en el repositorio de construcción. Con el tiempo, la caché se queda atrás. La página de Software marca cada paquete que está **fuera de sincronización** (se ha publicado una versión más nueva que la que está en caché). Desde la misma página puedes extraer esas actualizaciones en la caché sin salir de OmniWeb:

- **Sincronizar todo**: extraer todos los paquetes actualizados del repositorio a la caché.
- **Sincronizar** (por fila): extraer solo un paquete. Haz clic en varios y se **enfilan**: se descargan uno tras otro, y OmniWeb regenera el índice de paquetes **una vez** al final (no por paquete), por lo que la caché nunca queda medio actualizada.

Mientras se realiza una sincronización, la página muestra el progreso en vivo (qué paquete se está descargando, cuántos están en cola y un registro de progreso en tiempo real). Actualiza la comparación de versiones cuando termina.

Una sincronización en progreso: `omni-msc` descargando con `omni-upf` en cola, el banner de fase y el registro en vivo. Cuando la cola se vacía, el índice de caché se regenera una vez y el estado de sincronización se actualiza.



La sincronización se ejecuta en el propio espejo de caché (OmniWeb la activa y transmite el progreso); el espejo extrae los `.deb` actualizados del repositorio de construcción y regenera su índice. Los hosts en el sitio luego instalan los paquetes actualizados desde la caché como de costumbre.

Versionado

OmniWeb informa su propia versión de construcción (versión, commit y fecha de construcción) para que los operadores puedan confirmar exactamente qué versión del portal están ejecutando. Este es el punto de referencia al informar problemas o coordinar una actualización del propio portal.

Gestión de Licencias

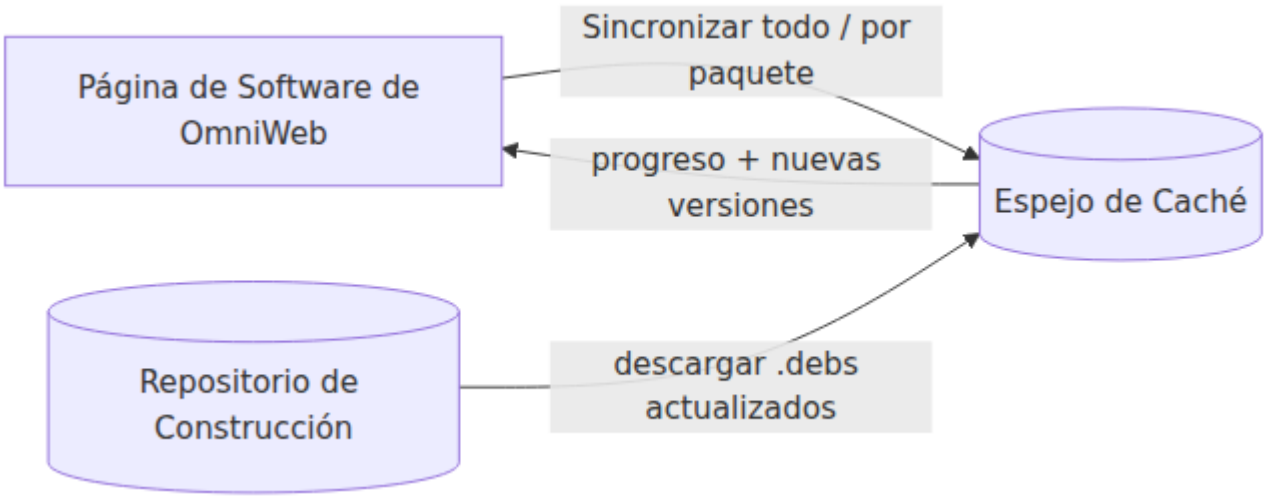
El **Servidor de Licencias** se administra a través de OmniWeb como cualquier otro elemento, utilizando los mismos patrones genéricos (ver Operaciones Comunes). Muestra:

Resumen del Servidor de Licencias: estado actual de la licencia y validez, incluyendo el estado de tiempo de confianza.

Vista	Descripción
Resumen	Estado actual de la licencia, fechas de validez y derechos de características.
Registros de Solicitudes	Solicitudes de licencia históricas, con filtrado. Esto es útil para auditar qué se verificó y cuándo.
Consulta	Consultar el estado de la licencia para un licenciatario/producto específico bajo demanda.

La concesión de licencias se integra en el ciclo de vida del software: los derechos determinan qué productos y características está autorizado a ejecutar una implementación, y los registros de solicitudes proporcionan un rastro de auditoría de la actividad de licencias a lo largo del tiempo.

Ciclo de Vida a Primera Vista



1. **Ver qué está disponible**: la página de Software muestra actualizaciones pendientes.
2. **Confirmar derechos**: el Servidor de Licencias muestra para qué está licenciada la implementación.
3. **Aplicar**: las actualizaciones se ejecutan a través de APT/Ansible en los hosts.
4. **Verificar**: confirmar versiones, luego observar los Registros y Tableros de elementos para confirmar un resultado saludable.

SS7: Pila de Señalización (STP / HLR / IP-SM-GW / CAMEL-GW)

La **pila SS7** (OmniSS7) termina el transporte SIGTRAN (asociaciones SCTP que llevan **M3UA**) y enruta el tráfico SS7/MAP a través de la red de señalización. Un único servicio proporciona toda la pila, y OmniWeb la presenta como cuatro vistas de elementos para sus diferentes roles: **STP** (Punto de Transferencia de Señales, el enrutador SS7), **HLR** (Registro de Ubicación del Hogar), **IP-SM-GW** (Puerta de Enlace de Mensajes Cortos IP) y **CAMEL-GW** (Puerta de Enlace CAMEL). Los cuatro están respaldados por el mismo cliente compartido, por lo que el transporte y enrutamiento SIGTRAN que comparten es la misma pila subyacente vista desde diferentes ángulos.

← Guía de Operaciones

Cada vista es una página de elemento por instancia que se alcanza desde la barra lateral cuando una pila SS7 se ejecuta en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API de la pila, por lo que permanece detrás de la única puerta de enlace autenticada. Las respuestas regresan en un sobre `{status, response}`. El enlace de documentación en el encabezado de cada página de elemento (el botón de ayuda contextual) abre esta página. Cada vista está organizada en pestañas. Las tasas de mensajes y otras series temporales se presentan como paneles de Grafana que se alcanzan desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

La pila de un vistazo

El transporte SIGTRAN debajo de cada rol es el mismo, por lo que las pestañas de **Pares** y **Conexiones SCTP** aparecen en las cuatro vistas y leen los mismos

datos.

La pestaña de **Pares** informa el estado de los pares M3UA (`/api/m3ua-status`): cada par M3UA/M2PA, con su **estado de ASP**, **estado de asociación**, **puntos finales** locales y remotos, **contexto de enrutamiento**, protocolo y modo, y estadísticas de **tiempo de actividad** por par. Aquí es donde confirmas que el proceso del servidor de aplicaciones de cada vecino de señalización está activo y en servicio.

La pestaña de **Conexiones SCTP** lista el transporte subyacente (`/api/sctp-connections`): cada asociación SCTP con su **estado**, **rol**, **IP/puerto** locales y remotos, conteos de **flujos** entrantes y salientes, **bytes** y **mensajes** enviados y recibidos, **última actividad**, y cualquier último error, además de totales agregados a través de todas las conexiones. Cuando un par muestra estar inactivo, verifica esta capa para ver si la asociación SCTP en sí está establecida.

STP: enrutamiento

La vista de **STP** es el enrutador SS7. Junto a las pestañas de transporte compartido, lleva la pestaña de **Enrutamiento**, además de **Mapa de Red**, **Resumen** y un feed de **Eventos SS7**.

La pestaña de **Enrutamiento** muestra la configuración completa de enrutamiento M3UA (`/api/routing`): los **pares** configurados, las **rutas de código de punto (PC)** y las **rutas de título global (GT)**.

- Las **rutas de código de punto** dirigen el tráfico a un código de punto de destino (`dest_pc`) a través de un **par** objetivo, con un **indicador de red**, **máscara** de código de punto y **prioridad**. Los operadores pueden **agregar** una ruta PC (`POST /api/routing/pc-routes`, proporcionando el código de punto de destino y el par objetivo) y **eliminar** una (`DELETE /api/routing/pc-routes/{dest_pc}-{peer_id}`).
- Las **rutas de título global** coinciden con un **prefijo** GT y reenvían a un **par** objetivo con una **prioridad** y detalles opcionales de SSN, tipo de traducción y naturaleza de la dirección, además de una descripción. Los operadores pueden **agregar** una ruta GT (`POST /api/routing/gt-routes`, proporcionando el prefijo y el par objetivo) y **eliminar** una (`DELETE /api/routing/gt-routes/{prefix}:{peer_id}`).

Aquí es donde confirmas y ajustas cómo el STP reenvía los mensajes SS7 hacia cada destino.

HLR

La vista de **HLR** muestra los suscriptores activos del registro y el enlace al backend de HLR, junto a las pestañas de transporte compartido, un **Resumen** y una pestaña de **Cliente SS7**.

La pestaña de **Suscriptores** lista el registro de suscriptores activos (`/api/subscribers`): cada suscriptor que ha enviado un **UpdateLocation** y aún no un **CancelLocation**, cada fila muestra **IMSI**, **VLR**, **MSC** que sirve, tiempo de registro y **duración**, con conteos de VLRs y MSCs únicos. Un operador puede **eliminar** todos los suscriptores activos rastreados (`DELETE /api/subscribers`) para restablecer la vista del registro.

La pestaña de **Enlaces HLR** verifica la conectividad a la API de HLR configurada (`/api/hlr-links`): el **estado** (activo, degradado o inactivo), **latencia** medida, **versión** reportada y el **host** objetivo. Es la forma más rápida de confirmar que la pila puede alcanzar el backend de HLR.

IP-SM-GW

La vista de **IP-SM-GW** es la puerta de enlace de mensajes cortos. Lleva el rastreador de suscriptores SMSc y el enlace al backend de SMSc, junto a las pestañas de transporte compartido y un **Resumen**.

La pestaña de **Enlaces SMSc** verifica la conectividad a la API de SMSc configurada (`/api/smsc-links`): **estado** (activo, degradado o inactivo), **latencia**, **versión** reportada y **host** objetivo. Es el equivalente en el camino SMS de la verificaci��n de enlace HLR.

La pestaña de **Suscriptores SMSc** lista los suscriptores rastreados por el rastreador de suscriptores SMSc (`/api/smsc-subscribers`): cada uno con **MSISDN**, **IMSI**, **GT HLR** y **GT VLR**, **mensajes enviados** y **recibidos**, estado y última actualización, además de conteos de activos/fallidos y HLR únicos. Un operador puede **eliminar** todos los suscriptores SMSc rastreados (`DELETE /api/smsc-subscribers`).

CAMEL-GW

La vista de **CAMEL-GW** muestra las sesiones CAMEL que la puerta de enlace está ejecutando, junto a las pestañas de transporte compartido y un **Resumen**.

La pestaña de **Sesiones CAMEL** lista todas las sesiones CAMEL activas gestionadas por la puerta de enlace (`/api/camel-sessions`): el **estado** de cada sesión, **versión CAP**, **clave de servicio**, **IMSI**, números **llamantes** y **llamados**, hora de inicio y **duración**, con conteos de sesiones iniciadas y respondidas. Aquí es donde observas el manejo de llamadas CAMEL en vivo en tiempo real.

Estado

El endpoint de **Estado** (`/api/status`) informa la salud general del nodo que los **Resumenes** resumen: la identidad del nodo y **rol**, si el servicio está **ok**, su **tiempo de actividad**, y un resumen de pares de cuántos pares de señalización están activos del total. Esta es la primera lectura para confirmar que la pila está funcionando y sus pares están en servicio.

Relacionados

- **STP**: el elemento de enrutamiento SS7 (rutas de código de punto y rutas de título global).
- **HLR**: el elemento del Registro de Ubicación del Hogar (registro de suscriptores activos y enlace HLR).
- **IP-SM-GW**: el elemento de la Puerta de Enlace de Mensajes Cortos IP (suscriptores SMSc y enlace).
- **CAMEL-GW**: el elemento de la Puerta de Enlace CAMEL (sesiones CAMEL en vivo).
- El **MSC/VLR** genera el UpdateLocation y la señalización CAMEL que esta pila enruta y rastrea.
- El **SMSc** es el backend contra el que se resuelven el enlace y el rastreador de suscriptores SMSc de la IP-SM-GW.
- ← Guía de Operaciones

Cliente de SIM Toolkit (STK)

OmniWeb incluye un cliente interactivo de **SIM Toolkit**. Úsalo para navegar y controlar applets de STK en cualquier tarjeta SIM física insertada en el lector PC/SC de un agente conectado. El cliente de STK envía un perfil de terminal a la tarjeta, luego presenta cada comando proactivo como una pantalla interactiva. Respondes como lo haría un terminal, por lo que el applet avanza a su siguiente paso.

Esta herramienta se encuentra en la barra lateral bajo **SIMs - SIM Toolkit**, junto al Terminal APDU y Explorador de Sistema de Archivos SIM.

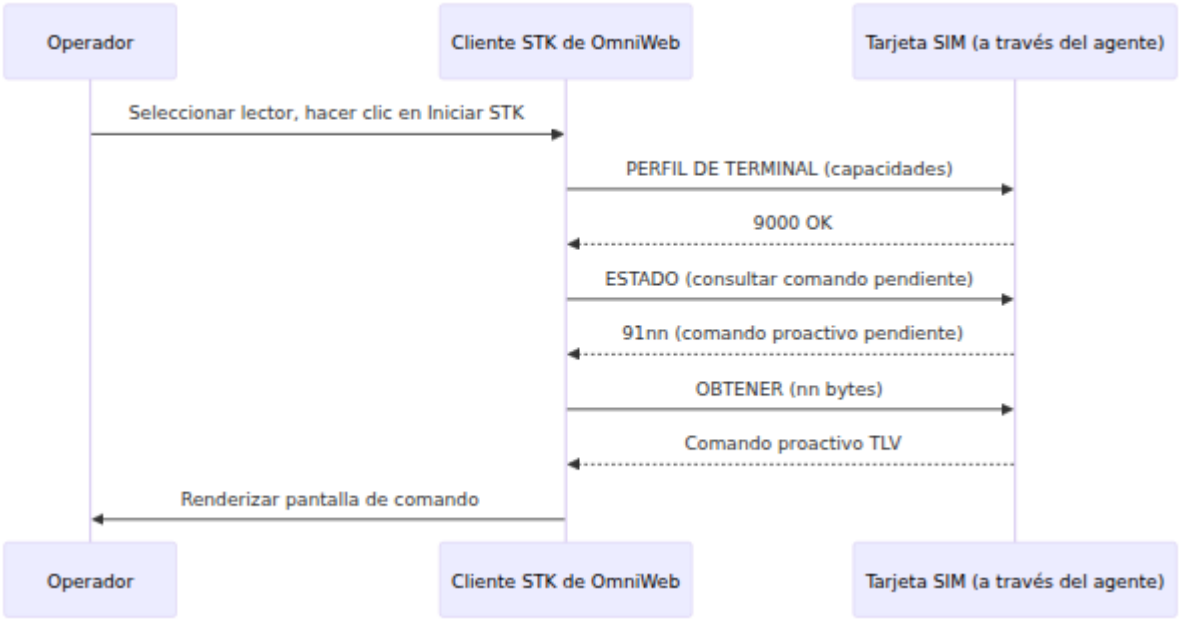
¿Qué es SIM Toolkit?

El SIM Application Toolkit (STK) es un estándar definido en ETSI TS 102.223 que permite a una tarjeta SIM iniciar acciones en el terminal. Un applet de SIM emite **comandos proactivos** - solicitudes como "muestra este texto" o "muestra este menú" - y el terminal responde con la selección o entrada del usuario. Los casos de uso comunes incluyen menús de recarga de operador, consultas de saldo, disparadores de configuración OTA y portales de servicio residentes en la SIM.

Requisitos

- Un lector con una tarjeta SIM que contenga un applet de STK.
- El permiso de **control del banco de SIM**. Sin él, puedes ver lectores pero no puedes abrir sesiones ni controlar tarjetas.
- El lector no debe estar ocupado por otra herramienta. Si lo está, OmniWeb muestra quién lo tiene y ofrece una opción de **Tomar control**. Tomar control cancela la otra sesión.

Abrir una Sesión



1. Selecciona el lector del menú desplegable **Lector**. Solo aparecen los lectores con una tarjeta presente.
2. Haz clic en **Iniciar STK**. OmniWeb abre una sesión exclusiva en la tarjeta, envía un perfil de terminal y consulta el primer comando proactivo.
3. Interactúa con cada pantalla a medida que aparece. OmniWeb envía una RESPUESTA DE TERMINAL después de cada paso y obtiene automáticamente el siguiente comando.
4. La sesión termina cuando la tarjeta emite un comando de FIN DE SESIÓN, o cuando haces clic en **Finalizar sesión**.

Pantallas de Comando

OmniWeb renderiza cada comando proactivo como una pantalla interactiva. La tabla a continuación enumera los tipos de comando soportados.

Comando	Descripción	Acción del usuario
MOSTRAR TEXTO	La tarjeta muestra un mensaje.	Haz clic en **OK** para reconocer, o **Atrás** para volver al paso anterior.
SELECCIONAR ELEMENTO / CONFIGURAR MENÚ	La tarjeta presenta una lista numerada de opciones.	Haz clic en el elemento que deseas seleccionar.
OBTENER TECLA	La tarjeta solicita una única pulsación de tecla.	Escribe un carácter y haz clic en **Enviar**, o elige **Sí** / **No** para indicaciones de sí-no.
OBTENER ENTRADA	La tarjeta solicita una cadena de texto de una longitud especificada.	Escribe el texto y haz clic en **Enviar**. El campo muestra el conteo mínimo y máximo de caracteres.

Si la tarjeta emite un tipo de comando que el cliente no renderiza de forma interactiva (por ejemplo, ENVIAR MENSAJE CORTO o CONFIGURAR LLAMADA), OmniWeb muestra los datos del comando en bruto y envía automáticamente una respuesta de **OK** para que la sesión pueda continuar.

Historial de Sesiones

Un panel de **Historial de sesión** aparece en el lado derecho de la pantalla una vez que comienzas a interactuar. Registra cada tipo de comando y la respuesta que diste (elemento seleccionado, texto de entrada, o OK/Atrás). Úsalo para retroceder por el camino a través de un árbol de menú.

Finalizando una Sesión

La sesión termina de una de tres maneras:

- **Fin iniciado por la tarjeta**: el applet emite un comando proactivo de FIN DE SESIÓN. OmniWeb cierra la sesión automáticamente y muestra un mensaje de finalización.
- **Fin iniciado por el operador**: haz clic en **Finalizar sesión** en cualquier momento. OmniWeb envía un resultado de sesión terminada a la tarjeta y cierra la sesión del lector.
- **Navegación hacia atrás más allá de la raíz**: hacer clic en **Atrás** en la primera pantalla envía un resultado de movimiento hacia atrás a la tarjeta. La tarjeta decide cómo responder: puede mostrar una pantalla anterior o finalizar la sesión.

Después de que la sesión termina, el lector se vuelve a poner a disposición para otras herramientas.

Relación con Otras Herramientas SIM

Herramienta	Propósito
SIM Toolkit (esta página)	Controlar applets de STK de forma interactiva.
Terminal APDU	Enviar APDUs en bruto manualmente, uno a la vez o en una sesión persistente.
Explorador de Sistema de Archivos SIM	Navegar y editar el sistema de archivos de la tarjeta.
Registro APDU	Rastrear pasivamente comandos entre un módem y una SIM remota.

Solución de Problemas

Fallo en Iniciar STK con "TERMINAL PROFILE failed"

La tarjeta rechazó el perfil de terminal o el agente no pudo alcanzar la tarjeta. Verifica que:

- La tarjeta esté correctamente colocada en el lector.
- Ninguna otra herramienta esté ocupando el lector. Si lo está, usa **Tomar control**.
- El agente que posee el lector esté en línea (verifica la página del Banco de SIM).

La sesión se detiene después del primer comando

Algunos applets de SIM finalizan la sesión inmediatamente si el perfil de terminal no declara las capacidades que el applet necesita. El cliente declara un conjunto amplio de capacidades, pero algunas tarjetas verifican bits específicos. Si esto sucede, utiliza el Terminal APDU en modo de sesión para enviar PERFIL DE TERMINAL y OBTENER manualmente y examinar los datos del comando proactivo en bruto.

Atrás devuelve una pantalla inesperada

La acción de **Atrás** envía el código de resultado 0x11 (movimiento hacia atrás) a la tarjeta. La tarjeta controla lo que esto significa. Algunos applets regresan al menú anterior; otros reinician la sesión desde el menú raíz; unos pocos ignoran el movimiento hacia atrás y reemiten el mismo comando.

OBTENER ENTRADA rechaza mi texto

La tarjeta establece un conteo mínimo y máximo de caracteres. El campo de entrada muestra ambos. Si la tarjeta también restringe solo a dígitos, la

etiqueta del campo dice **solo dígitos**. Ingresa un valor dentro del rango requerido.

TAS: Servidor de Aplicaciones de Telefonía

El **TAS** (Servidor de Aplicaciones de Telefonía) es el servidor de aplicaciones IMS que proporciona la experiencia telefónica del suscriptor. Maneja el **control de llamadas** y los **servicios suplementarios** (desvío de llamadas, bloqueo, espera, retención y el resto), ejecuta **conferencias**, toma y reproduce **correo de voz**, registra **CDRs** para cada llamada, resuelve **enrutamiento** y traducción de números, y se comunica con el **OCS** a través de Diameter para que las llamadas se cobren en tiempo real. Donde el CSCF decide *cómo* se señaliza una llamada, el TAS decide *qué* hace el servicio. OmniWeb presenta sus llamadas en vivo, registros de suscriptores, puertas de enlace, pares de Diameter y configuración en una página de elemento. Los gráficos de volumen de llamadas y tendencias se encuentran en los paneles de Grafana accesibles desde la misma página.

← Guía de Operaciones

El TAS es una página de elemento por instancia que se accede desde la barra lateral cuando se está en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del TAS, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda en contexto) abre esta página. Está organizada en pestañas.

Resumen

La pestaña de inicio es una lectura de salud de pantalla única para el servidor de aplicaciones: el número de **llamadas activas**, **suscriptores registrados**, conferencias **en curso** y registros de **correo de voz** almacenados, la salud de los pares de **Diameter** y **puertas de enlace SIP**, y el estado de la **licencia**. Es la forma más rápida de confirmar que el TAS está operativo y manejando tráfico.

Llamadas Activas

Cada llamada actualmente en progreso, cada fila muestra las partes que llaman y son llamadas, la **dirección**, el **estado** de la llamada y su **duración**. Selecciona una llamada para abrir sus detalles y ver cómo se ha establecido una llamada específica y dónde se encuentra en el plan de marcado. Es el primer lugar para mirar cuando un suscriptor informa de una llamada con problemas en este momento.

CDR

Los **registros de detalles de llamadas** que el TAS ha escrito: una fila por llamada completada, con las partes, **hora de inicio**, **duración** y **disposición**. Abre cualquier registro para ver sus detalles completos. Los CDR son la contabilidad y la pista de resolución de problemas posterior al hecho: úsalos para confirmar que una llamada ocurrió, cuánto tiempo duró y cómo terminó.

Suscriptores

Los **registros** de suscriptores que el TAS conoce, cada uno con la **identidad** del suscriptor, el **estado** de registro y el **contacto** actual. Abre un suscriptor para ver los detalles completos del registro. Aquí es donde confirmas que un suscriptor está registrado en el servidor de aplicaciones antes de investigar por qué un servicio no está funcionando para ellos.

Diameter

Los **pares de Diameter** a los que se conecta el TAS, incluyendo la ruta al **OCS** para el cobro y el **HSS** para los datos del usuario, con el nombre de host de cada par y el **estado de conexión**. Abre un par para ver sus detalles. Cuando el cobro o las búsquedas de suscriptores fallan, esta pestaña es donde confirmas que las rutas subyacentes de Diameter están operativas.

Puertas de Enlace

Las **puertas de enlace SIP** que el TAS utiliza para alcanzar otras redes y troncos, cada una mostrando su nombre y **estado** actual. Abre una puerta de enlace para ver sus detalles. Usa esta pestaña para confirmar que las puertas de enlace de interconexión están registradas y disponibles antes de diagnosticar llamadas fallidas fuera de la red.

Conferencias

Las **conferencias** activas y sus participantes. Abre una conferencia para ver quién está en ella y actúa en el lugar: **bloquea** o **desbloquea** el puente, **expulsa** a un participante, activa o desactiva **video**, o **destruye** la conferencia por completo. Este es el control en vivo del operador sobre un puente en funcionamiento.

Correo de Voz

Los registros de **correo de voz** almacenados, por suscriptor. Cada registro puede ser **eliminado** individualmente, por ejemplo, para borrar un mensaje dejado por error o para liberar un buzón lleno.

Prueba OCS

Las **sesiones OCS (Sistema de Cobro en Línea)** activas que el TAS está manejando, para que puedas ver qué llamadas están utilizando un saldo en tiempo real. Una sesión de cobro individual puede ser **terminada** desde aquí. Esto es útil para limpiar una sesión que ha quedado abierta después de que su llamada ha finalizado.

Enrutamiento

Las **plantillas de plan de marcado** contra las que el TAS enruta llamadas. La lista muestra cada plantilla; abre una para leer su contenido. Esta es la referencia para cómo se emparejan los números y dónde se envían las llamadas. Léelo junto con la herramienta de **Traducción de Números** para confirmar que un número dado se enruta como se pretende.

Configuración

La **configuración de la aplicación** que el TAS está ejecutando, agrupada por aplicación. Abre una entrada para leer sus ajustes. Esta es la referencia de lectura para confirmar que el servidor está configurado como se esperaba sin salir de OmniWeb.

Avisos

Las **grabaciones de avisos de texto a voz** que el TAS reproduce para los llamantes, los anuncios y los avisos de menú, con el estado de cada uno. Usa esta pestaña para confirmar que los avisos esperados están presentes y se han renderizado.

Herramientas

Junto a las pestañas anteriores, la página del TAS lleva un conjunto de herramientas bajo demanda para validar el enrutamiento y los datos de suscriptores. Cada una toma un pequeño formulario, ejecuta la solicitud contra el servidor de aplicaciones a través del proxy de OmniWeb y muestra el resultado en el lugar.

Simulador de Llamadas

Realiza una llamada de prueba a través del TAS para validar el enrutamiento y el medio. Ingresa un **destino** (y opcionalmente un número de origen, IP de origen y una disposición forzada). El simulador lleva la llamada a través del plan de marcado **sin hacer sonar a nadie**. Devuelve el **tipo de llamada** resuelto (MT, MO o emergencia), la decisión de dentro/fuera de la red, cada **variable de plan de marcado** que configuró, y una lista paso a paso de **notas de procesamiento**, para que puedas ver exactamente cómo se manejaría un número antes de realizar una llamada real. La autorización del OCS y la búsqueda del HLR pueden ser omitidas para aislar una etapa. Una acción de **llamada de prueba de eco** separada hace sonar un destino y devuelve el audio de la parte, lo que confirma la ruta de voz en vivo hacia un teléfono.

Consulta Sh

Consulta al HSS a través de la interfaz **Sh** para obtener los datos de usuario de un suscriptor. Ingresa la **identidad pública** del suscriptor y elige la **referencia de datos** a obtener, desde los **datos del repositorio** completos hasta un elemento específico como el estado del usuario IMS, el nombre del S-CSCF que sirve, los criterios de filtro iniciales, el MSISDN o el IMSI. La herramienta devuelve los datos de servicio transparentes y del repositorio que el HSS tiene. Úsalo para confirmar lo que el servidor de aplicaciones ve para un suscriptor cuando un servicio no se comporta como se esperaba.

Búsqueda HLR

Realiza una **búsqueda HLR** a través de SS7 MAP (una solicitud de Enviar Información de Enrutamiento) para resolver el estado de enrutamiento y roaming de un suscriptor. Ingresa el **MSISDN** en formato internacional y la herramienta devuelve la respuesta HLR junto con las **variables de plan de marcado** que el resultado establecería en una llamada. Así es como confirmas la ubicación actual de un número en la red antes de diagnosticar por qué las llamadas a él se enrutan de la manera en que lo hacen.

Traducción de Números

Prueba cómo un número marcado es **normalizado y traducido** por las reglas de enrutamiento del TAS. Ingresa un **código de país**, el **número de teléfono** y una **disposición** opcional. La herramienta devuelve el número traducido que el plan de marcado utilizaría. Léelo junto con la pestaña de **Enrutamiento** para confirmar que un número dado se empareja y se reescribe como se pretende.

ESL

Una **consola** interactiva para emitir comandos al estilo del Servidor de Medios al motor TAS para diagnósticos. Escribe un comando y presiona Enter. La salida se imprime de nuevo en la consola, y las flechas Arriba/Abajo recuerdan comandos anteriores. Se ofrecen comandos de ejemplo como `status`, `sofia status`, `show channels` y `show registrations` como chips de un clic. Es la vista de nivel más bajo del motor en funcionamiento, para confirmar canales en vivo, estado de puertas de enlace y registros directamente.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo del TAS para solucionar problemas de un solo servidor de aplicaciones sin salir de OmniWeb.

Paneles de Monitoreo

Los volúmenes de llamadas, contadores por servicio y otras series temporales para el TAS se presentan como paneles de Grafana, accesibles desde la página

de elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionado

- El **CSCF** señaliza las llamadas a las que el TAS aplica servicios. Juntos entregan voz IMS.
- El **HSS** contiene los datos de suscriptor y de usuario Sh que el TAS resuelve.
- El **OCS** califica y cobra las llamadas del TAS en tiempo real a través de Diameter.
- El **DRA** retransmite la señalización Diameter del TAS (Sh, Gy) a esos pares.

Dispositivos de Prueba

Dispositivos de Prueba convierte teléfonos Android reales en sitios remotos en una granja de pruebas controlable de forma remota. Desde OmniWeb puedes ver la pantalla de un teléfono en vivo, controlarlo (tocar, deslizar, escribir, teclas de hardware), realizar llamadas y enviar mensajes de texto, y ejecutar chequeos de salud programados. Estas verificaciones cubren el registro de VoLTE, señal y conectividad. OmniWeb exporta sus resultados de aprobado/reprobado a Prometheus para alertas y paneles.

← Volver a la Guía de Operaciones

Existe para responder a la pregunta que un NOC sigue haciendo sobre un sitio celular remoto: *"¿está funcionando realmente un teléfono en esta red en este momento?"* El teléfono debe estar registrado para VoLTE y ser capaz de llamar, enviar mensajes de texto y acceder a internet. Nadie tiene que conducir hasta el sitio.

Arquitectura

Cada host con teléfonos conectados a través de ADB ejecuta un **agente** ligero. El agente marca *hacia afuera* a OmniWeb central, por lo que los sitios detrás de NAT no necesitan acceso entrante. El video en vivo utiliza **WebRTC** (UDP) por lo que sobrevive mejor a enlaces con pérdida y alta latencia que el uso de TCP para compartir pantalla. Central retransmite la entrada y los resultados de la prueba.

> **Los caminos de red importan.** La interfaz web, la entrada y la configuración de llamadas ("señalización") utilizan el plano de control sobre HTTPS hacia el servidor de OmniWeb. Sin embargo, el video en vivo de la pantalla se transmite **directamente entre el navegador del operador y el host del agente a través de UDP**. No pasa por el servidor. Si un navegador puede alcanzar el servidor pero no el host del agente a través de UDP, la consola se queda en "Conectando…". Consulta **Requisitos de Red** para la regla de firewall a solicitar y cómo reconocer el problema.



Componente	Rol
Agente del teléfono	Descubre dispositivos ADB, captura la pantalla, inyecta entrada, ejecuta scripts de prueba del host. Uno por sitio; instalado por el rol de Ansible `device_tester`.
OmniWeb Central	Registro de dispositivos, retransmisión de señalización WebRTC, despacho de scripts, historial de resultados, métricas de Prometheus.
Prometheus	Extrae resultados de pruebas programadas de `/api/android/metrics`.

Tipos de dispositivos

La granja ya no es solo de teléfonos. Cada dispositivo conectado es uno de tres tipos, detectados automáticamente por el agente y mostrados con su propia insignia (y el logo del robot Android para teléfonos) en la flota:

Tipo	Qué es	Consola
Teléfono Android	Un teléfono normal (Android 5.0+ / API 21+) a través de ADB	Pantalla en vivo + control total
Módem USB	Un módulo celular que expone puertos AT (por ejemplo, Quectel EP06)	Consola celular controlada por AT: estado, llamadas, SMS, bloqueo de celda, VoLTE
Dongle de Android antiguo	Un dongle LTE barato que ejecuta Android antiguo (API < 21, por ejemplo, UZ801) demasiado viejo para la vista de pantalla en vivo	Vista de **screencap** basada en sondeo + control
Simulador RAN UE	Un UE virtual del Simulador RAN, sin hardware	Panel de control UE: adjuntar/desadjuntar, inactivo, fuera de cobertura, registro IMS, SMS, llamadas

Hacer clic en un dispositivo abre la consola apropiada para su tipo. Dentro de cualquier consola, el botón **Cambiar teléfono** (arriba a la derecha) cambia a otro dispositivo sin volver a la cuadrícula de la flota.

UEs simulados del Simulador RAN aparecen en la flota etiquetados como simuladores, por lo que puedes controlar suscriptores emulados junto a teléfonos reales. El filtro de Dispositivos de Prueba te permite reducir a solo los UEs del Simulador RAN. Utilizan el **mismo panel de control UE** mostrado en el propio Mapa de Red del Simulador RAN, por lo que hay un lugar para adjuntar, inactivar, salir de cobertura, registrarse en IMS y enviar SMS/llamadas. Consulta Simulador RAN para el ciclo de vida completo del UE.

Agregar un dispositivo a un sitio

Un dispositivo se une a la flota automáticamente una vez que el **host del agente** en ese sitio puede verlo a través de ADB. Hay dos pasos. Primero, habilitar ADB en el teléfono. Luego, si el agente se ejecuta en una VM o contenedor, pasar el dispositivo USB a él.

1. Habilitar ADB en el teléfono

1. En el teléfono, abre **Configuración → Acerca del teléfono** y toca **Número de compilación** siete veces para desbloquear **Opciones de desarrollador**.
2. En **Configuración → Sistema → Opciones de desarrollador**, activa **Depuración USB**.
3. Conecta el teléfono al host del agente con un cable USB **capaz de datos**.
4. El teléfono muestra un aviso de *"¿Permitir depuración USB?"* con la clave RSA del host. Marca **Siempre permitir desde esta computadora** y acepta. (Sin la marca, el aviso vuelve cada vez que se reconecta y el dispositivo aparece como `no autorizado`.)

Un teléfono normal no necesita nada más. Los scripts de prueba y la pantalla en vivo utilizan solo ADB estándar. Mantén la pantalla desbloqueada para la primera conexión para que se pueda aceptar el aviso.

2. Pasar el dispositivo USB al host del agente

Salta esto si el agente se ejecuta en hardware físico. Si el host del agente es una máquina virtual o contenedor, el hipervisor posee el puerto USB, por lo que debes reenviar el dispositivo:

Plataforma	Cómo reenviar el dispositivo
Proxmox (VM)	`qm set <vmid> -usbN host=<bus>-<port>` para vincular un puerto físico (el mapeo sobrevive al intercambio de teléfonos en ese puerto), o `host=<vendor>:<product>` para seguir un dispositivo específico. Encuentra los ids con `lsusb` en el host de Proxmox.
Proxmox (contenedor LXC)	Agregar a `/etc/pve/lxc/<ctid>.conf`: un permiso de grupo de dispositivos para USB (`lxc.cgroup2.devices.allow: c 189:* rwm`) y un montaje de enlace del bus USB (`lxc.mount.entry: /dev/bus/usb/<bus> dev/bus/usb/<bus> none bind,optional,create=dir`), luego reinicia el contenedor. Volver a enchufar un dispositivo en un bus diferente necesita que el bus coincidente esté montado.
VMware	Con la VM en ejecución, **VM → Dispositivos extraíbles → <teléfono> → Conectar** (o agrega un controlador USB y adjunta el dispositivo en la configuración de la VM).

> Los módems USB y los dongles de Android antiguos se reenvían de la misma manera. Aparecen como la misma clase de dispositivo USB, por lo que un bus que se pasa lleva teléfonos, módems y dongles por igual.

3. Confirmar que aparece

En el host del agente, `adb devices` debería listar el teléfono como `device` (no `unauthorized` o `offline`). Dentro de unos segundos aparece en la **Vista de Flota** para ese sitio. Si no lo hace, consulta Solución de Problemas.

Vista de Flota

La vista de **Dispositivos de Prueba** lista cada teléfono conectado en todos los sitios, agrupados por sitio. Cada tarjeta muestra el modelo, fabricante,

versión de Android, resolución de pantalla, operador de red, batería y compilación. De un vistazo puedes ver qué teléfonos están en línea y saludables.

La flota agrupa dispositivos por sitio (por ejemplo, "Sitio Celular 12", "Laboratorio Norte"). Cada tarjeta muestra estado en vivo, batería y operador. Selecciona teléfonos y un script para distribuir una prueba entre ellos. Haz clic en una tarjeta para abrir su consola.

Etiquetado de un dispositivo. El lápiz en una tarjeta de flota abre **Editar metadatos del dispositivo**, donde puedes darle un **nombre** amigable a un dispositivo y registrar su **operador**, **IMSI** y **MSISDN**. Estos son asignados por el operador (Android moderno oculta el IMSI/MSISDN de ADB) y se mantienen en el dispositivo incluso cuando está fuera de línea. El nombre es lo que se muestra en los encabezados de la consola y en los selectores de dispositivos.

La entrada **Dispositivos de Prueba** de la barra lateral se expande para mostrar cada sitio (con un conteo de dispositivos), la vista de **Agentes**, la biblioteca de scripts, el programador y las herramientas de dispositivos, para que puedas saltar directamente a donde necesitas.

Ejecutando pruebas en varios dispositivos

Selecciona uno o más teléfonos, elige un script y **Ejecutar en seleccionados** lo distribuye en paralelo. Los resultados se transmiten a una tabla, una fila por dispositivo con una insignia de aprobado/reprobado, código de salida, duración y salida expandible.

Agentes

La vista de **Agentes** (barra lateral → Dispositivos de Prueba → Agentes) lista cada banco conectado a este servidor, una fila por host de sitio, con su estado en línea, IP, los dispositivos que lleva, cuándo se registró y su versión de software. Responde a "¿qué sitios están realmente reportando y desde dónde?" de un vistazo, y es donde confirmas que un banco recién instalado ha marcado.

Consola del Dispositivo

Hacer clic en un teléfono abre su **consola**: una vista en vivo de la pantalla con control remoto completo.

*La consola transmite la pantalla del teléfono en vivo. Haz clic para tocar, arrastra para deslizar, escribe para ingresar texto. Una insignia de **calidad de red** (arriba a la derecha de la pantalla) muestra verde/ámbar/rojo de un vistazo. Haz clic en ella para ver las estadísticas completas de la transmisión (resolución, FPS, bitrate, %, pérdida de paquetes en 5 segundos, jitter, RTT). La barra de teclas de hardware (atrás, inicio, recientes, volumen, encendido) y las acciones rápidas (Avión, Marcador, Mensajes, Configuración) están debajo. Un panel de herramientas con pestañas se encuentra al lado: Validación celular, Scripts, Shell, Logcat, Archivos y Grabar.*

> **Un espectador a la vez.** Un dispositivo transmite a un operador a la vez. Si alguien más ya lo está viendo, la consola muestra *"En uso por <usuario> (<IP>)"*. La IP te permite saber si eres tú en otra máquina o un operador diferente. Un botón de **Tomar control** reclama la transmisión. Una consola desconectada o recargada se reconecta automáticamente a su propia sesión en lugar de pelear por ella.

Control remoto

Acción	Cómo
Tocar	Haz clic en cualquier lugar de la pantalla
Deslizar	Haz clic y arrastra
Escribir	Haz clic en la pantalla, luego escribe en tu teclado
Teclas de hardware	Botones de Atrás, Inicio, Recientes, Volumen ±, Encendido
Acciones rápidas	Alternar modo avión con un clic, o abrir la aplicación Marcador, Mensajes o Configuración. Estas se ejecutan en segundo plano. No ejecutan una prueba ni bloquean la consola.

La pantalla transmitida es el dispositivo en vivo. Cualquier aplicación o página web se renderiza y se puede controlar completamente desde la consola. Aquí un teléfono de prueba tiene una página abierta en el navegador, controlada de forma remota:

Ver más de un teléfono

Para ver varios teléfonos a la vez (ambos extremos de una llamada de prueba, por ejemplo), abre la consola de un teléfono y haz clic en **Teléfono extra** (arriba a la derecha). Elige otro teléfono de la lista y su pantalla en vivo se abre junto a la primera, con sus propios controles completos: tocar/deslizar/escribir, teclas de hardware, acciones rápidas, escuchar audio y estadísticas de transmisión. La lista permanece abierta para que puedas seguir agregando, y las pantallas se distribuyen a través de la página — no hay un límite fijo, así que agrega tantos como tenga el banco.

Para abrir todo un grupo de una vez, marca los teléfonos que deseas en la lista de Dispositivos de Prueba y haz clic en **Ver seleccionados**: el primero se convierte en el dispositivo principal (el que la columna de herramientas actúa sobre) y el resto se distribuyen a su lado.

Cada pantalla extra tiene su propio selector para **cambiar** qué teléfono muestra y un ✕ para cerrarla. La disposición se captura en la dirección de la página (`?with=…`), por lo que un diseño específico de múltiples teléfonos puede ser marcado o compartido.

El panel de herramientas con pestañas (Celular, Scripts, Shell, …) siempre actúa sobre el teléfono **principal**, el que abriste. El encabezado del panel lo nombra para que quede claro dónde se ejecutará un script o comando.

Herramientas de Consola

Junto a la pantalla, un **panel de herramientas con pestañas** mantiene juntas las herramientas por dispositivo. Cambia de pestaña sin perder el estado de cada herramienta:

Pestaña	Qué hace
Celular	Las herramientas de validación de llamada / texto / ping / prueba de velocidad (abajo)
Scripts	Ejecuta un script de la biblioteca en este dispositivo y ve su historial completo de ejecución, con un re-ejecución de un clic en cualquier ejecución pasada
Shell	Una consola interactiva de comando/respuesta para el dispositivo
Logcat	Transmisión de registro en vivo del dispositivo con filtrado de texto + nivel
Archivos	Navegar, descargar, subir, renombrar y eliminar archivos en el dispositivo
Grabar	Captura una secuencia de toque/deslizamiento como líneas de script reproducibles

Panel de Validación Celular

Herramientas integradas para las verificaciones que un operador realiza manualmente, cada una tomando las entradas que esperarías:

Herramienta	Entradas	Qué hace
Llamada	Número, tiempo de espera	Marca, confirma que la llamada se desconecta, mantiene, cuelga
Texto	Número, mensaje	Envía un SMS y confirma que salió del dispositivo
Ping	Host, conteo	Pinge un host a través de la conexión de datos del dispositivo
Prueba de Velocidad	URL de prueba	Mide el rendimiento de descarga a través del enlace de datos del dispositivo

La caja de **Número** recuerda los números que has llamado o enviado mensajes recientemente (guardados solo en tu navegador, no en el servidor) y los ofrece como un menú desplegable, por lo que volver a marcar un número de prueba es un clic.

Scripts

La pestaña **Scripts** ejecuta cualquier script de biblioteca contra este dispositivo y mantiene su historial completo de ejecución sin salir de la consola. Puedes filtrar ese historial por fuente, estado y prueba. Cada ejecución pasada tiene un botón de **re-ejecución**, por lo que repetir un chequeo (o un script que acaba de fallar) es un clic. Los scripts que toman entradas vuelven a solicitarlo.

Shell

La pestaña **Shell** es una consola interactiva de comando/respuesta para el dispositivo. Escribe un comando, ve su salida y código de salida, con ↑/↓ para recordar el historial. Es el análogo del dispositivo de la consola AT del módem, para las veces que un comando rápido es más rápido que escribir un script.

Logcat

La pestaña **Logcat** transmite el registro del sistema en vivo del dispositivo. Filtra por texto libre y nivel mínimo (Verbose → Fatal). Los niveles están codificados por colores. **Iniciar**/**Detener** controla la transmisión. Detener mantiene lo que has capturado en pantalla para que puedas desplazarte hacia atrás a través de él.

Archivos

La pestaña **Archivos** es un administrador de archivos para el dispositivo. Navega por directorios (comenzando en `/sdcard`), **descarga** un archivo a tu máquina, **sube** un archivo al dispositivo, y **renombra**, **elimina** o crea carpetas. Útil para extraer un archivo de captura o diagnóstico de un dispositivo, o para cargar una configuración en él.

Grabación de gestos

Activa **Grabar**, realiza una secuencia de toque/deslizamiento en la pantalla, y la consola emite las líneas equivalentes de `adb input`. Pégalas en un script de carpeta para convertir un flujo de UI manual en una prueba repetible.

Consola de Módem USB

Un módem celular USB (Quectel EP06 y similares) aparece en la flota como un **módem** y abre una consola celular en lugar de una pantalla. El agente retransmite comandos AT al módem a través de su puerto serial (AT). Registra cada comando y respuesta en la pestaña **Terminal** como un rastro de auditoría.

Pestaña	Qué hace
Estado	Lectura única de modelo / firmware / IMEI / IMSI / SIM, señal (CSQ + CSQ por RAT), operador, registro EPS, adjuntar, IMS, IP, APN, DNS/PCO
Acciones	Establecer APN (preestablecido o personalizado, con **PDP / tipo de IP**), adjuntar/desadjuntar datos, mostrar IP + DNS, ping, enviar SMS, radio (modo avión / reiniciar)
Redes	Escaneo de operador (`AT+COPS=?`) y una **medición de celda** de servicio/vecina (`AT+QENG`) → tabla EARFCN / PCI / banda / RSRP / RSRQ / SINR
Bloqueo de celda	Bloquear a un **EARFCN específico (+PCI)** (`AT+QNWLOCK`), bloqueo de banda (`AT+QCFG="band"`), preferencia de RAT, o liberar de nuevo a automático
Llamadas	Marcar / responder / colgar, una tabla de llamadas `AT+CLCC`, y un control de **Habilitar / Deshabilitar VoLTE** (`AT+QCFG="ims"`)
SMS	Leer la bandeja de entrada (`AT+CMGL`), eliminar y enviar
Eventos	Habilita los URCs relevantes y los sondea en un registro con marca de tiempo (registro / llamada / señal / cambios de nuevo-SMS)
Terminal	Entrada AT en bruto más el registro completo de solicitud/respuesta

La referencia completa de comandos AT, con respuestas reales de EP06, está en **modem-at-commands.md**.

> **VoLTE:** el EP06 es solo VoLTE/IMS para voz. *Habilitar VoLTE* establece `AT+QCFG="ims",1`; un reinicio `AT+CFUN=1,1` puede ser necesario para

> (de)registrar IMS, y solo se registra si la red + SIM lo provisionan y se selecciona el MBN correcto del operador.

Dongles de Android antiguos (modo de captura de pantalla)

Dongles LTE baratos de ~$10 "MiFi" (por ejemplo, el UZ801, Qualcomm msm8916) ejecutan **Android 4.4 (API 19)**, que es demasiado viejo para la vista de pantalla en vivo. Estos dispositivos retroceden a una consola de **captura de pantalla**: el agente sondea `adb screencap` para fotogramas (unos pocos por segundo, porque `screencap` en sí es el cuello de botella en este hardware) e inyecta `adb input` para control. Obtienes una vista de clic-para-tocar, escribir-para-texto. No es un video fluido, pero es suficiente para controlarlo.

El agente suaviza los bordes ásperos de estos dongles en el lado del host:

- **Desbloqueo ADB**: se envían en modo RNDIS. Un servicio activado por udev `curl` el `usbdebug.html` del dongle para cambiarlo a modo ADB. Consulta agent/host-setup/mifi-dongle.
- **Auto-Inglés**: se envían en chino. El agente establece `persist.sys.language` en `en-US` la primera vez que ve un dispositivo API-<21 (deshabilitar con `OMNIWEB_DONGLE_AUTO_ENGLISH=0`).

Scripts

Las pruebas son scripts bash que se ejecutan en el **host del agente** (por lo que herramientas del host como `grep`/`awk` están disponibles) y apuntan a un dispositivo a través de ADB. Hay dos tipos:

- **Scripts de carpeta**: chequeos de salud que aparecen en la biblioteca, el corredor de distribución y el programador. Algunos se ejecutan solo con el dispositivo (Dispositivo Conectado, Registro de VoLTE, Reportar Fuerza de Señal). Otros toman entradas opcionales (`@param`). La Prueba de Ping toma un host y un conteo. La Prueba de Rendimiento de Datos toma una URL. Las pruebas de conectividad y voz (Ping, Rendimiento de Datos, Enviar

SMS, Realizar Llamada) son scripts de carpeta, por lo que puedes programarlas así como ejecutarlas manualmente. Dos pruebas de recuperación de flap de modo avión confirman que un dispositivo se recupera después de perder radio. **Flap de Modo Avión → Recuperación de Ping** activa el modo avión, luego lo desactiva, espera a que los datos se vuelvan a conectar, luego hace ping. **Flap de Modo Avión → Recuperación de IMS** hace lo mismo, luego confirma que VoLTE se vuelve a registrar.

- **Herramientas integradas**: los accesos directos para abrir aplicaciones (Marcador, Mensajes, Configuración) y el simple interruptor de modo avión en las acciones rápidas de la consola. Cada uno realiza una acción de UI sin resultado de aprobado o reprobado, por lo que no está en la biblioteca ni en el programador.

La biblioteca de scripts lista los scripts de carpeta sin argumentos. Cada uno muestra su descripción y tiempo de espera. Haz clic en uno para ver su código fuente (solo lectura). Las ejecuciones recientes aparecen a continuación.

Un script informa su resultado mediante **código de salida**: `0` es un aprobado, cualquier otra cosa un reprobado. Su salida capturada se muestra en la tabla de resultados.

Pruebas Programadas

Las pruebas programadas se definen de manera declarativa en `schedules.json` en el directorio de scripts. El archivo se vuelve a leer en cada ciclo, por lo que las ediciones tienen efecto sin un reinicio. Cada entrada ejecuta un script de carpeta contra sus dispositivos objetivo en un intervalo.

Configuración

```
{
  "schedules": [
    {
      "name": "Registro de VoLTE",
      "script": "volte_registration.sh",
      "interval_seconds": 120,
      "serials": [],
      "enabled": true
    }
  ]
}
```

Parámetro	Tipo	Requerido	Predeterminado	Descr
`name`	Cadena	Sí	-	Etiqueta para el h Aparece etiqueta `schedul` métrica exportad
`script`	Cadena	Sí	-	Nombre archivo script de en el dir de script ejecutar
`interval_seconds`	Entero	No	300	Con qué frecuenc ejecutar en segu Mínimo
`serials`	Lista	No	`[]`	Seriales dispositi apuntar. **lista va significa los disp actualm conecta** lo que e sigue automát lo que es conecta

Parámetro	Tipo	Requerido	Predeterminado	Descr
`params`	Objeto	No	`{}`	Entradas script qu declara `@param`. claves s nombres parámet ejemplo Prueba c acepta `count`.
`enabled`	Booleano	No	true	Si el hor activo. E `false` p pausarlo eliminar entrada.
`exclusive`	Booleano	No	false	Reserva teléfono la durac esta pru Mientras ejecute prueba e ninguna prueba program comienz dispositi prueba e en sí esp que el d esté libr

Parámetro	Tipo	Requerido	Predeterminado	Desc
				de come Úsalo pa pruebas disruptiv flap de r avión o reinicio podrían corromp prueba (ejemplo llamada que se e en el mi teléfono mismo t

Ejemplo: Verificación de VoLTE en un sitio

```
{
  "name": "VoLTE Registration",
  "script": "volte_registration.sh",
  "interval_seconds": 120,
  "serials": [],
  "enabled": true
}
```

Cómo funciona: Cada 120 segundos, el programador ejecuta `volte_registration.sh` en cada teléfono conectado. El script verifica que el dispositivo esté registrado para voz (`IN_SERVICE`) en LTE con soporte de VoPS (Voice-over-PS), y sale con `0` si VoLTE está registrado. El resultado se convierte en un medidor de Prometheus por dispositivo.

Caso de uso: Probar continuamente que los teléfonos reales en un sitio pueden registrarse para VoLTE y alertar en el momento en que uno no pueda.

Ejemplo: Hacer ping a cada teléfono

```
{
  "name": "Ping Test",
  "script": "ping_test.sh",
  "interval_seconds": 120,
  "serials": [],
  "params": { "host": "8.8.8.8", "count": "5" },
  "enabled": true
}
```

Cómo funciona: Cada 120 segundos, el programador ejecuta `ping_test.sh` en cada teléfono conectado. Los `params` proporcionan las entradas del script. El script hace ping a `8.8.8.8` cinco veces a través del enlace de datos del dispositivo y sale con `0` si recibe respuestas. Cambia `host` para probar un objetivo específico.

Caso de uso: Probar que los teléfonos reales en un sitio tienen datos funcionales y alertar sobre la pérdida de paquetes.

Pausa automática mientras un teléfono está en uso

Abrir la pantalla en vivo de un teléfono pausa las pruebas programadas **para ese teléfono**. Una prueba disparada en un dispositivo que alguien está observando y tocando pelearía por la pantalla y registraría un pase o fallo sin sentido, por lo que el programador omite cualquier teléfono que tenga un espectador en vivo y lo retoma tan pronto como se cierra la vista.

- La pausa es por teléfono. Cada otro teléfono que un programa objetivo sigue funcionando en su intervalo normal.
- Una ejecución omitida no se cuenta como realizada: el programa se dispara en su próximo ciclo una vez que el teléfono está libre, en lugar de esperar un intervalo completo.
- Una prueba que ya estaba en ejecución cuando se abrió la pantalla se deja terminar.
- Cierra la vista del teléfono (o navega a otra parte) y las pruebas se reanudan en aproximadamente un minuto. Si el navegador desaparece sin

cerrarse correctamente, la pausa se levanta por sí sola.
- **Ejecutar ahora** no se ve afectado: una ejecución solicitada explícitamente siempre avanza.

La pestaña de Pruebas Programadas del teléfono muestra un banner mientras la pausa está en efecto, y la flota marca un teléfono retenido **en uso** con quién lo tiene.

Métricas

Central OmniWeb expone el último resultado de cada prueba programada, por dispositivo, en formato Prometheus en `/api/android/metrics`. Prometheus lo extrae como el trabajo `android_device_tests` (configurado automáticamente por el rol de monitoreo).

Métrica: `omniweb_android_test_pass` **Tipo**: Medidor **Descripción**: Resultado de la ejecución programada más reciente: `1` para pasar, `0` para fallar **Etiquetas**:

- `phone`: modelo del dispositivo (por ejemplo, `SM-A536E`)
- `serial`: número de serie del dispositivo
- `site`: la etiqueta del sitio del agente (por ejemplo, `Cell Site 12`)
- `agent`: el host del agente al que está conectado el dispositivo
- `script`: el script que se ejecutó
- `schedule`: el nombre del programa
- `status`: el resultado de la ejecución (`passed`, `failed`, `timeout`, o `error`)

Los medidores complementarios comparten las mismas etiquetas:

Métrica	Descripción
`omniweb_android_test_duration_ms`	Duración de la última ejecución, en milisegundos
`omniweb_android_test_last_run_timestamp`	Tiempo Unix de la última ejecución

Un medidor separado informa qué teléfonos están actualmente retenidos por un espectador, para que una alerta de obsolescencia pueda distinguir un teléfono deliberadamente pausado de una prueba rota:

Métrica	Descripción	Etiquetas
`omniweb_android_device_in_use`	`1` mientras alguien tenga la pantalla del teléfono abierta (sus pruebas programadas están pausadas), `0` en caso contrario	`serial`, `phone`, `site`, `agent`

Ejemplos de consultas:

```
# Teléfonos que actualmente están fallando en el registro de VoLTE
omniweb_android_test_pass{schedule="VoLTE Registration"} == 0

# Pruebas fallidas agrupadas por sitio
count by (site) (omniweb_android_test_pass == 0)

# Una prueba que no se ha ejecutado recientemente (agente obsoleto
o dispositivo fuera de línea)
time() - omniweb_android_test_last_run_timestamp > 600

# Lo mismo, ignorando teléfonos que alguien tiene abiertos
actualmente (las pruebas están pausadas para esos)
(time() - omniweb_android_test_last_run_timestamp > 600)
  unless on (serial) omniweb_android_device_in_use == 1

# Teléfonos actualmente en uso
omniweb_android_device_in_use == 1
```

Panel de Grafana

El rol de monitoreo envía un panel de **Pruebas de Teléfonos / Dispositivos** (carpeta de Grafana **Devices**). Lee las métricas anteriores y muestra, por teléfono y programa:

- una línea de tiempo de estado de pase o fallo,
- el último resultado para cada teléfono y prueba,
- frescura de la prueba (tiempo desde la última ejecución, para detectar un agente estancado),
- duración de la ejecución a lo largo del tiempo.

Filtra el panel por sitio, teléfono o prueba en la parte superior. El panel se provisiona automáticamente. Consulta Grafana.

Solución de problemas

Un teléfono no aparece en la flota

Síntomas: Un dispositivo está conectado en un sitio pero no está listado bajo Dispositivos de Prueba.

Causas posibles:

- El teléfono no está autorizado para ADB en el host del agente
- El agente no está en ejecución o no puede alcanzar el central
- El teléfono está en un estado de ADB fuera de línea/no autorizado
- El servicio de Dispositivos de Prueba central no está en ejecución (Dispositivos de Prueba es servido por su propio servicio backend dedicado, separado del grupo de solicitudes principal)

Resolución:

1. Confirma que el teléfono aparece como `device` (no `unauthorized`/`offline`) en ADB en el host del agente, aceptando el aviso RSA en el dispositivo si es necesario.
2. Verifica que el servicio del agente esté en ejecución y que su URL central y token configurados sean correctos.
3. En central, confirma que el servicio de Dispositivos de Prueba esté en ejecución y que la puerta de enlace dirija `/api/android/*` a él. Si el agente se registró pero la flota está vacía, este servicio es la causa habitual.

4. Verifica la conexión USB del teléfono; vuelve a conectar el cable si aparece como fuera de línea.

La pantalla de la consola permanece en "Conectando"

Síntomas: La consola del dispositivo se abre pero la pantalla nunca aparece, mientras que el resto de la interfaz de usuario (lista de flota, detalles del dispositivo, entrada) funciona normalmente y el dispositivo muestra **en línea**.

Causas posibles:

- UDP está bloqueado entre la red del navegador y el host del agente (los flujos de video en vivo **directamente** del navegador → host del agente, no a través del servidor, y esta es de lejos la causa más común)
- El agente no puede iniciar la captura de pantalla en ese dispositivo

Esto **no** es un problema de SSL o MTU: TLS está comprobado que funciona (la interfaz se cargó), y con problemas de MTU el video se conectaría y *luego* se cortaría en lugar de nunca comenzar. La señal reveladora es un dispositivo que muestra **en línea** en la flota, pero cuya vista en vivo no comenzará.

Resolución:

1. Confirma que la red del navegador puede alcanzar el host del agente a través de **UDP** (el camino del video). Esto generalmente significa una regla de firewall/VLAN que permita la subred del operador a los hosts de banco a través de UDP. Consulta **Requisitos de Red** para la regla exacta a solicitar y cómo confirmar la solución.
2. Verifica el registro del agente en busca de errores de captura de pantalla. Algunos dispositivos no pueden tener su pantalla capturada a través de ADB.

Las verificaciones de VoLTE / señal informan "no legible"

Síntomas: Los scripts de VoLTE o señal fallan con el estado de telefonía ilegible.

Causas posibles:

- El dispositivo restringe el estado de telefonía a acceso privilegiado

Resolución:

1. Utiliza dispositivos de prueba que expongan el estado de telefonía a ADB. Los dispositivos de consumo bloqueados por el vendedor pueden ocultarlo sin acceso privilegiado.

Dispositivos de Prueba: Requisitos de Red

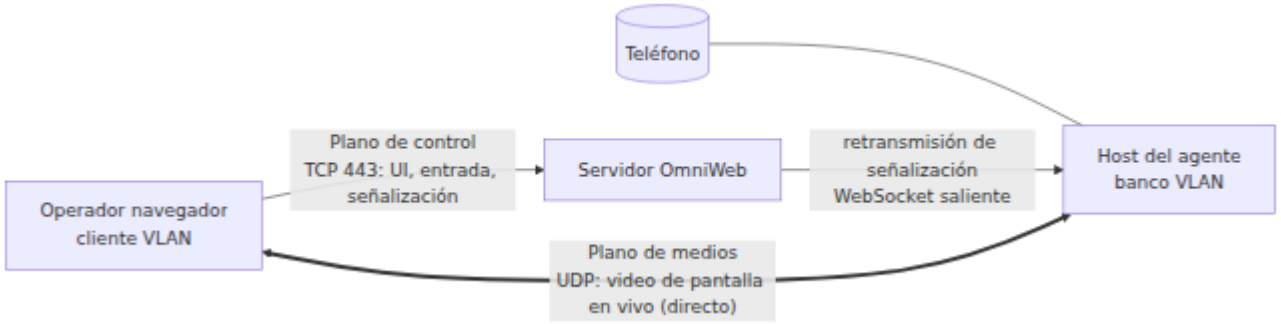
La visualización de teléfonos en vivo en **Dispositivos de Prueba** utiliza **dos rutas de red separadas**. Comprender la división para que funcione a través de cortafuegos y VLANs. La división también te ayuda a diagnosticar el síntoma más común, una consola que se queda en **"Conectando..."** para siempre.

← Volver a Dispositivos de Prueba

Las dos rutas

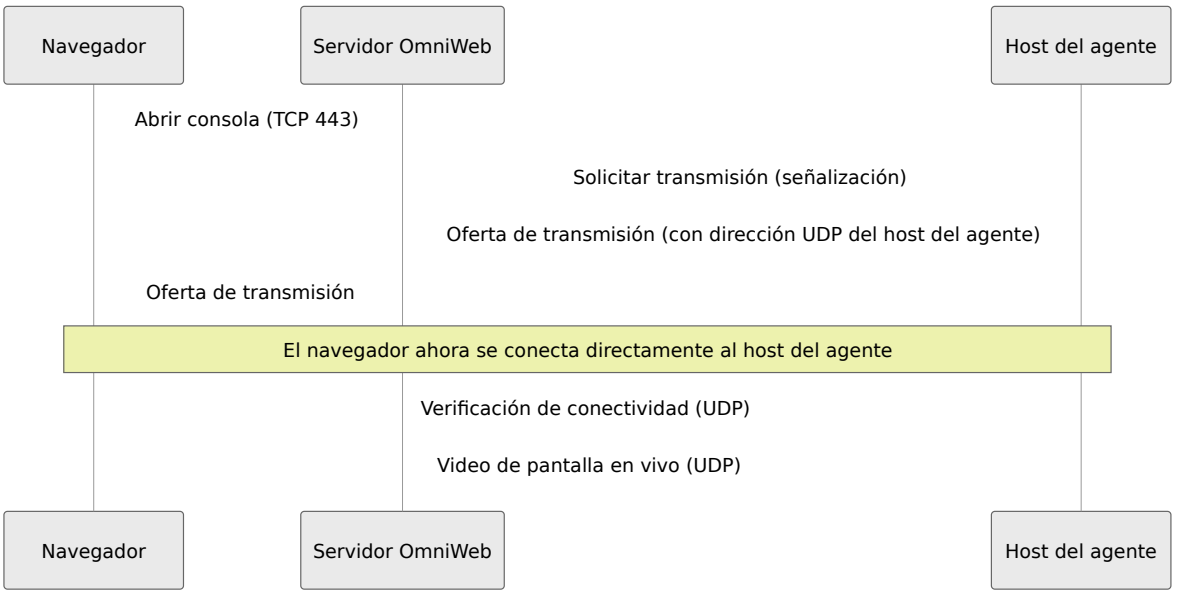
Ruta	Transporta	Dirección	Transporte	Punto final
Plano de control	La interfaz web, inicio de sesión, la lista de dispositivos, entrada remota, resultados de pruebas y la configuración de llamadas ("señalización") para una vista en vivo	Navegador → servidor OmniWeb	**TCP 443 (HTTPS)**	El servidor OmniWeb
Plano de medios	El video de la pantalla en vivo	Navegador ⇄ **host del agente** (el banco al que está conectado el teléfono)	**UDP** (WebRTC)	El host del agente, **no** el servidor

El punto crucial: **el video en vivo no fluye a través del servidor OmniWeb.** Una vez que el servidor ha intermediado la conexión, el video se transmite **directamente entre el navegador del operador y el host del agente** a través de UDP. Si una red permite que el navegador alcance el *servidor* pero no el *host del agente*, carga la interfaz, muestra la lista de dispositivos y luego se queda atascada en "Conectando…".



Por qué el camino de medios es directo

El video de pantalla en vivo se envía de igual a igual con **WebRTC sobre UDP** para que sobreviva a los enlaces de alta latencia y con pérdida típicos de los sitios celulares remotos mucho mejor que retransmitirlo a través de un servidor central sobre TCP. La compensación es que el navegador del operador necesita un **camino UDP directo al host del agente**. No hay retransmisión de medios en el medio a la que recurrir.



Requisitos del cortafuegos

Para que un operador vea teléfonos en un sitio, **ambas** rutas deben estar permitidas desde la red del operador a los hosts relevantes.

Plano de control (generalmente ya abierto)

Campo	Valor
Acción	Permitir (con estado)
Protocolo	TCP
Fuente	VLAN(s) del operador / cliente
Destino	Servidor OmniWeb
Puerto de destino	`443`

Si la interfaz de usuario de OmniWeb se carga, esta ruta ya está abierta. No se necesita ningún cambio.

Plano de medios (el que generalmente falta)

Campo	Valor
Acción	Permitir (**con estado**, por lo que se permite automáticamente el video de retorno)
Protocolo	**UDP**
Fuente	VLAN(s) del operador / cliente, donde se ejecutan los navegadores
Destino	La **subred del host del banco de dispositivos** (los hosts del agente), por ejemplo, `10.0.20.0/24`
Puertos de destino	**`32768–60999`** (el rango efímero predeterminado de Linux del que el agente toma puertos de medios)

El navegador siempre inicia la conexión de medios, por lo que un permiso **con estado** en `cliente → host del agente` también permite automáticamente el video de retorno del agente. No se involucran puertos STUN/TURN u otros.

> **No cambies el puerto 443 para esto.** La señalización ya utiliza el plano de control. Solo se necesita abrir el camino de medios UDP hacia los hosts del agente.

Recomendado: fijar el rango de puertos de medios

Abrir todo el rango efímero (`32768–60999`) es amplio. En su lugar, puedes configurar el agente para que tome sus puertos de medios de un pequeño rango fijo. Esto reduce la regla del cortafuegos a un bloque ordenado:

Campo	Valor
Acción	Permitir (con estado)
Protocolo	UDP
Fuente	VLAN(s) del operador / cliente
Destino	Subred del host del banco de dispositivos
Puertos de destino	**`50000–50100`** (rango fijado)

Esta es la forma preferida para entregar a un equipo de red. 100 puertos a una subred es mucho más fácil de aprobar y auditar que el rango efímero completo. El rango fijado se establece en el host del agente. Coordina el rango exacto con quien mantenga los bancos para que la regla del cortafuegos y la configuración del agente coincidan.

Reconociendo el problema

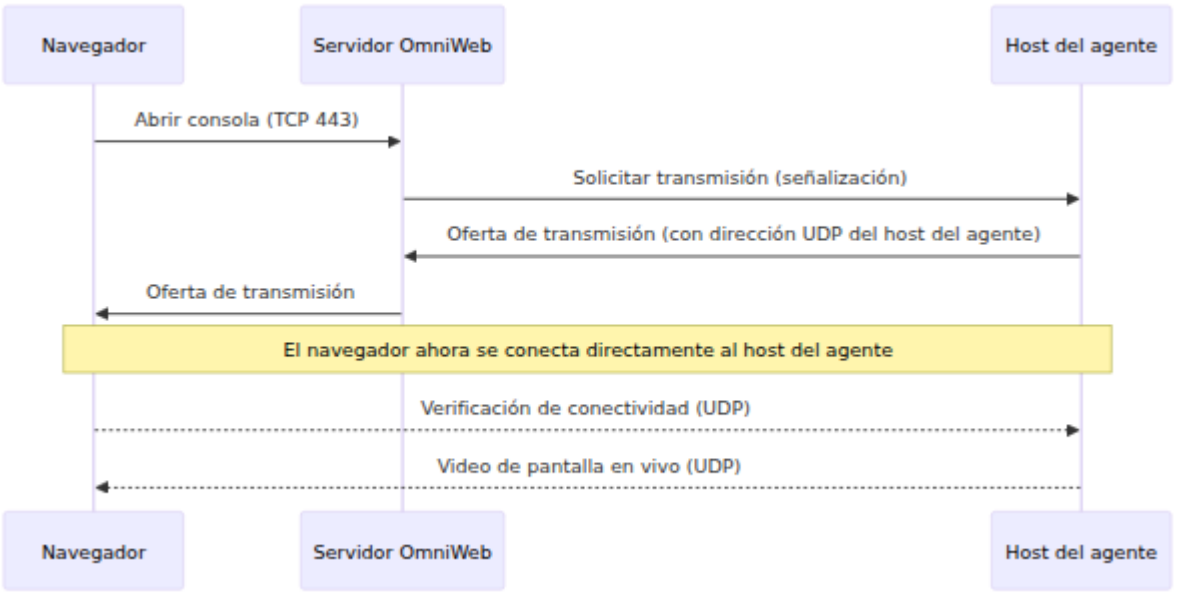
Síntoma: la consola del dispositivo se abre, pero la pantalla nunca aparece. Se queda en **"Conectando…"** indefinidamente. Todo lo demás funciona: la lista de flota, los detalles del dispositivo, incluso la configuración de entrada remota.

Esto es casi siempre el camino UDP del plano de medios bloqueado. **No es** un problema de TLS/certificado y **no es** un problema de MTU:

Causa sospechada	Por qué no es esto	Lo que realmente verías si lo fuera
SSL / certificado	La UI, inicio de sesión, lista de dispositivos y señalización tienen éxito a través de HTTPS, por lo que TLS claramente está funcionando	La página en sí fallaría al cargar o mostraría una advertencia de certificado
MTU / fragmentación	MTU solo importa una vez que fluyen los paquetes de video. Aquí **ningún** paquete de video llega nunca	El video **conectaría**, luego se detendría o se rompería, no se quedaría en "Conectando…"
Agente / teléfono apagado	El dispositivo muestra **en línea** en la flota con datos de batería/operador en vivo	El dispositivo faltaría en la flota o estaría marcado como fuera de línea
Ruta UDP bloqueada ✓	El navegador puede alcanzar el servidor (la UI se carga) pero no el host del agente a través de UDP	"Conectando…" permanente, exactamente este síntoma

Una pista útil: el mosaico del dispositivo muestra el teléfono como **en línea** (por lo que el agente y el teléfono están saludables y el servidor puede verlos),

sin embargo, la vista en vivo no comenzará. Esa combinación apunta directamente al camino del cortafuegos del plano de medios.



Confirmando la solución

Después de aplicar la regla del cortafuegos, vuelve a abrir la consola del dispositivo. Si la pantalla aparece dentro de unos segundos y la insignia de **calidad de red** (en la parte superior derecha de la vista en vivo) se vuelve verde, el camino de medios está funcionando. Las estadísticas de transmisión de la insignia (resolución, FPS, bitrate, porcentaje de pérdida de paquetes, jitter, RTT) confirman que el video está fluyendo de extremo a extremo.

Si aún se queda atascado, verifica dos cosas con quien mantenga los bancos. Primero, la **subred y puertos de destino** de la regla del cortafuegos deben coincidir con los hosts del agente y su rango de puertos de medios configurado. En segundo lugar, la regla debe aplicarse a la VLAN de **origen real** del operador (una laptop en Wi-Fi de invitados es una fuente diferente que la LAN corporativa).

Múltiples ubicaciones de operadores

Cada red de operador que necesite ver teléfonos debe tener la regla del plano de medios para su propia VLAN de origen. La regla es por subred de origen → subred de banco, por lo que agregar una nueva oficina, grupo de VPN o sitio significa agregar su subred como un **Origen** adicional en el mismo permiso UDP. Los sitios cuyos operadores solo ven teléfonos desde la LAN del banco en sí no necesitan ninguna regla inter-VLAN.

Topología de Red y Vista Única

Las vistas de topología de OmniWeb son el punto de entrada "vista única" a toda la red. Muestran cómo se conectan los elementos, cuáles están desplegados y te permiten saltar directamente desde un nodo en el mapa al espacio de trabajo de ese elemento.

← Volver a la Guía de Operaciones

Vistas de Topología

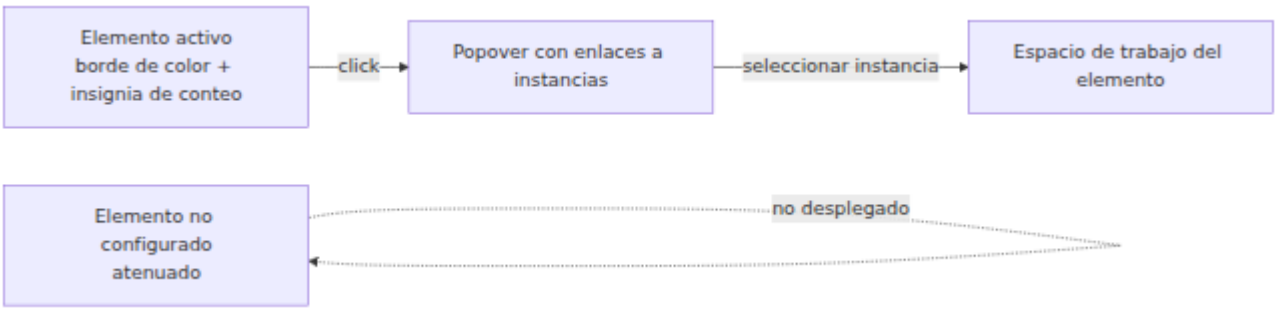
La página de inicio/topología presenta la red a través de cuatro pestañas de dominio. Cada una es un mapa interactivo de los elementos relevantes y sus interfaces.

Topología EPC: UE → eNB → MME → SGW-C → PGW-C → UPF, con señalización Diameter a través del DRA al HSS. Los elementos activos muestran un borde de

color y una insignia de conteo de instancias.

Pestaña	Elementos mostrados
Núcleo (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; Derecho (OmniSEP)
Núcleo CS	BTS → BSC → MSC; STP ↔ HLR / CAMEL GW / IP-SM-GW; HSS; SMSC; OCS
Núcleo 5G	gNB → AMF → SMF → UPF; NRF, SCP, AUSF, UDM, UDR, PCF; CHF → OCS; NSSF; BSF

Leyendo el Mapa



- **Elementos activos** son aquellos con instancias declaradas en `omniweb.json`. Aparecen con un borde de color y una insignia que muestra cuántas instancias existen. Haz clic en uno para abrir un popover con enlaces directos a cada instancia. Luego puedes navegar desde la topología directamente a las páginas de un elemento.
- **Elementos no configurados** aparecen atenuados, por lo que el mapa también sirve como un inventario rápido de lo que está y no está desplegado.
- **Conexiones** indican la interfaz entre elementos (por ejemplo, SIP, Diameter, PFCP, GTP-C, SS7), distinguiendo tipos de señalización.

Esto hace que la página de topología sea el punto de partida natural: ver la forma de la red, identificar lo que está desplegado y profundizar.

Topología a Nivel de Elemento

Algunos elementos también proporcionan su propia vista de topología enfocada. La pestaña **PGW-C → Topología**, por ejemplo, muestra las relaciones de ese nodo con sus pares SGW-C, UPF y Diameter, anotadas con conteos de sesiones en vivo y utilización. Esto proporciona una vista de panel único localizada para el vecindario de ese elemento.

Topología de PGW-C: relaciones con SGW-C, UPF y pares Diameter con distribución de sesiones por par.

Lista de Hosts e Infraestructura

Más allá de las funciones de red en sí, la página de **Lista de Hosts** es la vista única para la *infraestructura* que las ejecuta. Enumera todos los hosts de infraestructura por categoría, cada uno con un enlace directo a su interfaz web:

Categoría	Ejemplos
Monitoreo	Grafana, Prometheus, Loki
Captura SIP	Interfaz web de Homer
Facturación	Interfaz web de OCS
DNS	Servidores DNS
Virtualización	Consolas de hipervisor Proxmox
Fuera de banda	Gestión de servidores iDRAC
Enrutadores	MikroTik WebFig, Peplink
Microondas	Enlaces SAF, Ubiquiti AirFiber
NAS	Synology DSM

La Lista de Hosts: cada host de infraestructura y elemento por categoría, cada uno con un enlace directo a su interfaz web (Grafana, Prometheus, Loki, APIs de elementos y más).

Esto proporciona a los operadores un lugar para acceder a todos los sistemas de soporte: monitoreo, hipervisores, gestión fuera de banda y transporte. No necesitan buscar marcadores.

TWAG: Puerta de Acceso WLAN Confiable

El **TWAG** (Puerta de Acceso WLAN Confiable) trae acceso Wi-Fi confiable al núcleo móvil. Autentica dispositivos Wi-Fi con EAP-AKA/AKA′ contra el AAA/HSS a través de Diameter, asigna a cada cliente autenticado una dirección IP mediante DHCP y ancla sus datos de regreso al núcleo de paquetes a través de un túnel GTP hacia el PGW. Así, un suscriptor en Wi-Fi recibe el mismo APN, políticas y cargos que en la red celular. Su panel de control es el lugar para ver quién está conectado, si las rutas de Diameter y GTP están saludables y para limpiar sesiones individuales.

← Guía de Operaciones

El panel de control es una página de elemento por instancia que se alcanza desde la barra lateral cuando un TWAG se ejecuta en el inventario del sitio. Todo el tráfico pasa a través del proxy de backend de OmniWeb hacia la API del TWAG, por lo que permanece detrás de la única puerta de enlace autenticada. Está organizado en pestañas.

Visión General

La pestaña de inicio es una lectura de salud de pantalla única: **sesiones** activas y totales, **pares Diameter** conectados/desconectados, **suscriptores** aceptados, el número de **puntos de acceso**, conteo de arrendamientos **DHCP**, estado del túnel **GTP** y su dirección PGW, el **modo de autenticación** en uso (por ejemplo, EAP-AKA), **tráfico** agregado hacia adentro y hacia afuera, tiempo de actividad y un **feed de actividad reciente** en vivo de autenticaciones y comienzos/paradas de sesiones.

Sesiones

Cada sesión Wi-Fi autenticada, cada fila muestra la **identidad** del suscriptor (el identificador de acceso a la red), **estado**, **IP** asignada, **MAC** del cliente, **SSID**, **IP NAS** que sirve, **duración** de la sesión y **bytes entrantes/salientes**. Un operador puede **eliminar** una sesión para desconectar forzosamente a un cliente, por ejemplo, para limpiar un dispositivo atascado o que se comporta mal.

Puntos de Acceso

Los puntos de acceso WLAN (dispositivos NAS) actualmente conectados a la puerta de enlace. Cada uno puede ser **eliminado** individualmente cuando un punto de acceso es dado de baja o necesita ser limpiado.

Contabilidad

Las sesiones de contabilidad que el TWAG ha registrado: los registros de uso generados para clientes autenticados. Las sesiones de contabilidad individuales pueden ser **eliminadas**.

Diameter

Las conexiones de pares Diameter al AAA/HSS que llevan autenticación, con conteos conectados y desconectados. Esta pestaña también ofrece una **prueba de Diameter**. Envía una solicitud de autenticación multimedia de prueba (MAR) para confirmar que la ruta de autenticación al AAA/HSS está activa, que es la forma más rápida de probar la conectividad de Diameter cuando las autenticaciones están fallando.

DHCP

Los arrendamientos DHCP que el TWAG ha emitido a clientes Wi-Fi, con la dirección, cliente y estado de arrendamiento para cada uno, para que puedas confirmar que los clientes están siendo direccionados y ver cuánto del grupo está en uso.

Registros

La pestaña de **Registros** muestra en tiempo real la salida de registros del TWAG para solucionar problemas de una puerta de enlace individual sin salir de OmniWeb.

Acciones

Cada acción solicita confirmación primero:

- **Eliminar una sesión**: desconectar forzosamente una sesión Wi-Fi autenticada (pestaña Sesiones, por fila).

- **Eliminar un punto de acceso**: limpiar una entrada de punto de acceso / NAS individual (pestaña Puntos de Acceso, por fila).
- **Eliminar una sesión de contabilidad**: eliminar un registro de contabilidad individual (pestaña Contabilidad, por fila).
- **Prueba de Diameter**: enviar un MAR de prueba para validar la ruta de Diameter al AAA/HSS (pestaña Diameter).

Relacionado

- El **PGW** ancla el plano de usuario del TWAG sobre GTP. Ver los elementos del núcleo de paquetes.
- El **HSS** contiene los datos de autenticación del suscriptor contra los cuales se resuelven las solicitudes de Diameter del TWAG.
- ePDG: el contraparte de Wi-Fi no confiable para llamadas Wi-Fi.

UPF: Función de Plano de Usuario

La **UPF** (Función de Plano de Usuario) es el nodo de reenvío de paquetes del núcleo móvil. Transporta el tráfico real de cada suscriptor: recibe túneles GTP-U de la red de acceso en **N3** (S1-U en el EPC), reenvía paquetes hacia y desde la red de datos, aplica QoS por flujo y contabilidad de volumen, y almacena paquetes de bajada cuando un dispositivo está inactivo. No tiene lógica propia. El plano de control (un **SGW-C** en el EPC sobre **Sxa**, o un **SMF** en un núcleo 5G sobre **N4**) lo programa completamente a través de **PFCP**. El plano de control instala las reglas de detección de paquetes, reenvío, QoS y reporte de uso que describen cómo la UPF maneja el tráfico de cada sesión. El **OmniUPF** de Omnitouch implementa la ruta de reenvío como un **dataplane eBPF/XDP** en el kernel, por lo que las reglas que instala el plano de control se convierten en entradas en mapas eBPF que el programa XDP consulta para cada paquete. OmniWeb presenta las asociaciones y sesiones PFCP de la UPF, el contenido en vivo de los mapas eBPF, estadísticas del dataplane, enrutamiento, buffers de bajada, estado del jardín amurallado y configuración. Accede a los gráficos de rendimiento y tendencias en los paneles de Grafana desde la misma página.

← Guía de Operaciones

La UPF es una página de elemento por instancia que se accede desde la barra lateral cuando se ejecuta en el inventario del sitio, con un selector de instancia donde se despliegan varias y una vista de flota para el estado agregado. Todo el tráfico pasa a través del proxy backend de OmniWeb hacia la API de la UPF, por lo que permanece detrás de la única puerta de enlace autenticada. El enlace de documentación en el encabezado de la página (el botón de ayuda contextual) abre esta página. Está organizada en pestañas.

Selección de flota e instancia

Donde un sitio ejecuta más de una UPF, la **vista de flota** lista cada instancia con su salud de un vistazo. Esta es la forma más rápida de confirmar que todo el plano de usuario está activo antes de profundizar en un nodo.

Desde cualquier pestaña, el **selector de instancia** en el encabezado de la página cambia cuál UPF lee la página. Todo lo que está debajo (sesiones, asociaciones, mapas eBPF, estadísticas) está limitado a la instancia seleccionada, por lo que eliges el nodo una vez y toda la página lo sigue.

Descripción general

Una lectura de salud de pantalla única de la UPF: su estado de **salud**, el número de **asociaciones PFCP** que mantiene con pares del plano de control, el total de **sesiones activas** a través de esos pares, y los **contadores de acción XDP**: cuántos paquetes ha pasado, descartado, redirigido, transmitido o abortado el dataplane, lo que es la confirmación más rápida de que el tráfico realmente está fluyendo. Debajo, cada **par PFCP** se lista con su estado de asociación, conteo de sesiones y cualquier latido perdido, y los **tamaños de los mapas eBPF** muestran la capacidad de los mapas PDR, FAR, QER y URR y el conteo máximo de sesiones. Un cuadro de búsqueda salta directamente a una sesión por **UE IP** o **TEID**, y una acción de **Informe de Nodo** envía una Solicitud de Informe de Nodo PFCP al primer par activo del plano de control.

Sesiones

Cada **sesión PFCP**: el estado de plano de usuario por portadora / por sesión PDU que ha instalado el plano de control. Cada fila está identificada por su **SEID local y remoto** y muestra el **IMSI** de la sesión, **APN/DNN**, la **asociación** (qué par del plano de control la posee), y el conteo de reglas de **detección de paquetes**, **acción de reenvío**, **aplicación de QoS** y **reportes de uso** que lleva. Busca **por UE IP o TEID** para encontrar la sesión que atiende a un dispositivo o túnel específico.

Donde se despliegan varias UPFs, la misma pestaña en la **vista de flota** lista cada sesión PFCP a través de todas ellas en una tabla, con la UPF portadora mostrada contra cada fila. UE IP y TEID se buscan en cada UPF; IMSI y APN/DNN se emparejan en la lista combinada. Abrir una fila va a los detalles de esa sesión en su propia instancia. Una UPF que no se puede alcanzar se nombra encima de la tabla, por lo que una lista corta nunca se confunde con un plano de usuario inactivo.

Detalle de la sesión

Abrir una sesión muestra su estado completo de reglas. Un **mapa de reglas de sesión** dibuja cómo cada **Regla de Detección de Paquetes (PDR)** hace referencia a la **Regla de Acción de Reenvío (FAR)**, **Regla de Aplicación de QoS (QER)** y **Reglas de Reporte de Uso (URR)** que aplica. Haz clic en cualquier nodo para resaltar solo las reglas conectadas a él, para que puedas rastrear el camino de un solo flujo a través del dataplane. Debajo del mapa, cuatro tablas dan el detalle:

- **Reglas de Detección de Paquetes (PDR)**: cómo la UPF clasifica los paquetes entrantes. Esto cubre la dirección (uplink / downlink), la UE IP o TEID entrante que coinciden, los filtros SDF (protocolos y rangos de puertos), y qué FAR, QER y URRs resuelven.
- **Reglas de Acción de Reenvío (FAR)**: qué sucede con los paquetes coincidentes. La acción es **Reenviar**, **Descartar**, **Almacenar** o **Notificar CP**, con los detalles del túnel GTP-U saliente (IP remota y TEID) y la instancia de red. Puedes editar los FAR en su lugar.
- **Reglas de Aplicación de QoS (QER)**: la QoS por flujo. Esto cubre el **QFI**, el estado de **puerta** de uplink y downlink (abierta / cerrada) y los

máximos y **garantizados** de tasas de bits. Puedes editar los QER en su lugar.

- **Reglas de Reporte de Uso (URR)**: los contadores de volumen. Estos son los bytes de uplink y downlink actuales y los últimos reportados y el número de secuencia del reporte, que es lo que la UPF retroalimenta al plano de control para cobro y cuota.

Desde el encabezado de la sesión también puedes **activar o eliminar una redirección de jardín amurallado** para esa sesión específica (ver Jardín Amurallado a continuación).

Asociaciones

Las **asociaciones PFCP**: las relaciones Sxa/N4 que la UPF mantiene con sus pares del plano de control (el SGW-C o SMF). Cada fila muestra la **IP y puerto remotos** del par, su **conteo de sesiones**, si está actualmente **asociado**, el número de **latidos perdidos**, y cuándo se **conectó** o **desconectó** por última vez. Aquí confirmas que el plano de usuario y el plano de control están sincronizados. Aquí también puedes detectar un par cuyos latidos están fallando.

Estadísticas

Los números en tiempo real del dataplane. **Uso de Mapas eBPF** muestra cuán llenos están cada mapa (sesiones, PDR, FAR, QER y URR) como barras de uso versus capacidad que se tornan ámbar y rojas a medida que se acercan a su límite, por lo que puedes ver una UPF acercándose a su capacidad dimensionada antes de que comience a rechazar sesiones. **Estadísticas XDP** desglosa los contadores de paquetes pasados / descartados / redirigidos / TX / abortados, y la sección de **Métricas** presenta los contadores de Prometheus de la UPF como cifras individuales.

Una verificación de capacidad lee el mismo modelo de uso versus capacidad. De un vistazo puedes decir si el recurso limitante es la tabla de sesiones o uno de los mapas de reglas.

Enrutamiento

Las rutas que dirigen el tráfico de suscriptores hacia y desde la UPF. La tabla de **Rutas Activas de UE IP** lista las rutas que la UPF mantiene actualmente para los grupos de IP de UE asignados, y una acción de **Sincronizar Rutas** las reconcilia con el dataplane. Debajo de esto, una **consola FRR** proporciona un terminal vtysh en contexto contra el demonio de enrutamiento de la UPF. Para inspeccionar el estado de enrutamiento, escribe un comando `show` (por ejemplo `show ip route` o `show ip ospf neighbor`), con autocompletado y historial de comandos. Para hacer un cambio, cambia a **modo de configuración**. Así es como la UPF publicita sus grupos de UE en la red circundante sin salir de OmniWeb.

Buffers

Los **buffers de paquetes de bajada**. Cuando llegan datos de bajada para un dispositivo que está inactivo (sin túnel activo), el dataplane mantiene esos paquetes contra el FAR relevante y pide al plano de control que pagine el dispositivo. Una vez que el túnel se restablece, la UPF vacía los paquetes almacenados (este es el lado del plano de usuario de la **Notificación de Datos de Bajada**). La pestaña muestra el **total de paquetes almacenados** y **total de FARs** que mantienen paquetes, los límites de buffer **por FAR** y **total**, y una **búsqueda por ID de FAR** para ver cuántos paquetes está sosteniendo un FAR específico. Los buffers pueden ser **vaciados** individualmente o **borrados** en bloque.

Mapas eBPF

Un navegador directo a los **mapas eBPF** que son el dataplane de la UPF. Estas son las entradas crudas del lado del kernel que el programa XDP consulta para cada paquete, divididas en pestañas:

- **PDR de Uplink**: identificada por TEID entrante, que mapea un túnel a su PDR y FAR.
- **PDR de Downlink**: identificada por UE IP, que mapea el downlink de un suscriptor a su PDR y FAR.
- **FAR**: las acciones de reenvío, con acción decodificada, IP remota, TEID saliente y creación de encabezado externo.
- **QER**: las entradas de QoS, con QFI, estado de puerta y límites de tasa de bits.
- **URR**: los contadores de uso, con volúmenes de uplink/downlink actuales y últimos reportados.

Haz clic en cualquier fila para **editar la entrada del mapa crudo**, que es una herramienta de solución de problemas y reparación de bajo nivel. PFCP

normalmente impulsa los mapas completamente, por lo que editas manualmente una entrada para diagnóstico en lugar de operación rutinaria.

Configuración

Una vista de solo lectura de cómo está configurada la UPF: su identidad de **red** (ID de nodo, dirección y puerto PFCP, puerto API, direcciones N3 y N9), las **características** que tiene habilitadas (FTUP, UEIP, el administrador de rutas y su tipo, y el modo de adjunto XDP: nativo, genérico o descargado), el intervalo de **latidos PFCP**, tiempo de espera y ajustes de reintento, y las direcciones N3/N9 del **dataplane**. Un interruptor de **JSON Crudo** muestra el documento de configuración completo para soporte. Aquí es donde confirmas que una UPF está dimensionada y direccionada como se espera.

Diagnósticos

Ejecuta un **ping desde el nodo UPF** a un host objetivo. Ingresa un objetivo y un conteo de paquetes, y la salida cruda del ping regresa con un veredicto de éxito/fallo. Es una forma rápida de confirmar que la UPF tiene conectividad de red de datos (por ejemplo, a un servidor DNS o puerta de enlace ascendente) desde donde realmente salen los paquetes, sin tener que acceder al nodo.

Jardín Amurallado

El **jardín amurallado**: reenvío restringido para sesiones que deben alcanzar solo un portal cautivo antes de ser autenticadas o autorizadas. Cuando activas una redirección en el SEID de una sesión, reescribe el downlink para que el dispositivo vaya a una **URL de redirección / IP de portal** en lugar de a internet abierto. La pestaña lista cada **redirección activa** con la UE IP, IP del portal, URL de redirección, IP de gNB y los TEIDs involucrados. Para liberar la sesión al reenvío normal, elimina la redirección. Una **lista blanca** de IPs o CIDRs nombra los destinos que una sesión de jardín amurallado aún puede alcanzar directamente (por ejemplo, el portal y sus activos). También puedes activar y eliminar redirecciones por sesión desde la página de detalles de la sesión.

Registros

La pestaña de **Registros** sigue la salida de registro en vivo de la UPF para solucionar problemas de una sola instancia sin salir de OmniWeb.

Paneles de monitoreo

El rendimiento, las tasas de paquetes por interfaz, las tendencias de conteo de sesiones y otras series temporales para la UPF se presentan como paneles de Grafana, accesibles desde la página del elemento. OmniWeb no duplica esos gráficos de forma nativa.

Relacionados

- **SGW-C**: el par de control del EPC que programa esta UPF (como el SGW-U) sobre **Sxa/PFCP** y reenvía tráfico en **S1-U / N3**.
- **PGW-C / SMF**: ancla la conexión PDN y, como el SMF, programa el plano de usuario 5G sobre **N4/PFCP**.

- **MME**: impulsa la configuración de portadoras que finalmente instala las sesiones vistas aquí.
- **SCEF**: transporta pequeños payloads no-IP a través del plano de control y elude deliberadamente este plano de usuario.
- Guía de Operaciones: de vuelta al índice de elementos.