

Dongle MiFi LTE UZ801 — Activation automatique ADB (côté hôte)

Des dongles MiFi LTE Qualcomm bon marché (~10 \$) (`05c6:90b6`, "Android"/UZ801, msm8916) démarrent en **mode RNDIS** avec une interface web à `http://192.168.100.1`. En accédant à `http://192.168.100.1/usbdebug.html`, ils passent en **mode ADB** (et ils démarrent déjà root). Réf : <https://nickvsnetworking.com/adventures-with-a-10-lte-mifi-dongle/>

L'étape d'activation doit être exécutée sur l'**hôte USB** (l'hyperviseur Proxmox), car seulement l'hôte a le lien RNDIS vers `192.168.100.1` — l'agent de téléphone OmniWeb s'exécute dans le LXC non privilégié (CT 102) et atteint le dongle uniquement en tant que périphérique USB une fois qu'il est en mode ADB. Donc, cette automatisation est udev + systemd côté hôte, pas de code d'agent.

Fichiers

- `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
```

Flux : dongle branché (RNDIS) → udev s'active → `mifi-adb-enable.service` → le script active l'interface RNDIS, curl `usbdebug.html` → le dongle redémarre en mode ADB → se réénumère avec l'interface ADB → la règle udev CT-102 (ci-dessous) remet le nœud au conteneur → l'`adb` de l'agent le voit. Lors de la réénumération en mode adb, le script s'exécute à nouveau, détecte l'interface ADB (`ff/42/01`) et se termine — pas de boucle.

Changement udev de passage USB CT-102 (REQUIS)

Le VID Qualcomm du dongle `05c6` doit être remis au conteneur, et le groupe **doit être plugdev (gid hôte 100046)**, pas root du conteneur, sinon l'adb de l'agent (utilisateur `omniweb-agent`, membre de plugdev) ne peut pas ouvrir le nœud. Il en va de même pour les règles du téléphone Android : elles étaient `GROUP="100000"` (root du conteneur) auquel l'agent n'a pas accès — les périphériques ne fonctionnaient que pendant que l'adb détenait le fd depuis le temps d'énumération et étaient abandonnés à chaque réénumération. Corrigé en `GROUP="100046"`.

Dans `/etc/udev/rules.d/99-ct102-android.rules`, toutes les règles de téléphone utilisent `OWNER="100000", GROUP="100046", MODE="0660"`, plus le VID du 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"
```

Ces changements côté hôte sont appliqués en direct dans le laboratoire mais devraient être codifiés dans le rôle ansible d'OmniCore (surveillance/hôte) afin qu'ils survivent à une reconstruction de l'hôte.

AMF : Fonction de Gestion d'Accès et de Mobilité

Le **AMF** est l'ancre du plan de contrôle du cœur 5G. Il termine le signalement **N1** vers l'UE et l'association **N2** (NGAP) à chaque gNodeB. Il gère l'enregistrement et la gestion des connexions : il attache les UEs, les maintient accessibles et les interroge lorsqu'ils sont inactifs. Il possède les **contextes UE** (un par abonné enregistré, indexé par SUPI) et les **associations gNB** (une par radio connectée, indexée par l'association SCTP). Il sélectionne le SMF pour chaque session PDU et relaie les demandes de session entre l'UE et le SMF. Lorsqu'un abonné est sur le réseau, l'AMF est le NF qui sait où il se trouve et comment le joindre.

← Cœur 5G

Dans le tableau de bord

The screenshot displays the AMF Dashboard in the OmniWeb interface. The dashboard is organized into several sections:

- Header:** Includes the OmniWeb logo, the title "AMF Dashboard", and the IP address "10.115.173.238:8443".
- Left Sidebar:** Contains navigation links for Host List, Network Topology, Elements, and various network components (HSS, DRA, OCS, TWAG, MME, SGW-C, PGW-C, UPF, SCEF, MSC, STP, HLR, CAMEL-GW, IP-SMGW, Settings).
- Main Content Area:**
 - Overview Tab:** Displays four health cards: API Health (OK), NRF Registration (registered), NF Status (OK), and License (OK).
 - Statistics Section:** Shows five metrics: Registered Ues (3,847), Connected Ues (2,913), Idle Ues (934), Connected GNBs (3), and Registration Success Rate (99.4%).
 - NF-Specific Status:** Shows "ok".
 - NRF Registration:** Shows "registered".

Le tableau de bord AMF s'ouvre avec les quatre cartes de santé standard : **Santé de l'API**, **Enregistrement NRF** (si l'AMF est actuellement enregistré auprès du NRF), **État NF**, et **Licence**. Chacune interroge à un intervalle. En dessous, il montre les données que possède l'AMF :

- **Liste des UE** : chaque contexte UE que l'AMF détient, indexé par SUPI, avec son état d'enregistrement et de connexion. C'est la vue "qui est attaché en ce moment". Sélectionnez un UE pour ouvrir son contexte détaillé. L'AMF peut également lister les sessions PDU actives d'un UE par SUPI.
- **gNodeBs** : les radios connectées, une ligne par association SCTP. Le tableau décode les valeurs NGAP brutes en **gNB-ID**, **TAC** (zone de suivi), **PLMN**, et **SST** (type de tranche/service). Un opérateur peut donc confirmer quelles cellules sont actives et quelles zones de suivi et tranches elles desservent sans décoder les identifiants à la main. Sélectionnez une ligne pour ouvrir le gNB détaillé par son ID d'association SCTP.
- **Statistiques** : les compteurs en direct de l'AMF (UE enregistrés, gNB connectés, et volumes de signalement), pour une lecture rapide de la

charge et de l'activité.

- **Mode Maintenance** : si l'AMF est en maintenance. Utilisez-le pour vider ou maintenir un nœud pendant un travail planifié.
- **Configuration** : la configuration d'exécution que le service utilise actuellement.

Actions

Le tableau de bord expose des actions pour récupérer d'un état bloqué. Le tableau de bord confirme chacune avant de l'exécuter, car elles effacent l'état en direct :

- **Effacer tous les contextes UE** (en masse) : supprime chaque contexte UE de l'AMF. Utilisez-le en dernier recours pour récupérer un nœud qui détient des contextes obsolètes ou corrompus. Chaque UE affecté doit se réenregistrer.
- **Effacer le cache** (en masse) : efface le cache de découverte NF de l'AMF et les caches UE. Utilisez-le lorsque l'AMF agit sur des données de pair ou de recherche obsolètes, par exemple après qu'un NF a déménagé ou s'est réenregistré.
- **Désenregistrer** (par UE) : désenregistre un seul UE et nettoie son état. Utilisez-le pour supprimer le contexte d'un abonné qui ne se videra pas de lui-même, plutôt que de réinitialiser tout le nœud.

Au-delà des boutons du tableau de bord, l'API OAM de l'AMF expose des contrôles de récupération plus fins qu'un opérateur peut atteindre via le proxy backend :

- **Forcer la déconnexion d'un gNB** : détruit un gNB unique par son ID d'association SCTP. Utilisez-le pour effacer une association radio bloquée ou mal comportée sans toucher aux autres.
- **Forcer la libération d'une session PDU** : libère une session PDU par son identifiant `supi:psi`. Utilisez-le pour supprimer une session qui est bloquée du côté de l'AMF pendant que l'UE reste enregistrée.
- **Désenregistrer ou interroger un UE** : force un UE à se désenregistrer, ou interroge un UE inactif pour le ramener à l'état connecté. Utilisez

l'interrogation pour tester la connectivité. Utilisez la désinscription forcée pour évincer un UE proprement.

Opérations

- **Diagnostics d'exécution** (`/api/oam/diagnostics`) : montre les diagnostics de bas niveau pour le service en cours d'exécution.
- **Utilisation des ressources** (`/api/oam/resources`) : rapporte l'utilisation de la mémoire, des processus et du planificateur de l'exécution pour un contrôle de santé sur le nœud.
- **Pairs** (`/api/oam/peers`) : liste les URI de pairs NF configurés et découverts et les associations SCTP actuelles, afin qu'un opérateur puisse voir avec qui l'AMF communique.
- **Cache de découverte NRF** (`/api/oam/nrf_discovery`) : montre le contenu du cache de découverte : quelles instances NF l'AMF a apprises du NRF.
- **Définir le niveau de journalisation** (`/api/oam/log_level`) : change le niveau de journalisation à l'exécution (un des `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) pour augmenter le détail pendant le dépannage.
- **Forcer la réinscription NRF** (`/api/oam/nrf/reregister`) : réinscrit l'AMF auprès du NRF. Utilisez-le pour récupérer une inscription perdue ou obsolète.

Liens connexes

- **SMF : Fonction de Gestion de Session** : l'AMF sélectionne le SMF et relaie les demandes de session PDU à celui-ci.
- **UDM : Gestion Unifiée des Données** : les données d'abonné que l'AMF utilise lors de l'enregistrement.
- **AUSF : Fonction de Serveur d'Authentification** : authentifie l'UE lors de l'enregistrement au nom de l'AMF.
- **NSSF : Fonction de Sélection de Tranche Réseau** : résout la sélection de tranche pour l'AMF.

- ← Cœur 5G : l'aperçu de tous les tableaux de bord NF.

AUSF : Fonction du Serveur d'Authentification

L'**AUSF** authentifie les abonnés au nom de l'AMF. Lorsqu'un UE se connecte, l'AMF demande à l'AUSF d'exécuter 5G-AKA (ou EAP-AKA') pour cet abonné. L'AUSF travaille avec le **UDM** pour obtenir le matériel de clé, dérive la clé d'ancrage qu'il renvoie à l'AMF, et confirme le résultat de l'authentification. Il maintient une session d'authentification active pour chaque authentification en cours ou établie afin qu'un opérateur puisse suivre son avancement et son résultat et, si nécessaire, l'annuler.

← 5G Core

Dans le tableau de bord

Le tableau de bord de l'AUSF s'ouvre avec les cartes de santé standard en haut (**Santé de l'API**, **Enregistrement NRF** (l'AUSF est-il enregistré auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à intervalle régulier. En dessous se trouvent les sections de données de l'AUSF, lues en direct depuis son API OAM via le proxy OmniWeb :

- **Statistiques** : les propres compteurs de l'AUSF (`AUSF Statistics`), qui donnent une vue en cours de l'activité d'authentification.
- **Sessions d'authentification AUSF actives** : la liste des sessions d'authentification que l'AUSF détient actuellement (`List Active AUSF Authentication Sessions`). Chaque ligne est identifiée par son identifiant de session, permettant à un opérateur de voir d'un coup d'œil quelles authentifications sont en cours ou établies.

Actions

Les deux actions effacent l'état d'authentification et demandent d'abord une confirmation, car elles sont destructrices :

- **Effacer une session d'authentification spécifique** (par ligne) : supprime une seule session d'authentification par son identifiant. Utilisez ceci pour supprimer une session bloquée ou obsolète sans perturber l'authentification des autres abonnés.
- **Effacer toutes les sessions d'authentification** : supprime toutes les sessions d'authentification que l'AUSF détient. Utilisez ceci pour récupérer l'AUSF d'un état bloqué généralisé. Chaque abonné affecté se ré-authentifie lors de sa prochaine tentative.

Opérations

Contrôles OAM standard disponibles sur l'AUSF :

- **Diagnostics** (`/api/oam/diagnostics`) : diagnostics en temps réel pour le service.
- **Ressources** (`/api/oam/resources`) : l'utilisation des ressources du service.

- **Forcer la réinscription NRF** (`/api/oam/nrf/reregister`) : fait en sorte que l'AUSF se réinscrive auprès du NRF, pour récupérer si son enregistrement est devenu obsolète.

Liens connexes

- **AMF : Gestion de l'Accès et de la Mobilité** : demande l'authentification de l'AUSF pour chaque UE se connectant.
- **UDM : Gestion Unifiée des Données** : fournit le matériel de clé que l'AUSF utilise pour authentifier un abonné.
- **← 5G Core** : aperçu du tableau de bord 5GC et des autres NF.

BSF : Fonction de Support de Liaison

Le **BSF** enregistre et résout la liaison entre la session PDU d'un UE et le PCF qui la sert. Lorsqu'une session est établie, le BSF enregistre quel PCF gère la politique pour cette session, identifié par les identifiants de la session : l'adresse IP de l'UE, le DNN et le S-NSSAI. D'autres NFs et fonctions d'application interrogent ensuite le BSF pour découvrir le bon PCF pour une session UE donnée, afin que les demandes de politique atteignent le PCF qui détient déjà le contexte de cette session plutôt qu'un autre arbitraire. Le BSF détient une liaison par session PDU active et les expose, avec des statistiques résumées, pour le suivi.

← 5G Core

Dans le tableau de bord

Le tableau de bord BSF s'ouvre avec les cartes de santé standard en haut (**Santé API**, **Enregistrement NRF** (le BSF est-il enregistré auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à intervalle régulier. En dessous se trouvent les sections de données du BSF, lues en direct depuis son API OAM via le proxy OmniWeb :

- **Liaisons PCF** : la liste des liaisons actives que le BSF détient actuellement (`List all PCF bindings with binding ID, UE IP, DNN, S-NSSAI, PCF FQDN/IP`). Chaque ligne est identifiée par son ID de liaison et montre l'adresse IP de l'UE, le DNN et le S-NSSAI qui identifient la session, ainsi que le FQDN ou l'IP du PCF qui la sert. Cela répond à la question "quel PCF gère la politique pour cette session UE ?" d'un coup d'œil. Sélectionnez une liaison pour ouvrir ses détails complets (`Get detailed PCF binding by binding ID`).
- **Statistiques** : les propres compteurs du BSF (`BSF statistics: total bindings, bindings by DNN`), qui donnent une vue en cours du nombre total de liaisons actives et de leur répartition par DNN.

Actions

Le tableau de bord BSF est orienté vers la lecture et le suivi. Il met en avant les liaisons et les statistiques pour inspection et n'expose pas d'actions destructrices par ligne ou au niveau NF.

Opérations

Contrôles OAM standard disponibles sur le BSF :

- **Forcer la réinscription NRF** (`/api/oam/nrf/reregister`) : fait en sorte que le BSF se réinscrive auprès du NRF, pour récupérer si son enregistrement est devenu obsolète.

Liens connexes

- **PCF : Contrôle de Politique** : le NF auquel chaque liaison pointe. Le BSF est comment les consommateurs trouvent le bon PCF pour une session UE.
- **SMF : Gestion de Session** et fonctions d'application : consommateurs Nbsf qui s'enregistrent et recherchent des liaisons à mesure que les sessions vont et viennent.
- **← 5G Core** : l'aperçu du tableau de bord 5GC et les autres NFs.

CHF : Fonction de Chargement

La **CHF** (Fonction de Chargement) fournit un chargement en ligne et hors ligne convergé pour le cœur 5G. Le SMF l'utilise via l'interface N40 : alors que les sessions PDU transportent du trafic, la CHF gère les quotas d'utilisation, évalue cette utilisation via le moteur de tarification/chargement, et génère les CDR (Enregistrements de Données de Chargement) qui alimentent la facturation et la réconciliation. Son tableau de bord affiche les sessions de chargement en direct, la santé du lien vers le moteur de tarification, et l'historique des CDR complétés. Un opérateur peut alors répondre à la question "un abonné est-il facturé correctement, et le moteur de tarification est-il accessible ?" sans quitter OmniWeb.

← Cœur 5G

Dans le tableau de bord

En haut se trouvent les **cartes de santé** standard (**Santé de l'API**, **Enregistrement NRF** (la CHF est-elle enregistrée auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à un intervalle. En dessous, les sections de données spécifiques à la CHF se rafraîchissent automatiquement :

- **Sessions de chargement actives** : les sessions en direct que la CHF mesure, chacune montrant sa référence de chargement (`chargingDataRef`), l'abonné (SUPI), le DNN, l'utilisation accumulée, et les horodatages de début/mise à jour. C'est l'ensemble de travail de "qui est facturé en ce moment".
- **Statistiques** : une vue récapitulative du nombre total de sessions, de la connectivité au moteur de tarification/chargement, et du volume total facturé.
- **Santé de la connectivité du moteur de tarification** : un contrôle de santé dédié qui confirme que la CHF peut atteindre le moteur de tarification/chargement qui effectue la tarification réelle. Si cela est malsain, la CHF ne peut pas évaluer les sessions et le chargement est en danger.
- **Recherche de CDR complétés** : une vue consultable sur les CDR finalisés, filtrable par SUPI, DNN, et plage de dates, pour confirmer ce que la CHF a enregistré après la fermeture d'une session.
- **Configuration** : la configuration d'exécution de la CHF telle que le service la voit actuellement.

Sélectionnez une session pour ouvrir ses détails complets par référence de données de chargement, ce qui montre l'état complet d'utilisation et de mesure pour cette session.

Actions

- **Abandonner une session de chargement** : termine une session de chargement en cours par sa `chargingDataRef`. Utilisez ceci pour effacer une session bloquée ou orpheline que le SMF ne maintient plus, afin qu'elle cesse de consommer du quota et de l'état de mesure.
- **Rechercher des CDR** : interroge l'historique des CDR complétés par SUPI, DNN, et plage de dates. Utilisez ceci après la fin d'une session pour

confirmer quelle utilisation la CHF a évaluée et enregistrée. Cela prend en charge les demandes de facturation, les enquêtes sur les litiges, ou un contrôle ponctuel que la CHF écrit correctement le chargement.

Opérations

- **Définir le niveau de journalisation** : change la verbosité des journaux de la CHF à l'exécution (urgence, alerte, critique, erreur, avertissement, notice, info, débogage) pour recueillir plus de détails pendant que vous enquêtez sur un problème de chargement, puis revenez à la normale.
- **Forcer la réinscription NRF** : fait en sorte que la CHF se réinscrive auprès du NRF. Utilisez-le pour récupérer si la CHF est tombée hors du registre et que le SMF ne peut plus la découvrir.

Liens Connexes

- **SMF** : le consommateur N40 qui gère le chargement alors que les sessions PDU transportent du trafic.
- **PCF** : le côté politique du contrôle de la politique et du chargement qui régit ce que la CHF mesure.
- Le moteur de tarification/chargement (OCS) : le système en aval par lequel la CHF évalue. La carte de santé de la connectivité du moteur de tarification reflète le lien vers celui-ci.
- **← Cœur 5G** : l'aperçu de tous les tableaux de bord NF.

NRF : Fonction de Répertoire de Réseau

L'ensemble du cœur 5G est construit autour du registre **NRF**. Au démarrage, chaque NF enregistre son **profil NF** auprès du NRF : son type, ses adresses, ses PLMN, les **services** qu'il offre, ainsi que sa capacité et sa priorité. Il découvre ensuite ses pairs en demandant au NRF qui est disponible. Le NRF suit le **statut** de chaque instance enregistrée. Il détient des **abonnements de changement de statut**, afin qu'il puisse informer une NF lorsque l'un de ses pairs dont elle dépend arrive ou part. Il surveille les **battements de cœur** pour expirer les instances qui cessent de se signaler. Lorsque n'importe quelle NF a besoin de trouver une autre, le NRF est la source de vérité pour ce qui est opérationnel et comment y accéder.

← Cœur 5G

Dans le tableau de bord

Le NRF dispose de son propre tableau de bord dédié, plus riche que la page NF standard car il possède le registre que le reste du cœur découvre à travers. Il s'ouvre avec les cartes de santé standard : **Santé API**, **Enregistrement NRF** (si le NRF lui-même est enregistré), **Statut NF**, et **Licence**. Chacune interroge à un intervalle.

Au-dessus des données, il affiche quatre **cartes métriques** qui résument le registre : **Types de NF**, **Total des instances**, **Enregistrées** (avec une barre de pourcentage du total), et **Services** (avec le nombre d'abonnements). En dessous se trouvent les vues principales du NRF :

- **Instances NF enregistrées** : chaque instance enregistrée, regroupée par **type de NF** (AMF, SMF, UDM, PCF, etc.). Le tableau de bord code par couleur chaque carte d'instance par type. La carte montre son statut d'enregistrement, le minuteur de battement de cœur, le nombre de services et le PLMN. Sélectionnez une instance pour ouvrir son **profil NF** complet : l'enregistrement détaillé que le NRF détient, avec un lien **Ouvrir le tableau de bord** vers la propre page de cette NF et un bouton **Désenregistrer**. C'est la vue "quelles NFs sont opérationnelles et sont-elles toutes enregistrées ?".
- **Services enregistrés** : un tableau plat de chaque service que chaque instance annonce, avec ses versions et son statut. Un opérateur peut donc voir quelles capacités le cœur offre actuellement à travers toutes les NFs.
- **Abonnements** : les abonnements de changement de statut NF actuellement détenus. Chacun est une demande permanente d'une NF pour être informée lorsque le statut d'un pair change.
- **Statistiques** : les compteurs en direct du NRF : total des NFs par type, abonnements et demandes de découverte, pour une lecture rapide sur la taille du registre et l'activité de recherche.

Actions

Le tableau de bord expose des actions pour gérer le registre. Le tableau de bord confirme chacune avant de l'exécuter, car cela modifie l'état d'enregistrement en direct :

- **Désenregistrer une instance NF** (par ligne) : supprime l'enregistrement d'une instance du NRF. Utilisez-le pour effacer un enregistrement obsolète ou bloqué pour une seule NF. Cette NF doit ensuite se réenregistrer avant que d'autres NFs puissent la redécouvrir.
- **Désenregistrer toutes les NFs** (en masse) : supprime chaque enregistrement du NRF d'un coup. Utilisez-le en dernier recours pour réinitialiser un registre qui contient des entrées obsolètes. Chaque NF doit ensuite se réenregistrer.
- **Supprimer un abonnement** : supprime un abonnement de changement de statut. Utilisez-le pour effacer un abonnement obsolète ou orphelin laissé par une NF qui n'en a plus besoin.
- **Mettre à jour un profil NF** : corrige le profil d'une instance enregistrée (par exemple sa capacité, sa priorité ou son statut). Les opérateurs peuvent donc ajuster la manière dont le NRF dirige la découverte vers ou loin d'une instance sans désenregistrement.

Opérations

L'API OAM du NRF expose d'autres contrôles auxquels un opérateur peut accéder via le proxy backend :

- **Diagnostics en temps réel** (`/api/oam/diagnostics`) : montre les diagnostics de bas niveau pour le service en cours d'exécution.
- **Utilisation des ressources** (`/api/oam/resources`) : rapporte l'utilisation de la mémoire, des processus et du planificateur du runtime pour un contrôle de santé sur le nœud.
- **Vérification manuelle du battement de cœur** (`/api/oam/heartbeat`) : déclenche une vérification de battement de cœur à la demande pour une instance NF. Cela confirme si la NF est toujours active plutôt que d'attendre son minuteur.
- **Temps de fonctionnement NF** (`/api/oam/nf_uptime/{id}`) : montre le temps d'enregistrement d'une instance et combien de temps elle a été enregistrée, pour confirmer combien de temps une NF a été opérationnelle.
- **Définir le niveau de journalisation** (`/api/oam/log_level`) : change le niveau de journalisation à l'exécution (un des `emergency`, `alert`,

`critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) pour augmenter le détail pendant le dépannage.

- **Forcer la réinscription du NRF** (`/api/oam/nrf/reregister`) : réinscrit le NRF. Utilisez-le pour récupérer une auto-inscription perdue ou obsolète.

Liens connexes

- **AMF : Fonction de Gestion d'Accès et de Mobilité** : s'enregistre auprès du NRF et découvre ses pairs à travers lui, comme chaque NF ci-dessous.
- **SMF : Fonction de Gestion de Session** : découvert à travers le NRF pour la gestion de session.
- **UDM : Gestion Unifiée des Données** : l'une des NFs de données d'abonnés pour lesquelles le NRF détient des enregistrements.
- **PCF : Fonction de Contrôle de Politique** : enregistré auprès du NRF pour la découverte de politique.
- **SCP : Proxy de Communication de Service** : achemine le signal entre les NFs en utilisant les enregistrements et les données de découverte que le NRF détient.
- **← Cœur 5G** : l'aperçu de tous les tableaux de bord NF.

NSSF : Fonction de Sélection de Tranche Réseau

Le **NSSF** sélectionne l(es) instance(s) de tranche réseau et le NSSAI autorisé pour un UE. Lorsque l'AMF gère une demande d'enregistrement ou de tranche, il demande au NSSF de résoudre les S-NSSAIs demandés par l'UE par rapport aux tranches configurées pour ce PLMN. Le NSSF associe chacun à son instance de tranche réseau (NSI) et à l'ensemble AMF qui la sert, et renvoie le NSSAI autorisé que l'UE peut utiliser. Il conserve les définitions de tranche configurées et suit la disponibilité du NSSAI par AMF afin qu'un opérateur puisse raisonner et surveiller la sélection de tranche.

← 5G Core

Dans le tableau de bord

Le tableau de bord NSSF s'ouvre avec les cartes de santé standard en haut (**Santé API**, **Enregistrement NRF** (le NSSF est-il enregistré auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à intervalles réguliers. En dessous se trouvent les sections de données du NSSF, lues en direct depuis son API OAM via le proxy OmniWeb :

- **Tranches** : chaque S-NSSAI configuré, listé avec ses associations NSI, les ensembles AMF qui le servent, et le NSSAI autorisé par PLMN (`List all configured S-NSSAIs with NSI mappings, AMF sets, and allowed NSSAI per PLMN`). C'est la vue autoritaire de la manière dont les tranches demandées se résolvent en instances de tranche et ensembles AMF pour chaque PLMN.
- **Disponibilité NSSAI** : l'état de disponibilité NSSAI par AMF (`Per-AMF NSSAI availability state`), qui montre quelles tranches chaque AMF a signalé qu'il peut actuellement servir.
- **Statistiques** : les propres compteurs du NSSF (`NSSF statistics: total slices, NS selection request counts`), qui donnent une vue en cours du nombre de tranches configurées et du volume des demandes de sélection de tranche.

Une vue de **configuration de tranche** séparée (`Query Slice Configuration`) fait surface la configuration de tranche en temps réel du NSSF pour référence.

Actions

Le tableau de bord NSSF est orienté vers la lecture et la surveillance. Il fait surface les tranches, la disponibilité NSSAI et les statistiques sans actions de contrôle par élément.

Opérations

Les contrôles OAM que le NSSF expose sont :

- **Voir la configuration en temps réel** (`/api/oam/config`) : la configuration en temps réel du NSSF.

- **Forcer la réinscription NRF** (`/api/oam/nrf/reregister`) : fait en sorte que le NSSF se réinscrive auprès du NRF, pour récupérer si son enregistrement est devenu obsolète.

Liés

- **AMF : Gestion de l'Accès et de la Mobilité** : interroge le NSSF pour résoudre les S-NSSAIs demandés en NSSAI autorisé et ensemble AMF servant pour un UE.
- **NRF : Fonction de Référentiel Réseau** : où le NSSF s'enregistre afin que d'autres NF puissent le découvrir.
- **← 5G Core** : aperçu du tableau de bord 5GC et des autres NF.

PCF : Fonction de Contrôle de Politique

Le **PCF** prend les décisions de politique que le reste du cœur 5G applique. Il répond à l'AMF via N15 pour la **politique d'accès et de mobilité (AM)** : les restrictions de mobilité et le RFSP qu'un UE obtient lors de l'enregistrement. Il répond à l'SMF via N7 pour la **politique de gestion de session (SM)** : les règles PCC qui définissent la QoS de chaque session, le contrôle d'accès, le contrôle de facturation et la surveillance de l'utilisation. Le PCF lie les associations de politique SM d'un UE à lui-même via le BSF afin que tout NF puisse trouver le bon PCF pour une session. Le tableau de bord du PCF est l'endroit pour répondre à la question "quelles politiques sont actives, pour quels UEs et sessions, et sont-elles conformes à mes attentes ?" sans quitter OmniWeb. Chaque réponse OAM est enveloppée dans `{status, response}`, et le tableau de bord la déplie pour vous.

[← Cœur 5G](#)

Dans le tableau de bord

En haut se trouvent les quatre cartes de santé standard (**Santé API**, **Enregistrement NRF** (le PCF est-il enregistré auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à un intervalle. Utilisez l'indicateur de sondage dans l'en-tête pour mettre en pause le rafraîchissement ou lire l'heure de la dernière mise à jour. En dessous des cartes se trouve la barre **Actions** (voir ci-dessous), puis les sections de données du PCF, chacune se rafraîchissant automatiquement.

Statistiques : les compteurs en direct du PCF (`GET /api/statistics`), les totaux d'association de politique et les comptes actuels. C'est la lecture la plus rapide pour savoir si le PCF sert activement la politique AM et SM.

Politiques AM : chaque association de politique AM active (`GET /api/am_policy`), une ligne par UE pour lequel l'AMF a une politique AM. C'est la vue du PCF sur la politique de mobilité actuellement appliquée à chaque UE enregistré.

Politiques SM : chaque association de politique SM active (`GET /api/sm_policy`), une ligne par session PDU pour laquelle l'SMF détient une

politique. Sélectionnez une ligne pour ouvrir ses détails (`GET /api/sm_policy/{id}`), qui renvoie les règles PCC complètes sur cette session : les décisions de QoS, de contrôle d'accès, de facturation et de surveillance de l'utilisation que l'SMF applique.

Contexte de Politique : la vue des contextes de politique actifs (`GET /api/policy_context`), les contextes que le PCF détient à travers ses associations AM et SM. Il est utile pour réconcilier ce que le PCF croit être actif par rapport à l'AMF et à l'SMF.

Configuration : la configuration d'exécution du PCF (`GET /api/oam/config`), les paramètres avec lesquels le service fonctionne actuellement.

Actions

Chaque action par ligne demande d'abord une confirmation, car la suppression d'une association active perturbe l'UE ou la session qu'elle affecte.

Supprimer une politique AM : sur n'importe quelle ligne de Politiques AM,

Supprimer efface cette association de politique AM (`DELETE /api/am_policy/{id}`). Utilisez-le pour effacer une politique de mobilité bloquée ou obsolète pour un UE.

Supprimer une politique SM : sur n'importe quelle ligne de Politiques SM,

Supprimer efface cette association de politique SM (`DELETE /api/sm_policy/{id}`). Utilisez-le pour supprimer la politique d'une session qui ne se libérera pas d'elle-même.

Mettre à jour une politique SM : vous pouvez également modifier une association de politique SM. Envoyez `PATCH` ou `PUT /api/oam/sm_policy/{id}` pour mettre à jour les règles PCC sur une politique SM active en place, afin que vous puissiez ajuster la QoS ou les décisions de facturation d'une session sans détruire l'association. Utilisez-le pour réappliquer une politique à une session existante plutôt que de la supprimer et de la recréer.

Opérations

La section Opérations contient les contrôles communs à chaque NF :

- **Diagnostics** (`GET /api/oam/diagnostics`) : diagnostics d'exécution pour le service.
- **Utilisation des ressources** (`GET /api/oam/resources`) : mémoire, processus et planificateurs du service en cours d'exécution.
- **Pairs** (`GET /api/oam/peers`) : les URIs de pairs NF configurés avec lesquels le PCF communique et leur statut de connectivité.
- **Cache de découverte NRF** (`GET /api/oam/nrf_discovery`) : le cache de découverte NRF, ou les URIs NF configurés par lesquels le PCF résout les pairs.
- **Niveau de journalisation** (`POST /api/oam/log_level`) : changez le niveau de journalisation à l'exécution. Choisissez l'un des niveaux d'urgence, d'alerte, critique, erreur, avertissement, notice, info ou débogage.
- **Réenregistrement NRF** (`POST /api/oam/nrf/reregister`) : forcez le PCF à se réenregistrer auprès du NRF, par exemple après qu'un redémarrage du NRF l'ait laissé obsolète.

Liés

- **SMF** : demande une politique SM au PCF via N7 et applique les règles PCC que le PCF renvoie.
- **AMF** : demande une politique AM au PCF via N15.
- **BSF** : la fonction de liaison avec laquelle le PCF enregistre les associations de politique SM afin que tout NF puisse trouver le PCF en service.
- **CHF** : la fonction de facturation. Les décisions de contrôle de facturation du PCF déterminent ce que l'SMF rapporte via N40.
- [← Aperçu du Cœur 5G](#)

SCP : Proxy de Communication de Service

Le **SCP** se situe entre les fonctions réseau du cœur 5G et transporte leur trafic basé sur les services. Plutôt que chaque NF consommateur se connecte directement à chaque producteur, les demandes peuvent être routées via le SCP, qui transmet chaque message à une instance saine du type de NF cible, équilibrant la charge entre les instances et réessayant en cas d'échecs. Il peut effectuer la découverte au nom d'un consommateur (découverte déléguée) et met en cache la connectivité des NF afin que, une fois qu'il connaît un type cible, il dirige les demandes ultérieures sans nouvelle recherche. Le résultat est une communication indirecte : les producteurs et les consommateurs n'ont pas besoin de se connaître ou de maintenir des connexions entre eux, et le SCP gère le routage, l'équilibrage et la fraîcheur du cache entre les deux.

← Cœur 5G

Dans le tableau de bord

Le tableau de bord SCP suit la même mise en page que chaque page NF 5GC. Quatre **cartes de santé** s'étendent en haut (**Santé de l'API**, **Enregistrement NRF** (le SCP lui-même est-il enregistré auprès du NRF ?), **État du NF**, et **Licence**), chacune interrogeant à intervalles réguliers.

Sous les cartes, le SCP présente ses propres données opérationnelles :

- **Santé du NF** : la vue de l'équilibreur de charge sur les NF qu'il proxy, avec des comptes de santé et d'échecs par instance, afin qu'un opérateur puisse voir quelles instances productrices le SCP considère comme accessibles et lesquelles échouent.
- **Cache de Découverte** : le contenu du cache de découverte du SCP, quels types de NF sont mis en cache, leurs TTL, et les taux de réussite/échec du cache. C'est ce qui permet au SCP de diriger les demandes répétées sans redécouverte.
- **Statistiques** : le débit du SCP, le nombre total de demandes proxyées, une répartition des demandes par type de NF cible, et le taux global de réussite du cache.

- **Configuration** : la configuration d'exécution actuelle du SCP.

Chaque section se rafraîchit automatiquement, et les valeurs de type NF sont liées au tableau de bord de ce NF.

Actions

Le tableau de bord SCP n'expose pas de boutons d'action destructeurs au niveau NF ou par ligne. Il proxy le trafic plutôt que de posséder l'état de session ou d'abonné qu'un opérateur pourrait effacer. Son cache, cependant, est gérable : l'API OAM permet à un opérateur de visualiser le cache de découverte et d'expulser une seule entrée obsolète afin que le SCP redécouvre cette cible lors de la prochaine demande (voir **Opérations**). Pour récupérer d'un producteur qui a déménagé ou a été remplacé mais est toujours mis en cache comme accessible, effacez son entrée.

Opérations

L'API OAM du SCP expose les contrôles suivants :

- **Voir / gérer le cache de découverte** : lire le cache de découverte actuel, et supprimer une entrée de cache individuelle par id pour forcer la redécouverte de cette cible.
- **Voir la configuration d'exécution** : lire la configuration en direct du SCP.
- **Définir le niveau de journalisation** : changer la verbosité des journaux à l'exécution. Choisissez l'un des niveaux suivants : `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, ou `debug`.
- **Forcer la réinscription NRF** : faire en sorte que le SCP se réinscrive auprès du NRF. Cela est utile après que le NRF ou le SCP a redémarré et que l'enregistrement est devenu obsolète.

Liens Associés

- **NRF** : le registre que le SCP découvre et avec lequel il se réinscrit.

- AMF, SMF, UDM, AUSF, PCF, CHF, NSSF, BSF : les NF dont le trafic basé sur les services peut être proxyé par le SCP et dont la connectivité est mise en cache.
- ← Cœur 5G : l'aperçu de la section 5GC et la mise en page du tableau de bord partagé.

SMF : Fonction de Gestion de Session

Le **SMF** gère la session PDU. Il établit, modifie et libère chaque session de données de l'UE, attribue à l'UE son adresse IP à partir d'un pool local, et gère le plan utilisateur via N4/PFCP. Il programme le UPF avec les règles de détection de paquets, de transfert et de QoS pour chaque session. Il communique également avec le PCF (N7) pour la politique de session et le CHF (N40) pour la facturation. Utilisez le tableau de bord SMF pour répondre à la question "les sessions sont-elles en cours, le SMF est-il toujours associé à son UPF, et est-il à court d'adresses ?" sans quitter OmniWeb. Le SMF encapsule chaque réponse OAM {status, response}. Le tableau de bord le décompresse pour vous.

← 5G Core

Dans le tableau de bord

En haut se trouvent les quatre cartes de santé standard : **Santé de l'API**, **Enregistrement NRF** (le SMF est-il enregistré auprès du NRF ?), **État NF**, et **Licence**. Chacune interroge à intervalle régulier. Utilisez l'indicateur de sondage dans l'en-tête pour mettre en pause le rafraîchissement ou lire l'heure de la dernière mise à jour. En dessous des cartes se trouve la barre des **Actions** (voir ci-dessous). Ensuite viennent les sections de données du SMF, chacune se rafraîchissant automatiquement.

Statistiques : les compteurs en direct du SMF (`GET /api/statistics`) : totaux d'établissement / modification / libération de session et comptes de sessions actuelles. C'est la lecture la plus rapide pour savoir si le SMF met réellement en place des sessions.

Sessions PDU : chaque session PDU active (`GET /api/pdu_session`), retournée sous la forme `{ pdu_sessions: [...], total }`. Chaque ligne contient à la fois un `sm_context_ref` (un UUID qui identifie de manière unique le contexte SM) et un `pdu_session_id` (le PSI 3GPP, un petit entier qui **n'est pas** unique entre les UEs, puisque chaque UE numérote ses propres sessions à partir d'une base basse). Chaque opération par session (recherche de détails et libération) se base donc sur `sm_context_ref`. L'action **Libérer** par ligne du tableau de bord passe cet UUID plutôt que le PSI. À côté des identifiants, une ligne montre le DNN de la session, l'IP UE attribuée et l'état.

Pool IP : le pool d'adresses à partir duquel le SMF attribue des IPs UE (`GET /api/ip_pool/detail`) : le résumé du pool (sous-réseau, total, comptes alloués et disponibles) plus la liste des IPs actuellement allouées. Ici, vous pouvez voir si le SMF est proche d'épuiser son espace d'adresses.

Association UPF : l'état de la liaison N4/PCF au plan utilisateur (`GET /api/upf`) : si le SMF est actuellement associé à son UPF. Si les sessions échouent à s'établir, vérifiez d'abord cela.

Pairs PCF : l'état d'association des pairs PCF (UPF) (`GET /api/oam/pcf_peers`) : la vue du SMF de chaque UPF avec lequel il s'associe via N4, y compris l'état d'association.

Actions

Chaque action demande d'abord une confirmation. Plusieurs sont destructrices pour les sessions en cours.

Libérer toutes les sessions PDU : détruit chaque session PDU et son état PFCP sur le UPF. Utilisez-le pour ramener le SMF à un état vierge, par exemple après un échange de UPF ou lorsque vous videz un nœud pour maintenance.

Effacer le Cache : efface les caches de session du SMF sans libération de session. Utilisez-le lorsque le tableau de bord ou la vue interne du SMF semble obsolète ou incohérente avec la réalité.

Réassocier PFCP : rétablit l'association PFCP avec le UPF (initié par le SMF). Utilisez-le lorsque l'association UPF a chuté et que de nouvelles sessions ne peuvent pas s'établir.

Réassocier UPF : force une réassociation PFCP avec le UPF **configuré**. L'adresse UPF est pilotée par la configuration. Il n'y a pas d'action add-UPF ou inject-UPF ici. Cela redirige l'association vers le UPF déjà dans la configuration du SMF. En pratique, cela sert le même objectif de récupération que la réassociation PFCP.

Libérer par DNN : tapez un DNN dans le champ **DNN** modifiable (par exemple `internet`). Cela libère **toutes** les sessions sur ce DNN. Utilisez-le pour vider ou réinitialiser un seul réseau de données, par exemple pour forcer les UEs à quitter un APN/DNN, sans toucher aux sessions sur d'autres DNN.

Libération par ligne : sur n'importe quelle ligne de Sessions PDU, **Libérer** détruit cette session et son contexte PFCP sur le UPF. Cela libère par `sm_context_ref`, donc cela cible toujours exactement la session dans cette ligne même si plusieurs UEs peuvent partager le même `pdu_session_id`. Utilisez-le pour supprimer une seule session bloquée.

Opérations

La section Opérations contient les contrôles communs à chaque NF :

- **Diagnostics** (GET /api/oam/diagnostics) : diagnostics en temps réel pour le service.
- **Utilisation des ressources** (GET /api/oam/resources) : mémoire, processus et planificateurs du service en cours d'exécution.
- **Pairs** (GET /api/oam/peers) : les URI de pairs NF configurés avec lesquels le SMF communique (AMF, PCF, CHF, NRF, et ses pairs PFCP UPF via les Pairs PFCP ci-dessus).
- **Niveau de journalisation** (POST /api/oam/log_level) : change le niveau de journalisation en temps réel. Choisissez l'un des niveaux d'urgence, d'alerte, critique, erreur, avertissement, préavis, info ou débogage.
- **Réenregistrement NRF** (POST /api/oam/nrf/reregister) : force le SMF à se réenregistrer auprès du NRF, par exemple après qu'un redémarrage du NRF l'ait laissé obsolète.

Liens connexes

- **AMF** : demande la configuration de session auprès du SMF via Nsmf.
- **PCF** : fournit la politique de session au SMF via N7.
- **CHF** : la fonction de facturation à laquelle le SMF rapporte l'utilisation via N40.
- **UPF** : le pair N4/PFCP du SMF. C'est le plan utilisateur que le SMF programme et associe.
- [← aperçu du 5G Core](#)

UDM : Gestion Unifiée des Données

Le **UDM** est l'autorité des données d'abonnement du cœur 5G. Il gère les profils d'abonnement pour chaque abonné. Il suit quels NFs de service gèrent chaque UE et enregistre l'AMF et le SMF contre un abonné. Il fournit les données d'authentification utilisées pour défier l'UE. Il lit les enregistrements d'abonné sous-jacents depuis le **UDR**, son magasin de soutien, et les met en cache pour un accès rapide. L'**AMF** le consulte lors de l'enregistrement. Le **SMF** le consulte lors de la configuration de session. L'**AUSF** tire son matériel d'authentification de celui-ci. Lorsque d'autres NF ont besoin de connaître le profil d'un abonné ou où le réseau les sert, l'UDM est le NF qui répond.

← Cœur 5G

Dans le tableau de bord

Le tableau de bord UDM s'ouvre avec les quatre cartes de santé standard : **Santé API**, **Enregistrement NRF** (si l'UDM est actuellement enregistré auprès du NRF), **Statut NF**, et **Licence**. Chacune interroge à un intervalle. En dessous, il montre les données que possède l'UDM :

- **Liste UE** : chaque contexte UE que l'UDM détient, indexé par SUPI. C'est la vue "quels abonnés l'UDM sert actuellement". L'UDM peut également retourner un contexte détaillé pour un seul abonné par SUPI. Il montre les enregistrements de NF de service de cet abonné et les données d'abonnement mises en cache.
- **Statistiques** : les compteurs en direct de l'UDM, pour une lecture rapide de la charge et de l'activité.
- **Configuration** : la configuration d'exécution que le service utilise actuellement.

Actions

Le tableau de bord expose des actions pour effacer les données d'abonné mises en cache. Le tableau de bord confirme chacune avant de l'exécuter, car cela supprime l'état en direct :

- **Effacer le cache des abonnés** (en masse) : efface l'intégralité du cache des données d'abonnés. Utilisez-le lorsque l'UDM sert des profils obsolètes, par exemple après que les enregistrements d'abonnement aient changé dans l'UDR et que l'UDM devrait les relire plutôt que de servir ses copies mises en cache.

Au-delà du bouton du tableau de bord, l'API OAM de l'UDM expose un contrôle plus fin auquel un opérateur peut accéder via le proxy backend :

- **Purger le cache d'un UE** (`/api/oam/ue_cache/{id}`) : supprime les données d'abonné mises en cache pour un seul abonné par SUPI. Utilisez-le pour forcer une relecture pour un abonné dont le profil a changé, plutôt que de vider le cache pour tout le monde.

Opérations

- **Diagnostics d'exécution** (`/api/oam/diagnostics`) : montre des diagnostics de bas niveau pour le service en cours d'exécution.
- **Utilisation des ressources** (`/api/oam/resources`) : rapporte l'utilisation de la mémoire, du processus et du planificateur de l'exécution pour un contrôle de santé sur le nœud.
- **Définir le niveau de journalisation** (`/api/oam/log_level`) : change le niveau de journalisation à l'exécution (un des `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) pour augmenter le détail pendant que vous dépannez.
- **Forcer la réinscription NRF** (`/api/oam/nrf/reregister`) : réinscrit l'UDM auprès du NRF. Utilisez-le pour récupérer une inscription perdue ou obsolète.

Liens connexes

- **UDR : Référentiel de Données Unifié** : le magasin de soutien dont l'UDM lit les enregistrements d'abonnés.
- **AUSF : Fonction de Serveur d'Authentification** : tire son matériel d'authentification de l'UDM.
- **AMF : Fonction de Gestion d'Accès et de Mobilité** : consulte l'UDM lors de l'enregistrement et s'enregistre en tant que NF de service.
- **SMF : Fonction de Gestion de Session** : consulte l'UDM lors de la configuration de session et s'enregistre en tant que NF de service.
- **← Cœur 5G** : l'aperçu de tous les tableaux de bord NF.

UDR : Dépôt de données unifié

Le **UDR** est le stockage persistant des données d'abonnement, de politique et d'application qui se trouve derrière le UDM et le PCF. Alors que le UDM et le PCF sont les fonctions réseau frontales avec lesquelles d'autres NF communiquent, le UDR est la base de données qu'ils lisent et écrivent. C'est la source unique de vérité sur l'identité d'un abonné et ce à quoi il a droit. Dans le cœur d'Omnicore, le UDR partage son stockage d'abonnés avec le **HSS**, de sorte qu'un dépôt unifié contient des abonnés 4G et 5G plutôt que deux bases de données parallèles.

← 5G Core

Dans le tableau de bord

Le tableau de bord UDR s'ouvre avec les cartes de santé NF standard en haut (**Santé API**, **Enregistrement NRF** (le UDR est-il enregistré auprès du NRF ?), **État NF**, et **Licence**), chacune interrogeant à un intervalle.

Sous les cartes se trouvent les deux sections de données spécifiques au UDR :

- **Santé HSS** : un contrôle de santé de connectivité qui confirme que le UDR peut atteindre le stockage d'abonnés HSS partagé qu'il représente. Cela répond à la question "la base de données des abonnés est-elle accessible et en bonne santé ?" d'un coup d'œil.
- **Abonnés** : la liste des abonnés tirée du HSS, paginée et consultable par **IMSI**. Sélectionnez un abonné pour retourner le détail complet de cet abonné pour cet IMSI, afin qu'un opérateur puisse confirmer le provisionnement d'un abonné sans quitter OmniWeb.

Actions

Le tableau de bord UDR n'expose aucune action destructive au niveau NF ou par ligne. C'est une vue de lecture et de consultation sur le stockage d'abonnés partagé. Sa valeur réside dans l'interrogation : vérifiez que le stockage est accessible via la section santé HSS, listez les abonnés et explorez le détail complet de n'importe quel abonné par IMSI.

Opérations

Aux côtés des sections de données, le UDR porte les opérations communes à chaque fonction réseau 5GC :

- **Définir le niveau de journalisation** : augmenter ou diminuer la verbosité des journaux d'exécution (`emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`) via `/api/oam/log_level`, pour augmenter les détails pendant que vous diagnostiquez un problème.
- **Forcer la réinscription NRF** : pousser le UDR à se réinscrire auprès du NRF (`/api/oam/nrf/reregister`) si son enregistrement est devenu obsolète.

- **Voir la configuration d'exécution** : inspecter la configuration en direct du UDR via le point de terminaison de configuration OAM.

Liens connexes

- **UDM : Gestion des données unifiée** : la fonction réseau frontale qui sert les données d'abonnement à partir de ce dépôt.
- **PCF : Fonction de contrôle de politique** : lit les données de politique conservées dans le UDR.
- **HSS** : la base de données d'abonnés partagée avec laquelle le UDR s'unifie, de sorte que les abonnés 4G et 5G vivent dans un seul dépôt.
- **← 5G Core** : l'aperçu complet du tableau de bord 5GC.

Référence API (OpenAPI / Swagger)

Le contrôleur d'OmniWeb (backend central) expose une seule API REST derrière le même login JWT qui régit le reste du portail. Cette API est auto-documentée :

- **Swagger UI** : `/api/docs`. Parcourez chaque point de terminaison. Développez une route pour voir sa méthode, ses paramètres de chemin/requête, si elle nécessite un jeton, et son résumé. Cliquez sur **Authorize** et collez un JWT porteur pour essayer des appels en direct contre l'instance en cours d'exécution.
- **Spécification OpenAPI 3** : `/api/openapi.json`. C'est le document lisible par machine. Utilisez-le pour l'importer dans Postman/Insomnia ou pour générer des clients.

[← Retour au Guide des Opérations](#)

Ce qui est documenté

La spécification est **générée à l'exécution** en introspectant la carte des routes en direct, donc elle correspond toujours aux points de terminaison que l'instance en cours d'exécution sert réellement. Aucun fichier maintenu à la main ne peut dériver. Pour chaque route, elle capture :

- la méthode HTTP et le chemin (avec les paramètres de chemin/requête),
- un résumé et une description tirés du code,
- si un **JWT porteur** est requis, et
- le cas échéant, la permission **vue/contrôle** par élément que la route impose.

Les points de terminaison sont regroupés par zone (Auth, Admin, SIM Bank, Remote SIM, APDU, Test Devices, IR.38, RAEX, TAP, etc.) afin que vous puissiez trouver rapidement les routes d'une fonctionnalité.

Obtention d'un jeton

La plupart des points de terminaison nécessitent un jeton porteur. Obtenez-en un avec `POST /api/auth/login` (les mêmes identifiants que vous utilisez pour le portail), puis envoyez-le comme `Authorization: Bearer <token>`. Dans Swagger UI, utilisez le bouton **Authorize** afin que chaque appel "Try it out" porte automatiquement le jeton.

Portée

Cela documente uniquement l'API **contrôleur**. L'agent de périphérique qui fonctionne sur des sites distants ne fait pas partie de cette API : il compose *vers* le contrôleur via un WebSocket et n'expose aucun point de terminaison REST entrant, donc il n'y a rien à appeler directement.

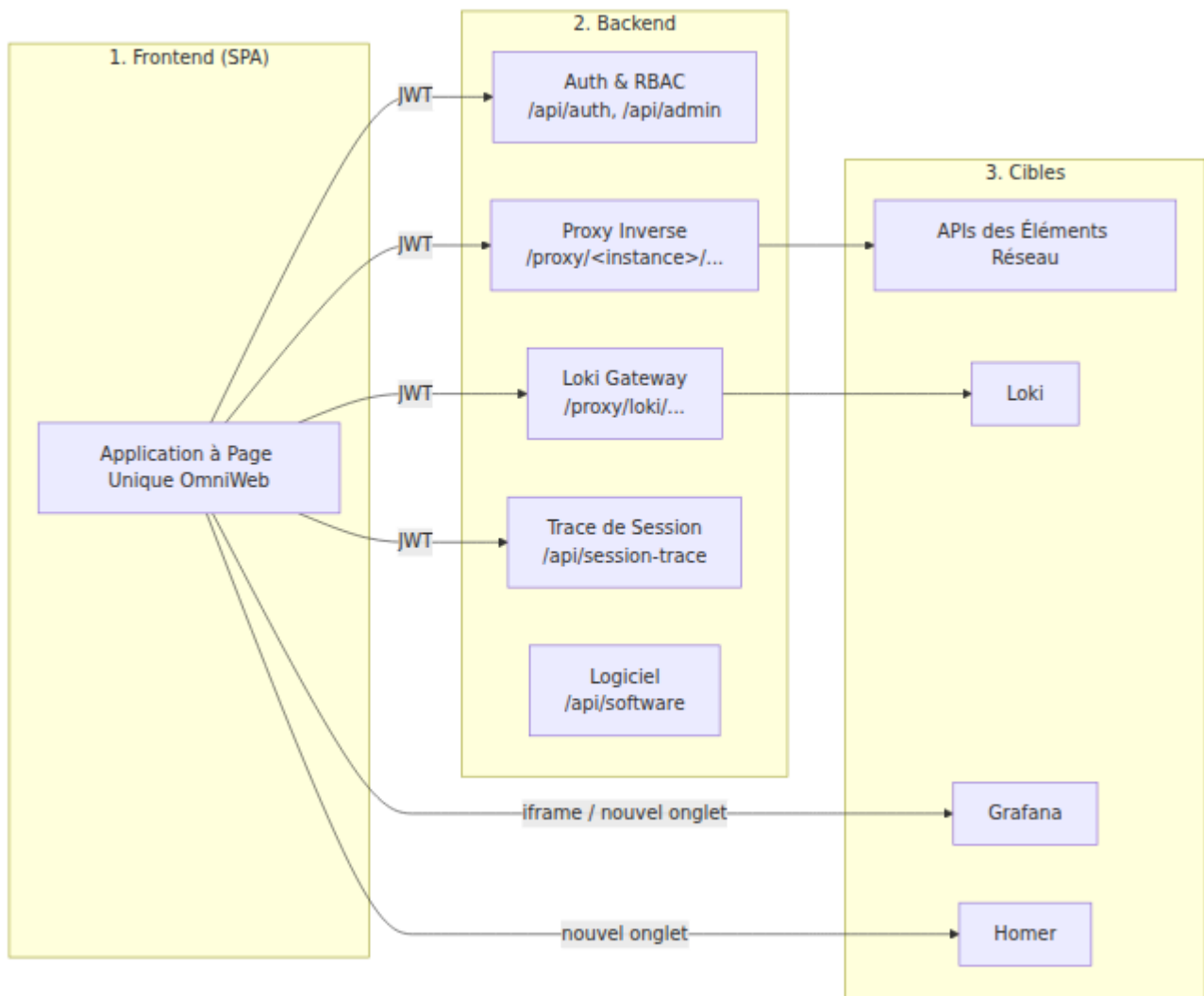
Architecture d'OmniWeb

Cette page explique comment OmniWeb est structuré et comment une seule session de navigateur atteint chaque fonction réseau, Grafana et Loki. Si vous ne lisez qu'une seule page pour comprendre le système, lisez celle-ci.

[← Retour au Guide des Opérations](#)

Composants

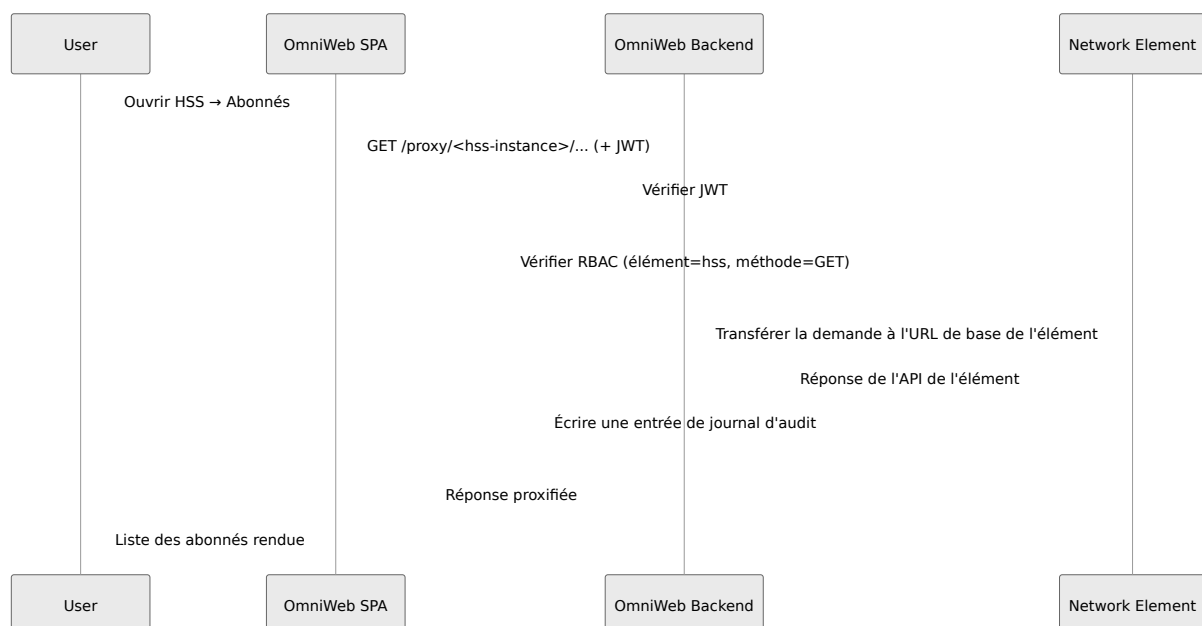
OmniWeb a trois parties mobiles :



Composant	Rôle
Frontend SPA	L'interface utilisateur. Une application web à page unique qui rend les pages d'éléments, la topologie, les journaux, les traces et les tableaux de bord intégrés.
Backend	La couche de sécurité et d'intégration. Elle authentifie les utilisateurs, applique le RBAC et reverse-proxy chaque demande vers la bonne API d'élément, Loki ou Grafana.
Cibles	Les éléments gérés et observés : les propres APIs de gestion des éléments réseau, ainsi que Grafana, Loki et Homer.

Flux de Demande

Chaque demande opérationnelle suit le même chemin. Rien dans le navigateur ne communique directement avec un élément. Cela passe toujours par le backend afin que l'authentification, l'autorisation et l'audit soient appliqués de manière centralisée.



Le chemin du proxy encode l'**ID d'instance**, de sorte qu'OmniWeb puisse gérer plusieurs instances du même type d'élément (par exemple, plusieurs nœuds

HSS) et acheminer chaque demande vers le bon backend.

Le Modèle de Configuration

OmniWeb est **piloté par la configuration**. L'ensemble des éléments, leurs instances et l'emplacement de leurs APIs est déclaré dans un seul fichier : `public/config/omniweb.json`. Le backend le charge au démarrage et le frontend l'utilise pour construire la barre latérale, la topologie et les cibles de proxy.

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

Paramètre	Type	Requis	Par Défaut	Description
<code>type</code>	Chaîne	Oui	-	Type d'élément. Détermine quel module UI rend l'élément. Voir types pris en charge .
<code>displayName</code>	Chaîne	Oui	-	Nom lisible par l'homme affiché dans la barre latérale et la topologie.
<code>description</code>	Chaîne	Non	-	Description plus longue affichée dans les infobulle et les pages de synthèse.
<code>instances</code>	Liste	Oui	-	Une entrée par nœud déployé de ce type. Voir les paramètres d'instance ci-dessous.
<code>defaults.pollIntervalMs</code>	Entier	Non	5000	À quelle fréquence les pages opérationnelles s'actualisent automatiquement en millisecondes.

Paramètre	Type	Requis	Par Défaut	Description
<code>defaults.timeoutMs</code>	Entier	Non	10000	Délai d'attente du proxy pour ce type d'élément. Les APIs lentes (par exemple, OCS) utilisent une valeur plus grande.

Paramètres d'instance :

Paramètre	Type	Requis	Par Défaut	Description
<code>id</code>	Chaîne	Oui	-	Identifiant unique de l'instance. Utilisé dans les URLs (<code>/hss/<id></code>) et dans le chemin du proxy (<code>/proxy/<id>/...</code>).
<code>name</code>	Chaîne	Oui	-	Nom d'affichage pour l'instance.
<code>baseUrl</code>	Chaîne	Oui	-	L'URL de base de l'API de gestion de l'élément. Le proxy transfère les demandes ici. TLS auto-signé est accepté.
<code>tags</code>	Liste	Non	<code>[]</code>	Étiquettes en libre format (par exemple, <code>primary</code> , <code>geo-redundant</code>) affichées sous forme de chips.

Types d'Éléments Pris en Charge

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.

Chaque type est associé à un module UI avec son propre ensemble d'onglets, mais tous sont opérés à travers les mêmes modèles génériques. Voir [Opérations Communes](#).

Comment OmniWeb Communique avec Chaque NF

Le proxy backend est agnostique à l'élément. Il transfère tout ce que le module frontend demande à l'`baseUrl` de l'élément. La *forme* de ces appels dépend de l'API native de l'élément :

Style d'API	Éléments	Remarques
API d'Élément	Toutes les fonctions réseau	L'API de gestion propre de l'élément, proxifiée telle quelle sous <code>/proxy/<instance-id>/...</code> . OmniWeb transfère <code>GET/POST/PUT/PATCH/DELETE</code> comme l'élément s'y attend ; la forme de la demande/réponse est celle que cet élément définit.
Requête de journal (LogQL)	Tous (onglet Journaux)	Routée via <code>/proxy/loki/...</code> vers Loki. Voir Journaux & Tracage .

Comme tout est proxifié, l'ajout d'une instance est purement un changement de configuration dans `omniweb.json`. Aucun changement de code n'est requis pour gérer un autre nœud.

Référence API (OpenAPI)

Un document OpenAPI/Swagger consolidé (`swagger-doc.json`) est fourni avec OmniWeb et décrit les schémas backend et élément (par exemple, enregistrements frontend SMSC et emplacements d'abonnés IMS). C'est un artefact de référence plutôt qu'un serveur API en direct.

Délais d'Attente du Proxy

Chaque type d'élément a un délai d'attente de proxy configurable (`defaults.timeoutMs`). La plupart des éléments répondent bien dans le délai par défaut de 10 secondes. Les éléments avec des requêtes plus lourdes ont plus de marge :

Élément	Délai par Défaut	Pourquoi
La plupart des éléments	10 secondes	Temps de réponse standard de l'API
OCS	180 secondes	Requêtes de notation/CDR sur de grands ensembles de données

Intégration de Surveillance

OmniWeb ne réimplémente pas Grafana, Loki ou Homer. Il les intègre de sorte qu'une seule connexion couvre l'ensemble de la pile :

- **Grafana** est servi derrière la passerelle authentifiée et intégré en tant qu'iframe. Chaque demande est autorisée contre votre connexion OmniWeb, donc il n'y a pas de second mot de passe. Voir [Grafana](#).
- **Loki** est atteint via la passerelle `/proxy/loki/*` du backend, qui exécute des requêtes LogQL au nom de l'opérateur. Voir [Journaux & Tracage](#).
- **Homer** (capture SIP) est détecté automatiquement au démarrage (`/api/homer/status`) et, lorsqu'il est présent, s'ouvre dans un nouvel

onglet. Il est également autorisé contre votre connexion OmniWeb.

Référence d'Environnement

Les points de terminaison d'intégration backend sont configurés via des variables d'environnement :

Variable	Par Défaut	Description
GRAFANA_URL	http://localhost:3000	URL de base de l'instance Grafana à laquelle OmniWeb se connecte.
LOKI_URL	http://localhost:3100	URL de base de l'instance Loki utilisée pour les journaux et le traçage.
LDAP_URI	ldap://localhost:389	Serveur OpenLDAP pour la synchronisation des utilisateurs/clés SSH (optionnel).
LDAP_BASE_DN	dc=omniweb,dc=local	DN de base LDAP.
LDAP_ADMIN_DN	cn=admin,dc=omniweb,dc=local	DN de liaison pour les écritures LDAP.
LDAP_ADMIN_PASSWORD	omniweb-admin	Mot de passe de liaison LDAP (changez cela).
AUDIT_API_KEY	omniweb-audit-key	Secret partagé pour les

Variable	Par Défaut	Description
		rappels d'audit de connexion SSH (changez cela).

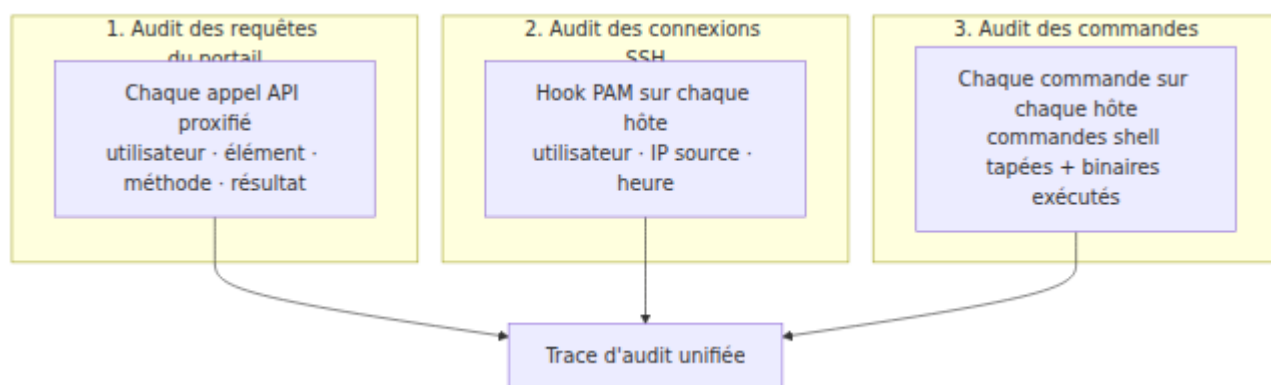
Voir [Authentification & Contrôle d'Accès](#) pour les détails LDAP/SSH et d'audit.

Journal d'Audit

Parce qu'OmniWeb est la seule passerelle vers le réseau, c'est aussi le seul endroit où l'activité peut être enregistrée. L'audit dans OmniWeb a **trois couches** qui, ensemble, répondent à la question "qui a fait quoi, où" à la fois à travers le portail et les hôtes qu'il gère.

[← Authentification & Contrôle d'Accès](#) · [← Guide des Opérations](#)

Les Trois Couches



Couche	Capture	Où cela apparaît
Audit des requêtes du portail	Chaque action effectuée <i>via</i> OmniWeb	Paramètres → Audit
Audit des connexions SSH	Chaque connexion SSH à <i>un hôte géré</i>	Paramètres → Audit (via rappel d'hôte)
Audit des commandes	Chaque commande <i>exécutée sur un hôte</i> (tapée + exécutée)	Paramètres → Commandes

Audit des Requêtes du Portail

Chaque requête qui passe par le proxy OmniWeb est enregistrée, qu'elle ait réussi, échoué ou été rejetée par **RBAC**. Chaque entrée capture :

- L'**utilisateur** qui a fait la requête.
- Le **type et l'instance d'élément** ciblés.
- La **méthode HTTP** (qui indique s'il s'agissait d'une vue, d'un changement ou d'une suppression).
- Le **résultat** (code d'état).
- L'**horodatage**.

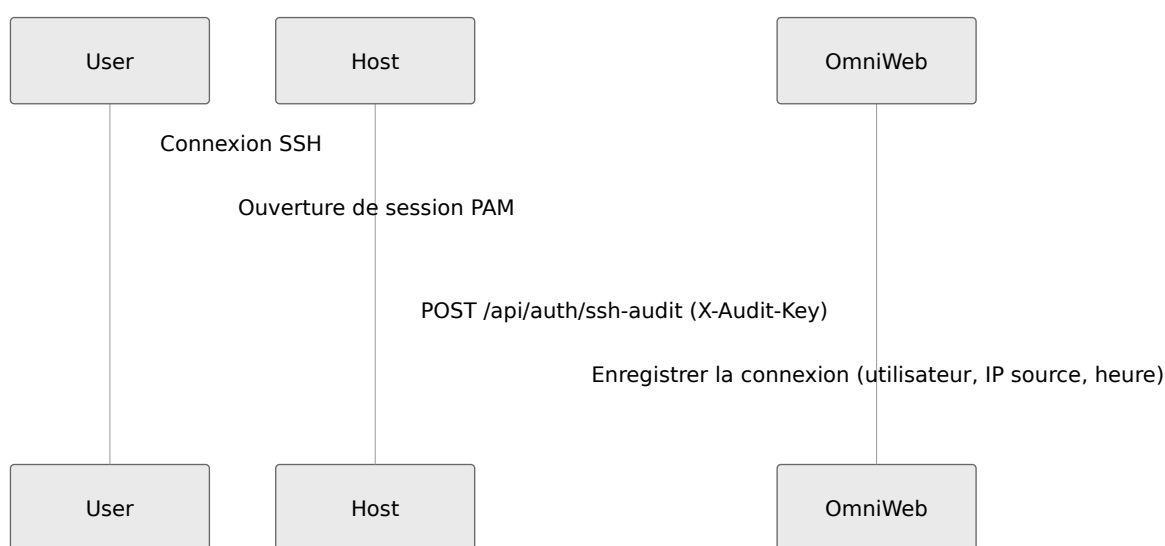
Cela donne un enregistrement complet de qui a changé quoi, où et quand, à l'intérieur du portail. Cela se trouve sous **Paramètres → Audit**. Étant donné que les lectures (**GET**), les écritures (**POST/PUT/PATCH**), et les suppressions sont toutes distinguables par méthode, le journal d'audit fait également office d'historique des changements pour le réseau.

La Trace d'Audit (Paramètres → Audit) : chaque action avec l'utilisateur, le type d'événement, l'élément/instance, la méthode HTTP, le résultat et l'IP source.

Notez le `DELETE` refusé (403), les événements `permission_changed` et `ssh_login` aux côtés des requêtes API ordinaires. Filtrez par type d'événement, utilisateur, élément ou plage de dates.

Audit des Connexions SSH

Les hôtes peuvent signaler les connexions SSH à OmniWeb afin que l'accès à l'hôte apparaisse dans la même vue d'audit que l'activité du portail. Un petit hook PAM sur chaque hôte appelle OmniWeb lorsqu'une session s'ouvre, signalant le nom d'utilisateur, l'IP source et les détails du service.



Le rappel est authentifié avec un secret partagé afin que seuls les hôtes de confiance puissent écrire des entrées d'audit :

Variable	Par défaut	Description
<code>AUDIT_API_KEY</code>	<code>omniweb-audit-key</code>	Secret partagé que le hook PAM de l'hôte présente (en tant que <code>X-Audit-Key</code>) lors du signalement d'une connexion. Changez cela , et définissez la valeur correspondante sur chaque hôte.

Avec cela en place, chaque connexion SSH à un hôte géré apparaît sous **Paramètres → Audit** aux côtés des actions du portail, reliant l'activité d'une

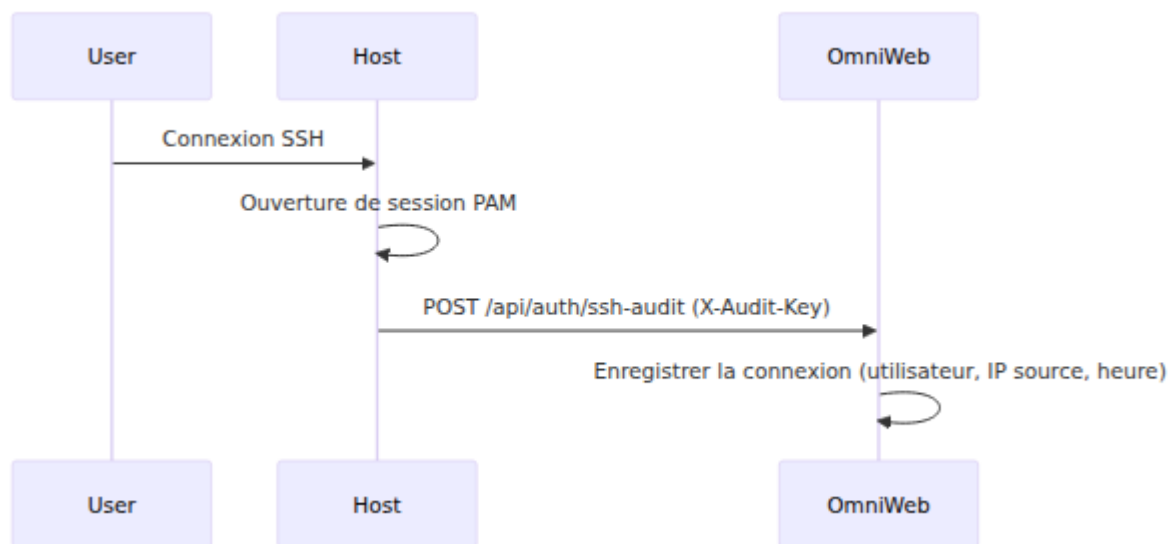
personne sur le portail et l'hôte.

Audit des Commandes

Pour une visibilité au niveau des commandes sur les hôtes, OmniWeb collecte **deux flux complémentaires**, tous envoyés à Loki et consultables sous **Paramètres → Commandes** avec un commutateur de source :

Source	Capture	Flux Loki
Commandes tapées	Les lignes de commande exactes qu'un utilisateur tape dans un shell interactif, y compris les commandes intégrées au shell comme <code>echo</code> , <code>cd</code> , <code>export</code>	<code>job="cmdaudit"</code>
Exécutions de binaires	Chaque binaire qui a réellement été exécuté sur l'hôte (scripts, outils, automatisation)	<code>job="auditd"</code>

Aucun ne remplace l'autre : les intégrées n'exécutent jamais un binaire séparé, donc seul le flux des commandes tapées les voit ; et l'automatisation/scripts qui ne se trouvent jamais à un prompt interactif n'apparaissent que dans le flux d'exécution de binaire. Ensemble, ils couvrent *ce qu'une personne a tapé* et *ce qui a réellement été exécuté*.



Les **commandes tapées** sont capturées par un hook léger de shell interactif qui enregistre chaque commande qu'un utilisateur exécute (avec utilisateur, répertoire de travail et TTY). C'est la couche qui capture les intégrées qu'un traceur de binaire ne peut pas voir structurellement.

Les **exécutions de binaires** proviennent d'un agent hôte léger qui enregistre chaque binaire exécuté sur l'hôte. Comme il fonctionne dans l'espace utilisateur, il fonctionne à l'intérieur des conteneurs LXC sans support d'audit du noyau. Chaque entrée capture :

Champ	Signification
<code>login</code>	L'utilisateur qui s'est initialement connecté ; survit à <code>sudo/su</code> , donc les changements de privilèges ne cachent pas qui agit
<code>uid</code>	UID effectif sous lequel la commande a réellement été exécutée
<code>filename</code>	Le binaire qui a été exécuté
<code>cwd</code>	Répertoire de travail au moment de l'exécution
(après <code>l:)</code>	La ligne de commande complète

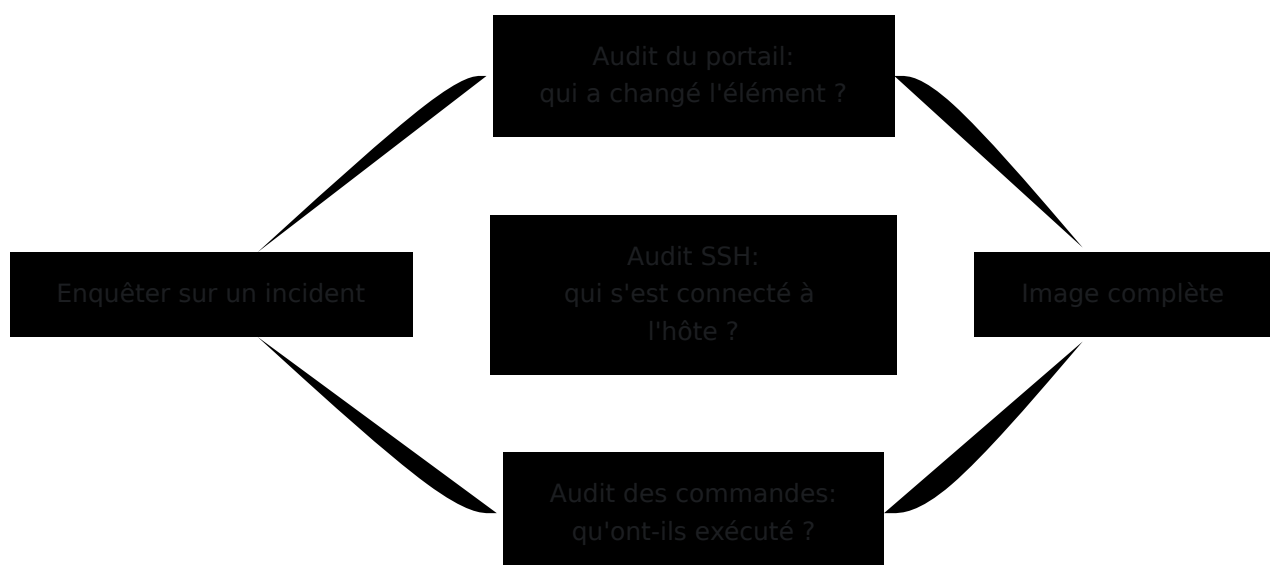
Une entrée d'exécution représentative :

```
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 vue **Paramètres** → **Commandes** par défaut au flux de commandes tapées et vous permet de filtrer par hôte, de rechercher par utilisateur ou commande, et de suivre en direct l'activité à travers la flotte, avec le commutateur de source pour passer à la vue d'exécution de binaire brute lorsque vous souhaitez voir exactement ce qui a été exécuté.

Remarque : les flux de commandes sont un outil de visibilité pour l'opérateur capturé dans l'espace utilisateur. Un utilisateur root déterminé peut les contourner ; l'audit au niveau du noyau est l'étape de durcissement si vous avez besoin d'une capture non contournable. Pour l'enregistrement structuré et pertinent pour la sécurité (connexions, changements de permissions, refus), comptez sur l'**Audit du Portail** et l'**Audit des Connexions SSH** ci-dessus, qui sont écrits dans la propre base de données d'OmniWeb.

Comment les Couches S'Intègrent



- Un changement de configuration effectué **via OmniWeb** → audit des requêtes du portail.

- Un changement effectué **manuellement sur un hôte** → audit des connexions SSH (qui est entré) + audit des commandes (ce qu'ils ont fait).

Ensemble, ils ne laissent aucun angle mort entre "changé dans l'UI" et "changé sur la machine".

Liens Connexes

- [Journaux & Traçage des Abonnés](#) : l'explorateur de journaux général derrière les flux de commandes.
- [Connexion par Clé SSH](#) : le côté accès de l'activité des hôtes.
- [RBAC](#) : les permissions dont l'utilisation est enregistrée par l'audit du portail.

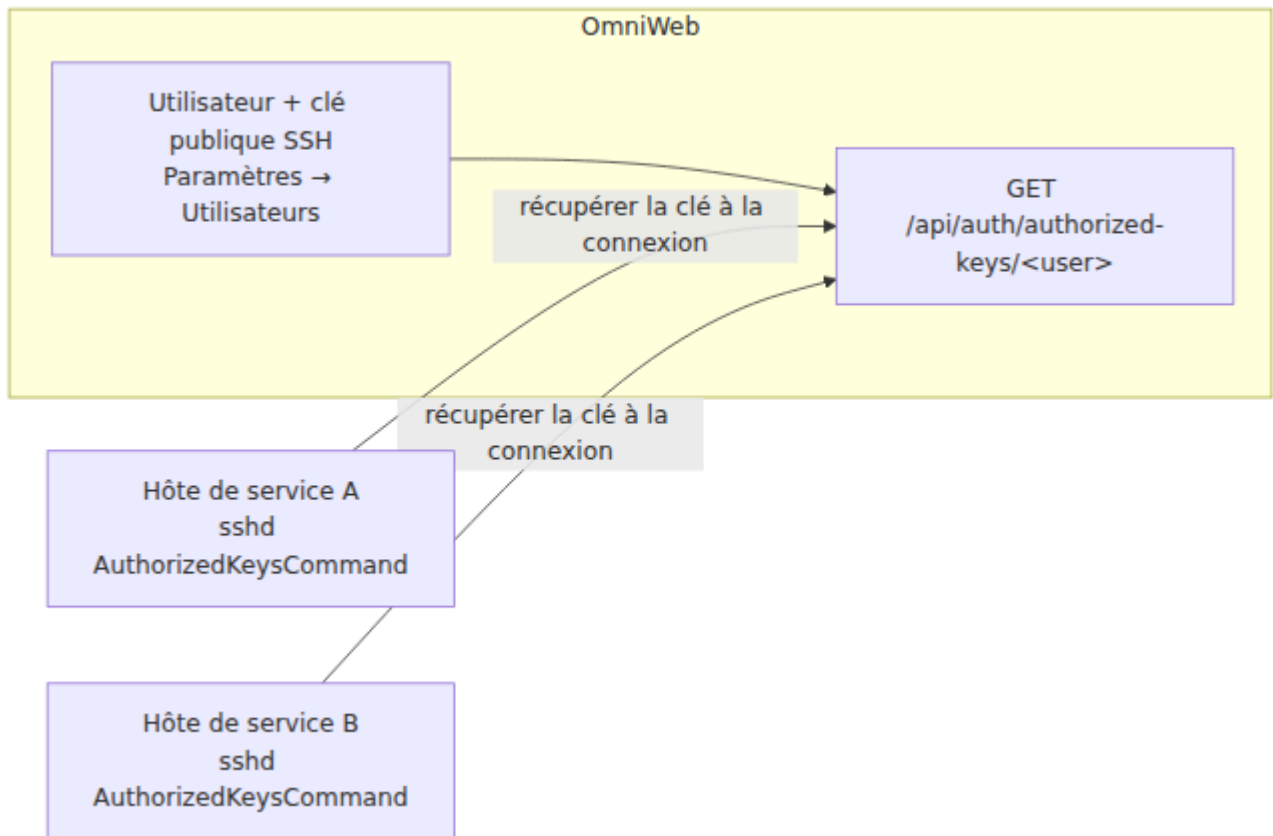
Connexion par clé SSH (Accès aux hôtes)

Le contrôle d'accès d'OmniWeb s'étend au-delà du portail vers les **hôtes** qui exécutent le réseau. Chaque utilisateur peut posséder une **clé publique SSH**, et les hôtes gérés récupèrent ces clés **en direct depuis OmniWeb** au moment de la connexion. Ainsi, OmniWeb est le seul endroit pour gérer *qui peut SSH où*, et, combiné avec **l'audit logging**, qui l'a réellement fait.

Il n'y a pas de serveur de répertoire à exécuter et pas de fichiers `authorized_keys` par hôte à maintenir. (Cela remplace un ancien design de synchronisation OpenLDAP ; le répertoire est disparu, et les clés sont servies à la demande via HTTPS.)

[← Authentification & Contrôle d'accès](#) · [← Guide des opérations](#)

Ce que cela fait



Vous donnez à un utilisateur une clé publique SSH dans OmniWeb une seule fois. Chaque `sshd` d'hôte géré est configuré pour demander à OmniWeb la clé de cet utilisateur **au moment de la connexion** (via `AuthorizedKeysCommand` d'OpenSSH). Ajoutez une clé dans OmniWeb et l'utilisateur peut SSH vers chaque hôte inscrit ; désactivez l'utilisateur et cet accès disparaît partout lors de sa **prochaine** tentative de connexion, sans synchronisation, sans dérive, et sans fichiers de clés à nettoyer.

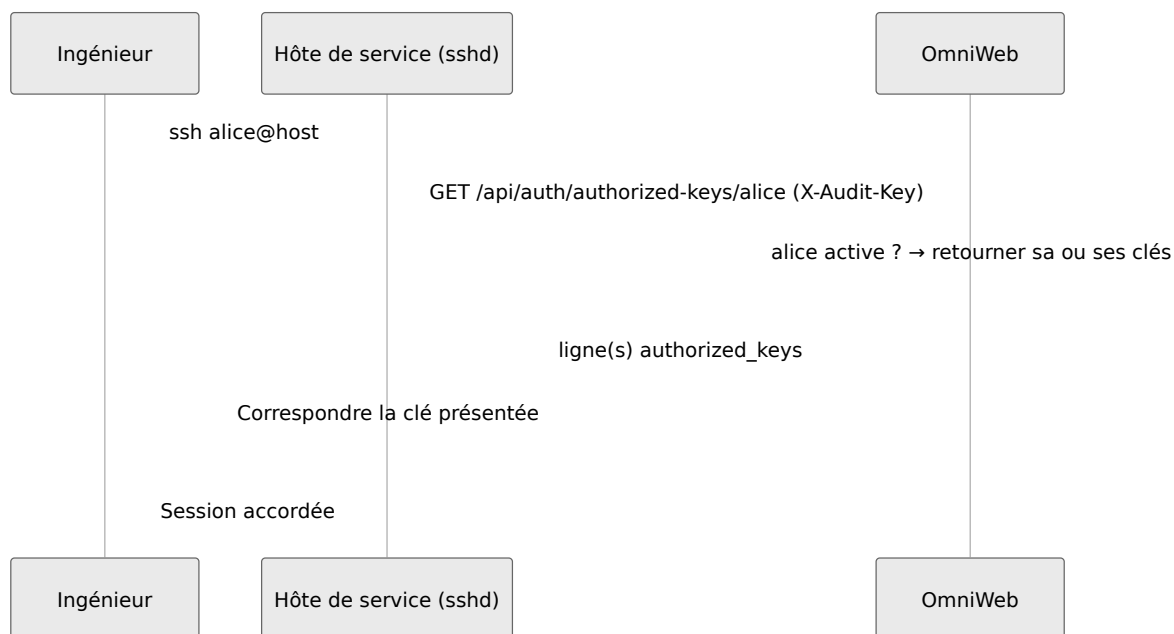
Définir la clé d'un utilisateur

Les clés sont gérées dans **Paramètres → Utilisateurs**, le même écran qui gère les comptes du portail, RBAC, et l'état actif/désactivé. Chaque ligne d'utilisateur indique si une clé SSH est configurée ; créez ou éditez un utilisateur pour y coller une clé.

Paramètres → Utilisateurs : chaque utilisateur avec une indication si une clé publique SSH est configurée. La clé que vous collez ici est celle qui accorde l'accès à l'hôte ; il n'y a nulle part ailleurs pour la maintenir.

Comment les hôtes l'utilisent

Chaque hôte géré exécute un petit helper intégré dans `sshd` comme son `AuthorizedKeysCommand`. Lorsque quelqu'un se connecte, `sshd` exécute le helper, qui récupère les clés autorisées de cet utilisateur depuis OmniWeb via HTTPS et les renvoie pour la correspondance :



Propriétés clés de ce flux :

- **En direct** : la clé est récupérée par connexion, donc les changements prennent effet immédiatement.
- **Utilisateurs actifs uniquement** : OmniWeb ne retourne que les clés pour les utilisateurs **actifs**. Lorsque vous désactivez ou supprimez un utilisateur dans OmniWeb, cela refuse leur prochaine connexion sur chaque hôte à la fois. C'est le bouton de révocation.
- **Pas d'énumération** : un utilisateur inconnu ou désactivé, ou un sans clé, retourne un résultat vide. La connexion ne trouve tout simplement pas de clé et est refusée, donc le point de terminaison ne fuit pas les noms d'utilisateur existants.
- **Survit à une panne d'OmniWeb** : le helper met en cache le dernier bon résultat par utilisateur sur l'hôte, donc une brève panne d'OmniWeb ne verrouille pas tout le monde.

Le compte lui-même (l'utilisateur Unix, le répertoire personnel, le shell) est provisionné par la gestion de configuration aux côtés du helper `sshd`. OmniWeb possède **l'identité et les clés**, et l'automatisation de la flotte possède **l'existence du compte** sur chaque hôte.

Configuration

Le point de terminaison de service de clés est protégé par le même secret partagé que le **callback d'audit** :

Variable	Par défaut	Description
<code>AUDIT_API_KEY</code>	<code>omniweb-audit-key</code>	Secret partagé que le helper <code>AuthorizedKeysCommand</code> de chaque hôte présente (en tant que <code>X-Audit-Key</code>) lors de la récupération des clés. Changez ceci , et définissez la valeur correspondante sur chaque hôte.

Parce qu'OmniWeb est la seule chose qui devrait être interrogée et que le helper s'exécute sur des hôtes de confiance, le point de terminaison est servi via HTTPS et le secret est une seconde porte sur le chemin réseau.

Pourquoi cela importe

- **Un seul endroit pour accorder/révoquer l'accès SSH** à l'ensemble de la flotte : l'état actif de l'utilisateur *est* son accès à l'hôte.
- **Pas de fichiers de clés éparpillés** dérivant hors de synchronisation sur des hôtes individuels, et pas de serveur de répertoire à faire fonctionner et à sauvegarder.
- **Une seule identité** liant l'accès d'une personne au portail, son accès SSH, et, à travers **l'audit logging**, son activité enregistrée.

Liens connexes

- **Audit Logging** : enregistrer les connexions SSH et chaque commande exécutée sur les hôtes.

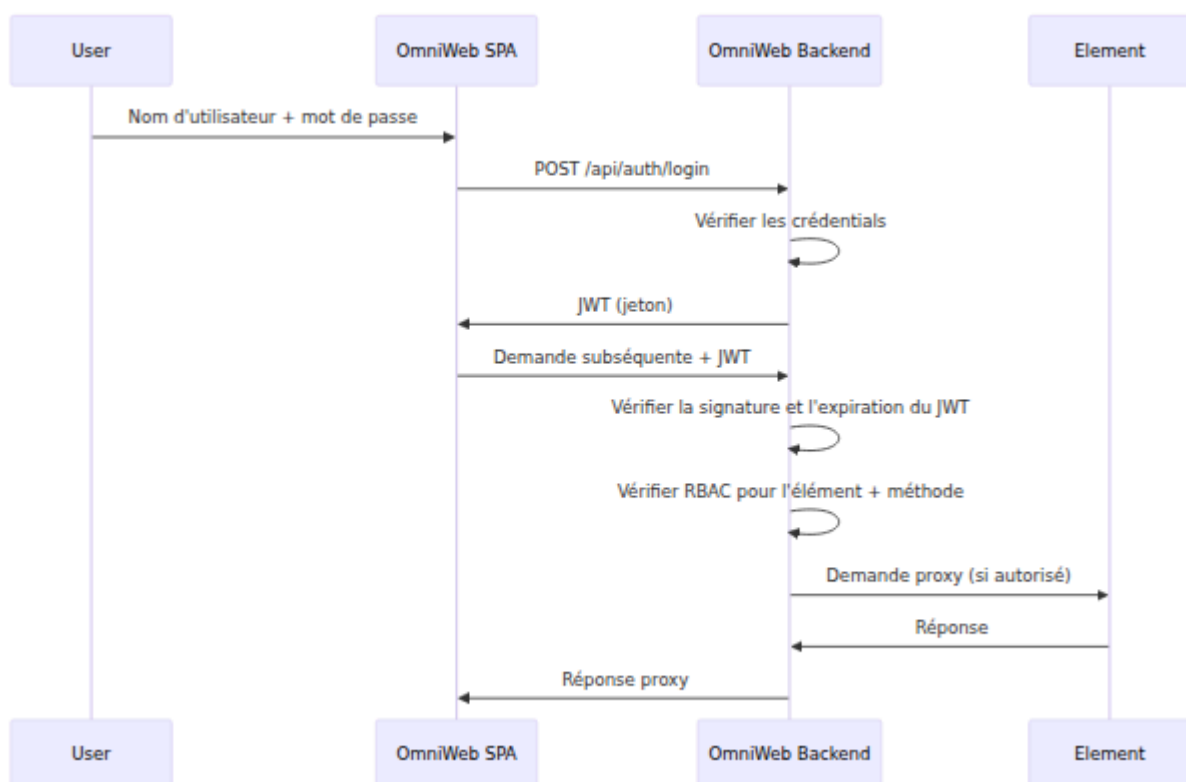
- **RBAC** : contrôler ce que les mêmes utilisateurs peuvent faire *à l'intérieur* d'OmniWeb.

Connexion & Sessions JWT

OmniWeb authentifie les opérateurs avec un nom d'utilisateur et un mot de passe et délivre un **JSON Web Token (JWT)**. Ce jeton prouve qui vous êtes à chaque demande subséquente. Il est crucial que ce soit la *même* credential qui autorise Grafana, Loki et Homer intégrés. Une connexion couvre l'ensemble de la pile.

← [Authentification & Contrôle d'Accès](#) · ← [Guide des Opérations](#)

Flux de Connexion



Le jeton est délivré par `POST /api/auth/login`. Une fois obtenu, le SPA le présente à chaque appel API, et le backend vérifie la signature et l'expiration avant de faire quoi que ce soit d'autre.

L'écran de connexion. S'authentifier ici permet d'obtenir le JWT qui régit l'ensemble de la pile : APIs des éléments, Loki, Grafana et Homer.

Comment le Jeton est Transporté

Le backend accepte le JWT à trois emplacements, ce qui permet au même jeton de fonctionner pour les appels API XHR, les navigations dans le navigateur et les iframes intégrées :

Emplacement	Utilisé pour
En-tête d'autorisation	Requêtes API standard (XHR/fetch) depuis le SPA
Cookie (<code>access_token</code> , <code>HttpOnly</code>)	Navigations dans le navigateur et contenu intégré (iframe Grafana, onglet Homer)
Chaîne de requête	Cas où ni un en-tête ni un cookie ne peuvent être définis

Le cookie est **HttpOnly** (non lisible par JavaScript) et utilise `SameSite=Lax`, ce qui protège le jeton contre le vol via l'accès par script inter-sites tout en permettant les navigations de niveau supérieur vers les outils intégrés.

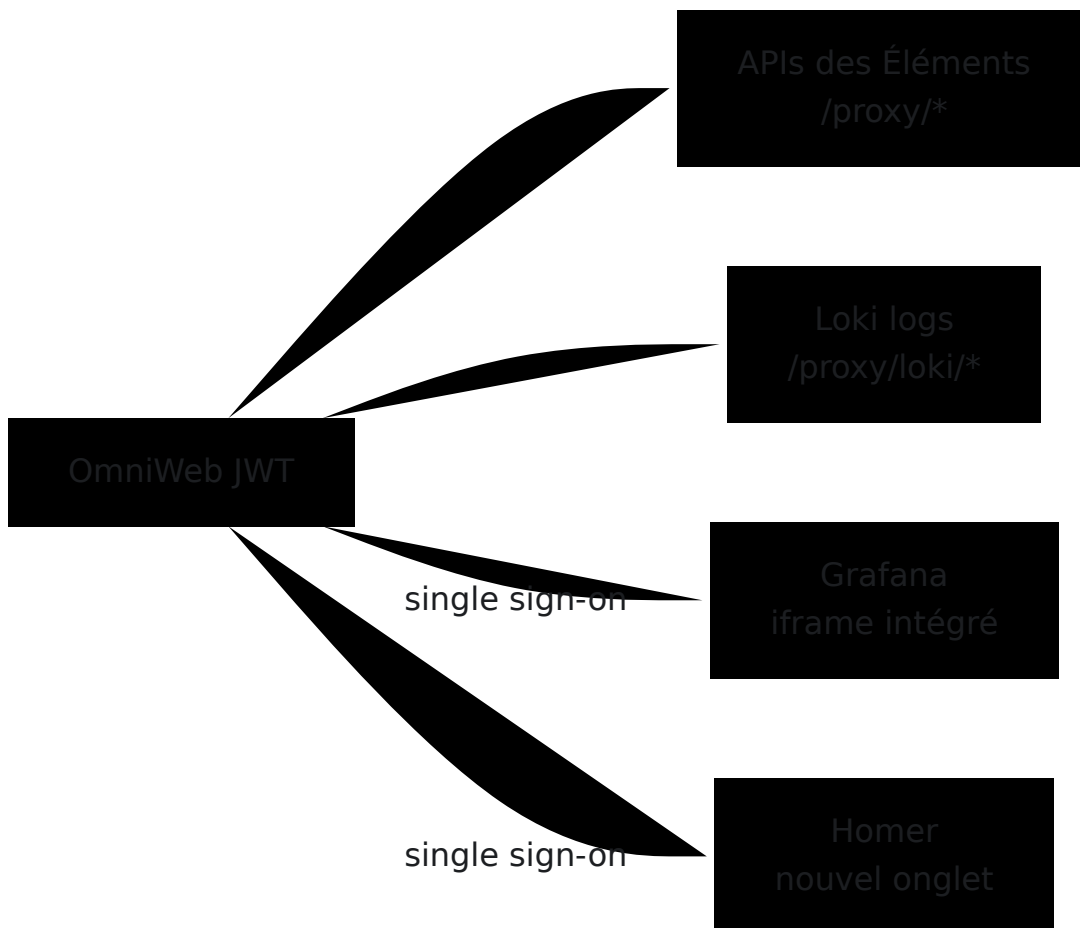
Durée de Vie du Jeton

Le jeton d'accès a une expiration configurable, **24 heures par défaut** (`JWT_ACCESS_TOKEN_EXPIRES`, en secondes). Lorsqu'il expire, l'opérateur est renvoyé à l'écran de connexion et se ré-authentifie. Il n'y a pas de session silencieuse indéfinie ; la durée de vie est une limite de sécurité délibérée.

Paramètre	Par défaut	Description
<code>JWT_ACCESS_TOKEN_EXPIRES</code>	<code>86400</code> (24 h)	Durée de vie du jeton d'accès en secondes. Réduisez-la pour des sessions plus strictes ; augmentez-la pour moins de reconnections.
<code>JWT_SECRET_KEY</code>	<i>(généré)</i>	Secret utilisé pour signer et vérifier les jetons. À définir explicitement en production afin que les jetons survivent à un redémarrage du backend et soient cohérents entre les instances.

Une Connexion, Toute la Pile

Le même JWT autorise les outils de surveillance intégrés, donc les opérateurs ne se connectent jamais deux fois :



- **APIs des Éléments et Loki** sont atteints via le proxy backend, qui vérifie le JWT directement.
- **Grafana et Homer** sont atteints via la passerelle authentifiée, qui vérifie votre connexion OmniWeb avant de faire le proxy, sans second mot de passe. Voir [Grafana](#) et [Homer](#).

C'est pourquoi une seule session OmniWeb régit toute la surface opérationnelle : tableaux de bord, journaux, traces et gestion des éléments reposent tous sur le même jeton.

Première Connexion & Changement de Crédentials

Un déploiement frais est livré avec un compte administrateur par défaut (`admin` / `admin`). **Changez cela immédiatement** après la première connexion, via les paramètres. Le défaut existe uniquement pour démarrer le système et ne doit pas survivre en production.

Déconnexion & Expiration

Se déconnecter rejette le jeton. Un jeton expiré ou invalide entraîne le rejet de la prochaine demande et le SPA retourne à l'écran de connexion. Comme les actions sur les éléments ne sont jamais effectuées que par un appel proxy authentifié et vérifié par RBAC, une session expirée ne peut jamais effectuer une action privilégiée.

Liens Connexes

- [Contrôle d'Accès Basé sur les Rôles](#) : ce qu'un utilisateur connecté est autorisé à faire.
- [Journalisation d'Audit](#) : chaque action authentifiée est enregistrée.

Contrôle d'accès basé sur les rôles (RBAC)

Être authentifié indique à OmniWeb *qui* vous êtes. Le RBAC détermine *ce que vous pouvez faire*. L'accès est accordé avec une grande précision, **par type d'élément, par méthode HTTP**, ce qui correspond directement aux opérations réelles qu'un opérateur effectue : visualiser, modifier ou supprimer.

[← Authentification & Contrôle d'accès](#) · [← Guide des opérations](#)

Niveaux de permission

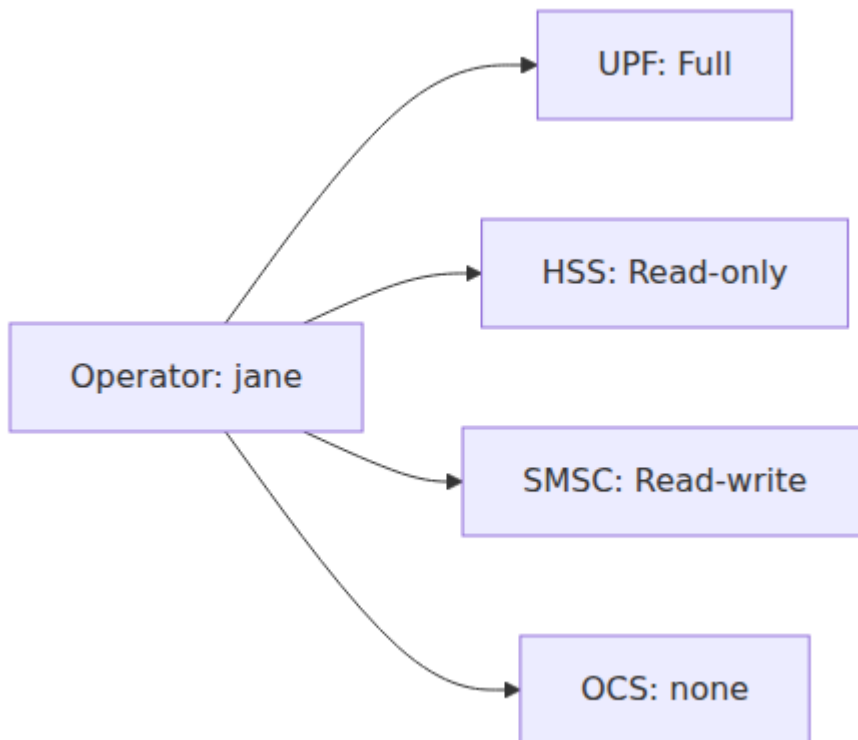
Chaque type d'élément peut être accordé à un utilisateur à l'un des trois niveaux. Le niveau est exprimé comme l'ensemble des méthodes HTTP que l'utilisateur peut utiliser contre cet élément via le proxy :

Permission	Méthodes autorisées	Ce que l'opérateur peut faire
Lecture seule	GET	Visualiser les données uniquement, aucune modification
Lecture-écriture	GET, POST, PUT, PATCH	Visualiser et modifier : par exemple, ajouter un abonné, éditer une route, changer une règle de QoS
Complet	GET, POST, PUT, PATCH, DELETE	Tout, y compris la suppression et le nettoyage des sessions

Parce que les permissions sont liées aux méthodes HTTP, elles s'alignent exactement avec le **modèle d'édition générique** : un formulaire "Ajouter" est un POST, un "Modifier" est un PUT/PATCH, et un "Supprimer"/"vider" est un DELETE.

Granularité par élément

Les permissions sont attribuées **indépendamment par type d'élément**. Un utilisateur peut avoir différents niveaux sur différents éléments :



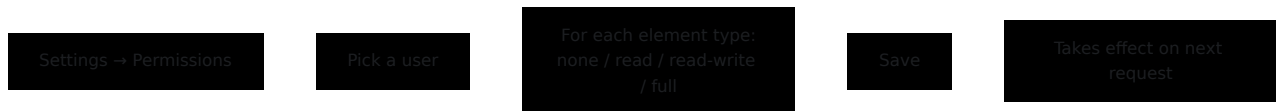
Dans cet exemple, Jane peut vider les sessions UPF, peut visualiser mais ne peut pas changer le HSS, peut ajouter des routes SMSC, et ne peut pas voir l'OCS du tout. Cela vous permet de donner, par exemple, à un ingénieur de plan de données un contrôle total sur le UPF tout en gardant les données des abonnés en lecture seule.

Administrateurs

Les administrateurs ont un accès complet à tous les types d'éléments automatiquement. Le rôle d'administrateur est également ce qui accorde l'accès à la gestion des utilisateurs et des permissions. Gardez le nombre d'administrateurs faible, et préférez des attributions spécifiques par élément pour tout le monde d'autre.

Gestion des rôles et des permissions

Les permissions sont gérées sous **Paramètres → Permissions**. Pour chaque utilisateur que vous choisissez, par type d'élément, vous décidez s'ils ont un accès en lecture seule, en lecture-écriture ou complet (ou aucun).

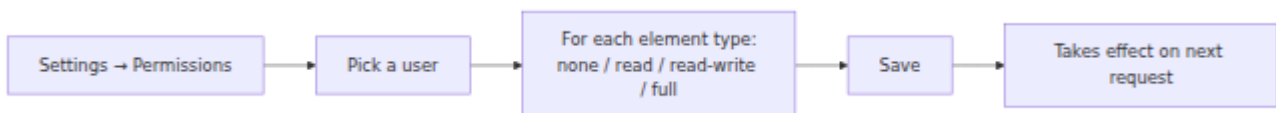


Comment fonctionne l'application

Le RBAC est appliqué à deux endroits complémentaires :

1. **Dans l'interface utilisateur** : les contrôles pour les actions que vous ne pouvez pas effectuer ne sont pas affichés. Si vous n'avez qu'un accès en lecture au HSS, vous ne verrez pas les boutons Ajouter/Modifier/Supprimer là-bas.
2. **Dans le backend** : chaque requête proxy est re-vérifiée par rapport à vos permissions *côté serveur*. Même une requête conçue pour contourner l'interface utilisateur est rejetée si votre rôle ne permet pas cet élément/méthode.

Cette "défense en profondeur" signifie que l'interface utilisateur est une commodité, pas la frontière de sécurité. Le proxy backend est la frontière.



Paramètres → Permissions : sélectionnez un utilisateur, puis accordez un niveau (lecture seule, lecture-écriture ou complet) par type d'élément.

Bonnes pratiques

- **Moindre privilège** : accordez le niveau le plus bas qui permet à quelqu'un de faire son travail ; élargissez uniquement si nécessaire.
- **Lecture seule par défaut** pour les éléments qu'un opérateur n'a besoin que d'observer.
- **Réserver Complet (DELETE)** pour ceux qui ont réellement besoin de vider des sessions ou de supprimer des enregistrements.
- **Peu d'administrateurs** : utilisez des attributions ciblées par élément au lieu de distribuer des droits d'administrateur.

Liens connexes

- [Connexion & Sessions JWT](#) : authentification sur laquelle le RBAC est basé.

- **Opérations courantes** : comment les permissions façonnent l'interface utilisateur quotidienne.
- **Journalisation d'audit** : les actions autorisées et refusées sont enregistrées.

Authentification et Contrôle d'Accès

OmniWeb est la porte d'entrée unique vers l'ensemble du réseau, donc le contrôle d'accès est l'une de ses responsabilités les plus importantes. Il utilise une connexion basée sur JWT, un contrôle d'accès basé sur des rôles (RBAC) granulaire sur chaque élément, une connexion par clé SSH pour l'accès aux hôtes, et une piste d'audit unifiée couvrant le portail et les hôtes qu'il gère.

Cette zone est divisée en pages ciblées :

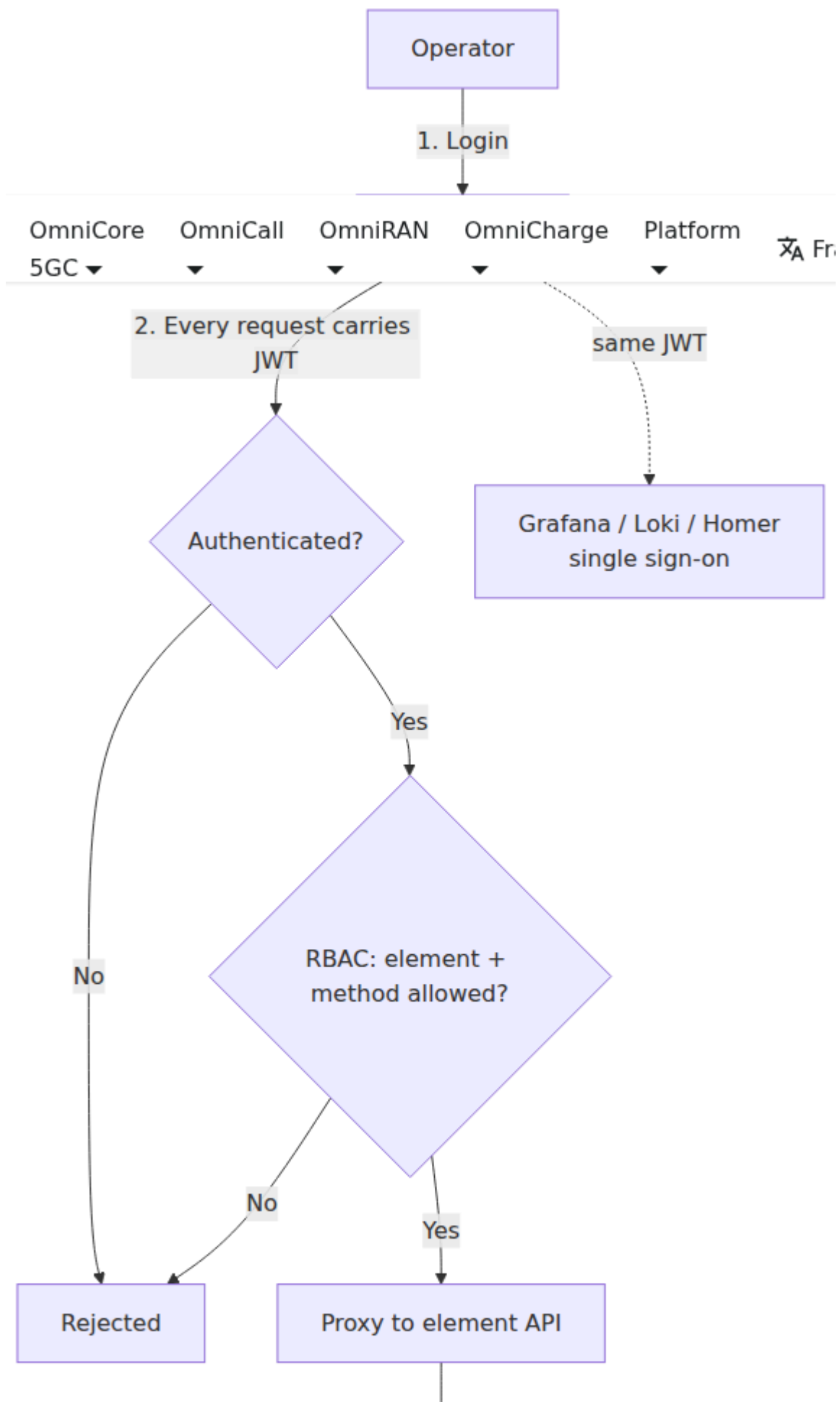
[← Retour au Guide des Opérations](#)

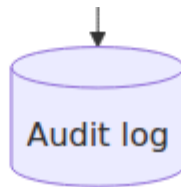
Dans Cette Section

- **Connexion & Sessions JWT** : Comment les opérateurs se connectent, comment le JWT fonctionne, la durée de vie du jeton, et comment une seule connexion couvre Grafana, Loki et Homer.
- **Contrôle d'Accès Basé sur les Rôles (RBAC)** : Permissions par élément, par méthode ; comment les accorder ; et comment elles sont appliquées.
- **Connexion par Clé SSH** : Les hôtes gérés récupèrent la clé publique SSH de chaque utilisateur en direct depuis OmniWeb (AuthorizedKeysCommand), donc l'accès aux hôtes est accordé/révoké de manière centralisée.
- **Journalisation des Audits** : Les trois couches d'audit : audit des requêtes du portail, audit des connexions SSH, et audit des commandes.

Le Modèle de Contrôle d'Accès

OmniWeb superpose quatre contrôles. Une demande doit passer par chacun avant d'atteindre un élément, et toute la chaîne est enregistrée.





Couche	Ce qu'elle contrôle	Page
Authentification	Qui vous êtes, prouvé par un JWT signé	Connexion & JWT
Autorisation (RBAC)	Ce que vous pouvez faire, par type d'élément et méthode HTTP	RBAC
Accès aux hôtes	Qui peut SSH où ; clés servies en direct depuis OmniWeb	Connexion par Clé SSH
Audit	Ce qui s'est réellement passé, à travers le portail et les hôtes	Journalisation des Audits

Pourquoi C'est Important

Parce qu'OmniWeb proxy chaque élément, tableau de bord Grafana, requête Loki et session Homer, cette chaîne de contrôle d'accès unique gouverne l'*ensemble* de la surface opérationnelle du réseau. Il y a un endroit pour accorder l'accès, un endroit pour le révoquer, et une piste qui enregistre qui a fait quoi, sur le portail et sur les hôtes sous-jacents.

Une piste pour tout : requêtes API, connexions, connexions SSH, et changements de permissions, avec utilisateur, élément, méthode, résultat, et IP source. Voir [Journalisation des Audits](#).

Commencez par [Connexion & Sessions JWT](#).

Trace d'appel (Trace SIP)

Trace d'appel est l'outil OmniWeb pour le dépannage des appels vocaux. Il enregistre le signalement SIP et le média RTP des appels qui traversent l'IMS. Il vous permet ensuite de rechercher ces appels, d'ouvrir un rapport complet par appel, de suivre l'appel comme une échelle de signalisation à travers le réseau, de mesurer la qualité de la voix, d'écouter l'audio et de télécharger la capture de paquets brute (PCAP).

Trace d'appel est un outil au niveau du site. Il apparaît dans la barre latérale sous **Trace de session** comme **Trace SIP**. L'outil n'apparaît que lorsque le service de capture est configuré et accessible pour le site sélectionné.

[← Guide des opérations](#)

Contenu

- [Ce que c'est](#)
- [Architecture](#)
- [Recherche](#)
- [Détails de l'appel](#)
- [Échelle \(Trace de session\)](#)
- [Onglet QoS](#)
- [Écouter](#)
- [Téléchargement PCAP](#)
- [Appels actifs](#)
- [Sniffer en direct](#)
- [Agents de capture à distance](#)
- [Règles d'enregistrement et conservation](#)
- [Confidentialité et interception légale](#)
- [Comment Trace d'appel se compare à Homer et Trace de session](#)

Ce que c'est

Trace d'appel répond à une question en profondeur : **que s'est-il passé avec cet appel ?** Pour tout appel enregistré, il vous donne :

- Les deux parties, leurs numéros, leurs domaines SIP et le nom d'affichage.
- L'adresse IP SIP de chaque partie, liée à son élément réseau OmniWeb.
- La réponse SIP finale et la raison de la déconnexion (SIP et Q.850).
- La qualité de la voix de chaque direction média : MOS, gigue, perte de paquets et délai aller-retour.
- Le flux complet des messages SIP (échelle) à travers chaque élément IMS qui a touché l'appel.
- L'audio enregistré et le PCAP brut.

Trace d'appel enregistre les appels de première main. Parce qu'il capture le SIP Call-ID et le média sur le fil, un appel est mappé à sa capture de paquets sans conjecture.

La qualité de la voix est rapportée sous forme de **MOS** (Mean Opinion Score). Le MOS est un score de 1 à 5. Un score de 4.0 ou plus est bon, de 3.0 à 4.0 est juste, et en dessous de 3.0 est mauvais. OmniWeb colore les valeurs MOS : vert pour bon, ambre pour juste, et rouge pour mauvais. Les appels AMR-WB (large bande) dans un réseau sain obtiennent environ 4.5.

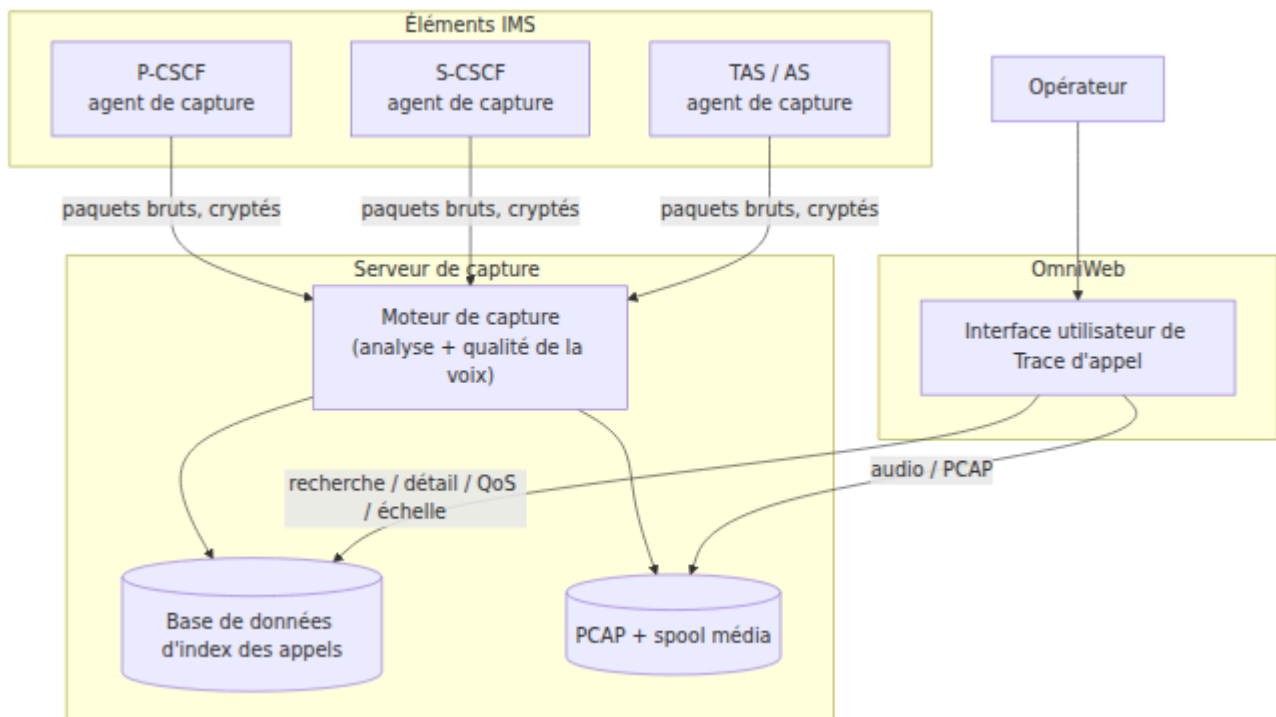
Architecture

Trace d'appel utilise deux parties :

1. **Agents de capture** qui fonctionnent sur les éléments IMS (P-CSCF, S-CSCF et TAS). Chaque agent capture les paquets SIP et RTP qu'il voit sur son hôte. Les agents ne stockent ni ne analysent les paquets localement. Ils transmettent les paquets bruts au serveur de capture central via un canal crypté.
2. Le **serveur de capture central** analyse chaque paquet, calcule la qualité de la voix et écrit un index dans sa base de données. Il conserve le spool de capture de paquets et les médias enregistrés. OmniWeb lit ce serveur

unique pour la recherche, les détails de l'appel, l'échelle, la QoS, l'audio et le PCAP.

Ce design garde toutes les données enregistrées sur un serveur central. Les éléments IMS ne conservent aucune donnée de capture propre.



Les agents de capture donnent à Trace d'appel une vue de nombreux points dans le réseau. Un seul appel est assemblé à partir de chaque agent qui l'a vu. C'est ce qui permet à l'échelle de montrer le flux SIP multi-sauts à travers le P-CSCF, le S-CSCF et le TAS.

Recherche

Ouvrez Trace d'appel pour atteindre la vue **Recherche**. La recherche trouve les appels complétés dans l'index central des appels.

La vue de recherche. Chaque ligne empile l'appelant et la partie appelée (numéro, domaine, nom, IP SIP et agent utilisateur) à côté des cellules RTP par direction qui montrent l'IP source, le codec, trois estimations MOS, la gigue et la perte.

Filtres

Définissez un ou plusieurs filtres, puis sélectionnez **Recherche**. Tous les filtres se combinent avec ET.

Filtre	Ce qu'il correspond
Numéro	Le numéro de l'appelant OU le numéro du appelé.
Plage horaire	Une fenêtre prédéfinie (Dernières 15m à Derniers 7j) ou un début et une fin personnalisés.
Direction	Inbound, Outbound ou Interne. La direction provient du rôle de l'appelant et de l'IP appelée.
Min MOS	Conserver uniquement les appels dont le MOS dans la pire direction est à ou au-dessus de cette valeur. Utilisez ceci pour trouver de bons appels, ou inversez votre lecture pour trouver de mauvais.
Max perte	Conserver uniquement les appels dont la perte de paquets dans la pire direction est à ou en dessous de cette valeur.

Grille des résultats

Chaque ligne de résultat montre :

- **Temps** : le début et la fin de l'appel.
- **Appelant** et **Appelé** : une cellule empilée avec le numéro et le domaine (num@domain), le nom d'affichage, l'IP SIP (un lien vers cet élément dans OmniWeb) et l'agent utilisateur. Une puce **raccroché** marque la partie qui a envoyé le BYE.
- **Résultat** : le code de réponse SIP final et le texte.
- **RTP A** et **RTP B** : une cellule par direction média. Chaque cellule montre l'IP source, le codec, trois estimations MOS (fixe 50 | fixe 200 | adaptatif), la gigue et le nombre de paquets perdus. Les trois valeurs MOS sont codées par couleur.
- **Durée (s)** : la durée de l'appel en secondes.
- **PCAP** : un bouton de téléchargement par ligne pour la capture de paquets de cet appel.

Sélectionnez une ligne pour ouvrir les [détails de l'appel](#).

Détails de l'appel

La vue des détails de l'appel est le rapport complet pour un appel. Elle s'ouvre lorsque vous sélectionnez un résultat de recherche. L'URL porte l'identifiant de l'appel, vous pouvez donc mettre en signet ou partager un appel.

La vue de détail de l'appel. L'en-tête montre le Call-ID et le contexte. La bande de résumé montre Début, Durée, PDD, Sonnerie, Connecté, la dernière réponse SIP et les raisons de déconnexion. Le tableau à deux colonnes montre l'identité et la qualité de la voix pour les jambes Appelant (A) et Appelé (B).

En-tête et contexte

L'en-tête montre le **Call-ID** sur le fil. Un bloc de contexte en dessous montre la **Direction** de l'appel, le **Capteur** propriétaire (l'agent de capture), quelle partie a **raccroché**, l'heure à laquelle l'appel a **pris fin**, et le **Nom de l'appelant**.

Bande de résumé

La bande de résumé est un aperçu en une ligne de l'appel :

Champ	Signification
Début	Quand l'appel a commencé.
Durée	Longueur totale de l'appel.
PDD	Délai post-dial : le temps entre l'INVITE et la première indication de sonnerie.
Sonnerie	Combien de temps le téléphone a sonné avant de répondre.
Connecté	Combien de temps l'appel a été connecté (média circulant).
Dernière réponse SIP	Le code de réponse SIP final et le texte.
Raison SIP	La cause de déconnexion SIP, lorsque le moteur de capture enregistre une.
Raison Q.850	La cause de déconnexion Q.850 et le texte, le cas échéant.
Appelant et Appelé	Les deux parties sous la forme <code>num@domain</code> .

Tableau d'identité et de qualité de la voix

Le tableau principal a deux colonnes : **Appelant (A)** et **Appelé (B)**. Chaque IP est liée à son élément réseau OmniWeb lorsque l'élément est connu. Le tableau a trois groupes.

Identité :

Ligne	Signification
IP SIP	L'IP de signalement SIP de la partie.
IP RTP	L'IP média RTP de la partie.
Port RTP	Le port média RTP.
Agent utilisateur	L'agent utilisateur SIP de la partie.
Codec	Le codec audio, par exemple AMR-WB.
Paquets reçus	Le nombre de paquets RTP reçus.
Paquets perdus	Le nombre de paquets RTP perdus.

MOS : trois estimateurs MOS, chacun affiché sous la forme `moyenne | minimum` :

Ligne	Signification
MOS fixe 50	MOS sur une fenêtre fixe de 50 paquets.
MOS fixe 200	MOS sur une fenêtre fixe de 200 paquets.
MOS adaptatif 500	MOS sur une fenêtre adaptative jusqu'à 500 paquets.

Gigue et RTCP : la gigue RTP (max et moyenne), la gigue RTCP, le compte de perte et de fraction perdue RTCP, et le délai aller-retour RTCP (max et moyen).

Échelle (Trace de session)

L'onglet **Échelle** dessine l'appel comme un flux de signalisation ordonné dans le temps. Trace d'appel assemble les messages SIP de chaque agent de capture

qui a vu l'appel. Le résultat est une échelle multi-sauts à travers les éléments IMS : par exemple P-CSCF à S-CSCF à TAS.

L'onglet Échelle. Les colonnes sont les éléments IMS que l'appel a traversés. Chaque échelon est un message SIP. L'échelle montre le flux INVITE à 100 à 180 à 200 à ACK à BYE, avec des deltas de temps par message et le délai aller-retour de la demande à la réponse.

Chaque colonne est un élément IMS, étiqueté avec son rôle et son nom d'hôte. Chaque échelon est un message SIP tiré de la source à la destination. L'échelle montre :

- Le **delta de temps par message** (l'écart depuis le message précédent).
- Le **délai aller-retour demande-réponse** pour chaque réponse, associé à sa demande.
- Les modes de temps **absolu**, **relatif** et **écoulé** pour la colonne de temps.
- **Décodage de paquet en ligne** : sélectionnez un échelon pour voir le texte complet du message SIP et une vue hexadécimale.

Un panneau **Détails de session** répertorie les sessions dans l'échelle. Pour un seul appel, il y a une session, donc le panneau reste replié.

L'échelle utilise le même rendu que les Flux en direct de Trace de session à l'échelle du réseau. Voir [Journaux et traçage des abonnés](#) pour l'outil Trace de session plus large.

Onglet QoS

L'onglet **QoS** montre la qualité de la voix pendant la durée de l'appel.

L'onglet QoS. Les tableaux montrent les seaux de distribution de délai PDV et la répartition des pertes consécutives pour chaque direction. Un graphique interactif de qualité de délai et de MOS est dessiné sur la durée de l'appel en dessous des tableaux.

L'onglet QoS a trois parties :

- Un **graphique interactif de délai / gigue et qualité MOS** sur l'appel. Le graphique est par direction média. Vous pouvez lire le délai et le MOS à tout moment de l'appel, ce qui montre où la qualité a chuté.
- La **distribution de délai PDV** : combien de paquets sont tombés dans chaque seau de délai (par exemple 50 à 70 ms, 70 à 90 ms, et ainsi de

suite jusqu'à plus de 300 ms). Une distribution qui reste dans les seaux bas est saine.

- La **répartition des pertes consécutives** : combien de fois 1, 2, 3 et jusqu'à 10 paquets ont été perdus consécutivement. Les pertes isolées sont beaucoup moins audibles que les longues séries de pertes.

Les deux répartitions sont montrées par direction (Appelant et Appelé), vous pouvez donc dire quelle jambe avait le problème.

Écouter

Le panneau **Écouter** joue l'appel enregistré dans le navigateur. L'audio est décodé à partir du RTP capturé. L'appelant est le canal gauche et l'appelé est le canal droit, vous pouvez donc entendre chaque côté séparément.

Écouter ne fonctionne que lorsque le média de l'appel a été enregistré et que son codec peut être décodé. Voir [Règles d'enregistrement et conservation](#) pour savoir comment la capture de média est armée.

Téléchargement PCAP

Chaque appel a un bouton **Télécharger PCAP**, à la fois dans la grille de recherche et dans l'en-tête des détails de l'appel. Le téléchargement est la capture de paquets brute (SIP et, lorsqu'enregistrée, RTP) pour cet appel. Utilisez le PCAP pour inspecter l'appel dans un outil externe tel que Wireshark.

Appels actifs

La vue **Appels actifs** montre les appels qui sont en cours en ce moment. Elle lit la liste des appels en direct à partir des agents de capture et se rafraîchit à court intervalle, de sorte que les lignes apparaissent et disparaissent à mesure que les appels se mettent en place et se terminent.

La vue Appels actifs. Chaque ligne est un appel en direct avec son état (Connecté ou Configuration), les deux parties et leurs adresses IP, la direction, la durée croissante, le codec, le MOS en direct et l'agent de capture propriétaire.

Chaque ligne montre l'**État** de l'appel (Connecté, Configuration ou Échec), les deux parties, le chemin IP de l'appelant au appelé, la **Direction**, la **Durée** croissante, le **Codec**, le **MOS** en direct, la dernière réponse SIP, et le **Capteur** propriétaire (agent de capture). Désactivez **Rafraîchissement automatique** pour maintenir la liste actuelle.

Sniffer en direct

La vue **Sniffer en direct** montre la santé du serveur de capture central et de ses agents de capture.

La vue Sniffer en direct. Le panneau Serveur Central montre la version, le temps de fonctionnement, le nombre d'appels actifs, le débit, les pertes de paquets et la moyenne de charge. Le tableau des Agents de Capture à Distance répertorie chaque agent. Le panneau I/O du disque de spool montre l'utilisation et le débit.

La vue montre :

- **Serveur Central** : version et build, temps de fonctionnement, nombre d'appels actifs, débit de capture, pertes de paquets, moyenne de charge, et la dernière fois qu'un enregistrement d'appel a été écrit.
- **Agents de Capture à Distance** : les agents par élément et leur statut (voir [Agents de capture à distance](#)).
- **I/O du disque de spool** : l'utilisation, le débit de lecture et d'écriture, les IOPS, la latence, la capacité utilisée et le niveau de tampon du disque de spool de capture.
- Un flux d'activité en direct des appels en cours.

Surveillez cette vue pour confirmer que le moteur de capture est sain, ne perd pas de paquets et a de la marge sur le disque de spool.

Agents de capture à distance

Le tableau **Agents de capture à distance** (dans la vue Sniffer en direct) répertorie les agents de capture qui fonctionnent sur les éléments IMS. Chaque ligne montre :

Colonne	Signification
Agent	Le nom d'hôte de l'agent. Sélectionnez-le pour ouvrir cet hôte dans la liste des hôtes.
ID de capteur	L'identifiant numérique de l'agent dans l'index de capture.
Statut	Actif, Inactif ou Inconnu, dérivé des appels en direct et des enregistrements d'appels récents.
Appels actifs	Combien d'appels l'agent capture en ce moment.
CDRs	Combien d'enregistrements d'appels l'agent a produits.
Dernière vue	Quand l'agent a produit pour la dernière fois un enregistrement d'appel.

Utilisez ce tableau pour confirmer que chaque élément IMS qui devrait capturer est en train de capturer. Un agent qui est inactif ou manquant de manière inattendue signifie que le trafic de cet élément n'est pas enregistré.

Règles d'enregistrement et conservation

La vue **Règles d'enregistrement** contrôle quels appels ont leur **média** enregistré et montre la conservation du spool de capture et de la base de données d'index.

La vue Règles d'enregistrement. Les règles sont regroupées par type de correspondance : Par IP, Par numéro et Par domaine SIP (un groupe Par en-tête SIP existe également). Chaque règle arme la capture de média RTP, saute une cible ou sauvegarde les données de graphique QoS.

Règles d'enregistrement

Par défaut, le moteur de capture enregistre le signalement SIP pour chaque appel, mais il ne **registre pas** le média RTP. Une règle d'enregistrement arme la capture de média pour une cible spécifique. Le moteur de capture relit les règles en direct, sans redémarrage.

Les règles sont regroupées par la façon dont elles correspondent à un appel :

Groupe	Correspond à
Par IP	Une IP source ou de destination et un masque.
Par numéro	Un préfixe de numéro d'appelant ou d'appelé.
Par domaine SIP	Un domaine SIP.
Par en-tête SIP	Une valeur d'en-tête SIP arbitraire.

Chaque règle porte un ensemble de drapeaux :

Drapeau	Effet
RTP	Arme la capture de média RTP pour la cible correspondante. C'est ce qui vous permet d' écouter l'appel et d'obtenir le PCAP média complet. Gardez RTP désactivé globalement et armez-le par cible.
Skip	Supprime complètement la cible correspondante : pas d'enregistrement d'appel et pas de capture. Utilisez ceci pour le trafic de test connu.
Graph	Sauvegarde les données de graphique QoS détaillées pour la cible correspondante, qui alimentent le graphique QoS .
rtcp	Enregistre les rapports de qualité RTCP pour la cible correspondante.
enabled	Active ou désactive la règle sans la supprimer.

Pour armer la capture pour une cible, ajoutez une règle dans le groupe de correspondance, remplissez la valeur de correspondance et activez **RTP**. Pour arrêter l'enregistrement du trafic de test connu, ajoutez une règle avec **Skip** activé.

Conservation

Le panneau de conservation montre combien de temps les données enregistrées sont conservées. La conservation est définie centralement sur le serveur de capture. Le panneau est en lecture seule dans OmniWeb.

Les paramètres de conservation contrôlent deux choses : les limites de taille et d'âge du spool sur disque (divisé par SIP, RTP et données de graphique), et la limite d'âge de l'index des appels et des lignes de qualité par flux dans la base de données. Le tableau ci-dessous liste les paramètres que le panneau rapporte :

Paramètre	Signification
<code>maxpoolsize_gb</code>	Taille maximale totale du spool, en Go. Les données les plus anciennes sont supprimées lorsque cela est atteint.
<code>maxpooldays</code>	Âge maximal de toute donnée de spool, en jours.
<code>maxpoolsipsize_gb</code>	Taille maximale du spool SIP, en Go.
<code>maxpoolsipdays</code>	Âge maximal du spool SIP, en jours.
<code>maxpoolrtpsize_gb</code>	Taille maximale du spool RTP (média), en Go.
<code>maxpoolrtpdays</code>	Âge maximal du spool RTP, en jours.
<code>maxpoolgraphsize_gb</code>	Taille maximale du spool de graphique QoS, en Go.
<code>maxpoolgraphdays</code>	Âge maximal du spool de graphique QoS, en jours.
<code>cleandatabase_cdr_days</code>	Âge maximal des enregistrements d'appels dans la base de données d'index, en jours.
<code>cleandatabase_rtp_stat_days</code>	Âge maximal des lignes de qualité par flux dans la base de données, en jours.

Les données médias (RTP) sont volumineuses. Gardez la conservation RTP plus courte que la conservation SIP, et armez la capture RTP uniquement pour les cibles dont vous avez besoin.

Confidentialité et interception légale

L'enregistrement du **média** des appels est une décision d'interception légale. La capture de signalement enregistre qui a appelé qui et quand. La capture de média enregistre le **contenu** de l'appel : l'audio vocal. Armez la capture de média (une règle d'enregistrement **RTP**) uniquement pour les cibles que vous êtes autorisé à enregistrer, et uniquement aussi longtemps que vous êtes autorisé.

Gardez la capture RTP désactivée par défaut et armez-la par cible. Réglez la conservation RTP sur la période la plus courte que votre politique autorise. Suivez votre loi locale sur la confidentialité et les règles de consentement pour la capture de signalement et de média.

Comment Trace d'appel se compare à Homer et Trace de session

OmniWeb a trois façons de regarder le signalement. Choisissez la bonne :

	Trace d'appel (Trace SIP)	Homer (Capture SIP)	Trace de session
Portée	SIP et média RTP pour les appels IMS	SIP uniquement	L'ensemble du réseau : Diameter, GTP-C, PFCP, SIP, MAP
Question à laquelle il répond	"Que faisait cet appel, et quelle était la qualité de la voix ?"	"Que faisait le flux SIP de cet appel ?"	"Que s'est-il passé pour cet abonné à travers chaque élément ?"
Qualité de la voix (MOS)	Oui	Non	Non
Audio enregistré	Oui	Non	Non
Téléchargement PCAP	Oui, par appel	Non	Non
Meilleur pour	Diagnostiquer la qualité, le média et le flux d'un appel VoLTE	Un aperçu rapide d'un flux SIP	Suivre un abonné de bout en bout

Choisissez Trace d'appel lorsque vous devez juger de la **qualité de la voix** d'un appel, écouter l'audio ou obtenir le PCAP média. Choisissez **Trace de session** lorsque vous suivez un abonné à travers l'ensemble de la pile.

Liens connexes

- [Journaux et traçage des abonnés](#) : le Trace de session à l'échelle du réseau et l'échelle partagée.
- [Homer : Capture SIP](#) : l'outil de capture uniquement SIP.
- [Topologie du réseau](#) : la liste des hôtes à laquelle les agents de capture se connectent.

Opérations Courantes

Chaque élément de réseau dans OmniWeb est différent à l'intérieur, mais la façon dont vous *travaillez* avec eux est délibérément la même. Cette page documente les modèles partagés par tous les éléments : visualisation des données, édition et modification des configurations NF, lecture de la configuration, exécution d'actions, consultation des journaux, et compréhension du polling et des permissions. Apprenez-les une fois et ils s'appliquent au HSS, au UPF, au SMSC, au MSC, et à chaque autre NF.

Les captures d'écran ci-dessous proviennent d'éléments spécifiques, mais elles illustrent le modèle *générique* : les mêmes contrôles apparaissent, avec des champs différents, sur chaque élément.

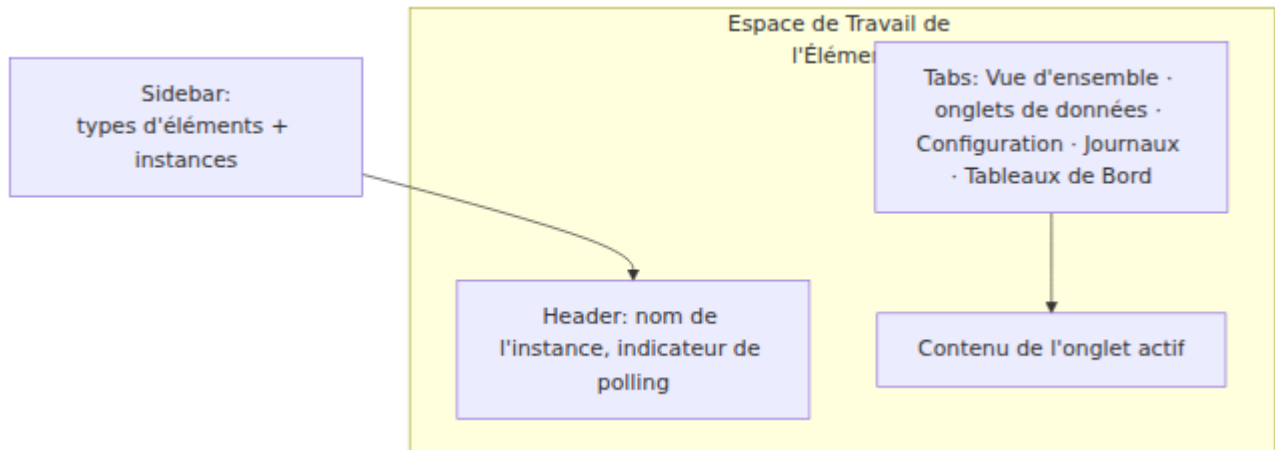
[← Retour au Guide des Opérations](#)

Table des Matières

- [Anatomie de la Page](#)
- [Visualisation des Données](#)
- [Vues Détails](#)
- [Édition & Modification des Configurations NF](#)
- [Exécution d'Actions \(clear, release, test, ping\)](#)
- [Visualisation de la Configuration](#)
- [Journaux sur Chaque Élément](#)
- [Tableaux de Bord sur Chaque Élément](#)
- [Polling en Temps Réel](#)
- [Permissions & Ce Que Vous Pouvez Changer](#)
- [Vues Multi-Instances & Flotte](#)

Anatomie de la Page

Sélectionner une instance d'élément dans la barre latérale ouvre son espace de travail. Chaque espace de travail d'élément partage la même mise en page :



- **Vue d'ensemble** : l'onglet d'accueil : santé, comptes clés, et statut des composants pour cette instance.
- **Onglets de données** : les vues spécifiques à l'élément (sessions, abonnés, pairs, routage, etc.).
- **Configuration** : une vue structurée de la configuration d'exécution de l'élément (lorsqu'elle est exposée).
- **Journaux** : un visualiseur de journaux Loki en direct limité à cet élément.
- **Tableaux de Bord** : tableaux de bord Grafana intégrés pour cet élément (lorsque les balises Grafana correspondent).

Les entrées de la barre latérale sont des liens ordinaires, vous pouvez donc **Ctrl/Cmd-click** (ou clic du milieu, ou clic droit → *Ouvrir dans un nouvel onglet*) sur n'importe lequel d'eux pour ouvrir cet espace de travail dans un nouvel onglet de navigateur. Cela est pratique pour surveiller deux éléments à la fois.

Visualisation des Données

Les données opérationnelles sont présentées dans un tableau cohérent et triable à travers OmniWeb. Les tableaux offrent :

- **Tri** par colonne.
- **Pagination** pour les grands ensembles de résultats.

- **Recherche / filtrage** lorsque l'API de l'élément le supporte (par exemple, recherche par IMSI/MSISDN ou IP UE).
- **Chargement en squelette** pendant que les données sont récupérées, et un **état vide** clair lorsqu'il n'y a rien à montrer.
- **Clic sur la ligne** pour accéder à une vue détaillée lorsqu'elle existe.

Les valeurs sont formatées pour la lisibilité : horodatages en heure locale, durées en h m s, comptes de bytes en Ko/Mo/Go, et grands nombres avec des séparateurs de milliers.

Le modèle de liste générique (ici, une liste d'abonnés) : consultable, triable, paginé, avec clic et édition en ligne. Le même tableau alimente les sessions, pairs, routes, et chaque autre liste.

Les tableaux peuvent rendre des cellules plus riches : ici, des barres d'utilisation par ligne. Le modèle est le même ; seules les colonnes diffèrent.

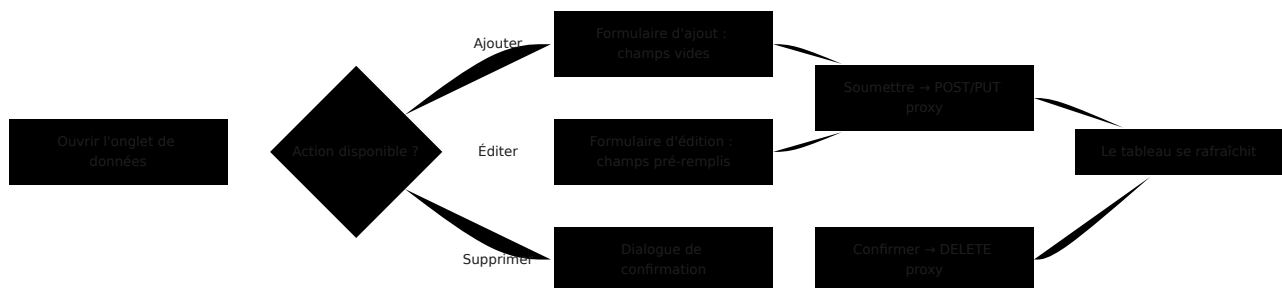
Vues Détails

Lorsqu'une ligne a plus à montrer, cliquez dessus pour ouvrir une vue détaillée. Celles-ci réutilisent le même chrome (en-tête, polling, actions) mais présentent l'enregistrement unique en profondeur, par exemple une carte de relation interactive pour un objet complexe :

Une vue détaillée ouverte à partir d'une ligne de tableau : ici, une carte interactive des règles internes d'une session. Les vues détaillées sont accessibles de la même manière partout : cliquez sur la ligne.

Édition & Modification des Configurations NF

Partout où l'API d'un élément supporte la modification, OmniWeb l'expose à travers un **formulaire d'action** cohérent. Le même composant de formulaire alimente "ajouter un abonné", "ajouter une route", "éditer une règle QoS", et "changer un profil". Seuls les champs diffèrent.



Les formulaires d'action supportent ces types de champs : **texte**, **nombre**, **sélection** (menu déroulant), **booléen** (interrupteur), **mot de passe** (masqué, avec un interrupteur afficher/cacher), et **texte multi-lignes**. Chaque champ peut être marqué comme requis, porter un espace réservé, et afficher un texte d'aide. Le formulaire montre un état de chargement pendant la soumission et rapporte le succès ou l'échec via une notification à l'écran.

La méthode HTTP derrière chaque action correspond à un niveau de permission. Voir [Permissions](#).

Le même modèle, trois éléments

Ceci illustre le *même* mécanisme appliqué à différents NF :

Tâche	Où	Que se passe-t-il
Ajouter/éditer un abonné	HSS → Abonnés → Ajouter	Remplir le formulaire (IMSI, MSISDN, profil, clés) → POST/PUT proxy → le tableau se rafraîchit
Ajouter/changer une route	SMSC → Routage → Ajouter (ou MSC → Routage)	Remplir la règle (modèle, destination, priorité) → écriture proxy → le tableau se rafraîchit
Effacer/libérer une session	UPF → Sessions (ou MSC → Appels)	Sélectionner l'enregistrement → confirmer → DELETE proxy → le tableau se rafraîchit

Les mécanismes sont identiques : formulaire ou dialogue de confirmation, écriture proxy, rafraîchissement du tableau. Seuls l'élément et les champs changent.

Changer le routage est le même modèle d'édition : le tableau de routage est une liste que vous ajoutez et éditez ; certains éléments analysent également les destinations en puces lisibles et offrent un simulateur pour tester un changement avant qu'il ne soit mis en production.

Exécution d'Actions

Au-delà de CRUD, de nombreux éléments exposent des **actions opérationnelles** qui ne s'intègrent pas dans un simple formulaire. Celles-ci sont présentées sous forme de boutons qui déclenchent un appel proxy et affichent le résultat en ligne. Exemples du même modèle bouton-action :

Action exemple	Élément	Effet
Libération forcée d'un appel	MSC → Appels	Met fin à un appel actif
Ping OPTIONS d'un pair SIP	MSC → Pairs SIP	Teste la connectivité d'un tronc SIP
Test MAR d'un pair Diameter	TWAG → Diameter	Envoie une requête de test Multimedia-Auth-Request
Activer/désactiver une redirection	UPF → Jardin Clos	Redirige ou restaure un abonné
Ping depuis le nœud	UPF → Diagnostics	Exécute un ping depuis l'élément lui-même
Déconnecter une session	TWAG → Sessions	Met fin à une session WiFi authentifiée
Paging manuel	MSC → Paging	Déclenche une demande de paging

Les actions destructrices (libérer, supprimer, désactiver) nécessitent toujours une confirmation explicite avant de s'exécuter.

Les actions opérationnelles apparaissent sous forme de boutons à côté des données qu'elles affectent : ici, activer/désactiver les redirections d'abonnés et gérer les IP blanches. Les actions destructrices demandent d'abord une confirmation.

Visualisation de la Configuration

Les éléments qui exposent leur configuration d'exécution ont un onglet **Configuration**. OmniWeb le rend dans une mise en page structurée et lisible avec un basculement **JSON Brut** pour le document sous-jacent complet.

Deux comportements valent la peine d'être connus :

- **Les formats de configuration mixtes sont normalisés.** Certains éléments retournent la configuration sous forme de dictionnaires de style Python (`'key' : True`, `None`) plutôt que du JSON strict. OmniWeb les analyse automatiquement dans une vue propre et retombe gracieusement s'il ne peut pas analyser une valeur.
- **Les secrets sont masqués.** Tout champ dont le nom semble sensible (correspondant à `password`, `secret`, `token`, ou `credential`) est affiché

comme ******* plutôt que sa vraie valeur, tant dans les vues de configuration que dans les champs de formulaire.

La vue de configuration générique : paramètres dans une mise en page structurée, avec un basculement JSON Brut et des valeurs sensibles masquées. Les éléments qui exposent la configuration (UPF, TAS, ePDG, interfaces SMSC, OCS, RAN Monitor) utilisent tous ce modèle.

Journaux sur Chaque Élément

Chaque élément a un onglet **Journaux** soutenu par Loki. Il interroge les journaux de service de cet élément par hôte/étiquette, supporte le filtrage structuré, et diffuse les nouvelles lignes à mesure qu'elles arrivent. Comme le modèle de journal est identique à travers les éléments, il est documenté en entier sur sa propre page :

→ **Journaux & Traçage des Abonnés**

L'onglet Journaux de chaque élément utilise le même visualiseur : journaux Loki structurés, codés par couleur, diffusés en direct avec filtrage par service et sévérité.

Tableaux de Bord sur Chaque Élément

Les éléments étiquetés pour Grafana affichent un onglet **Tableaux de Bord**. OmniWeb découvre les tableaux de bord correspondants par étiquette et les rend en ligne, vous permettant de voir les statistiques pour un élément sans quitter son espace de travail. Voir :

→ **Tableaux de Bord & Statistiques Grafana**

Polling en Temps Réel

Les pages opérationnelles se rafraîchissent automatiquement. L'**Indicateur de Polling** dans l'en-tête de chaque page montre :

- **Actif (point vert)** ou **mis en pause**.
- L'**intervalle** (par défaut 5 secondes, défini par élément via `pollIntervalMs`).
- Un **spinner** pendant qu'une récupération est en cours.
- L'**horodatage** de la dernière mise à jour réussie.

Le polling peut être basculé par page. Les pages construites autour d'actions interactives ou ponctuelles (consoles, diagnostics, exécuteurs JSON) ne pollent pas par défaut et sont rafraîchies manuellement. Mettez le polling en pause lorsque vous souhaitez une vue stable pendant que vous lisez un grand tableau ou pendant qu'un traçage est en cours.

Permissions & Ce Que Vous Pouvez Changer

Ce que vous pouvez *faire* sur un élément dépend de votre rôle. L'accès est accordé **par type d'élément, par méthode HTTP** :

Permission	Méthodes autorisées	Utilisation typique
Lecture seule	GET	Voir les données, sans modifications
Lecture-écriture	GET, POST, PUT, PATCH	Voir et modifier (ajouter un abonné, éditer une route)
Complet	GET, POST, PUT, PATCH, DELETE	Tout, y compris la suppression / l'effacement

Les permissions sont attribuées indépendamment par élément : vous pourriez avoir un accès complet au UPF mais en lecture seule sur le HSS. Si une action n'est pas autorisée pour votre rôle, son contrôle est indisponible. Les administrateurs ont un accès complet à tous les éléments. Voir [Authentification](#)

& Contrôle d'Accès pour gérer les rôles, et notez que **chaque requête proxy est enregistrée dans un audit** indépendamment du rôle.

Vues Multi-Instances & Flotte

De nombreux types d'éléments fonctionnent en tant que plusieurs instances : plusieurs UPF derrière un PGW-C, une paire de SMSC, des STP redondants. OmniWeb gère cela au niveau du type d'élément : un type avec plus d'une instance configurée obtient deux modes de navigation.

Sélection de la Barre Latérale & des Instances

Lorsqu'un type a plusieurs instances, l'entrée de la barre latérale s'étend pour lister chacune par nom. Cliquez sur une instance nommée pour ouvrir directement l'espace de travail de cette instance. Un menu déroulant d'instance apparaît également dans l'en-tête de l'espace de travail. Il vous permet de passer d'instances sans revenir à la barre latérale, ce qui est utile lorsque vous comparez le comportement entre les nœuds sans perdre votre position sur un onglet particulier.

*Le sélecteur d'instance en haut à droite de l'en-tête de l'espace de travail.
L'ouverture montre chaque instance configurée ainsi que "Toutes les Instances"
pour revenir à la vue de flotte, sans quitter votre onglet actuel.*

Vue de Flotte

Cliquez sur le nom du type d'élément dans la barre latérale (plutôt que sur une instance spécifique), ou sélectionnez **Toutes les Instances** dans le menu déroulant, pour ouvrir la **vue de flotte** pour ce type. La vue de flotte montre une carte récapitulative par instance avec le statut de santé et des métriques clés, vous permettant d'évaluer l'ensemble de la flotte d'un coup d'œil avant de creuser dans un nœud spécifique.

*Vue de flotte UPF : une carte par instance, toutes interrogées en parallèle.
Cliquez sur n'importe quelle carte d'instance ou utilisez le menu déroulant pour approfondir.*

Quand Utiliser Chaque Vue

Situation	Utiliser
Vérifier la santé globale de la flotte	Vue de flotte : toutes les instances d'un coup d'œil
Enquêter sur un nœud spécifique	Menu déroulant d'instance ou sous-élément de la barre latérale
Comparer les comptes de session de deux UPF	Ouvrir chacun dans le menu déroulant d'instance à tour de rôle
Effacer une session sur un UPF spécifique	Naviguer vers cette instance, puis Sessions

DRA: Agent de Routage Diameter

Le **DRA** est le hub de routage Diameter du cœur. Plutôt que chaque nœud détienne une maillage complet de connexions Diameter, les fonctions EPC et IMS se connectent au DRA et il relaie et route leur signalisation : **S6a** entre le MME et le HSS, **Gx/Gy** vers le PCF/PCRF et l'OCS, **Cx/Dx** et **Sh** pour l'IMS, et ainsi de suite. Il choisit où chaque message va à partir des **règles de routage** (correspondant à l'application Diameter, au domaine ou à l'AVP) et d'un algorithme de sélection de pairs, et il peut réécrire des messages avec des **règles de transformation**. C'est le pendant Diameter d'un STP SS7. OmniWeb expose les pairs du DRA, les règles de routage, l'état en direct et une carte de connexion. Les graphiques de débit et de tendance se trouvent sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le DRA est une page d'élément par instance accessible depuis la barre latérale lorsqu'on navigue dans l'inventaire du site, avec une vue de flotte (la carte du réseau) où plusieurs sont déployés. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du DRA, donc il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Carte du réseau

Une vue en hub et spoke du DRA et de chaque pair Diameter qu'il connaît, avec le nombre de connexions en un coup d'œil (par exemple *5/6 connectés*). Les pairs connectés sont liés au DRA en vert. Un pair **désactivé** ou **déconnecté** est montré en gris et en pointillé. C'est le moyen le plus rapide de voir, en une image, quels voisins de signalisation sont actifs.

État

L'onglet **État** rapporte l'identité et la configuration propres du DRA : son **Origin-Host, domaine, l'IP et le port d'écoute** (Diameter est généralement 3868), le **nom du produit** rapporté, et l'**algorithme de sélection de pairs** en cours d'utilisation (par exemple, round-robin). C'est ici que vous confirmez que le DRA fonctionne et est configuré comme prévu.

Pairs

Chaque pair Diameter, chaque ligne montrant le **Origin-Host** du pair, **IP et port**, **produit** rapporté, **transport** (SCTP ou TCP), **domaine**, les **applications Diameter** négociées, et son **état de connexion**. Les pairs peuvent être filtrés par nom, application, domaine ou état. Chaque pair a un bascule **activer/désactiver**. Désactiver un pair administrativement le retire du routage sans détruire sa configuration, ce qui est comment vous drainer un voisin pour maintenance.

Règles

Les **règles de routage** et **règles de transformation** actives, et l'**algorithme de routage** sous lequel elles fonctionnent. Chaque règle de routage correspond à un filtre (une application Diameter, un AVP, ou tout le trafic) et se résout à une destination : soit un ensemble explicite de pairs soit une stratégie nommée telle que *destination-host* ou *destination-realm*. C'est ici que vous confirmez, par exemple, que S6a est routé vers le HSS et Gx vers le PCF.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du DRA pour résoudre les problèmes d'un seul agent de routage sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux de message, le débit par interface et d'autres séries temporelles pour le DRA sont présentés sous forme de tableaux de bord Grafana, accessibles

depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens connexes

- **MME** et le **HSS** : le DRA relaie **S6a** entre eux.
- Le **PCF/PCRF (Gx)** et l'**OCS (Gy)** : pairs de politique et de facturation routés via le DRA.
- Le **CSCF** et le **HSS** : signalisation IMS **Cx/Dx**.
- **STP** : le pendant de routage SS7 du DRA dans le plan de signalisation.

Serveur d'Attribution : OmniSEP

Le **Serveur d'Attribution (OmniSEP)** décide quels services un abonné et son appareil sont autorisés à utiliser. Lorsqu'un téléphone demande s'il peut activer **VoWiFi**, **VoLTE** ou **Appels Wi-Fi**, ou exécute le provisionnement d'appareil **ODSA** pour ajouter ou activer un appareil, il se connecte au serveur d'attribution. Le serveur autorise la demande via l'interface **d'attribution (TS.43)**, résout les données de l'abonné via **Diameter**, et applique les profils de service **XCAP** de l'abonné. OmniWeb présente ses attributions en direct, l'activité, les sessions, les jetons, les pairs Diameter et les profils XCAP sur une page d'élément ; des graphiques de volume et de tendance vivent sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des Opérations](#)

OmniSEP est une page d'élément par instance accessible depuis la barre latérale lorsque l'on est dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du serveur d'attribution, de sorte qu'il reste derrière la seule passerelle authentifiée. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

L'onglet d'accueil est une lecture de santé sur écran unique pour le serveur d'attribution : son **état du système**, le nombre de **sessions** et **jetons** actifs, les abonnés portant des **attributions** personnalisées, et la santé de ses pairs **Diameter**. C'est le moyen le plus rapide de confirmer que le serveur est opérationnel et autorise les appareils.

Attributions

Les abonnés qui portent des **attributions personnalisées** : des remplacements pour l'ensemble de services par défaut, par abonné. Ouvrez un abonné pour voir quels services sont activés pour lui. Un opérateur peut **supprimer toutes les attributions** d'un abonné pour le ramener à la valeur par défaut du réseau. Cela est utile pour effacer un mauvais remplacement lors d'un incident.

Activité

Les enregistrements récents d'**activité** : un fil des demandes d'attribution que le serveur a traitées, chacune montrant l'abonné ou l'appareil, le service demandé et le résultat. Ouvrez un enregistrement pour ses détails. C'est la piste d'audit pour confirmer si un téléphone a réellement demandé VoWiFi/VoLTE et quelle réponse lui a été donnée.

Sessions

Les **sessions EAP-AKA** actives que le serveur maintient pour l'authentification des appareils, chacune avec son identité d'abonné et son état. Une session individuelle peut être **expirée** depuis ici pour forcer un appareil à se ré-authentifier. C'est le moyen le plus rapide d'effacer une session qui est bloquée.

Jetons

Les **jetons d'authentification** actifs que le serveur a émis aux appareils après leur authentification. Chaque jeton peut être **révoqué** individuellement, ce qui retire l'autorisation d'un appareil et nécessite qu'il s'authentifie à nouveau. C'est l'équivalent d'attribuer de forcer une nouvelle connexion.

Diameter

Les **pairs Diameter** auxquels le serveur d'attribution se connecte pour les données des abonnés, avec l'**état de connexion** de chaque pair. Lorsque les décisions d'attribution commencent à échouer pour des raisons qui ressemblent à des données d'abonné manquantes, cet onglet est l'endroit où vous confirmez que le chemin Diameter est opérationnel.

Profils XCAP

Les **profils XCAP** : les paramètres de service par abonné (tels que la configuration de services supplémentaires) que le serveur d'attribution applique. Ouvrez un profil pour le lire. Un profil peut être **supprimé** pour effacer les paramètres stockés d'un abonné et revenir à la valeur par défaut.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du serveur d'attribution pour le dépannage d'un seul serveur sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux de demande, les compteurs par service et d'autres séries temporelles pour le serveur d'attribution sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page d'élément. OmniWeb ne duplique pas ces graphiques nativement.

Connexes

- Le **HSS** détient les données des abonnés que les demandes Diameter du serveur d'attribution résolvent.
- Le **CSCF** et le **TAS** fournissent les services VoLTE/VoWiFi que le serveur d'attribution autorise.
- Le **ePDG** et le **TWAG** transportent l'accès aux appels Wi-Fi que le serveur d'attribution active.
- Le **DRA** relaie le signalement Diameter du serveur d'attribution à ses pairs.

ePDG : Passerelle de Données Évoluée

Le **ePDG** est la passerelle sécurisée pour l'**accès Wi-Fi non fiable** : le nœud derrière l'appel Wi-Fi (VoWiFi) et les données WLAN non fiables. Un appareil construit un tunnel IPsec/IKEv2 vers le ePDG via n'importe quelle connexion Internet ; le ePDG authentifie l'abonné contre le AAA/HSS via Diameter (SWm/SWx), ancre la session au cœur de paquets (S2b vers le PGW), et applique des limites de taux par abonné et une politique géo-IP. OmniWeb affiche les tunnels en direct du ePDG, ses pairs Diameter, la configuration de limitation de taux et de géo-IP, ainsi que les paramètres d'exécution ; les tendances à long terme sont sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le ePDG est une page d'élément par instance accessible depuis la barre latérale lorsqu'on navigue dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb, il reste donc derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : le **statut** du ePDG, le nombre de **sessions actives** (tunnels IPsec), et un résumé de l'état opérationnel de la passerelle. C'est la confirmation la plus rapide que le ePDG est opérationnel et transporte des tunnels d'appel Wi-Fi.

Sessions

Chaque session active : les tunnels IPsec/IKEv2 actuellement établis, identifiés par abonné, avec l'état du tunnel et du porteur. Vous pouvez inspecter une session pour voir ses détails. C'est ici que vous confirmez qu'un tunnel d'appel Wi-Fi spécifique d'un abonné est opérationnel.

Diameter

Les connexions de pairs Diameter au AAA/HSS qui portent l'authentification (SWm/SWx), avec l'état de connexion de chaque pair. C'est le premier endroit à vérifier lorsque les authentifications d'appel Wi-Fi échouent.

Limiteur de taux

Le ePDG termine les tunnels IPsec/IKEv2 Wi-Fi non fiables (SWu) et les relie à l'EPC via S2b, ce qui les rend exposés à tout appareil (ou toute source) sur Internet ouvert. Le **Limiteur de taux** est la défense contre un client saturant la configuration du tunnel : il limite les inondations IKE afin qu'un seul appareil malveillant ou une source attaquante ne puisse pas épuiser la passerelle. L'onglet montre les **seuils** appliqués avec un compte en direct de combien d'**IP** et d'**IMSI** sont **actuellement bloqués**. Les seuils sont les limites de requêtes **par IP** et **par IMSI**, chacun exprimé comme un nombre de tentatives d'authentification dans une **fenêtre** glissante, et la **durée de blocage** appliquée une fois qu'une limite est dépassée.

Sous les seuils, vous pouvez **rechercher** n'importe quelle adresse IP ou IMSI pour voir si elle est bloquée et combien d'échecs elle a accumulés, et **supprimer** ce bloc afin que les futures tentatives d'authentification soient à nouveau autorisées ; une seule action **Tout effacer** supprime chaque bloc et réinitialise tous les compteurs d'échecs en une seule fois. C'est ici qu'un opérateur confirme pourquoi le tunnel d'appel Wi-Fi d'un abonné est refusé, et libère un bloc une fois que la source fautive s'est stabilisée.

GeoIP

GeoIP est le contrôle d'admission basé sur le pays du ePDG : comment un opérateur restreint l'établissement de tunnels VoWiFi aux pays autorisés en faisant correspondre l'adresse IP source de chaque tunnel entrant avec une base de données GeoIP. L'onglet montre si le filtrage est **activé** et si la base de données est **prête** (chargée et utilisable), le **mode**, et la **liste des pays** à laquelle le mode s'applique. Le mode est soit **liste blanche** (seuls les pays listés peuvent se connecter) soit **liste noire** (les pays listés sont refusés). Il montre également la **base de données GeoIP en cours d'utilisation** et si les **IPs de pays inconnus** sont autorisées ou bloquées. Ce sont des adresses sources que la base de données ne peut pas résoudre à un pays.

Une fois que le fichier de la base de données GeoIP a été mis à jour sur le disque, l'onglet peut **recharger** afin que le nouveau mappage prenne effet sans perturber les tunnels établis. C'est le contrôle qui maintient la configuration des tunnels VoWiFi confinée aux régions que dessert un opérateur.

Configuration

La **configuration** d'exécution du ePDG, les règles de **limitation de taux** (limites par abonné / par source qui protègent la passerelle), et la politique de **géo-IP** (quelles régions sources sont autorisées à établir des tunnels). Ce sont les contrôles qui déterminent qui peut se connecter et à quelle intensité.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du ePDG pour le dépannage d'une seule passerelle sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux de tunnels, le débit et d'autres séries chronologiques pour le ePDG sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens connexes

- Le **PGW** ancre le plan utilisateur du ePDG via **S2b**.
- Le **AAA/HSS** détient les données d'authentification des abonnés que les requêtes Diameter du ePDG résolvent.
- **TWAG** : le correspondant Wi-Fi *fiable*.

Noyau 5G

La section **Noyau 5G** donne à chaque fonction de réseau 5GC (NF) son propre tableau de bord en direct. Chaque tableau de bord montre la santé, l'enregistrement et les données opérationnelles que possède la NF (contextes UE, sessions PDU, pools IP, enregistrements NRF, politiques, sessions de facturation). Il fournit également des actions par NF et par élément pour effacer l'état. C'est l'équivalent 5GC des pages par élément pour les fonctions EPC/IMS. Il lit l'API OAM de chaque NF via le proxy backend OmniWeb.

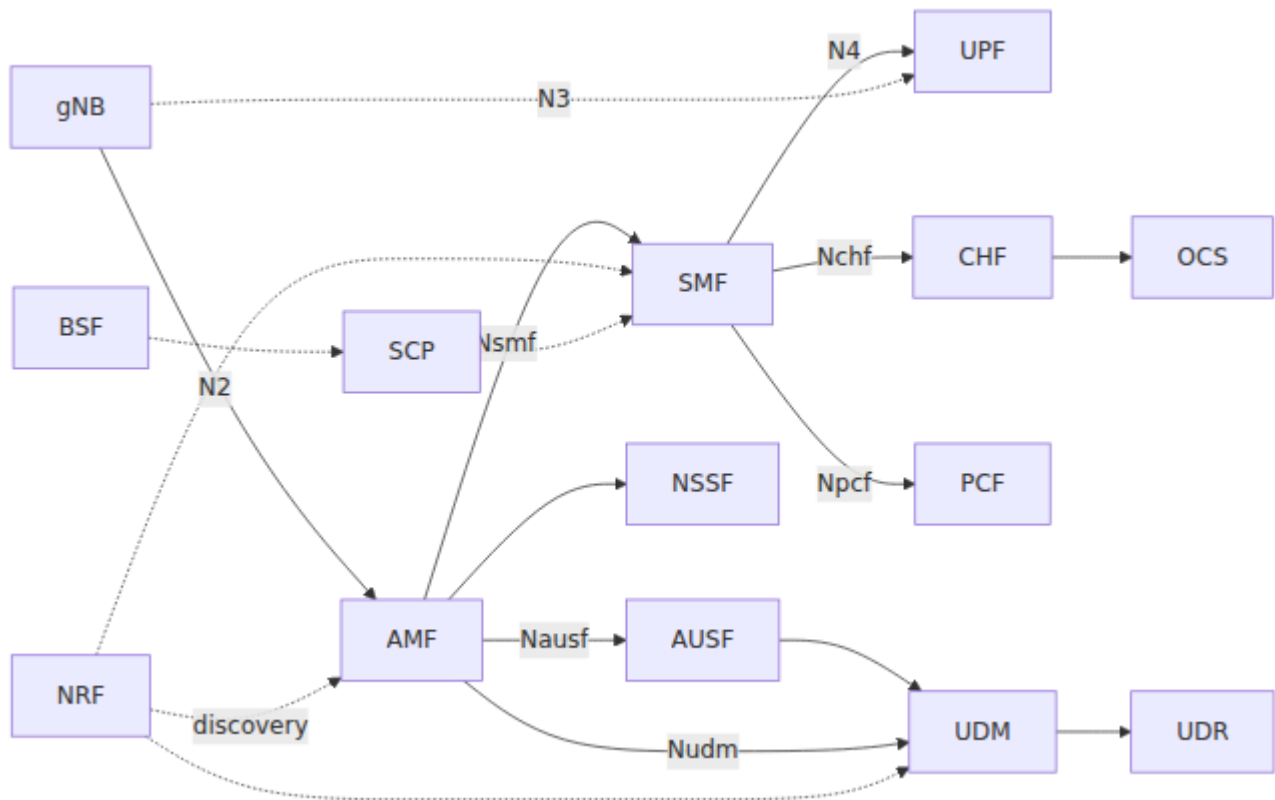
[← Guide des opérations](#)

Quand il apparaît

Le groupe **Noyau 5G** n'apparaît dans la barre latérale que lorsque le site sélectionné exécute réellement un plan de contrôle 5GC. OmniWeb se base sur la présence d'un **AMF et/ou SMF** dans l'inventaire du site. Un UPF ou CHF isolé partagé avec l'EPC n'est pas un 5GC et ne montre pas cette section.

OmniWeb déduit quelles NFs apparaissent, et l'adresse de l'API OAM de chaque NF, **directement à partir de l'inventaire Ansible du site** : les groupes NF 5GC définis dans le fichier hôte. Ajouter ou déplacer une NF est donc un changement d'inventaire sans rien à modéliser manuellement. Chaque NF se résout à une étiquette, une description, une IP et un port. OmniWeb sert le registre résolu via `/api/5gc/nf-registry`. Les tableaux de bord interrogent ensuite l'API OAM de chaque NF via le proxy (`/api/5gc/nf/<id>/...`), de sorte que tout le trafic reste derrière la seule passerelle authentifiée. Voir [le modèle de configuration](#). Les déploiements qui n'exécutent aucun inventaire (par exemple, le service hébergé) reviennent à un bloc statique `fivegc` dans la configuration d'OmniWeb.

Les NFs



Chaque NF a son propre tableau de bord :

NF	Fonction	Données clés affichées
NRF	Fonction de dépôt de réseau	Instances NF enregistrées (groupées par type), services enregistrés, abonnements : voir ci-dessous
AMF	Gestion d'accès et de mobilité	Liste UE, gNodeBs connectés (avec gNB-ID / TAC / PLMN / SST décodés), statistiques, mode maintenance
SMF	Gestion de session	Sessions PDU, Pools IP , association UPF, statistiques
UDM	Gestion unifiée des données	Liste UE, statistiques
UDR	Dépôt unifié de données	Santé HSS, abonnés
AUSF	Serveur d'authentification	Sessions AUSF (auth), statistiques
PCF	Contrôle des politiques	Politiques AM, politiques SM, statistiques
CHF	Fonction de facturation	Sessions de facturation, santé CGrateS, enregistrements CDR
NSSF	Sélection de tranche de réseau	Tranches, disponibilité NSSAI, statistiques
BSF	Support de liaison	Liaisons PCF, statistiques
SCP	Proxy de communication de service	Santé NF, cache de découverte, statistiques

Tous les déploiements n'exécutent pas chaque NF. Seules les NFs définies dans l'inventaire du site apparaissent. Chaque NF a sa propre page de référence. Suivez les liens ci-dessus.

L'onglet Pools IP du SMF

Comme exemple des données possédées par la NF que ces tableaux de bord affichent : le tableau de bord SMF a un onglet **Pools IP** montrant les pools d'adresses à partir desquels le SMF alloue des IPs UE, aux côtés de ses **Sessions PDU** en direct et de son **Association UPF** (l'état de lien N4/PFCP vers le plan utilisateur). Ensemble, cela répond à la question "le SMF est-il connecté à son UPF, quelles sessions sont actives, et est-il à court d'adresses ?" sans quitter OmniWeb.

Un tableau de bord en un coup d'œil

Chaque tableau de bord NF suit la même mise en page :

1. **Cartes de santé** en haut : Santé de l'API, Enregistrement NRF (cette NF est-elle enregistrée auprès du NRF ?), État de la NF, et Licence. Chacune interroge à un intervalle. Utilisez l'**Indicateur de sondage** dans l'en-tête pour mettre en pause ou voir l'heure de la dernière mise à jour (le sondage est un modèle partagé : voir [Opérations communes](#)).
2. **Actions** : opérations au niveau de la NF (voir ci-dessous).
3. **Sections de données** : le détail de l'état de l'API, le détail de l'enregistrement NRF, et les tableaux spécifiques à la NF du tableau ci-dessus, chacun se rafraîchissant automatiquement. Les tableaux décodent automatiquement ce qu'ils peuvent : PLMN/TAC/SST à partir des termes S1AP encodés en Erlang, horodatages en temps relatif, états en jetons colorés, et liens croisés (une valeur de type NF renvoie au tableau de bord de cette NF).

Actions

Les tableaux de bord exposent des actions pour effacer l'état de la NF. Chacune demande d'abord une confirmation, car elles sont destructrices :

NF	Actions au niveau de la NF	Actions par ligne
AMF	Effacer tous les contextes UE · Effacer le cache	Désenregistrer un UE
SMF	Libérer toutes les sessions PDU · Effacer le cache · Réassocier PFCP (rétablir l'association UPF)	Libérer une session PDU
NRF	Désenregistrer toutes les NFs	Désenregistrer une NF · Supprimer un abonnement
AUSF	Effacer toutes les sessions d'authentification	Effacer une session
UDM	Effacer le cache des abonnés	-
PCF	-	Supprimer une politique AM ou SM

Ceci permet à un opérateur de se remettre d'un état bloqué. Par exemple, forcer un SMF qui a perdu son UPF à se réassocier, supprimer un contexte UE qui ne peut pas être effacé, ou désenregistrer une NF obsolète du NRF.

Le tableau de bord NRF

Le NRF obtient une vue plus riche car il est le registre que tout le 5GC découvre à travers :

- **Cartes de métriques** : types de NF, instances totales, enregistrées (avec une barre de pourcentage du total), et services/abonnements.
- **Instances NF enregistrées** : groupées par type de NF. Le tableau de bord code en couleur chaque carte d'instance. La carte montre l'état d'enregistrement, le minuteur de battement, le nombre de services et le PLMN. Cliquez sur une instance pour son profil complet (avec un lien **Ouvrir le tableau de bord** vers cette NF et un bouton **Désenregistrer**).
- **Services enregistrés** : un tableau plat de chaque service que chaque instance annonce, ses versions et son état.
- **Désenregistrer toutes les NFs** : efface chaque enregistrement (chaque NF doit alors se réenregistrer).

Cela fait du NRF l'endroit pour répondre à la question "quelles NFs sont actives, sont-elles toutes enregistrées, et quels services offrent-elles ?"

Liens associés

- **Topologie du réseau** : les vues de topologie qui se lient à ces tableaux de bord.
- **Opérations communes** : les modèles de sondage, de configuration et de RBAC partagés avec chaque page d'élément.
- **PGW-C / SMF** et **UPF** : les pages de session/plan utilisateur côté EPC pour un EPC+5GC convergé.

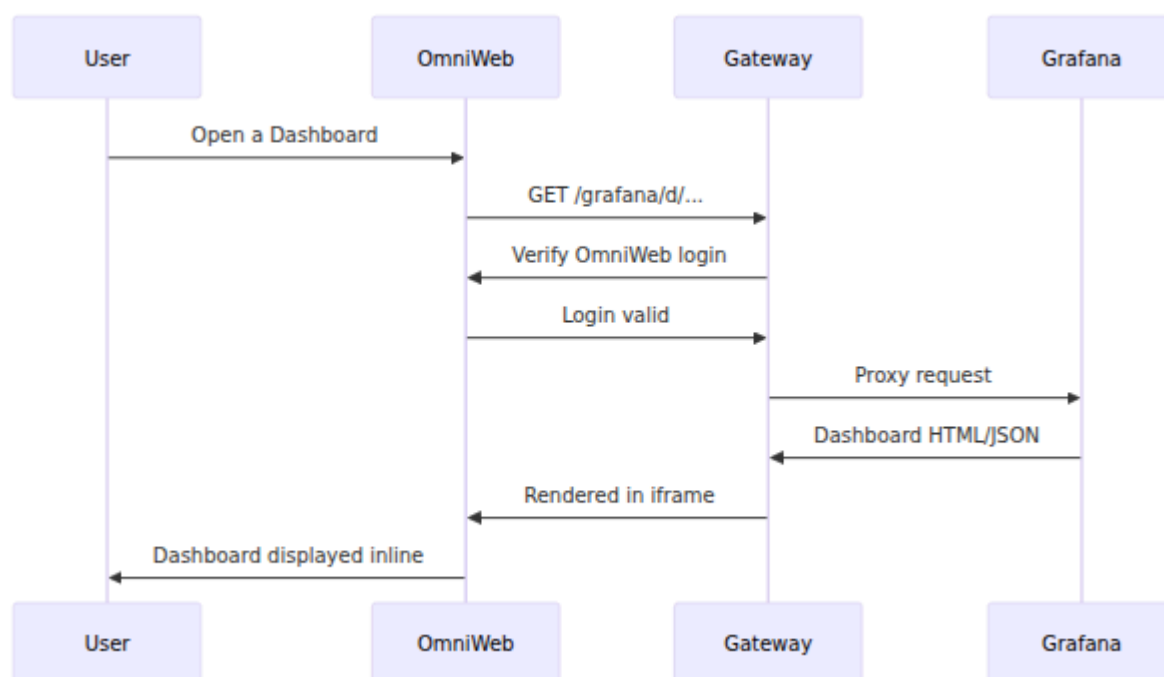
Tableaux de bord et statistiques Grafana

OmniWeb intègre Grafana directement dans le portail. Les opérateurs peuvent voir des tableaux de bord et des statistiques pour n'importe quel élément, ainsi que pour le réseau dans son ensemble, sans avoir besoin d'une connexion ou d'un onglet de navigateur séparé.

[← Retour au Guide des opérations](#)

Comment ça fonctionne

Grafana est servi derrière la passerelle authentifiée au chemin `/grafana/` et intégré en tant qu'iframe à l'intérieur d'OmniWeb. L'authentification est transparente : lorsque vous êtes connecté à OmniWeb, l'accès à Grafana est automatiquement autorisé en fonction de votre connexion OmniWeb. Il n'y a pas de deuxième mot de passe.



L'instance Grafana à laquelle OmniWeb se connecte est configurée par la variable d'environnement `GRAFANA_URL` (par défaut `http://localhost:3000`).

La passerelle gère le proxy et la vérification du single sign-on de manière transparente.

Deux façons d'accéder aux tableaux de bord

1. Onglet Tableaux de bord par élément

Les éléments qui sont étiquetés pour Grafana affichent un onglet **Tableaux de bord** dans leur espace de travail. OmniWeb interroge Grafana pour les tableaux de bord correspondant aux étiquettes de cet élément et rend celui qui est pertinent en ligne. Cela maintient les statistiques d'un élément à côté de ses données opérationnelles.

La correspondance des étiquettes est insensible à la casse. Ensembles d'étiquettes représentatifs :

Élément	Étiquettes Grafana correspondantes
UPF	upf
P-CSCF	pcscf, cscf
I-CSCF	icscf, cscf
S-CSCF	scscf, cscf
PGW-C, MME, SMSC, DRA, OCS, TAS	étiquettes spécifiques à l'élément

Pour faire apparaître un tableau de bord sous un élément, étiquetez-le dans Grafana avec l'étiquette de cet élément (par exemple, étiquetez un tableau de bord UPF `upf`).

2. Barre latérale Grafana

L'entrée **Grafana** → **Tableaux de bord** de la barre latérale liste tous les tableaux de bord disponibles. En sélectionnant un, il s'ouvre en ligne dans OmniWeb, et l'URL se met à jour pour refléter le chemin du tableau de bord afin que vous puissiez créer un lien direct vers un tableau de bord spécifique.

Statistiques

Les tableaux de bord intégrés sont l'endroit où se trouvent les **statistiques** à l'échelle du réseau et par élément : comptes et taux de sessions, débit, latence, taux de perte, santé des pairs Diameter/PFCP au fil du temps, volumes de CDR, comptes d'enregistrement et tendances de capacité. Les propres pages d'éléments d'OmniWeb vous donnent l'état *actuel* (et vous permettent d'agir dessus) ; Grafana vous donne la vue *historique* et les tendances. Ils sont conçus pour être utilisés ensemble. Enquêtez sur une alerte Grafana en passant aux pages opérationnelles de l'élément, aux journaux et aux traces.

Alertes

Le moteur d'alerte intégré de Grafana gère toutes les alertes basées sur des seuils. Les règles d'alerte sont définies dans Grafana et peuvent notifier par email, Slack, PagerDuty ou webhook. OmniWeb ne duplique pas les alertes. Il fournit le contexte opérationnel (pages d'éléments, journaux, traces) nécessaire pour enquêter lorsque qu'une alerte se déclenche.

Catégories d'alerte courantes :

Catégorie	Exemples
Disponibilité	Élément injoignable, pair Diameter hors ligne, association PFCP perdue
Capacité	Épuisement du pool IP, utilisation de la carte eBPF > 80%, seuil de compte d'abonnés VLR
Performance	Latence de configuration de session, taux de perte XDP, échecs de heartbeat
Trafic	Volume de CDR anormal, taux de perte d'appels, échecs de livraison de SMS

Enquête sur une alerte : Flux recommandé

Grafana alert fires

Open element
Dashboards tab
confirm the trend

Open element Overview
check current health

Open element Logs
find errors at the time

Session Trace
follow an affected
subscriber

1. Confirmez la tendance dans Grafana (Tableaux de bord).
2. Vérifiez l'état actuel sur l'aperçu de l'élément.
3. Consultez les journaux de l'élément autour du moment de l'alerte.
4. Si spécifique à un abonné, exécutez une trace de session. Voir [Journaux et traçage d'abonnés](#).

Homer : Capture SIP et Analyse de Flux d'Appels

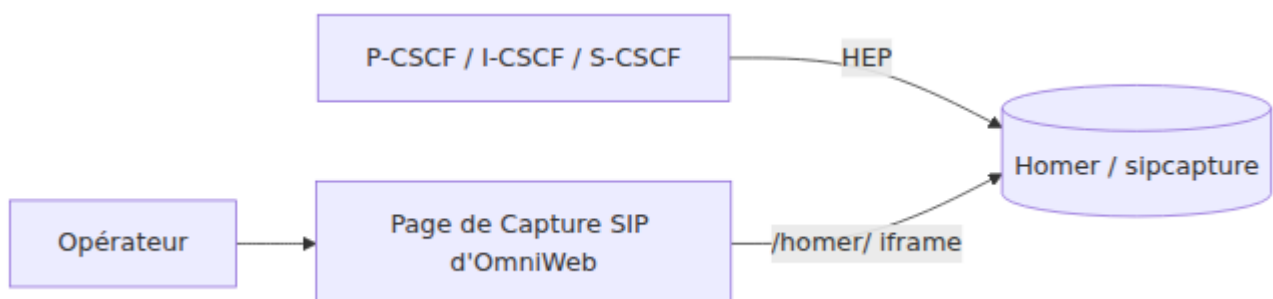
Homer est un système de capture et de recherche SIP (HEP / sipcapture).

OmniWeb intègre directement l'interface web de Homer, vous permettant de rechercher le trafic SIP capturé et de reconstruire l'échelle de signalisation d'un appel sans quitter le portail ou vous connecter séparément.

[← Guide des opérations](#)

Ce que c'est

Homer collecte les messages SIP de l'IMS (via le protocole HEP) et les stocke de manière à pouvoir les rechercher par call-id, numéro d'origine/destination, heure, et plus encore. Son interface web vous permet de trouver un appel et de dessiner son **diagramme de flux** complet : chaque message SIP entre les points de terminaison et les CSCF, avec les temps et toute cause d'échec/de raccrochage. OmniWeb ne réimplémente rien de tout cela. Il **intègre l'application Homer** dans un iframe sous **Capture SIP** (imbriqué sous Trace de session dans la barre latérale).



Authentification unique

Vous ne vous connectez pas à Homer séparément. OmniWeb proxy l'application Homer à `/homer/` et injecte les en-têtes d'auth-proxy en cours de route, de sorte que l'interface intégrée est **déjà authentifiée**, sans invite de connexion Homer. Elle est accessible via le même portail OmniWeb authentifié que Grafana et Loki, donc une connexion OmniWeb la régit également.

L'entrée **Capture SIP** n'apparaît dans la barre latérale que lorsque Homer est **configuré et accessible** pour le déploiement. OmniWeb le sonde et cache l'entrée si elle n'est pas présente, vous n'accédez donc jamais à une page morte.

Homer vs Trace de session

OmniWeb dispose de deux manières complémentaires d'examiner la signalisation, et il est utile de savoir laquelle utiliser :

	Homer (Capture SIP)	Trace de session
Portée	SIP uniquement, en profondeur	L'ensemble du réseau : Diameter, GTP-C, PFCP, SIP, MAP
Question à laquelle il répond	"Que faisait le flux SIP de cet <i>appel</i> , message par message, avec le timing et la cause de raccrochage ?"	"Que s'est-il passé pour ce <i>client</i> à travers chaque élément ?"
Meilleur pour	Diagnostiquer un appel VoIP/VoLTE, un enregistrement échoué, un raccrochage spécifique	Suivre un IMSI/MSISDN de bout en bout à travers le cœur

Utilisez Homer lorsque vous avez un appel à disséquer ; utilisez Trace de session lorsque vous suivez un abonné à travers l'ensemble de la pile. Homer

est également lié au guide [Logs & Tracing des abonnés](#).

Liens connexes

- [Logs & Tracing des abonnés](#) : Trace de session inter-réseaux et où Homer s'intègre.
- [Tableaux de bord Grafana & Statistiques](#) : l'autre outil de surveillance intégré, accessible de la même manière authentifiée.

HSS : Serveur d'Abonnés à Domicile

Le **HSS** (Serveur d'Abonnés à Domicile) est la base de données principale des abonnés pour le cœur mobile. Il contient les identités de chaque abonné (IMSI, MSISDN et SIM/ICCID), le matériel de clé d'authentification qui prouve qui ils sont, et les profils de service EPC, IMS, PCRF et de roaming qui indiquent ce que chaque abonné peut faire sur le réseau. Le MME le lit via S6a pour authentifier et localiser un appareil et pour apprendre son abonnement EPC. Le CSCF le lit via Cx pour l'enregistrement IMS et les déclencheurs de service iFC. Le PCRF tire ses règles de politique et de facturation de celui-ci. Un opérateur utilise son tableau de bord pour provisionner et rechercher des abonnés, organiser les profils de service partagés, et vérifier la santé du HSS.

[← Guide des Opérations](#)

Le tableau de bord est une page d'élément par instance. Il s'ouvre depuis la barre latérale lorsqu'un HSS fonctionne dans l'inventaire du site. Tout le trafic passe par le proxy backend OmniWeb vers l'API du HSS, il reste donc derrière la passerelle authentifiée unique. Les réponses reviennent dans une enveloppe `{status, response}`. Un lien de documentation dans l'en-tête de la page fournit une aide contextuelle. La page a des onglets.

Abonnés

L'onglet d'accueil est le répertoire des abonnés. Recherchez **par IMSI, MSISDN ou ICCID** pour trouver un enregistrement. La recherche résout également un abonné **par adresse IP** lorsque vous tracez une session en direct jusqu'à son propriétaire. Ouvrez un enregistrement pour afficher l'aperçu de l'abonné : un diagramme de relation qui relie l'abonné à son **identité** (IMSI), son **statut** (activé, et si IMS est activé), et les profils **EPC, IMS** et de **roaming** qui lui sont assignés. La page montre les APN du profil sous le profil EPC. Le HSS détient des valeurs de clé sensibles mais ne les affiche pas. Vous pouvez les mettre à jour, mais elles sont lues comme étant expurgées.

Provisionnement

Créez ou modifiez un abonné à partir du formulaire de provisionnement. Le formulaire regroupe l'identité, les informations d'identification, la SIM et les profils en un seul endroit :

- **Identité de l'abonné** : IMSI, un nom d'abonné, et les commutateurs **activé** et **IMS-activé**.
- **Jeu de clés d'authentification** : l'algorithme d'authentification, **Ki** et **OPc** (ou **OP**), **AMF**, **SQN**, et le mot de passe SIP utilisé pour IMS.
- **Carte SIM** : l'**ICCID**, si c'est un eSIM, les valeurs PIN/PUK et les détails de lot et de fournisseur.
- **Numéros de téléphone** : assignez un ou plusieurs **MSISDN**. Recherchez des numéros existants au fur et à mesure que vous tapez afin de ne pas créer un numéro deux fois.
- **Attribuer des profils** : attachez les profils **EPC**, **IMS** et de **roaming** qui donnent à l'abonné son service.

Vous pouvez mettre à jour les abonnés existants de la même manière. Vous pouvez supprimer un abonné de son enregistrement.

SIMs

L'inventaire des SIM contient chaque **SIM** que le HSS connaît. Recherchez-le **par ICCID**. Chaque SIM porte son **ICCID**, indicateur eSIM, nom de lot et fournisseur, ses valeurs de clé de transport (**KIC**, **KID**) et eSIM **LPA**, et l'ensemble complet des **clés ADM**. Gérez les **jeux de clés** d'authentification qui soutiennent les SIM (Ki/OPc/AMF/SQN) ici. Ils forment le magasin d'informations d'identification auquel se réfèrent les enregistrements des abonnés. Vous pouvez créer, modifier et supprimer des SIM.

MSISDNs

Le répertoire MSISDN contient le pool de numéros de téléphone provisionnés. Recherchez **par chiffres** pour une correspondance partielle afin de trouver ou vérifier un numéro avant de l'assigner. Vous pouvez créer, modifier et supprimer des numéros. Vous attachez des numéros aux abonnés lors du provisionnement.

Profils de service

Les profils de service sont les blocs de construction réutilisables qui indiquent ce qu'un abonné peut faire. Un abonné les référence plutôt que de porter sa propre copie. Un changement dans un profil s'applique donc à tous ceux qui l'utilisent.

Profils EPC

L'abonnement au cœur de paquets que le MME applique. Un **profil EPC** définit le **mode d'accès au réseau**, la bande passante agrégée **downlink/uplink** UE-AMBR, l'**intervalle TAU**, et la liste des **profils APN** que l'abonné peut utiliser. Un APN est le **APN par défaut**. Chaque **profil APN** associe un **identifiant APN** à un **profil QoS APN** et un **profil PCRF**. Vous pouvez marquer un profil APN comme par défaut. Un profil EPC doit référencer au moins un profil APN. L'APN par défaut doit être l'un des APN assignés.

Développez un profil EPC pour lister ses profils APN. **Ajouter APN** attache un APN au profil. L'action de désassociation sur chaque ligne **le retire uniquement de ce profil EPC**. Le HSS conserve le profil APN lui-même. Vous pouvez le réajouter plus tard, ou d'autres profils EPC peuvent le réutiliser. Un profil doit conserver au moins un APN, donc vous ne pouvez pas supprimer le dernier. Le HSS efface automatiquement l'APN par défaut si vous retirez l'APN auquel il faisait référence.

Profils APN

L'onglet Profils APN liste chaque profil APN indépendamment des profils EPC qui l'utilisent. Il montre son **identifiant APN**, **profil QoS APN** et **profil PCRF**. La colonne **Utilisé par** nomme chaque profil EPC qui référence l'APN. Il marque l'APN comme **Orphelin** lorsque aucun profil EPC ne le référence. Un APN atteint cet état une fois que vous l'avez retiré du dernier profil EPC qui l'utilisait. Le filtre **Orphelin uniquement** filtre la liste pour ne montrer que ceux-ci, afin que vous puissiez trouver et nettoyer les APN inutilisés.

Vous pouvez créer des profils ici, les modifier et les supprimer. Un nouveau profil commence sans attachement. Pour le lier au service d'un abonné, ajoutez-le à un profil EPC. Vous ne pouvez pas supprimer un profil APN qui est encore lié à un ou plusieurs profils EPC. Retirez-le d'abord de ces profils, puis supprimez-le de cet onglet.

Profils QoS APN

L'onglet Profils QoS APN gère les modèles QoS au niveau APN réutilisables auxquels les profils EPC et APN pointent. Chaque abonné dont l'APN référence

un modèle obtient la même qualité de service sur son porteur par défaut. Chaque modèle porte un **nom** et un **QCI** (l'Identifiant de Classe QoS qui associe le porteur à un comportement de délai et de perte standardisé). Il porte également un **ARP** (la priorité d'allocation/de rétention), avec des indicateurs de **capacité de préemption** et de **vulnérabilité à la préemption**. Ces indicateurs décident si le porteur peut être priorisé ou être priorisé par d'autres lorsque les ressources sont rares. Chaque modèle porte également les taux agrégés **APN-AMBR** uplink et downlink, et si la facturation **en ligne** et **hors ligne** sont activées.

Vous pouvez créer, modifier et supprimer des modèles. Vous pouvez également cloner un modèle pour en dériver une nouvelle variante. Un profil APN référence un modèle QoS plutôt que de porter sa propre copie. Si vous modifiez un modèle, vous redéfinissez la QoS de chaque APN qui l'utilise. Vous ne pouvez pas supprimer un modèle que référence encore un profil APN. Réaffectez d'abord ces APN.

Profils QoS APN

Les paramètres de qualité de service par APN auxquels un profil APN pointe : le **QCI**, **ARP** et la **capacité/vulnérabilité de préemption**, la bande passante **downlink/uplink** APN-AMBR, et si la facturation **en ligne (Gy)** et **hors ligne (Rf)** s'applique. Vous pouvez cloner un profil pour en dériver une nouvelle variante à partir d'un existant.

Profils IMS

L'abonnement IMS que le CSCF lit via Cx. Un **profil IMS** porte un **modèle iFC** : les Critères de Filtrage Initiaux qui décident quels serveurs d'application reçoivent le trafic SIP d'un abonné. Vous pouvez créer, modifier et supprimer des profils.

IPs Statique

Allocations d'IP fixes pour les abonnés qui doivent toujours recevoir la même adresse, gérées aux côtés des données d'abonnement EPC.

PCRF

La couche de politique que le PCRF applique. Une vue de relation lie les trois parties :

- **Profils PCRF** : la politique nommée à laquelle l'APN d'un abonné fait référence, composée d'un ensemble de règles de facturation.
- **Règles de facturation** : chacune avec un **type de règle** et une **précédence**, un **QCI** et un **ARP**, des limites MBR/GBR **downlink/uplink**, et un **groupe de notation** et un **identifiant de service** pour la facturation. Un porteur dédié transporte une règle avec un MBR ou GBR.
- **Règles d'information de flux** : les modèles de flux de trafic attachés à une règle de facturation qui définissent quels paquets elle correspond.

Vous pouvez créer, modifier et supprimer les trois. Si vous modifiez une règle de facturation, vous affectez chaque profil qui l'utilise.

Roaming

La politique de roaming que le HSS applique aux abonnés entrants et sortants. Un **profil de roaming** définit une **action de données par défaut**, une **action IMS par défaut**, et une liste de **règles de roaming**. Chaque règle se base sur un **MCC/MNC** et définit l'**action de données** et l'**action IMS** pour ce réseau. Vous pouvez donc autoriser ou bloquer des réseaux visités spécifiques tandis que le profil par défaut couvre le reste. Pour ajouter une règle, utilisez la recherche d'opérateur pour trouver le MCC/MNC d'un réseau à partir d'un nom d'opérateur (à partir d'IR.21). Les règles sont partagées. Si vous modifiez une règle, vous affectez chaque profil qui l'utilise.

EIR

Le Registre d'Identité d'Équipement. Chaque **règle EIR** correspond à un **IMEI** par expression régulière et définit une **action** : autoriser ou bloquer. Vous pouvez donc interdire un modèle de dispositif ou un téléphone spécifique du réseau. Une recherche par modèle de dispositif aide à construire le modèle IMEI. Vous pouvez créer, modifier et supprimer des règles.

Statut

Une lecture de santé sur une seule page du HSS lui-même : la santé de l'**API**, de la **base de données** et de la **licence**, et les **comptes d'entités** pour le total des **abonnés**, **profils EPC**, **profils IMS**, **SIMs**, **MSISDNs** et **profils de roaming**. C'est la confirmation la plus rapide que le HSS est opérationnel et combien il gère. Les intégrations Grafana fournissent les tableaux de bord de surveillance et de statistiques.

L'onglet **Réplication** montre l'état de la réplication de la base de données vers toutes les instances HSS pairs. L'onglet **Journaux** suit la sortie de journal en direct du HSS. Utilisez-le pour dépanner une seule instance sans quitter OmniWeb.

Réplication

L'onglet Réplication lit la santé de la réplication PostgreSQL de la base de données des abonnés du nœud HSS et la dessine comme une topologie en direct. Chaque nœud montre si sa base de données est un **primaire** ou un **de secours**. Un de secours est un nœud qui est en récupération. Il rejoue les changements du primaire plutôt que d'accepter des écritures de sa propre part. Pour un primaire, l'onglet dessine chaque de secours connecté comme un lien en aval. Le lien montre l'**adresse client** du de secours, le **slot de réplication** par lequel il diffuse, son **état de streaming**, et le **retard de réplication** mesuré par rapport à la position WAL actuelle du primaire. L'onglet montre le retard en octets, donc un réplique qui accuse un retard se distingue d'un coup d'œil. Si chaque slot de réplication est actuellement **actif**, cela détermine si son lien est considéré comme sain ou cassé.

Un opérateur utilise cet onglet pour confirmer que la base de données des abonnés se réplique à travers le cluster HSS : qu'un changement provisionné sur un nœud atteindra les autres, et qu'un de secours existe pour basculer. Un réplique en retard montre un chiffre de retard croissant. Un réplique cassé ou déconnecté perd son lien. Si deux instances HSS ou plus fonctionnent mais qu'aucune d'elles ne se réplique, l'onglet signale l'ensemble du cluster comme

un écart de réplication. Corrigez cela avant que cela ne devienne un risque de perte de données.

Opérations

Deux opérations au niveau des abonnés agissent sur une session en direct plutôt que sur l'enregistrement stocké :

- **Annuler-Location (CLR)** : envoyer une demande d'annulation de localisation S6a à l'MME de service d'un abonné. Cela détache l'abonné, afin qu'il se rattache et prenne les données d'abonnement modifiées.
- **PCRF Re-Auth** : demander au PCRF de ré-authentifier un abonné pour une session PDN donnée. Cela pousse des règles de politique ou de facturation mises à jour sur une session active.

Liens Associés

- **MME** : lit les données d'authentification des abonnés et d'abonnement EPC via **S6a**. C'est la cible d'une annulation de localisation.
- **CSCF** : lit le profil IMS et iFC via **Cx** pour l'enregistrement IMS et le déclenchement de service.
- **PCRF / PCF** : applique les profils PCRF, les règles de facturation et les règles de flux conservées ici. C'est la cible d'une ré-authentication.
- **UDR** : le magasin de données d'abonnés partagé que le HSS front-end dans un cœur 5G.
- [Guide des Opérations](#) : retour à l'index des éléments.

LCS : Services de localisation (OmniLCS)

La fonction **LCS** fournit des **services de localisation** pour le cœur. Elle répond à la question "où se trouve cet abonné ?" et génère des alertes par diffusion cellulaire. Elle détermine la position d'un UE à partir de la cellule de service (et de la géométrie de cellule configurée), traite les demandes de localisation du réseau (immédiates et différées), et envoie des alertes commerciales mobiles / des avertissements par diffusion cellulaire à une zone. OmniWeb affiche l'inventaire des cellules du LCS, les corrections de localisation récentes et en direct, les demandes de localisation différées, les alertes et diffusions CAP ; les tendances à long terme se trouvent sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le LCS est une page d'élément par instance accessible depuis la barre latérale lorsque l'on navigue dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb, il reste donc derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : le **statut** du LCS, ses **pairs Diameter** (vers le MME/réseau de service), les sessions de localisation **actives** et **terminées**, le nombre de **cellules chargées**, et le résultat de la **synchronisation des cellules**. C'est la confirmation la plus rapide que le LCS est opérationnel et dispose d'une géométrie de cellule actuelle.

Cellules

L'**inventaire des cellules** contre lequel le LCS se positionne : l'id de chaque cellule, latitude/longitude, rayon, hauteur, TAC/LAC, PCI, EARFCN, azimuth et RAT. Vous pouvez ajouter, modifier et supprimer des cellules ici. Cette géométrie est ce qui transforme un id de cellule de service en une position.

Localisation

Corrections de **localisation récentes** : l'abonné de chaque correction, la cellule de résolution, la position calculée, la précision et la méthode. Une localisation peut être **demandée** pour un abonné depuis ici, et l'ouverture d'une correction montre sa position autorisée connue pour la dernière fois. C'est ici qu'un opérateur confirme un résultat de positionnement.

Différé

Les **demandes de localisation différées en attente** que le LCS détient. Alors que l'onglet Localisation répond à la question "où se trouve cet abonné *maintenant*", une **MT-LR différée** (demande de localisation mobile terminée différée) demande au réseau de rapporter la position d'un abonné **plus tard, lorsqu'un déclencheur se déclenche**, plutôt qu'immédiatement : le GMLC arme la demande et le rapport revient lorsque la condition est remplie. Les déclencheurs courants sont la **disponibilité de l'UE** (rapporter la prochaine fois que l'appareil devient accessible, ayant été inactif ou inaccessible lorsque la demande a été faite), la localisation **périodique** (rapporter à un **intervalle** fixe pour un **nombre de rapports** défini), et les événements de zone/mouvement (rapporter lorsque l'UE entre, sort ou se déplace dans une zone désignée). C'est ainsi qu'un opérateur planifie le positionnement pour un abonné qui ne peut pas être trouvé pour le moment ou qui doit être suivi dans le temps.

Chaque ligne liste l'abonné de la session différée par **IMSI**, son **type d'événement/déclencheur** (périodique ou déclenché), l'**intervalle** de rapport en secondes et le **nombre** de rapports à envoyer, et son **statut** : en attente tant qu'il attend le déclencheur, actif une fois le rapport commencé. Un

opérateur peut **créer** une nouvelle demande différée depuis ici, en nommant l'IMSI cible, le type de déclencheur et, pour le rapport périodique, l'intervalle et le nombre. Un opérateur peut également **annuler** une session en attente à tout moment, ce qui désarme la demande armée afin qu'aucun rapport supplémentaire ne soit produit. La liste interroge donc le statut d'une session qui se met à jour au fur et à mesure que le réseau l'arme et que le déclencheur se déclenche.

Alertes CAP

Les alertes du **Protocole d'Alerte Commun (CAP)** que le LCS connaît, chacune avec son identifiant, son statut, son urgence, sa gravité et sa zone cible. Ce sont les messages d'urgence/alerte éligibles à être diffusés.

Diffusions

L'onglet **Diffusions** montre les messages de **diffusion cellulaire** actifs (type d'alerte, identifiant de message, série, cellules cibles et statut) : les alertes actuellement envoyées à une zone.

Journaux

L'onglet **Journaux** affiche en temps réel la sortie des journaux du LCS pour le dépannage sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux de demande de localisation et d'autres séries chronologiques sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens connexes

- Le **MME** demande le positionnement via les interfaces de localisation et est le pair Diameter du LCS.
- Les **alertes CAP** et les **diffusions** alimentent le système d'alerte par diffusion cellulaire.

Serveur de Licence : Licences Omnitouch

Le **Serveur de Licence** est l'autorité de licence Omnitouch contre laquelle les fonctions du réseau vérifient. Chaque produit Omnitouch (le MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF et les autres) valide son droit d'utilisation auprès du Serveur de Licence avant de fonctionner, demandant si un **titulaire de licence** donné est autorisé pour ce **produit** et si la licence est toujours dans sa période de validité. Le serveur détient des **licences signées** cryptographiquement, chacune accordant à un titulaire de licence un ensemble de produits avec une période de validité et des métadonnées, et il répond aux requêtes de droit d'utilisation et enregistre chaque demande qui lui est faite. Parce qu'une licence n'a de sens que contre une horloge de confiance, le serveur suit également une source de **temps de confiance** afin qu'une licence ne puisse pas être réactivée en faisant reculer l'horloge d'un nœud. OmniWeb affiche ce qui est licencié et sa santé, le journal des requêtes de droit d'utilisation que les fonctions du réseau ont effectuées, un outil de requête à la demande, et les journaux en direct du serveur.

[← Guide des Opérations](#)

Le Serveur de Licence est une page d'élément par instance accessible depuis la barre latérale lorsque l'on se trouve dans l'inventaire du site, avec une vue de flotte où plusieurs sont déployés. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du Serveur de Licence, de sorte qu'il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu / Statut

Une lecture sur un seul écran de ce que le serveur licence et s'il est en bonne santé. Les cartes récapitulatives donnent le nombre de **produits totaux**, combien sont **valides** et **invalides**, et le nombre de **titulaire de licences** distincts. Un panneau de **temps de confiance** montre l'état de la source d'horloge du serveur : **valide**, **période de grâce** ou **invalid**. Lorsque le temps de confiance n'est pas disponible, le serveur ne peut pas valider les licences en toute sécurité, et cela élève la santé de la page à un avertissement ou une erreur.

Le tableau des **Produits Licenciés** liste une ligne par produit licencié, chacun montrant le **produit**, le **titulaire de licence** auquel il est accordé, quand il a été **émis**, ses dates de **début** et **d'expiration** (avec un indicateur "jours restants" ou "expiré il y a N jours" qui devient ambre dans les 30 jours précédant l'expiration et rouge une fois dépassé), et son statut **valide/invalid**. Ouvrir une ligne développe le détail complet : les horodatages de validité exacts, si la **signature cryptographique** est valide, toutes les métadonnées du produit, et la signature elle-même. C'est la confirmation la plus rapide que les fonctions du réseau sont toutes licenciées et que rien n'est sur le point d'expirer.

Journaux de Requêtes

La trace d'audit des **requêtes de droit d'utilisation** que les fonctions du réseau ont faites contre le serveur. Chaque ligne enregistre l'**horodatage**, l'**IP source** d'où provient la demande (quel hôte de fonction réseau a demandé), le **titulaire de licence** et le **produit** sur lequel il a posé la question, la **décision** (**autorisé** ou **rejeté**), et, en cas de rejet, la **raison**. La liste peut être filtrée par décision, par produit, et par une recherche partielle d'**IP source** ou de **titulaire de licence**, et elle est paginée. C'est ici que vous voyez, par exemple, qu'une fonction nouvellement déployée est rejetée parce que son produit n'a jamais été licencié, ou confirmez qu'une fonction s'enregistre avec succès.

Requête de Licence

Une **vérification de droit d'utilisation** à la demande. Entrez un **titulaire de licence** et un **produit** et l'outil demande au serveur la même question qu'une fonction réseau poserait (ce titulaire de licence a-t-il droit à ce produit en ce moment) et retourne le verdict : **valide** ou **invalide**, la date **valide jusqu'à** de la licence, l'**horodatage** de la réponse, toutes les **métadonnées**, et la **signature**. C'est le moyen direct de confirmer un droit d'utilisation spécifique sans attendre que la fonction propriétaire s'enregistre, et cela liste les identifiants de produit connus (par exemple `omnihss`, `omniupf`, `omnimme`) afin que vous puissiez interroger le bon.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du Serveur de Licence pour le dépannage d'une seule instance sans quitter OmniWeb.

Liens Connexes

- **Chaque fonction réseau Omnitouch** : le MME, HSS, DRA, PGW-C, UPF, SGW-C, SMSC, CSCF et les autres valident leur droit d'utilisation ici ; l'onglet **Aperçu / Statut** de chaque produit montre un badge de santé de licence dérivé de cette vérification.
- [Guide des Opérations](#) : retour à l'index des éléments.

Journaux et Traçage des Abonnés

OmniWeb offre aux opérateurs plusieurs vues complémentaires en temps réel sur ce que fait le réseau :

1. **Journaux** : journaux de service structurés et en direct pour tout élément unique, alimentés par Loki.
2. **Traçage de Session** : une vue trans-réseau qui suit un abonné à travers chaque protocole et élément (Diameter, GTP-C, PFCP, SIP, MAP).
3. **Homer** : capture approfondie des paquets SIP/VoIP et analyse du flux d'appels.

[← Retour au Guide des Opérations](#)

Passer à un Abonné depuis un NF

De nombreuses fonctions réseau affichent un abonné, un UE ou une session par IMSI. Cela inclut le **MME** (UEs), **SGW-C**, **PGW-C** et **ePDG** (Sessions), **MSC** et **TAS** (Abonnés), et **SMSC** (Localisation). Dans chaque cas, une rangée de boutons de lien rapide vous permet de passer directement à cet abonné ailleurs, sans avoir à copier l'IMSI :

- **Aller au Dossier HSS** ouvre le dossier de provisionnement de l'abonné sur le HSS (résolu par IMSI à travers les instances HSS configurées).
- **Voir le Traçage de Session** ouvre l'échelle de signalisation en direct de l'abonné dans le Traçage de Session, limité à cet IMSI.
- **Voir les Journaux** ouvre l'onglet Journaux de *cet* élément pré-filtré à cet IMSI, afin que vous ne voyiez que les lignes de journal pour cet abonné.

Chaque bouton n'apparaît que lorsqu'il s'applique : l'IMSI est connu, et un HSS ou un Traçage de Session est configuré pour le site. L'ensemble s'adapte donc au déploiement.

Les liens rapides pour l'abonné (ici sur un MME UE) : un clic vers le dossier HSS, l'échelle de signalisation en direct, ou les journaux de cet élément filtrés pour l'abonné.

Journaux en Temps Réel (Loki)

Chaque élément a un onglet **Journaux**. Il interroge les journaux de service de l'élément depuis **Loki** et diffuse de nouvelles lignes à mesure qu'elles arrivent, vous permettant de suivre un élément en direct pendant que vous effectuez un changement ou reproduisez un problème.

L'onglet Journaux (ici sur un UPF) : lignes de journal structurées et codées par couleur diffusées depuis Loki, avec des filtres de service, de gravité, de protocole et d'abonné (IMSI). Chaque élément expose le même visualiseur.

Comment fonctionnent les requêtes de journaux

Le frontend construit une requête **LogQL** et l'envoie à travers la passerelle Loki du backend. Rien ne consulte Loki directement depuis le navigateur. C'est proxifié (et donc authentifié et audité) comme toute autre requête.



La cible Loki du backend est définie par la variable d'environnement `LOKI_URL` (par défaut `http://localhost:3100`). Les requêtes utilisent l'API de requête de plage de Loki avec une expression LogQL, une fenêtre temporelle, une limite de résultats et une direction (du plus récent au plus ancien ou vice versa).

Sélecteurs vs. filtres de pipeline

OmniWeb construit des requêtes structurées à partir de deux types de filtres :

Placement du filtre	Position LogQL	Exemple	Utilisation
Sélecteur	À l'intérieur du sélecteur de flux { ... }	<code>{hostname="omni-eval-upf01"}</code>	Choisir quels flux (quel hôte/service) lire. Indexé et rapide.
Pipeline	Après un	<code> level="error"</code>	Filtrer les lignes correspondantes par un champ structuré.

Un onglet Journaux typique d'un élément fixe l'hôte/service comme sélecteur et vous permet d'ajouter des filtres de pipeline (gravité, composant, identifiants d'abonné) par-dessus. Étant donné que les services Omnitouch émettent des lignes de journal **structurées**, vous pouvez filtrer sur de vrais champs plutôt que de greffer du texte libre.

Données de journalisation structurées

Les hôtes envoient des journaux structurés à Loki (configurés par le rôle commun Ansible). Deux sources structurées particulièrement utiles :

- **Journaux de service** : la sortie structurée propre à chaque NF, étiquetée par `hostname`/service, disponible sur l'onglet Journaux de cet élément.
- **Audit des commandes** : chaque commande exécutée sur un hôte, y compris qui s'est connecté (survivant de `sudo`/`su`), l'UID effectif, le binaire, le répertoire de travail et la ligne de commande complète. Envoyé à Loki. Voir [Journalisation des Audits](#) pour la référence des champs.

Utilisation de l'onglet Journaux

1. Ouvrez n'importe quel élément et sélectionnez **Journaux**.

2. Le visualiseur charge les lignes récentes pour cet élément et commence à interroger pour de nouvelles.
3. Affinez la vue avec des filtres de pipeline (par exemple, gravité, ou un IMSI/MSISDN si les journaux de service l'incluent).
4. Ajustez la fenêtre temporelle pour revenir à un événement passé.
5. Mettez en pause l'interrogation (indicateur d'en-tête) pour maintenir une vue stable pendant la lecture.

Astuce : Lors de l'investigation d'un abonné, filtrer les journaux d'élément par leur IMSI/MSISDN est la première étape rapide ; pour voir l'abonné à travers *plusieurs* éléments à la fois, utilisez le Traçage de Session ci-dessous.

Traçage de Session : Suivre un Abonné à Travers le Réseau

Le moteur de **Traçage de Session** corrèle la signalisation pour un seul abonné à travers plusieurs éléments et protocoles, fournissant une chronologie unifiée depuis l'attachement radio jusqu'à l'authentification, l'établissement de session et la livraison d'appels/SMS. C'est l'outil pour répondre à la question "que s'est-il passé avec cet abonné ?" sans sauter entre les CLI des éléments.

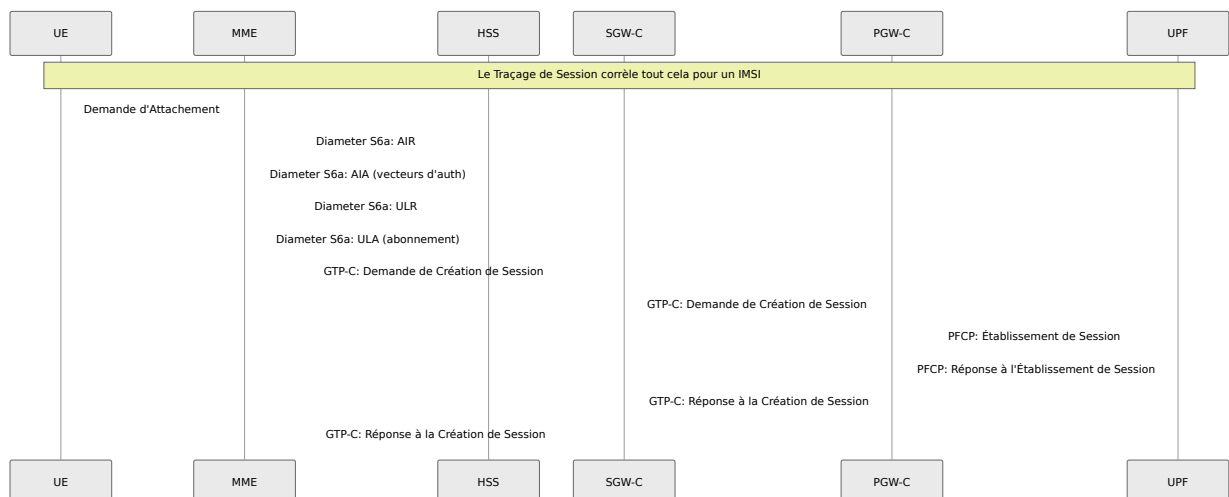
Traçage de Session : recherchez par IMSI ou MSISDN et corrélerez l'activité d'un abonné à travers Diameter, GTP-C, PFCP, SIP et MAP, avec des onglets par protocole en haut.

Protocoles pris en charge

Protocole	Ce qu'il montre	Éléments impliqués
Diameter	Authentification, politique, facturation	HSS, DRA, PGW-C, PCRF, OCS, CSCF (Cx/Dx/Rx)
GTP-C	Gestion de session (S5/S8, S11)	SGW-C, PGW-C, MME
PFCP	Règles de session du plan utilisateur (N4)	PGW-C/SMF ↔ UPF
SIP	Contrôle d'appel IMS	P-CSCF, I-CSCF, S-CSCF, TAS
MAP	Localisation SS7, authentification, SMS	MSC, HLR, CAMEL GW, IP-SM-GW

Traçage Utilisateur

La vue **Traçage Utilisateur** vous permet de rechercher par **IMSI** ou **MSISDN** et de voir chaque interaction de protocole corrélée pour cet abonné à travers le réseau. Un seul attachement, par exemple, fait ressortir l'authentification Diameter, la création de session GTP-C et l'installation de règle PFCP comme une séquence cohérente :



Onglets spécifiques aux protocoles

Chaque protocole a son propre onglet (**Diameter, GTP-C, PFCP, SIP, MAP**), plus un aperçu **Tous Protocoles**. Les onglets par protocole sont des vues filtrées. Ils aident lorsque vous poursuivez un problème spécifique à un protocole (par exemple, uniquement l'échange SIP d'un appel VoLTE) plutôt que de suivre un seul abonné à travers tout.

Échelle PCAP

L'onglet **Échelle PCAP** transforme une capture de paquets en une échelle : un diagramme de séquence ordonné dans le temps de la signalisation.

Téléchargez une capture PCAP ou PCAPNG (par exemple, depuis un tap réseau ou un traçage au niveau de l'élément) et OmniWeb analyse les paquets, identifie les nœuds de signalisation par adresse IP et rôle inféré (MSC/VLR, HSS, S-CSCF, etc.), et corrèle les requêtes avec leurs réponses en sessions. Le résultat est dessiné comme une échelle de messages à travers ces nœuds, ordonnée dans le temps, afin que vous puissiez lire un échange entier de haut en bas d'un coup d'œil.

Échelle PCAP : une capture téléchargée rendue comme une échelle à travers les nœuds détectés. Cliquez sur n'importe quel message pour voir son cadre décodé et son hexadécimal.

Cliquez sur un message sur l'échelle pour ouvrir son décodage complet et son hexadécimal brut, le même détail que vous obtiendriez d'un analyseur de protocole. L'outil reconnaît les familles de signalisation que vous rencontrez à travers un cœur mobile : MAP, CAMEL, TCAP, Diameter, SIP, GTP-C, PFCP et GSM SMS. Chaque capture que vous téléchargez est listée sur l'onglet afin qu'elle puisse être rouverte ou partagée avec un collègue plutôt que de faire circuler le fichier.

Flux en Direct

L'onglet **Flux en Direct** montre la même vue d'échelle, mais provenant en direct des journaux de signalisation structurés du réseau (via Loki) plutôt que d'un fichier téléchargé. À mesure que les éléments du réseau émettent des télémetries de signalisation, les flux d'appels récents par abonné apparaissent ici automatiquement, regroupés par IMSI, sans capture à télécharger.

Sélectionnez un flux pour le reconstruire dans la même échelle qu'un PCAP, de sorte qu'un flux en direct soit aussi riche que celui lu à partir d'un fichier, jusqu'au décodage par message et à l'hexadécimal.

Flux en Direct : flux d'appels récents tirés directement de la télémétrie de signalisation du réseau. Filtrez par IMSI, nœud ou protocole, puis ouvrez un flux pour rendre son échelle en direct.

Ouvrez un flux et OmniWeb le reconstruit dans la même échelle qu'un PCAP, mais à partir de la télémétrie propre du réseau, sans rien à capturer ou à télécharger. L'exemple ci-dessous est un attachement LTE d'un seul abonné, corrélé à travers chaque élément qui l'a touché : l'échange S1AP/NAS avec le **eNodeB**, l'authentification Diameter S6a et la mise à jour de localisation contre le **HSS**, et la configuration de session GTP-C à travers le **SGW-C** et le **PGW-C**. Tout cela apparaît sur une échelle ordonnée dans le temps, avec des temps de réponse aller-retour par message et un décodage complet à portée de clic.

Un flux en direct ouvert dans son échelle : l'attachement LTE d'un abonné à travers le eNodeB, MME, HSS, SGW-C et PGW-C, corrélant S1AP, Diameter S6a et GTP-C. Cliquez sur n'importe quel message pour son décodage et son hexadécimal, ou sur n'importe quel nœud pour se concentrer sur ses échanges.

Si aucune télémétrie de signalisation ne circule encore, l'onglet montre un état vide ; les flux se remplissent d'eux-mêmes à mesure que les éléments du réseau commencent à émettre de la télémétrie.

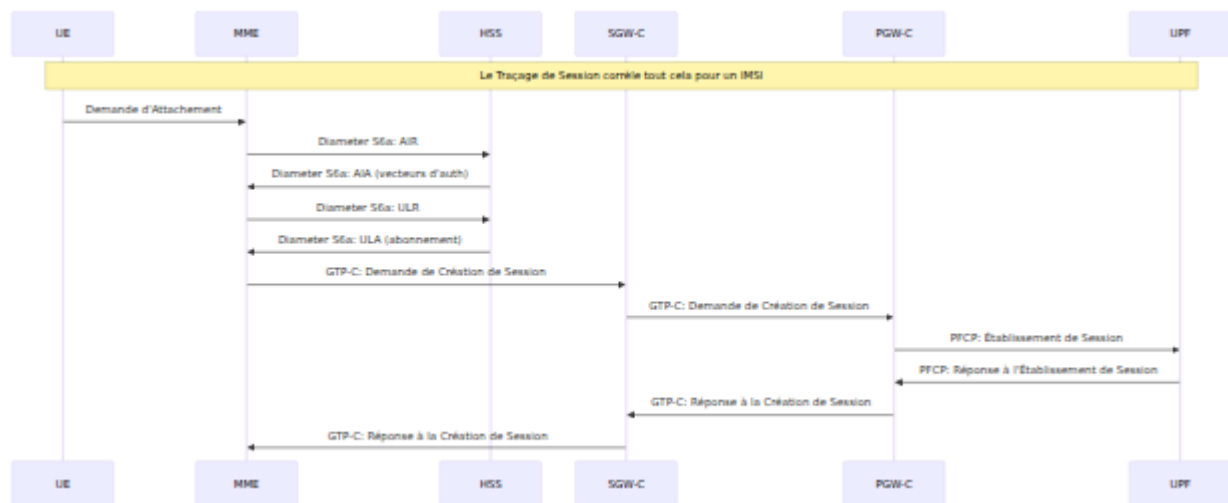
Homer : Capture SIP et Analyse des Flux d'Appels

OmniWeb s'intègre à **Homer**, la plateforme open-source de capture SIP et de dépannage VoIP, pour une visualisation approfondie des flux d'appels, un décodage de protocole et une recherche à travers la signalisation SIP capturée. Alors que le Traçage de Session donne un *résumé* inter-protocoles pour un abonné, Homer fournit le détail complet, message par message, des paquets SIP.

Disponibilité et accès

Homer est **optionnel** et détecté automatiquement. Au démarrage, OmniWeb vérifie `/api/homer/status` :

- Si Homer est configuré (`HOMER_URL` défini sur le backend) et accessible, une entrée **Homer** apparaît dans la barre latérale.
- Si Homer n'est pas déployé, l'entrée est simplement cachée, et rien d'autre ne change.



Cliquer sur **Homer** ouvre l'interface web Homer dans un nouvel onglet de navigateur. L'authentification est transparente : la passerelle vérifie votre connexion OmniWeb via le même système de connexion unique utilisé pour Grafana, donc il n'y a pas de seconde connexion. L'`HOMER_URL` du backend (et `HOMER_PROXY_SECRET`, lorsqu'il est défini) configurent l'intégration.

Cas d'utilisation

Homer est l'outil à utiliser lorsque le problème se situe dans la couche SIP elle-même :

- **Analyse des flux d'appels VoLTE** : tracez les séquences SIP `INVITE`/`BYE` à travers P-CSCF, I-CSCF, S-CSCF et TAS.
- **Dépannage VoWiFi** : analysez les interactions SIP entre ePDG ↔ P-CSCF.
- **Débogage d'enregistrement IMS** : inspectez les échanges `REGISTER` / `401` / `REGISTER` / `200 OK`.

- **Problèmes d'interconnexion** : capturez la signalisation SIP-trunk entre le MSC et les pairs SIP.

Traçage de Session vs. Homer

Les deux aident au dépannage, mais ils répondent à des questions différentes. Ils sont complémentaires, pas alternatifs :

Outil	Meilleur pour	Portée	Où il s'ouvre
Traçage de Session	"Suivez cet abonné à travers tout le réseau"	Diameter, GTP-C, PFCP, SIP, MAP corrélés par IMSI/MSISDN	En ligne dans OmniWeb
Homer	"Montrez-moi les messages SIP exacts pour cet appel"	Signalisation SIP/VoIP, décodage complet des paquets (VoLTE/VoWiFi/IMS)	Nouvel onglet (détecté automatiquement)

Un flux commun consiste à repérer une anomalie liée à SIP dans le Traçage de Session, puis à sauter vers Homer pour le flux d'appel détaillé.

Dépannage

Aucun journal n'apparaît sur l'onglet Journaux d'un élément

Symptômes : L'onglet Journaux est vide ou affiche "aucun résultat".

Causes possibles :

- Loki n'est pas accessible depuis le backend (`LOKI_URL` mal configuré).

- L'hôte n'envoie pas de journaux à Loki (expédition de journaux non exécutée / mal configurée).
- La fenêtre temporelle sélectionnée précède les journaux disponibles, ou l'étiquette de l'hôte ne correspond pas.

Résolution :

1. Confirmez que `LOKI_URL` pointe vers une instance Loki accessible.
2. Vérifiez que l'hôte de l'élément expédie des journaux (vérifiez l'agent d'expédition de journaux sur cet hôte).
3. Élargissez la fenêtre temporelle et retirez les filtres de pipeline pour confirmer que des lignes arrivent.

Le Traçage de Session ne retourne rien pour un abonné

Symptômes : Un Traçage Utilisateur par IMSI/MSISDN ne montre aucun événement.

Causes possibles :

- L'abonné était inactif dans la fenêtre sélectionnée.
- L'identifiant est mal tapé (IMSI vs. MSISDN).
- Les sources de traçage pour le protocole pertinent n'alimentent pas le moteur.

Résolution :

1. Vérifiez à nouveau l'identifiant et essayez l'autre (IMSI ↔ MSISDN).
2. Élargissez la fenêtre temporelle.
3. Confirmez avec l'onglet Journaux de l'élément que l'abonné était actif.

L'entrée Homer est manquante dans la barre latérale

Symptômes : Aucun lien **Homer** n'apparaît.

Causes possibles :

- Homer n'est pas déployé, ou `HOMER_URL` n'est pas défini sur le backend.
- Homer est inaccessible, donc `/api/homer/status` le signale comme indisponible.

Résolution :

1. Confirmez que Homer est déployé et que `HOMER_URL` est défini sur le backend d'OmniWeb.
2. Vérifiez que le backend peut atteindre Homer, puis rechargez OmniWeb (la détection s'exécute au démarrage).

MME : Entité de gestion de mobilité

Le **MME** est l'ancre du plan de contrôle de l'EPC. Il termine le **S1AP** vers les eNodeBs, exécute les procédures d'attachement, d'authentification et de mobilité pour chaque UE, et maintient un **contexte UE** pour chaque abonné attaché. Il récupère les données d'abonnement et d'authentification depuis le HSS via **S6a** (Diameter), établit des bearers sur la passerelle de service via **S11**, et coordonne les transferts inter-MME et inter-systèmes via **S10/N26**. En résumé, c'est le nœud qui décide où et comment chaque abonné s'attache, est paginé et se déplace à travers le réseau. OmniWeb affiche les eNodeBs en direct du MME, les contextes UE, les SGW et les pairs Diameter, les états des interfaces et le statut des transferts. Les tendances à long terme sont sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le MME est une page d'élément par instance accessible depuis la barre latérale lorsque l'on navigue dans l'inventaire du site, et, là où plusieurs sont déployés, une vue de flotte pour le statut agrégé. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du MME, ce qui le maintient derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : l'**état de l'API** du MME et un résumé de sa charge en direct, y compris les **eNodeBs** connectés, les **UEs** attachés, les **pairs SGW** et l'état de ses pairs **Diameter** (S6a). C'est le moyen le plus rapide de confirmer que le MME est opérationnel et de voir combien du réseau d'accès il dessert.

eNodeBs

Chaque eNodeB avec lequel le MME a une association S1AP, chaque ligne montrant l'**ID eNB global**, le nom et l'**état** de connexion. Ouvrez un eNodeB pour afficher son contexte : les cellules desservies et les TACs ainsi que les UEs qui y sont connectés. Un opérateur peut **mettre à jour la capacité MME** annoncée à un eNodeB, ce qui ajuste la manière dont l'eNodeB équilibre la charge des UEs à travers le pool MME (utilisé pour vider ou pondérer un MME pour maintenance ou rééquilibrage).

UEs

Le **contexte UE** de chaque abonné attaché, chaque ligne étant indexée par **IMSI** et **GUTI** avec son état de connexion et de mobilité et l'eNodeB de service. Ouvrir un UE montre son contexte complet. Une gamme d'actions par UE est disponible :

- **Pager** l'UE.
- **Envoyer à l'inactif** : libérer la connexion radio tout en conservant le contexte.
- **Décharger** l'UE vers un autre MME.
- **Demander un ré-attachement** : forcer l'UE à se ré-attacher.
- **Envoyer un SMS** à l'UE.
- **Supprimer** le contexte UE : effacer un abonné obsolète ou bloqué.

Vous pouvez également **rechercher l'opérateur / PLMN** pour un IMSI afin d'identifier les abonnés domestiques par rapport aux abonnés en itinérance.

Pairs S-GW

Les passerelles de service avec lesquelles le MME communique via **S11** (GTP-C), chaque ligne montrant l'**IP** du pair, sa **vivacité / atteignabilité**, le **compteur de redémarrage (récupération)** GTP et le **compteur de session** ancré sur cette passerelle. Le compteur s'incrémente lorsque le S-GW redémarre, ce qui indique au MME de rétablir les sessions qu'il détenait. Que le pair ait été appris par **DNS** ou soit une entrée **statique** est indiqué aux côtés de la **méthode de sélection** S-GW que le MME applique pour les abonnés domestiques et en itinérance. Ouvrez un pair pour lister les **sessions** qu'il transporte, chacune identifiée par **IMSI** avec ses **TEIDs S11** (les points de terminaison de tunnel côté MME et S-GW). C'est là qu'un opérateur confirme quels S-GWs sont opérationnels et voit comment les sessions UE sont réparties entre eux. Cela aide lors de l'équilibrage de charge ou du diagnostic des raisons pour lesquelles des bearers pour un groupe d'abonnés sont tombés avec une seule passerelle.

Réallocation GUTI et déchargement S10

Deux actions de mobilité sont pilotées par IMSI plutôt que par ligne :

- **Réallocation GUTI** : réallouer le **GUTI** d'un abonné connecté pour rafraîchir l'identité temporaire que l'UE présente (utilisé lors de la rotation des identifiants ou de l'effacement d'un décalage d'identité).
- **Déchargement S10** : forcer le déchargement d'un abonné vers **un autre MME**. Cela déplace le contexte d'un abonné spécifique hors de ce MME via S10, et complète le contrôle de capacité de l'eNodeB lorsque vous videz un MME.

S10

L'interface **S10/N26 inter-MME** est le chemin par lequel le contexte d'un UE est relocalisé lorsqu'il se déplace entre des MMEs dans un pool lors d'un **TAU** ou d'un **transfert** (et, via **N26**, entre le MME et un AMF pour l'interopérabilité EPC-5GC). L'onglet a deux parties. **Transferts actifs** liste les relocalisations en

cours, chacune montrant le MME **source** et **cible** et l'**IMSI** en cours de transfert, permettant à un opérateur de suivre un événement de mobilité ou de repérer un qui est bloqué. **Découverte des pairs MME** montre comment le MME trouve ses pairs dans le pool : les recherches **DNS / NAPTR** qu'il effectue et tout pair **statique** configuré, avec le FQDN et l'adresse de chaque pair. C'est là que vous confirmez que la mobilité inter-MME est saine et que le MME peut réellement atteindre les voisins dont il a besoin pour transférer des contextes. Cela complète l'action de **déchargement S10** par abonné pilotée depuis l'onglet UEs.

Diameter

Les pairs Diameter du MME, principalement le HSS via **S6a**, chaque ligne montrant l'**hôte** du pair, le **domaine** et l'**état** de connexion. Ouvrez un pair pour afficher ses détails. C'est là que vous confirmez que le chemin d'authentification et d'abonnement vers le HSS est opérationnel lorsque les attachements échouent.

Interfaces

La vue **Interfaces** rapporte l'état de chaque interface MME en un seul endroit : **S1AP** vers les eNodeBs, **GTP-C** (S11) vers le SGW, **Diameter** pour **S6a** (HSS) et **SLg** (services de localisation), **SGsAP** (vers le MSC pour le retour CS et SMS), **LCS-AP / SLs** (services de localisation), et **S10/N26** (transfert inter-MME et transfert EPC-5GC). C'est l'écran unique pour confirmer lesquels des chemins de signalisation du MME sont opérationnels et lesquels sont hors service.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du MME pour dépanner un seul MME sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux d'attachement, les comptes d'UE, les taux de transfert et d'autres séries chronologiques pour le MME sont présentés sous forme de tableaux de

bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liés

- Le **HSS** détient les données d'abonnement et d'authentification que le MME récupère via **S6a**.
- Le **SGW-C** est le pair de contrôle via **S11**. Le MME gère la configuration des sessions et des bearers sur celui-ci.
- Le **MSC** est atteint via **SGsAP** pour le retour CS et SMS.
- D'autres **MMEs** sont atteints via **S10** pour la mobilité inter-MME, et l'**AMF** via **N26** pour le transfert EPC-5GC.

Référence des commandes AT Quectel EP06 (test de réseau cellulaire)

Référence pour la console modem des appareils de test. Cible le **Quectel EP06** (firmware EP06ELAR04A05M4G, IMEI 868186042000040) sur le conteneur de laboratoire, mais s'applique à la famille EC25 / EG06 / EG06 / EM06. Chaque commande ci-dessous a été testée contre l'EP06 en direct ; les réponses d'exemple sont les **vraies réponses capturées de ce modem** (il était dans un état NO SERVICE / SEARCH à ce moment-là, donc les champs de signal sont vides, et les analyseurs doivent gérer cela).

Le relais est en demande/réponse : `sendModemAt(serial, command, readMs, timeoutMs)` → backend `modem_at` → agent `modem.run_at(serial, command, min_read, timeout)`. `min_read` continue de lire le port pendant au moins ce temps afin que les URCs asynchrones soient capturés avant que l'appel ne retourne. Il n'y a **pas de flux URC persistant**. Voir "Journalisation des événements" ci-dessous.

Informations sur l'appareil / SIM

Commande	But	Réponse en direct
ATI	Fabricant / modèle / firmware	Quectel / EP06 / Révision : EP06ELAR04A05M4G
AT+CGMM	Modèle	EP06
AT+CGMR	Révision du firmware	EP06ELAR04A05M4G
AT+CGSN	IMEI	868186042000040
AT+CIMI	IMSI	(IMSI SIM)
AT+QCCID	ICCID	(ICCID SIM)
AT+CPIN?	État du PIN SIM	+CPIN: READY

Signal / mesure

Commande	But	Réponse en direct
AT+CSQ	RSSI/BER (héritage)	+CSQ: 99,99 (99 = pas de signal). dBm = -113 + 2*rssi.
AT+QCSQ	Signal par RAT	+QCSQ: "NOSERVICE". Lorsqu'il est connecté : +QCSQ: "LTE", <rssi>, <rsrp>, <sinr>, <rsrq>.
AT+QNWINFO	RAT / bande / canal actuel	+QNWINFO: No Service. Lorsqu'il est connecté : +QNWINFO: "FDD LTE", "<mccmnc>", "LTE BAND 3", 1850.
AT+QENG="servingcell"	Mesures complètes de la cellule de service	+QENG: "servingcell", "SEARCH" (inactif). Voir le format ci-dessous.
AT+QENG="neighbourcell"	Cellules voisines	OK (aucune lorsque non connecté).

Format 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 (tous des entiers signés).

- SINR est une valeur **convertie** : dB réel = $(1/5) * \text{SINR} - 20$ (plage 0..250 → -20..+30 dB).
- cellID/PCI/EARFCN sont généralement hex/décimaux par champ ; band est l'indicateur de bande LTE.

Format LTE de AT+QENG="neighbourcell"

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

Enregistrement / attachement

Commande	But	Réponse en direct
AT+CFUN?	Fonctionnalité radio	+CFUN: 1 (complet). 0 = minimum/avancé
AT+CEREG?	Enregistrement EPS	+CEREG: 2,2 (2 = recherche).
AT+CEREG=2	Activer l'URC d'enregistrement avec localisation (TAC/cellID)	OK
AT+CGATT? / AT+CGATT=1 / =0	État d'attachement PS / attacher / détacher	+CGATT: 0
AT+COPS?	Sélection de l'opérateur actuel	+COPS: 0 (auto, non enregistré).
AT+COPS=?	Scan de réseau (recherche d'opérateur, lent)	liste de tuples (stat,"long","court","numérique",Ac
AT+COPS=0	Sélection automatique de l'opérateur	OK
AT+COPS=1,2,"<mccmnc>"[,	Sélection manuelle par ID	OK

Commande	But	Réponse en direct
<AcT>]	numérique	

Verrouillage de cellule / bande / RAT

Commande	But	Réponse en direct
AT+QNWLOCK=?	Capacités	+QNWLOCK: "common/4g", <num de cellules>, [[<freq>,<pci>],...] et +QNWLOCK: "common/lte" [,<action>[,<EARFCN>,<PCI>[,<status>]]]
AT+QNWLOCK="common/4g"	Interroger le verrou de cellule	+QNWLOCK: "common/4g",0 (0 cellules = pas de verrou) ; après verrou +QNWLOCK: "common/4g",1,1850,0.
AT+QNWLOCK="common/4g",<n>,<EARFCN>,<PCI>[,<EARFCN>,<PCI>...]	Verrouiller à n cellules (fonctionne sur ce firmware)	OK
AT+QNWLOCK="common/4g",0	Déverrouiller	OK (efface le verrou).
AT+QNWLOCK="common/lte"	Interroger le verrou LTE à cellule unique (lecture seule)	+QNWLOCK: "common/lte",0,0,0,0.

Comportement du firmware (vérifié en direct sur EP06ELAR04A05M4G)

: la forme `common/4g` est celle qui accepte une *action* de verrou sur cette unité. `AT+QNWLOCK="common/4g",1,<EARFCN>,<PCI>` verrouille (retourne `OK`, le verrou persiste) et `AT+QNWLOCK="common/4g",0` l'efface. Les formes `set common/lte (... ,1,<EARFCN>,<PCI>` et `... ,0)` retournent toutes `ERROR` sur ce firmware, donc `common/lte` est en lecture seule ici. L'interface utilise donc `common/4g` pour verrouiller et déverrouiller. | `AT+QCFG="band" |` Interroger le masque de bande | `+QCFG: "band",0x8d0,0x1a0880800d5,0x0` = (masque GSM, masque LTE, masque TDS). | | `AT+QCFG="band",0, <lte_hex_mask>,0 |` **Verrouillage de bande** (LTE). `0x0` masque LTE = toutes les bandes. | `OK | | AT+QCFG="nwscanmode" |` Mode de scan RAT | `+QCFG: "nwscanmode",0` (0 = auto, 1 = GSM, 2 = WCDMA, 3 = LTE). | | `AT+QCFG="nwscanmode",<m>[,1] |` Définir la préférence RAT (`1` = effective immédiatement) | `OK | | AT+QCAINFO |` Informations sur l'agrégation de porteuse | `OK` (aucune agrégée lorsque inactif). |

Masque de bande LTE : bit `(band-1)`, c'est-à-dire bande $N \rightarrow 1 \ll (N-1)$. par exemple `B3 = 0x4`, `B7 = 0x40`, `B28 = 0x8000000`. `0x0` (ou tous les uns) = toutes les bandes activées.

Remarque sur le firmware : `AT+QCFG="nwscanseq"` retourne `ERROR` sur ce firmware EP06 (EP06ELAR04A05M4G). L'interface ne le surface **pas**.

`AT+QSCAN` n'est également pas pris en charge sur ce firmware EP06 (c'est une commande de la série RG/RM 5G). Le scan de réseau utilise `AT+COPS=?` plus `AT+QENG` à la place.

Appels vocaux (VoLTE / IMS)

La voix EP06 est **uniquement VoLTE** : elle nécessite IMS enregistré sur LTE.

`AT+QCFG="ims"` sur cette unité retourne `+QCFG: "ims",1,0` (IMS activé par configuration, statut actuel 0).

Commande	But
AT+QCFG="ims"	Interroger/activer IMS. AT+QCFG="ims",1 pour forcer l'activation.
ATD<number>;	Composer un appel vocal (point-virgule final ; = voix, pas de données).
ATA	Répondre à un appel entrant.
ATH / AT+CHUP	Raccrocher.
AT+CLCC	Lister les appels en cours : +CLCC: <id>,<dir>,<state>,<mode>,<mpty>,"<number>",<type>. Vide OK = pas d'appels.
AT+CLIP=1	Activer l'URC d'identification de l'appelant (+CLIP:) sur RING.

États d'appel AT+CLCC : 0 actif, 1 en attente, 2 composition, 3 alerte, 4 entrant, 5 en attente.

SMS (mode texte)

Commande	But	Réponse en direct
AT+CMGF=1	Mode texte (vs PDU)	OK
AT+CPMS?	Zones de stockage / comptes	+CPMS: "ME",0,255,"ME",0,255,"ME",0,255
AT+CMGL="ALL"	Lister les messages (mode texte)	par message : +CMGL: <index>," <stat>","<sender>"," <timestamp>" puis ligne de corps.
AT+CMGR=<index>	Lire un message	+CMGR: "<stat>","<sender>"," <timestamp>" + corps.
AT+CMGS=" <number>" puis corps + Ctrl-Z	Envoyer (géré par l'agent send_sms).	+CMGS: <mr>
AT+CMGD=<index>[, <delflag>]	Supprimer le message (delflag 4 = tous).	OK
AT+CNMI? / AT+CNMI=2,1,0,0,0	Configuration de l'indication de nouveau message	+CNMI: 2,1,0,0,0

PDP / données

Commande	But	Réponse en direct
AT+CGDCONT?	Lister les contextes PDP (APNs)	+CGDCONT: 1,"IPV4V6","ims",...
AT+CGDCONT=<cid>,"<type>","<apn>"	Définir le contexte. types : IP, IPV6, IPV4V6, Non-IP.	OK
AT+CGACT=1,<cid> / =0,<cid>	Activer / désactiver le contexte.	OK
AT+CGPADDR[=<cid>]	Afficher l'IP assignée.	+CGPADDR: 1,"<ip>"
AT+CGCONTRDP=<cid>	DNS / passerelle / PCO.	+CGCONTRDP: ...
AT+QPING=1,"<host>"	Ping depuis le modem (les réponses URC ; nécessite min_read).	+QPING: ...

Journalisation des événements (URCs) : et la limitation du relais

Le relais de l'agent est **demande/réponse avec un port ouvert par appel**. Il ouvre le port série, envoie une commande, lit jusqu'à OK/ERROR (ou min_read s'écoule), puis ferme. Il ne **maintient pas** le port ouvert pour diffuser des codes de résultats non sollicités (URCs) vers le navigateur. Donc, un véritable flux d'événements en direct n'est pas possible par ce chemin sans modifications de l'agent.

URCs dignes d'être activés (chacun est une commande OK à usage unique) :

Commande	Active URC
AT+CEREG=2	+CEREG: changements d'enregistrement (avec TAC/cellID).
AT+CGEREP=2,1	+CGEV: événements PS/porteuse.
AT+CLIP=1	+CLIP: identification de l'appelant sur RING.
AT+CNMI=2,1,0,0,0	+CMTI: indication de nouveau SMS.
AT+QINDCFG="all",1	+QIND: indications Quectel.

Approche pragmatique utilisée dans l'interface : l'onglet Événements active les URCs ci-dessus, puis **interroge** le modem à intervalles réguliers (AT+CEREG?, AT+CLCC, AT+QENG, AT+CSQ, AT+CMGL) et rend les changements d'état dans un journal horodaté. Chaque interrogation utilise également une courte fenêtre `min_read` afin que tout URC qui arrive pendant la lecture soit capturé de manière opportuniste. Cela capture les transitions d'état (enregistrement gagné/perdu, appel commencé/terminé, nouveau SMS, changement de signal) à la cadence d'interrogation, ce qui est suffisant pour les tests en laboratoire. La limitation est documentée dans l'interface.

MSC : Centre de Commutation Mobile

Le **MSC** est le cœur de contrôle des appels du noyau à commutation de circuits. Il contient le registre de localisation des visiteurs (VLR) pour les abonnés actuellement dans sa zone de service, établit et termine les **appels vocaux**, transporte les **SMS** et gère la **mobilité** (mises à jour de localisation, pagination et transferts) pour ces abonnés. Il atteint le côté radio via des connexions **RAN/BSC** (interface A, pilotée par M3UA/SS7), relie la voix à l'IMS et interconnecte via des **pairs SIP**, et dirige les médias réels à travers une ou plusieurs **passerelles multimédias**. OmniWeb affiche les abonnés en direct du MSC, les appels, les transactions SMS, les RAN et les pairs SIP, la table de routage et les pages en attente. Les tendances à long terme sont sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le MSC est une page d'élément par instance accessible depuis la barre latérale lorsque l'on navigue dans l'inventaire du site, et, là où plusieurs sont déployés, une vue de flotte pour un état agrégé. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du MSC, il reste donc derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : l'**état de l'API** du MSC et un résumé de ce qu'il gère actuellement, y compris les **abonnés** enregistrés dans le VLR, les **appels actifs**, les transactions **SMS** en cours, les **connexions RAN** en direct et l'état des **pairs SIP** et des liens de signalisation **STP**. C'est le moyen le plus rapide de confirmer que le MSC est opérationnel et de voir, d'un coup d'œil, sa charge en direct.

Abonnés

Chaque abonné que le VLR détient actuellement, chaque ligne étant identifiée par **IMSI** et **MSISDN** avec son état d'enregistrement et de localisation. Ouvrez un abonné pour afficher son contexte VLR complet. De là, un opérateur peut :

- **Purger** un abonné du VLR pour effacer un enregistrement obsolète ou bloqué afin que l'abonné se réenregistre proprement.
- Exécuter une **action sur l'abonné** contre un abonné spécifique.
- Gérer les **services complémentaires** : inspecter et modifier le renvoi d'appel, le blocage et les services connexes actifs pour l'abonné.
- Envoyer un **Avis de Charge (AoC)** à l'abonné.
- Envoyer un **SMS silencieux (Type 0)** ou initier un **appel silencieux** : une sonde de localisation/joignabilité qui n'alerte pas le terminal.

Appels

Chaque appel actif, chaque ligne montrant les parties **appelantes** et **appelées**, l'**état** de l'appel et sa **durée**. Ouvrez un appel pour afficher ses détails complets : les jambes, la connexion RAN en service et le chemin multimédia. Un opérateur peut **forcer la libération** d'un appel pour effacer un appel bloqué ou indésirable.

SMS

Les transactions SMS que le MSC gère actuellement, chacune montrant l'**expéditeur**, le **destinataire** et l'**état de livraison**, afin que vous puissiez confirmer que les messages sont transportés et repérer ceux qui sont bloqués.

RAN

Le côté radio du MSC. Il liste les **connexions RAN** actives (les associations A-interface en direct transportant le signalement des abonnés) et les **BSC** connus, appris lors des échanges RESET sur les liens SS7/M3UA. C'est ici que vous confirmez que les contrôleurs de station de base sont connectés et voyez quels abonnés sont sur quelle connexion.

Pairs SIP

Les pairs SIP par lesquels le MSC relie la voix sont les IMS, les commutateurs logiciels et les trunks d'interconnexion, chaque ligne montrant l'**adresse** du pair et son **état** de joignabilité. Ouvrez un pair pour afficher ses détails. Un opérateur peut **déclencher un ping OPTIONS** sur un pair pour tester activement la joignabilité, ce qui est le moyen le plus rapide de prouver qu'un chemin SIP est opérationnel lorsque les appels vers celui-ci échouent.

Passerelles multimédias

Les passerelles multimédias par lesquelles le MSC dirige les porteurs de voix, chaque ligne montrant la passerelle et son **état**, afin que vous puissiez confirmer que le plan média est disponible pour l'établissement des appels.

Routage

La table de routage par numéro du MSC contient les règles qui décident, par préfixe de numéro composé, où un appel est envoyé. Chaque règle montre son **préfixe** et sa **destination**. Un opérateur peut :

- **Ajouter une route** : un nouveau préfixe et sa destination.
- **Supprimer une route** par préfixe.
- **Tester une recherche de route** pour un numéro : entrez un numéro et voyez quelle route il résout, pour confirmer les plans de numérotation avant ou après un changement.

Pagination

Les demandes de pagination en attente sont les abonnés que le MSC essaie actuellement de localiser sur le réseau radio pour un appel entrant ou un SMS. Un opérateur peut également **pager un abonné** directement depuis ici.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du MSC pour dépanner un seul commutateur sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux d'appels, les volumes de SMS, les comptes d'abonnés et d'autres séries temporelles pour le MSC sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens connexes

- Le **HSS** contient les données des abonnés que le VLR résout et où le MSC s'enregistre en tant que nœud de service.
- Le **CSCF / IMS** est relié via les **pairs SIP** du MSC pour la voix.
- Les **BSC** se connectent sur le côté radio via l'interface A, transportée sur les liens de signalisation SS7/M3UA.

Test de Réseau (Test de Charge)

Test de Réseau génère une charge de signalisation synthétique sur un cœur en direct afin que vous puissiez mesurer son comportement sous stress. Ce n'est pas un seul générateur mais une *flotte* de ceux-ci : les générateurs de charge autonomes s'enregistrent auprès d'OmniWeb et apparaissent ici. Vous les contrôlez depuis une seule console : définissez un taux, augmentez progressivement, mettez en pause, videz, arrêtez. Vous pouvez les contrôler par générateur ou sur l'ensemble du pool à la fois.

[← Guide des Opérations](#)

Le Test de Réseau couvre trois types de charge, chacun sur son propre sous-onglet sous **Test de Réseau** dans la barre latérale :

Sous-onglet	Générateur	Stress	Mesuré en tant que
Test de Charge Diameter	Seagull	Le DRA + HSS (signalisation Diameter)	Requêtes par seconde (rps)
Test de Charge SIP	SIPp	Les CSCFs + HSS : enregistrements IMS, avec IPsec	Nouveaux enregistrements/sec, UEs tenus (enregistrés)
Test de Charge RAN / Simulateur RAN	Simulateur RAN	Le chemin radio→cœur complet (S1AP/NAS, GTP-U, IMS)	Voir Simulateur RAN

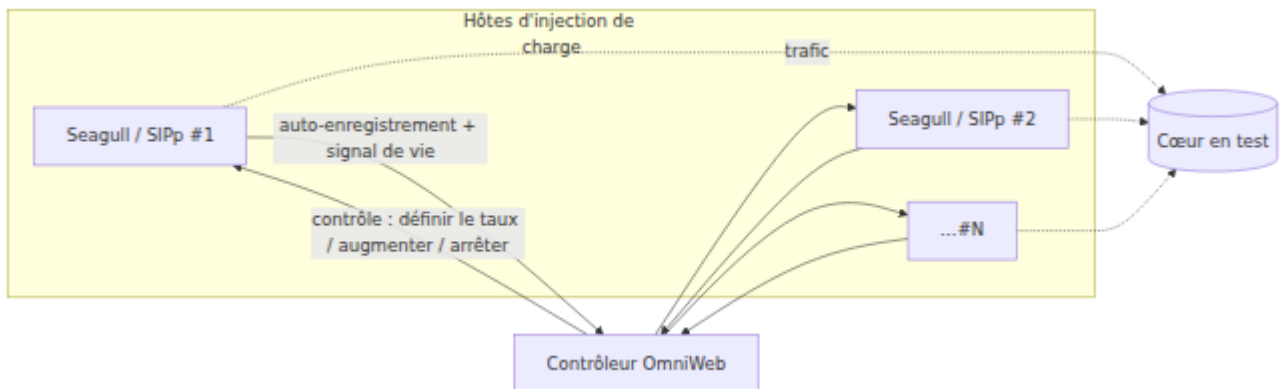
Les onglets Diameter et SIP sont la console de générateur auto-enregistrée décrite sur cette page. Les onglets **RAN** sont le [Simulateur RAN](#), eNodeBs et

UEs virtuels, documentés séparément.

Comment les générateurs apparaissent

Vous ne lancez pas les générateurs depuis OmniWeb. Chaque générateur de charge (Seagull pour Diameter, SIPp pour SIP) est démarré sur un hôte d'injection de charge et pointé vers OmniWeb ; à partir de ce moment, il **s'auto-enregistre**, envoyant un signal de vie au contrôleur toutes les quelques secondes avec "J'existe, voici mon adresse de contrôle, et voici mes compteurs en direct." Dans quelques secondes, il apparaît dans le sous-onglet correspondant.

Si un onglet est vide, il vous indique exactement comment en démarrer un. Copiez le drapeau qu'il affiche (il dérive l'URL de l'adresse que vous parcourez, donc il est toujours correct pour ce déploiement) et démarrez le générateur avec.



Le registre est uniquement une télémétrie en direct. Il n'est pas persistant. Un générateur qui cesse d'envoyer des signaux de vie après son TTL est affiché **hors ligne** (et, étant hors ligne, ne fonctionne pas). Il réapparaît dès qu'il envoie à nouveau un signal de vie.

Lecture d'un générateur

Chaque générateur est une ligne dans la liste de gauche (point vert = en ligne, RUN/IDLE/OFF). Sélectionnez-en un pour voir ses détails :

- Une **ligne de statut** : en cours d'exécution (avec le scénario actif) ou arrêté/hors ligne, l'état de lien Diameter (en ligne, et le pair) pour Seagull, ou le nombre de SAs IPsec actifs pour SIPp.
- **Métriques en direct**, adaptées à l'outil :
 - *Diameter* : taux offert, réussi, échoué (délai d'attente), temps de réponse moyen, appels ouverts actuels.
 - *SIP* : taux offert, **tenu** (UEs actuellement enregistrés), enregistrés OK (200s), SAs IPsec, créés/tentés, pic concurrent, échoué, échec IPsec.
- **Jauges CPU des pairs** : lorsque le site sélectionné a un rôle de Surveillance (Prometheus), OmniWeb lit la CPU par nœud directement depuis Prometheus et affiche une jauge par DRA/HSS/CSCF que le trafic atteint, plus (Diameter) les taux de requêtes/réponses DRA et le délai de réponse DRA→pair. Cela vous permet de surveiller l'effet de la charge sur le cœur, pas seulement les chiffres du générateur lui-même.
- **Messages de scénario** (SIPp) : un tableau par étape du flux REGISTER : combien de chaque message ont été envoyés/reçus, et tout délai d'attente, messages inattendus ou retransmissions, afin que vous puissiez voir exactement où un flux échoue sous charge.

MAXED

Un processus SIPp qui atteint sa pleine capacité "Max UEs" ne peut ouvrir aucun nouvel appel, donc il cesse d'envoyer du trafic même si vous avez demandé plus. OmniWeb le signale comme **MAXED** (sur la ligne, l'en-tête de détail, et la métrique Tenue). Pour le corriger, augmentez la limite Max UEs. Voir ci-dessous.

Générer du trafic

Pour le générateur sélectionné (**Contrôle du Trafic** carte) :

- **Scénario** : changez le scénario en cours d'exécution en direct (Seagull), ou voyez le scénario fixé au lancement (SIPp).
- **Taux** : définissez le taux offert avec un curseur, des pré-réglages, ou une zone de saisie (rps pour Diameter, nouveaux enregistrements/sec pour SIP). 0 = inactif/tenu.

- **Augmenter** (Seagull) : au lieu d'un changement brusque, grimpez au taux cible sur N secondes.
- **Max UEs** (SIPp) : le plafond sur les UEs tenus (enregistrés) simultanés, appliqué **en direct sans redémarrage**. Augmentez-le pour pousser un processus MAXED plus fort.
- **Pause / Reprendre / Vider** (SIPp) : maintenir et libérer le trafic, ou vider (laisser les appels tenus se terminer sans en ouvrir de nouveaux).
- **Injecter un appel** (SIPp) : déclencher un seul appel, pour des vérifications ponctuelles.
- **Réinitialiser les statistiques** : effacer les compteurs cumulés et le tableau par message.
- **Arrêter le trafic** : arrêter le générateur d'envoyer de la charge.

Les commandes sont envoyées d'OmniWeb au point de contrôle du générateur (un socket UDP pour SIPp, un port de contrôle pour Seagull) ; les boutons qui apparaissent dépendent de ce que l'outil prend en charge.

Contrôler l'ensemble du pool à la fois

Lorsque plus d'un générateur est enregistré, une carte **Contrôle du Pool** apparaît au-dessus de la liste. Elle répartit les mêmes actions sur chaque générateur en ligne en parallèle, vous permettant de contrôler "tous les 30" depuis un seul endroit :

- **Portée** : tous les générateurs, ou un groupe d'hôtes (générateurs supervisés sur le même hôte, par exemple `sipp-bsc01-01/-02/-03`, se regroupent en un seul groupe).
- **Totaux de la flotte** : taux offert, tenus/réussis, créés, SAs IPsec, pic, échoués, et taux d'échec **sommés sur la portée**, afin que vous puissiez voir la charge agrégée que le pool offre, pas des chiffres par processus.
- **Définir un taux constant** : appliquer un taux par processus à chaque générateur (la carte montre le total du pool résultant : N instances × taux).
- **Max UEs** (SIPp) : définir le plafond des tenus sur chaque processus à la fois. La carte indique combien sont actuellement MAXED.

- **Augmenter progressivement** : faire grimper chaque instance de 0 à un objectif sur une durée en étapes. L'augmentation s'exécute **dans votre navigateur**, donc quitter la page l'arrête.
- **Cycle de vie en masse** : Pause / Reprendre / Vider / Arrêter tous, et Réinitialiser les statistiques.

Utilisation typique

1. Démarrez un ou plusieurs générateurs Seagull (Diameter) ou SIPp (SIP) sur vos hôtes de charge, pointés vers OmniWeb ; confirmez qu'ils apparaissent en ligne.
2. Choisissez un taux constant modeste sur un générateur et confirmez que le cœur répond (surveillez Réussi / Enregistré OK et les jauges CPU des pairs).
3. Augmentez progressivement le pool vers l'objectif et surveillez les totaux de la flotte, le taux d'échec, et les jauges de délai de réponse/jauge CPU des pairs pour le point où le cœur commence à se dégrader.
4. Pour les tests de saturation SIP, définissez un plafond Max UEs et laissez la flotte maintenir une grande population enregistrée ; augmentez le plafond si des processus deviennent MAXED.
5. Videz/Arrêtez lorsque vous avez terminé.

Liens Connexes

- **Simulateur RAN** : les sous-onglets RAN : eNodeBs/UEs virtuels pour des tests fonctionnels et de charge sur l'ensemble du chemin radio→cœur.
- **Tableaux de Bord & Statistiques Grafana** : les jauges CPU des pairs ici lisent le même Prometheus que les tableaux de bord. Utilisez Grafana pour avoir une vue d'ensemble pendant un test.

OmniRoam : Accords de Roaming & Automatisation des Emails

Le côté **accords** d'OmniRoam transforme la paperasse nécessaire à la mise en place d'un partenaire de roaming (les emails, les formulaires AA.12/AA.13, les tarifs IOT, les échanges de SIM, et le travail de provisionnement) en un seul enregistrement suivi par partenaire. Il automatise les parties qui étaient auparavant du copier-coller. Son astuce principale : **transmettez un email de partenaire à OmniRoam et il lit le fil de discussion, extrait les faits, et met à jour l'accord pour vous**. Il génère ensuite et signe électroniquement les contrats, les archive, et élève les ordres de travail pour lancer le partenaire.

[← Retour au Guide des Opérations](#)

Deux "OmniRoam" différents. Ce document concerne le côté **accords / email / documents** d'OmniRoam (le cycle de vie commercial et de provisionnement avec un partenaire de roaming). Ce n'est **pas** la même chose que les **carnets de test de roaming** (IR.38 / IR.48 / tests de conformité VoLTE). Ceux-ci sont couverts séparément dans [OmniRoam : Automatisation des Tests de Roaming](#). Un produit, deux tâches : *faire signer l'accord* (ici) et *prouver que le roaming fonctionne* (là).

Table des Matières

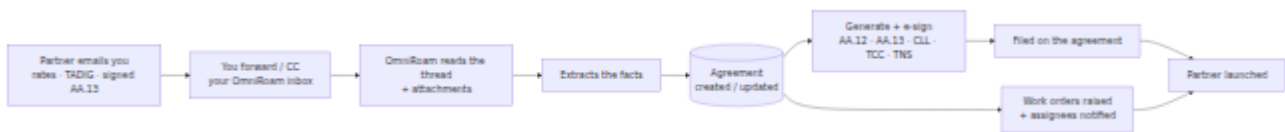
- [La Grande Image](#)
- [1. Ingestion des Emails Entrants : "extraction des données"](#)
- [2. Accords & Partenaires](#)
- [3. Génération Automatique de Documents & Signature](#)
- [4. Archivage & Stockage](#)

- 5. Ordres de Travail & Notifications des Assignés
 - Le Cycle de Vie Complet, de A à Z
 - Ce que Vous Configurez Une Foix
-

La Grande Image

Tout dans OmniRoam repose sur un enregistrement : l'**Accord**, un par partenaire de roaming. Un accord porte le nom du partenaire, le pays, les TADIG(s)/PLMN, son **statut** de cycle de vie, ses contacts, les **tarifs** commerciaux convenus, les SIM échangées, les **documents** générés et reçus, une **chronologie** d'activités, et les **ordres de travail** qui rendent le partenaire opérationnel.

Vous pouvez construire tout cela manuellement dans l'interface utilisateur. Mais l'objectif d'OmniRoam est que la plupart des informations arrivent *par email*, et OmniRoam les archive pour vous.



Le locataire dans lequel vous travaillez est un **Opérateur** (votre propre réseau, le côté "domestique"). Tout est lié à cela : votre en-tête et signataire remplissent les documents générés, votre adresse d'entrée pilote l'automatisation des emails, et vos équipes sont les assignés des ordres de travail.

1. Ingestion des Emails Entrants : "extraction des données"

Ce que vous faites

Négocier avec un partenaire est une conversation par email. Pour l'intégrer dans OmniRoam, vous faites une seule chose : **transmettez l'email, ou CC**

l'adresse d'entrée d'OmniRoam sur le fil. C'est tout. Votre adresse d'entrée dédiée (par exemple `roaming@yourdomain`) est configurée une fois par opérateur (Paramètres → détails de la paperasse, `Email entrant`).

- **Transmettez un fil entier** une fois et OmniRoam construit l'accord à partir de l'historique enfoui dans les messages cités.
- **CC l'adresse sur une négociation en cours** et chaque nouvel email maintient l'enregistrement à jour. Le statut avance, les contacts et TADIGs se remplissent, les tarifs arrivent, et la paperasse jointe est archivée, email par email.

Vous ne remplissez jamais de formulaire pour faire cela. L'email est l'entrée.

Ce que fait OmniRoam

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

Réessayer

Étape par étape, une fois qu'un email atteint OmniRoam :

1. **Il détermine pour quel opérateur (locataire) l'email est destiné** en faisant correspondre une adresse To/Cc à l'adresse d'entrée configurée d'un opérateur. Si rien ne correspond, l'email est enregistré comme `no-operator` et *rien n'est changé* : une opération sans risque.
2. **Il lit les pièces jointes, pas seulement le corps.** Les tarifs convenus ou les termes signés se trouvent souvent dans un **AA.13** joint, une **fiche tarifaire IOT**, ou un tableur. OmniRoam extrait donc le texte des pièces jointes PDF, Word, Excel et CSV et alimente également l'extracteur. Les logos de blocs de signature (PNG/JPG) sont ignorés.
3. **Il extrait les faits** en utilisant l'API ChatGPT. L'extracteur est spécifiquement informé que l'expéditeur extérieur est généralement en train de *transmettre* le fil (souvent votre propre responsable roaming) et de lire **l'ensemble de l'historique cité**. Il attribue les tarifs, contacts, adresses et SIMs à ceux qui les ont réellement déclarés, jamais à l'expéditeur. Il retourne un enregistrement structuré : nom du partenaire, pays, adresse, TADIG(s)/PLMN, statut de cycle de vie le plus approprié,

tarifs convenus (uniquement si *les deux* parties ont explicitement convenu), contacts du partenaire, SIMs échangées/demandées, si un accord signé est joint, et un résumé en une ligne.

4. **Il trouve le bon accord, ou en crée un.** La correspondance est délibérément tolérante afin qu'un fil ne génère jamais un duplicata : nom exact du partenaire, puis une correspondance de "nom normalisé" (ainsi *AT&T Mobility* rejoint *AT&T*), puis une correspondance de **PLMN partagé** (MCC+MNC). C'est un signal de très haute précision, car un PLMN identifie de manière unique un réseau. Pas de correspondance → un tout nouvel accord.
5. **Il fusionne uniquement ce qui est nouveau.** Pour les accords nouveaux et existants, OmniRoam applique ce que *cet* email révèle de nouveau et **ne remplace jamais** les valeurs existantes :
 - **Statut** ne progresse que *vers l'avant* dans le cycle de vie (jamais en arrière).
 - **Pays / adresse** définis s'ils sont vides ou changés.
 - **TADIGs** ajoutés, mais uniquement des codes qui existent dans le catalogue IR.21 (ainsi l'IA ne peut pas en inventer un), et jamais les codes de votre propre réseau domestique.
 - **Contacts** ajoutés, ou existants *enrichis* (champs vides remplis).
 - **SIMs** enregistrées (SIMs de test partagées par le partenaire) et **demandes de SIM** (lots que quelqu'un a demandé à être expédiés à une adresse).
 - Les **tarifs convenus** deviennent un niveau tarifaire, uniquement lorsque les deux parties ont explicitement convenu, et jamais un duplicata d'un niveau existant.
 - Un **AA.12/AA.13 signé** (joint, ou déclaré dans l'email) fait avancer le statut à *IRA Signé*.
6. **Il écrit deux enregistrements.** Une **entrée de journal d'activité** amicale sur la chronologie de l'accord ("Email de *Jane chez Partner* (transmis) : tarif de données convenu ; statut → *rates_agreed*, contact Jane ajouté, tarifs convenus enregistrés"), et une **ligne d'audit entrant** brute (voir ci-dessous).

Le traitement est **idempotent** : le même email (par Message-ID) n'est traité qu'une seule fois, donc CC plusieurs personnes ou retransmettre un fil ne compte jamais double.

Trois façons dont l'email arrive

Vous n'avez besoin que d'une seule. Les trois finissent par appeler la même logique de traitement :

Chemin	Comment cela fonctionne	Quand l'utiliser
Cloudflare Email Worker	Cloudflare Email Routing transmet le message brut à un petit Worker qui envoie le <code>.eml</code> directement au webhook d'OmniRoam.	Domaines utilisant déjà Cloudflare ; pas de boîte aux lettres à interroger.
Poller IMAP	OmniRoam se connecte à une vraie boîte aux lettres toutes les ~60 s, traite les messages non lus, et les marque comme lus.	Toute boîte aux lettres standard (TLS implicite, STARTTLS, ou simple).
Provider inbound-parse	Un fournisseur de messagerie (Mailjet/SendGrid) envoie le message analysé + pièces jointes au webhook.	Si vous exécutez déjà l'analyse entrante.

Le webhook (`/api/roaming/inbound-email`) est protégé par un **secret partagé**, donc seul votre chemin de messagerie configuré peut y poster.

Le Journal des Emails Entrants : votre trace d'audit

Chaque email traité, succès *ou* échec, écrit une ligne dans le **Journal des Emails Entrants** (dans l'interface utilisateur sous la vue Emails de l'opérateur). Chaque ligne montre l'expéditeur, les destinataires, l'objet, les pièces jointes, si l'**extraction AI a réussi**, exactement ce qu'elle a extrait, et ce que l'email **a changé** (ou pourquoi il n'a rien fait : `no-operator`, `no-partner`). C'est votre fenêtre sur l'automatisation : si un tarif n'a pas été récupéré, le journal vous dit ce que l'extracteur a réellement vu.

Le Journal des Emails Entrants : une ligne par email traité, avec le résultat de l'extraction et les changements qu'il a effectués. C'est la trace d'audit pour toute l'automatisation email→accord.

2. Accords & Partenaires

La liste des **Accords** est votre registre de partenaires de roaming pour l'opérateur actuel. Chaque ligne est un partenaire, avec son **statut** de cycle de vie, TADIG/pays, priorité, et sur qui la prochaine action attend ("Nous" ou "Eux").

La liste des Accords. Les statuts s'étendent de gauche à droite le long du cycle de vie ; la barre de filtre se resserre par statut. Vous créez des accords ici manuellement, ou ils arrivent automatiquement d'un email entrant.

Le cycle de vie (statut)

Un accord progresse à travers ces étapes. L'automatisation des emails ne fait avancer que le statut, donc l'enregistrement reflète le point le plus éloigné que la conversation a atteint :

Demandé → Négociation IOT → IOT En Attente de Signature → IRA
Négociation → En Attente de Signatures IRA → IRA Signé → Tarifs
Convenus → Échange de SIM → Test → Lancé (plus Lancement par Défaut,
Suspendu, Terminé).

Ouverture d'un partenaire

Cliquez sur un partenaire pour ouvrir sa page de **détails** : un ensemble d'onglets/sections couvrant tout sur la relation :

- **Aperçu & chronologie** : statut, priorité, notes, et le journal d'activité (chaque email, document généré, signature, et note manuelle dans l'ordre des dates).
- **TADIGs** : les codes réseau du partenaire (avec MCC/MNC, type de connexion et direction). Une action "**trouver des candidats**" peut extraire les autres TADIGs de l'opérateur partenaire du catalogue IR.21 pour que vous les examiniez et les ajoutiez.
- **Contacts** : personnes commerciales/techniques/roaming chez le partenaire.
- **Tarifs** : les niveaux tarifaires commerciaux convenus (données/SMS/voix, devise, unité).
- **SIMs & demandes de SIM** : SIMs de test échangées, et lots demandés pour expédition.
- **Documents** : paperasse générée et reçue (voir ci-dessous).
- **Routage** : routes DRA, titres globaux SS7, plages DNS et IP pour le provisionnement (une grande partie pré-remplie à partir de l'IR.21 du partenaire).

Tout sur la page de détails est **modifiable**. L'automatisation vous donne un coup de pouce, et vous corrigez ou ajoutez manuellement si nécessaire.

Le catalogue IR.21

Les recherches TADIG s'appuient sur un **catalogue mondial d'opérateurs IR.21** indexé par TADIG (organisation, réseau, MCC/MNC, DNS, plages IP, nœuds SS7, contacts). C'est ainsi qu'OmniRoam valide un TADIG extrait par l'IA, découvre les TADIGs frères d'un partenaire, et pré-remplit les données de routage.

3. Génération Automatique de Documents & Signature

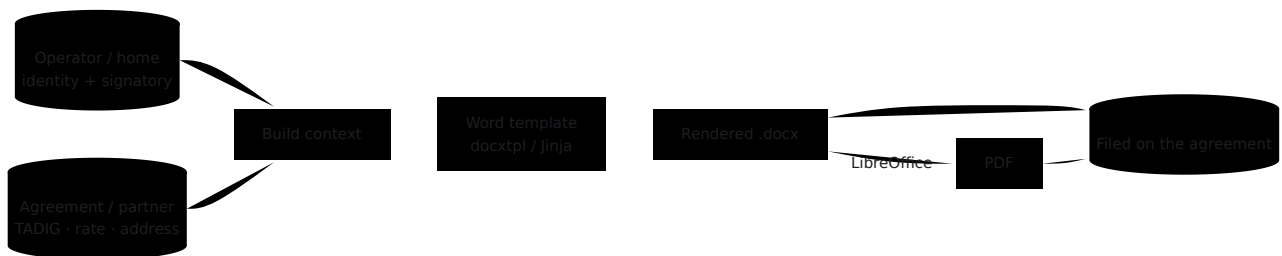
Génération d'un document

Dans la section **Documents** d'un accord, vous choisissez un type de document et cliquez sur **Générer**. OmniRoam rend le véritable formulaire Word, rempli avec les détails des deux parties, prêt à être signé :

Type	Ce que c'est	Format
AA.12	Accord de roaming GSMA AA.12 IREG (le véritable formulaire, pré-rempli des deux côtés)	.docx / PDF
AA.13	Annexes communes GSMA AA.13, y compris l'annexe de facturation/règlement (voir options de règlement AA.13)	.docx / PDF
CLL	Lettre de Lancement Commercial (générique)	.docx / PDF
CLL (Bilatéral / Unilatéral, après test)	Lettre de lancement confirmant la date de début après des tests IREG & TADIG réussis	.docx / PDF
CLL (Bilatéral / Unilatéral, par défaut)	Lettre de lancement pour un lancement par défaut, sans compléter les tests IREG/TADIG	.docx / PDF
TCC (VoLTE)	Achèvement de l'Appel de Test VoLTE	.docx / PDF
Achèvement TADIG	Formulaire d'achèvement TADIG	.docx / PDF
Formulaire d'Accord de Roaming TNS	Demande de clearing TNS (livrée sous forme de .doc héritée)	.doc
Demande TNS 3G-4G	Demande de clearing TNS	.docx

Comment les champs sont remplis. Chaque document est un modèle Word avec des espaces réservés (docxtpl / Jinja). OmniRoam les remplit à partir de :

- **Le côté domestique** : de votre enregistrement **Opérateur** : votre nom, nom légal, TADIG, PLMN, pays, **signataire & titre**, lieu, et adresse. Comme cela provient du locataire, chaque opérateur hébergé obtient automatiquement son *propre* en-tête et signataire.
- **Le côté partenaire** : de l'**Accord** : nom du partenaire, son abréviation courte utilisée dans le corps du contrat, TADIG(s), PLMN(s), pays et adresse. Le signataire/titre du partenaire reste par défaut vide, de sorte que cette ligne est laissée prête pour qu'ils signent.
- **Valeurs dérivées** : date d'entrée en vigueur, direction (bilatérale/entrant/ sortant), entreprise hub, domaines Diameter, devise, et le tarif IOT confirmé.



Format de sortie : Word par défaut, PDF pour la signature

La génération produit un **Word .docx** modifiable par défaut. C'est la copie de travail que vous examinez et modifiez manuellement si nécessaire. Vous obtenez un PDF uniquement lorsque vous avez réellement besoin d'un rendu fixe et final :

- Cochez la case **Sortie PDF** avant de cliquer sur Générer pour rendre un PDF au lieu du **.docx**.
- Le flux de **signature électronique** utilise toujours un PDF (l'artefact signé ne doit pas changer).
- **Téléchargez / prévisualisez** un document archivé *au format PDF* à la demande.

Un email de **Pack de Roaming** joint l'AA.12/AA.13 en tant que **.docx** modifiable afin que le partenaire puisse l'examiner et commenter. Ce n'est pas l'étape de signature, donc il n'est pas envoyé en PDF.

Options de règlement AA.13 (Annexe C.3.2)

L'annexe C.3.2 de GSMA AA.13 (facturation & règlement) est un **menu de choix** que chaque partenaire négocie : quel modèle de facture, quelle méthode de paiement, le seuil et la période de règlement, les conditions de paiement, et les intérêts. Plutôt que de verrouiller un ensemble de choix dans le modèle, OmniRoam les expose comme un panneau d'options de règlement dans la section **Documents** : développez **options de règlement AA.13**, définissez les valeurs pour ce partenaire, puis cliquez sur **Générer AA.13**. L'annexe générée contient uniquement les options que vous avez choisies. Les alternatives (et l'échafaudage GSMA "supprimez celles qui ne s'appliquent pas") sont supprimées automatiquement.

Chaque champ a un défaut sensé, donc générer sans toucher au panneau donne les termes standards ; changez uniquement ce qui diffère pour un partenaire donné.

Option	Défaut	Description
Type de facture	Facture à réseau unique (SNI)	Sélectionne l'annexe de règlement : Réseau unique (SNI) → Annexe C.3.2 H, ou Réseau multiple (MNI) → Annexe C.3.2 I. L'annexe inutilisée est supprimée.
Méthode de paiement	Règlement net	Le mécanisme de règlement : Règlement net, Paiement direct intégral (sans conversion), Paiement direct intégral (avec conversion), ou Netting sans conversion . Seule la clause de la méthode choisie est conservée.
Règlement par seuil	Option 1 (Netting)	Option 1 (Netting) applique un seuil de faible solde convenu ; Option 2 (Paiement direct) utilise des seuils par partie (Partie A / Partie B).
Seuil	50	Montant du seuil de règlement de faible solde, dans la devise de règlement de l'accord (par exemple, DTS). En dessous de ce montant agrégé mensuel, le règlement peut être différé.
Début de période / Fin de période	Janvier / Décembre	La période non de règlement pour les soldes inférieurs au seuil, généralement l'année financière.
Jours de paiement	60	Jours à partir de la date de facturation dans lesquels le débiteur doit payer.
Intérêt maison %	8	Intérêt annuel que le créancier peut facturer sur les soldes en retard lorsque l'opérateur domestique est le créancier.

Option	Défaut	Description
Intérêt partenaire %	8	Intérêt annuel lorsque l'opérateur partenaire est le créancier.
Envoyer des factures à valeur nulle	Désactivé	Lorsqu'il est désactivé, l'annexe indique que chaque partie n'enverra pas de factures mensuelles avec un montant nul (0,00).
BCE sur facture TAP	Désactivé	Lorsqu'il est désactivé, l'annexe indique que l'utilisation de BCE ne sera pas incluse sur la facture de Roaming TAP.

Comment cela fonctionne. Les choix sont transmis à la génération comme des remplacements par rapport aux défauts intégrés. Le modèle AA.13 les résout dans l'annexe finie : il sélectionne les bons blocs d'options, remplit les montants/périodes/taux, et formule les bascules. La devise de règlement elle-même provient de la devise configurée de l'accord, pas de ce panneau.

Cas d'utilisation. Un partenaire insiste sur des conditions de 90 jours, un seuil de 100 DTS et une année financière d'avril à mars : ouvrez le panneau, définissez **Jours de paiement 90**, **Seuil 100**, **Début de période** avril, **Fin de période** mars, et générez. Chaque autre clause reste aux termes standards.

Les formulaires de clearing TNS sont spéciaux. Les deux demandes TNS ne sont *pas* des modèles docxtpl. Ce sont les véritables formulaires TNS de l'opérateur avec uniquement les champs remplissables modifiés et les bonnes cases cochées, afin que TNS reçoive exactement la mise en page qu'il attend. Ils sont **gated IOT** : OmniRoam ne les génère pas tant que l'accord n'a pas un **tarif confirmé (convenu)**. Essayer plus tôt renvoie un message clair "un IOT confirmé est requis". Les états des cases à cocher (type d'accord, direction, services, interfaces LTE, GRX) sont dérivés automatiquement de l'accord, et tous les champs sont modifiables au moment de la génération.

LibreOffice sans tête sur le serveur effectue la génération de PDF (et le `.doc` hérité pour TNS). Vous obtenez simplement le fichier terminé.

La section Documents d'un accord. Générez un contrat à gauche ; les documents générés et reçus (avec statut de signature) sont listés ci-dessous, chacun téléchargeable.

Signature : en ligne ou hors ligne

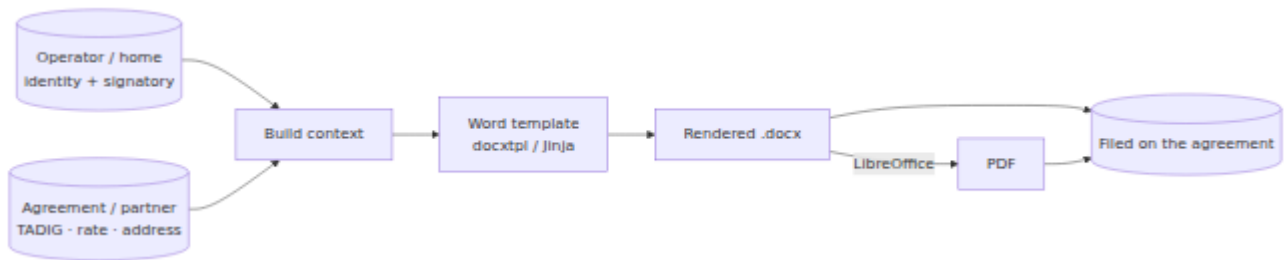
OmniRoam prend en charge deux voies de signature :

Signature électronique en ligne (le partenaire signe dans le navigateur, sans connexion). À partir d'un AA.12/AA.13 généré, vous cliquez sur **Envoyer pour signature**, nommez le signataire et son email, et OmniRoam :

1. Crée une demande de signature avec un jeton opaque et envoie au partenaire un **lien sécurisé** (aucun compte requis).
2. Lorsqu'ils l'ouvrent, OmniRoam marque la demande comme *vue* et l'enregistre sur la chronologie. Ils examinent le document, corrigent éventuellement leur nom/titre/entreprise de signataire, et **signent** en tapant leur nom et/ou en dessinant une signature.
3. OmniRoam produit le **PDF signé** et l'envoie par email à **les deux parties** (signataire + boîte aux lettres de retour de votre opérateur), l'archive sur

l'accord, et enregistre "Signé par ... le ...".

4. Le partenaire peut également **décliner** (avec une raison), ce qui est également enregistré.



Signature hors ligne. Préférez-vous signer à l'ancienne ? Téléchargez le document généré, signez-le à l'extérieur, et téléchargez la copie signée sur l'accord. Un nom de fichier contenant *signé/exécuté/contresigné* est reconnu comme une copie signée. Un email entrant qui en joint une fait automatiquement avancer le statut à *IRA Signé*.

Le Pack de Roaming : premier contact en un clic

Au lieu de générer chaque formulaire séparément, **Envoyer le pack de roaming** envoie à un contact partenaire l'**AA.12 + AA.13 + offre IOT** ensemble dans un seul message. Il génère les contrats en tant que PDFs à la volée et joint votre offre IOT la plus récente. Choisissez un contact (ou tapez un nom + email, qui est complété en tant que contact), et OmniRoam envoie le pack avec votre formulation de modèle enregistrée. C'est l'email d'ouverture "laissons-nous conclure un accord de roaming", envoyé depuis l'intérieur d'OmniRoam.

Modèles d'email modifiables

Les trois emails automatisés (**demande de signature**, **copie signée**, et **pack de roaming**) utilisent des modèles modifiables (remplacement par opérateur, sinon un défaut global), avec des espaces réservés comme `{{ signer_name }}`, `{{ partner }}`, `{{ operator }}`, `{{ sign_url }}` et `{{ document_name }}`. Ajustez la formulation une fois dans les Paramètres et chaque envoi l'utilise.

Comment les emails quittent réellement OmniRoam. Tous les mails sortants passent par l'**API d'envoi HTTPS de Mailjet**, pas SMTP. Les plateformes d'hébergement (Railway) bloquent les ports SMTP sortants, donc OmniRoam POST à Mailjet via HTTPS à la place. Les envois sont **meilleure effort et non-bloquants** : le bouton de l'interface utilisateur retourne immédiatement et le mail sort sur un fil d'arrière-plan, donc un serveur de mail lent ne bloque jamais l'application.

4. Archivage & Stockage

Chaque document est archivé **directement sur l'accord** auquel il appartient. Cela couvre les documents **générés** (AA.12, AA.13, CLL, TCC, TNS...) et les documents **reçus** (une copie signée jointe à un email, un IR.21 téléchargé, une fiche IOT). Il n'y a pas de magasin de documents séparé à gérer :

- Les documents sont stockés sous forme de blobs **dans la base de données**, étiquetés avec un **type** (`aa12`, `aa13`, `aa12_signed`, `iot`, `ir21`, `cll`, `other`, ...), nom de fichier, type de contenu, taille, et si OmniRoam l'a **généré**.
- Les copies signées sont étiquetées distinctement (par exemple `aa12_signed`) afin que l'ensemble signé soit toujours distinguable des brouillons.
- **Les pièces jointes entrantes sont déduplicuées** : une copie identique (même nom de fichier + longueur d'octet) qui arrive à nouveau n'est pas réarchivée.
- Chaque génération, téléchargement, signature, et exportation IOT écrit une **entrée de chronologie**, donc le journal d'activité de l'accord est une trace complète de ce qui a été produit et reçu, et quand.

Pour récupérer un document, ouvrez la section **Documents** de l'accord et téléchargez-le (Word/PDF généré, ou l'original reçu). Les PDFs signés produits par le flux de signature en ligne sont stockés sur la demande de signature et également envoyés par email aux deux parties.

Vous pouvez également **exporter le tarif convenu en tant que fichier XML GSMA RAEX IOT 5.0** depuis l'accord. C'est la même sélection de tarifs que les

formulaire TNS utilisent, donc l'IOT exporté et les formulaires générés sont toujours d'accord.

5. Ordres de Travail & Notifications des Assignés

Rendre un partenaire opérationnel est un *travail* : expédition de SIMs, changement de routage, exécution de tests IREG/TADIG, audits, résolution de problèmes. Dans OmniRoam, ce travail est suivi sous forme d'**Ordres de Travail** : l'unité unique de travail de roaming suivie. Un ordre de travail peut être associé à un accord (un partenaire) ou être autonome.

La vue des Ordres de Travail. Chaque ordre a un type, une priorité, un statut, un lien partenaire optionnel, et un assigné : la partie notifiée lorsqu'il est assigné.

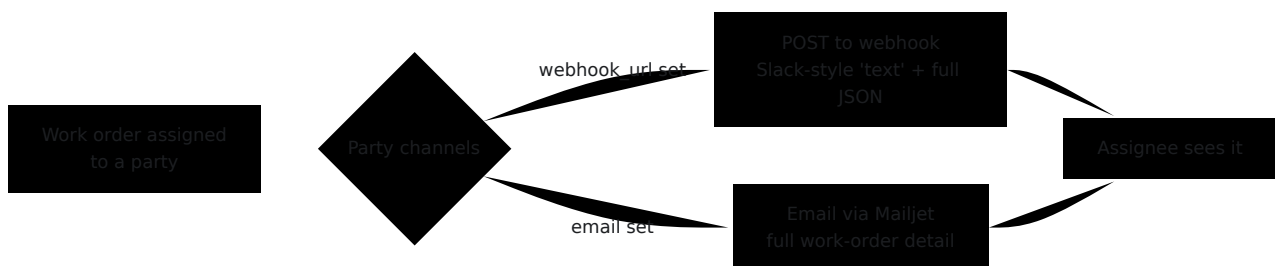
Création et assignation

Un ordre de travail a un **type** (Expédition de SIM, Routage, Test IREG, Test TADIG, Audit, Problème), un titre, une priorité, un statut (Ouvert / En Cours / Bloqué / Fait / Annulé), un lien partenaire (accord) optionnel, des détails en texte libre, une date d'échéance, et des champs structurés spécifiques au type (par exemple, une expédition de SIM comporte la quantité, l'adresse postale, le transporteur et le suivi).

Vous assignez un ordre de travail à une **partie** : une équipe interne nommée ou un contact externe (par exemple, "NOC Roaming", "administrateur TADIG") géré par opérateur dans **Paramètres**. Vous pouvez définir un **assigné par défaut par type d'ordre de travail**, donc une nouvelle expédition de SIM s'assigne automatiquement à celui qui gère l'expédition, sauf si vous le remplacez.

La notification : webhook + email

Lorsqu'un ordre de travail est **assigné** (créé avec un assigné, ou réassigné à une nouvelle partie), OmniRoam **notifie cet assigné** par les canaux que la partie a configurés :



- **Webhook** : si la partie a une URL de webhook (par exemple, un **webhook entrant Slack**), OmniRoam POST un message avec un bloc **text** lisible par l'homme *et* l'intégralité de l'ordre de travail sous forme de JSON structuré (type, priorité, statut, partenaire, la charge utile spécifique au type, un lien vers la page des Ordres de Travail).
- **Email** : si la partie a une adresse email, OmniRoam envoie le même détail par email (via Mailjet), sujet **[Ordre de Travail] <titre> vous a été assigné**.

Une partie avec **aucun** canal défini est simplement un assigné silencieux (sans opération). Les deux notifications sont des efforts de meilleure qualité et non-bloquants, donc un webhook ou un serveur de mail lent ne peut jamais bloquer l'application. La réassignation ne notifie que lorsque l'assigné change réellement à une nouvelle partie (donc modifier d'autres champs ne renvoie pas de notification).

Du point de vue de l'assigné : vous recevez un message Slack (ou un email) au moment où un travail arrive dans votre équipe, avec tout ce dont vous avez besoin : quoi faire, pour quel partenaire, le nombre de SIM et l'adresse d'expédition (ou le changement de routage, ou la portée du test), la priorité et la date d'échéance, et un lien direct vers l'ordre de travail.

Le Cycle de Vie Complet, de A à Z

Pour tout rassembler, voici le parcours de "un partenaire nous a envoyé un email" à "le partenaire est opérationnel" :

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

Work order: SIM
Dispatch
→ Roaming NOC notified

Work order: Routing
DRA / SS7 / DNS
provisioning

Work order: IREG /
TADIG Testing

Generate TNS forms
IOT now confirmed

status → Launched

À chaque étape, la **chronologie** de l'accord enregistre ce qui s'est passé, et le **journal des emails entrants** conserve la preuve brute de ce que chaque email a contribué.

Ce que Vous Configurez Une Foix

La plupart de l'automatisation nécessite juste une petite configuration unique par opérateur (dans **Paramètres**) :

Paramètre	Pourquoi	Où il est utilisé
Détails de la paperasse (nom légal, TADIG, PLMN, pays, signataire & titre , lieu, adresse)	Remplit le côté domestique de chaque document généré	Génération de documents
Adresse email entrante	L'adresse à laquelle vous transmettez/CC les mails des partenaires	Ingestion des emails
Boîte aux lettres de retour signée	Où vont les emails signés hors ligne et les copies signées	Signature
Modèles d'email (demande de signature, copie signée, pack de roaming)	Votre formulation pour les emails automatisés	Email sortant
Parties des ordres de travail + assignés par défaut par type	Qui reçoit des notifications pour chaque type de travail	Ordres de travail

Avec cela en place, transmettre un email de partenaire devient vraiment :
email entrant → accord sortant → contrats générés et signés → ordres de travail

élevés et votre équipe notifiée.

Voir Aussi

- **OmniRoam : Automatisation des Tests de Roaming** : l'*autre* OmniRoam. Il exécute les carnets de tests de roaming GSMA (IR.38 / IR.48 / VoLTE) contre un réseau en direct. Ceci est complémentaire : signez l'accord ici, prouvez qu'il fonctionne là.
- **Opérations Communes** : les modèles de visualisation/édition partagés à travers tout OmniWeb.

OmniRoam : Automatisation des Tests de Roaming

OmniRoam est la fonctionnalité d'automatisation des livres de tests de roaming d'OmniWeb. Elle exécute les livres de tests de conformité au roaming de la GSMA contre un réseau en direct. Elle exécute automatiquement les cas de test individuels à partir d'un appareil de test. Elle enregistre un verdict de réussite/échec avec des preuves à l'appui pour chaque cas. Elle produit ensuite un classeur de test GSMA complété, prêt à être envoyé à un partenaire de roaming ou à un hub.

En résumé : OmniRoam transforme un exercice de conformité au roaming manuel de plusieurs heures en une pression de bouton (ou un travail programmé). Elle restitue le même tableau officiel de la GSMA qu'un testeur remplirait autrement à la main.

OmniRoam a deux volets. Ce document couvre les **livres de tests de roaming** (IR.38 / IR.48 / tests de conformité VoLTE : *le roaming fonctionne-t-il réellement ?*). L'autre volet concerne les **accords de roaming et l'automatisation des e-mails**. Il transforme un e-mail partenaire en un accord signé, générant des documents AA.12/AA.13/CLL/TCC/TNS, et les ordres de travail pour mettre le partenaire en service. Cela est documenté séparément dans **Accords de Roaming & Automatisation des E-mails**. Un produit, deux tâches : *faire signer l'accord* (là) et *prouver que le roaming fonctionne* (ici).

L'écran des Livres de Tests de Roaming. Chaque ligne est un livre exécuté contre un partenaire de roaming, avec son statut actuel.

Liens Rapides

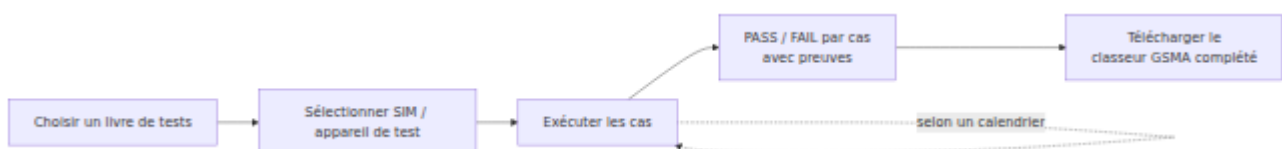
- **Livres de Tests** : les livres disponibles (IR.38, IR.48, VoLTE) et chaque cas de test qu'ils contiennent
- **Exécution des Tests** : comment créer un livre, l'exécuter, personnaliser l'ensemble des cas, et programmer des exécutions routinières
- **Explorateur de Livres de Tests** : comment inspecter ce que chaque livre teste et comment chaque cas est exécuté
- **Documents de Livres de Tests Complétés** : comment OmniRoam génère le classeur GSMA rempli
- **Accords de Roaming & Automatisation des E-mails** : le *autre* volet d'OmniRoam. Transmettez un e-mail partenaire → accord créé, contrats générés et signés électroniquement, archivés, et ordres de travail émis

Ce Que Fait OmniRoam

Un livre de tests de roaming est une liste de contrôle définie par la GSMA : une liste de cas de test qui prouvent qu'un abonné d'un réseau (le **PLMN D'origine**, "PLMN(a)") reçoit les services attendus tout en roaming sur un autre réseau (le **PLMN Visité**, "PLMN(b)"). Historiquement, chaque cas est effectué manuellement et le résultat est écrit dans un tableau.

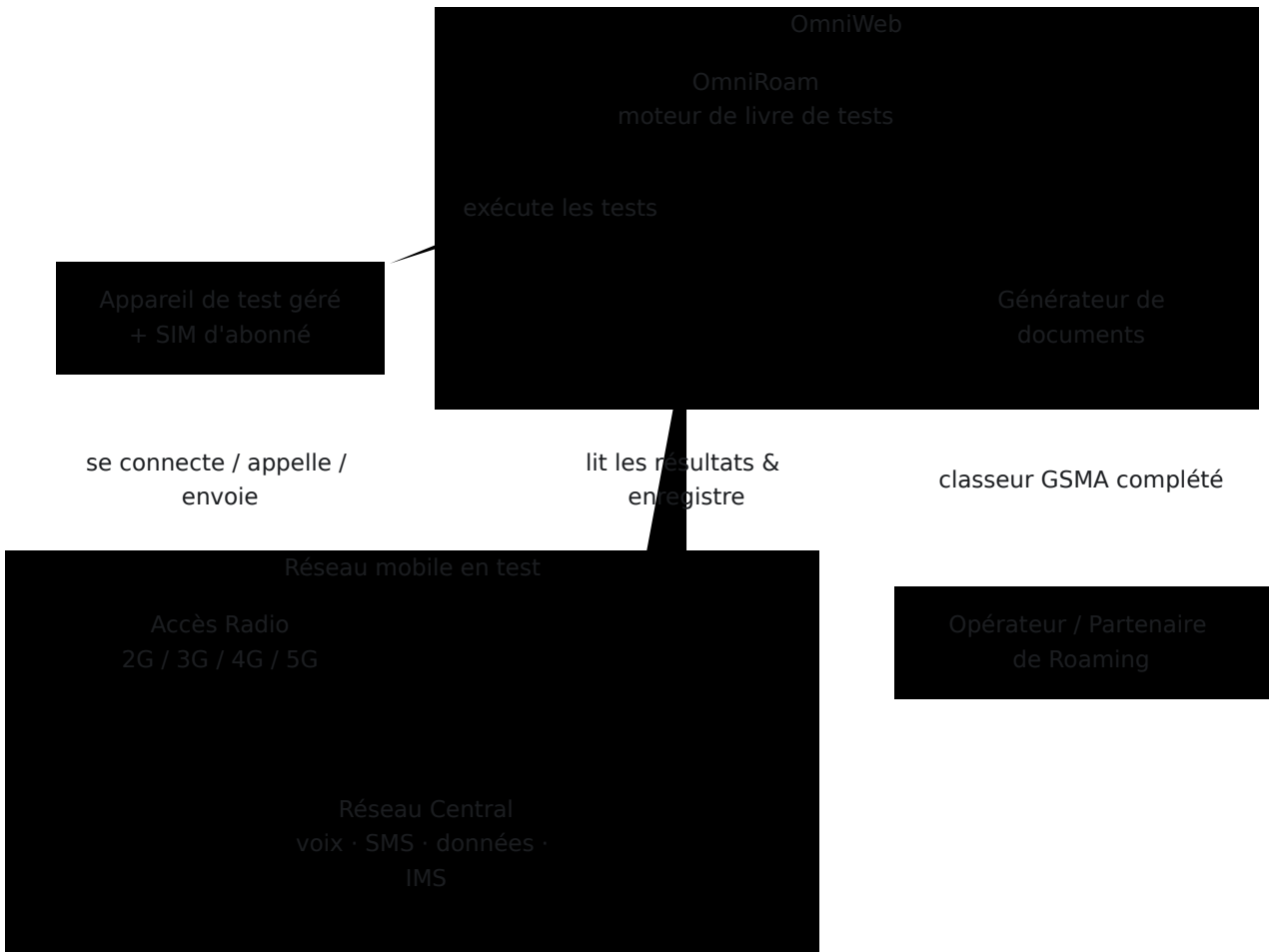
OmniRoam automatise trois choses :

1. **Exécution du test** : elle passe l'appel, envoie le SMS, exécute la session de données, ou provisionne le service complémentaire sur un appareil de test.
2. **Évaluation du résultat** : elle compare ce qui s'est passé avec le résultat attendu de la GSMA. Elle enregistre **PASS**, **FAIL** ou **NOT PERFORMED**, avec les preuves à l'appui (temps, débit, causes de libération du réseau, etc.).
3. **Production du document** : elle remplit le classeur officiel de la GSMA avec les résultats et toutes les métadonnées environnantes (identités, dates, détails du testeur).



Où Cela S'inscrit

OmniRoam teste un véritable abonné sur le véritable réseau en utilisant un appareil de test géré. Chaque cas automatisé pilote l'appareil, puis lit le résultat depuis l'appareil et, le cas échéant, depuis les propres enregistrements du réseau (par exemple, les enregistrements de facturation de la passerelle de service pour une session de données). Rien n'est simulé : un appel qui est signalé comme connecté l'est réellement.



Concepts Clés

Terme	Signification
Livre de tests	Un ensemble de cas de test défini par la GSMA (par exemple, IR.38, IR.48, VoLTE). Voir Livres de Tests .
Cas de test	Un contrôle unique au sein d'un livre, identifié par son numéro GSMA (par exemple, cas IR.48 2.3, "Interdiction de tous les appels sortants").
Exécution	Une exécution d'un livre (ou d'un sous-ensemble choisi de ses cas) contre un appareil et une SIM.
Verdict	Le résultat enregistré d'un cas : <code>PASS</code> , <code>FAIL</code> , ou <code>NOT PERFORMED</code> .
Preuve	Le détail de soutien capturé pour un verdict : temps, chiffres de débit, causes réseau, retours de lecture d'interrogation, etc.
PLMN D'origine (a)	Le réseau qui possède l'abonné testé.
PLMN Visité (b)	Le réseau sur lequel l'abonné est en roaming.

Cas Automatisés vs. Manuels

La plupart des cas dans chaque livre sont **auto-exécutés** : OmniRoam les effectue de bout en bout et enregistre le verdict sans interaction de l'opérateur. Quelques cas dépendent de conditions réseau que vous ne pouvez pas induire à partir d'un appareil de test seul (par exemple, les tests négatifs CAMEL prépayés optionnels, ou la livraison de messages multimédias). Ceux-ci restent

manuels. OmniRoam les liste toujours dans le livre et l'opérateur enregistre le résultat à la main, de sorte que le document final soit complet.

L'[Explorateur de Livres de Tests](#) montre exactement quels cas dans un livre sont automatisés et comment chacun est exécuté.

Normes Référencées

OmniRoam suit les Documents de Référence Permanents de la GSMA et les spécifications 3GPP sous-jacentes :

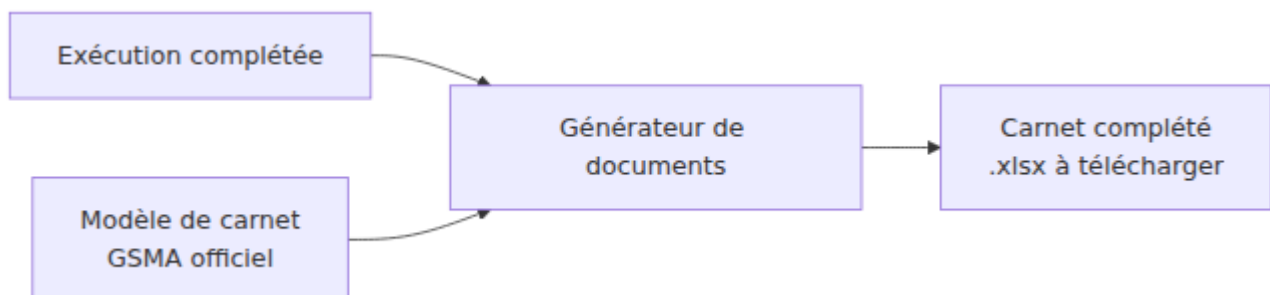
Référence	S'applique à
GSMA IR.38	Livre de tests de données de roaming LTE
GSMA IR.48 / IR.24	Livre de tests de roaming bilatéral (voix / SMS / MMS / données)
GSMA BA.65	Tests de roaming VoLTE
GSMA IR.92	Profil IMS pour voix et SMS (comportement VoLTE)
GSMA IR.88	Directives de roaming LTE (causes de rejet de connexion)
3GPP TS 22.011	Accessibilité du service (interdiction déterminée par l'opérateur)
3GPP TS 23.011	Statut du service complémentaire (Actif/Enregistré/Provisionné/Quiescent)
3GPP TS 22.082	Services complémentaires de renvoi d'appel
3GPP TS 22.088	Services complémentaires d'interdiction d'appel

Documents de Test-Book Complétés

Le produit final d'une exécution d'OmniRoam est un **carnet de test GSMA complété** : le tableau officiel GSMA pour le livre, rempli avec les résultats de l'exécution et tous les détails environnants, prêt à être envoyé à un partenaire ou un hub de roaming. OmniRoam le produit avec une seule action **Télécharger le Test Book**. Il n'a pas besoin de transcription manuelle.

Ce que vous obtenez

OmniRoam prend le modèle officiel GSMA pour le livre et le remplit sur place, de sorte que le résultat est le même carnet que le partenaire s'attend à recevoir (mêmes feuilles, même numérotation des cas, même mise en page), mais peuplé avec de vrais résultats au lieu de champs vides.



Ce qui est rempli

Trois catégories d'informations sont écrites dans le carnet.

1. Résultats par cas

Pour chaque cas dans le livre, la cellule de résultat du carnet est définie sur le verdict enregistré (**PASS**, **FAIL**, ou **NOT PERFORMED**). La cellule de commentaires du cas est remplie avec les preuves de soutien capturées pendant l'exécution.

Dans le document	Provient de
Résultat du cas de test (PASS / FAIL / NOT PERFORMED)	Le verdict du cas
Commentaires du cas de test	Les preuves : temps, débit, causes réseau, lectures d'interrogation, etc.

2. Identités et métadonnées

Les sections d'en-tête et d'informations sur l'opérateur sont remplies à partir de l'exécution :

Dans le document	Provient de
IMSI	La carte SIM de test
MSISDN	La carte SIM de test
PLMN d'origine (a) / PLMN visité (b)	Le partenaire de roaming / PLMNs choisis pour le livre
Date des tests	La date de l'exécution
Nom, téléphone, email du testeur	Les détails du testeur sur le livre
APN (le cas échéant)	La configuration de données utilisée

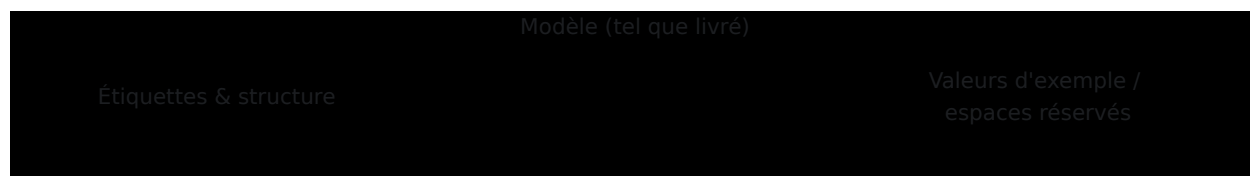
3. Valeurs mesurées

Pour les cas de données et de services supplémentaires, les valeurs mesurées spécifiques demandées par la feuille GSMA sont écrites dans leurs cellules dédiées :

Dans le document	Provient de
Heures de début / fin de session de données	La session de données
Volumes de données envoyés / reçus	Les enregistrements de facturation de la passerelle de service
Durée de la session	La session de données
Débit / taux de données moyen	La mesure de débit
Indications de succès du service (Oui/Non)	Le résultat du cas

Sortie Propre et Présentable

Les modèles GSMA vierges sont livrés avec du contenu d'exemple et des espaces réservés dans les cellules à remplir : des temps d'exemple et des notes de référence destinées à guider un testeur manuel. OmniRoam supprime ce contenu d'espace réservé lorsqu'il génère le document, de sorte que le carnet complété montre uniquement vos vrais résultats et des champs vides là où une valeur n'a pas été capturée. Il ne transporte jamais les données d'exemple du fournisseur dans votre rapport livré, et il ne remplace jamais les étiquettes, en-têtes ou structures GSMA.



Quand Générer

Vous pouvez télécharger le document à tout moment. Il reflète toujours l'état actuel de l'exécution. Un flux typique consiste à exécuter le livre (ou une routine programmée), à examiner les verdicts par cas, à relancer les cas qui nécessitent une attention, puis à télécharger le carnet terminé une fois que les résultats semblent corrects. Comme l'exportation reflète l'exécution en direct, une ré-exportation après une nouvelle exécution produit simplement un document mis à jour.

Cas Manuels dans le Document

Les cas qu'OmniRoam ne peut pas conduire automatiquement apparaissent toujours dans le carnet avec leur numéro de cas et leur titre, prêts pour que le testeur enregistre un résultat à la main. Cela garde le document livré complet : les cas automatisés sont remplis avec de vraies preuves, et les cas manuels sont présentés au bon endroit pour que le testeur termine.

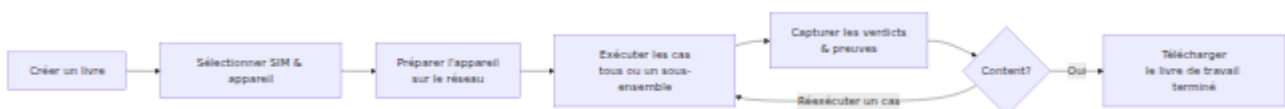
Voir [Exécution des Tests](#) pour savoir comment les verdicts sont produits et [Explorateur de Test Book](#) pour le mappage exact cellule par cellule de ce qui est rempli.

Exécution des Tests OmniRoam

Ce guide couvre l'ensemble du cycle de vie d'un test de roaming : création d'un livre, exécution, observation des cas en cours d'exécution, personnalisation des cas à exécuter, réexécution d'un seul cas et planification d'exécutions de routine non surveillées.

- [Le Cycle de Vie du Test](#)
- [Création d'un Livre de Test](#)
- [Exécution d'un Livre](#)
- [Comment les Cas Automatisés Sont Pilotés](#)
- [Personnalisation d'une Exécution](#)
- [Réexécution d'un Cas Unique](#)
- [Exécutions de Routine et Planifiées](#)
- [Lecture des Résultats](#)

Le Cycle de Vie du Test



Création d'un Livre de Test

L'écran des Livres de Test de Roaming liste chaque livre avec son type, les réseaux d'origine et visités, l'identité de l'abonné, le testeur, et le statut actuel.

Un livre de test est créé à partir de l'écran **Livres de Test de Roaming**. Lors de la création d'un livre, vous choisissez :

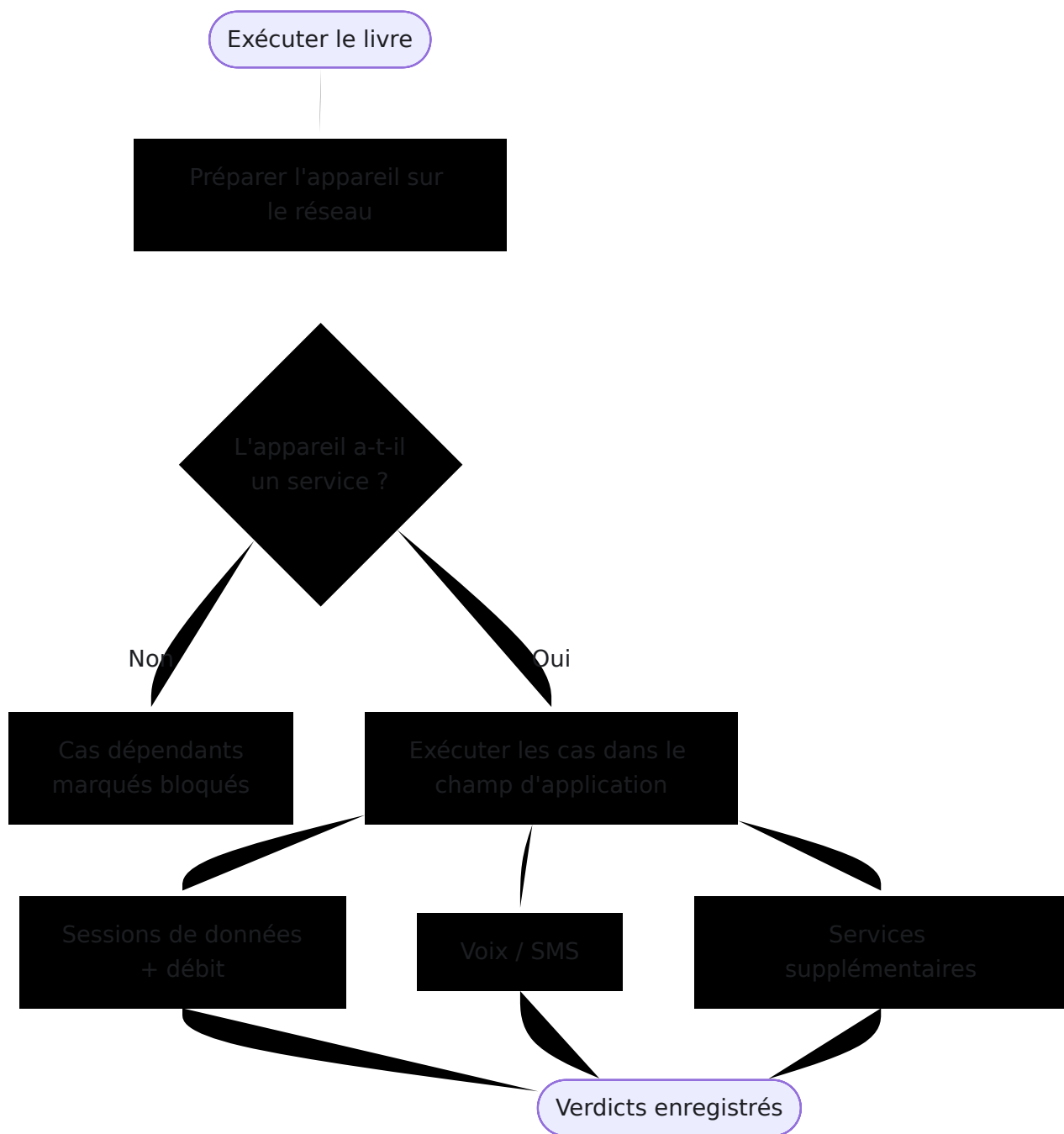
Champ	Objectif
Type de livre	Quel livre GSMA exécuter : IR.38, IR.48, ou VoLTE. Cela sélectionne l'ensemble des cas.
Partenaire de roaming / PLMNs	Les réseaux d'origine (PLMN a) et visités (PLMN b). Utilisé pour remplir l'en-tête du document et pour choisir le bon seuil de débit.
SIM	La SIM de l'abonné à tester. Son IMSI et MSISDN sont lus et utilisés tout au long de l'exécution et dans le document final.
Détails du testeur	Nom, téléphone et e-mail de la personne responsable, écrits dans le livre de travail terminé.

Une fois créé, le livre liste chaque cas du livre GSMA choisi, chacun commençant dans un état "non encore exécuté".

Exécution d'un Livre

L'exécution d'un livre effectue chaque cas dans le champ d'application à tour de rôle. Avant que les cas de test ne s'exécutent, OmniRoam prépare l'appareil de test sur le réseau. Il présente la SIM et confirme que l'appareil est connecté et a un service. C'est une **porte d'entrée préalable** : si l'appareil ne peut pas obtenir de service, les cas dépendants sont signalés comme bloqués plutôt que comme échoués, car il n'y a aucun intérêt à un test de données ou de voix sans porteur.

Dans le cadre de la préparation de l'appareil, OmniRoam **lit l'identité de l'abonné à partir du modem et remplit automatiquement le livre** : l'**IMSI** est lu à partir de la SIM, le **réseau d'origine (HPLMN)** en est dérivé, et le **réseau visité (VPLMN)** est lu à partir du réseau sur lequel l'appareil est actuellement campé. Cela remplit l'en-tête du livre, et donc le document final, avec ce qui a réellement été testé, plutôt qu'avec des valeurs saisies manuellement.



Pendant qu'un livre s'exécute, l'écran montre chaque étape au fur et à mesure qu'elle se produit, avec l'étape actuelle mise en surbrillance et une indication en direct de réussite/échec par cas.

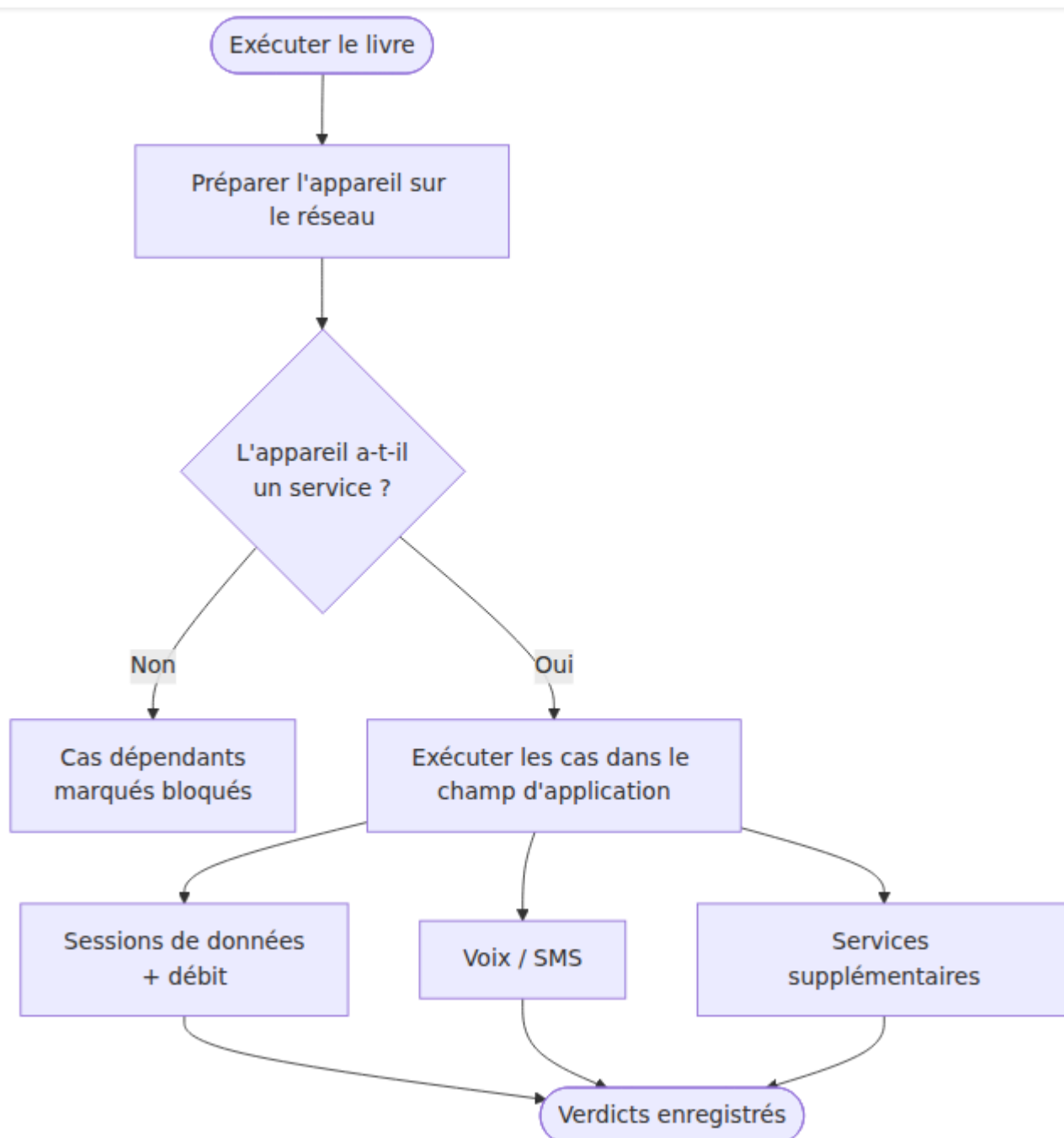
Comment les Cas Automatisés Sont Pilotés

Chaque cas automatisé pilote l'appareil de test, observe ce que le réseau fait, et compare le résultat avec le résultat attendu par la GSMA. Un cas ne réussit

que sur des preuves positives. Une étape qui ne peut pas être confirmée est enregistrée comme un échec avec la raison, jamais comme un succès silencieux.

Sessions de données et débit

Pour les cas de données, OmniRoam établit une session de données par paquets, exécute du trafic pour mesurer le taux de téléchargement/téléversement atteint et la latence, puis se déconnecte afin que le réseau écrive un enregistrement de facturation propre pour la session. Les volumes de données et les temps sont lus à partir des enregistrements de facturation de la passerelle de service. Pour le cas de vitesse IR.38, le taux mesuré est affirmé par rapport au seuil de débit pour la distance d'origine/visitée.



Appels vocaux

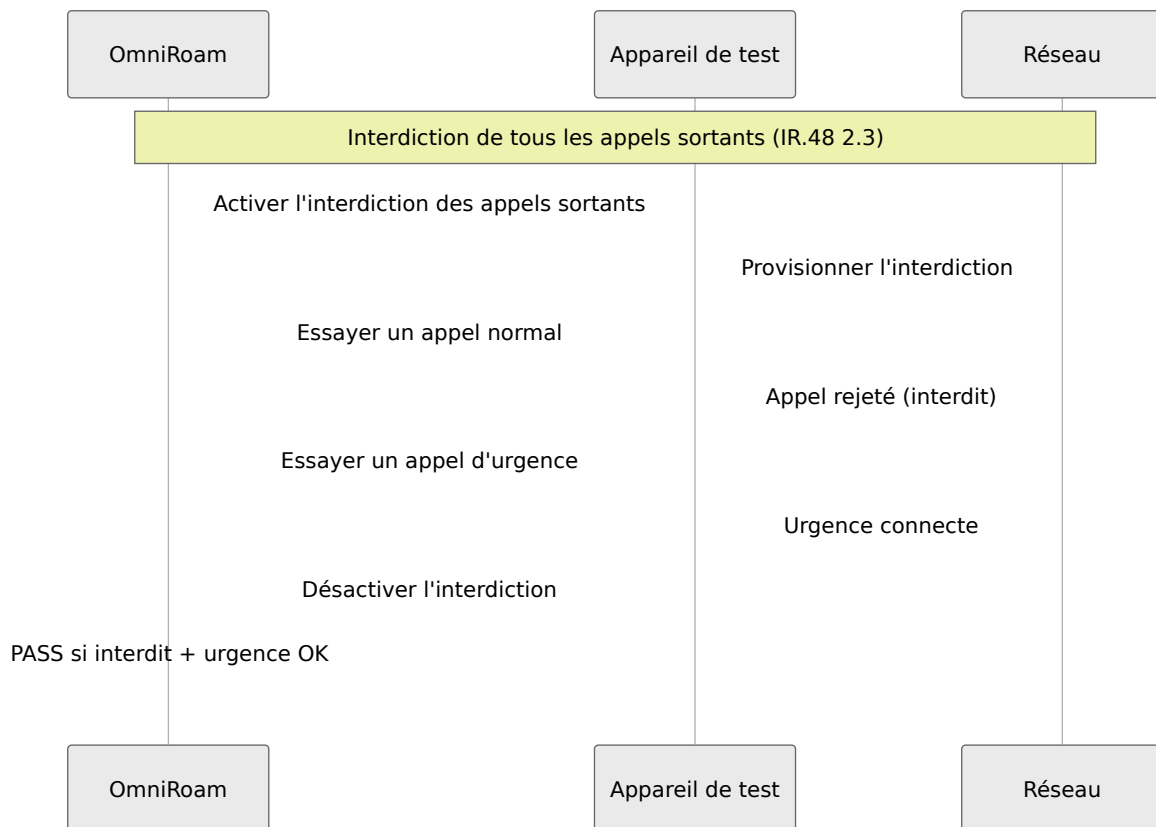
OmniRoam passe un appel de l'appareil à un service de réponse de laboratoire, confirme que l'appel atteint l'état actif (répondu), le maintient éventuellement pour confirmer la stabilité, puis le termine. Le verdict enregistre le temps de connexion et si l'appel est resté actif.

SMS

OmniRoam envoie un message avec un corps unique à un service de réponse de laboratoire et attend la réponse. La livraison de la réponse confirme les SMS d'origine mobile et terminés mobile de bout en bout. Une réponse manquante est un échec clair avec la raison, pas un plantage.

Services supplémentaires (interdiction d'appels et renvoi)

OmniRoam provisionne des services supplémentaires par voie aérienne depuis l'appareil de test lui-même, exactement comme un abonné le ferait avec les codes de contrôle de service standard, puis les exerce :



Pour **Renvoi d'Appel en Cas de Non Réponse**, OmniRoam enregistre le renvoi vers un numéro cible avec un minuteur de sonnerie, puis interroge le service et confirme que le réseau a stocké le numéro et le minuteur de renvoi qui ont été enregistrés.

Annulation de Localisation (IR.38 3.1.2)

Certains cas sont pilotés depuis le côté réseau plutôt que depuis l'appareil.

Pour **Annulation de Localisation LTE**, OmniRoam demande au serveur d'abonnés d'origine d'annuler la localisation de l'abonné sur le réseau visité, et enregistre un succès lorsque la demande est acceptée. Cela confirme que le réseau d'origine peut retirer un enregistrement de roaming.

Enregistrement IMS (VoLTE)

Pour VoLTE, OmniRoam confirme d'abord que l'appareil est enregistré auprès de l'IMS. Cela conditionne les cas dépendants de l'IMS : si l'enregistrement n'est pas confirmé, les cas d'appel VoLTE et de SMS sur IMS sont signalés comme bloqués.

Personnalisation d'une Exécution

Une exécution n'a pas besoin de couvrir l'ensemble du livre. En utilisant le **sélecteur de test**, l'opérateur sélectionne exactement quels cas exécuter. Cela est utile pour :

- Re-valider uniquement les cas qui ont échoué précédemment.
- Exécuter uniquement les cas vocaux, ou uniquement les cas de données, lors de la recherche de pannes.
- Sauter des cas qui dépendent d'un arrangement qui n'est pas encore en place (par exemple, un accord CAMEL).

Les cas laissés de côté conservent leur verdict existant et ne sont pas touchés.

Réexécution d'un Cas Unique

Chaque cas a un contrôle de réexécution. Le sélectionner exécute à nouveau ce seul cas, contre le même appareil et la même SIM, et met à jour uniquement le verdict de ce cas. C'est le moyen le plus rapide de confirmer un correctif (par exemple, réexécuter le cas de débit après un changement de transport) sans répéter l'ensemble du livre.

Exécutions de Routine et Planifiées

OmniRoam peut exécuter des tests **non surveillés selon un calendrier** afin qu'une relation de roaming soit continuellement validée plutôt que vérifiée une seule fois.

- **Vérifications de routine** exécutent un ensemble compact de vérifications de santé contre un appareil (données, vitesse, voix et SMS) et rapportent un succès/échec combiné. Ce sont les mêmes drives utilisés par les livres complets, emballés comme un contrôle de confiance rapide récurrent.
- **Les horaires** exécutent une routine choisie à intervalles récurrents automatiquement. Chaque exécution planifiée enregistre son propre résultat, construisant une histoire au fil du temps afin qu'une régression (par exemple, un débit tombant en dessous du seuil, ou un échec de livraison de SMS) soit détectée et visible sans que quiconque n'exécute un test manuellement.



Configuration d'un Horaire

Les horaires sont gérés sur l'écran **Horaires** sous Tests de Roaming. Un horaire définit :

Paramètre	Objectif
Nom	Identifie l'horaire (et étiquette ses métriques et son historique).
Modem(s)	L'appareil(s) de test contre lequel la routine s'exécute.
Vérifications	Quelles vérifications la routine effectue : données, test de vitesse, voix, SMS.
Intervalle	À quelle fréquence la routine s'exécute (par exemple, toutes les heures).

Une fois enregistré, l'horaire s'exécute automatiquement à son intervalle sans autre interaction. L'écran **Test de Routine** montre l'historique des exécutions : le succès/échec combiné de chaque exécution, les vitesses mesurées, et le détail par vérification. Une exécution échouée fait surface les mêmes preuves qu'une exécution interactive.

Surveillance Prometheus

Les résultats de routine planifiés sont exportés en tant que **métriques Prometheus**, de sorte que la santé du roaming puisse être alertée et affichée aux côtés du reste du réseau, de la même manière que les tests planifiés sur les appareils de test sont surveillés. L'exposition est servie à `/api/ir38/routine/metrics` (lit la dernière exécution planifiée par horaire et modem) :

Métrique	Type	Significat
<code>omniweb_ir38_routine_pass</code>	gauge	Dernier résu de routine planifié (1 = succès, 0 = échec)
<code>omniweb_ir38_routine_check_pass</code>	gauge	Résultat par vérification dernière exécution (étiquette <code>check</code> : données/tes vitesse/voix
<code>omniweb_ir38_routine_download_mbps</code>	gauge	Taux de téléchargem mesuré lors dernière exécution
<code>omniweb_ir38_routine_upload_mbps</code>	gauge	Taux de téléverseme mesuré lors dernière exécution
<code>omniweb_ir38_routine_latency_ms</code>	gauge	Latence me lors de la dernière exécution
<code>omniweb_ir38_routine_last_run_timestamp_seconds</code>	gauge	Temps Unix dernière

Métrique	Type	Significat
		exécution planifiée

Chaque série porte des étiquettes `schedule`, `serial`, `modem`, et `imsi` (plus `check` sur la métrique par vérification), vous permettant d'alerter par horaire, par appareil, ou par abonné d'origine. Le point de terminaison ne nécessite pas de connexion (les scrapers ne peuvent pas en porter une) et peut être sécurisé avec un jeton porteur si nécessaire.

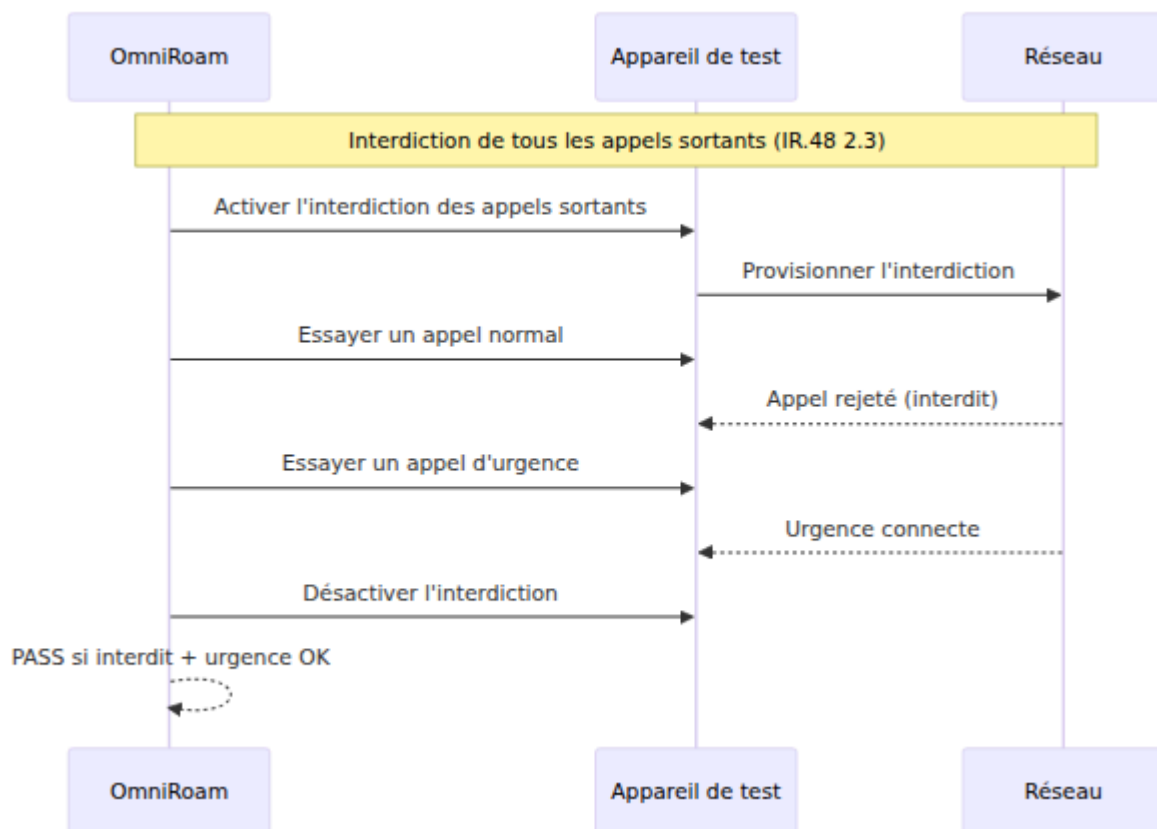
Exemple d'alerte : la voix de roaming échoue sur un appareil depuis 15 minutes :

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

Les résultats planifiés s'accumulent dans un historique qui peut être consulté à tout moment, et une exécution échouée fait surface les mêmes preuves qu'une exécution interactive.

Lecture des Résultats

Chaque cas montre son verdict (**PASS**, **FAIL**, ou **NON EXÉCUTÉ**) accompagné des preuves qui le soutiennent :



- **PASS** : le résultat attendu par la GSMA a été confirmé, avec les chiffres de soutien.
- **FAIL** : le résultat attendu n'a pas été atteint ; la raison est enregistrée (par exemple, "débit en dessous du seuil", "pas de réponse d'écho", ou la cause de libération du réseau pour un appel qui ne s'est pas connecté).
- **NON EXÉCUTÉ** : le cas n'a pas été exécuté, ou est un cas manuel en attente d'un testeur.

Lorsque les résultats semblent corrects, générez le document terminé. Voir [Documents de Livre de Test Complétés](#).

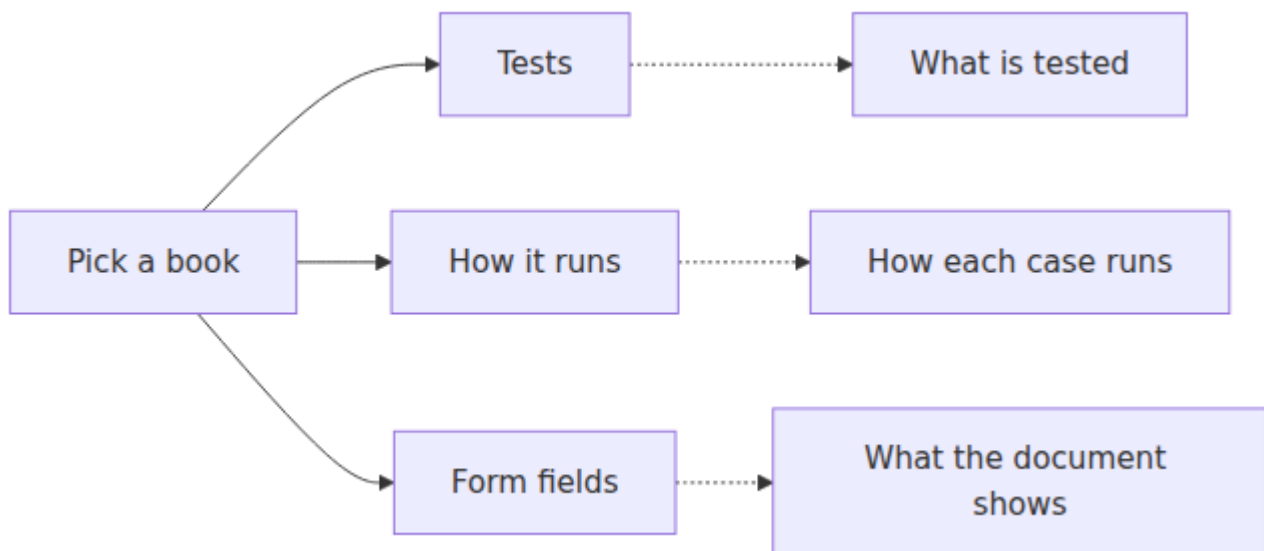
Explorateur de Livre de Test

L'Explorateur de Livre de Test est une vue de référence en lecture seule qui montre, pour chaque livre de test, exactement ce qu'il teste et comment. Il répond à trois questions qu'un opérateur pose généralement avant de faire confiance à une exécution automatisée :

1. **Quels cas sont dans ce livre, et lesquels sont automatisés ?**
2. **Comment chaque cas est-il réellement exécuté ?**
3. **Que contient le document final, et d'où provient-il ?**

L'Explorateur est accessible depuis l'écran des Livres de Test Itinérants via **Explorer les livres**, et vous permet de basculer entre IR.38, IR.48, et VoLTE.

L'Explorateur montrant le livre IR.48. Chaque cas est listé avec s'il est automatisé ou manuel et une description de comment il est exécuté.



Tests

La vue **Tests** liste chaque cas dans le livre avec :

- le **numéro de cas** et **titre** (correspondant à la spécification GSMA),
- si le cas est **automatisé** ou **manuel**, et
- une description simple de **comment il est exécuté** : par exemple "session de données + vérification d'enregistrement de facturation", "appel vocal", "activation de barring et tentative d'appel", ou "le testeur enregistre le résultat" pour les cas manuels.

C'est le moyen le plus rapide de voir, d'un coup d'œil, combien d'un livre donné OmniRoam exécute pour vous et ce qui reste à vérifier manuellement.

Comment Cela S'exécute

La vue **Comment cela s'exécute** montre la **séquence d'étapes** qu'une exécution complète du livre effectuera, dans l'ordre : préparation de l'appareil, les sessions de données, la vérification du débit, les tests de voix et SMS, les tests de services supplémentaires, et ainsi de suite. Elle reflète les cas actuellement en scope, donc c'est un aperçu précis de ce qu'une exécution fera avant que vous ne la commenciez.

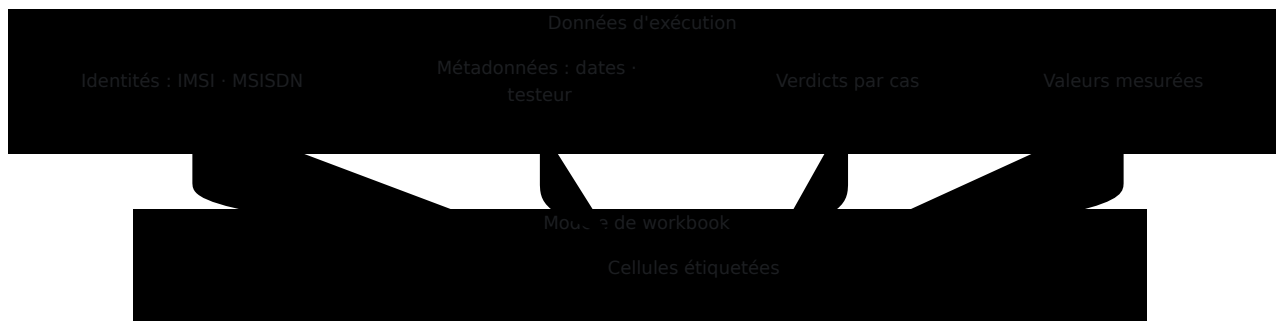
Cette vue est utile pour comprendre la structure d'une exécution et pour confirmer qu'un scope personnalisé effectuera les étapes que vous attendez.

Champs de Formulaire

La vue **Champs de Formulaire** liste chaque cellule dans le workbook GSMA complété que remplit OmniRoam, chaque cellule annotée avec :

- la **feuille et cellule** dans le modèle GSMA,
- l'**étiquette de champ GSMA** (lue à partir du modèle lui-même), et
- la **source** de la valeur : par exemple le MSISDN de l'abonné, la date de test, un verdict de réussite/échec par cas, ou une valeur mesurée telle que le volume de données.

Parce que cette liste est dérivée de la même logique qui produit le document, elle ne peut pas s'écarter de l'exportation réelle : ce que l'Explorateur dit sera rempli est exactement ce qui est rempli. Voir [Documents de Livre de Test Complétés](#) pour le document lui-même.



Télécharger le Modèle

L'Explorateur propose également une action **Télécharger le Modèle**, qui télécharge le workbook GSMA vierge pour le livre sélectionné : le modèle officiel avec le contenu d'exemple/placeholder du fournisseur supprimé, prêt à être rempli à la main si nécessaire. C'est le pendant vide du document complété qu'une exécution produit (voir [Documents de Livre de Test Complétés](#)).

Pourquoi Cela Compte

Un partenaire de roaming acceptant un livre de test complété a besoin de confiance que les résultats sont réels et que le document représente fidèlement ce qui a été testé. L'Explorateur rend la cartographie transparente : chaque cas automatisé peut être retracé depuis le numéro de cas GSMA, à travers la manière dont il est exécuté, jusqu'à la cellule exacte dans laquelle il se trouve sur le document final.

Livres de Test OmniRoam

OmniRoam expédie trois livres de test de roaming GSMA. Chaque livre est l'ensemble de tests GSMA officiel, avec des cas identifiés par leurs numéros de cas GSMA, de sorte que le document complété correspond un à un à la spécification publiée.

- [IR.38 : Test de Données de Roaming LTE](#)
- [IR.48 : Roaming Bilatéral \(Voix / SMS / MMS / Données\)](#)
- [VoLTE : Test de Roaming VoLTE](#)

Pour savoir comment chaque cas automatisé est réellement piloté et jugé, voir [Exécution des Tests](#). Pour parcourir les cas d'un livre de manière interactive, utilisez l'[Explorateur de Livre de Test](#).

Dans les tableaux ci-dessous, **Piloté** indique si OmniRoam exécute le cas automatiquement (**Auto**) ou le laisse au testeur pour enregistrement (**Manuel**).

IR.38 : Test de Données de Roaming LTE

Basé sur **GSMA IR.38 v3.0**. Prouve qu'un abonné en roaming peut s'attacher pour des données sur le réseau LTE visité, accéder aux services via le réseau d'origine, et recevoir un débit acceptable. Il prouve également le fallback voix et SMS par circuit commuté, et les données 2G/3G, lorsque ceux-ci sont dans le champ d'application.

Cas	Titre	Piloté	Ce qu'il prouve
3.1.1	Test de vitesse LTE (données + débit)	Auto	Une session de données s'établit via la passerelle d'origine, transporte du trafic, et atteint le seuil de débit.
3.1.2	Annulation de Localisation LTE	Auto	Le réseau d'origine peut annuler la localisation de l'abonné sur le réseau visité (déclenché depuis le serveur d'abonnés d'origine).
3.1.3	Interdiction Déterminée par l'Opérateur LTE	Manuel	L'interdiction déterminée par l'opérateur appliquée dans l'enregistrement de l'abonné d'origine est respectée.
3.2.2	Fallback CS : Appel Voix Mobile Originaire	Auto	Un appel voix originaire de l'abonné réussit via le fallback CS.
3.2.3	Fallback CS : Appel Voix Mobile Terminé	Manuel	Un appel à l'abonné réussit via le fallback CS.
3.2.4	SMS sur SGs	Auto	Les SMS d'origine mobile et terminés fonctionnent sur l'interface SGs.
3.3.1	Accès aux Données depuis 2G/3G en utilisant PGW dans HPLMN	Auto	Une session de données 2G/3G atteint des services via la passerelle d'origine.
3.4	Accès aux Données depuis 4G + 5G NSA sur S8	Auto	Les données par paquet sont disponibles et atteignent Internet (confirmé par une session de

Cas	Titre	Piloté	Ce qu'il prouve
			données avec vérification de connectivité).

Annulation de Localisation (3.1.2)

OmniRoam automatise l'Annulation de Localisation en demandant au serveur d'abonnés d'origine d'annuler la localisation de l'abonné sur le réseau visité, puis en confirmant que la demande a été acceptée. Il s'agit de la suppression de l'enregistrement de roaming initiée par le réseau d'origine (conformément à la procédure d'annulation de localisation dans [3GPP TS 29.272](#)).

Le KPI de Débit

Le cas [3.1.1](#) fait plus que confirmer une session de données. Il mesure le taux de téléchargement atteint et le compare au seuil de débit IR.38. Le seuil dépend de la distance géographique entre les réseaux d'origine et visité (des chemins plus longs permettent des taux plus bas) :

Protocole	Distance < 4000 km	Distance ≥ 4000 km
HTTP	≥ 11 Mbit/s	≥ 5 Mbit/s
FTP	≥ 13.5 Mbit/s	≥ 6 Mbit/s

OmniRoam estime la distance à partir des identités des réseaux d'origine et visité et sélectionne automatiquement le seuil correct ; l'opérateur peut remplacer la distance ou le protocole lorsque les valeurs par défaut ne correspondent pas à la configuration du test. Enregistrer une vitesse sans la tester par rapport au seuil n'est jamais considéré comme un succès.

IR.48 : Roaming Bilatéral (Voix / SMS / MMS / Données)

Basé sur **GSMA IR.48 v2.1** (interne à l'ensemble de tests IR.24). Le livre classique de roaming bilatéral 2G/3G : appels de base, services supplémentaires, SMS et données par paquet, exercés pour un abonné en roaming dans le réseau visité.

Cas	Titre	Piloté	Ce qu'il prouve
2.1	MS1(a) appelle MS2(a), tous deux en roaming dans VPLMN(b)	Auto	Un appel voix de base s'établit et se maintient.
2.2	Test négatif CAMEL (MOC, prépayé, pas d'accord)	Manuel	Un appel prépayé est correctement interdit lorsqu'il n'y a pas d'accord CAMEL actif.
2.3	Interdiction de Tous les Appels Sortants (BAOC)	Auto	Avec l'interdiction des appels sortants active, les appels normaux échouent tandis que les appels d'urgence réussissent.
2.4	Renvoi d'Appel en Cas de Non-Réponse (CFNRY)	Auto	Le renvoi d'appel en cas de non-réponse peut être enregistré et interrogé, avec la configuration stockée confirmée.
2.5	SMS d'Origine / Terminé	Auto	Un SMS envoyé par l'abonné en roaming est livré et une réponse est reçue.
2.6	Test négatif CAMEL (SMS-MO, prépayé)	Manuel	Comportement des SMS prépayés lorsqu'il n'y a pas d'accord CAMEL actif.
2.7	Accès Intranet / FAI en utilisant la passerelle d'origine	Auto	Une session de données atteint Internet/intranet via la passerelle d'origine.
2.8	MMS utilisant la passerelle d'origine et MMSC	Manuel	Un message multimédia est livré via le MMSC d'origine.

Services Supplémentaires dans IR.48

Deux cas de services supplémentaires sont entièrement automatisés :

- **BAOC (2.3) : Interdiction de Tous les Appels Sortants.** OmniRoam active l'interdiction des appels sortants sur l'abonné test, confirme qu'un appel sortant normal est rejeté par le réseau, confirme qu'un appel d'urgence se connecte toujours (l'exception requise), puis retire l'interdiction pour laisser la SIM propre.
- **CFNRY (2.4) : Renvoi d'Appel en Cas de Non-Réponse.** OmniRoam enregistre le renvoi d'appel en cas de non-réponse vers un numéro cible avec un minuteur de sonnerie, puis interroge le service (l'équivalent de composer le code d'état `*#61#`) et confirme que le réseau a stocké le numéro et le minuteur vers lesquels le renvoi a été enregistré. Observer le renvoi en direct nécessite un appel entrant d'un tiers, donc ce dernier segment est laissé pour une vérification manuelle ; le provisionnement et l'interrogation sont automatisés.

OmniRoam rapporte l'état de chaque service supplémentaire en utilisant les quatre indicateurs standard 3GPP : **Provisionné**, **Enregistré**, **Actif**, et **Quiescent** (voir [3GPP TS 23.011](#)).

VoLTE : Test de Roaming VoLTE

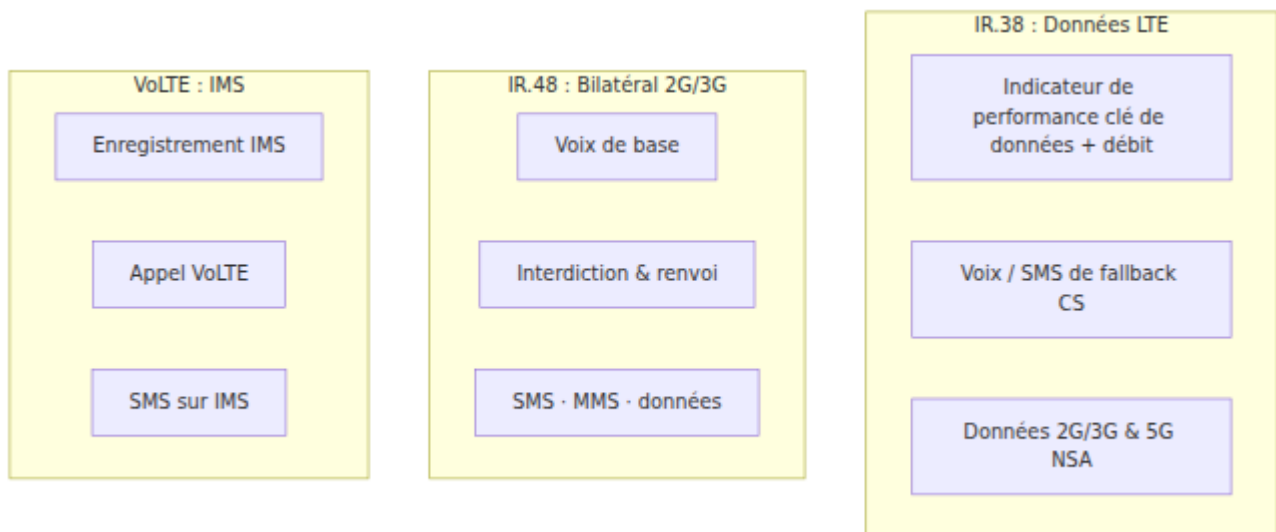
Basé sur **GSMA BA.65 §5.3**, avec un comportement VoLTE selon **GSMA IR.92**.
Prouve que l'abonné peut s'enregistrer à IMS tout en étant en roaming et passer/recevoir des appels VoLTE et des SMS sur IMS.

Cas	Titre	Piloté	Ce qu'il prouve
ims_reg	Enregistrement IMS en roaming	Auto	L'appareil s'enregistre à IMS en roaming (la condition préalable pour tous les services VoLTE).
mo_call	Appel VoLTE d'origine mobile	Auto	Un appel VoLTE d'origine de l'abonné s'établit et se maintient.
mt_call	Appel VoLTE terminé mobile	Manuel	Un appel à l'abonné via VoLTE s'établit.
sms_ims	SMS sur IMS (SMSoIP)	Auto	Les SMS sont livrés sur le réseau IMS.
emergency	Appel d'urgence VoLTE	Manuel	Les appels d'urgence fonctionnent via VoLTE (jamais composés automatiquement).

La Porte d'Enregistrement IMS

Les services VoLTE dépendent de l'enregistrement IMS. OmniRoam exécute `ims_reg` en premier comme une **porte** : si l'appareil n'est pas enregistré à IMS, les cas dépendants d'IMS (`mo_call`, `sms_ims`) sont signalés comme bloqués plutôt que échoués. Il n'y a aucune valeur à composer un appel VoLTE lorsque IMS est hors service, et un résultat bloqué indique à l'opérateur exactement pourquoi.

Comment les Livres se Comparsent



Livre	Domaine principal	Meilleur pour
IR.38	Données LTE / EPC	Valider une nouvelle relation de données de roaming LTE et le débit
IR.48	Circuit commuté 2G/3G + paquet	Valider la voix, les services supplémentaires, les SMS et les données de base
VoLTE	IMS	Valider le roaming VoLTE une fois l'interconnexion IMS en place

Gestion des SIM OTA : RFM/RAM par voie hertzienne

Le module **OTA** gère les SIM **par voie hertzienne** : il lit et édite des fichiers sur une carte distante. Il envoie des **paquets sécurisés** (ETSI TS 102 225 / 3GPP TS 31.115, "03.48" / SCP80) qui transportent des commandes de Gestion de Fichiers à Distance (RFM) et de Gestion d'Applications à Distance (RAM). La carte vérifie et déchiffre chaque paquet, exécute les commandes et renvoie une **preuve de réception (POR)** signée.

En pratique, cela vous donne le même niveau d'édition de fichiers qu'avec l'outil hors ligne **Explorateur de Système de Fichiers SIM** : parcourez l'arborescence des fichiers, décidez un EF, éditez les champs, réécrivez-le. La différence est que l'OTA atteint la carte **à distance** : via un lecteur PC/SC sur l'hôte central, un lecteur chez un **agent**, ou via **SMPP** vers une SIM sur le terrain.

Il repose sur le même magasin de clés par ICCID que le **Magasin de Clés SIM**. Un profil indique *quel ensemble de clés et quels algorithmes*, et le magasin de clés contient le **KIC/KID** réel pour cette carte. Le moteur ne journalise jamais ni ne renvoie les clés. Il renvoie uniquement le texte chiffré résultant et la POR.

Ce qu'est un paquet sécurisé

Un paquet sécurisé protège les APDUs de commande de bout en bout, indépendamment du porteur (clair). Le moteur a été validé contre des cartes ISIM physiques.

```
Command Packet = CPL | CHL | SPI | KIC | KID | TAR(3) | CIPHERED
CIPHERED       = 3DES-CBC( CNTR(5) | PCNTR(1) | CC(8) |
APDUs+padding ) IV=0
CC             = last8( 3DES-CBC( KID,
zeropad(CPL+hdr+CNTR+PCNTR+APDUs) ) )
```

- **TAR** (Référence d'Application Toolkit, 3 octets) dirige le paquet vers un service sur la carte : une application RFM spécifique ou le RAM (gestionnaire de carte).
- Les indicateurs **SPI** sélectionnent le chiffrement, le code de contrôle cryptographique (CC), la politique de compteur et ce que la POR doit contenir.

- **KIC / KID** indexent quel transport (chiffrement) et quel ensemble de clés d'authentification la carte utilise ; les **valeurs** proviennent du magasin de clés par ICCID.

Les APDUs à l'intérieur sont un script C-APDU ordinaire : `SELECT` + `READ BINARY` pour une lecture RFM, `SELECT` + `UPDATE BINARY` pour une écriture, `DELETE` / `INSTALL` GlobalPlatform pour RAM.

Sur le fil (un SMS-PP), le paquet circule dans le TP-User-Data avec un Identifiant de Paquet de Commande UDH (IEI `0x70`), PID `0x7F` (téléchargement de données SIM), DCS `0xF6` (8 bits, classe de message 2). En shell, il est livré comme un APDU CAT `ENVELOPE(SMS-PP-Download)` et la POR revient de manière synchrone.

Profils, contextes et routage automatique

Un **profil OTA** est un préréglage de sécurité réutilisable. Il ne contient **aucun matériel clé** :

Champ	Signification
tar	Référence d'Application Toolkit de 3 octets (le service cible).
kic_index / kid_index	Quel ensemble de clés (1/2/3) → KIC{n}/KID{n} de la ligne du magasin de clés de la carte.
cipher_algo / cc_algo	Algorithme de chiffrement et de contrôle (triple_des_cbc2, aes_cbc, ...).
ciphering, rc_cc_ds, counter_mode	SPI : chiffrer ? CC vs RC vs aucun ? politique de compteur de répétition.
por, por_ciphred, por_rc_cc_ds	POR requise ? chiffrée ? signée ?

Deux profils sont préconfigurés, correspondant aux valeurs validées sur sysmoSIM :

- **RFM-USIM-3DES-keyset3** : TAR B00011, ensemble de clés 3, 3DES, chiffrement + CC, POR requise + chiffrée + CC. Fonctionne à l'intérieur de **ADF.USIM**.
- **RFM-SIM-3DES-keyset2** : TAR B00010, ensemble de clés 2. Fonctionne sur l'arborescence 2G **racine MF** (DF.GSM / DF.TELECOM).

Différentes applications nécessitent différents services, donc l'explorateur **route le profil et le contexte SELECT automatiquement par fichier**, à partir de l'application du fichier :

Application de fichier	Contexte	Profil (par TAR)	Pré-SELECT avant l'ENVELOPPE
ADF.USIM	usim	TAR B00011	SELECT ADF.USIM (par AID)
DF.GSM, DF.TELECOM	sim	TAR B00010	aucun (racine MF)
ADF.ISIM	isim	TAR B00013	SELECT ADF.ISIM (par AID)

Chaque contexte est associé à l'un de vos profils (défini par correspondance TAR, modifiable dans l'explorateur). Choisissez une carte et cliquez sur n'importe quel fichier (USIM, GSM ou TELECOM). OmniWeb applique le bon profil, ensemble de clés et SELECT sans changer quoi que ce soit. ISIM fonctionne dès que vous créez un profil pour cela (son TAR varie selon la carte).

Transports

Un transport livre le paquet sécurisé et, là où le porteur le permet, collecte la POR. Les adaptateurs pluggables partagent une interface :

Type	Atteint	POR	Remarques
<code>local_pcsc</code>	une carte dans un lecteur PC/SC sur l'hôte central	synchrone	le chemin de validation directement connecté.
<code>agent_reader</code>	une carte dans un lecteur chez un agent distant	synchrone	circule sur le même WebSocket d'agent que Appareils de Test / Banque SIM (relais <code>session_apdu</code>).
<code>smpp</code>	une SIM de terrain via SMPP <code>submit_sm</code>	asynchrone	SMS MT vers un SMSC ; la POR revient plus tard sous forme de SMS MO.

L'**Explorateur** utilise uniquement les transports en shell (il a besoin d'une POR synchrone) ; **Campagnes** peuvent utiliser n'importe quel transport, y compris SMPP.

Explorateur

`src/pages/ota/0taExplorer.tsx` : l'éditeur de fichiers SIM distant.

1. Choisissez un **ICCID cible** (du Magasin de Clés SIM) et un **transport**.
2. Parcourez le **catalogue de fichiers** : chaque EF connu du modèle de fichier hors ligne (ADF.USIM, ADF.ISIM, DF.GSM, DF.TELECOM), regroupé par application et recherché par code / nom / description.
3. Sélectionnez un fichier → **Lire par OTA**. La lecture sécurisée RFM est livrée, la POR décodée, et l'EF rendu : statut de la POR, dernier SW, hexadécimal brut + ASCII, et un **formulaire de champ typé** (décodé en champs nommés).

4. Éditez les **champs** (ré-encodés automatiquement) ou l'**hexadécimal brut**, puis **Écrire par OTA**. La commande RFM sécurisée `UPDATE` est envoyée et le fichier est **lu à nouveau** automatiquement afin que vous puissiez voir l'état sur la carte après l'écriture.

Les lectures/écritures sont régulées par la permission de contrôle `ota` ; tout est enregistré comme un **travail**.

Campagnes

`src/pages/ota/OtaCampaigns.tsx` : une opération sauvegardée répartie sur un ensemble de SIMs : **requête cible** → **opération** → **profil** → **transport**.

- **Requête cible** est évaluée par rapport à l'inventaire de la **Banque SIM** au moment de l'exécution : liste ICCID / préfixe, préfixe ou plage IMSI, agent, banque. Une requête vide correspond délibérément à rien (pas de fan-out accidentel).
- **Opération** est la commande RFM/RAM (lecture/mise à jour binaire ou enregistrement, GP supprimer / obtenir le statut / installer).

- **Exécuter** crée un **travail** par carte correspondante. Les campagnes SMPP sont de type feu-et-oublie (la POR arrive plus tard sous forme de SMS MO).

Une exécution est limitée (`CAMPAIGN_MAX_TARGETS`) afin qu'une requête mal formulée ne puisse pas affecter des milliers de cartes en une seule demande.

Travaux

`src/pages/ota/0taJobs.tsx` : chaque livraison OTA (lectures/écritures de l'explorateur et exécutions de campagnes) avec son statut et sa POR. Le tiroir de détails montre le **paquet de demande sécurisé** (texte chiffré), la **preuve de réception**, et le résultat décodé (commandes exécutées, dernier SW, données de réponse). Les secrets de carte ne sont **jamais** stockés sur un travail : seul le texte chiffré et la POR.

API REST (/api/ota, JWT, type

d'élément RBAC ota)

Méthode	Route	But
GET	/profiles · POST · /profiles/<id> PUT/DELETE	Profils de sécurité OTA.
GET	/campaigns · POST · /campaigns/<id> GET/PUT/DELETE	Campagnes.
GET	/campaigns/<id>/targets	Prévisualiser quelles SIMs la requête correspond actuellement.
POST	/campaigns/<id>/run	Exécuter : un travail par carte correspondante.
GET	/jobs, /jobs/<id>	Historique des travaux (filtrer par campaign_id / iccid).
GET	/files/catalog	Le catalogue EF navigable (modèle de fichier hors ligne).
POST	/explore/read	Lire un EF par OTA ; renvoie le travail + EF décodé.
POST	/execute	Exécuter une opération (mise à jour RFM, RAM, brut) contre une carte.

Méthode	Route	But
POST	/preview	Construire le paquet sécurisé sans envoyer (inspecter le texte chiffré + les encadrements SMS).
POST	/decode · /encode	Décoder les octets EF ↔ champs typés (hors ligne).

RBAC reflète `simbank/ir38` : les administrateurs passent toujours ; sinon, une permission JWT avec `element_type == "ota"` accorde la vue, et `POST` dans ses méthodes accorde le contrôle. Les lectures sont considérées comme un contrôle (elles transmettent un paquet à la carte). Les routes sont auto-documentées dans la [Référence API](#).

Schéma de base de données

Table	Ligne	Colonnes clés
ota_profiles	un préréglage de sécurité	name, tar, kic_index/kid_index, algorithmes, indicateurs SPI.
ota_campaigns	un fan-out sauvegardé	name, profile_id, target_query (JSON), operation (JSON), transport (JSON), status.
ota_jobs	une livraison à une carte	iccid, operation, request_hex (texte chiffré), response_hex (POR), por_status, result (JSON), status.

Les clés vivent dans la table existante `simbank_keys` (le [Magasin de Clés SIM](#)), référencées par ICCID par l'index de l'ensemble de clés du profil. Elles ne sont **pas** dupliquées ici.

Comment ça fonctionne

Le moteur OTA gère le cryptage, la structure des paquets sécurisés, les TLV CAT/SMS et le modèle de fichier hors ligne nécessaires pour construire et décoder les paquets RFM/RAM 03.48/SCP80. Il fonctionne dans le service backend de rôle agent et partage la connexion de l'agent pour le transport en shell. La livraison est pluggable à travers les transports local-reader, remote-agent-reader et SMPP.

Notes de sécurité

- Les secrets de carte (KIC/KID) sont lus à partir du magasin de clés pour construire des paquets mais ne sont **jamais** écrits dans le journal d'audit ou renvoyés dans une réponse. Seule la demande chiffrée et la POR sont stockées.
- Écrire un fichier est destructeur ; l'explorateur confirme avant chaque écriture et lit à nouveau le résultat.
- Le paquet sécurisé est un véritable 03.48 : altérez un octet et la carte le rejette (le CC échoue) ; avec le chiffrement activé, les APDUs en clair n'apparaissent jamais sur le fil.
- SCP80 seulement : ce n'est **pas** SCP81 (pas de PSK-TLS / HTTPS Admin Agent).

PGW-C : Passerelle PDN (Plan de Contrôle)

Le **PGW-C** est la moitié du plan de contrôle de la **Passerelle PDN** EPC. C'est le point d'ancrage pour chaque session de données d'abonné : il termine **S5/S8** vers le SGW-C, établit et maintient chaque **connexion PDN**, attribue à l'UE son adresse IP à partir d'un **pool IP** de l'opérateur, et sélectionne et contrôle le plan utilisateur (**UPF**) via **Sx/PFCP**. Il gère également la politique et la facturation de la session via Diameter : **Gx** vers le PCF/PCRF pour la politique et la QoS, et **Gy** vers l'OCS pour la facturation en ligne. Il génère également des **CDRs** pour la facturation hors ligne. Dans le cœur 5G, la fonction équivalente est le **SMF**. OmniWeb présente les sessions actives du PGW-C, les pools IP, les UPF et les pairs Diameter, une carte topologique et l'historique des sessions, ainsi que des outils de diagnostic. Les tableaux de bord Grafana accessibles depuis la même page affichent les tendances à long terme.

[← Guide des opérations](#)

Le PGW-C est une page d'élément par instance accessible depuis la barre latérale lorsque l'on navigue dans l'inventaire du site, avec une vue de flotte où plusieurs sont déployés. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du PGW-C, de sorte qu'il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : le **statut de l'API** du PGW-C et un résumé de son état en direct (nombre de sessions actives, utilisation du pool IP, pairs UPF et pairs Diameter). C'est le moyen le plus rapide de confirmer que le nœud est opérationnel et gère des sessions.

Sessions

Chaque session PGW active, chaque ligne identifiée par **IMSI** et **MSISDN** de l'abonné avec son **IP UE** et son **APN** attribués. Les sessions peuvent être recherchées par IMSI, IP UE, MSISDN ou APN. L'ouverture d'une session montre son état complet : la connexion PDN et les porteurs, le SGW de service et l'UPF sélectionné, ainsi que le contexte de politique et de facturation Gx/Gy en direct. Vous pouvez modifier une session ici. Un opérateur peut ajuster l'état en direct tel que le **AMBR** de la session (qui pousse un nouveau APN-AMBR vers l'UPF) et les **déclencheurs d'événements Gx** demandés qui contrôlent le rapport de changement de localisation. Un opérateur peut également **supprimer** une session pour libérer de force un abonné bloqué ou malveillant. Comme l'opérateur applique les modifications directement à l'état en direct, elles prennent effet immédiatement.

Pools IP

Les pools IP de l'opérateur à partir desquels le PGW-C attribue des adresses UE, chacun montrant sa **taille**, son nombre **alloué** et son **utilisation**. L'ouverture d'un pool liste les adresses individuelles allouées. Ici, vous confirmez qu'un pool n'est pas épuisé (un pool épuisé est une cause courante d'échecs d'établissement de session) et voyez quel abonné détient une adresse donnée.

Pairs UPF

Les pairs du plan utilisateur (UPF) que le PGW-C contrôle via **Sx/PFCP**, chacun montrant son **adresse IP** et son **état d'association** PFCP. L'ouverture d'un pair montre ses détails. C'est ici que vous confirmez que les associations PFCP qui transportent le plan utilisateur de chaque session sont opérationnelles.

Diameter

Les pairs Diameter avec lesquels le PGW-C communique (le **PCF/PCRF** via **Gx** pour la politique et l'**OCS** via **Gy** pour la facturation en ligne), chacun avec son **nom d'hôte** et son **état de connexion**. L'ouverture d'un pair montre ses détails. Lorsque des sessions sont rejetées ou limitées, c'est ici que vous confirmez que les chemins de politique et de facturation sont opérationnels.

Historique

Un journal consultable et paginé des **événements** du cycle de vie de la session : *créé, modifié, supprimé, transfert* et *échoué*. Vous pouvez filtrer les événements par type et les rechercher par IMSI, MSISDN, adresse IP ou TEID. Ici, vous reconstruisez ce qui est arrivé à la session d'un abonné spécifique au fil du temps, y compris les échecs.

Topologie

Une carte du PGW-C et des voisins avec lesquels il travaille : les SGW pour lesquels il ancre des sessions, les UPF qu'il contrôle, et ses pairs Diameter. Cela donne une vue d'ensemble des voisins de signalisation et de plan utilisateur auxquels le nœud est connecté.

Sélection UPF

Les règles qui décident sur quel UPF une nouvelle session est placée, ainsi que l'état de **santé** actuel de chaque UPF candidat et la configuration **PCO** (Options de Configuration de Protocole) que le PGW-C retourne à l'UE. C'est ici que vous confirmez pourquoi les sessions se posent sur un UPF particulier et vérifiez que tous les candidats sont en bonne santé.

Recherche UE

Une recherche directe d'un seul abonné par **IMSI**, **MSISDN** ou **adresse IP**, retournant les informations de cet UE sur le PGW-C. C'est le moyen le plus rapide de trouver la session d'un abonné sans faire défiler la liste complète des Sessions.

Facturation

L'état de **facturation en ligne (Gy/OCS)** en direct de chaque session active, chaque ligne identifiée par **IMSI** et **MSISDN** et recherchable par l'un ou l'autre. D'un coup d'œil, chaque session montre si la facturation en ligne **Gy** est activée (avec son **id de session**, et l'**hôte OCS** et le **domaine** avec lesquels il communique), si la comptabilité **hors ligne (Gz)** fonctionne également, et si l'OCS a poussé l'abonné dans une redirection de **jardin clos**. L'ouverture d'une session développe ses détails de facturation complets : les quotas **accordés** par URR par rapport au volume **utilisé** (octets montants, descendants et totaux), l'**action finale** que l'OCS a définie pour lorsque le crédit s'épuise, les compteurs hors ligne (Gz), et toute cible de redirection. C'est ainsi que vous lisez l'état de contrôle de crédit en direct d'un abonné : s'il a du crédit, combien de son allocation il a consommée, et pourquoi il a pu être limité ou redirigé.

CDRs

Les **enregistrements de facturation** hors ligne que le PGW-C écrit pour la facturation : une ligne par événement de **début**, **intermédiaire** et **arrêt** de session, le plus récent en premier, et filtrable par **IMSI** ou **MSISDN**. Chaque enregistrement contient l'**IMSI**, **MSISDN** et **IMEI** de l'abonné, l'**APN** et le **QCI**, l'**id de facturation** qui relie les enregistrements d'une session, les **octets montants/descentes** comptés pour cet intervalle, les adresses IP de **S-GW**, **PGW** et **UE**, et le **fichier source** à partir duquel l'enregistrement a été lu. Ici, vous réconciliez l'utilisation des données d'un abonné avec la comptabilité hors ligne (Gz) sur laquelle l'opérateur facture, et tracez dans quel fichier d'enregistrement une session donnée a atterri.

Test Gy

Un outil pour l'opérateur qui émet une **demande de contrôle de crédit Gy** contre l'OCS pour valider le chemin de facturation en ligne de bout en bout. Vous fournissez un **IMSI** (et éventuellement un MSISDN et un nombre d'octets demandés/utilisés) et choisissez le type de demande. Utilisez **Initial (CCR-I)** pour ouvrir une session et demander des unités, **Update (CCR-U)** pour signaler l'utilisation et demander plus, ou **Terminate (CCR-T)** pour signaler l'utilisation finale et la fermer. Ensuite, envoyez-la. Le PGW-C par défaut le groupe de tarification, l'Id de Service-Context et l'Id d'Application d'Auth. La réponse de **contrôle de crédit** analysée revient sur le même écran. Contrairement aux autres onglets, celui-ci **ne récupère rien au chargement** : c'est un formulaire que vous soumettez. Lorsque la facturation en ligne ne fonctionne pas correctement, c'est le moyen le plus rapide de prouver que l'OCS est accessible et accorde du crédit.

Moniteur P-CSCF

L'état et les métriques du moniteur de découverte P-CSCF. Le PGW-C retourne une adresse P-CSCF aux dispositifs VoLTE lors de la configuration de la PDN, et cet onglet confirme que la découverte est saine afin que l'enregistrement IMS puisse se poursuivre.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du PGW-C pour dépanner un seul nœud (échecs d'établissement de session, erreurs PFCP et Diameter) sans quitter OmniWeb.

Surveillance

Les tendances du nombre de sessions, le débit et d'autres séries chronologiques pour le PGW-C sont présentées sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liés

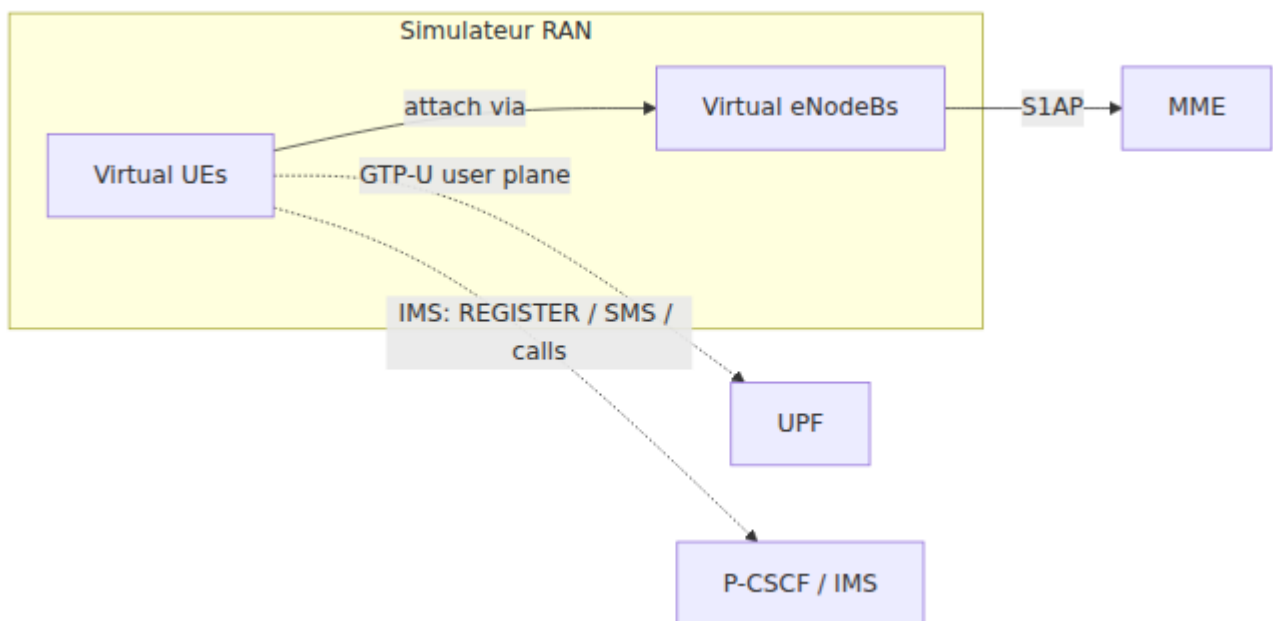
- Le **SGW-C** est le pair de contrôle via **S5/S8** ; il ancre les porteurs côté accès auxquels le PGW-C se connecte à la PDN.
- Le **UPF** est le plan utilisateur que le PGW-C sélectionne et contrôle via **Sx/PFCP**.
- Le **PCF/PCRF** fournit la politique et la QoS via **Gx**.
- Le **CHF/OCS** effectue la facturation en ligne via **Gy** ; le PGW-C génère également des CDR pour la facturation hors ligne.

Simulateur RAN

Le **Simulateur RAN** vous permet d'exercer un réseau de cœur en direct sans radios ou terminaux physiques. Il met en place des **eNodeBs** et des **UEs** virtuels qui communiquent en S1AP/NAS avec le MME et en GTP-U avec les passerelles, afin que vous puissiez gérer les attachements, les sessions de données, les enregistrements IMS, les SMS et les appels. Utilisez-le pour des tests fonctionnels, des tests de charge ou pour reproduire des scénarios de terrain, le tout depuis OmniWeb.

[← Guide des opérations](#)

Ce que c'est



Le simulateur fonctionne aux côtés du cœur qu'il cible. Dans OmniWeb, il apparaît comme sa propre zone **Simulateur RAN** (Carte du réseau, eNodeBs, UEs, IMS, Test de charge, Horaires de scénarios). Comme un UE simulé se comporte comme un appareil, ses UEs apparaissent également dans **Appareils de test** afin que vous puissiez les gérer depuis le même endroit que de vrais terminaux.

Par défaut, il commence avec **aucun eNodeB**. Vous configurez exactement la topologie que vous souhaitez.

eNodeBs

La mise en service d'un eNodeB l'attache au MME (Configuration S1). Un eNB peut être connecté à **plus d'un MME** (un pool de MME). La Carte du réseau montre l'ensemble des MMEs auxquels un eNB est associé.

La mise en service est **fire-and-forget** : OmniWeb demande au simulateur de mettre en service l'eNB et revient ; le lien S1 s'établit en arrière-plan (surveillez la Carte du réseau / liste des eNodeBs pour confirmer qu'il est en service).

Déconnexion d'un eNodeB

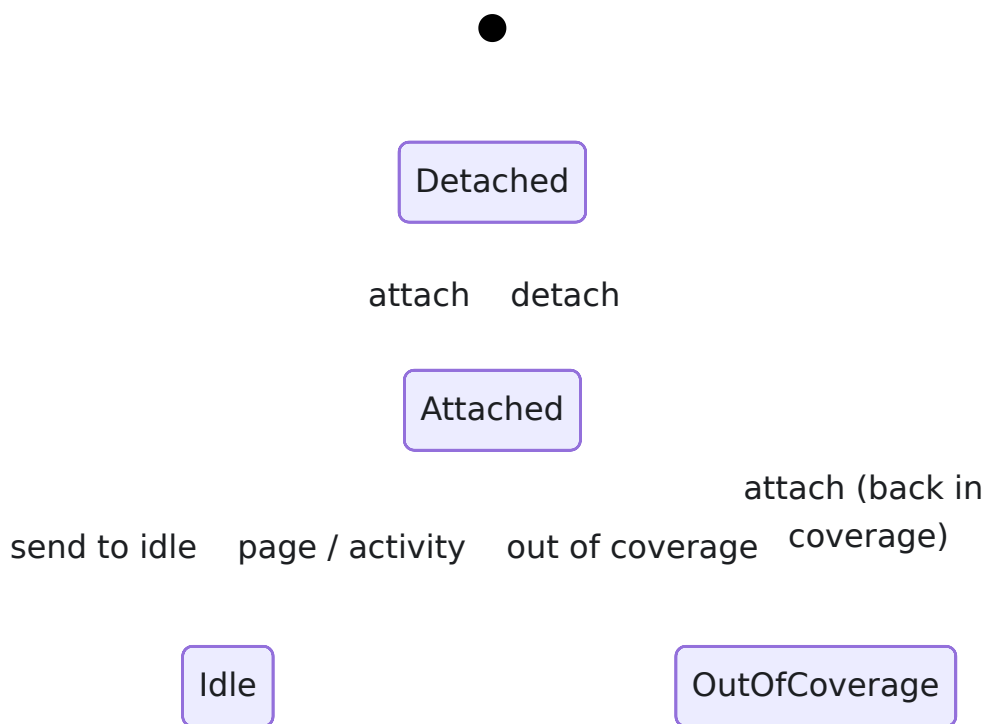
Vous pouvez retirer un eNB de deux manières, qui modélisent différents événements du monde réel :

Action	Modèles	Effet sur les UEs
Déconnexion S1 propre	Un arrêt ordonné de l'eNB / réinitialisation S1	Les UEs sont libérés proprement et survivent . Ils se réattachent lorsqu'un lien est disponible
Perte de lien	L'eNB perd brusquement son S1 (coupure de fibre, perte de courant)	L'association S1 est interrompue ; les UEs survivent à la disparition de l'eNB et se réattachent plutôt que d'être supprimés

Critiquement, retirer un eNB ne détruit **pas** ses UEs. Les UEs persistent et se réattachent, vous permettant de simuler des pannes de transport sans reconstruire votre flotte d'abonnés.

UEs

Chaque UE simulé a un cycle de vie que vous pouvez gérer directement :

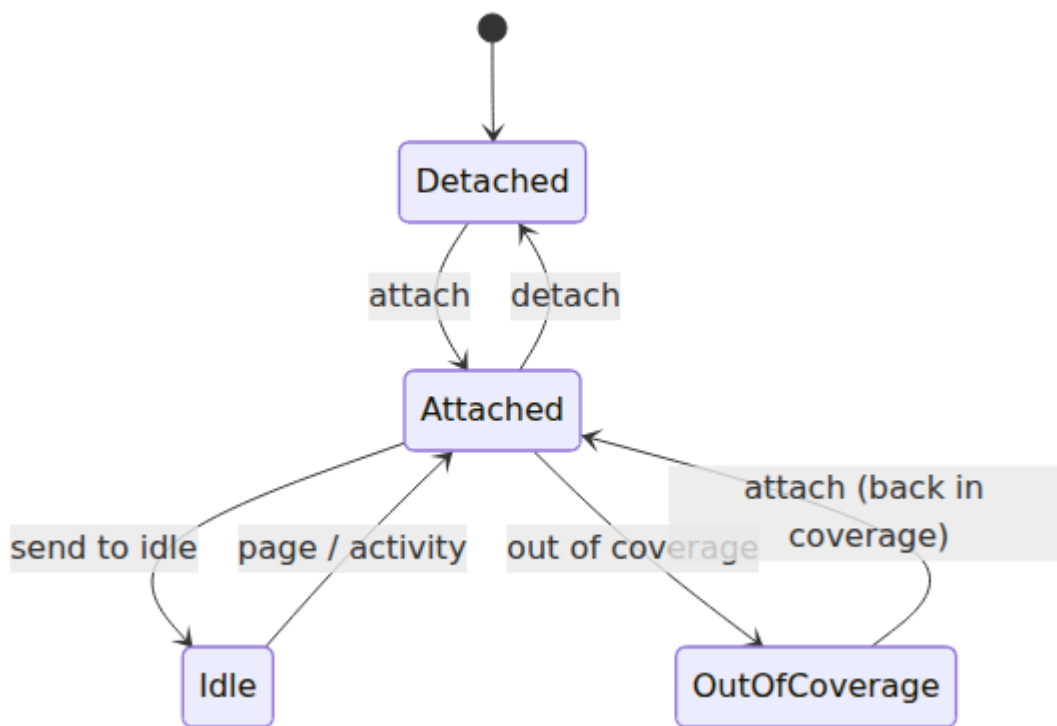


- **Attacher / Détacher** : rejoindre ou quitter le réseau.
- **Envoyer à l'inactivité** : passer à ECM-IDLE (comme un vrai UE le fait entre les activités). La recherche ou une nouvelle activité le ramène.
- **Hors de couverture** : une perte de radio *non propre* (l'UE se déconnecte sans signalement), pour tester comment le cœur gère un UE qui disparaît simplement. Se réattacher le ramène dans la couverture.

Pour chaque UE, le simulateur montre le **MME de service** auquel il est attaché : l'ID de groupe MME et le code MME (décodé à partir du GUTI de l'UE). Ainsi, dans un déploiement en pool, vous pouvez voir quel MME a pris chaque abonné.

Enregistrement IMS & localisation

Un UE simulé peut s'enregistrer auprès de l'IMS et passer des SMS/appels. Lorsqu'il s'enregistre, il inclut sa **localisation cellulaire** (**P-Access-Network-Info** avec le **utran-cell-id-3gpp** pour sa cellule de service), exactement comme un vrai UE. Ainsi, le REGISTER tiers du S-CSCF propage cette localisation au SMSc, TAS et autres serveurs d'applications. Cela vous permet de tester le comportement IMS dépendant de la localisation de bout en bout sans vraies radios.



Gestion des UEs depuis les appareils

Comme un UE simulé est juste un autre appareil, il apparaît dans **Appareils de test** étiqueté comme un simulateur, et peut être filtré là. Vous utilisez le **même panneau de contrôle UE** que vous ouvriez un UE depuis la Carte du réseau du Simulateur RAN ou depuis la flotte d'appareils. C'est un seul endroit pour attacher/détacher, inactif, gérer hors couverture, s'enregistrer auprès de l'IMS, envoyer un SMS ou passer un appel, et consulter le journal d'action.

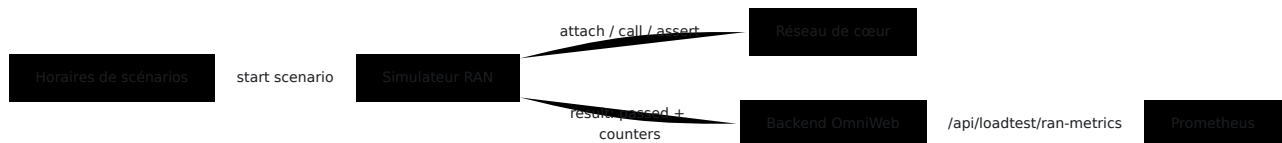
Filtrez les appareils de test pour les UEs du Simulateur RAN afin de gérer les abonnés émulés aux côtés de vrais terminaux.

Scénarios programmés

Un **scénario** est une recette de test enregistrée : une séquence nommée d'actions UE (attacher, inactif, réveil, enregistrement IMS, appel, SMS, transfert, détachement) que le simulateur joue contre le cœur. Le simulateur expédie une bibliothèque de préréglages, regroupés par catégorie (par exemple cycle de vie d'attachement, VoLTE et cas de rejet négatif). Exécutez un scénario une fois

depuis la vue Test de charge, ou exécutez-le selon un calendrier répétitif pour surveiller le cœur en continu.

La page **Horaires de scénarios** (barre latérale : Test de charge → Horaires de scénarios) gère les exécutions répétées. Pour chaque horaire, vous choisissez un scénario et la fréquence de son exécution. OmniWeb enregistre le résultat de réussite ou d'échec de chaque exécution et l'exporte vers Prometheus, afin que vous puissiez alerter à ce sujet et le tracer.



Les exécutions sont **sérialisées**. OmniWeb exécute un scénario programmé à la fois, car un scénario peut démarrer de nombreux UEs et met une réelle charge sur le cœur. Si une exécution est encore active lorsque le prochain horaire est dû, OmniWeb attend et la démarre lors du prochain cycle libre. Utilisez le bouton **Exécuter maintenant** sur un horaire enregistré pour le démarrer immédiatement.

Paramètres de l'horaire

Champ	Type	Requis	Par défaut	Description
Nom	Chaîne	Oui	-	Étiquette unique pour l'horaire. Également l'étiquette <code>schedule</code> sur la métrique exportée.
Scénario	Chaîne	Oui	-	Le scénario prédéfini à exécuter. Le sélecteur regroupe les scénarios par catégorie.
Chaque (s)	Entier	Non	3600	À quelle fréquence exécuter le scénario, en secondes. Minimum 60.
Compte UE	Entier	Non	100	Nombre d'abonnés que le scénario exécute.
RPS	Nombre	Non	10	Nombre cible de nouveaux scénarios par seconde.
Concurrence	Entier	Non	50	Nombre maximum de scénarios en vol à la fois.
APNs	Liste	Non	défaut du scénario	APNs à attacher, sous forme de liste séparée par des virgules. Remplace le défaut du scénario.

Réussite et échec

Une exécution programmée **réussit** lorsque le simulateur signale que toutes les assertions ont réussi et qu'aucun scénario d'abonné n'a été interrompu. Une exécution **échoue** si une assertion échoue ou si un scénario est interrompu. Un scénario sans assertions réussit tant qu'aucun scénario n'est interrompu. Si OmniWeb ne peut pas démarrer l'exécution, ou si l'exécution ne se termine pas à temps, OmniWeb enregistre l'exécution comme une **erreur**.

La page affiche un tableau **Exécutions récentes** avec le résultat, le nombre d'assertions, le nombre de scénarios interrompus et la durée de chaque exécution.

Métriques

OmniWeb expose le dernier résultat de chaque horaire au format Prometheus à `/api/loadtest/ran-metrics`. Prometheus le scrute en tant que tâche `ransim_scenarios`, que le rôle de surveillance configure automatiquement.

Métrique : `ransim_scenario_pass` **Type :** Jauge **Description :** Résultat de la dernière exécution programmée : `1` pour réussite, `0` pour non réussi

Étiquettes :

- `schedule` : le nom de l'horaire
- `scenario` : l'ID du scénario qui a été exécuté
- `category` : la catégorie du scénario
- `status` : le résultat de l'exécution (`passed`, `failed`, ou `error`)

Les jauges complémentaires partagent les mêmes étiquettes :

Métrique	Description
<code>ransim_scenario_duration_ms</code>	Durée de la dernière exécution, en millisecondes
<code>ransim_scenario_assertions_passed</code>	Assertions réussies lors de la dernière exécution
<code>ransim_scenario_assertions_failed</code>	Assertions échouées lors de la dernière exécution
<code>ransim_scenario_scenarios_aborted</code>	Scénarios d'abonnés interrompus lors de la dernière exécution
<code>ransim_scenario_last_run_timestamp</code>	Heure Unix de la dernière exécution

Exemples de requêtes :

```
# Scénarios dont la dernière exécution n'a pas réussi
ransim_scenario_pass == 0

# Total des échecs d'assertions à travers tous les scénarios
programmés
sum(ransim_scenario_assertions_failed)

# Un horaire qui n'a pas été exécuté au cours des deux dernières
heures
time() - ransim_scenario_last_run_timestamp > 7200
```

Tableau de bord Grafana

Le rôle de surveillance expédie un tableau de bord **Scénarios du Simulateur RAN** (dossier Grafana **RAN**). Il lit les métriques ci-dessus et affiche une chronologie de réussite ou d'échec, le dernier résultat pour chaque horaire, les échecs d'assertions, la fraîcheur des scénarios et la durée d'exécution. Filtrez par catégorie, scénario ou horaire en haut. Voir [Grafana](#).

Utilisations typiques

- **Tests fonctionnels** : mettre en service un eNB et un UE, attacher, établir une session de données, s'enregistrer auprès de l'IMS, envoyer un SMS, puis confirmer le bon fonctionnement de chaque élément du cœur.
- **Tests de charge** : mettre en service de nombreux UEs pour générer une charge d'attachement/session/IMS contre le cœur (voir la vue Test de charge).
- **Reproduction de scénarios** : modéliser des pannes (perte de lien, hors de couverture) et le comportement des MME en pool pour reproduire et diagnostiquer des problèmes de terrain.
- **Surveillance continue** : programmer un scénario pour s'exécuter sur un minuteur et alerter sur la métrique de réussite ou d'échec (voir [Scénarios programmés](#)).

Liés

- [Appareils de test](#) : vrais terminaux et UEs simulés, gérés depuis un seul endroit.
- [Trace de session](#) : corréler le signalement généré par le simulateur.

SIM à distance & SIM virtuelle

OmniWeb peut présenter **n'importe quelle SIM à n'importe quel modem via le réseau**. Il peut également présenter une SIM qui **n'existe pas physiquement** : OmniWeb l'émule à partir d'une image de carte sauvegardée ainsi que des clés de l'abonné détenues dans le HSS. Cela transforme un rack de lecteurs SIM, d'émulateurs de cartes ("cardems") et de modems à un ou plusieurs sites en un pool partagé. Tout testeur peut utiliser n'importe quel profil d'abonné contre n'importe quel modem sans avoir à se déplacer pour transporter une SIM en plastique vers un emplacement de carte.

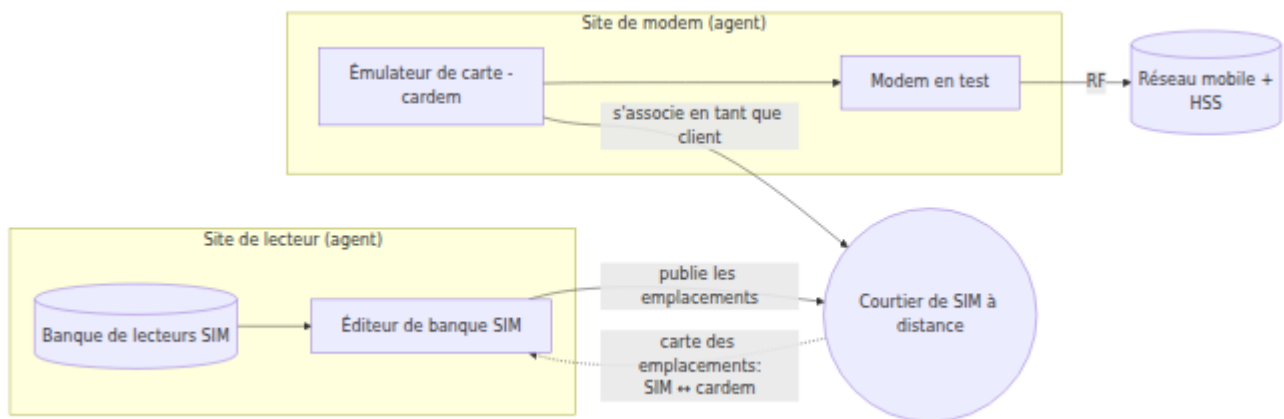
Cette page est le guide opérationnel pour cette capacité. La moitié **inventaire** découvre quelles SIMs se trouvent dans quels lecteurs. [SIM Bank](#) couvre cette moitié. Cette page couvre comment **présenter** une SIM (réelle ou virtuelle) à un modem et l'utiliser dans un test. [Images SIM \(Packages de Profil SAIP\)](#) couvre comment sauvegarder le système de fichiers d'une carte en tant que package de profil portable et comment en utiliser un pour soutenir une SIM virtuelle.

Table des Matières

- [Aperçu de l'Architecture](#)
- [Concepts](#)
- [La Banque SIM : où est quoi](#)
- [SIM à distance : connecter une SIM à un cardem](#)
- [La Console Cardem](#)
- [SIM Virtuelle : un abonné sans carte physique](#)
- [Utiliser une SIM dans un Livre de Test de Roaming](#)
- [Dépannage](#)

Aperçu de l'Architecture

Une banque de lecteurs SIM, un ou plusieurs émulateurs de cartes, et les modems en test se connectent à OmniWeb via ses agents de périphériques. Un courtier central associe un emplacement de SIM choisi à un cardem choisi ; le cardem présente ensuite cette SIM au modem qui y est connecté.



Pour une SIM **virtuelle**, une carte logicielle remplace la banque de lecteurs. OmniWeb construit cette carte logicielle à partir d'une image SIM sauvegardée et des clés de l'abonné. Tout le reste est identique :



Concepts

Terme	Signification
Banque SIM	Un ensemble de lecteurs de cartes à puce sur un agent, publiés afin que leurs SIMs puissent être présentées ailleurs. Chaque lecteur peuplé est un emplacement .
cardem	Une carte émulateur (USB) qui fait semblant d'être une SIM pour un modem qui y est connecté. Elle rejoue n'importe quelle carte à laquelle elle est mappée.
Carte des emplacements	Le lien "présenter cette SIM à ce cardem". La création de celui-ci connecte les deux à travers le réseau ; le retirer les déconnecte.
Modem en test	Le modem derrière un cardem. Il se connecte au réseau en direct en utilisant la SIM que le cardem présente.
SIM Virtuelle	Une carte logicielle construite à partir d'une image SIM sauvegardée plus les clés d'un abonné. OmniWeb la présente à un cardem exactement comme une SIM réelle. Aucune carte physique n'est requise.

La Banque SIM : où est quoi

La page **Banque SIM** liste chaque emplacement de lecteur sur chaque agent connecté, regroupé par agent. La disposition de la banque est la vérité : les emplacements vides, illisibles et en cours d'utilisation s'affichent tous, pas seulement ceux peuplés.

Chaque ligne est un lecteur physique. La puce d'état montre si une carte est présente et lisible. La ligne montre ensuite l'identité de la SIM (ICCID, IMSI, MCC/MNC, pays, nom de l'opérateur). Les lecteurs détenus par une session d'émulation active apparaissent comme **En utilisation**. Les SIMs persistées dont le lecteur est actuellement hors ligne apparaissent sous **Déjà vues**. Elles réapparaissent lorsque l'agent se reconnecte avec la SIM insérée.

Puce d'état	Signification
SIM	Une carte est présente et son identité a été lue.
Carte présente	Une carte est physiquement insérée mais son identité n'a pas pu être lue (par exemple, un appairage lecteur/carte incompatible).
En utilisation	Le lecteur est détenu par une session de SIM à distance/émulation en ce moment.
Vide	Pas de carte dans l'emplacement.

Les actions par ligne ouvrent l'explorateur de **Système de fichiers SIM** ou le **Terminal APDU** pour cet emplacement exact, et **Rescan** relit les lecteurs d'un agent à la demande.

SIM à distance : connecter une SIM à un cardem

La page **SIM à distance** est l'endroit où vous associez une SIM à un cardem. Les liaisons fonctionnent **à travers les agents et les sites** : la SIM peut être dans un lecteur à un emplacement et le cardem/modem à un autre.

Étapes

1. **Démarrer la banque SIM** sur l'agent qui détient les lecteurs (**Démarrer bankd**). Cela publie ses emplacements de lecteurs.
2. **Démarrer le client cardem** pour l'émulateur de carte que vous souhaitez utiliser (**Démarrer client**). Cela lie le cardem afin qu'une SIM puisse y être mappée.
3. Sous **Connecter une SIM**, choisissez un emplacement publié et choisissez un cardem auquel le lier. Le mappage est créé et apparaît sous **Mappages actifs** comme **ACTIF**.
4. Le cardem présente maintenant cette SIM à son modem. Réinitialisez le modem (voir [la console cardem](#)) pour qu'il lise la SIM nouvellement présentée et s'attache.

Réinitialisation Globale détruit tous les mappages et renvoie chaque cardem à un état inactif. Utilisez-le pour récupérer d'un banc d'essai confus.

Champ (Mappages actifs)	Signification
État	ACTIF une fois que le cardem présente la SIM.
SIM (banque/emplacement)	Dans quelle banque et emplacement de quel agent la carte vit.
ICCID	La SIM présentée.
Cardem (client/emplacement)	Quel cardem (et quel agent) la présente.
Par	L'opérateur qui a créé le mappage.

La Console Cardem

Dans **Appareils**, OmniWeb montre un émulateur de carte comme son propre type de périphérique (**ngff-cardem**), à côté des modems et des téléphones. Il n'est jamais ouvert comme un téléphone. OmniWeb étiquette les types de périphériques inconnus simplement plutôt que de les deviner.

Ouvrez le cardem pour obtenir une console dédiée pour l'émulateur et son modem.

Contrôle	Ce qu'il fait
Démarrer client	Lie le cardem en tant que client de SIM à distance afin qu'une SIM puisse y être mappée.
Réinitialiser modem	Réprésente la carte émule, ce qui fait que le modem relit la SIM et relance l'attachement. C'est ainsi que vous "changez la SIM" sans toucher au matériel.
SIM à distance	Connecter ou déconnecter quelle SIM à distance est présentée à ce cardem.

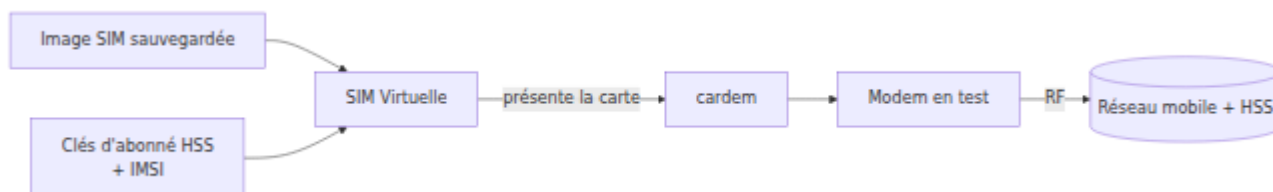
Le panneau **Source SIM** indique honnêtement ce qui est et n'est pas disponible : le cardem alimente le modem avec une SIM à *distance*. La console n'offre pas encore de présenter une carte *locale* insérée sur la carte émulateur. La console le dit plutôt que de montrer un contrôle qui ne fait rien.

SIM Virtuelle : un abonné sans carte physique

Une **SIM virtuelle** permet à un modem de s'attacher en tant qu'abonné **pour lequel vous n'avez pas de SIM**. OmniWeb la construit à partir de deux choses que vous avez déjà :

1. Une **image SIM de base** : un instantané sauvegardé de la structure de fichiers d'une vraie carte (n'importe quelle SIM de test compatible fonctionne comme base ; voir **Images SIM**).
2. L'**identité et les clés de l'abonné du HSS** : l'IMSI et les clés d'authentification d'un abonné déjà provisionné dans le réseau.

OmniWeb les combine en une carte logicielle. Cette carte répond aux lectures de fichiers du modem à partir de l'image et répond au défi d'authentification du réseau avec les clés HSS. Elle superpose l'IMSI de l'abonné choisi. À travers un cardem, le modem ne peut pas faire la différence avec une SIM en plastique : il lit l'IMSI, exécute l'authentification, et **s'attache au réseau en direct**.



Quand l'utiliser

- Reproduire le comportement de roaming ou d'attachement d'un abonné spécifique sans source pour leur SIM physique.
- Tester de nombreux abonnés provisionnés contre un modem, consécutivement.
- Tester des profils qui n'existent que dans le HSS (nouvellement provisionnés, pré-expédition).

Ce que cela prouve. Un modem sur le banc s'est attaché au réseau en direct (enregistré, réseau domestique) en tant qu'abonné HSS pour lequel aucune SIM en plastique n'existe. Il a lu l'IMSI de cet abonné et a complété l'authentification du réseau entièrement à partir de la carte virtuelle.

Un élément **Lecteur SIM Virtuel** dédié est la prochaine étape de cette capacité. Là, vous "chargez" une SIM virtuelle à partir d'une image et d'un abonné choisis et la présentez comme n'importe quel autre emplacement de lecteur. Aujourd'hui, OmniWeb connecte la carte virtuelle à travers le même courtier de SIM à distance et le chemin cardem décrit ci-dessus.

Utiliser une SIM dans un Livre de Test de Roaming

Les **Livres de Test** de Roaming (GSMA IR.38 / IR.48) peuvent gérer la présentation de la SIM dans le cadre d'une exécution. Dans le panneau **Exécuter des Tests** d'un livre de test, vous pouvez choisir :

- une **SIM (par ICCID / IMSI)** : suivie par identité, son lecteur actuel résolu automatiquement au moment de l'exécution, et
- un **Modem Cardem** : le cardem auquel la SIM est émule.

Présenter la SIM au cardem établit le mappage avant que vous ne testiez. **Go: Exécuter Tous les Tests** présente d'abord la SIM (lorsque les deux, une SIM et un cardem sont sélectionnés), puis lit l'IMSI et exécute les cas de données. Si la SIM n'est pas actuellement dans un lecteur, ou si le client du cardem ne fonctionne pas, le panneau indique exactement pourquoi. Il ne s'exécute pas contre le mauvais cardem en silence.

Voir [Appareils de Test](#) et la documentation du livre de test pour le reste du flux IR.38.

Dépannage

Une SIM n'apparaît pas dans la banque

Symptômes : un lecteur est branché mais aucun emplacement (ou un emplacement vide) n'apparaît.

Causes possibles & résolution :

- La carte n'est pas insérée, ou l'appairage lecteur/carte ne peut pas alimenter la carte. L'emplacement montre **Carte présente** ou **Vide**. Réinsérez la SIM.
- Le lecteur vient d'être branché. OmniWeb re-scanne les lecteurs lors du branchement à chaud, mais vous pouvez forcer cela avec **Rescan** dans le groupe de l'agent.

Le modem ne s'attache pas après avoir connecté une SIM

Causes possibles & résolution :

- Le modem n'a pas relu la SIM. Utilisez **Réinitialiser le modem** sur la [console cardem](#) pour représenter la carte.
- Le mappage n'est pas **ACTIF**. Confirmez sous **Mappages actifs** sur la page SIM à distance que la SIM est liée au bon cardem.
- L'abonné n'est pas provisionné (ou est interdit) dans le HSS du réseau de service.

"Carte présente (illisible)" sur un lecteur

Symptômes : une carte est détectée mais son identité ne peut pas être lue.

Résolution : ce lecteur ne peut pas communiquer avec cette carte (communément un désaccord de tension/protocole sur des lecteurs peu coûteux). Déplacez la SIM vers un autre lecteur dans la banque.

SIM Virtuelle : le modem lit la carte mais ne s'attache pas

Causes possibles & résolution :

- L'abonné choisi doit être **activé** et entièrement provisionné (avec un profil de données) dans le HSS pour le réseau de service.
- L'image de base doit provenir d'un type de carte compatible. Si l'initialisation se bloque, reprenez l'image de base à partir d'une SIM connue comme fonctionnelle.

SCEF : Fonction d'Exposition des Capacités de Service

Le **SCEF** (Fonction d'Exposition des Capacités de Service), **OmniSCEF** d'OmniTouch, est la **passerelle nord** du réseau pour l'Internet des Objets. Il expose les capacités du réseau central aux serveurs d'application externes via l'**API RESTful T8** définie dans [TS 29.122](#), permettant à une plateforme machine-à-machine de s'abonner à des événements concernant une flotte de dispositifs et d'échanger de petites quantités de données avec eux sans jamais utiliser Diameter ou GTP. Il gère deux familles de services. Les **Événements de Surveillance** demandent au réseau de signaler lorsqu'un dispositif devient accessible, perd sa connectivité, change de localisation, etc. La **Livraison de Données Non-IP (NIDD)** transporte de petites charges utiles non-IP vers et depuis des dispositifs NB-IoT contraints via le plan de contrôle. En interne, le SCEF atteint le MME via l'interface Diameter **T6a** ([TS 29.128](#)). OmniWeb affiche son statut, les ressources T8 qu'un serveur d'application a créées, et les sessions NIDD en cours qu'il gère.

[← Guide des Opérations](#)

Le tableau de bord est une page d'élément par instance accessible depuis la barre latérale lorsqu'un SCEF fonctionne dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API T8 du SCEF, de sorte qu'il reste derrière la passerelle authentifiée unique. Un lien de documentation dans l'en-tête de la page fournit une aide contextuelle. La page est organisée en onglets.

Le modèle ID SCS/AS

Chaque ressource T8 (chaque abonnement de surveillance et chaque configuration NIDD) est **définie par l'identité SCS/AS** sous laquelle le serveur d'application s'est enregistré (le *Serveur de Capacités de Services* /

Serveur d'Application). L'API T8 n'a **aucun point de terminaison qui énumère les ID SCS/AS** en cours d'utilisation, donc OmniWeb ne peut pas les découvrir pour vous : l'opérateur **définit l'ID SCS/AS** sur la page, et OmniWeb s'en souvient **à travers les onglets SCEF** afin que vous le définissiez une fois et qu'il soit transféré de l'aperçu aux événements de surveillance puis au NIDD. Tant qu'un ID SCS/AS n'est pas défini, les onglets définis demandent un ID plutôt que de montrer une liste vide. Les ressources existent sous une identité que vous devez nommer. Entrez l'ID SCS/AS avec lequel un serveur d'application a été intégré (par exemple `iot-platform-01@omnitouch`) pour travailler avec les abonnements et configurations de cette plateforme.

Aperçu

Une lecture de santé sur un seul écran du SCEF lui-même : son **statut**, le nom du **produit**, l'état de la **licence** et l'**hôte Diameter** qu'il utilise pour T6a vers le MME. En dessous se trouve le **contexte d'application** (le champ ID SCS/AS décrit ci-dessus) et, une fois qu'un ID SCS/AS est défini, le compte des **abonnements de surveillance** et des **configurations NIDD** actuellement détenus pour ce serveur d'application. C'est la confirmation la plus rapide que le SCEF est opérationnel et combien une plateforme donnée transporte. Des

tableaux de bord de surveillance et de statistiques sont fournis sous forme d'intégrations Grafana, accessibles depuis la même page.

Événements de Surveillance

Les **abonnements d'événements de surveillance** qu'un serveur d'application a créés pour l'ID SCS/AS actuel. Chaque abonnement demande au réseau de signaler une classe d'événement et de l'envoyer par POST au serveur d'application ; chaque ligne montre :

- **Type d'événement** : le type de surveillance, tel que **Accessibilité UE**, **Perte de Connectivité**, **Rapport de Localisation**, **Disponibilité après Échec DDN**, **Statut de Roaming** ou **Nombre d'UEs dans une Zone**.
- **Cible** : le dispositif ou le groupe que l'abonnement surveille, identifié par un **ID Externe**, un **MSISDN** ou un **ID de Groupe Externe** pour une flotte entière.
- **Destination de notification** : l'**URL de rappel** à laquelle le SCEF envoie chaque rapport d'événement par POST. Cela doit être une adresse `http(s)` absolue que le serveur d'application expose.

- **Max Rapports** et, pour un abonnement de connectivité, le **type de connectivité** (SMS ou DATA). Avec la **durée/expiration** de la surveillance, cela limite combien d'événements sont envoyés et jusqu'à quand l'abonnement est actif.

Les abonnements peuvent être créés, modifiés et supprimés ; supprimer un abonnement empêche le serveur d'application de recevoir ces rapports d'événements.

NIDD

Les **configurations NIDD** sont les liaisons de Livraison de Données Non-IP qu'un serveur d'application a créées pour l'ID SCS/AS actuel. Une configuration autorise l'échange de petites charges utiles non-IP avec un dispositif via le plan de contrôle. Chaque ligne montre :

- **Cible** : le dispositif par **ID Externe**, **MSISDN** ou **ID de Groupe Externe**.
- **DNN / APN** : le Nom de Réseau de Données (APN) que la connexion PDN NIDD utilise (par exemple nidd.iot.omnitouch).
- **Statut** : **ACTIF**, ou terminé (**TERMINÉ**, **TERMINÉ_UE_NON_AUTORISÉ**).

- **Max Paquet** : la **taille maximale de paquet** en octets que la charge utile non-IP peut atteindre.
- **RDS** : si le **Service de Données Fiable** est activé. Cela ajoute un transport léger reconnu avec des ports source/destination sur le lien non-IP.

Une configuration porte également une **option d'établissement de PDN** qui décide de ce qui se passe lorsque des données descendantes arrivent alors que le dispositif n'a pas de connexion PDN NIDD active : **attendre que l'UE** en établisse une, **indiquer une erreur**, ou **établir la connexion PDN** en paginant le dispositif.

Livraison de données descendantes

À partir d'une configuration NIDD, vous pouvez **livrer une charge utile descendante** au dispositif. Entrez la charge utile sous forme de texte. Le SCEF **l'encode en base64** avant qu'elle ne soit envoyée via NIDD, et chaque livraison peut porter une **priorité** et une **latence maximale**. Les livraisons récentes sont listées avec leur **statut de livraison** : `SUCCÈS`, `EN_COURS_DE_BUFFER`, `ENVOI`, ou l'une des raisons d'échec telles que `ÉCHEC_UE_NON_ATEIGNABLE`. Vous pouvez annuler une livraison en attente ou

en cours de buffer. C'est ainsi qu'une plateforme envoie une commande ou une mise à jour de firmware à un dispositif contraint qui n'a pas d'adresse IP.

Sessions NIDD

Les **sessions NIDD T6a en direct** sont les liaisons actives de Livraison de Données Non-IP que le SCEF maintient avec le MME en ce moment. Contrairement aux configurations NIDD, qui sont des ressources T8 définies par un ID SCS/AS, celles-ci sont des **états d'exécution globaux du serveur** : elles sont **en lecture seule** et ne sont pas définies par l'ID SCS/AS, donc cet onglet montre chaque session active indépendamment du contexte d'application que vous visualisez. Chaque ligne montre l'**IMSI** du dispositif, l'**APN** que la connexion PDN NIDD utilise, l'**Identité de Porteur EPS (EBI)**, l'**état de la session** (**ACTIF**, **INACTIF**), l'**id de session T6a**, l'**hôte MME** et le **realm MME**, et l'**id de configuration** contre lequel la session a été configurée. C'est le moyen le plus rapide de voir quels dispositifs ont effectivement une liaison non-IP active, et à travers quel MME.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du SCEF pour le dépannage d'une seule instance sans quitter OmniWeb.

Tableaux de bord de surveillance

Les taux de requêtes T8, le débit des rapports d'événements et les comptes de livraison NIDD pour le SCEF sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page d'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens Connexes

- **MME** : le SCEF y accède via **T6a** pour établir des connexions PDN NIDD et pour recueillir les événements de surveillance rapportés ici. L'hôte MME et le realm utilisés par chaque session sont affichés dans l'onglet Sessions NIDD.
- **HSS** : détient les données d'abonnement (Identifiants Externes, autorisation NIDD) dont dépendent les services de surveillance et NIDD du SCEF.
- **PGW-C / SMF** et **UPF** : transportent le plan de données IP ordinaire. NIDD les contourne délibérément pour déplacer de petites charges utiles non-IP via le plan de contrôle à la place.
- [Guide des Opérations](#) : retour à l'index des éléments.

SGW-C : Passerelle de Service (Plan de Contrôle)

La **SGW-C** est la moitié du plan de contrôle de la Passerelle de Service EPC. Elle ancre les porteurs de chaque abonné entre le réseau d'accès et la passerelle de paquets : elle termine **S11** vers le MME (signalisation de session et de porteur), **S5/S8** vers le PGW-C (la connexion PDN), et programme le plan utilisateur (SGW-U) qui transfère le trafic sur **S1-U** vers l'eNodeB. En résumé, c'est le nœud qui maintient l'état des porteurs actifs pour chaque abonné connecté et synchronise le MME, le PGW et le plan utilisateur. OmniWeb affiche les sessions actives de la SGW-C, les comptes de session et les journaux ; les tendances à long terme (débit, croissance des sessions) se trouvent sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des Opérations](#)

La SGW-C est une page d'élément par instance accessible depuis la barre latérale lorsque l'on navigue dans l'inventaire du site. Lorsque plusieurs sont déployées, elle fournit également une vue d'ensemble de la flotte pour l'état agrégé. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API de la SGW-C, de sorte qu'il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran : l'**état de l'API** de la SGW-C, le **nombre de sessions actives**, et un résumé dérivé des sessions actives : le nombre de **MMEs** uniques (pairs S11 distincts), de **PGWs** uniques (pairs S5/S8 distincts), et les **porteurs totaux** actuellement ancrés. C'est le moyen le plus rapide de confirmer que la SGW-C est opérationnelle, combien de sessions elle détient, et combien de MMEs et de PGWs elle utilise.

Sessions

Chaque session ancrée, chaque ligne identifiée par l'**IMSI** et le **MSISDN** de l'abonné avec son **état** de connexion. Ouvrir une session montre son état complet des porteurs : les points de terminaison de contrôle **S11** (F-TEIDs côté MME et côté SGW), chaque **connexion PDN** (APN, porteur par défaut, et les F-TEIDs de contrôle S5/S8 vers le PGW), et chaque **porteur** (EBI, les F-TEIDs de plan utilisateur S1-U et S5/S8, et sa QoS). C'est ici que vous confirmez que les porteurs d'un abonné spécifique sont établis et voyez quel MME et PGW les servent.

Journaux

L'onglet **Journaux** affiche en temps réel la sortie des journaux de la SGW-C pour le dépannage d'une seule passerelle sans quitter OmniWeb.

Tableaux de bord de surveillance

Les tendances de débit, de nombre de sessions et d'autres séries temporelles pour la SGW-C sont présentées sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens Connexes

- **MME** : le pair de contrôle sur **S11** ; il gère la configuration des sessions et des porteurs sur la SGW-C.
- La **PGW-C** ancre la connexion PDN sur **S5/S8**.
- La **SGW-U / UPF** est le plan utilisateur que la SGW-C programme pour transférer le trafic sur S1-U.

Outils de carte SIM : Système de fichiers, APDU & eSIM

OmniWeb fait plus que découvrir et présenter des SIM. Il vous offre un ensemble d'**outils de carte de bas niveau** qui passent par n'importe quel lecteur sur n'importe quel agent pour communiquer directement avec la carte. Vous pouvez parcourir et éditer son système de fichiers, envoyer des APDUs brutes à la main, observer la trace APDU en direct d'une session de SIM distante, et gérer des profils eSIM sur un eUICC. Cette page est le guide des opérations pour ces outils.

[← Guide des opérations](#)

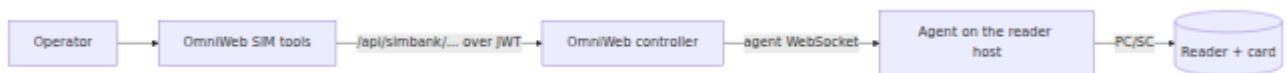
Ces outils se trouvent à côté des fonctionnalités SIM existantes et les réutilisent. Commencez ici pour avoir une vue d'ensemble :

- **SIM Bank** : l'inventaire : quelles SIM sont dans quels lecteurs à travers chaque agent. Chaque outil sur cette page cible un lecteur de cet inventaire, et les actions par emplacement de la SIM Bank renvoient directement à ceux-ci.
- **Images SIM (Paquets de profil SAIP)** : comment sauvegarder un système de fichiers lu en tant qu'image portable, et comment parcourir ou comparer des images sauvegardées.
- **SIM distante & SIM virtuelle** : comment présenter une SIM (réelle ou virtuelle) à un modem sur le réseau via des émulateurs de carte.
- **Gestion OTA des SIM** : le même editing au niveau des fichiers, mais il atteint une carte **par voie aérienne** avec des paquets sécurisés (03.48 / SCP80) au lieu d'un lecteur local.

Tous les quatre outils ci-dessous se trouvent dans la barre latérale sous le groupe **SIMs**.

Un lecteur, un consommateur à la fois

Une seule chose à la fois peut piloter un lecteur PC/SC physique. Un outil sur cette page peut nécessiter un lecteur que quelque chose d'autre détient déjà : un autre opérateur qui le lit, ou une session de banque SIM distante en direct qui le présente à un modem. L'outil montre alors **qui le détient et pourquoi**, et propose un **Prendre le contrôle** explicite. Il n'y a pas de coup silencieux : lorsque vous prenez le contrôle, OmniWeb annule l'autre session (et, pour une session de banque, déconnecte ce lien SIM↔cardem). Pour éditer ou envoyer, c'est une action de contrôle soumise à la permission de contrôle de la SIM Bank. Sans cela, vous pouvez voir les lecteurs mais pas piloter les cartes.



Explorateur de système de fichiers SIM

Choisissez un lecteur et **lisez l'ensemble de l'arborescence de fichiers** de sa carte : le MF, DF.GSM / DF.TELECOM, ADF.USIM et ADF.ISIM et tous leurs EFs, avec chaque fichier lisible décodé en champs nommés. Une lecture complète touche de nombreux fichiers, donc une barre de progression montre la marche ("lire X sur Y fichiers : EF....").

- **Recherchez** dans l'arborescence par code de fichier (FID), nom court ou description. Une recherche pour "Codes d'appel d'urgence" trouve EF.ECC, pas seulement 6FB7.
- **Les fichiers protégés par PIN sont signalés, jamais lus** : l'explorateur ne brûlera pas les tentatives de PIN.
- **Éditez un EF** (avec la permission de contrôle) : le panneau de détails propose un formulaire basé sur un schéma (champs décodés, typés) lorsque disponible, et revient à l'hexadécimal brut. Une écriture est destructive et demande une confirmation. Lorsque qu'un EF nécessite une authentification, utilisez d'abord **Vérifier CHV/ADM**. Cela teste une clé

PIN/ADM contre la carte (il rapporte les tentatives restantes et ne brûle jamais la dernière tentative). Une fois prouvé, l'explorateur le réutilise pour l'écriture. Le magasin de clés SIM offre automatiquement des clés sauvegardées pour l'ICCID d'une carte.

- **Sauvegarder une image** capture l'arborescence décodée en tant qu'**Image SIM** nommée. **Comparer avec l'image** compare la carte en direct avec une sauvegardée. **Images sauvegardées** ouvre la bibliothèque d'images. Vous pouvez également ouvrir une image sauvegardée *comme* une arborescence (`?image=<id>`) pour parcourir une carte que vous n'avez plus dans un lecteur.

Le lecteur doit être libre (non détenu par une session de SIM distante), ou vous pouvez prendre le contrôle comme ci-dessus.

Terminal APDU

Le Terminal APDU est une **console manuelle pour la carte** : tapez une APDU brute en hexadécimal, envoyez-la à la carte dans un lecteur choisi, et voyez la réponse décodée. Le décodage montre le nom de la commande INS, le mot d'état et sa signification, et une interprétation étendue de toute donnée de réponse (un arbre TLV FCP, des champs EF décodés, ou un résultat AUTHENTICATE). Des boutons préconfigurés (SELECT MF, STATUS, READ BINARY, GET RESPONSE, ...) remplissent les commandes courantes. L'entrée est tolérante aux espaces/aux deux-points et validée (octets entiers, au moins CLA/INS/P1/P2).

Deux modes :

Mode	Comportement	Utiliser pour
Coup unique	Chaque APDU est autonome ; la carte se réinitialise au MF entre les envois.	Probes ponctuels.
Session	Ouvre une session de carte persistante et exclusive, donc l'état (sélection, authentification) persiste à travers les APDUs : un SELECT puis un READ BINARY fonctionne, et un VERIFY partage son auth avec une mise à jour ultérieure. Le lecteur reste détenu jusqu'à ce que vous fermiez la session.	Séquences avec état.

L'action **APDU** par emplacement de la SIM Bank renvoie ici avec ce lecteur exact pré-sélectionné. Les mêmes règles de consommateur unique/Prendre le contrôle s'appliquent.

Journal APDU

Alors que le terminal est vous pilotant une carte, le **Journal APDU** est une **trace en direct passive** des APDUs de commande/réponse échangées entre un **modem et une (distante) SIM** à travers la chaîne SIM distante / cardem. Activez **la capture** et cela suit l'échange : chaque ligne associe une commande `modem→carte` avec son mot d'état décodé, plus le même décodage de réponse que le terminal (arbre FCP, champs EF, événements ATR/réinitialisation). Vous pouvez mettre la vue en pause (la capture continue de fonctionner), filtrer par commande/hex/SW, et faire défiler automatiquement.

Utilisez-le pour voir ce qu'un modem demande réellement à la SIM lors d'une attache ou d'un **test IR.38** : quels fichiers il sélectionne, où un VERIFY échoue, si un AUTHENTICATE réussit. Vous n'avez pas besoin d'instrumenter le modem. Cela s'associe naturellement avec **SIM distante**, qui établit le lien modem↔SIM que le journal suit ensuite.

eSIM (LPA)

L'outil **eSIM** gère un **eUICC** via l'**Assistant de profil local (LPA)** de l'agent. Un eUICC est une puce eSIM physique dans l'un de vos lecteurs. Il contient plusieurs profils, mais un seul est actif à la fois.

- **Carte eUICC** : montre l'**EID** de la puce.
- **Profils installés** : chaque profil sur la carte : son état (actif/désactivé), son surnom, son fournisseur, son nom et son ICCID. Par profil, vous pouvez **activer** (le rendre l'eSIM active), **désactiver**, **renommer** (surnom), ou **supprimer**. Une suppression retire le profil de l'eUICC et est irréversible, donc elle demande d'abord confirmation.
- **Télécharger un profil** : tirer un nouveau profil d'un SM-DP+ d'opérateur et l'installer sur la carte. Utilisez un **code d'activation** complet (`LPA:1$sm dp .example.com$MATCHING-ID`) ou une adresse **SM-DP+ fractionnée + ID correspondant**, avec un code de confirmation optionnel.

Ceci est spécifiquement pour les cartes eSIM (eUICC). Pour l'édition de fichiers SIM/UICC classique, utilisez l'Explorateur de système de fichiers ci-dessus. Pour éditer une carte **à distance**, utilisez **OTA**.

Kit d'outils SIM (STK)

Le client **Kit d'outils SIM** pilote les applets STK sur une carte SIM. Il envoie un profil de terminal à la carte, puis présente chaque commande proactive sous forme d'écran interactif : menus, affichage de texte, saisie à touche unique, et saisie de texte. Utilisez-le pour naviguer dans les services résidents de l'opérateur, déclencher des flux de configuration OTA, ou tester la logique des applets résidents sur la SIM.

Voir **Kit d'outils SIM** pour le guide complet des opérations.

Liés

- **SIM Bank** : l'inventaire lecteur/SIM que ces outils ciblent.
- **Images SIM** : sauvegarder, parcourir et comparer des systèmes de fichiers lus.
- **SIM distante & SIM virtuelle** : présenter une SIM à un modem sur le réseau (le lien que trace le Journal APDU).
- **Gestion OTA des SIM** : le même editing de fichiers, par voie aérienne.
- **Kit d'outils SIM** : interagir avec des applets STK sur une carte dans un lecteur.

Images SIM : Paquets de Profil SAIP

Une **Image SIM** est un instantané enregistré de l'ensemble du système de fichiers d'une carte. OmniWeb stocke chaque image en tant que **Paquet de Profil Non Protégé SAIP (UPP)** en encodage DER. C'est le même format interopérable utilisé par les profils eUICC, défini par la *Spécification Technique du Format Interopérable des Paquets de Profil eUICC* du TCA. Une carte capturée devient un fichier portable `.der` que tout outil compatible SAIP peut lire.

Cette page est le guide des opérations. Elle couvre comment capturer, exporter, télécharger, parcourir et comparer des images SIM, et comment utiliser une image enregistrée pour soutenir un **SIM virtuel**. **SIM Bank** couvre l'inventaire des lecteurs en direct.

Table des Matières

- [Pourquoi SAIP UPP](#)
- [Aperçu de l'Architecture](#)
- [Que contient une Image](#)
- [Capturer une Image](#)
- [Exporter une Image](#)
- [Télécharger une Image](#)
- [Parcourir une Image dans l'Explorateur](#)
- [Comparer Deux Images](#)
- [Soutenir un SIM Virtuel avec une Image](#)
- [Référence des Éléments de Profil](#)
- [Dépannage](#)

Pourquoi SAIP UPP

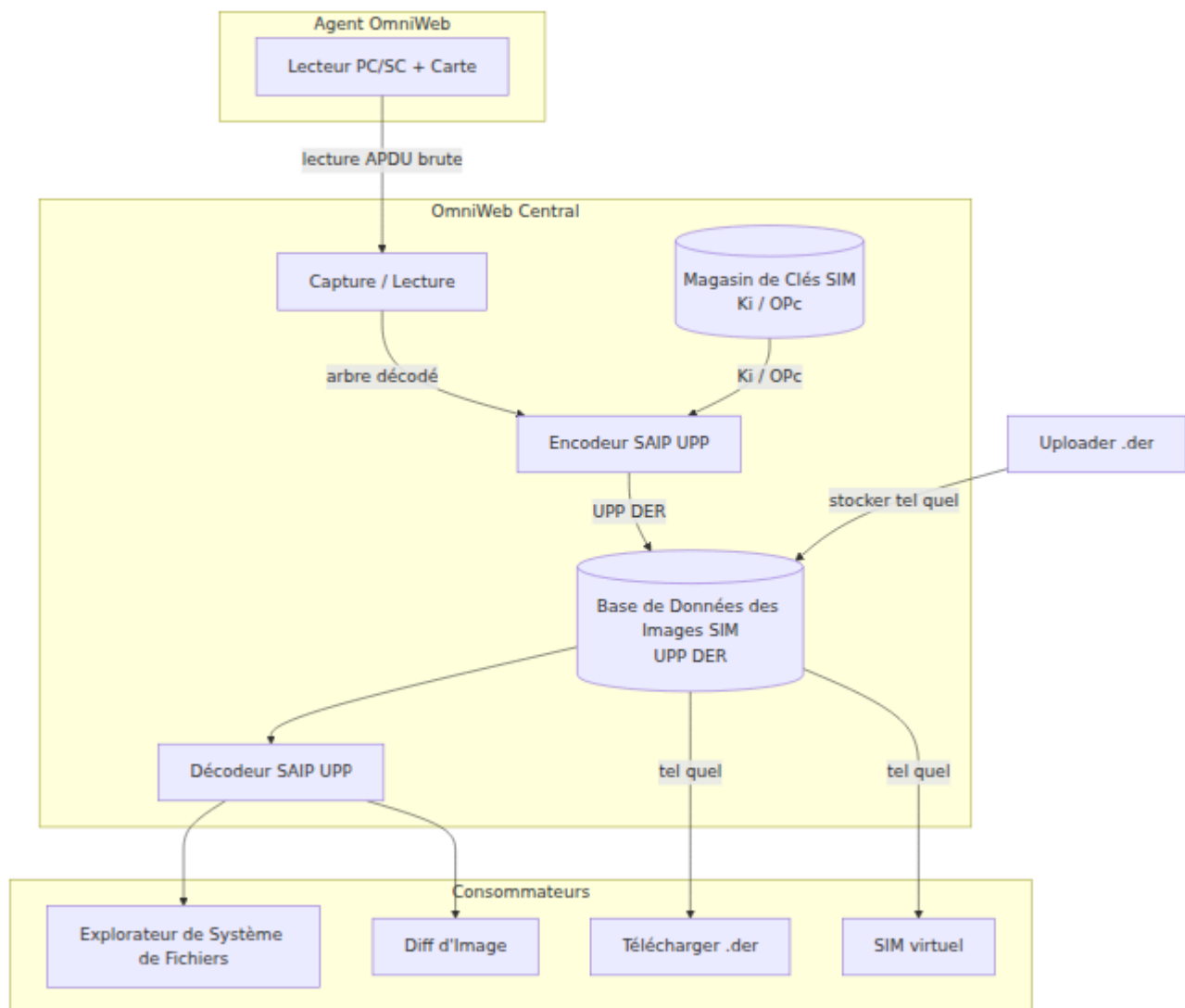
Les versions antérieures stockaient une image SIM sous forme d'arbre JSON décodé utilisé uniquement pour la comparaison. Ce format était privé à OmniWeb et aucun outil externe ne pouvait le consommer.

Lorsque OmniWeb stocke l'image en tant que **SAIP UPP**, vous obtenez :

- **Portabilité** : le `.der` exporté est un paquet de profil standard. Il se charge dans les validateurs de profil SAIP et tout outil compatible SAIP.
- **Un format partout** : le même `.der` qu'un opérateur télécharge est celui qui soutient un SIM virtuel et que l'explorateur de fichiers rend. Il n'y a pas de seconde représentation divergente.
- **Reprovisionnement** : lorsque les clés d'authentification de la carte sont connues (voir [Capturer une Image](#)), l'UPP inclut un élément `PE-AKAPParameter` qui transporte Ki et OPc. Le paquet décrit alors un profil complet et installable plutôt qu'un dump en lecture seule.

Le paquet est une concaténation brute des Éléments de Profil encodés en DER. Il **n'est pas** chiffré (c'est un *Paquet de Profil Non Protégé*). Traitez un `.der` exporté avec le même soin que tout fichier contenant Ki/OPc. Voir [Dépannage](#).

Aperçu de l'Architecture



La capture lit la carte, l'encodeur produit un UPP (il intègre Ki/OPc du Magasin de Clés SIM si disponible), et OmniWeb stocke le paquet. Chaque consommateur lit à partir de ce paquet stocké unique. L'explorateur et le diff le décodent en arbre à la demande. Le téléchargement et le SIM virtuel utilisent les octets tels quels.

Que contient une Image

Une image capturée contient, pour la disposition standard MF / ADF.USIM de la carte :

Élément	Élément de Profil SAIP	Contenu
Système de fichiers	PE - GenericFileManagement	Chaque EF accessible : ses Paramètres de Contrôle de Fichier (FCP) et contenu brut (EFs transparents) ou chaque enregistrement (EFs linéaires/cycliques)
Identité	PE-Header	L'ICCID de la carte
Authentification	PE-AKAParameter	Ki et OPc pour Milenage. Présent uniquement lorsque les clés de la carte sont dans le Magasin de Clés SIM

Les fichiers sont créés avec PE-GenericFileManagement (un groupe d'opérations par DF) plutôt qu'avec les modèles de système de fichiers SAIP standardisés : une lecture de carte récupère des octets bruts, pas le modèle qu'un créateur de profil a utilisé à l'origine, donc la représentation générique est toujours exacte.

Capter une Image

La capture se fait à partir de l'Explorateur de Système de Fichiers SIM ou des actions de slot de SIM Bank :

1. Lire le système de fichiers d'une carte dans l'explorateur.
2. Choisir **Enregistrer l'image** et lui donner une étiquette.

Le système de fichiers décodé est encodé en un UPP et stocké. Si une entrée de Magasin de Clés SIM existe pour l'ICCID de la carte avec à la fois **Ki** et **OPc**, ces clés sont écrites dans un PE-AKAParameter afin que le paquet résultant soit entièrement installable. Sans une entrée dans le magasin de clés, le paquet

capture toujours le système de fichiers complet ; seul l'élément d'authentification est omis.

Les **colonnes d'identité** (ICCID, IMSI, type de carte, nombre de fichiers) sont dérivées du système de fichiers au moment de la capture afin que la liste des images et l'en-tête de diff n'aient jamais besoin de redécoder le paquet.

Exporter une Image

Chaque ligne de la liste des images enregistrées a une action **télécharger** qui sert le paquet stocké tel quel sous le nom `UPP_<iccid>.der`.

Le `.der` téléchargé est un UPP SAIP standard et peut être inspecté avec tout outil de profil compatible SAIP.

Comment cela fonctionne : Le fichier est exactement les octets stockés lors de la capture (ou du téléchargement), sans ré-encodage au téléchargement, donc un téléchargement aller-retour est byte-identique à ce qui est stocké.

Télécharger une Image

La page des images enregistrées a une action **Uploader .der** qui accepte un fichier UPP SAIP et le stocke en tant que nouvelle image. Utilisez-le pour importer des profils générés ailleurs : par exemple, les paquets de *Profil de Test eUICC Générique* GSMA TS.48, ou un UPP produit par un autre outil SAIP.

Lors du téléchargement, OmniWeb :

1. Valide que le fichier commence par une balise d'Élément de Profil SAIP (une balise construite de classe de contexte : `A0`, `A1` ou `B0`).
2. Stocke le paquet tel quel.
3. Décode le `PE-Header` pour peupler la colonne ICCID lorsque présente.

Une image téléchargée est une image de première classe : elle peut être téléchargée, parcourue dans l'explorateur, comparée, modifiée et utilisée pour soutenir un SIM virtuel exactement comme une image capturée.

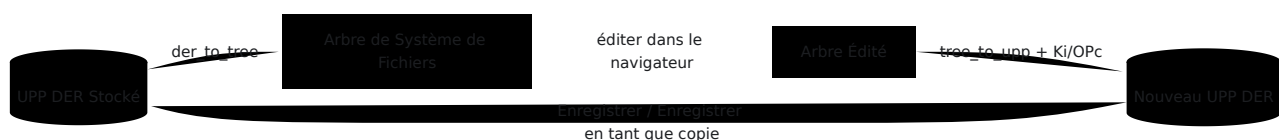
Modifier une Image

Une image enregistrée est un **fichier**, pas une carte. Pour en modifier une, il suffit de changer le paquet de profil stocké uniquement et **jamais d'écrire sur une SIM**. À partir de la liste des images enregistrées, l'action **Modifier le système de fichiers** ouvre l'**Explorateur de Système de Fichiers SIM** en mode édition (`?image=<id>&edit=1`). Aucun lecteur et aucun accès à la carte de l'agent ne sont impliqués.

Vous pouvez :

- **Modifier le contenu d'un fichier** : changer les octets de n'importe quel EF. Comme avec une carte en direct, l'éditeur propose un **Formulaire** guidé par un schéma, une vue **JSON** de tout l'enregistrement, et un **Hex brut** pour les échappements. Il n'y a pas de demande de PIN/ADM (un fichier n'a pas de conditions d'accès à satisfaire).
- **Ajouter un fichier** : créer un nouvel EF (transparent ou structuré par enregistrement) ou DF sous n'importe quel DF/MF/ADF, et donner son FID, sa structure et son contenu initial.
- **Supprimer un fichier** : retirer n'importe quel EF ou DF (la racine MF est l'image entière et ne peut pas être supprimée).
- **Renommer** l'image (métadonnées uniquement) depuis la liste.

Le navigateur conserve les modifications jusqu'à ce que vous **Enregistriez l'image** (écraser sur place) ou **Enregistriez en tant que copie** (forker une nouvelle image et laisser l'original intact). Lors de l'enregistrement, OmniWeb ré-encode l'arbre de système de fichiers modifié en un UPP SAIP. Il intègre Ki/OPc du **Magasin de Clés SIM** lorsqu'il est connu. Il préserve tel quel tout Éléments de Profil que l'arbre ne modélise pas (PIN, PUK, Domaine de Sécurité, modèles), donc une modification ne supprime jamais le reste du profil.

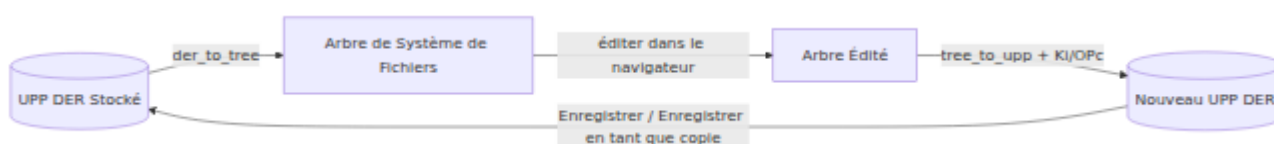


Édition de champs Form / JSON hors ligne. Pour décoder un EF en champs nommés et les ré-encoder, utilisez le même modèle de fichier que l'éditeur en direct utilise, exécuté sur n'importe quel agent en ligne, mais sans **carte** :

l'image détient déjà les octets, donc l'agent exécute uniquement le codec. Si aucun agent n'est en ligne, l'édition revient à Hex brut, qui n'a besoin de rien externe.

Parcourir une Image dans l'Explorateur

Chaque image enregistrée a une action **Parcourir dans l'explorateur de système de fichiers**. Cela ouvre l'**Explorateur de Système de Fichiers SIM** contre le paquet stocké. **Aucune carte physique et aucun lecteur ne sont nécessaires**. OmniWeb décode le paquet en l'arbre de système de fichiers que l'explorateur rend pour une carte en direct, vous permettant d'inspecter le contenu brut de chaque EF hors ligne.



Comparer Deux Images

La page des images enregistrées vous permet de choisir deux images et de les comparer. Les deux paquets sont décodés en arbres de système de fichiers et alignés par chemin EF, de sorte que la comparaison est fichier par fichier, indépendamment de l'ordre de capture :

Statut	Signification
same	EF présent dans les deux avec contenu identique
changed	EF présent dans les deux, contenu différent
only_a	EF présent uniquement dans la première image
only_b	EF présent uniquement dans la seconde image

Pour un EF **modifié**, le diff rapporte les plages d'octets différents (et les deltas par enregistrement pour les fichiers structurés par enregistrement), vous permettant de voir exactement quels octets ont changé : par exemple, un SIM de test avant et après un changement de personnalisation, ou deux SIM d'opérateurs côte à côte.

Soutenir un SIM Virtuel avec une Image

Une image enregistrée peut remplacer une carte physique lors de la présentation d'un **SIM virtuel**. Dans le compositeur de SIM virtuel, les images enregistrées apparaissent aux côtés des images rspro capturées comme sources de système de fichiers sélectionnables. Associez-en une à une identité d'abonné (provenant de l'HSS ou du Magasin de Clés SIM) et OmniWeb lance un **bankd** virtuel soutenu par le système de fichiers de cette image, avec Ki/OPc de l'abonné superposé pour l'authentification.



Le système de fichiers que le modem lit est rejoué à partir de l'image ; l'identité et les clés sont superposées à partir de l'abonné choisi, de sorte qu'une image peut soutenir plusieurs abonnés.

Référence des Éléments de Profil

L'UPP est une séquence d'Éléments de Profil, chacun étant un DER TLV dont la balise de classe de contexte identifie son type. OmniWeb écrit et lit le sous-ensemble ci-dessous ; d'autres éléments dans un paquet téléchargé (PIN, PUK, Domaine de Sécurité, modèles de système de fichiers) sont préservés lors du stockage et ignorés lors du décodage en un arbre de système de fichiers.

Balise	Élément de Profil	Utilisé par OmniWeb
A0	PE-Header	ICCID ; métadonnées du profil
A1	PE- GenericFileManagement	Le système de fichiers (FCP + contenu)
A4	PE-AKAPparameter	Ki et OPc (Milenage)
AA	PE-End	Marqueur de fin de paquet
B0	PE-MF	(MF modélisé : lu lors du téléchargement, non émis)

Pour le catalogue complet des éléments et les règles d'encodage, voir la [Spécification Technique du Format Interopérable des Paquets de Profil eUICC du TCA](#).

Dépannage

L'image exportée n'a pas de clés d'authentification

Symptômes : Un .der téléchargé n'a pas de PE-AKAPparameter ; un SIM virtuel soutenu par l'image ne peut pas s'authentifier sans clés fournies séparément.

Causes possibles :

- Aucune entrée de Magasin de Clés SIM n'existait pour l'ICCID de la carte au moment de la capture.
- L'entrée du magasin de clés manquait Ki ou OPc.

Résolution :

1. Ajoutez Ki et OPc de la carte au Magasin de Clés SIM, indexé par son ICCID.

2. Re-capturez l'image. La nouvelle capture intègre les clés dans un `PE-AKAPparameter`.
3. Alternativement, fournissez les clés au moment de la présentation du SIM virtuel (provenant de l'HSS ou d'un remplacement explicite).

Téléchargement rejeté comme "ne ressemble pas à un SAIP UPP"

Symptômes : Le téléchargement d'un fichier renvoie une erreur de validation.

Causes possibles :

- Le fichier n'est pas un UPP SAIP : il ne commence pas par une balise d'Élément de Profil (`A0`, `A1` ou `B0`).
- Le fichier est un paquet de profil *protégé* (chiffré), pas un *non protégé*.

Résolution :

1. Confirmez que le fichier est un **Paquet de Profil Non Protégé** en encodage DER.
2. Vérifiez qu'il commence par un `PE-Header` (`A0`). La plupart des UPP bien formés le font.
3. Si le paquet est protégé/chiffré, il ne peut pas être stocké ou parcouru ; seuls les paquets non protégés sont pris en charge.

Parcourir une image téléchargée montre des fichiers par FID, pas par nom

Symptômes : Les EFs dans l'explorateur sont étiquetés par identifiant de fichier (par exemple `EF.6FXX`) plutôt que par un nom convivial.

Causes possibles :

- Une lecture de carte récupère des identifiants de fichiers et du contenu brut, pas les noms symboliques qu'un créateur de profil a utilisés. OmniWeb associe les EFs USIM bien connus à des noms conviviaux ; tout EF en dehors de cette carte est affiché par son FID.

Résolution : Aucune action n'est nécessaire. Le FID est l'identifiant autoritaire et le contenu brut est exact. Cela est attendu pour des fichiers non standards ou spécifiques à un fournisseur.

Manipulation des paquets exportés en toute sécurité

Un UPP exporté est **non chiffré** et, lorsque les clés étaient disponibles lors de la capture, contient Ki et OPc. Traitez un `.der` téléchargé comme un matériel clé sensible :

- Ne l'envoyez pas par des canaux non fiables.
- Supprimez les copies locales lorsqu'elles ne sont plus nécessaires.
- Préférez garder les images à l'intérieur d'OmniWeb (où l'accès est contrôlé par la permission de la SIM Bank) plutôt que de distribuer des fichiers `.der`.

Banque SIM : inventaire distribué de SIM

La **Banque SIM** montre chaque SIM dans chaque lecteur de carte à puce à travers chaque agent OmniWeb. Chaque agent scanne ses lecteurs PC/SC locaux, lit l'identité de chaque SIM et rapporte l'inventaire au central exactement comme il le fait déjà pour les modems/téléphones en tant que dispositifs. Le central agrège l'inventaire par agent et persiste une base de données de SIMs indexée par ICCID, de sorte que la vue "quelles SIMs sont où" survive aux déconnexions de lecteurs et d'agents.

Ceci est la moitié inventaire d'un banc d'essai distribué de SIM à distance. La couche d'émulation de carte SIM à distance/banking vous permet de **connecter n'importe quelle SIM à n'importe quelle carte sur le réseau**. [SIM à distance](#) documente cette couche séparément. Cette page couvre la découverte et l'inventaire. [Images SIM \(Packages de Profil SAIP\)](#) couvre comment sauvegarder, exporter et réutiliser le système de fichiers d'une carte en tant que package de profil portable.

La page est **centrée sur le lecteur** : une ligne par emplacement de lecteur physique, regroupée par agent. Les emplacements vides, illisibles et en cours d'utilisation sont tous affichés. La disposition de la banque est la vérité, pas seulement les emplacements peuplés.

Comment l'agent lit une SIM

Le scanner de l'agent reflète le scanner de modem : l'énumération est lente, donc les résultats sont mis en cache et rescannés à intervalles réguliers.

Pour chaque lecteur PC/SC sur l'hôte :

1. **Énumérer** les lecteurs PC/SC attachés à l'hôte.
2. **Interroger** chaque lecteur avec une connexion *exclusive*.
 - Pas de carte → `present=false`.
 - La connexion soulève une **violation de partage** → le lecteur est occupé par un autre processus (par exemple, un `bankd` de SIM à distance ou une session d'émulation de carte) → `present=true`, `in_use=true`, et **aucune lecture n'est tentée**. Un lecteur occupé ne fait jamais planter le scan.
 - Carte présente et libre → la lire.
3. **Lire** l'identité de la SIM avec un ensemble autonome d'APDUs bruts :
 - Détection de SIM UICC-vs-classique (sélectionner `3F00`; `6E00` → GSM classique, donc utiliser `CLA=A0` et le mode de sélection classique),
 - EF.ICCID (`2FE2`), EF.IMSI (`6F07`), EF.SPN (`6F46`),

- EF.AD (6FAD) pour la longueur de MNC (donc MCC/MNC sont correctement séparés),
- un **PIN** par défaut **sûr** (0000) VERIFY sur une carte verrouillée. Il interroge d'abord le compteur de réessai (un VERIFY vide non-décrémentant) et **refuse** si un seul réessai reste, donc il **ne** brûle **jamais** le dernier réessai ou ne touche le PUK (une banque SIM ne doit pas briquer les cartes),
- l'ATR de la carte.

Chaque lecteur devient un dictionnaire :

```
{
  "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..."
}
```

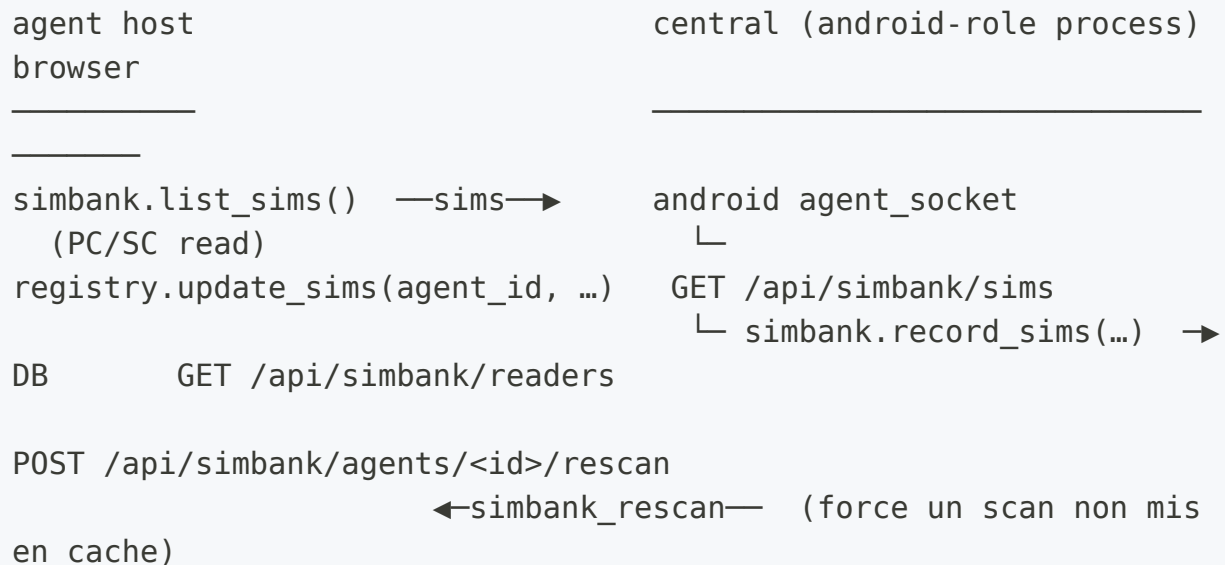
La liste est envoyée au central sous forme de message `sims` (avec la liste des dispositifs) lors de l'enregistrement et chaque fois qu'elle change ; une commande `simbank_rescan` force un scan non mis en cache immédiat.

Capacité de lecture de carte

Un hôte lit les SIMs à travers sa pile de cartes à puce PC/SC. Lorsque le décodage de carte plus approfondi est nécessaire, l'agent utilise une bibliothèque de cartes à puce optionnelle, sous licence séparée, maintenue isolée du reste de l'agent (elle n'est pas intégrée dans le code d'OmniWeb). Un hôte **sans** la pile de cartes à puce fonctionne toujours bien avec l'agent et rapporte simplement aucune SIM. La banque SIM est une capacité optionnelle par hôte, comme les modems.

Le lecteur de référence est un SCM/Identiv SCR35xx. Plusieurs lecteurs par hôte sont supportés.

Inventaire → central → flux UI



- L'agent compose **vers** le central via le même WebSocket qu'il utilise pour les téléphones (`/api/android/agent`). L'inventaire des SIMs utilise cette connexion. Il n'y a pas de nouveau transport.
- Le central maintient un instantané **en direct** des lecteurs par agent dans le `android.Registry` en mémoire (`update_sims` / `all_sims`), et reflète chaque ICCID dans la table persistante `simbank_sims` via `simbank.record_sims`.
- Parce que cela dépend du registre d'agent à processus unique, l'API de la banque SIM est servie **uniquement par le processus backend de rôle d'agent** (même contrainte que les dispositifs de test).

API REST (/api/simbank, JWT, type d'élément RBAC simbank)

Méthode	Route	But
GET	/sims	Chaque SIM à travers tous les agents (y compris les persistés hors ligne uniquement), avec en direct présent/en cours d'utilisation superposé.
GET	/readers	Chaque lecteur PC/SC sur chaque agent connecté (en direct), y compris les lecteurs vides et en cours d'utilisation.
GET	/sims/<iccid>	Une SIM.
PATCH	/sims/<iccid>	Modifier les champs assignés par l'opérateur (notes aujourd'hui). Crée la ligne si l'ICCID est inconnu.
DELETE	/sims/<iccid>	Oublier une SIM (supprime l'enregistrement persistant ; réapparaît lors du prochain scan si toujours insérée).
POST	/agents/<id>/rescan	Forcer un rescan PC/SC non mis en cache immédiat sur un agent et retourner son inventaire frais.

RBAC reflète `ir38/android-control` : les administrateurs passent toujours ; sinon, un JWT avec `element_type == "simbank"` accorde la vue, et `POST` dans ses méthodes accorde le contrôle.

Frontend

`src/pages/simbank/SimBank.tsx` : un tableau filtrable et consultable de toutes les SIMs : statut (présent / en cours d'utilisation / hors ligne), agent/site, lecteur, ICCID, IMSI, MCC/MNC, pays, SPN, notes modifiables, dernière vue. Bouton **Rescan** par agent. Routé à `/simbank` et lié à partir de la barre latérale sous **Tests de Roaming** > **Banque SIM**.

Schéma de base de données

`simbank_sims` : une ligne par ICCID jamais vue :

Colonne	Notes
<code>iccid</code> (PK)	Numéro de série de la SIM.
<code>imsi</code> , <code>mcc</code> , <code>mnc</code> , <code>country</code> , <code>spn</code> , <code>atr</code>	Dernière identité connue (écrasée uniquement par des lectures non vides).
<code>notes</code>	Assigné par l'opérateur, modifiable.
<code>last_agent_id</code> , <code>last_site</code> , <code>last_reader_name</code> , <code>last_reader_index</code>	Où il a été vu pour la dernière fois (ou est actuellement) .
<code>first_seen</code> , <code>last_seen</code>	Horodatages (UTC).
<code>remsim_bank_id</code> , <code>remsim_slot_nr</code> , <code>remsim_mapped_cardem</code>	Phase-2 réservé (nullable, inutilisé).

Les lecteurs vides et en cours d'utilisation ne portent **aucun** ICCID, donc ils ne sont pas persistés en tant que SIMs. Ils apparaissent uniquement dans l'instantané en direct `/readers`.

Futur : SIM à distance

La phase 2 mappe un lecteur/SIM physique dans une banque de SIM à distance afin qu'une SIM dans un site puisse être présentée à un modem/téléphone dans un autre (SIM à distance). Les crochets sont déjà en place. Recherchez le code pour `# TODO remsim` :

- `simbank_sims.remsim_bank_id / remsim_slot_nr / remsim_mapped_cardem` (colonnes nullable, affichées dans `to_dict` et le type TS `SimRow` comme `null`),
- le drapeau `in_use` par lecteur de l'agent distingue déjà un lecteur occupé par un `bankd`/session d'émulation. C'est le lecteur que la phase 2 va mapper,
- `PATCH /api/simbank/sims/<iccid>` est l'endroit où l'édition du mapping `remsim` sera câblée.

Rien ici ne conduit `remsim` aujourd'hui ; la forme est réservée afin que le mapping s'insère sans retravailler le chemin chaud de l'inventaire.

Éditeur de Site : Visualiseur de Configuration de Site

L'**Éditeur de Site** montre le fichier de configuration brut pour le site actuellement sélectionné : le fichier YAML d'hôte/inventaire qui définit les fonctions réseau, l'infrastructure et les paramètres de ce déploiement. C'est une vue en lecture seule, avec syntaxe mise en surbrillance, vous permettant de voir exactement sur quoi OmniWeb travaille pour un site sans ouvrir un shell sur un hôte.

[← Guide des Opérations](#)

Ce qu'il montre

OmniWeb gère chaque site à partir d'un fichier de configuration par site. Ce fichier liste les éléments du site (quels NFs sont présents et à quelles adresses), ses hôtes d'infrastructure, son rôle de surveillance, son bloc `fivegc` (voir [5G Core](#)), et ainsi de suite : tout ce dont la barre latérale, la topologie, les pages d'éléments et les tableaux de bord dérivent.

L'Éditeur de Site charge ce fichier pour le site choisi dans le menu déroulant de la barre supérieure et l'affiche dans un panneau d'éditeur complet (Monaco, le même éditeur utilisé par VS Code) avec mise en surbrillance YAML, numéros de ligne, pliage et une minimap. L'en-tête montre le client, le site et le nom du fichier source.

```
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'
```

Réessayer

Si aucun site n'est sélectionné, la page vous invite d'abord à en choisir un dans le menu déroulant.

Lecture seule par conception

L'Éditeur de Site est un **visualiseur** : le panneau est en lecture seule (marqué avec une puce **lecture seule** dans l'en-tête). Il est là pour *inspecter* la configuration effective, pas pour la modifier.

La configuration du site n'est pas modifiée depuis le navigateur. Comme noté tout au long de ce guide, le déploiement et la configuration d'OmniWeb sont gérés via **Ansible**. Ne modifiez pas les fichiers de configuration directement sur les hôtes, et ajouter ou changer un élément est un changement de configuration effectué via ce pipeline (voir [le modèle de configuration](#)). L'Éditeur de Site vous permet de lire le résultat de ce pipeline pour le site sélectionné.

Quand l'utiliser

- **Confirmer avec quoi un site est configuré** : quels éléments, hôtes et NFs 5GC OmniWeb pense être présents, et à quelles adresses.
- **Déboguer l'interface utilisateur par rapport à la configuration** : si un élément, une entrée de barre latérale ou une section 5GC est manquant ou pointe vers le mauvais hôte, le fichier brut est la source de vérité à vérifier.
- **Référencer le nom de fichier exact et son contenu** lors de la préparation d'un changement Ansible.

Liens Connexes

- [Architecture : le modèle de configuration](#) : comment la configuration du site pilote OmniWeb et comment elle est gérée.
- [5G Core](#) : le bloc `fivegc` de la configuration du site et ce qu'il expose.

- **Topologie Réseau** : les vues de topologie et de liste d'hôtes construites à partir de la même configuration de site.

Passerelle SMPP

La **Passerelle SMPP** relie les pairs SMPP externes au cœur de messagerie. Les applications externes et les partenaires d'interconnexion, les **ESMEs** (Entités de Message Court Externes), se connectent via SMPP soit en tant que clients que la passerelle appelle, soit en tant que serveurs auxquels la passerelle accepte des liaisons, et la passerelle transporte leurs messages courts vers et depuis le SMSC. Chaque connexion est un **bind** SMPP (transceiver, émetteur ou récepteur). La passerelle maintient ces liaisons, les authentifie et les contrôle, et transmet le trafic au cœur de messagerie. OmniWeb affiche l'état des liaisons en direct, les pairs clients et serveurs configurés, et les journaux de la passerelle.

[← Guide des opérations](#)

La Passerelle SMPP est une page d'élément par instance accessible depuis la barre latérale lorsqu'on fonctionne dans l'inventaire du site, avec une vue de flotte où plusieurs sont déployés. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API de la passerelle, donc il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

Une lecture de santé sur un seul écran des statistiques agrégées des liaisons : le **nombre total** de liaisons et la répartition **connectée / déconnectée** divisée entre les liaisons **client** (sortantes) et **serveur** (entrantes). C'est le moyen le plus rapide de confirmer que la passerelle est opérationnelle et que ses pairs sont liés, et de repérer d'un coup d'œil si une connexion attendue a été interrompue.

État des liaisons

Chaque liaison activée, client et serveur, avec son **état de connexion** actuel, les **détails de session** sous-jacents et les **métriques** par liaison. C'est la vue en direct de qui est lié en ce moment. De là, un opérateur peut agir sur une liaison :

- **Supprimer** une liaison active. Pour une liaison client, cela termine la connexion sortante. Pour une liaison serveur, cela déconnecte toutes les connexions clients actives. Utilisez-le pour libérer une connexion bloquée ou mal comportée.
- **Reconnecter** une liaison client. Cela force une liaison (sortante) client à rappeler son hôte distant, ce qui est le moyen le plus rapide de ramener un pair sortant après un problème réseau.

Pairs clients

Les connexions SMPP **client** sortantes configurées sont les pairs que la passerelle compose. Chacune montre son **nom**, l'**hôte** distant et le **port**, l'**ID système** avec lequel elle se lie, et le **type de liaison** (transceiver, émetteur ou récepteur). Les pairs clients sont entièrement modifiables ici : un opérateur peut **ajouter** un pair, **modifier** un existant (hôte, port, identifiants, type de liaison, intervalle de lien de demande, limite TPS et les autres paramètres de liaison), et **supprimer** un qui n'est plus nécessaire. Activer un pair met sa liaison sortante en service. Le désactiver retire le pair sans supprimer sa configuration.

Pairs serveurs

Les autorisations SMPP **serveur** entrantes configurées sont les identifiants et règles pour les pairs qui se lient *dans* la passerelle. Chaque entrée définit un **ID système** et un mot de passe, les **types de liaison autorisés**, et les garde-fous qui contrôlent une liaison entrante : une **liste blanche IP** des adresses sources autorisées et une **liste blanche d'adresses sources** des motifs d'adresses d'origine autorisés, plus une **limite TPS**. Les pairs serveurs sont modifiables ici de la même manière (**ajouter**, **modifier** et **supprimer**), de sorte qu'un opérateur peut intégrer un nouveau partenaire entrant, resserrer ses listes blanches, ou le révoquer. Activer et désactiver une autorisation contrôle si ce partenaire est autorisé à se lier.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct de la passerelle pour dépanner une seule passerelle (échecs de liaison, rejets d'authentification et connexions interrompues) sans quitter OmniWeb.

Surveillance

Les taux de messages, le débit et d'autres séries temporelles pour la Passerelle SMPP sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens associés

- Le **SMSC** est le cœur de messagerie auquel la passerelle transmet les messages courts.
- Le **IP-SM-GW** transporte les SMS sur IMS pour les appareils VoLTE et complète le chemin SMPP vers les pairs externes.

SMSC : Centre de Service de Messages Courts

Le **SMSC** (Centre de Service de Messages Courts) est le cœur de stockage et de transfert des SMS dans le cœur du réseau. Il **accepte** les messages du réseau (via SS7 (MAP) depuis le côté mobile, via Diameter, et via SMPP depuis les interfaces d'application). Il **achemine**, **traduit** et **livre** ensuite ces messages. Il conserve tout message qu'il ne peut pas livrer immédiatement et réessaie jusqu'à ce que le message soit livré, expire ou soit abandonné. En cours de route, il suit l'état de livraison de chaque message, traduit les numéros appelants et appelés, fédère avec des SMSCs pairs afin qu'un message puisse être remis à n'importe quel nœud capable d'atteindre le destinataire, et gère des **campagnes** SMS en masse. OmniWeb expose tout cela à partir d'une seule page par instance : état des messages en direct, emplacements des abonnés, enregistrements des interfaces, santé de Diameter et de la fédération, ensembles de règles d'acheminement et de traduction, et gestion des campagnes.

[← Guide des opérations](#)

Le SMSC est une page d'élément par instance accessible depuis la barre latérale lorsque l'on se trouve dans l'inventaire du site, avec une vue de flotte où plusieurs sont déployés. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du SMSC, de sorte qu'il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

L'onglet d'accueil est une lecture de santé sur un seul écran pour le nœud : comptes de messages actuels et état de livraison, santé des interfaces et des pairs en un coup d'œil, et une **recherche par MSISDN** qui examine à la fois les messages stockés et les emplacements des abonnés. C'est le moyen le plus rapide de répondre à la question "que se passe-t-il avec le SMS de cet abonné en ce moment" depuis une seule boîte.

Messages

Chaque message que le SMSC détient ou a traité, chaque ligne montrant les numéros d'envoi et de réception, l'**état** du message (en attente, livré, échoué, expiré, abandonné ou réponse automatique), le nombre de **tentatives de livraison**, et son âge. Vous pouvez filtrer les messages par état, par **SMSC**, et inclure le trafic **de lettres mortes** ou **non acheminé**, et rechercher par MSISDN, nom de nœud ou ID de message. Sélectionnez un message pour ouvrir ses détails, y compris le texte en clair décodé. Un opérateur peut **réacheminer** un message pour le forcer à repasser par l'acheminement, par exemple après avoir corrigé une règle d'acheminement.

Interfaces

Les **interfaces** d'application et SMPP actuellement enregistrées avec le SMSC sont les clients qui soumettent et reçoivent des messages. Chaque entrée montre son nom d'hôte, quand elle a été **dernièrement vue**, et quand son enregistrement **expire**, vous permettant de confirmer que les interfaces de traitement des messages sont connectées et que leurs enregistrements sont actifs.

Emplacements

Les **emplacements des abonnés** que le SMSC a appris sont le dernier emplacement de service connu pour chaque abonné par **IMSI** et **MSISDN**. Le SMSC utilise ces informations pour atteindre un destinataire. Vous pouvez le rechercher par IMSI ou MSISDN et le filtrer pour inclure les entrées expirées. C'est là que vous confirmez que le SMSC sait où se trouve un abonné avant de pouvoir lui livrer.

Diameter

Les connexions de pairs Diameter que le SMSC utilise pour le messaging, chaque ligne montrant le **domaine** du pair, l'**adresse IP**, le **transport**, la direction d'initiation de connexion, le **nom du produit** rapporté, les **ID d'application** négociés et l'**état de connexion**. C'est là que vous confirmez que le chemin Diameter dont dépend le SMSC est opérationnel.

Fédération

La vue de **fédération** montre comment ce SMSC coopère avec des SMSCs pairs afin qu'un message puisse être remis à n'importe quel nœud capable d'atteindre le destinataire. Elle rapporte **ce nœud**, le nombre de pairs **sains**, **dégradés** et **malades**, le nombre de **messages fédérés mis en cache** (souligné lorsqu'il est non nul), la méthode de **découverte** utilisée (domaine DNS ou pairs statiques), et un tableau par pair avec le nom du nœud, l'état, les échecs récents, le dernier contrôle de santé réussi et les interfaces que chaque pair offre. C'est le moyen le plus rapide de voir si les SMSCs dans une fédération se rejoignent.

Acheminement

Les **règles d'acheminement des SMS** qui décident où chaque message va, listées par **priorité**. Chaque règle correspond à un motif de numéro **appelant** et **appelé** (et éventuellement à un SMSC source ou un type source tel que SS7 ou circuit commuté), et se résout à une **destination** (un SMSC cible ou une recherche **ENUM**) avec une description et un état activé. Les règles sont entièrement modifiables : un opérateur peut les ajouter, les modifier, les activer, les désactiver ou les supprimer, et exporter et réimporter l'ensemble des règles.

Traductions

Les **règles de traduction de numéros** qui réécrivent les numéros appelants et appelés au fur et à mesure que les messages passent : elles normalisent les formats, appliquent des préfixes, etc. Chaque règle est listée par **priorité** avec sa correspondance appelante et appelée, un SMSC source optionnel, un drapeau **continuer** (pour que plusieurs règles puissent s'appliquer en séquence), une description et un état activé. Comme pour l'acheminement, les règles sont modifiables (ajouter, modifier, activer, désactiver, supprimer), et vous pouvez les exporter et les réimporter.

Campagnes

Les **campagnes** SMS en masse sont créées et gérées depuis cet onglet. Une **Nouvelle Campagne** est définie avec un nom et une description, un numéro **d'expéditeur**, le SMSC source, une **liste de destinataires**, un **public** (uniquement les destinataires actifs ou tout le monde dans la liste), un taux de **goutte** en messages par seconde, une fenêtre de **validité** du message, un temps **de livraison après** optionnel et le **modèle de message**. Une fois créée, une campagne est contrôlée depuis ici (**démarrer**, **mettre en pause**, **reprendre** ou **annuler**). Vous pouvez inspecter ses **cibles** pour voir l'état d'envoi et de livraison par destinataire au fur et à mesure que la campagne progresse.

Listes de Campagnes

Les **listes** de destinataires auxquelles les campagnes envoient. Les listes sont entièrement gérées ici : créez une **Nouvelle Liste de Destinataires** avec un nom, une description et un ensemble initial de destinataires, **ajoutez** plus de destinataires plus tard, modifiez ou supprimez une liste. Vous fournissez les destinataires sous forme de **CSV**, vous pouvez donc importer directement une liste de contacts existante plutôt que de l'entrer manuellement.

Test NAPTR

L'onglet **Test NAPTR** est un outil pour l'opérateur qui résout un **numéro E.164 (ou domaine) via ENUM/NAPTR DNS** pour voir comment le SMSC acheminera un message vers celui-ci. Entrez le numéro de téléphone et le **domaine ENUM** à interroger (`e164.arpa` par défaut) et soumettez. Rien n'est récupéré jusqu'à ce que vous le fassiez. Le SMSC inverse les chiffres du numéro dans la zone ENUM, recherche les enregistrements **NAPTR** publiés là-bas, et les retourne dans l'**ordre** et la **préférence**. Chaque enregistrement porte ses **drapeaux**, **service**, le **regexp** de réécriture et le **remplacement**, et le **domaine de résultat** résolu vers lequel l'enregistrement pointe le message. C'est là que vous confirmez que les données ENUM derrière une règle d'acheminement résolvent réellement un numéro vers l'URI ou le chemin que vous attendez, avant de vous y fier en production.

MWI

L'onglet **MWI** envoie une mise à jour d'**Indication de Message en Attente** pour un abonné : la notification qui définit ou efface le drapeau "messages en attente" sur un appareil, généralement après qu'un message vocal ait été laissé ou récupéré. Donnez le **MSISDN de destination** à notifier et le **MSISDN source** d'où il provient, choisissez le **type d'indication** (messagerie vocale, fax, email ou autre), et définissez si l'indicateur doit être **actif** (on) ou effacé (off), avec un **corps de message** optionnel et un **SMSC** d'origine. C'est un formulaire de soumission : la mise à jour n'est envoyée que lorsque vous la publiez. C'est le moyen direct de lever ou d'effacer l'indicateur de message en attente d'un abonné manuellement.

Journaux Système

L'onglet **Journaux Système** est la propre vue de journal API du SMSC. Vous pouvez le filtrer par **niveau** (débogage, info, avertissement, erreur) et par une **limite** sur le nombre de lignes retournées, vous permettant de récupérer uniquement les erreurs récentes ou une trace plus complète lorsque vous enquêtez sur un problème spécifique, sans quitter OmniWeb.

Plus d'outils

En plus des onglets ci-dessus, la page SMSC propose quelques outils ciblés :

- **Soumettre** : un formulaire qui envoie un SMS unique directement depuis OmniWeb (de, à et texte du message), pour tester la livraison à un destinataire spécifique.
- **Opérations** : actions de maintenance à l'échelle du nœud, y compris le nettoyage des **interfaces** enregistrées, des **messages** stockés, des règles **d'acheminement** et des règles de **traduction**. Chacune est une action destructrice et demande d'abord une confirmation.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du SMSC pour dépanner un seul nœud sans quitter OmniWeb. Pour une vue filtrée, soutenue par l'API du même nœud, utilisez les **Journaux Système** ci-dessus.

Surveillance

Le débit de messages, les taux de succès de livraison, la profondeur de la file d'attente et d'autres séries chronologiques pour le SMSC sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liés

- **HSS** : détient les données des abonnés et les informations d'acheminement contre lesquelles les livraisons du SMSC se résolvent.
- Le **DRA** : relaie le signalement Diameter que le SMSC utilise pour le messaging.
- **STP** : le chemin de signalement SS7 par lequel le SMSC échange des messages MAP avec le réseau mobile.
- Le **CSCF/TAS** : le côté IMS qui origine et termine le messaging pour les abonnés VoLTE.

Gestion et Cycle de Vie des Logiciels

OmniWeb fournit un endroit unique pour voir et gérer les logiciels fonctionnant sur l'ensemble de la flotte : versions des paquets, mises à jour disponibles et licences. Le cycle de vie des logiciels du réseau est visible depuis le même portail utilisé pour l'exploiter.

[← Retour au Guide des Opérations](#)

Page des Logiciels (Dépôt APT)

La page **Logiciels** est un navigateur de dépôt APT pour les paquets Omnitouch. Elle se connecte au serveur de dépôt APT configuré et affiche, pour les paquets qu'elle gère :

- **Paquets disponibles** dans le dépôt.
- **Versions** proposées, y compris la dernière disponible.
- **État de mise à jour** : si une version plus récente existe par rapport à celle qui est déployée.

Cela permet aux opérateurs de voir d'un coup d'œil quels composants Omnitouch ont des mises à jour en attente et quelles versions sont actuelles, fournissant ainsi le côté inventaire du cycle de vie des logiciels.

L'installation/mise à jour des paquets sur les hôtes est effectuée via les outils standard APT/`dpkg` (et est généralement automatisée via Ansible) ; OmniWeb offre la couche de visibilité sur ce qui est publié et actuel.

La page des Logiciels : chaque paquet Omnitouch avec ses dernières versions de dépôt et de cache et un indicateur de synchronisation qui signale où une version plus récente est publiée que celle qui est mise en cache/déployée (ici `omni-upf` et `omni-msc` sont hors synchronisation).



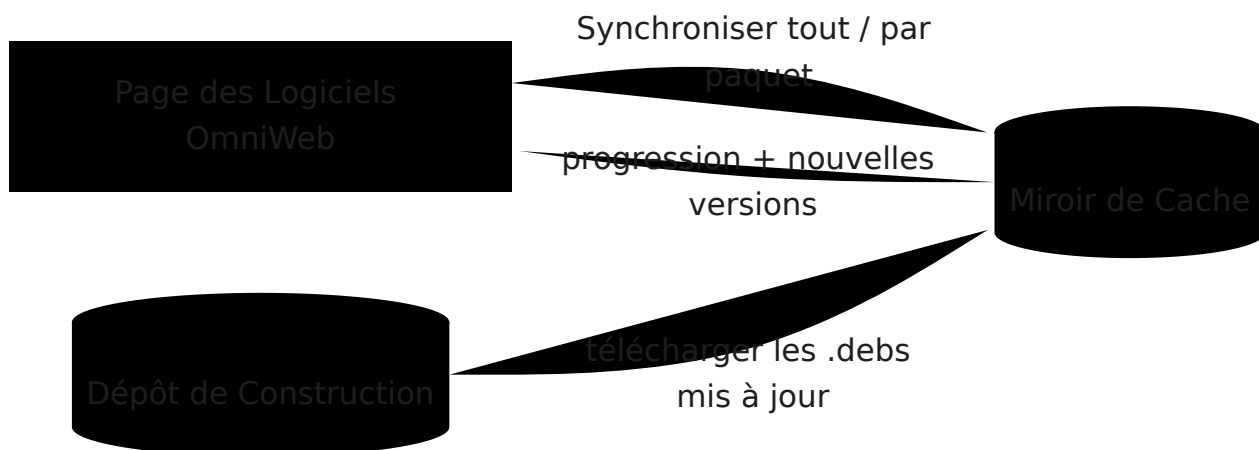
Synchronisation des Paquets dans le Cache

Les déploiements qui exécutent un **miroir de cache APT** sur site (pour les sites isolés ou à bande passante limitée) conservent une copie locale des paquets publiés sur le dépôt de construction. Avec le temps, le cache prend du retard. La page des Logiciels signale chaque paquet qui est **hors synchronisation** (une version plus récente est publiée que celle qui est mise en cache). Depuis la même page, vous pouvez tirer ces mises à jour dans le cache sans quitter OmniWeb :

- **Synchroniser tout** : tirer chaque paquet mis à jour du dépôt vers le cache.
- **Synchroniser** (par ligne) : tirer juste un paquet. Cliquez sur plusieurs et ils **s'alignent** : ils se téléchargent un après l'autre, et OmniWeb régénère l'index des paquets **une seule fois** à la fin (pas par paquet), de sorte que le cache n'est jamais laissé à moitié mis à jour.

Pendant qu'une synchronisation est en cours, la page montre la progression en direct (quel paquet est en cours de téléchargement, combien sont en attente, et un journal de progression en continu). Elle actualise la comparaison des versions lorsqu'elle se termine.

Une synchronisation en cours : `omni-msc` en cours de téléchargement avec `omni-upf` en attente, la bannière de phase, et le journal en direct. Lorsque la file d'attente se vide, l'index du cache est régénéré une fois et l'état de synchronisation est mis à jour.



La synchronisation s'exécute sur le miroir de cache lui-même (OmniWeb l'initie et diffuse la progression) ; le miroir tire les `.deb` mis à jour du dépôt de construction et régénère son index. Les hôtes sur le site installent ensuite les paquets mis à jour depuis le cache comme d'habitude.

Versionnage

OmniWeb rapporte sa propre version de construction (version, commit et date de construction) afin que les opérateurs puissent confirmer exactement quelle version du portail ils exécutent. C'est le point de référence lors du signalement de problèmes ou de la coordination d'une mise à niveau du portail lui-même.

Gestion des Licences

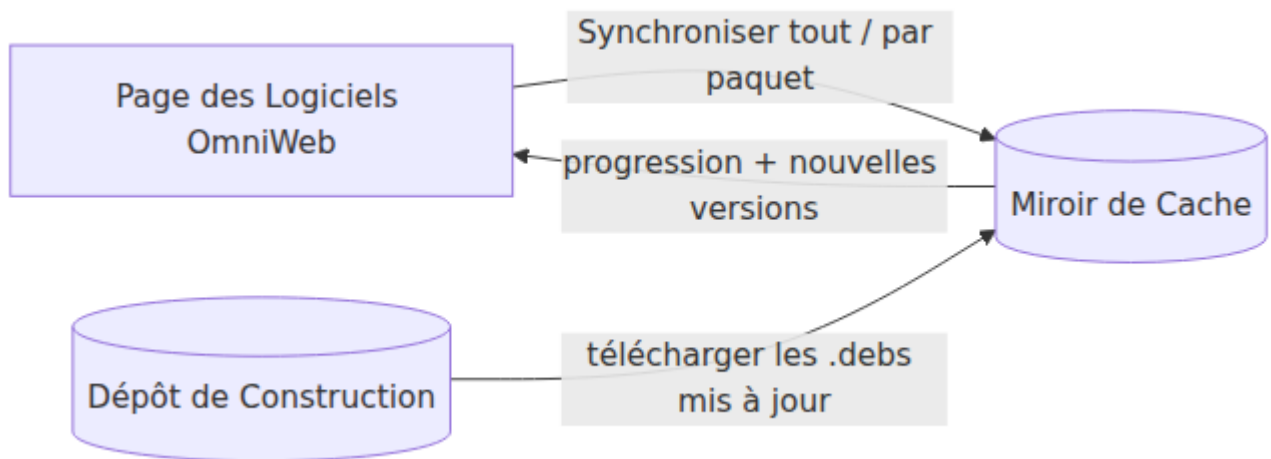
Le **Serveur de Licences** est administré via OmniWeb comme tout autre élément, en utilisant les mêmes modèles génériques (voir [Opérations Courantes](#)). Il présente :

Aperçu du Serveur de Licences : état actuel de la licence et validité, y compris l'état de temps de confiance.

Vue	Description
Aperçu	État actuel de la licence, dates de validité et droits d'utilisation des fonctionnalités.
Journaux de Demande	Demandes de licence historiques, avec filtrage. Cela est utile pour auditer ce qui a été vérifié et quand.
Requête	Rechercher l'état de la licence pour un licencié/produit spécifique à la demande.

La gestion des licences s'intègre dans le cycle de vie des logiciels : les droits déterminent quels produits et fonctionnalités un déploiement est autorisé à exécuter, et les journaux de demande fournissent une trace d'audit de l'activité de licence au fil du temps.

Cycle de Vie en Un Coup d'Œil



1. **Voir ce qui est disponible** : la page des Logiciels montre les mises à jour en attente.
2. **Confirmer les droits** : le Serveur de Licences montre ce pour quoi le déploiement est licencié.
3. **Appliquer** : les mises à niveau s'exécutent via APT/Ansible sur les hôtes.
4. **Vérifier** : confirmer les versions, puis surveiller les **Journaux** et **Tableaux de Bord** pour confirmer un résultat sain.

SS7 : Pile de signalisation (STP / HLR / IP-SM-GW / CAMEL-GW)

La **pile SS7** (OmniSS7) termine le transport SIGTRAN (associations SCTP transportant **M3UA**) et route le trafic SS7/MAP à travers le réseau de signalisation. Un seul service fournit l'ensemble de la pile, et OmniWeb la présente sous forme de quatre vues d'éléments pour ses différents rôles : **STP** (Point de Transfert de Signalisation, le routeur SS7), **HLR** (Registre de Localisation Domiciliaire), **IP-SM-GW** (Passerelle de Messages Courts IP) et **CAMEL-GW** (Passerelle CAMEL). Les quatre sont soutenus par le même client partagé, donc le transport et le routage SIGTRAN qu'ils partagent sont la même pile sous-jacente vue sous différents angles.

[← Guide des opérations](#)

Chaque vue est une page d'élément par instance accessible depuis la barre latérale lorsque une pile SS7 fonctionne dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API de la pile, donc il reste derrière la seule passerelle authentifiée. Les réponses reviennent dans une enveloppe `{status, response}`. Le lien de documentation dans l'en-tête de chaque page d'élément (le bouton d'aide contextuelle) ouvre cette page. Chaque vue est organisée en onglets. Les taux de messages et d'autres séries temporelles sont présentés sous forme de tableaux de bord Grafana accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

La pile en un coup d'œil

Le transport SIGTRAN sous-jacent à chaque rôle est le même, donc les onglets **Pairs** et **Connexions SCTP** apparaissent dans les quatre vues et lisent les

mêmes données.

L'onglet **Pairs** rapporte l'état des pairs M3UA (`/api/m3ua-status`) : chaque pair M3UA/M2PA, avec son **état ASP**, **état d'association**, **points de terminaison** locaux et distants, **contexte de routage**, protocole et mode, et statistiques de **temps de disponibilité** par pair. C'est ici que vous confirmez que le processus de serveur d'application de chaque voisin de signalisation est opérationnel et en service.

L'onglet **Connexions SCTP** liste le transport sous-jacent (`/api/sctp-connections`) : chaque association SCTP avec son **état**, **rôle**, **IP/port** locaux et distants, comptes de **flux** entrants et sortants, **bytes** et **messages** envoyés et reçus, **dernière activité**, et toute dernière erreur, plus les totaux agrégés sur toutes les connexions. Lorsqu'un pair montre qu'il est hors service, vérifiez ce niveau pour voir si l'association SCTP elle-même est établie.

STP : routage

La vue **STP** est le routeur SS7. Aux côtés des onglets de transport partagés, elle comporte l'onglet **Routage**, plus **Carte du réseau**, **Aperçu** et un fil d'**Événements SS7**.

L'onglet **Routage** montre la configuration complète de routage M3UA (/api/routing) : les **pairs** configurés, les **routes par code de point (PC)** et les **routes par titre global (GT)**.

- Les **routes par code de point** dirigent le trafic vers un code de point de destination (dest_pc) via un **pair** cible, avec un **indicateur de réseau**, un **masque** de code de point et une **priorité**. Les opérateurs peuvent **ajouter** une route PC (POST /api/routing/pc-routes, en donnant le code de point de destination et le pair cible) et **supprimer** une (DELETE /api/routing/pc-routes/{dest_pc}-{peer_id}).
- Les **routes par titre global** correspondent à un **préfixe** GT et transmettent à un **pair** cible avec une **priorité** et des détails optionnels sur le SSN, le type de traduction et la nature de l'adresse, ainsi qu'une description. Les opérateurs peuvent **ajouter** une route GT (POST /api/routing/gt-routes, en donnant le préfixe et le pair cible) et **supprimer** une (DELETE /api/routing/gt-routes/{prefix}:{peer_id}).

C'est ici que vous confirmez et ajustez comment le STP transmet les messages SS7 vers chaque destination.

HLR

La vue **HLR** met en avant les abonnés actifs du registre et le lien vers le backend HLR, aux côtés des onglets de transport partagés, d'un **Aperçu** et d'un onglet **Client SS7**.

L'onglet **Abonnés** liste le registre des abonnés actifs (`/api/subscribers`) : chaque abonné qui a envoyé une **UpdateLocation** et pas encore une **CancelLocation**, chaque ligne montrant **IMSI**, **VLR**, **MSC** de service, heure d'enregistrement et **durée**, avec des comptes de VLRs et MSCs uniques. Un opérateur peut **vider** tous les abonnés actifs suivis (`DELETE /api/subscribers`) pour réinitialiser la vue du registre.

L'onglet **Liens HLR** vérifie la connectivité à l'API HLR configurée (`/api/hlr-links`) : l'**état** (en service, dégradé ou hors service), la **latence** mesurée, la **version** rapportée et l'**hôte** cible. C'est le moyen le plus rapide de confirmer que la pile peut atteindre le backend HLR.

IP-SM-GW

La vue **IP-SM-GW** est la passerelle de messages courts. Elle gère le traqueur d'abonnés SMSc et le lien vers le backend SMSc, aux côtés des onglets de transport partagés et d'un **Aperçu**.

L'onglet **Liens SMSc** vérifie la connectivité à l'API SMSc configurée (`/api/smsc-links`) : **état** (en service, dégradé ou hors service), **latence**, **version** rapportée et **hôte** cible. C'est l'équivalent du chemin SMS pour la vérification du lien HLR.

L'onglet **Abonnés SMSc** liste les abonnés suivis par le traqueur d'abonnés SMSc (`/api/smsc-subscribers`) : chacun avec **MSISDN**, **IMSI**, **HLR GT** et **VLR GT**, **messages envoyés** et **reçus**, état et dernière mise à jour, plus les comptes actifs/échoués et HLR uniques. Un opérateur peut **vider** tous les abonnés SMSc suivis (`DELETE /api/smsc-subscribers`).

CAMEL-GW

La vue **CAMEL-GW** met en avant les sessions CAMEL que la passerelle exécute, aux côtés des onglets de transport partagés et d'un **Aperçu**.

L'onglet **Sessions CAMEL** liste toutes les sessions CAMEL actives gérées par la passerelle (`/api/camel-sessions`) : l'**état** de chaque session, la **version CAP**, la **clé de service**, **IMSI**, numéros **appelants** et **appelés**, heure de début et **durée**, avec des comptes de sessions initiées et répondues. C'est ici que vous regardez le traitement des appels CAMEL en direct en temps réel.

Statut

Le point de terminaison **Statut** (`/api/status`) rapporte la santé globale du nœud que les onglets **Aperçu** résument : l'identité du nœud et le **rôle**, si le service est **ok**, son **temps de disponibilité**, et un résumé des pairs indiquant combien de pairs de signalisation sont actifs sur le total. C'est la première lecture pour confirmer que la pile fonctionne et que ses pairs sont en service.

Liens connexes

- **STP** : l'élément de routage SS7 (routes par code de point et par titre global).
- **HLR** : l'élément Registre de Localisation Domiciliaire (registre des abonnés actifs et lien HLR).
- **IP-SM-GW** : l'élément Passerelle de Messages Courts IP (abonnés SMSc et lien).
- **CAMEL-GW** : l'élément Passerelle CAMEL (sessions CAMEL en direct).
- Le **MSC/VLR** déclenche la mise à jour de la localisation et la signalisation CAMEL que cette pile route et suit.
- Le **SMSc** est le backend contre lequel le lien SMSc de l'IP-SM-GW et le traqueur d'abonnés se résolvent.
- [← Guide des opérations](#)

Client SIM Toolkit (STK)

OmniWeb inclut un client **SIM Toolkit** interactif. Utilisez-le pour naviguer et piloter les applets STK sur n'importe quelle carte SIM physique insérée dans un lecteur PC/SC connecté à l'agent. Le client STK envoie un profil de terminal à la carte, puis présente chaque commande proactive sous forme d'écran interactif. Vous répondez comme le ferait un terminal, permettant ainsi à l'applet de passer à l'étape suivante.

Cet outil se trouve dans la barre latérale sous **SIMs - SIM Toolkit**, aux côtés de l'**APDU Terminal** et de l'**Explorateur de Système de Fichiers SIM**.

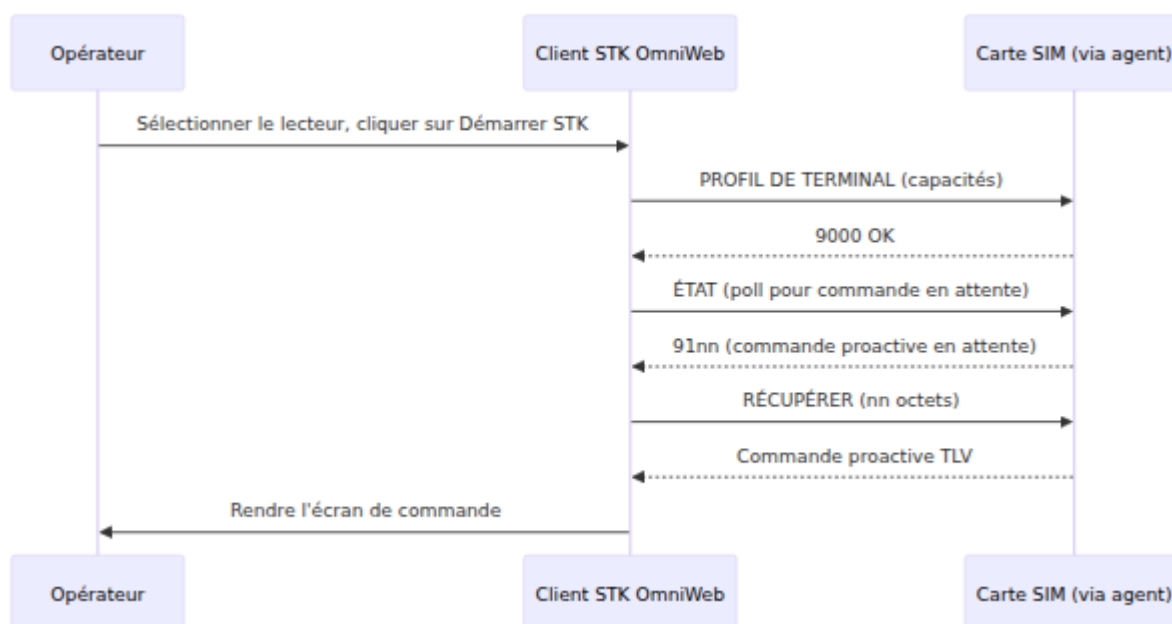
Qu'est-ce que le SIM Toolkit ?

Le SIM Application Toolkit (STK) est une norme définie dans **ETSI TS 102.223** qui permet à une carte SIM d'initier des actions sur le terminal. Un applet SIM émet des **commandes proactives** - des demandes telles que "afficher ce texte" ou "montrer ce menu" - et le terminal répond avec la sélection ou l'entrée de l'utilisateur. Les cas d'utilisation courants incluent les menus de recharge d'opérateur, les demandes de solde, les déclencheurs de configuration OTA et les portails de services résidents sur la SIM.

Exigences

- Un lecteur avec une carte SIM contenant un applet STK.
 - La permission de **contrôle de la banque SIM**. Sans cela, vous pouvez voir les lecteurs mais ne pouvez pas ouvrir de sessions ou piloter des cartes.
 - Le lecteur ne doit pas être occupé par un autre outil. Si c'est le cas, OmniWeb montre qui le détient et propose une option **Prendre le contrôle**. Prendre le contrôle annule l'autre session.
-

Ouverture d'une session



1. Sélectionnez le lecteur dans le menu déroulant **Lecteur**. Seuls les lecteurs avec une carte présente apparaissent.
2. Cliquez sur **Démarrer STK**. OmniWeb ouvre une session exclusive sur la carte, envoie un profil de terminal et interroge la première commande proactive.
3. Interagissez avec chaque écran au fur et à mesure qu'il apparaît. OmniWeb envoie une RÉPONSE DE TERMINAL après chaque étape et récupère automatiquement la commande suivante.
4. La session se termine lorsque la carte émet une commande de FIN DE SESSION, ou lorsque vous cliquez sur **Fin de session**.

Écrans de commande

OmniWeb rend chaque commande proactive sous forme d'écran interactif. Le tableau ci-dessous répertorie les types de commandes pris en charge.

Commande	Description	Action de l'utilisateur
AFFICHER LE TEXTE	La carte affiche un message.	Cliquez sur OK pour accuser réception, ou Retour pour revenir à l'étape précédente.
SÉLECTIONNER UN ÉLÉMENT / CONFIGURER UN MENU	La carte présente une liste numérotée d'options.	Cliquez sur l'élément que vous souhaitez sélectionner.
OBTENIR UNE TOUCHE	La carte demande une seule frappe.	Tapez un caractère et cliquez sur Envoyer , ou choisissez Oui / Non pour les invites oui-non.
OBTENIR UNE ENTRÉE	La carte demande une chaîne de texte d'une longueur spécifiée.	Tapez le texte et cliquez sur Envoyer . Le champ indique le nombre minimum et maximum de caractères.

Si la carte émet un type de commande que le client ne rend pas de manière interactive (par exemple, ENVOYER UN MESSAGE COURT ou CONFIGURER UN APPEL), OmniWeb affiche les données de commande brutes et envoie automatiquement une réponse **OK** afin que la session puisse continuer.

Historique de session

Un panneau **Historique de session** apparaît sur le côté droit de l'écran une fois que vous commencez à interagir. Il enregistre chaque type de commande et la réponse que vous avez donnée (élément sélectionné, texte d'entrée ou OK/Retour). Utilisez-le pour retracer le chemin à travers un arbre de menu.

Fin de session

La session se termine de trois manières :

- **Fin initiée par la carte** : l'applet émet une commande proactive de FIN DE SESSION. OmniWeb ferme automatiquement la session et affiche un message de complétion.
- **Fin initiée par l'opérateur** : cliquez sur **Fin de session** à tout moment. OmniWeb envoie un résultat de session terminée à la carte et ferme la session du lecteur.
- **Navigation en arrière au-delà de la racine** : cliquer sur **Retour** sur le premier écran envoie un résultat de mouvement en arrière à la carte. La carte décide comment répondre - elle peut afficher un écran précédent ou mettre fin à la session.

Après la fin de la session, le lecteur redevient disponible pour d'autres outils.

Relation avec d'autres outils SIM

Outil	Objectif
SIM Toolkit (cette page)	Piloter les applets STK de manière interactive.
APDU Terminal	Envoyer des APDUs bruts manuellement, un à la fois ou dans une session persistante.
Explorateur de Système de Fichiers SIM	Parcourir et éditer le système de fichiers de la carte.
Journal APDU	Suivre passivement les commandes entre un modem et une SIM distante.

Dépannage

Démarrer STK échoue avec "ÉCHEC DU PROFIL DE TERMINAL"

La carte a rejeté le profil de terminal ou l'agent n'a pas pu atteindre la carte. Vérifiez que :

- La carte est correctement insérée dans le lecteur.
- Aucun autre outil ne détient le lecteur. Si c'est le cas, utilisez **Prendre le contrôle**.
- L'agent qui possède le lecteur est en ligne (vérifiez la page de la Banque SIM).

La session s'arrête après la première commande

Certaines applets SIM terminent la session immédiatement si le profil de terminal ne déclare pas les capacités nécessaires à l'applet. Le client déclare un large éventail de capacités, mais certaines cartes vérifient des bits spécifiques. Si cela se produit, utilisez l'**APDU Terminal** en mode session pour envoyer PROFIL DE TERMINAL et RÉCUPÉRER manuellement et examiner les données de commande proactive brutes.

Retour renvoie un écran inattendu

L'action **Retour** envoie le code de résultat 0x11 (mouvement en arrière) à la carte. La carte contrôle ce que cela signifie. Certaines applets retournent au menu précédent ; d'autres redémarrent la session depuis le menu racine ; quelques-unes ignorent le mouvement en arrière et réémettent la même commande.

OBTENIR UNE ENTRÉE rejette mon texte

La carte définit un nombre minimum et maximum de caractères. Le champ de saisie affiche les deux. Si la carte restreint également aux chiffres uniquement,

l'étiquette du champ indique **chiffres uniquement**. Entrez une valeur dans la plage requise.

TAS : Serveur d'Applications de Téléphonie

Le **TAS** (Serveur d'Applications de Téléphonie) est le serveur d'applications IMS qui fournit l'expérience téléphonique de l'abonné. Il gère le **contrôle des appels** et les **services supplémentaires** (renvoi d'appel, barrages, attente, mise en attente, etc.), organise des **conférences**, prend et lit des **messages vocaux**, enregistre des **CDR** pour chaque appel, résout le **routage** et la traduction de numéros, et communique avec le **OCS** via Diameter afin que les appels soient facturés en temps réel. Là où le CSCF décide *comment* un appel est signalé, le TAS décide *ce que* le service fait. OmniWeb affiche ses appels en direct, les enregistrements d'abonnés, les passerelles, les pairs Diameter et la configuration sur une page d'élément. Les graphiques de volume d'appels et de tendances se trouvent sur les tableaux de bord Grafana accessibles depuis la même page.

[← Guide des opérations](#)

Le TAS est une page d'élément par instance accessible depuis la barre latérale lors d'une exécution dans l'inventaire du site. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API du TAS, de sorte qu'il reste derrière la seule passerelle authentifiée. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Aperçu

L'onglet de destination est une lecture de santé sur écran unique pour le serveur d'applications : le nombre d'**appels actifs**, d'**abonnés enregistrés**, de **conférences** en cours et de **messages vocaux** stockés, la santé des pairs **Diameter** et des **passerelles SIP**, et le statut de la **licence**. C'est le moyen le plus rapide de confirmer que le TAS est opérationnel et traite du trafic.

Appels Actifs

Chaque appel actuellement en cours, chaque ligne montrant les parties appelantes et appelées, la **direction**, l'**état** de l'appel et sa **durée**.

Sélectionnez un appel pour ouvrir ses détails afin de voir comment un appel spécifique est legged et où il se situe dans le plan de numérotation. C'est le premier endroit à consulter lorsqu'un abonné signale un appel en difficulté en ce moment.

CDR

Les **enregistrements de détails d'appels** que le TAS a écrits : une ligne par appel complété, avec les parties, l'**heure de début**, la **durée** et la **disposition**. Ouvrez n'importe quel enregistrement pour ses détails complets. Les CDR sont la comptabilité et la traçabilité des dépannages après coup : utilisez-les pour confirmer qu'un appel a eu lieu, combien de temps il a duré et comment il s'est terminé.

Abonnés

Les **enregistrements** d'abonnés que le TAS connaît, chacun avec l'**identité** de l'abonné, l'**état** d'enregistrement et le **contact** actuel. Ouvrez un abonné pour les détails complets de l'enregistrement. C'est ici que vous confirmez qu'un abonné est enregistré sur le serveur d'applications avant de chercher pourquoi un service ne fonctionne pas pour lui.

Diameter

Les **pairs Diameter** auxquels le TAS se connecte, y compris le chemin vers l'**OCS** pour la facturation et le **HSS** pour les données utilisateur, avec le nom d'hôte et l'**état de connexion** de chaque pair. Ouvrez un pair pour ses détails. Lorsque la facturation ou les recherches d'abonnés échouent, cet onglet est l'endroit où vous confirmez que les chemins Diameter sous-jacents sont opérationnels.

Passerelles

Les **passerelles SIP** que le TAS utilise pour atteindre d'autres réseaux et trunks, chacune montrant son nom et son **statut** actuel. Ouvrez une passerelle pour ses détails. Utilisez cet onglet pour confirmer que les passerelles d'interconnexion sont enregistrées et disponibles avant de diagnostiquer des appels échoués hors réseau.

Conférences

Les **conférences** actives et leurs participants. Ouvrez une conférence pour voir qui y participe, et agissez sur place : **verrouillez** ou **déverrouillez** le pont, **expulsez** un participant, activez ou désactivez la **vidéo**, ou **détruisez** complètement la conférence. C'est le contrôle en direct de l'opérateur sur un pont en cours.

Messagerie Vocale

Les enregistrements de **messagerie vocale** stockés, par abonné. Chaque enregistrement peut être **supprimé** individuellement, par exemple pour effacer un message laissé par erreur ou pour libérer une boîte vocale pleine.

Test OCS

Les **sessions OCS (Système de Facturation en Ligne)** actives que le TAS maintient, afin que vous puissiez voir quels appels utilisent un solde en temps réel. Une session de facturation individuelle peut être **terminée** depuis ici. Cela est utile pour libérer une session qui est restée ouverte après que son appel a disparu.

Routage

Les **modèles de plan de numérotation** que le TAS utilise pour router les appels. La liste montre chaque modèle ; ouvrez-en un pour lire son contenu. C'est la référence pour savoir comment les numéros sont appariés et où les appels sont envoyés. Lisez-le aux côtés de l'outil **Traduction de Numéros** pour confirmer qu'un numéro donné est routé comme prévu.

Configuration

La **configuration de l'application** que le TAS exécute, regroupée par application. Ouvrez une entrée pour lire ses paramètres. C'est la référence de lecture pour confirmer que le serveur est configuré comme prévu sans quitter OmniWeb.

Invites

Les **enregistrements d'invites de synthèse vocale** que le TAS joue aux appelants, les annonces et les invites de menu, avec le statut de chacune. Utilisez cet onglet pour confirmer que les invites attendues sont présentes et rendues.

Outils

En plus des onglets ci-dessus, la page TAS comporte un ensemble d'outils à la demande pour valider le routage et les données des abonnés. Chacun prend un petit formulaire, exécute la demande contre le serveur d'applications via le proxy OmniWeb, et affiche le résultat sur place.

Simulateur d'Appels

Passe un appel de test à travers le TAS pour valider le routage et les médias. Entrez un **numéro de destination** (et éventuellement un numéro source, une adresse IP source et une disposition forcée). Le simulateur fait passer l'appel à travers le plan de numérotation **sans faire sonner personne**. Il renvoie le **type d'appel** résolu (MT, MO ou d'urgence), la décision sur le réseau, chaque **variable de plan de numérotation** qu'il a définie, et une liste étape par étape de **notes de traitement**, afin que vous puissiez voir exactement comment un numéro serait traité avant qu'un véritable appel ne soit passé. L'autorisation OCS et la recherche HLR peuvent chacune être ignorées pour isoler une étape. Une action d'**appel de test d'écho** distincte fait sonner une destination et renvoie l'audio de la partie, ce qui confirme le chemin vocal en direct vers un combiné.

Requête Sh

Interroge le HSS via l'interface **Sh** pour les données utilisateur d'un abonné. Entrez l'**identité publique** de l'abonné et choisissez la **référence de données** à récupérer, des **données de référentiel** complètes à un élément spécifique tel que l'état utilisateur IMS, le nom du S-CSCF de service, les critères de filtre initiaux, le MSISDN ou l'IMSI. L'outil renvoie les données de service transparentes et de référentiel que le HSS détient. Utilisez-le pour confirmer ce que le serveur d'applications voit pour un abonné lorsque qu'un service ne se comporte pas comme prévu.

Recherche HLR

Effectue une **recherche HLR** via SS7 MAP (une demande d'envoi d'informations de routage) pour résoudre l'état de routage et d'itinérance d'un abonné. Entrez le **MSISDN** au format international et l'outil renvoie la réponse HLR ainsi que les **variables de plan de numérotation** que le résultat définirait sur un appel. C'est ainsi que vous confirmez l'emplacement réseau actuel d'un numéro avant de diagnostiquer pourquoi les appels vers celui-ci sont routés de la manière dont ils le sont.

Traduction de Numéros

Teste comment un numéro composé est **normalisé et traduit** par les règles de routage du TAS. Entrez un **code pays**, le **numéro de téléphone** et une **disposition** optionnelle. L'outil renvoie le numéro traduit que le plan de numérotation utiliserait. Lisez-le aux côtés de l'onglet **Routage** pour confirmer qu'un numéro donné est apparié et réécrit comme prévu.

ESL

Une **console** interactive pour émettre des commandes de style serveur multimédia au moteur TAS pour des diagnostics. Tapez une commande et appuyez sur Entrée. La sortie est imprimée dans la console, et les flèches Haut/Bas rappellent les commandes précédentes. Des commandes d'exemple telles que `status`, `sofia status`, `show channels` et `show registrations` sont proposées sous forme de puces à un clic. C'est la vue de plus bas niveau du moteur en cours d'exécution, pour confirmer les canaux en direct, l'état des passerelles et les enregistrements directement.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct du TAS pour dépanner un seul serveur d'applications sans quitter OmniWeb.

Tableaux de bord de surveillance

Les volumes d'appels, les compteurs par service et d'autres séries temporelles pour le TAS sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page d'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liens Connexes

- Le **CSCF** signale les appels auxquels le TAS applique des services. Les deux ensemble fournissent la voix IMS.
- Le **HSS** détient les données d'abonné et les données utilisateur Sh que le TAS résout.
- L'**OCS** évalue et facture les appels du TAS en temps réel via Diameter.
- Le **DRA** relaie le signalement Diameter du TAS (Sh, Gy) à ces pairs.

Appareils de Test

Appareils de Test transforme de vrais smartphones Android situés à distance en une ferme de test contrôlable à distance. Depuis OmniWeb, vous pouvez voir l'écran d'un téléphone en direct, le contrôler (toucher, glisser, taper, touches matérielles), passer des appels et envoyer des SMS, et exécuter des vérifications de santé programmées. Ces vérifications couvrent l'enregistrement VoLTE, le signal et la connectivité. OmniWeb exporte leurs résultats de réussite/échec vers Prometheus pour les alertes et les tableaux de bord.

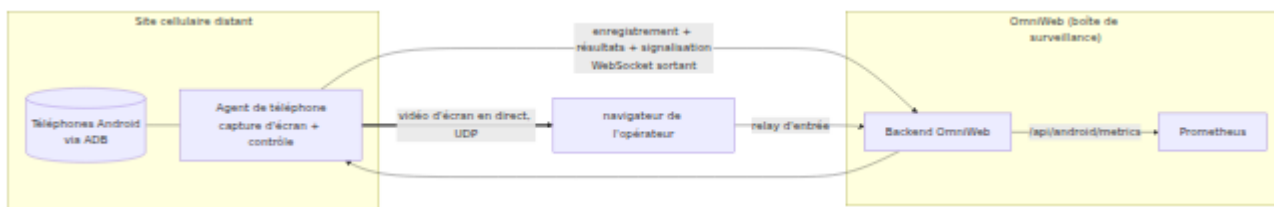
[← Retour au Guide des Opérations](#)

Il existe pour répondre à la question qu'un NOC ne cesse de poser à propos d'un site cellulaire distant : *"un vrai téléphone fonctionne-t-il réellement sur ce réseau en ce moment ?"* Le téléphone doit être enregistré pour VoLTE et capable d'appeler, d'envoyer des SMS et d'accéder à Internet. Personne n'a besoin de se rendre sur le site.

Architecture

Chaque hôte avec des téléphones branchés via ADB exécute un **agent** léger. L'agent compose vers le central OmniWeb, donc les sites derrière NAT n'ont pas besoin d'accès entrant. La vidéo en direct utilise **WebRTC** (UDP) afin de mieux survivre à des liens avec perte et à forte latence que le partage d'écran TCP. Central relaye l'entrée et les résultats des tests.

Les chemins réseau comptent. L'interface web, l'entrée et la configuration des appels ("signalisation") passent par le plan de contrôle via HTTPS vers le serveur OmniWeb. Cependant, les flux vidéo d'écran en direct **passent directement entre le navigateur de l'opérateur et l'hôte de l'agent via UDP**. Ils ne passent pas par le serveur. Si un navigateur peut atteindre le serveur mais pas l'hôte de l'agent via UDP, la console reste bloquée sur "Connexion...". Consultez [Exigences Réseau](#) pour la règle de pare-feu à demander et comment reconnaître le problème.



Composant	Rôle
Agent de téléphone	Découvre les appareils ADB, capture l'écran, injecte l'entrée, exécute des scripts de test d'hôte. Un par site ; installé par le rôle Ansible <code>device_tester</code> .
OmnWeb central	Registre des appareils, relais de signalisation WebRTC, dispatch de scripts, historique des résultats, métriques Prometheus.
Prometheus	Récupère les résultats de tests programmés depuis <code>/api/android/metrics</code> .

Types d'appareils

La ferme n'est plus uniquement composée de téléphones. Chaque appareil connecté est l'un des trois types, détectés automatiquement par l'agent et affichés avec leur propre badge (et le logo robot Android pour les téléphones) dans la flotte :

Type	Ce que c'est	Console
Téléphone Android	Un appareil normal (Android 5.0+ / API 21+) via ADB	Écran en direct + contrôle complet
Modem USB	Un module cellulaire qui expose des ports AT (par exemple, Quectel EP06)	Console cellulaire pilotée par AT : statut, appels, SMS, verrouillage de cellule, VoLTE
Dongle Android ancien	Un dongle LTE bon marché exécutant un ancien Android (API < 21, par exemple, UZ801) trop vieux pour la vue d'écran en direct	Vue screencap basée sur le polling + contrôle
Simulateur RAN UE	Un UE virtuel du Simulateur RAN , sans matériel	Panneau de contrôle UE : attacher/détacher, inactif, hors couverture, enregistrer IMS, SMS, appels

Cliquer sur un appareil ouvre la console appropriée à son type. À l'intérieur de n'importe quelle console, le bouton **Changer de téléphone** (en haut à droite) permet de passer à un autre appareil sans revenir à la grille de la flotte.

UE simulés du Simulateur RAN apparaissent dans la flotte étiquetés comme simulateurs, vous permettant de contrôler des abonnés émulés aux côtés de vrais smartphones. Le filtre Appareils de Test vous permet de restreindre à seulement les UE du Simulateur RAN. Ils utilisent le **même panneau de contrôle UE** montré dans la propre carte réseau du Simulateur RAN, donc il y a un seul endroit pour attacher, rester inactif, sortir de la couverture, s'enregistrer à IMS et envoyer des SMS/appels. Consultez **Simulateur RAN** pour le cycle de vie complet de l'UE.

Ajouter un appareil à un site

Un appareil rejoint la flotte automatiquement une fois que l'**hôte de l'agent** à ce site peut le voir via ADB. Il y a deux étapes. D'abord, activez ADB sur le smartphone. Ensuite, si l'agent fonctionne dans une VM ou un conteneur, passez le périphérique USB à travers.

1. Activer ADB sur le téléphone

1. Sur le smartphone, ouvrez **Paramètres** → **À propos du téléphone** et appuyez sept fois sur **Numéro de build** pour déverrouiller **Options de développement**.
2. Dans **Paramètres** → **Système** → **Options de développement**, activez **Débogage USB**.
3. Branchez le téléphone à l'hôte de l'agent avec un câble USB **capable de transférer des données**.
4. Le téléphone affiche une invite *"Autoriser le débogage USB ?"* avec la clé RSA de l'hôte. Cochez **Toujours autoriser à partir de cet ordinateur** et acceptez. (Sans la coche, l'invite revient chaque fois qu'il se reconnecte et l'appareil apparaît comme `non autorisé`.)

Un smartphone normal n'a besoin de rien de plus. Les scripts de test et l'écran en direct n'utilisent que l'ADB standard. Gardez l'écran déverrouillé pour la première connexion afin que l'invite puisse être acceptée.

2. Passer le périphérique USB à l'hôte de l'agent

Ignorez ceci si l'agent fonctionne sur du matériel nu. Si l'hôte de l'agent est une machine virtuelle ou un conteneur, l'hyperviseur possède le port USB, donc vous devez transférer le périphérique :

Plateforme	Comment transférer le périphérique
Proxmox (VM)	<code>qm set <vmid> -usbN host=<bus>-<port></code> pour lier un port physique (le mappage survit au changement de téléphones sur ce port), ou <code>host=<vendor>:<product></code> pour suivre un périphérique spécifique. Trouvez les identifiants avec <code>lsusb</code> sur l'hôte Proxmox.
Proxmox (conteneur LXC)	Ajoutez à <code>/etc/pve/lxc/<ctid>.conf</code> : une autorisation de groupe de périphériques pour USB (<code>lxc.cgroup2.devices.allow: c 189:* rwm</code>) et un montage de liaison du bus USB (<code>lxc.mount.entry: /dev/bus/usb/<bus> dev/bus/usb/<bus> none bind,optional,create=dir</code>), puis redémarrez le conteneur. Rebrancher un périphérique sur un bus différent nécessite que le bus correspondant soit monté.
VMware	Avec la VM en cours d'exécution, VM → Périphériques amovibles → &lt;phone> → Connecter (ou ajoutez un contrôleur USB et attachez le périphérique dans les paramètres de la VM).

Les modems USB et les dongles Android anciens se transfèrent de la même manière. Ils apparaissent comme la même classe de périphérique USB, donc un bus qui est passé à travers transporte des téléphones, des modems et des dongles.

3. Confirmer qu'il apparaît

Sur l'hôte de l'agent, `adb devices` devrait lister le smartphone comme `device` (pas `unauthorized` ou `offline`). Dans quelques secondes, il apparaît dans la **Vue de la Flotte** pour ce site. S'il n'apparaît pas, consultez [Dépannage](#).

Vue de la Flotte

La vue **Appareils de Test** liste chaque smartphone connecté à travers tous les sites, regroupés par site. Chaque carte montre le modèle, le fabricant, la version Android, la résolution d'écran, l'opérateur réseau, la batterie et la version. D'un coup d'œil, vous pouvez voir quels téléphones sont en ligne et en bonne santé.

La flotte regroupe les appareils par site (par exemple, "Site Cellulaire 12", "Laboratoire Nord"). Chaque carte montre le statut en direct, la batterie et l'opérateur. Sélectionnez des téléphones et un script pour étendre un test à travers eux. Cliquez sur une carte pour ouvrir sa console.

Étiquetage d'un appareil. Le crayon sur une carte de flotte ouvre **Modifier les métadonnées de l'appareil**, où vous pouvez donner un **nom** amical à un appareil et enregistrer son **opérateur**, **IMSI** et **MSISDN**. Ceux-ci sont assignés par l'opérateur (les Android modernes cachent l'IMSI/MSISDN de l'ADB) et restent avec l'appareil même lorsqu'il est hors ligne. Le nom est ce qui apparaît dans les en-têtes de console et les sélecteurs d'appareils.

L'entrée **Appareils de Test** de la barre latérale s'agrandit pour montrer chaque site (avec un compte d'appareils), la vue **Agents**, la bibliothèque de scripts, le planificateur et les outils d'appareil, vous permettant de sauter directement là où vous en avez besoin.

Exécution de tests sur plusieurs appareils

Sélectionnez un ou plusieurs téléphones, choisissez un script, et **Exécuter sur sélectionné** l'étend en parallèle. Les résultats s'affichent dans un tableau, une ligne par appareil avec un badge de réussite/échec, un code de sortie, une durée et une sortie extensible.

Agents

La vue **Agents** (barre latérale → Appareils de Test → Agents) liste chaque banc connecté à ce serveur, une ligne par hôte de site, avec son statut en ligne, son IP, les appareils qu'il transporte, quand il s'est enregistré, et sa version logicielle. Elle répond à la question "quels sites rapportent réellement, et d'où ?" d'un coup d'œil, et c'est là que vous confirmez qu'un nouveau banc installé a composé.

Console de l'Appareil

Cliquer sur un téléphone ouvre sa **console** : une vue en direct de l'écran avec un contrôle à distance complet.

*La console diffuse l'écran du téléphone en direct. Cliquez pour toucher, faites glisser pour glisser, tapez pour entrer du texte. Un badge de **qualité réseau** (en haut à droite de l'écran) montre vert/ambre/rouge d'un coup d'œil. Cliquez dessus pour voir les statistiques complètes du flux (résolution, FPS, débit binaire, % de perte de paquets sur 5 secondes, gigue, RTT). La barre des touches matérielles (retour, accueil, récents, volume, alimentation) et les actions rapides (Avion, Composeur, Messages, Paramètres) se trouvent en dessous. Un panneau d'outils à onglets se trouve à côté : Validation cellulaire, Scripts, Shell, Logcat, Fichiers et Enregistrement.*

Un seul visualiseur à la fois. Un appareil diffuse à un opérateur à la fois. Si quelqu'un d'autre le visualise déjà, la console affiche "*Utilisé par <utilisateur> (<IP>)*". L'IP vous permet de savoir si c'est vous sur une autre machine ou un autre opérateur. Un bouton **Prendre le contrôle** revendique le flux. Une console déconnectée ou rechargée se reconnecte automatiquement à sa propre session plutôt que de se battre pour elle.

Contrôle à distance

Action	Comment
Toucher	Cliquez n'importe où sur l'écran
Glisser	Cliquez et faites glisser
Taper	Cliquez sur l'écran, puis tapez sur votre clavier
Touches matérielles	Boutons Retour, Accueil, Récents, Volume $\pm$, Alimentation
Actions rapides	Basculer l'Avion en un clic, ou ouvrir l'application Compositeur, Messages ou Paramètres. Celles-ci s'exécutent en arrière-plan. Elles ne lancent pas de test ni ne bloquent la console.

L'écran diffusé est le véritable appareil. Toute application ou page web se rend et est entièrement contrôlable depuis la console. Ici, un téléphone de test a une page ouverte dans le navigateur, contrôlée à distance :

Visionner plusieurs téléphones

Pour regarder plusieurs smartphones à la fois (les deux extrémités d'un appel de test, par exemple), ouvrez la console d'un téléphone et cliquez sur **Voir le deuxième téléphone** (en haut à droite). Choisissez un autre téléphone dans la liste et son écran en direct s'ouvre à côté du premier, avec ses propres contrôles complets : toucher/glisser/taper, touches matérielles, actions rapides, écouter l'audio et statistiques de flux. Ajoutez-en d'autres de la même manière, jusqu'à **quatre écrans** à la fois.

Chaque écran supplémentaire dispose de son propre sélecteur pour **changer** le téléphone qu'il affiche et d'un ✕ pour le fermer. L'arrangement est capturé dans l'adresse de la page (`?with=...`), donc une disposition multi-téléphone spécifique peut être mise en signet ou partagée.

Le panneau d'outils à onglets (Cellulaire, Scripts, Shell, ...) agit toujours sur le téléphone **principal**, celui que vous avez ouvert. L'en-tête du panneau le nomme afin qu'il soit clair où un script ou une commande sera exécuté.

Outils de la Console

À côté de l'écran, un **panneau d'outils à onglets** garde les outils par appareil ensemble. Changez d'onglet sans perdre l'état de chaque outil :

Onglet	Ce qu'il fait
Cellulaire	Les outils de validation d'appel / texte / ping / test de vitesse (ci-dessous)
Scripts	Exécute un script de bibliothèque sur cet appareil et voit son historique complet d'exécution, avec un re-exécution en un clic sur n'importe quelle exécution passée
Shell	Une console interactive de commande/réponse pour l'appareil
Logcat	Flux de journal système en direct de l'appareil avec filtrage de texte + niveau
Fichiers	Parcourir, télécharger, télécharger, renommer et supprimer des fichiers sur l'appareil
Enregistrer	Capturer une séquence de tapotement/glisement sous forme de lignes de script rejouables

Panneau de Validation Cellulaire

Outils intégrés pour les vérifications qu'un opérateur effectue manuellement, chacun prenant les entrées que vous vous attendez :

Outil	Entrées	Ce qu'il fait
Appel	Numéro, temps de maintien	Compose, confirme que l'appel est décroché, maintient, raccroche
Texte	Numéro, message	Envoie un SMS et confirme qu'il a quitté l'appareil
Ping	Hôte, compte	Ping un hôte via la connexion de données de l'appareil
Test de vitesse	URL de test	Mesure le débit de téléchargement via le lien de données de l'appareil

La boîte **Numéro** se souvient des numéros que vous avez récemment appelés ou textés (conservés uniquement dans votre navigateur, pas sur le serveur) et les propose sous forme de menu déroulant, donc rappeler un numéro de test est un clic.

Scripts

L'onglet **Scripts** exécute n'importe quel script de bibliothèque contre cet appareil et conserve son historique complet d'exécution sans quitter la console. Vous pouvez filtrer cet historique par source, statut et test. Chaque exécution passée a un bouton de **re-exécution**, donc répéter une vérification (ou un script qui vient d'échouer) est un clic. Les scripts qui prennent des entrées redemandent pour elles.

Shell

L'onglet **Shell** est une console interactive de commande/réponse pour l'appareil. Tapez une commande, voyez sa sortie et son code de sortie, avec ↑/↓ pour rappeler l'historique. C'est l'analogue de l'appareil de la console AT du modem, pour les fois où une commande rapide est plus rapide que d'écrire un script.

Logcat

L'onglet **Logcat** diffuse le journal système en direct de l'appareil. Filtrer par texte libre et niveau minimum (Verbeux → Fatal). Les niveaux sont codés par couleur. **Démarrer/Arrêter** contrôle le flux. Arrêter conserve ce que vous avez capturé à l'écran afin que vous puissiez faire défiler en arrière.

Fichiers

L'onglet **Fichiers** est un gestionnaire de fichiers pour l'appareil. Parcourez les répertoires (à partir de `/sdcard`), **téléchargez** un fichier sur votre machine, **téléchargez** un fichier sur l'appareil, et **renommez**, **supprimez** ou créez des dossiers. Utile pour extraire un fichier de capture ou de diagnostic d'un appareil, ou pour pousser une configuration dessus.

Enregistrement de gestes

Activez **Enregistrer**, effectuez une séquence de tapotement/glissement sur l'écran, et la console émet les lignes `adb input` équivalentes. Collez-les dans un script de dossier pour transformer un flux d'interface utilisateur manuel en un test répétable.

Console du Modem USB

Un modem cellulaire USB (Quectel EP06 et similaires) apparaît dans la flotte comme un **modem** et ouvre une console cellulaire au lieu d'un écran. L'agent relaie les commandes AT au modem via son port série (AT). Il enregistre chaque commande et réponse dans l'onglet **Terminal** comme une piste d'audit.

Onglet	Ce qu'il fait
Statut	Lecture unique du modèle / firmware / IMEI / IMSI / SIM, signal (CSQ + CSQ par RAT), opérateur, enregistrement EPS, attachement, IMS, IP, APN, DNS/PCO
Actions	Définir l'APN (préconfiguré ou personnalisé, avec PDP / type IP), attacher/détacher des données, afficher IP + DNS, ping, envoyer SMS, radio (mode avion / redémarrer)
Réseaux	Scan de l'opérateur (AT+COPS=?) et mesure de cellule servante/voisine (AT+QENG) → tableau EARFCN / PCI / bande / RSRP / RSRQ / SINR
Verrouillage de cellule	Verrouiller à un EARFCN spécifique (+PCI) (AT+QNWLOCK), verrouillage de bande (AT+QCFG="band"), préférence RAT, ou libérer en mode automatique
Appels	Composer / répondre / raccrocher, un tableau d'appels AT+CLCC, et un contrôle Activer / Désactiver VoLTE (AT+QCFG="ims")
SMS	Lire la boîte de réception (AT+CMGL), supprimer, et envoyer
Événements	Active les URCs pertinents et les interroge dans un journal horodaté (enregistrement / appel / signal / changements de nouveaux SMS)
Terminal	Entrée AT brute plus le journal complet de requête/réponse

La référence complète des commandes AT, avec de vraies réponses EP06, se trouve dans [modem-at-commands.md](#).

VoLTE : le EP06 est uniquement VoLTE/IMS pour la voix. *Activer VoLTE* définit `AT+QCFG="ims",1` ; un redémarrage `AT+CFUN=1,1` peut être nécessaire pour (dé)enregistrer IMS, et il ne s'enregistre que si le réseau + SIM le provisionnent et que le bon MBN de l'opérateur est sélectionné.

Dongles Android anciens (mode screencap)

Des dongles LTE bon marché d'environ 10 \$ ("MiFi") (par exemple, le UZ801, Qualcomm msm8916) exécutent **Android 4.4 (API 19)**, ce qui est trop ancien pour la vue d'écran en direct. Ces appareils retombent sur une console **screencap** : l'agent interroge `adb screencap` pour des images (quelques par seconde, car `screencap` lui-même est le goulot d'étranglement sur ce matériel) et injecte `adb input` pour le contrôle. Vous obtenez une vue clic-pour-toucher, taper-pour-texte. Ce n'est pas une vidéo fluide, mais c'est suffisant pour le contrôler.

L'agent lisse les bords rugueux de ces dongles du côté hôte :

- **Déverrouillage ADB** : ils sont expédiés en mode RNDIS. Un service déclenché par udev `curl` le `usbdebug.html` du dongle pour le passer en mode ADB. Consultez [agent/host-setup/mifi-dongle](#).
- **Anglais automatique** : ils sont expédiés en chinois. L'agent définit `persist.sys.language` sur `en-US` la première fois qu'il voit un appareil API-`<21` (désactivez avec `OMNIWEB_DONGLE_AUTO_ENGLISH=0`).

Scripts

Les tests sont des scripts bash qui s'exécutent sur l'**hôte de l'agent** (donc les outils hôtes comme `grep/awk` sont disponibles) et ciblent un appareil via ADB. Il existe deux types :

- **Scripts de dossier** : vérifications de santé qui apparaissent dans la bibliothèque, le coureur de fan-out, et le planificateur. Certains s'exécutent uniquement avec l'appareil (Appareil Connecté, Enregistrement VoLTE, Rapport de Force de Signal). D'autres prennent des entrées optionnelles

(@param). Le Test de Ping prend un hôte et un compte. Le Test de Débit de Données prend une URL. Les tests de connectivité et de voix (Ping, Débit de Données, Envoyer SMS, Passer un Appel) sont des scripts de dossier, donc vous pouvez les programmer ainsi que les exécuter manuellement. Deux tests de récupération de battement d'avion confirment qu'un appareil se remet après avoir perdu le radio. **Battement d'Avion → Récupération de Ping** active le mode avion, puis le désactive, attend que les données se reconnectent, puis ping. **Battement d'Avion → Récupération IMS** fait la même chose, puis confirme que VoLTE se réenregistre.

- **Outils intégrés** : les raccourcis d'ouverture d'application (Composeur, Messages, Paramètres) et le simple basculement Avion dans les actions rapides de la console. Chacun effectue une action d'interface utilisateur sans résultat de réussite ou d'échec, donc il n'est pas dans la bibliothèque ou le planificateur.

La bibliothèque de scripts liste les scripts de dossier sans argument. Chacun montre sa description et son délai. Cliquez sur l'un pour voir sa source (lecture seule). Les exécutions récentes apparaissent ci-dessous.

Un script rapporte son résultat par **code de sortie** : 0 est un succès, tout autre est un échec. Sa sortie capturée est affichée dans le tableau des

résultats.

Tests Programmés

Les tests programmés sont définis de manière déclarative dans `schedules.json` dans le répertoire des scripts. Le fichier est relu à chaque cycle, donc les modifications prennent effet sans redémarrage. Chaque entrée exécute un script de dossier contre ses appareils cibles à un intervalle.

Configuration

```
{
  "schedules": [
    {
      "name": "Enregistrement VoLTE",
      "script": "volte_registration.sh",
      "interval_seconds": 120,
      "serials": [],
      "enabled": true
    }
  ]
}
```


Paramètre	Type	Requis	Par défaut	Description
<code>name</code>	Chaîne	Oui	-	Étiquette unique pour le programme. Apparaît comme l'étiquette <code>schedule</code> sur la métrique exportée.
<code>script</code>	Chaîne	Oui	-	Nom de fichier d'un script de dossier dans le répertoire des scripts à exécuter.
<code>interval_seconds</code>	Entier	Non	300	À quelle fréquence exécuter le script, en secondes. Minimum 30.
<code>serials</code>	Liste	Non	<code>[]</code>	Séries d'appareils à cibler. Une liste vide signifie tous les appareils actuellement connectés , donc le programme suit automatiquement tous les téléphones branchés.
<code>params</code>	Objet	Non	<code>{}</code>	Entrées pour un script qui déclare des valeurs <code>@param</code> . Les clés sont les noms des paramètres. Par exemple, le Test de

Paramètre	Type	Requis	Par défaut	Description
				Ping accepte <code>host</code> et <code>count</code> .
<code>enabled</code>	Booléen	Non	true	Si le programme est actif. Définissez <code>false</code> pour le mettre en pause sans supprimer l'entrée.
<code>exclusive</code>	Booléen	Non	false	Réserver le téléphone pendant la durée de ce test. Pendant qu'un test exclusif est en cours, aucun autre test programmé ne commence sur cet appareil, et le test exclusif lui-même attend que l'appareil soit libre avant de commencer. Utilisez-le pour des tests perturbateurs — un battement de mode avion ou un redémarrage — qui corrompraient un autre test (par exemple, un appel VoLTE) exécuté sur le même smartphone en même temps.

Exemple : Vérification VoLTE sur un site

```
{
  "name": "VoLTE Registration",
  "script": "volte_registration.sh",
  "interval_seconds": 120,
  "serials": [],
  "enabled": true
}
```

Comment ça fonctionne : Toutes les 120 secondes, le planificateur exécute `volte_registration.sh` sur chaque téléphone connecté. Le script vérifie que l'appareil est enregistré pour la voix (`IN_SERVICE`) sur LTE avec le support VoPS (Voice-over-PS), et se termine par `0` si VoLTE est enregistré. Le résultat devient un indicateur Prometheus par appareil.

Cas d'utilisation : Prouver en continu que de vrais appareils sur un site peuvent s'enregistrer pour VoLTE, et alerter au moment où l'un d'eux ne peut pas.

Exemple : Ping chaque téléphone

```
{
  "name": "Ping Test",
  "script": "ping_test.sh",
  "interval_seconds": 120,
  "serials": [],
  "params": { "host": "8.8.8.8", "count": "5" },
  "enabled": true
}
```

Comment ça fonctionne : Toutes les 120 secondes, le planificateur exécute `ping_test.sh` sur chaque téléphone connecté. Les `params` fournissent les entrées du script. Le script ping `8.8.8.8` cinq fois via le lien de données de l'appareil et se termine par `0` s'il reçoit des réponses. Changez `host` pour tester une cible spécifique.

Cas d'utilisation : Prouver que de vrais appareils sur un site ont des données fonctionnelles, et alerter en cas de perte de paquets.

Métriques

Central OmniWeb expose le dernier résultat de chaque test planifié, par appareil, au format Prometheus à `/api/android/metrics`. Prometheus le scrute en tant que travail `android_device_tests` (configuré automatiquement par le rôle de surveillance).

Métrique : `omniweb_android_test_pass` **Type :** Indicateur **Description :** Résultat de la dernière exécution planifiée : `1` pour réussite, `0` pour échec
Étiquettes :

- `phone` : modèle de l'appareil (par exemple, `SM-A536E`)
- `serial` : numéro de série de l'appareil
- `site` : l'étiquette du site de l'agent (par exemple, `Cell Site 12`)
- `agent` : l'hôte de l'agent auquel l'appareil est connecté
- `script` : le script qui a été exécuté
- `schedule` : le nom du programme
- `status` : le résultat de l'exécution (`passed`, `failed`, `timeout`, ou `error`)

Les indicateurs compagnons partagent les mêmes étiquettes :

Métrique	Description
<code>omniweb_android_test_duration_ms</code>	Durée de la dernière exécution, en millisecondes
<code>omniweb_android_test_last_run_timestamp</code>	Temps Unix de la dernière exécution

Exemples de requêtes :

```
# Téléphones échouant actuellement à l'enregistrement VoLTE
omniweb_android_test_pass{schedule="VoLTE Registration"} == 0

# Tests échoués regroupés par site
count by (site) (omniweb_android_test_pass == 0)

# Un test qui n'a pas été exécuté récemment (agent obsolète ou
appareil hors ligne)
time() - omniweb_android_test_last_run_timestamp > 600
```

Tableau de bord Grafana

Le rôle de surveillance fournit un tableau de bord **Tests de Téléphone / Appareil** (dossier Grafana **Devices**). Il lit les métriques ci-dessus et montre, par téléphone et programme :

- une chronologie de l'état de réussite ou d'échec,
- le dernier résultat pour chaque téléphone et test,
- la fraîcheur du test (temps écoulé depuis la dernière exécution, pour détecter un agent bloqué),
- la durée d'exécution dans le temps.

Filtrez le tableau de bord par site, téléphone ou test en haut. Le tableau de bord est provisionné automatiquement. Voir [Grafana](#).

Dépannage

Un téléphone n'apparaît pas dans la flotte

Symptômes : Un appareil est branché sur un site mais n'est pas listé sous Appareils de Test.

Causes possibles :

- Le téléphone n'est pas autorisé pour ADB sur l'hôte de l'agent
- L'agent ne fonctionne pas ou ne peut pas atteindre le central

- Le téléphone est dans un état ADB hors ligne/non autorisé
- Le service Appareils de Test central ne fonctionne pas (les Appareils de Test sont servis par leur propre service backend dédié, séparé du pool de requêtes principal)

Résolution :

1. Confirmez que le téléphone apparaît comme `device` (pas `unauthorized/offline`) dans ADB sur l'hôte de l'agent, en acceptant l'invite RSA sur le téléphone si nécessaire.
2. Vérifiez que le service de l'agent fonctionne et que son URL centrale configurée et son jeton sont corrects.
3. Sur le central, confirmez que le service Appareils de Test fonctionne et que la passerelle dirige `/api/android/*` vers lui. Si l'agent s'est enregistré mais que la flotte est vide, ce service est généralement la cause.
4. Vérifiez la connexion USB du téléphone ; rebranchez le câble s'il apparaît comme hors ligne.

L'écran de la console reste sur "Connexion"

Symptômes : La console de l'appareil s'ouvre mais l'écran n'apparaît jamais, tandis que le reste de l'interface utilisateur (liste de flotte, détails de l'appareil, saisie) fonctionne normalement et que l'appareil apparaît **en ligne**.

Causes possibles :

- UDP est bloqué entre le réseau du navigateur et l'hôte de l'agent (les flux vidéo en direct vont **directement** du navigateur à l'hôte de l'agent, pas via le serveur, et c'est de loin la cause la plus courante)
- L'agent ne peut pas démarrer la capture d'écran sur ce téléphone

Ce n'est **pas** un problème SSL ou MTU : TLS fonctionne (l'interface utilisateur s'est chargée), et avec des problèmes de MTU, la vidéo se connecterait et *puis* se déconnecterait plutôt que de ne jamais démarrer. Le signe révélateur est un appareil qui apparaît **en ligne** dans la flotte mais dont la vue en direct ne démarre pas.

Résolution :

1. Confirmez que le réseau du navigateur peut atteindre l'hôte de l'agent via **UDP** (le chemin vidéo). Cela signifie généralement une règle de pare-feu/VLAN permettant au sous-réseau de l'opérateur d'accéder aux hôtes de banc via UDP. Voir **Exigences Réseau** pour la règle exacte à demander et comment confirmer la correction.
2. Vérifiez le journal de l'agent pour des erreurs de capture d'écran. Certains téléphones ne peuvent pas avoir leur écran capturé via ADB.

Les vérifications VoLTE / signal rapportent "non lisible"

Symptômes : Les scripts VoLTE ou signal échouent avec l'état de téléphonie illisible.

Causes possibles :

- Le téléphone restreint l'état de téléphonie à un accès privilégié

Résolution :

1. Utilisez des téléphones de test qui exposent l'état de téléphonie à ADB. Les appareils consommateurs verrouillés par le fournisseur peuvent le cacher sans accès privilégié.

Appareils de test : Exigences réseau

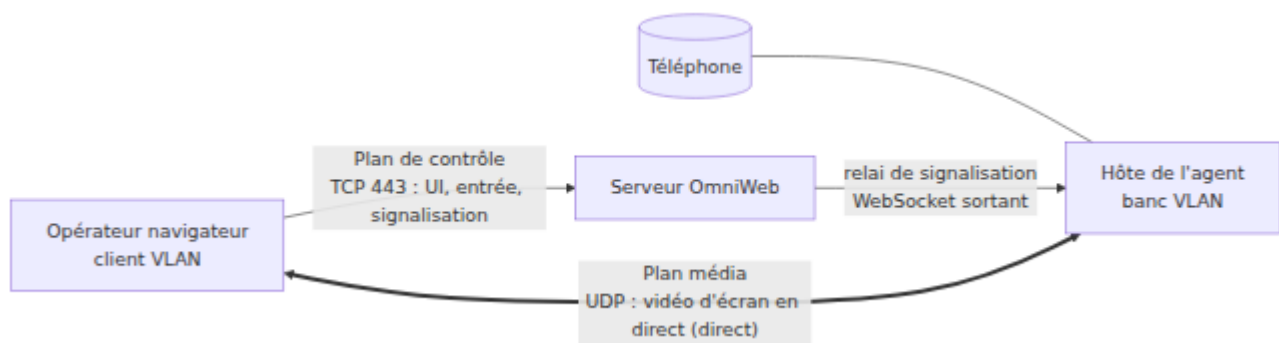
La visualisation en direct des téléphones dans **Appareils de test** utilise **deux chemins réseau séparés**. Comprenez la séparation pour faire fonctionner cela à travers les pare-feu et les VLAN. La séparation vous aide également à diagnostiquer le symptôme le plus courant, une console qui reste sur "**Connexion...**" indéfiniment.

[← Retour aux Appareils de test](#)

Les deux chemins

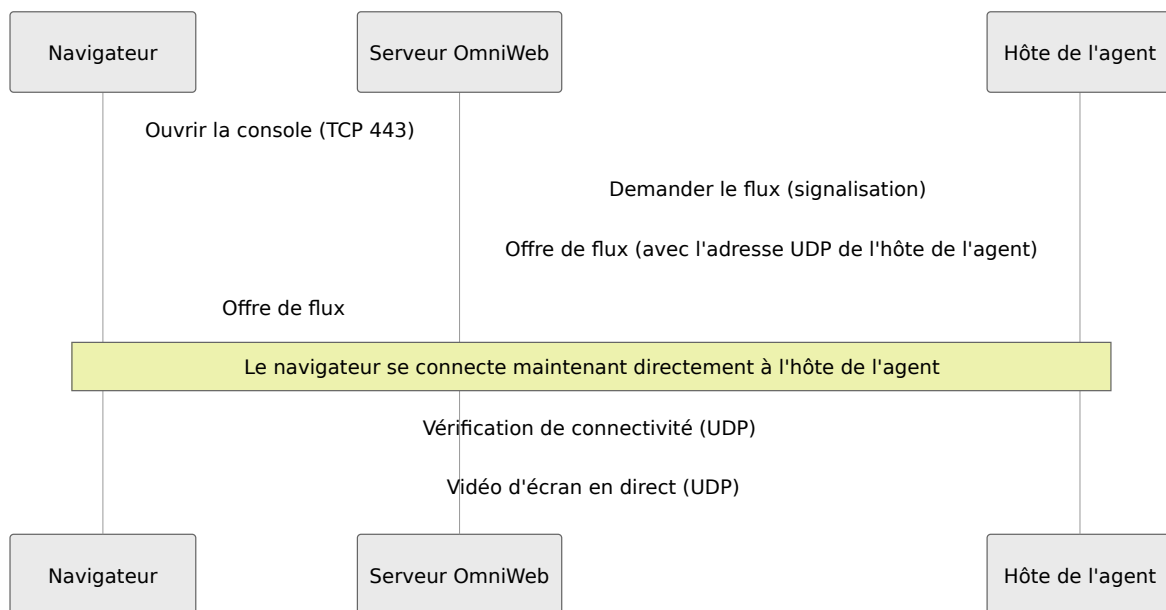
Chemin	Transporte	Direction	Transport	Point de terminaison
Plan de contrôle	L'interface web, la connexion, la liste des appareils, l'entrée à distance, les résultats des tests et la configuration de l'appel ("signalisation") pour une vue en direct	Navigateur → serveur OmniWeb	TCP 443 (HTTPS)	Le serveur OmniWeb
Plan média	La vidéo de l'écran en direct elle-même	Navigateur ⇔ hôte de l'agent (le banc dans lequel le téléphone est branché)	UDP (WebRTC)	L'hôte de l'agent, pas le serveur

Le point crucial : **la vidéo en direct ne passe pas par le serveur OmniWeb**. Une fois que le serveur a négocié la connexion, les flux vidéo **circulent directement entre le navigateur de l'opérateur et l'hôte de l'agent** via UDP. Si un réseau permet au navigateur d'atteindre le *serveur* mais pas l'*hôte de l'agent*, il charge l'interface utilisateur, affiche la liste des appareils, puis reste bloqué sur "Connexion...".



Pourquoi le chemin média est direct

La vidéo d'écran en direct est envoyée de pair à pair avec **WebRTC sur UDP** afin de mieux survivre aux liens à latence élevée et à perte de paquets typiques des sites cellulaires distants que de la relayer via un serveur central sur TCP. Le compromis est que le navigateur de l'opérateur a besoin d'un **chemin UDP direct vers l'hôte de l'agent**. Il n'y a pas de relais média au milieu sur lequel se reposer.



Exigences du pare-feu

Pour qu'un opérateur puisse visualiser des téléphones sur un site, **les deux** chemins doivent être autorisés depuis le réseau de l'opérateur vers les hôtes concernés.

Plan de contrôle (déjà ouvert dans la plupart des cas)

Champ	Valeur
Action	Autoriser (étatful)
Protocole	TCP
Source	VLAN(s) de l'opérateur / client
Destination	Serveur OmniWeb
Port de destination	443

Si l'interface utilisateur OmniWeb se charge, ce chemin est déjà ouvert. Aucun changement nécessaire.

Plan média (celui qui est généralement manquant)

Champ	Valeur
Action	Autoriser (étatful , donc le retour vidéo est automatiquement autorisé)
Protocole	UDP
Source	VLAN(s) de l'opérateur / client, où les navigateurs fonctionnent
Destination	Le sous-réseau de l'hôte du banc de l'appareil (les hôtes de l'agent), par exemple 10.0.20.0/24
Ports de destination	32768–60999 (la plage éphémère par défaut de Linux dont l'agent tire les ports média)

Le navigateur initie toujours la connexion média, donc un **permis étatful** sur `client → hôte de l'agent` UDP permet également le retour vidéo de l'agent automatiquement. Aucun port STUN/TURN ou autre n'est impliqué.

Ne changez pas le port 443 pour cela. La signalisation passe déjà par le plan de contrôle. Seul le chemin média UDP vers les hôtes de l'agent doit être ouvert.

Recommandé : fixer la plage de ports média

Ouvrir toute la plage éphémère (`32768–60999`) est large. Vous pouvez plutôt configurer l'agent pour tirer ses ports média d'une petite plage fixe. Cela réduit la règle de pare-feu à un bloc soigné :

Champ	Valeur
Action	Autoriser (étatful)
Protocole	UDP
Source	VLAN(s) de l'opérateur / client
Destination	Sous-réseau de l'hôte du banc d'appareils
Ports de destination	<code>50000–50100</code> (plage fixée)

C'est la forme préférée à remettre à une équipe réseau. 100 ports pour un sous-réseau est bien plus facile à approuver et à auditer que la plage éphémère complète. La plage fixée est définie sur l'hôte de l'agent. Coordonnez la plage exacte avec quiconque maintient les bancs afin que la règle de pare-feu et la configuration de l'agent correspondent.

Reconnaître le problème

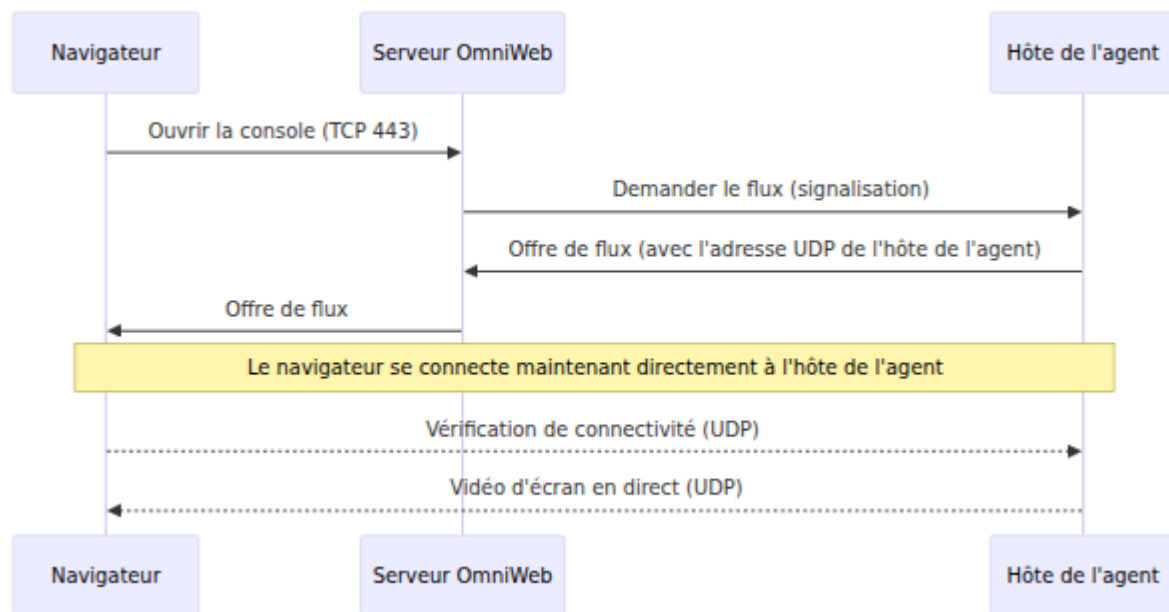
Symptôme : la console de l'appareil s'ouvre, mais l'écran n'apparaît jamais. Il reste sur "**Connexion...**" indéfiniment. Tout le reste fonctionne : la liste de la

flotte, les détails de l'appareil, même la configuration de l'entrée à distance.

C'est presque toujours le chemin UDP du plan média qui est bloqué. Ce n'est **pas** un problème de TLS/certificat et **pas** un problème de MTU :

Cause suspectée	Pourquoi ce n'est pas cela	Ce que vous verriez réellement si c'était le cas
SSL / certificat	L'UI, la connexion, la liste des appareils et la signalisation réussissent tous sur HTTPS, donc TLS fonctionne clairement	La page elle-même échouerait à se charger ou afficherait un avertissement de certificat
MTU / fragmentation	La MTU n'a d'importance qu'une fois que les paquets vidéo circulent. Ici, aucun paquet vidéo n'arrive jamais	La vidéo se connecterait , puis se bloquerait ou se déchirerait, ne resterait pas sur "Connexion..."
Agent / téléphone hors service	L'appareil apparaît en ligne dans la flotte avec des données de batterie/opérateur en direct	L'appareil manquerait dans la flotte ou serait marqué hors ligne
Chemin UDP bloqué ✓	Le navigateur peut atteindre le serveur (l'UI se charge) mais pas l'hôte de l'agent via UDP	"Connexion..." permanente, exactement ce symptôme

Un indicateur utile : la tuile de l'appareil montre le téléphone comme **en ligne** (donc l'agent et le téléphone sont sains et le serveur peut les voir), mais la vue en direct ne démarre pas. Cette combinaison pointe directement vers le chemin du pare-feu du plan média.



Confirmation de la correction

Après l'application de la règle de pare-feu, rouvrez la console de l'appareil. Si l'écran apparaît dans quelques secondes et que le badge **qualité du réseau** (en haut à droite de la vue en direct) devient vert, le chemin média fonctionne. Les statistiques de flux du badge (résolution, FPS, débit binaire, % de perte de paquets, gigue, RTT) confirment que la vidéo circule de bout en bout.

S'il reste toujours bloqué, vérifiez deux choses avec quiconque maintient les bancs. Tout d'abord, le **sous-réseau et les ports de destination** de la règle de pare-feu doivent correspondre aux hôtes de l'agent et à leur plage de ports média configurée. Deuxièmement, la règle doit s'appliquer au VLAN **réel** de l'opérateur (un ordinateur portable sur le Wi-Fi invité est une source différente que le LAN d'entreprise).

Plusieurs emplacements d'opérateurs

Chaque réseau d'opérateur qui doit visualiser des téléphones doit avoir la règle du plan média pour son propre VLAN source. La règle est par sous-réseau source → sous-réseau de banc, donc l'ajout d'un nouveau bureau, d'un pool VPN ou d'un site signifie ajouter son sous-réseau comme **Source**.

supplémentaire sur le même permis UDP. Les sites dont les opérateurs visualisent uniquement des téléphones depuis le LAN du banc lui-même n'ont besoin d'aucune règle inter-VLAN.

Topologie du Réseau & Vue Unique

Les vues de topologie d'OmniWeb sont le point d'entrée "vue unique" pour l'ensemble du réseau. Elles montrent comment les éléments se connectent, lesquels sont déployés, et vous permettent de passer directement d'un nœud sur la carte à l'espace de travail de cet élément.

[← Retour au Guide des Opérations](#)

Vues de Topologie

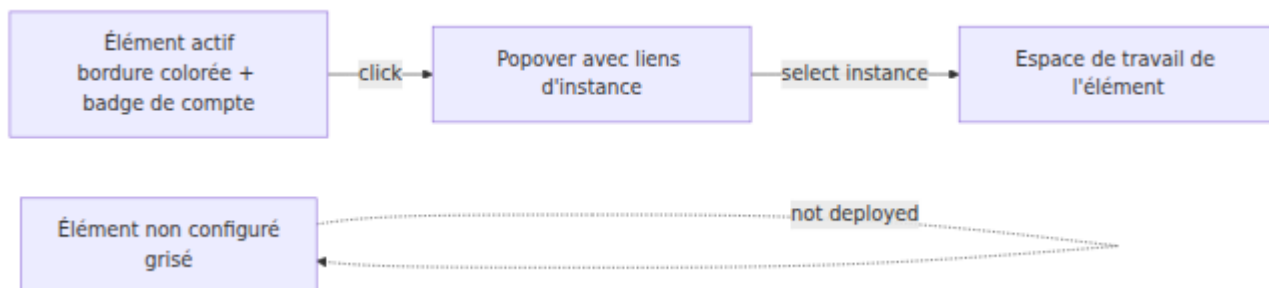
La page d'accueil/topologie présente le réseau à travers quatre onglets de domaine. Chacun est une carte interactive des éléments pertinents et de leurs interfaces.

Topologie EPC : UE → eNB → MME → SGW-C → PGW-C → UPF, avec signalisation Diameter à travers le DRA vers le HSS. Les éléments actifs affichent une

bordure colorée et un badge de compte d'instance.

Onglet	Éléments affichés
Noyau (EPC)	UE → eNB → MME → SGW-C → PGW-C → UPF ; DRA ↔ HSS ; OCS ; TWAG ; Moniteur RAN
IMS	P-CSCF → I-CSCF → S-CSCF ; DRA ↔ HSS ; TAS ; IMS SMSsc → SMSC → SMPP GW ; OCS ; Droit (OmniSEP)
Noyau CS	BTS → BSC → MSC ; STP ↔ HLR / CAMEL GW / IP-SM-GW ; HSS ; SMSC ; OCS
Noyau 5G	gNB → AMF → SMF → UPF ; NRF, SCP, AUSF, UDM, UDR, PCF ; CHF → OCS ; NSSF ; BSF

Lecture de la Carte



- **Les éléments actifs** sont ceux dont les instances sont déclarées dans `omniweb.json`. Ils apparaissent avec une bordure colorée et un badge qui montre combien d'instances existent. Cliquez sur l'un d'eux pour ouvrir un popover avec des liens directs vers chaque instance. Vous pouvez ensuite naviguer directement depuis la topologie vers les pages d'un élément.
- **Les éléments non configurés** apparaissent grisés, de sorte que la carte fait également office d'inventaire rapide de ce qui est et n'est pas déployé.
- **Les connexions** indiquent l'interface entre les éléments (par exemple, SIP, Diameter, PFCP, GTP-C, SS7), distinguant les types de signalisation.

Cela fait de la page de topologie le point de départ naturel : voir la forme du réseau, repérer ce qui est déployé et approfondir.

Topologie au Niveau de l'Élément

Certains éléments fournissent également leur propre vue de topologie ciblée. L'onglet **PGW-C → Topologie**, par exemple, montre les relations de ce nœud avec son SGW-C, UPF et ses pairs Diameter, annotées avec des comptes de session en direct et une utilisation. Cela donne une vue localisée à panneau unique pour le voisinage de cet élément.

Topologie PGW-C : relations avec SGW-C, UPF et Diameter avec distribution des sessions par pair.

Liste des Hôtes & Infrastructure

Au-delà des fonctions réseau elles-mêmes, la page **Liste des Hôtes** est la vue unique pour l'*infrastructure* qui les fait fonctionner. Elle liste tous les hôtes d'infrastructure par catégorie, chacun avec un lien direct vers son interface web :

Catégorie	Exemples
Surveillance	Grafana, Prometheus, Loki
Capture SIP	Interface Web Homer
Facturation	Interface Web OCS
DNS	Serveurs DNS
Virtualisation	Consoles de l'hyperviseur Proxmox
Gestion hors bande	Gestion de serveur iDRAC
Routeurs	MikroTik WebFig, Peplink
Micro-ondes	Liens SAF, Ubiquiti AirFiber
NAS	Synology DSM

La Liste des Hôtes : chaque hôte d'infrastructure et d'éléments par catégorie, chacun avec un lien direct vers son interface web (Grafana, Prometheus, Loki, API d'éléments, et plus).

Cela donne aux opérateurs un endroit pour accéder à chaque système de support : surveillance, hyperviseurs, gestion hors bande et transport. Ils n'ont pas besoin de chercher des signets.

TWAG : Passerelle d'accès WLAN de confiance

Le **TWAG** (Passerelle d'accès WLAN de confiance) apporte un accès Wi-Fi de confiance dans le cœur mobile. Il authentifie les appareils Wi-Fi avec EAP-AKA/AKA' contre le AAA/HSS via Diameter, attribue à chaque client authentifié une adresse IP par DHCP, et ancre ses données dans le cœur de paquets via un tunnel GTP vers le PGW. Ainsi, un abonné sur Wi-Fi bénéficie du même APN, des mêmes politiques et de la même facturation que sur le réseau cellulaire. Son tableau de bord est l'endroit pour voir qui est connecté, si les chemins Diameter et GTP sont sains, et pour effacer des sessions individuelles.

[← Guide des opérations](#)

Le tableau de bord est une page d'éléments par instance accessible depuis la barre latérale lorsqu'un TWAG fonctionne dans l'inventaire du site. Tout le trafic passe par le proxy backend OmniWeb vers l'API du TWAG, de sorte qu'il reste derrière la seule passerelle authentifiée. Il est organisé en onglets.

Aperçu

L'onglet d'accueil est une lecture de santé sur un seul écran : **sessions** actives et totales, **pairs Diameter** connectés/déconnectés, **abonnés** acceptés, le nombre de **points d'accès**, le nombre de baux **DHCP**, l'état du tunnel **GTP** et son adresse PGW, le **mode d'authentification** utilisé (par exemple EAP-AKA), le **trafic** agrégé entrant et sortant, le temps de fonctionnement, et un **fil d'activité récente** en direct des authentifications et des débuts/arrêts de session.

Sessions

Chaque session Wi-Fi authentifiée, chaque ligne montrant l'**identité** de l'abonné (l'identifiant d'accès au réseau), le **statut**, l'**IP** attribuée, le **MAC** du client, le **SSID**, l'**IP NAS** servant, la **durée** de la session, et les **bytes entrants/sortants**. Un opérateur peut **supprimer** une session pour déconnecter de force un client, par exemple pour effacer un appareil bloqué ou malveillant.

Points d'accès

Les points d'accès WLAN (appareils NAS) actuellement connectés à la passerelle. Chacun peut être **supprimé** individuellement lorsqu'un point d'accès est décommissionné ou doit être effacé.

Comptabilité

Les sessions de comptabilité que le TWAG a enregistrées : les enregistrements d'utilisation générés pour les clients authentifiés. Les sessions de comptabilité individuelles peuvent être **supprimées**.

Diameter

Les connexions de pairs Diameter au AAA/HSS qui transportent l'authentification, avec des comptes connectés et déconnectés. Cet onglet propose également un **test Diameter**. Il envoie une demande d'authentification multimédia (MAR) de test pour confirmer que le chemin d'authentification vers le AAA/HSS est opérationnel, ce qui est le moyen le plus rapide de prouver la connectivité Diameter lorsque les authentifications échouent.

DHCP

Les baux DHCP que le TWAG a émis aux clients Wi-Fi, avec l'adresse, le client et l'état du bail pour chacun, afin que vous puissiez confirmer que les clients sont adressés et voir combien de la piscine est utilisée.

Journaux

L'onglet **Journaux** affiche en temps réel la sortie des journaux du TWAG pour le dépannage d'une passerelle individuelle sans quitter OmniWeb.

Actions

Chaque action demande d'abord une confirmation :

- **Supprimer une session** : déconnecter de force une session Wi-Fi authentifiée (onglet Sessions, par ligne).
- **Supprimer un point d'accès** : effacer une entrée de point d'accès / NAS unique (onglet Points d'accès, par ligne).

- **Supprimer une session de comptabilité** : retirer un enregistrement de comptabilité unique (onglet Comptabilité, par ligne).
- **Test Diameter** : envoyer un MAR de test pour valider le chemin Diameter vers le AAA/HSS (onglet Diameter).

Liés

- Le **PGW** ancre le plan utilisateur du TWAG via GTP. Voir les éléments du cœur de paquets.
- Le **HSS** détient les données d'authentification des abonnés contre lesquelles les requêtes Diameter du TWAG se résolvent.
- **ePDG** : le contrepartie Wi-Fi non fiable pour les appels Wi-Fi.

UPF : Fonction de Plan Utilisateur

La **UPF** (Fonction de Plan Utilisateur) est le nœud de transfert de paquets du cœur mobile. Elle transporte le trafic réel de chaque abonné : elle reçoit des tunnels GTP-U du réseau d'accès sur **N3** (S1-U dans l'EPC), transfère des paquets vers et depuis le réseau de données, applique la QoS par flux et la comptabilité de volume, et met en mémoire tampon les paquets descendantes lorsqu'un appareil est inactif. Elle n'a pas de logique propre. Le plan de contrôle (un **SGW-C** dans l'EPC sur **Sxa**, ou un **SMF** dans un cœur 5G sur **N4**) la programme entièrement via **PCF**. Le plan de contrôle installe les règles de détection de paquets, de transfert, de QoS et de reporting d'utilisation qui décrivent comment la UPF gère le trafic de chaque session. **OmniUPF** d'Omnicore implémente le chemin de transfert comme un **dataplane eBPF/XDP** dans le noyau, de sorte que les règles installées par le plan de contrôle deviennent des entrées dans des cartes eBPF que le programme XDP consulte pour chaque paquet. OmniWeb expose les associations et sessions PCF de la UPF, le contenu des cartes eBPF en direct, les statistiques du dataplane, le routage, les tampons descendantes, l'état du jardin clos et la configuration. Il atteint les graphiques de débit et de tendance sur les tableaux de bord Grafana depuis la même page.

[← Guide des opérations](#)

La UPF est une page d'élément par instance accessible depuis la barre latérale lorsqu'on navigue dans l'inventaire du site, avec un sélecteur d'instance où plusieurs sont déployées et une vue de flotte pour l'état agrégé. Tout le trafic passe par le proxy backend d'OmniWeb vers l'API de la UPF, de sorte qu'il reste derrière la passerelle authentifiée unique. Le lien de documentation dans l'en-tête de la page (le bouton d'aide contextuelle) ouvre cette page. Elle est organisée en onglets.

Sélection de flotte et d'instance

Lorsqu'un site exécute plus d'une UPF, la **vue de flotte** liste chaque instance avec son état de santé d'un coup d'œil. C'est le moyen le plus rapide de confirmer que l'ensemble du plan utilisateur est opérationnel avant d'explorer un nœud.

Depuis n'importe quel onglet, le **sélecteur d'instance** dans l'en-tête de la page change quelle UPF la page lit. Tout ce qui suit (sessions, associations, cartes eBPF, statistiques) est limité à l'instance sélectionnée, donc vous choisissez le nœud une fois et toute la page le suit.

Aperçu

Une lecture de santé sur un seul écran de la UPF : son état de **santé**, le nombre d'**associations PFCP** qu'elle détient avec des pairs du plan de contrôle, le total des **sessions actives** à travers ces pairs, et les **compteurs d'actions XDP** : combien de paquets le dataplane a passés, abandonnés, redirigés, transmis ou avortés, ce qui est la confirmation la plus rapide que le trafic circule réellement. En dessous, chaque **pair PFCP** est listé avec son état d'association, le compte des sessions et tout battement de cœur manqué, et les **tailles des cartes eBPF** montrent la capacité des cartes PDR, FAR, QER et URR et le nombre maximum de sessions. Une zone de recherche permet d'accéder directement à une session par **UE IP** ou **TEID**, et une action **Rapport de nœud** envoie une demande de rapport de nœud PFCP au premier pair actif du plan de contrôle.

Sessions

Chaque **session PFCP** : l'état du plan utilisateur par porteur / par session PDU que le plan de contrôle a installé. Chaque ligne est identifiée par son **SEID local et distant** et montre l'**IMSI** de la session, l'**APN/DNN**, l'**association** (quel pair du plan de contrôle la possède), et le compte des règles de **détection de paquets, action de transfert, application de QoS** et **reporting d'utilisation** qu'elle porte. Recherchez **par UE IP ou TEID** pour trouver la session servant un appareil ou un tunnel spécifique.

Détail de la session

Ouvrir une session montre son état complet des règles. Une **carte de règles de session** illustre comment chaque **Règle de Détection de Paquet (PDR)** fait référence à la **Règle d'Action de Transfert (FAR)**, à la **Règle d'Application de QoS (QER)** et aux **Règles de Reporting d'Utilisation (URR)** qu'elle applique. Cliquez sur n'importe quel nœud pour mettre en surbrillance uniquement les règles qui lui sont connectées, afin que vous puissiez tracer le chemin d'un flux unique à travers le dataplane. En dessous de la carte, quatre tableaux donnent le détail :

- **Règles de Détection de Paquet (PDR)** : comment la UPF classe les paquets entrants. Cela couvre la direction (montante / descendante), l'UE IP ou le TEID entrant qu'ils correspondent, les filtres SDF (protocoles et plages de ports), et quelles FAR, QER et URR elles résolvent.
- **Règles d'Action de Transfert (FAR)** : ce qui arrive aux paquets correspondants. L'action est **Transférer**, **Abandonner**, **Mettre en mémoire tampon** ou **Notifier CP**, avec les détails du tunnel GTP-U sortant (IP distante et TEID) et l'instance réseau. Vous pouvez modifier les FAR sur place.

- **Règles d'Application de QoS (QER)** : la QoS par flux. Cela couvre le **QFI**, l'état de la **porte** montante et descendante (ouverte / fermée) et les **débts** maximum et **garantis**. Vous pouvez modifier les QER sur place.
- **Règles de Reporting d'Utilisation (URR)** : les compteurs de volume. Ce sont les octets montants et descendants actuels et dernier rapport❖❖s et le numéro de séquence de rapport, qui est ce que la UPF renvoie au plan de contrôle pour la facturation et le quota.

Depuis l'en-tête de la session, vous pouvez également **activer ou supprimer une redirection de jardin clos** pour cette session spécifique (voir Jardin Clos ci-dessous).

Associations

Les **associations PFCE** : les relations Sxa/N4 que la UPF entretient avec ses pairs du plan de contrôle (le SGW-C ou SMF). Chaque ligne montre l'**IP et le port distants** du pair, son **compte de sessions**, si elle est actuellement **associée**, le nombre de **battements de cœur manqués**, et quand elle s'est **connectée** ou **déconnectée** pour la dernière fois. Ici, vous confirmez que le

plan utilisateur et le plan de contrôle sont synchronisés. Ici, vous repérez également un pair dont les battements de cœur sont en retard.

Statistiques

Les chiffres en temps réel du dataplane. **Utilisation des cartes eBPF** montre à quel point chaque carte est pleine (sessions, PDR, FAR, QER et URR) sous forme de barres utilisées par rapport à la capacité qui deviennent ambrées et rouges à mesure qu'elles approchent de leur limite, afin que vous puissiez voir une UPF approchant de sa capacité dimensionnée avant qu'elle ne commence à rejeter des sessions. **Statistiques XDP** décompose les compteurs de paquets passés / abandonnés / redirigés / TX / avortés, et la section **Métriques** expose les compteurs Prometheus de la UPF sous forme de chiffres individuels.

Une vérification de capacité lit le même modèle utilisé par rapport à la capacité. D'un coup d'œil, vous pouvez dire si la ressource contraignante est la table de sessions ou l'une des cartes de règles.

Routage

Les routes qui dirigent le trafic des abonnés vers et depuis la UPF. Le tableau des **Routes IP UE Actives** liste les routes que la UPF détient actuellement pour les pools IP UE alloués, et une action **Synchroniser les Routes** les réconcilie avec le dataplane. En dessous, une **console FRR** fournit un terminal vtysh contextuel contre le démon de routage de la UPF. Pour inspecter l'état de routage, tapez une commande `show` (par exemple `show ip route` ou `show ip ospf neighbor`), avec auto-complétion et historique des commandes. Pour effectuer un changement, passez en **mode de configuration**. C'est ainsi que la UPF annonce ses pools UE dans le réseau environnant sans quitter OmniWeb.

Tampons

Les **tampons de paquets descendantes**. Lorsque des données descendantes arrivent pour un appareil qui est inactif (aucun tunnel actif), le dataplane conserve ces paquets contre la FAR pertinente et demande au plan de contrôle de contacter l'appareil. Une fois le tunnel rétabli, la UPF vide les paquets mis en mémoire tampon (c'est le côté plan utilisateur de la **Notification de Données Descendantes**). L'onglet montre le **total des paquets mis en mémoire tampon** et le **total des FAR** détenant des paquets, les **limites de tampon par FAR** et **totales**, et une **recherche par ID de FAR** pour voir combien de paquets une FAR spécifique détient. Les tampons peuvent être **vidés** individuellement ou **effacés** en masse.

Cartes eBPF

Un navigateur direct sur les **cartes eBPF** qui sont le dataplane de la UPF. Ce sont les entrées brutes côté noyau que le programme XDP consulte pour chaque paquet, réparties sur des onglets :

- **PDR Montante** : identifiée par le TEID entrant, qui mappe un tunnel à son PDR et FAR.
- **PDR Descendante** : identifiée par l'IP UE, qui mappe le lien descendant d'un abonné à son PDR et FAR.
- **FAR** : les actions de transfert, avec action décodée, IP distante, TEID sortant et création d'en-tête externe.
- **QER** : les entrées QoS, avec QFI, état de la porte et limites de débit.
- **URR** : les compteurs d'utilisation, avec les volumes montants/descendants actuels et dernier rapportés.

Cliquez sur n'importe quelle ligne pour **modifier l'entrée de carte brute**, qui est un outil de dépannage et de réparation de bas niveau. PFCP pilote normalement entièrement les cartes, donc vous modifiez manuellement une entrée pour le diagnostic plutôt que pour l'opération de routine.

Configuration

Une vue en lecture seule de la façon dont la UPF est configurée : son identité **réseau** (ID de nœud, adresse et port PFCP, port API, adresses N3 et N9), les **fonctionnalités** qu'elle a activées (FTUP, UEIP, le gestionnaire de routes et son type, et le mode d'attachement XDP : natif, générique ou déchargé), l'intervalle de **battement de cœur PFCP**, les paramètres de délai d'attente et de réessai, et les adresses **dataplane** N3/N9. Un basculement **JSON brut** montre le document de configuration complet pour le support. C'est ici que vous confirmez qu'une UPF est dimensionnée et adressée comme prévu.

Diagnostics

Exécute un **ping depuis le nœud UPF** vers un hôte cible. Entrez une cible et un nombre de paquets, et la sortie brute du ping revient avec un verdict de succès/échec. C'est un moyen rapide de confirmer que la UPF a une connectivité au réseau de données (par exemple vers un serveur DNS ou une passerelle en amont) depuis l'endroit où les paquets partent réellement, sans avoir à se connecter au nœud.

Jardin Clos

Le **jardin clos** : transfert restreint pour les sessions qui doivent atteindre uniquement un portail captif avant d'être authentifiées ou habilitées. Lorsque vous activez une redirection sur le SEID d'une session, cela réécrit le flux descendant afin que l'appareil aille à une **URL de redirection / IP de portail** au lieu d'Internet ouvert. L'onglet liste chaque **redirection active** avec l'IP UE, l'IP du portail, l'URL de redirection, l'IP gNB et les TEID impliqués. Pour libérer la session pour un transfert normal, supprimez la redirection. Une **liste blanche** d'IP ou de CIDR nomme les destinations qu'une session de jardin clos est encore autorisée à atteindre directement (par exemple le portail et ses actifs). Vous pouvez également activer et supprimer des redirections par session depuis la page de détail de la session.

Journaux

L'onglet **Journaux** suit la sortie de journal en direct de la UPF pour le dépannage d'une seule instance sans quitter OmniWeb.

Tableaux de bord de surveillance

Le débit, les taux de paquets par interface, les tendances du nombre de sessions et d'autres séries temporelles pour la UPF sont présentés sous forme de tableaux de bord Grafana, accessibles depuis la page de l'élément. OmniWeb ne duplique pas ces graphiques nativement.

Liés

- **SGW-C** : le pair de contrôle EPC qui programme cette UPF (en tant que SGW-U) via **Sxa/PFCP** et transfère le trafic sur **S1-U / N3**.
- **PGW-C / SMF** : ancre la connexion PDN et, en tant que SMF, programme le plan utilisateur 5G via **N4/PFCP**.

- **MME** : pilote la configuration des porteurs qui installe finalement les sessions vues ici.
- **SCEF** : transporte de petits payloads non-IP via le plan de contrôle et contourne délibérément ce plan utilisateur.
- [Guide des opérations](#) : retour à l'index des éléments.

