UZ801 LTE MiFi dongle — تفعيل ADB تلقائيًا (جانب المضيف)

تقوم دونجل Qualcomm LTE MiFi الرخيصة (~10 دولارات) (`05c6:90b6`, "Android"/UZ801, msm8916) بالتمهيد في **وضع RNDIS** مع واجهة ويب على `http://192.168.100.1`. إن الحصول على `http://192.168.100.1/usbdebug.html` يحولها إلى **وضع ADB** (وهي تأتي مفعلّة بالفعل). المرجع: https://nickvsnetworking.com/adventures-with-a-10-lte-mifi-dongle/

يجب أن تتم خطوة التفعيل على **المضيف** الهايبرفايزر (Proxmox)، لأن المضيف فقط هو غير LXC في OmniWeb إلى `192.168.100.1` — يعمل وكيل الهاتف RNDIS الذي لديه رابط ويصل إلى الدونجل فقط كجهاز USB في وضع ADB. لذا فإن بمجرد أن يكون الدونجل المميز (CT 102) هذه الأتمتة هي udev + systemd وليس كود الوكيل، على جانب المضيف.

الملفات

- `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
```

التدفق: توصيل الدونجل (RNDIS) → udev يتم تشغيله → `mifi-adb-enable.service` → الدونجل يعيد التشغيل → `usbdebug.html` لـ curl ويقوم بعمل، RNDIS السكربت يبدأ واجهة تسلم (أدناه) CT-102 الخاصة بـ udev قاعدة → ADB يعيد العد مع واجهة ADB → إلى وضع يتم تشغيل السكربت، adb، ذلك. عند إعادة العد في وضع `adb` العقدة إلى الحاوية → يرى وكيل مرة أخرى، ويكتشف واجهة ADB (`ff/42/01`) — لا حلقة وينتهي.

تغيير udev لتمرير USB CT-102 (مطلوب)

يجب تسليم VID Qualcomm `05`الخاص بالدونجل `c6` إلى الحاوية، ويجب أن تكون المجموعة (المستخدم adb) وليس جذر الحاوية، أو لا يمكن لوكيل، **plugdev (gid 100046 (المضيف** فتح العقدة. ينطبق نفس الشيء على قواعد الهاتف (plugdev عضو في، `omniweb-agent` التي لا يمكن للوكيل الوصول إليها — كانت (جذر الحاوية) `GROUP="100000"` كانت :Android من وقت العد وسقطت في كل إعادة عد. تم fd يحتفظ بـ adb الأجهزة تعمل فقط بينما كان إصلاحها إلى `GROUP="100046"`.

في `/etc/udev/rules.d/99-ct102-android.rules` تستخدم جميع قواعد الهاتف `OWNER="100000", GROUP="100046", MODE="0660"`، بالإضافة إلى VID الدونجل:

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

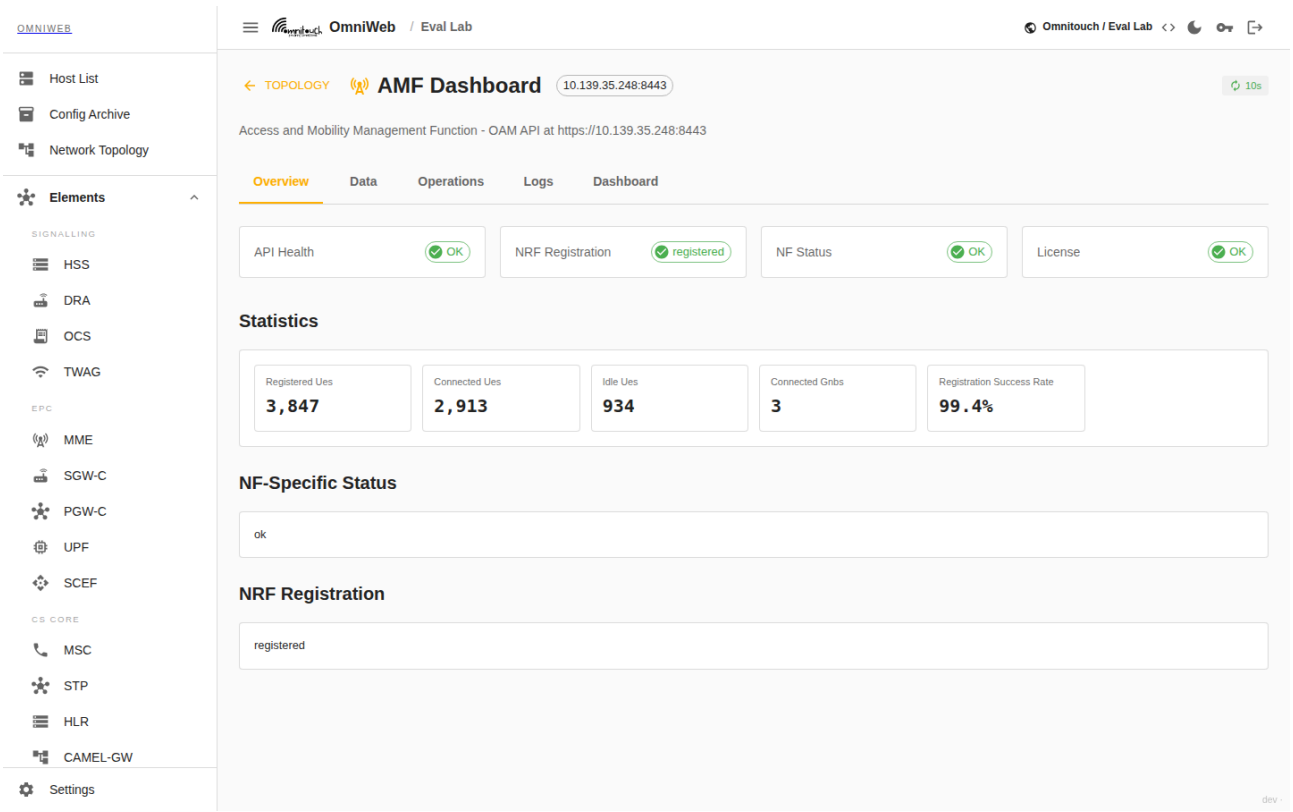
> يتم تطبيق هذه التغييرات على المضيف مباشرة في المختبر ولكن يجب توثيقها في OmniCore ansible (دور المراقبة/المضيف) حتى تبقى بعد إعادة بناء المضيف.

AMF: وظيفة إدارة الوصول والحركة

تعتبر **AMF** نقطة التحكم الأساسية في نواة 5G. إنها تنهي إشارة **N1** إلى UE وارتباط **N2** (NGAP) بكل gNodeB. تتعامل مع إدارة التسجيل والاتصال: تقوم بإرفاق UEs، وتحافظ على إمكانية الوصول إليهم، وتقوم بإرسال إشعارات لهم عندما يكونون في حالة خمول. تمتلك **سياقات** **UE** (SUPI واحدة لكل مشترك مسجل، مفاتيحها بواسطة) و**ارتباطات** **gNB** (واحدة لكل راديو متصل، مفاتيحها بواسطة SCTP). تختار SMF لكل جلسة PDU وتنقل طلبات الجلسة بين UE وSMF. عندما يكون المشترك على الشبكة، فإن AMF هي NF التي تعرف مكانه وكيفية الوصول إليه.

← 5G Core

في لوحة التحكم



تفتح لوحة التحكم AMF بأربع بطاقات صحة قياسية: **صحة** AMF (ما إذا كانت **NRF** **تسجيل**، **API**، **ترخيص**. كل منها يستعلم على فترات. أدناه، تظهر البيانات، **حالة** **NF**، مسجلة حاليًا مع NRF).

التي تمتلكها AMF:

- **قائمة UE**: كل سياق UE تحتفظ به AMF، مفاتيحها بواسطة SUPI، مع حالة التسجيل والاتصال الخاصة بها. هذه هي عرض "من متصل الآن". اختر UE لفتح سياقها التفصيلي. يمكن لـ AMF أيضًا سرد جلسات PDU النشطة لـ UE بواسطة SUPI.
- **gNodeBs**: الراديوهات المتصلة، صف واحد لكل ارتباط SCTP. تقوم الجدول بفك تشفير القيم الخام لـ NGAP إلى **gNB-ID**، **TAC** (منطقة التتبع)، **PLMN**، و**SST** (نوع الشريحة/الخدمة). يمكن للمشغل تأكيد أي الخلايا تعمل وأي مناطق تتبع وشرائح تخدمها. التفصيلي بواسطة معرف ارتباط gNB دون فك تشفير المعرفات يدويًا. اختر صفًا لفتح SCTP الخاص به.
- **الإحصائيات**: العدادات الحية لـ AMF (UEs المسجلة، gNBs المتصلة، وأحجام الإشارات)، لقراءة سريعة عن الحمل والنشاط.
- **وضع الصيانة**: ما إذا كانت AMF في وضع الصيانة. استخدمه لتفريغ أو احتجاز عقدة أثناء العمل المخطط.
- **التكوين**: التكوين في وقت التشغيل الذي تستخدمه الخدمة حاليًا.

الإجراءات

تظهر لوحة التحكم إجراءات للتعافي من الحالة العالقة. تؤكد لوحة التحكم كل واحدة قبل تنفيذها، لأنها تقوم بمسح الحالة الحية:

- **مسح جميع سياقات UE** (جملة): يزيل كل سياق UE من AMF. استخدمه كملاذ أخير متأثر إعادة التسجيل UE لاستعادة عقدة تحتفظ بسياقات قديمة أو تالفة. يجب على كل.
- **مسح الذاكرة المؤقتة** (جملة): يمسح ذاكرة اكتشاف AMF وذاكرات NF الخاصة بـ UE. بناءً على بيانات نظير أو بحث قديمة، على سبيل AMF استخدمه عندما تتصرف أو أعيد تسجيله NF المثال بعد أن انتقل.
- **إلغاء التسجيل** (لكل UE): يلغي تسجيل UE واحد وينظف حالته. استخدمه لإسقاط سياق مشترك واحد لن يتم مسحه بمفرده، بدلاً من إعادة تعيين العقدة بالكامل.

عن عناصر تحكم استرداد أكثر دقة AMF الخاص بـ API OAM بعيدًا عن أزرار لوحة التحكم، يكشف يمكن للمشغل الوصول إليها من خلال الوكيل الخلفي:

- **فصل gNB بالقوة**: يقوم بتفكيك gNB واحد بواسطة معرف ارتباط SCTP الخاص به. استخدمه لمسح ارتباط راديو عالق أو غير متصرف دون لمس الآخرين.
- **تحرير جلسة PDU بالقوة**: يحرر جلسة PDU واحدة بواسطة معرف `supi:psi` مسجلاً UE بينما يبقى AMF الخاص بها. استخدمه لإسقاط جلسة عالقة على جانب.

- **إلغاء تسجيل UE أو إرسال إشعار إلى**: يجبر UE على إلغاء التسجيل، أو يرسل إشعارًا إلى UE. استخدم الإشعارات لاختبار إمكانية الوصول إلى UE الخامل لإعادته إلى الاتصال. استخدم الإلغاء القسري للتسجيل لطرد UE بشكل نظيف.

العمليات

- **تشخيصات وقت التشغيل** (`/api/oam/diagnostics`): تظهر التشخيصات على مستوى منخفض للخدمة الجارية.
- **استخدام الموارد** (`/api/oam/resources`): تقارير عن استخدام الذاكرة والعمليات والجدولة في وقت التشغيل لفحص صحة العقدة.
- **الأقران** (`/api/oam/peers`): تسرد URIs الأقران NF المكونة والمكتشفة حالية، حتى يتمكن المشغل من رؤية من تتحدث إليه AMF والارتباطات SCTP.
- **ذاكرة اكتشاف NRF** (`/api/oam/nrf_discovery`): تظهر محتويات ذاكرة الاكتشاف: أي مثيلات NF التي تعلمت عنها AMF من NRF.
- **تعيين مستوى السجل** (`/api/oam/log_level`): يغير مستوى السجل في وقت التشغيل (واحد من `emergency`، `alert`، `critical`، `error`، `warning`، `warn`، `notice`، `info`، `debug`) لزيادة التفاصيل أثناء استكشاف الأخطاء وإصلاحها.
- **إعادة تسجيل NRF بالقوة** (`/api/oam/nrf/reregister`): يعيد تسجيل AMF مع NRF. استخدمه لاستعادة تسجيل تم إسقاطه أو قديم.

ذات صلة

- SMF: وظيفة إدارة الجلسات: تختار AMF SMF وتنقل طلبات جلسة PDU إليه.
- UDM: إدارة البيانات الموحدة: بيانات المشترك التي تستخدمها AMF أثناء التسجيل.
- AUSF: وظيفة خادم المصادقة: تصادق على UE أثناء التسجيل نيابة عن AMF.
- NSSF: وظيفة اختيار شريحة الشبكة: تحل اختيار الشريحة لـ AMF.
- ← 5G Core: نظرة عامة على جميع لوحات معلومات NF.

AUSF: وظيفة خادم المصادقة

تقوم **AUSF** بمصادقة المشتركين نيابة عن AMF. عندما يتصل UE، يطلب AMF من AUSF تشغيل 5G-AKA (أو EAP-AKA') للحصول على مواد المفتاح، **UDM** مع AUSF لذلك المشترك. تعمل وتؤكد نتيجة المصادقة. تحتفظ بجلسة مصادقة، AMF وتستخرج مفتاح التثبيت الذي تعيده إلى نشطة لكل مصادقة قيد التنفيذ أو تم إنشاؤها حتى يتمكن المشغل من تتبع تقدمها ونتيجتها، وإذا لزم الأمر، مسحها.

← 5G Core

في لوحة التحكم

تفتح لوحة تحكم AUSF الأعلى عبر بطاقات الصحة القياسية (هل **NRF** **تسجيل**، **API** **صحة**) مع كل منها يستعلم على فترات. تحتها توجد، (**وترخيص**، **NF** **حالة**، NRF؟)، تم تسجيل AUSF مع أقسام البيانات الخاصة بـ AUSF، تُقرأ مباشرة من واجهة OAM الخاصة بها عبر وكيل OmniWeb:

- **الإحصائيات** AUSF (`AUSF Statistics`)، التي تعطي رؤية للعدادات الخاصة بـ مستمرة لنشاط المصادقة.
- **جلسات المصادقة النشطة لـ AUSF**: قائمة بجلسات المصادقة التي تحتفظ بها AUSF حاليًا (`List Active AUSF Authentication Sessions`). يتم تحديد كل صف بواسطة معرف الجلسة الخاص به، بحيث يمكن للمشغل رؤية أي المصادقات قيد التنفيذ أو تم إنشاؤها بنظرة سريعة.

الإجراءات

تقوم كلا الإجراءين بمسح حالة المصادقة وتطلب التأكيد أولاً، لأنها إجراءات مدمرة:

- **مسح جلسة مصادقة محددة** (لكل صف): يزيل جلسة مصادقة واحدة بواسطة معرفها. استخدم هذا لإسقاط جلسة عالقة أو قديمة دون إزعاج مصادقات المشتركين الآخرين.
- **مسح جميع جلسات المصادقة**: يزيل كل جلسة مصادقة تحتفظ بها AUSF. استخدم هذا لاستعادة AUSF في حالة عالقة واسعة النطاق. يعيد كل مشترك متأثر المصادقة من محاولته التالية.

العمليات

تحكمات OAM القياسية المتاحة على AUSF:

- **التشخيصات** (`/api/oam/diagnostics`): تشخيصات وقت التشغيل للخدمة.
- **الموارد** (`/api/oam/resources`): استخدام موارد الخدمة.
- **إعادة تسجيل NRF بالقوة** (`/api/oam/nrf/reregister`): يجعل AUSF يعيد التسجيل مع NRF، لاستعادة إذا كانت تسجيله قد أصبحت قديمة.

ذات صلة

- AMF: إدارة الوصول والتنقل: يطلب المصادقة من AUSF لكل UE متصل.
- UDM: إدارة البيانات الموحدة: تزود مواد المفتاح التي تستخدمها AUSF لمصادقة مشترك.
- ← 5G Core: نظرة عامة على لوحة تحكم 5GC وNFs الأخرى.

BSF: وظيفة دعم الربط

تقوم **BSF** بتسجيل وحل الربط بين جلسة PDU لجهاز المستخدم (UE) و PCF الذي يخدمها. عندما يتم إنشاء جلسة، تسجل BSF أي PCF يتعامل مع السياسة لتلك الجلسة، معتمدة على معرفات الجلسة: عنوان IP لجهاز المستخدم، DNN، و S-NSSAI. ثم تستفسر NFs ووظائف التطبيقات الأخرى لاكتشاف BSF الصحيح لجلسة معينة لجهاز المستخدم، بحيث تصل طلبات السياسة بربط واحد BSF الذي يحمل بالفعل سياق تلك الجلسة بدلاً من واحد عشوائي. تحتفظ PCF إلى نشطة وتعرضها، مع إحصائيات ملخصة، للمراقبة PDU لكل جلسة.

← 5G Core

في لوحة التحكم

تفتح لوحة تحكم BSF في الأعلى القياسية بطاقات الصحة مع (هل تم **NRF تسجيل**، **API صحة**، كل منها يستعلم في فترة زمنية محددة. تحتها، و **ترخيص**، **NF حالة**)، تسجيل BSF مع NRF؟). توجد أقسام بيانات BSF، تُقرأ مباشرة من واجهة OAM الخاصة بها عبر وكيل OmniWeb:

- **ربط PCF**: حالياً BSF قائمة الروابط النشطة التي تحتفظ بها (`List all PCF bindings with binding ID, UE IP, DNN, S-NSSAI, PCF FQDN/IP`). يتم

تحديد كل صف بواسطة معرف الربط الخاص به ويظهر عنوان IP لجهاز المستخدم، الخاص بـ PCF أو FQDN التي تحدد الجلسة، جنباً إلى جنب مع S-NSSAI و DNN، يتعامل مع السياسة لهذه الجلسة لجهاز PCF الذي يخدمها. هذا يجيب على "أي المستخدم؟" (`Get detailed PCF binding by binding ID`) بنظرة سريعة. اختر ربطاً لفتح تفاصيله الكاملة).

- **الإحصائيات** BSF (`BSF statistics: total bindings, bindings by DNN`): العدادات الخاصة بـ، والتي تعطي رؤية مستمرة لعدد الروابط النشطة إجمالاً وكيفية توزيعها حسب DNN.

الإجراءات

توجه لوحة تحكم BSF نحو القراءة والمراقبة. تعرض الروابط والإحصائيات للتفتيش ولا تكشف عن إجراءات مسح مدمرة على مستوى الصف أو NF.

العمليات

التحكم القياسي في OAM المتاح على BSF:

- **إعادة تسجيل NRF بالقوة** (`/api/oam/nrf/reregister`): يجعل BSF يعيد التسجيل مع NRF، للتعافي إذا كانت تسجيله قد انتهت صلاحيتها.

ذات صلة

- PCF: التحكم في السياسة: NF الذي تشير إليه كل ربط. BSF هو الطريقة التي يجد بها PCF المستهلكون الصحيح لجلسة جهاز المستخدم.
- SMF: مستهلكو Nbsf ووظائف التطبيقات: إدارة الجلسات الذين يسجلون ويبحثون عن الروابط مع قدوم الجلسات وذهابها.
- ← 5G Core: نظرة عامة على لوحة تحكم 5GC و NFs الأخرى.

CHF: وظيفة الشحن

تقدم **CHF** (وظيفة الشحن) 5 شحنًا متقاربًا عبر الإنترنت وغير متصل لشبكة G Core. تستهلكها حصص الاستخدام، CHF حركة المرور، تدير PDU حيث تحمل جلسات :N40 عبر واجهة SMF وتقوم بتقييم تلك الاستخدامات من خلال محرك التقييم/الشحن، وتولد سجلات بيانات الشحن (CDRs) التي تغذي الفوترة والتسوية. تعرض لوحة التحكم الخاصة بها جلسات الشحن الحية، المكتمل. يمكن للمشغل بعد ذلك الإجابة على "هل CDR وصحة الرابط إلى محرك التقييم، وتاريخ يتم شحن المشترك بشكل صحيح، وهل يمكن الوصول إلى محرك التقييم؟" دون مغادرة OmniWeb.

← 5G Core

في لوحة التحكم

مع CHF هل تم تسجيل (**NRF تسجيل**، **API صحة**) في الأعلى توجد **بطاقات الصحة** القياسية كل منها يستعلم في فترة زمنية معينة. أدناه، يتم تحديث أقسام ،(و**الرخصة**، **NF حالة**، NRF؟)، البيانات الخاصة بـ CHF تلقائيًا:

- **جلسات الشحن النشطة**: الجلسات الحية التي تقوم CHF بقياسها، كل منها يظهر مرجع الشحن الخاص بها (`chargingDataRef`)، المشترك (SUPI)، DNN، الاستخدام المتراكم، وطوابع الزمن للبداية/التحديث. هذه هي مجموعة العمل لـ "من يتم شحنه الآن".
- **الإحصائيات**: عرض ملخص لإجمالي الجلسات، الاتصال بمحرك التقييم/الشحن، وإجمالي حجم الشحن.
- **صحة الاتصال بمحرك التقييم**: فحص صحة مخصص يؤكد أن CHF يمكنها الوصول إلى محرك التقييم/الشحن الذي يقوم بالتقييم الفعلي. إذا كانت هذه غير صحية، فلا يمكن لـ CHF تقييم الجلسات والشحن في خطر.
- **بحث CDR المكتمل**: عرض قابل للبحث على CDRs النهائية، قابل للتصفية حسب SUPI، DNN، ونطاق التاريخ، لتأكيد ما سجلته CHF بعد انتهاء الجلسة.
- **التكوين**: تكوين وقت التشغيل لـ CHF كما تراه الخدمة حاليًا.

اختر جلسة لفتح تفاصيلها الكاملة حسب مرجع بيانات الشحن، والذي يظهر حالة الاستخدام والقياس الكاملة لتلك الجلسة الواحدة.

الإجراءات

- **إلغاء جلسة الشحن**: ينهي جلسة الشحن الجارية حسب `chargingDataRef` الخاص بها، بحيث تتوقف عن تحتفظ SMF بها. استخدم هذا لمسح جلسة عالقة أو يتيمة لم تعد استهلاك الحصة وحالة القياس.
- **بحث CDRs**: يستعلم عن تاريخ CDR المكتمل حسب SUPI، DNN، ونطاق التاريخ. يدعم استخدم هذا بعد انتهاء الجلسة لتأكيد ما تم تقييمه وتسجيله من قبل CHF. استفسارات الفوترة، والتحقيق في النزاعات، أو فحص عشوائي للتأكد من أن CHF تكتب الشحن بشكل صحيح.

العمليات

- **تعيين مستوى السجل**: يغير verbosity سج�� CHF في وقت التشغيل (طوارئ، تنبيه، حرجة، خطأ، تحذير، تحذير، إشعار، معلومات، تصحيح) لجمع مزيد من التفاصيل أثناء التحقيق في مشكلة الشحن، ثم العودة إلى الوضع الطبيعي.
- **إجبار إعادة تسجيل NRF**: يجعل CHF تعيد تسجيل نفسها مع NRF. استخدمه قادرة على اكتشافها SMF قد خرجت من السجل ولم تعد CHF للتعافي إذا كانت.

ذات صلة

- SMF: المستهلك N40 الذي يدفع الشحن حيث تحمل جلسات PDU حركة المرور.
- PCF: الجانب السياسي من التحكم في السياسة والشحن الذي يحكم ما تقيسه CHF.
- محرك التقييم/الشحن (OCS): النظام downstream الذي تقوم CHF من بالتقييم خلاله. تعكس بطاقة صحة الاتصال بمحرك التقييم الرابط إليه.
- ← 5G Core: نظرة عامة على جميع لوحات معلومات NF.

NRF: وظيفة مستودع الشبكة

تُبنى نواة 5G بالكامل حول سجل **NRF**. يقوم كل NF عند بدء التشغيل، بتسجيل **ملف NF** آخر يقدمها، وسعته وأولويته. ثم يكتشف PLMNs، نوعه، عناوينه الخاص به مع NRF: **الخدمات** التي يقدمها، وسعته وأولويته. يحتفظ NRF بـ**اشتراكات** عن المتاح. يتتبع NRF الأقران من خلال سؤال كل مثيل مسجل. **حالة** عندما يأتي أو يذهب أحد الأقران الذي يعتمد عليه. يراقب NF **تغيير الحالة**، بحيث يمكنه إبلاغ إلى العثور على آخر، NF **نبضات القلب** لإنهاء المثيلات التي تتوقف عن التحقق. عندما يحتاج أي فإن NRF هو مصدر الحقيقة لما هو متاح وكيفية الوصول إليه.

← نواة 5G

في لوحة التحكم

يمتلك NRF القياسية لأنه يمتلك السجل الذي تكتشف NF لوحة تحكم مخصصة، أغنى من صفحة NRF (ما إذا كان **تسجيل NRF**، **API** من خلاله بقية النواة. تفتح مع بطاقات الصحة القياسية: **صحة** NRF (نفسه مسجلاً)، **حالة NF**، يقوم كل منها بالاستطلاع على فترات **وترخيص**.

إجمالي المثيلات، ،**NF** فوق البيانات، تظهر أربع **بطاقات قياس** تلخص السجل: **أنواع المسجلة** (مع شريط نسبة مئوية من الإجمالي)، و**الخدمات** (مع عدد الاشتراكات). أسفلها توجد وجهات نظر NRF الأساسية:

- **مثيلات NF المسجلة**: كل مثيل مسجل، مجمعة حسب **نوع NF** (AMF، SMF، UDM، PCF، وهكذا). تُظهر تقوم لوحة التحكم بتشفير لون كل بطاقة مثيل حسب النوع. اختر مثيلًا لفتح **ملف** PLMN. البطاقة حالة تسجيلها، مؤقت نبض القلب، عدد الخدمات، و مع رابط **فتح لوحة** NRF، الكامل الخاص به: السجل التفصيلي الذي يحتفظ به **NF** الخاصة به وزر NFs لصفحة **التحكم** NF أي "هذه هي وجهة النظر **إلغاء التسجيل**. متاحة وهل هي جميعها مسجلة؟".
- **الخدمات المسجلة**: جدول مسطح لكل خدمة يعلن عنها كل مثيل، مع إصداراتها وحالتها. يمكن للمشغل رؤية ما هي القدرات التي تقدمها النواة حاليًا عبر جميع NFs.
- **الاشتراكات**: اشتراكات تغيير حالة NF المحتفظ بها حاليًا. كل منها هو طلب قائم من NF ليتم إخطاره عندما تتغير حالة أحد الأقران.
- **الإحصائيات**: العدادات الحية لـ NRF: إجمالي NFs وطلبات حسب النوع، الاشتراكات، الاكتشاف، لقراءة سريعة على حجم السجل ونشاط البحث.

الإجراءات

تتيح لوحة التحكم إجراءات لإدارة السجل. تؤكد لوحة التحكم على كل واحدة قبل تنفيذها، لأنها تغير حالة التسجيل الحية:

- **إلغاء تسجيل مثيل NF** (لكل صف): يزيل تسجيل مثيل واحد من NRF. استخدمه بعد ذ��ك إعادة NF واحد. يجب على هذا NF لمسح تسجيل قديم أو عالق لمثيل الأخرى من اكتشافه مرة أخرى NFs التسجيل قبل أن تتمكن.
- **إلغاء تسجيل جميع NFs** (بالجملة): يزيل كل تسجيل من NRF دفعة واحدة. استخدمه كملاذ أخير لإعادة ضبط سجل يحتوي على إدخالات قديمة. يجب على كل NF بعد ذلك إعادة التسجيل.
- **إزالة اشتراك**: يحذف اشتراك تغيير حالة واحد. استخدمه لمسح اشتراك قديم أو يتيم لم يعد يحتاجه NF تركه.
- **تحديث ملف NF**: يقوم بتحديث ملف مثيل مسجل (على سبيل المثال سعته، أولويته، للاكتشاف نحو أو بعيدًا عن مثيل دون NRF أو حالته). يمكن للمشغلين ضبط كيفية توجيه إلغاء تسجيل.

العمليات

مزيدًا من التحكمات التي يمكن للمشغل NRF الخاصة بـ OAM تتيح واجهة برمجة التطبيقات الوصول إليها من خلال الوكيل الخلفي:

- **تشخيصات وقت التشغيل** (`/api/oam/diagnostics`): تظهر تشخيصات منخفضة المستوى للخدمة الجارية.
- **استخدام الموارد** (`/api/oam/resources`): تقارير عن استخدام الذاكر�والعمليات والجدولة في وقت التشغيل لفحص صحة العقدة.
- **فحص نبض القلب يدويًا** (`/api/oam/heartbeat`): يُفعّل فحص نبض القلب عند الطلب لمثيل NF. يؤكد ما إذا كان NF لا يزال نشطًا بدلاً من الانتظار لمؤقت النبض الخاص به.
- **مدة تشغيل NF** (`/api/oam/nf_uptime/{id}`): يظهر وقت تسجيل مثيل وما مدى طول فترة تسجيله، لتأكيد مدى طول فترة تشغيل NF.
- **تعيين مستوى السجل** (`/api/oam/log_level`): يغير مستوى السجل في وقت التشغيل (واحد من `emergency`، `alert`، `critical`، `error`، `warning`، `warn`، `notice`، `info`، `debug`) لزيادة التفاصيل أثناء استكشاف الأخطاء وإصلاحها.
- **فرض إعادة تسجيل NRF** (`/api/oam/nrf/reregister`): يعيد تسجيل NRF. استخدمه لاستعادة تسجيل ذاتي تم إسقاطه أو قديم.

ذات صلة

- AMF: وظيفة إدارة الوصول والتنقل: يسجل مع NRF ويكتشف أقرانه من خلاله، مثل كل NF أدناه.
- SMF: وظيفة إدارة الجلسات: يتم اكتشافه من خلال NRF لإدارة الجلسات.
- UDM: إدارة البيانات الموحدة: واحدة من NFs يحتفظ NRF بيانات المشترك التي بتسجيلاتها.
- PCF: وظيفة التحكم في السياسة: مسجلة مع NRF لاكتشاف السياسة.
- SCP: وكيل اتصالات الخدمة: يوجه الإشارات بين NFs باستخدام التسجيلات وبيانات الاكتشاف التي يحتفظ بها NRF.
- ← 5 نواةG: نظرة عامة على جميع لوحات تحكم NF.

NSSF: وظيفة اختيار شريحة الشبكة

تقوم **NSSF** باختيار مثيل (أو مثيلات) شريحة الشبكة و NSSAI المسموح به لـ UE. عندما تتعامل مقابل UE المطلوبة من S-NSSAIs حل NSSF مع تسجيل أو طلب شريحة، تطلب من AMF ومجموعة (NSI) بربط كل منها بمثيل شريحة الشبكة NSSF تقوم .PLMN الشرائح المكونة لذلك تحتفظ بتعريفات .UE المسموح به الذي يمكن أن يستخدمه NSSAI التي تخدمها، وتعيد AMF حتى يتمكن المشغل من التفكير في ومراقبة اختيار AMF لكل NSSAI الشرائح المكونة وتتتبع توفر الشريحة.

← 5G Core

في لوحة التحكم

تفتح لوحة تحكم NSSF القياسية عبر الأعلى (مع بطاقات الصح**NRF تسجيل**، **API صحة**، كل منها يستعلم على فترات. تحتها، (و **ترخيص**، **NF حالة**، NRF؟)، هل تم تسجيل (NSSF مع توجد أقسام بيانات NSSF، تُقرأ مباشرة من واجهة OAM API الخاصة بها عبر وكيل OmniWeb:

- **الشرائح**: كل S-NSSAI مكون، مدرج مع خرائط NSI ومجموعات AMF الخاصة به، و NSSAI المسموح به لكل PLMN التي تخدمه، و (`List all configured S-NSSAIs with NSI mappings, AMF sets, and allowed NSSAI per PLMN`). هذه هي الرؤية الرسمية لكيفية حل الشرائح المطلوبة إلى مثيلات الشرائح ومجموعات AMF لكل PLMN.
- **توفر NSSAI**: حالة توفر NSSAI لكل AMF (`Per-AMF NSSAI availability state`)، والتي تظهر أي الشرائح أبلغت كل AMF أنها يمكن أن تخدمها حالياً.
- **الإحصائيات**: العدادات الخاصة بـ NSSF (`NSSF statistics: total slices, NS selection request counts`)، والتي تعطي رؤية مستمرة لعدد الشرائح المكونة وحجم طلبات اختيار الشرائح.

تكوين الشريحة في (`Query Slice Configuration`) تظهر رؤية **تكوين الشريحة** المنفصلة للرجوع إليه NSSF وقت التشغيل لـ.

الإجراءات

تكون لوحة تحكم NSSF موجهة للقراءة والمراقبة. تظهر الشرائح، وتوفر NSSAI، والإحصائيات دون إجراءات تحكم لكل عنصر.

العمليات

هو NSSF الذي تعرضه OAM التحكم في:

- **عرض التكوين في وقت التشغيل** (`/api/oam/config`): التكوين المباشر في وقت التشغيل لـ NSSF.
- **إجبار إعادة تسجيل NRF** (`/api/oam/nrf/reregister`): يجعل NSSF يعيد التسجيل مع NRF، لاستعادة إذا كانت تسجيله قد انتهت صلاحيتها.

ذات صلة

- AMF: إدارة الوصول والحركة: يستعلم NSSF لحل S-NSSAIs المطلوبة إلى NSSAI الخادمة لـ UE المسموح به ومجموعة AMF.
- NRF: وظيفة مستودع الشبكة: حيث تسجل NSSF حتى يمكن اكتشافها من قبل NFs الأخرى.

- ← 5G Core: 5 نظرة عامة على لوحة تحكمGC و NFs الأخرى.

PCF: وظيفة التحكم في السياسة

تتخذ **PCF** 5 قرارات السياسة التي تفرضها بقية نواة 5G. إنها ترد على AMF عبر N15 بشأن **سياسة الوصول والتنقل (AM)**: القيود على التنقل و RFSP التي يحصل عليها UE عند التسجيل. إنها ترد على SMF عبر N7 بشأن **سياسة إدارة الجلسة (SM)**: قواعد PCC التي تحدد QoS وتقوم بربط ارتباطات سياسة PCF لكل جلسة، والتحكم في البوابة، ومراقبة الاستخدام. تقوم BSF بتخزين كل جلسة PCF بحيث يمكن لأي NF العثور على PCF الصحيح لجلسة UE الخاصة بـ SM من خلال UEs هي المكان للإجابة على "ما هي السياسات النشطة، لأي PCF معينة. لوحة معلومات OmniWeb. وجلسات، وهل هي كما أتوقع؟" دون مغادرة OAM محاطة بـ `{status, response}`، كل استجابة وتقوم لوحة المعلومات بفك تشفيرها لك.

← 5 نواةG

في لوحة المعلومات

مع PCF هل تم تسجيل) **NRF تسجيل**، **API صحة**) في الأعلى توجد أربع بطاقات صحة قياسية كل منها يقوم بالاستعلام على فترات. استخدم مؤشر الاستعلام في ،(و**ترخيص**، **NF حالة**، NRF؟)، الرأس لإيقاف التحديث أو قراءة وقت آخر تحديث. أسفل البطاقات توجد شريط **الإجراءات** (انظر أدناه)، ثم أقسام بيانات PCF، كل منها يقوم بالتحديث التلقائي.

الإحصائيات PCF (`GET /api/statistics`)، إجمالي ارتباطات السياسة، العدادات الحية لـ SMو AM تخدم سياسة PCF والعدادات الحالية. هذه هي القراءة الأسرع لمعرفة ما إذا كانت بنشاط.

سياسات AM: كل ارتباط سياسة AM نشط (`GET /api/am_policy`)، صف واحد لكل UE مسجل لسياسة التنقل المطبقة حاليًا على كل PCF لها. هذه هي رؤية AM سياسة AMF لدى.

سياسات SM: كل ارتباط سياسة SM نشط (`GET /api/sm_policy`)، صف واحد لكل جلسة، والذي (`GET /api/sm_policy/{id}`) بسياسة لها. اختر صفًا لفتح تفاصيله تحتفظ SMF PDU الكاملة لتلك الجلسة: QoS، قرارات الشحن ومراقبة، التحكم في البوابة، يعيد قواعد PCC الاستخدام التي تفرضها SMF.

سياق السياسة: عرض سياقات السياسة النشطة (`GET /api/policy_context`)، السياقات التي تحتفظ بها PCF عبر ارتباطاتها مع AMو SM. إنه مفيد لمصالحة ما تعتقد أنه نشط مقابل PCF وSMF وAMF.

التكوين PCF (`GET /api/oam/config`)، تكوين وقت التشغيل لـ الإعدادات التي يعمل بها الخدمة حاليًا.

الإجراءات

كل إجراء لكل صف يطلب تأكيدًا أولاً، حيث إن إزالة ارتباط نشط تعطل UE أو الجلسة التي تؤثر عليها.

إزالة سياسة AM: تحذف ارتباط سياسة AM، على أي صف من سياسات AM تلك (`DELETE /api/am_policy/{id}`). استخدمه لإزالة سياسة تنقل عالقة أو قديمة لواحد UE.

إزالة سياسة SM: تحذف ارتباط سياسة SM، على أي صف من سياسات SM تلك (`DELETE /api/sm_policy/{id}`). استخدمه لإسقاط سياسة جلسة لن يتم إزالتها بمفردها.

تحديث سياسة SM: يمكنك أيضًا تعديل ارتباط سياسة SM. أرسل `PATCH` أو `PUT /api/oam/sm_policy/{id}` لتحديث قواعد PCC على سياسة SM نشطة، بحيث يمكنك ضبط

للجلسة أو قرارات الشحن دون تفكيك الارتباط. استخدمه لإعادة دفع السياسة إلى جلسة QoS موجودة بدلاً من إزالتها وإعادة إنشائها.

العمليات

قسم العمليات يحمل عناصر التحكم الشائعة لكل NF:

- **التشخيصات** (`GET /api/oam/diagnostics`): تشخيصات وقت التشغيل للخدمة.
- **استخدام الموارد** (`GET /api/oam/resources`): الذاكرة، العمليات والمجدولات للخدمة الجارية.
- **الأقران** (`GET /api/oam/peers`): URIs الأقران NF المكونة التي تتحدث إليها PCF وحالة قابليتها للوصول.
- **ذاكرة اكتشاف NRF** (`GET /api/oam/nrf_discovery`): ذاكرة اكتشاف NRF، أو URIs NF المكونة التي تحل PCF الأقران من خلالها.
- **مستوى السجل** (`POST /api/oam/log_level`): تغيير مستوى السجل في وقت التشغيل. اختر واحدًا من الطوارئ، التنبيه، الحرج، الخطأ، التحذير، التحذير، الإشعار، المعلومات، أو التصحيح.
- **إعادة تسجيل NRF** (`POST /api/oam/nrf/reregister`): إجبار PCF على إعادة التسجيل مع NRF، على سبيل المثال بعد إعادة تشغيل NRF التي تركتها قديمة.

ذات صلة

- SMF: يطلب سياسة SM من PCF عبر N7 ويفرض قواعد PCC التي تعيدها PCF.
- AMF: يطلب سياسة AM من PCF عبر N15.
- BSF: وظيفة الربط التي تسجل PCF ارتباطات سياسة SM لأي NF بها بحيث يمكن العثور على PCF الخادم.
- CHF: وظيفة الشحن. تقود قرارات التحكم في الشحن لـ PCF ما تقاربه SMF عبر N40.
- ← 5G نظرة عامة على نواة

SCP: وكيل الاتصال بالخدمات

إن **SCP** 5 يجلس بين وظائف الشبكة في النواة 5G وينقل حركة المرور المعتمدة على الخدمات لها. الذي يقوم SCP، بدلاً من أن يتصل كل مستهلك مباشرة بكل منتج، يمكن توجيه الطلبات عبر NF المستهدف، مع توزيع الحمل عبر المثيلات NF بإعادة توجيه كل رسالة إلى مثيل صحي من نوع وإعادة المحاولة حول الفشل. يمكنه إجراء الاكتشاف نيابة عن المستهلك (الاكتشاف المفوض) بحيث، بمجرد أن يعرف نوع الهدف، يقوم بتوجيه الطلبات اللاحقة NF ويخزن إمكانية الوصول إلى دون الحاجة إلى بحث جديد. والنتيجة هي اتصال غير مباشر: لا يحتاج المنتجون والمستهلكون إلى التعامل مع التوجيه والتوازن وتجديد SCP معرفة أو الاحتفاظ بالاتصالات مع بعضهم البعض، ويتولى ذاكرة التخزين المؤقت في ما بينهم.

← النواة 5G

في لوحة التحكم

تعمل أربع **بطاقات صحة** عبر الجزء GC.في NF 5 نفس تخطيط كل صفحة SCP تتبع لوحة تحكم العلوي (**صحة API**، **تسجيل NRF** (هل تم تسجيل SCP نفسه مع NRF؟)، **حالة NF**، كل منها يستعلم في فترة زمنية محددة، (و**الرخصة**.

أسفل البطاقات، تعرض SCP بياناتها التشغيلية الخاصة:

- **صحة NF**: عرض موزع الحمل لـ NFs وعدد التي يتوسط لها، مع صحة كل مثيل قابلة للوصول وأيها الفشل SCP، بحيث يمكن للمشغل رؤية أي مثيلات منتجة تعتبرها تفشل.
- **ذاكرة التخزين المؤقت للاكتشاف**: محتويات ذاكرة التخزين المؤقت للاكتشاف الخاصة بها، ومعدلات النجاح/الفشل في TTLالمخزنة، و NF وأنواع ،SCP الخاصة بـ بتوجيه الطلبات المتكررة دون إعادة اكتشاف SCP الذاكرة. هذا هو ما يسمح لـ.
- **الإحصائي��ت**: معدل مرور SCP، تحليل الطلبات إجمالي الطلبات المتوسطة، المستهدف، ومعدل نجاح الذاكرة الإجمالي NF حسب نوع.
- **التكوين**: تكوين SCP الحالي أثناء التشغيل.

تتجدد كل قسم تلقائيًا، وترتبط قيم نوع NF بلوحة التحكم الخاصة بذلك NF.

الإجراءات

لا تعرض لوحة تحكم SCP أزرار إجراءات مدمرة على مستوى أو لكل صف. إنها تتوسط حركة NF المرور بدلاً من امتلاك حالة الجلسة أو المشترك التي قد يقوم المشغل بمسحها. ومع ذلك، فإن للمشغل عرض ذاكرة التخزين المؤقت OAM API ذاكرته المؤقتة قابلة للإدارة: تتيح واجهة اكتشاف ذلك الهدف في الطلب التالي (انظر SCP للاكتشاف وطرد إدخال قديم واحد بحيث يعيد **العمليات**). لاستعادة من منتج تم نقله أو استبداله ولكنه لا يزال مخزناً كقابل للوصول، قم بمسح إدخاله.

العمليات

تتيح واجهة OAM API ��ـ لخاصة SCP التحكمات التالية:

- **عرض / إدارة ذاكرة التخزين المؤقت للاكتشاف**: قراءة ذاكرة التخزين المؤقت الحالية للاكتشاف، وحذف إدخال ذاكرة مؤقتة فردي حسب المعرف لفرض إعادة اكتشاف ذلك الهدف.
- **عرض تكوين وقت التشغيل**: قراءة تكوين SCP المباشر.

- **تعيين مستوى السجل**: تغيير وضوح السجل أثناء التشغيل. اختر واحدًا من `emergency`، `alert`، `critical`، `error`، `warning`، `warn`، `notice`، `info`، أو `debug`.
- **فرض إعادة تسجيل NRF**: جعل SCP يعيد تسجيل نفسه مع NRF. هذا مفيد بعد أن يتم إعادة تشغيل NRF أو SCP وقد انتهت صلاحية التسجيل.

ذات صلة

- NRF: السجل الذي يكتشف SCP من خلاله ويعيد التسجيل معه.
- AMF، SMF، UDM، AUSF، PCF، CHF، NSSF، BSF: NFs التي يمكن لـ SCP أن يتوسط حركة المرور المعتمدة على الخدمات الخاصة بها والتي يخزن إمكانية الوصول إليها.
- ← 5 النواةG: نظرة عامة على قسم 5 GC المشتركة وتخطيط لوحة التحكم.

SMF: وظيفة إدارة الجلسات

تمتلك **SMF** جلسة PDU. تقوم بإنشاء وتعديل وإصدار جلسة بيانات كل UE، وتخصص لـ UE عنوان IP من مجموعة محلية، وتدير مستوى المستخدم عبر UPF بقواعد اكتشاف الحزم، وإعادة التوجيه، وجودة الخدمة لكل جلسة. كما تتواصل مع PCF (N7) لسياسة الجلسة و CHF (N40) للفوترة. استخدم لوحة معلومات SMF للإجابة على "هل الجلسات قيد الإنشاء، هل لا تزال مرتبطة بـ UPF دون مغادرة الخاص بها، وهل تنفد العناوين؟" تقوم SMF بتغليف كل استجابة OAM `{status, response}`. تقوم لوحة المعلومات بفك تغليفها لك.

← 5G Core

في لوحة المعلومات

في الأعلى توجد أربع بطاقات صحة قياسية: **صحة** مسجلة مع NRF (هل SMF **تسجيل** NRF، **API** والرخصة. كل منها يقوم بالاستطلاع على فترات. استخدم مؤشر الاستطلاع، **حالة NF**، NRF؟)،

في الرأس لإيقاف التحديث أو قراءة وقت التحديث الأخير. أسفل البطاقات توجد شريط **الإجراءات** (انظر أدناه). ثم تأتي أقسام بيانات SMF، كل منها يقوم بتحديث تلقائي.

الإحصائيات SMF (`GET /api/statistics`): / إجماليات إنشاء الجلسات: العدادات الحية لـ SMF تقوم فعلاً تعديلها / إصدارها وعدد الجلسات الحالية. هذه هي أسرع قراءة لمعرفة ما إذا كانت بإنشاء جلسات.

جلسات PDU: كل جلسة PDU نشطة (`GET /api/pdu_session`)، تُرجع كـ `{ pdu_sessions: [...], total }`. تحمل كل صف كلاً من `sm_context_ref` (UUID يحدد سياق SM فريداً عبر **ليس** 3GPP PSI)، `pdu_session_id` (عدد صحيح صغير و بشكل فريد لذلك، كل عملية لكل جلسة. (بترقيم جلساته من قاعد�� منخفضة UE حيث يقوم كل UEs، تمرر عملية **الإصدار** UUID لكل صف `sm_context_ref`. (بحث التفاصيل وإصدارها) تعتمد على والحالة UE المخصص لـ IP للجلسة، عنوان DNN بجانب المعرفات، يظهر الصف PSI. بدلاً من.

مجموعة IP: مجموعة العناوين التي تخصص منها SMF عناوين IP لـ UE (`GET /api/ip_pool/detail`): ملخص المجموعة (الشبكة الفرعية، الإجمالي، الأعداد المخصصة قريبة من SMF والمتاحة) بالإضافة إلى قائمة بالعناوين المخصصة حالياً. هنا يمكنك رؤية ما إذا كانت استنفاد مساحة عناوينها.

ارتباط UPF: حالة رابط N4/PFCP إلى مستوى المستخدم (`GET /api/upf`): ما إذا كانت مرتبطة حالياً بـ SMF الخاص بها. إذا فشلت الجلسات في الإنشاء، تحقق من هذا أولاً UPF.

أقران PFCP: حالة ارتباط نظير PFCP (UPF) (`GET /api/oam/pfcp_peers`): رؤية SMF لكل UPF ترتبط به عبر N4، بما في ذلك حالة الارتباط.

الإجراءات

تطلب كل إجراء تأكيد أولاً. العديد منها مدمرة للج��سات الحية.

إصدار جميع جلسات PDU: يقوم بإسقاط كل جلسة PDU وحالتها PFCP على UPF. استخدمه أو عند تصريف عقدة للصيانة UPF إلى حالة نظيفة، على سبيل المثال بعد تبديل SMF لإعادة.

مسح الذاكرة المؤقتة: يمسح ذاكرات الجلسات لـ SMF دون إصدار جلسة. استخدمه عندما تبدو قديمة أو غير متسقة مع الواقع SMF لوحة المعلومات أو العرض الداخلي لـ.

إعادة ارتباط PFCP: يعيد إنشاء ارتباط PFCP مع UPF (مبادرة SMF). استخدمه عندما ينقطع ارتباط UPF ولا يمكن إنشاء جلسات جديدة.

إعادة ارتباط UPF: يجبر إعادة ارتباط PFCP مع UPF. عنوان **المكون** UPF لا مدفوع بالتكوين. UPF الموجود بالفعل في تكوين UPF يعيد توجيه الارتباط إلى UPF. أو حقن UPF توجد هنا عملية إضافة SMF. في الممارسة العملية، يخدم نفس الغرض في الاسترداد مثل إعادة ارتباط PFCP.

إصدار DNN بواسطة: اكتب DNN في حقل **DNN** القابل للتحرير (على سبيل المثال `internet`). استخدمه لتصريف أو إعادة تعيين شبكة DNN. هذا يصدر **جميع** الجلسات على ذلك APN/DNN واحد، دون لمس بيانات واحدة، على سبيل المثال لإجبار UEs على الخروج من الجلسات على DNNs الأخرى.

إصدار لكل صف: في أي صف من جلسات PDU، **إصدار** يقوم بإسقاط تلك الجلسة الواحدة، لذا فإنه يستهدف `sm_context_ref`. يتم الإصدار بواسطة UPF الخاص بها على PFCP وسياق قد تشارك نفس UEs دائماً بالضبط الجلسة في ذلك الصف حتى لو كانت عدة `pdu_session_id`. استخدمه لإسقاط جلسة واحدة عالقة.

العمليات

تحمل قسم العمليات عناصر التحكم الشائعة لكل NF:

- **التشخيصات** (`GET /api/oam/diagnostics`): تشخيصات وقت التشغيل للخدمة.
- **استخدام الموارد** (`GET /api/oam/resources`): الذاكرة، العمليات، والجدولة للخدمة الجارية.
- **الأقران** (`GET /api/oam/peers`): URIs الأقران NF المكونة التي تتحدث إليها عبر أقران PFCP UPF وأقران PFCP أعلاه (SMF (AMF، PCF، CHF، NRF،).
- **مستوى السجل** (`POST /api/oam/log_level`): تغيير مستوى السجل في وقت التشغيل. اختر واحداً من الطوارئ، التنبيه، الحرجة، الخطأ، التحذير، التحذير، الإشعار، المعلومات، أو التصحيح.
- **إعادة تسجيل NRF** (`POST /api/oam/nrf/reregister`): إجبار SMF على إعادة التسجيل مع NRF، على سبيل المثال بعد أن تركها إعادة تشغيل NRF قديمة.

ذات صلة

- AMF: يطلب إعداد الجلسة من SMF عبر Nsmf.
- PCF: يوفر سياسة الجلسة لـ SMF عبر N7.
- CHF: وظيفة الفوترة التي تبلغ SMF عن الاستخدام عبر N40.

- UPF: نظير N4/PFCP لـ SMF. إنه مستوى المستخدم الذي تقوم SMF ببرمجته والارتباط به.
- ← 5 نظرة عامة علىG Core

UDM: إدارة البيانات الموحدة

إن **UDM** في نواة 5G هو سلطة بيانات الاشتراك. يتتبع يدير ملفات تعريف الاشتراك لكل مشترك مقابل مشترك. يوفر بيانات المصادقة المستخدمة SMF و AMF ويسجل UE خدم كل NFs أي مخزنه الداعم، ويخزنها مؤقتًا للبحث، **UDR** يقرأ السجلات الأساسية للمشتركين من UE. لتحدي مواد **AUSF** أثناء إعداد الجلسة. يستمد **SMF** أثناء التسجيل. يستشيره **AMF** السريع. يستشيره آخر إلى معرفة ملف تعريف مشترك أو أين تخدمه NF المصادقة الخاصة به منه. عندما يحتاج الشبكة، فإن UDM هو NF الذي يجيب.

← 5G Core

في لوحة التحكم

تفتح لوحة تحكم UDM **صحة** بأربع بطاقات صحة قياسية: **API**، **تسجيل NRF** (ما إذا كان UDM مسجلاً حاليًا مع NRF)، **حالة NF**، تظهر أدناه، كل منها يستعلم في فترة زمنية محددة. و **الرخصة**. البيانات التي يمتلكها UDM:

- **قائمة UE**: كل سياق UE يحتفظ به UDM، مفاتيحها بواسطة SUPI. هذه هي "أي UDM حاليًا" عرض. يمكن لـ UDM المشتركين يخدمهم أيضًا إرجاع سياق مفصل UDM الخدمية لذلك المشترك وبيانات NF يظهر تسجيلات SUPI. لمشترك واحد بواسطة الاشتراك المخزنة مؤقتًا.
- **الإحصائيات**: العدادات الحية لـ UDM، لقراءة سريعة عن الحمل والنشاط.
- **التكوين**: التكوين في وقت التشغيل الذي يستخدمه الخدمة حاليًا.

الإجراءات

تكشف لوحة التحكم عن إجراءات لمسح بيانات المشترك المخزنة مؤقتًا. تؤكد لوحة التحكم كل واحدة قبل تنفيذها، لأنها تسقط الحالة الحية:

- **مسح ذاكرة التخزين المؤقت للمشترك** (بالجملة): يمسح ذاكرة التخزين المؤقت لجميع بيانات المشتركين UDM على سبيل ملفات تعريف قديمة، عندما يخدم استخدمها. إعادة قراءتها بدلاً من UDM ويجب على UDR المثال بعد تغيير سجلات الاشتراك في تقديم نسخها المخزنة مؤقتًا.

بجانب زر لوحة التحكم، يكشف واجهة OAM API الخاصة بـ UDM عن تحكم أكثر دقة يمكن للمشغل الوصول إليه من خلال الوكيل الخلفي:

- **مسح ذاكرة التخزين المؤقت لـ UE واحد** (`/api/oam/ue_cache/{id}`): يمسح بيانات المشترك المخزنة مؤقتًا لمشترك واحد بواسطة SUPI. استخدمه لإجبار إعادة القراءة لمشترك واحد تغير ملفه الشخصي، بدلاً من مسح الذاكرة المؤقتة للجميع.

العمليات

- **تشخيصات وقت التشغيل** (`/api/oam/diagnostics`): يظهر تشخيصات منخفضة المستوى للخدمة الجارية.
- **استخدام الموارد** (`/api/oam/resources`): يبلغ عن استخدام الذاكرة والعمليات والجدولة في وقت التشغيل لفحص صحة العقدة.
- **ت��يين مستوى السجل** (`/api/oam/log_level`): يغير مستوى السجل في وقت التشغيل (واحد من `emergency`، `alert`، `critical`، `error`، `warning`، `warn`، `notice`، `info`، `debug`) لزيادة التفاصيل أثناء استكشاف الأخطاء وإصلاحها.
- **فرض إعادة تسجيل NRF** (`/api/oam/nrf/reregister`): يعيد تسجيل UDM مع NRF. استخدمه لاستعادة تسجيل تم إسقاطه أو قديم.

ذات الصلة

- UDR: مستودع البيانات الموحد: المخزن الداعم الذي يقرأ منه UDM سجلات المشتركين.
- AUSF: وظيفة خادم المصادقة: يستمد مواد المصادقة الخاصة به من UDM.
- AMF: وظيفة إدارة الوصول والتنقل: يستشير UDM ويسجل كـ NF خدم أثناء التسجيل.
- SMF: وظيفة إدارة الجلسة: يستشير UDM ويسجل كـ NF خدم أثناء إعداد الجلسة.
- ← 5G Core: نظرة عامة على جميع لوحات معلومات NF.

UDR: مستودع البيانات الموحد

الـ **UDR** هو التخزين الدائم لبيانات الاشتراك والسياسة والتطبيقات التي تقع خلف الـ PCF و UDM. هما وظائف الشبكة الأمامية التي تتحدث إليها الوظائف الأخرى، فإن الـ PCF و UDM حيث أن الـ UDR هو قاعدة البيانات التي تقرأ وتكتب فيها. إنه المصدر الوحيد للحقيقة حول من هو المشترك مخزن المشتركين الخاص به مع الـ UDR يشارك الـ OmniTouch، وما الذي يحق له. في نواة 5G و 4G لذا فإن مستودعًا موحدًا يحتفظ بمشتركي قاعدتي بيانات متوازيتين بدلاً من **HSS**.

← 5G Core

في لوحة التحكم

حة تحكم الـ UDR تفتح ل مع بطاقات صحة الوظائف القياسية عبر الأعلى (**API صحة**، كل منها يستعلم في، (و **ترخيص**، **NF حالة**، هل الـ UDR مسجل مع الـ NRF؟)، **NRF تسجيل** فترة زمنية محددة.

أسفل البطاقات توجد قسمان خاصان بالـ UDR:

- **صحة HSS**: فحص صحة الاتصال الذي يؤكد أن الـ UDR يمكنه الوصول إلى مخزن المشتركين المشترك الذي يتعامل معه. هذا يجيب على "هل قاعدة بيانات المشتركين قابلة للوصول وصحية؟" بنظرة سريعة.
- **المشتركون**: قائمة المشتركين المستخرجة من الـ HSS، مقسمة إلى صفحات وقابلة للبحث بواسطة **IMSI**. اختر مشتركًا لاسترجاع التفاصيل الكاملة لذلك IMSI، بحيث يمكن للمشغل تأكيد تزويد المشترك دون مغادرة OmniWeb.

الإجراءات

لا تعرض لوحة تحكم الـ UDR أي إجراءات مدمرة على مستوى NF أو لكل صف. إنها عرض للقراءة والبحث على مخزن المشتركين المشترك. قيمتها في الاستجواب: تحقق من أن المخزن قابل للوصو�� عبر قسم صحة HSS، قائمة المشتركين، والتعمق في التفاصيل الكاملة لأي مشترك بواسطة IMSI.

العمليات

بجانب أقسام البيانات، يحمل الـ UDR 5 العملياتGC الشائعة لكل وظيفة شبكة:

- **تعيين مستوى السجل**: رفع أو خفض verbosity سجل التشغيل (`emergency`، `alert`، `critical`، `error`، `warning`، `warn`، `notice`، `info`، `debug`) عبر `/api/oam/log_level`، لزيادة التفاصيل أثناء تشخيص مشكلة.
- **إجبار إعادة تسجيل NRF**: دفع الـ UDR لإعادة التسجيل مع NRF (`/api/oam/nrf/reregister`) إذا كانت تسجيله قد انتهت صلاحيته.
- **عرض التكوين في وقت التشغيل**: فحص تكوين الـ UDR المباشر من خلال نقطة نهاية تكوين OAM.

ذات صلة

- إدارة البيانات الموحدة: وظيفة الشبكة الأمامية التي تقدم بيانات الاشتراك من UDM: هذا المخزن.
- وظيفة التحكم في السياسة: تقرأ بيانات السياسة المحتفظ بها في الـ UDR.
- HSS: قاعدة بيانات المشتركين المشتركة التي يوحدها الـ UDR، لذا يعيش مشتركو 4G و5G في مستودع واحد.
- ← 5G Core: نظرة عامة كاملة على لوحة تحكم 5GC.

مرجع API (OpenAPI / Swagger)

تقوم وحدة التحكم في OmniWeb (الخلفية المركزية) بتوفير واجهة برمجة تطبيقات REST واحدة خلف نفس تسجيل الدخول JWT الذي يحكم بقية البوابة. هذه الواجهة موثقة ذاتيًا:

- **واجهة Swagger:** `/api/docs`. قم بتوسيع مسار لرؤية تصفح كل نقطة نهاية. طريقتها، ومعلمات المسار/الاستعلام، وما إذا كانت تحتاج إلى رمز، و ملخصها. انقر على حاملاً لتجربة المكالمات مباشرة ضد النسخة الجارية JWT والصق **تفويض**.
- **مواصفات OpenAPI 3:** `/api/openapi.json`. هذه هي الوثيقة القابلة للقراءة آليًا. استخدمها للاستيراد إلى Postman/Insomnia أو لتوليد العملاء.

← العودة إلى دليل العمليات

ما هو موثق

تتم **توليد المواصفات في وقت التشغيل** عن طريق استكشاف خريطة المسار الحية، لذا فهي تتطابق دائمًا مع نقاط النهاية التي تخدمها النسخة الجارية فعليًا. لا يمكن أن تنحرف أي ملف يتم صيانته يدويًا. لكل مسار يتم التقاطه:

- طريقة HTTP (مع معلمات المسار/الاستعلام)، والمسار،

- ملخص ووصف مأخوذ من الكود،
- ما إذا كان **JWT** و **حاملاً** مطلوبًا،
- حيثما ينطبق، إذن **عرض/تحكم** لكل عنصر يفرضه المسار.

تُجمع نقاط النهاية حسب المنطقة (وما إلى ذلك TAP، RAEX، IR.38، الاختبار، حتى تتمكن من العثور على مسارات ميزة بسرعة.

الحصول على رمز

تتطلب معظم نقاط النهاية رمز حاملاً. احصل على واحد باستخدام `POST /api/auth/login` (نفس بيانات الاعتماد التي تستخدمها للبوابة)، ثم أرسله كـ `Authorization: Bearer <token>`. في واجهة Swagger، استخدم زر **تفويض** حتى تحمل كل مكالمة "جربها" الرمز تلقائيًا.

النطاق

توثق هذه الواجهة **API** ليس **وحدة التحكم** فقط. وكيل الجهاز الذي يعمل في المواقع البعيدة ولا يكشف عن أي نقاط WebSocket جزءًا من هذه الواجهة: يتصل *خارجًا* بالوحدة التحكم عبر نهاية REST واردة، لذا لا يوجد شيء للاتصال به مباشرة.

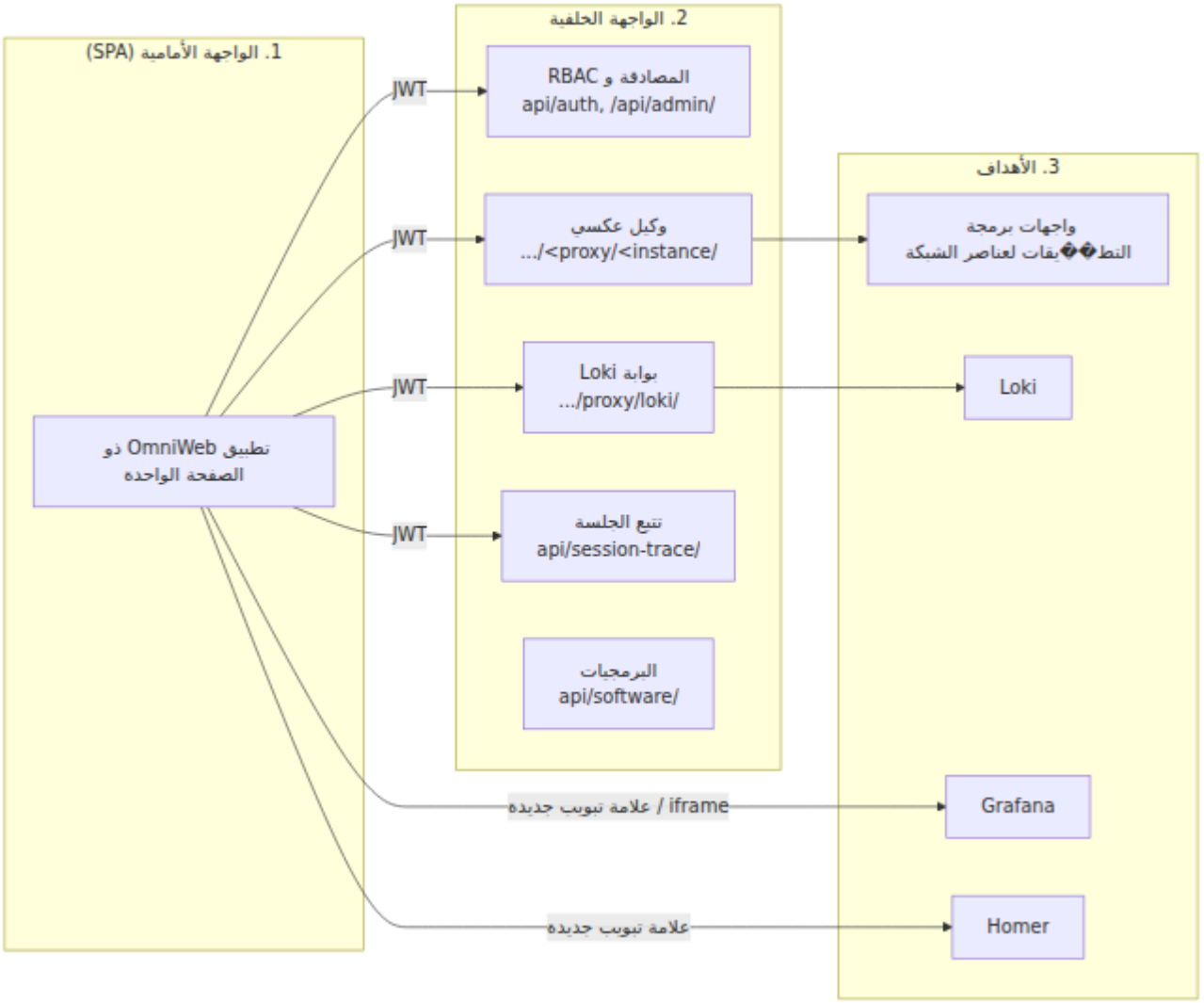
بنية OmniWeb

تشرح هذه الصفحة كيفية تجميع OmniWeb وكيف تصل جلسة المتصفح الفردية إلى كل وظيفة Loki. إذا كنت ستقرأ صفحة واحدة فقط لفهم النظام، اقرأ هذه الصفحة.، Grafana، وشبكة.

← العودة إلى دليل العمليات

المكونات

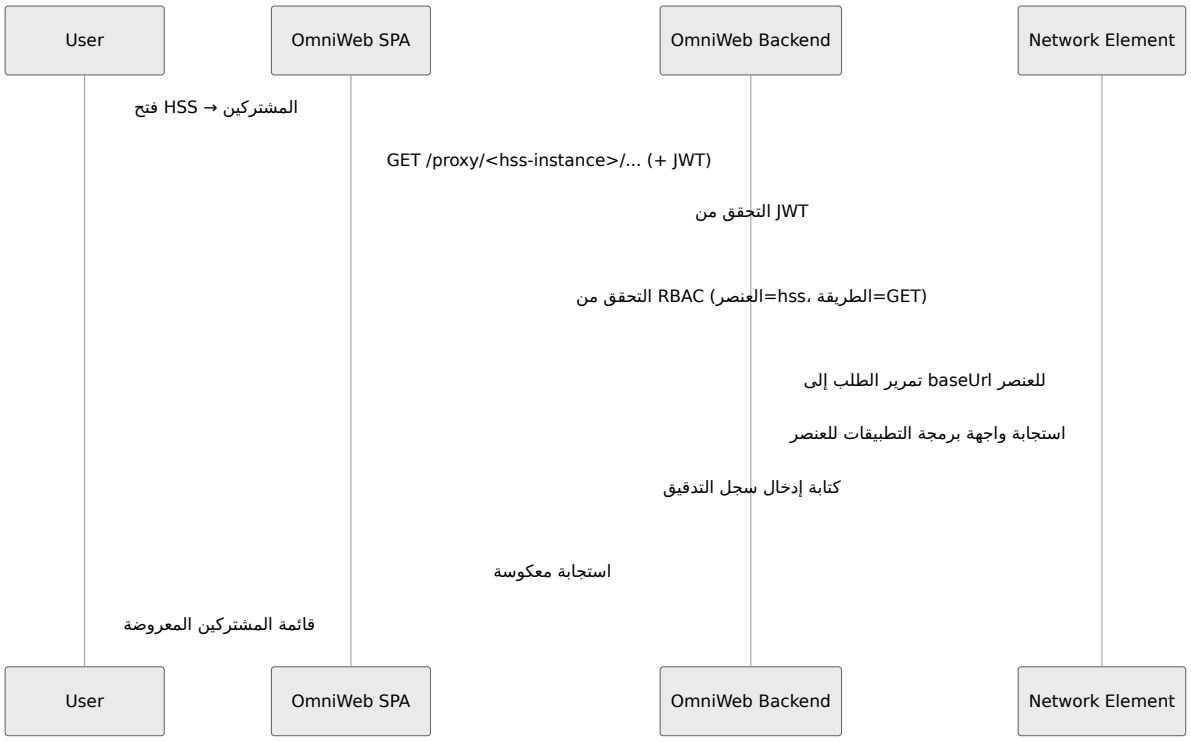
تحتوي OmniWeb على ثلاثة أجزاء متحركة:



المكون	الدور
واجهة SPA الأمامية	واجهة المستخدم. تطبيق ويب ذو صفحة واحدة يعرض صفحات العناصر، والتوبولوجيا، والسجلات، والتتبع، ولوحات المعلومات المدمجة.
الواجهة الخلفية	طبقة الأمان والتكامل. تقوم بمصادقة المستخدمين، وتطبيق RBAC، وعكس كل طلب إلى واجهة برمجة التطبيقات الصحيحة للعناصر، أو Loki، أو Grafana.
الأهداف	الأشياء التي يتم إدارتها ومراقبتها: واجهات برمجة التطبيقات الخاصة بعناصر الشبكة، بالإضافة إلى Grafana، Loki، وHomer.

تدفق الطلبات

يتبع كل طلب تشغيلي نفس المسار. لا يتحدث أي شيء في المتصفح إلى عنصر مباشرة. يمر دائمًا عبر الواجهة الخلفية بحيث يتم تطبيق المصادقة، والتفويض، والتدقيق مركزيًا.



يشفّر مسار الوكيل OmniWeb من نفس **معرف الحالة**، بحيث يمكن لـ إدارة العديد من الحالات وتوجيه كل طلب إلى الواجهة الخلفية الصحيحة (HSS مثل عدة عقد) نوع العنصر.

نموذج التكوين

تعتبر OmniWeb **مدفوعة بالتكوين**. يتم إعلان مجموعة العناصر، وحالاتها، وأين توجد واجهات برمجة التطبيقات الخاصة بها في ملف واحد: `public/config/omniweb.json`. تقوم الواجهة الخلفية بتحميله عند بدء التشغيل وتستخدمه الواجهة الأمامية لبناء الشريط الجانبي، والتوبولوجيا، وأهداف الوكيل.

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

المعامل	النوع	مطلوب	الافتراضي	الوصف
`type`	سلسلة	نعم	-	نوع العنصر. يحدد أي وحدة واجهة مستخدم تعرض العنصر. انظر الأنواع المدعومة.
`displayName`	سلسلة	نعم	-	اسم قابل للقراءة البشرية يظهر في الشريط الجانبي والتوبولوجيا.
`description`	سلسلة	لا	-	وصف أطول يظهر في التلميحات وصفحات النظرة العامة.
`instances`	قائمة	نعم	-	إدخال واحد لكل عقدة تم نشرها من هذا النوع. انظر معلمات الحالة أدناه.
`defaults.pollIntervalMs`	عدد صحيح	لا	5000	مدى تكرار تحديث الصفحات التشغيلية تلقائيًا، بالمللي ثانية.
`defaults.timeoutMs`	عدد صحيح	لا	10000	مهلة الوكيل لهذا النوع من العناصر. تستخدم واجهات برمجة التطبيقات

الوصف	الافتراضي	مطلوب	النوع	المعامل
مثل) البطيئة قيمة أكبر (OCS.				

معلمات الحالة:

الوصف	الافتراضي	مطلوب	النوع	المعامل
معرف الحالة الفريد. يستخدم في عناوين URL (`/hss/<id>`) وفي مسار الوكيل (`/proxy/<id>/...`).	-	نعم	سلسلة	`id`
اسم العرض للحالة.	-	نعم	سلسلة	`name`
عنوان URL الأساسي لواجهة برمجة التطبيقات الخاصة بإدارة العنصر. يقوم الوكيل بتمرير الطلبات هنا. يتم قبول الموقعة ذاتيًا TLS.	-	نعم	سلسلة	`baseUrl`
تسميات حرة الشكل (مثل `رئيسي`، `جغرافي`) تظهر كرقائق في- احتياطي.	`[]`	لا	قائمة	`tags`

أنواع العناصر المدعومة

`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`.

كل نوع يتوافق مع وحدة واجهة مستخدم خاصة به مع مجموعة من علامات التبويب الخاصة به، ولكن يتم تشغيل جميعها من خلال نفس الأنماط العامة. انظر العمليات الشائعة.

كيف تتواصل OmniWeb مع كل NF

`baseUrl` الوكيل الخلفي غير مرتبط بالعناصر. يقوم بتمرير ما يطلبه نموذج الواجهة الأمامية إلى *شكل* للعنصر. يعتمد تلك المكالمات على واجهة برمجة التطبيقات الأصلية للعنصر:

نمط واجهة برمجة التطبيقات	العناصر	ملاحظات
واجهة برمجة التطبيقات للعنصر	جميع وظائف الشبكة	واجهة برمجة التطبيقات الخاصة بإدارة العنصر، يتم تمريرها كما هي تحت `/proxy/<instance-id>/...`. يقوم OmniWeb بتمرير `GET`/`POST`/`PUT`/`PATCH`/`DELETE` كما يتوقع العنصر؛ شكل الطلب/الاستجابة هو ما يحدده ذلك العنصر.
استعلام السجل (LogQL)	جميعها (علامة تبويب السجلات)	يتم توجيهها عبر `/proxy/loki/...` إلى Loki. انظر السجلات والتتبع.

نظرًا لأن كل شيء يتم تمريره عبر الوكيل، فإن إضافة حالة هي مجرد تغيير في التكوين في `omniweb.json`. لا يتطلب الأمر أي تغيير في الكود لإدارة عقدة أخرى.

مرجع واجهة برمجة التطبيقات (OpenAPI)

وتصف الواجهة OmniWeb مع (`swagger-doc.json`) موحدة OpenAPI/Swagger تأتي وثيقة الأمامية ومواقع مشتركي SMSC على سبيل المثال تسجيلات واجهة) الخلفية ومخططات العناصر IMS). إنها عنصر مرجعي بدلاً من خادم واجهة برمجة التطبيقات المباشر.

مهلات الوكيل

تستجيب معظم العناصر. (`defaults.timeoutMs`) كل نوع عنصر له مهلة وكيل قابلة للتكوين بشكل جيد ضمن المهلة الافتراضية البالغة 10 ثوانٍ. تُعطى العناصر ذات الاستعلامات الأثقل مزيدًا من المجال:

العنصر	المهلة الافتراضية	لماذا
معظم العناصر	10 ثوانٍ	الوقت القياسي لاستجابة واجهة برمجة التطبيقات
OCS	180 ثانية	استعلامات التصنيف/CDR عبر مجموعات بيانات كبيرة

تكامل المراقبة

لا تعيد OmniWeb تنفيذ Grafana، Loki، أو Homer. بل تقوم بدمجها بحيث يمتد تسجيل دخول واحد عبر كامل المكدس:

- **Grafana** يتم تقديمه خلف بوابة مصادقة ومضمن كـ iframe. يتم تفويض كل طلب الخاص بك، لذا لا يوجد كلمة مرور ثانية. انظر OmniWeb ضد تسجيل دخول Grafana.
- **Loki** يتم الوصول إليه من خلال بوابة `/proxy/loki/*` الخاصة بالواجهة الخلفية، نيابة عن المشغل. انظر السجلات والتتبع التي تقوم بتشغيل استعلامات LogQL.
- **Homer** (التقاط SIP) يتم اكتشافه تلقائيًا عند بدء التشغيل (`/api/homer/status`) وعند وجوده، يفتح في علامة تبويب جديدة. يتم أيضًا تفويضه ضد تسجيل دخول OmniWeb الخاص بك.

مرجع البيئة

تتم تكوين نقاط تكامل الواجهة الخلفية عبر متغيرات البيئة:

المتغير	الافتراضي	الوصف
`GRAFANA_URL`	`http://localhost:3000`	عنوان URL الأساسي لحالة Grafana التي يقوم OmniWeb بالتمرير إليها.
`LOKI_URL`	`http://localhost:3100`	عنوان URL الأساسي لحالة Loki المستخدمة للسجلات والتتبع.
`LDAP_URI`	`ldap://localhost:389`	خادم OpenLDAP لمزامنة المستخدم/مفتاح SSH (اختياري).
`LDAP_BASE_DN`	`dc=omniweb,dc=local`	الأساسي لـ DN LDAP.
`LDAP_ADMIN_DN`	`cn=admin,dc=omniweb,dc=local`	الربط لكتابات DN LDAP.
`LDAP_ADMIN_PASSWORD`	`omniweb-admin`	كلمة مرور الربط لـ LDAP (غيرها).
`AUDIT_API_KEY`	`omniweb-audit-key`	السر المشترك لاستدعاءات تدقيق تسجيل الدخول عبر SSH (غيرها).

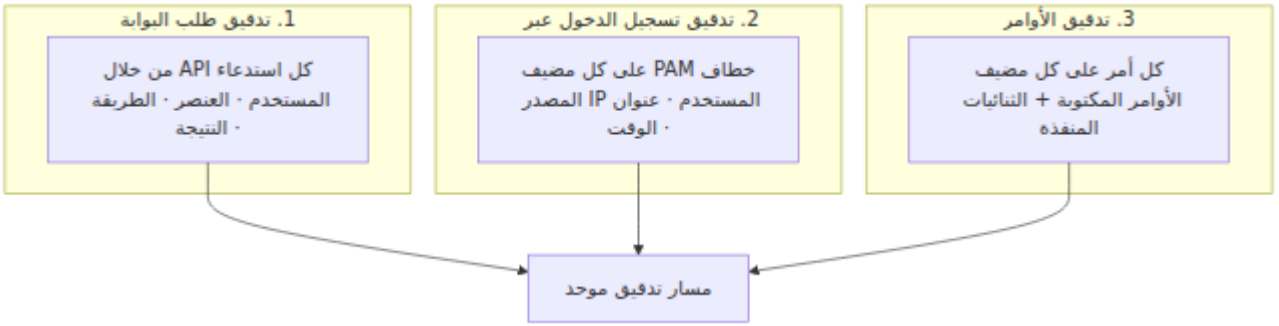
للحصول على تفاصيل انظر المصادقة والتحكم في الوصول LDAP/SSH والتدقيق.

تسجيل التدقيق

هو البوابة الوحيدة إلى الشبكة، فإنه أيضًا المكان الوحيد الذي يمكن فيه OmniWeb نظرًا لأن على **ثلاث طبقات** تجيب معًا على "من فعل OmniWeb تسجيل النشاط. يحتوي التدقيق في ماذا، وأين" عبر كل من البوابة والمضيفين الذين يديرهم.

المصادقة والتحكم في الوصول · ← دليل العمليات ←

الطبقات الثلاث



الطبقة	تلتقط	أين تظهر
تدقيق طلب البوابة	كل إجراء يتم *من خلال* OmniWeb	الإعدادات → التدقيق
تدقيق تسجيل الدخول عبر SSH	كل تسجيل دخول عبر SSH *إلى* *مضيف مُدار*	الإعدادات → التدقيق (عبر استدعاء المضيف)
تدقيق الأوامر	كل أمر *تم تشغيله على مضيف* (مكتوب + منفذ)	الإعدادات → الأوامر

تدقيق طلب البوابة

بغض النظر عما إذا كان قد نجح أو فشل أو تم رفضه بواسطة RBAC، يتم تسجيل كل طلب يمر عبر وكيل OmniWeb. كل إدخال يلتقط:

- **المستخدم** الذي قام بالطلب.

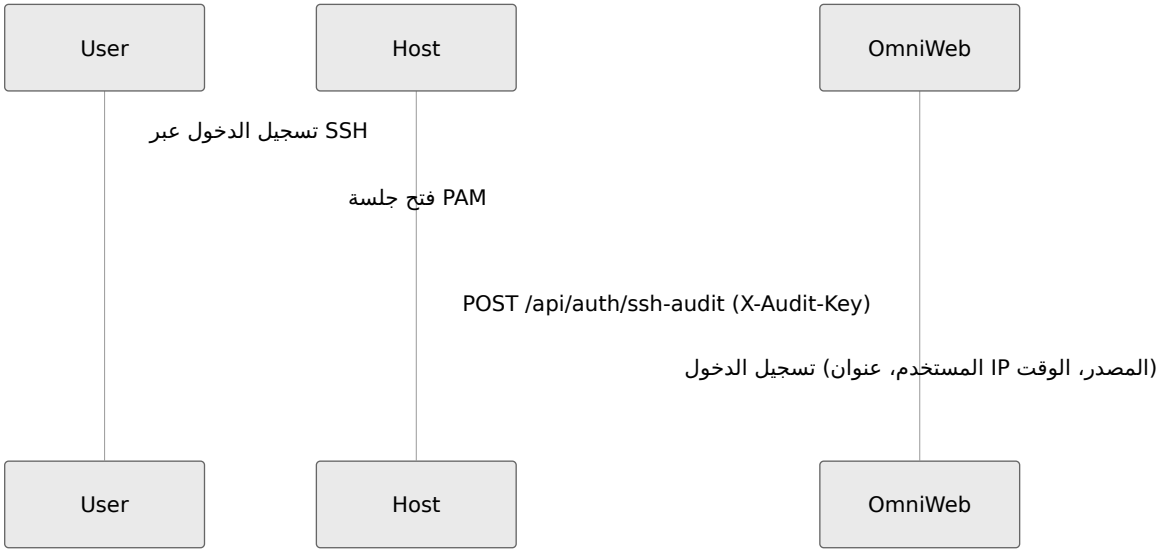
- **نوع العنصر والحالة** المستهدفة.
- **طريقة HTTP** (التي تخبرك ما إذا كانت عرضًا أو تغييرًا أو حذفًا).
- **النتيجة** (رمز الحالة).
- **الطابع الزمني**.

هذا يوفر سجلًا كاملاً لمن قام بتغيير ماذا، وأين، ومتى، داخل البوابة. إنه موجود تحت **الإعدادات** ← **التدقيق**. نظرًا لأن القراءات (`GET`) والكتابات (`POST`/`PUT`/`PATCH`) والحذفات كلها قابلة للتفريق حسب الطريقة، فإن سجل التدقيق يعمل كـ تاريخ تغيير للشبكة.

مسار التدقيق (الإعدادات ← التدقيق): كل إجراء مع المستخدم، نوع الحدث، العنصر/الحالة، طريقة HTTP، وعنوان IP المصدر. لاحظ الحذف المرفوض (403)، وحدث `DELETE` النتيجة، وعنوان العادية. قم بالتصفية API جنبًا إلى جنب مع طلبات `ssh_login`، وحدث `permission_changed` حسب نوع الحدث، المستخدم، العنصر، أو نطاق التاريخ.

تدقيق تسجيل الدخول عبر SSH

يمكن للمضيفين الإبلاغ عن تسجيلات الدخول عبر SSH إلى OmniWeb بحيث يظهر الوصول إلى PAM المضيف في نفس عرض التدقيق مثل نشاط البوابة. يستدعي خطاف صغير على كل مضيف IP عند فتح جلسة، مُبلغًا عن اسم المستخدم، عنوان OmniWeb المصدر، وتفاصيل الخدمة.



يتم مصادقة الاستدعاء باستخدام سر مشترك بحيث لا يمكن للمضيفين الموثوق بهم فقط كتابة إدخالات التدقيق:

المتغير	القيمة الافتراضية	الوصف
`AUDIT_API_KEY`	`omniweb-audit-key`	السر المشترك الذي يقدمه خطاف PAM للمضيف عند الإبلاغ عن تسجيل الدخول (كـ `X-Audit-Key`). **قم بتغيير هذا**، واضبط القيمة المطابقة على كل مضيف.

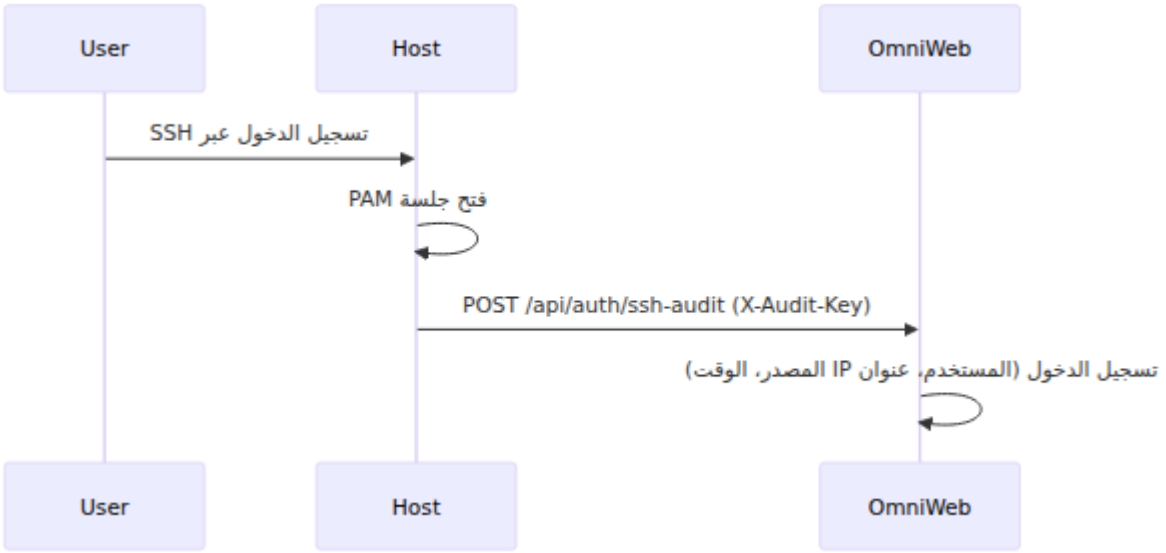
مع وجود هذا في مكانه، يظهر كل تسجيل دخول عبر SSH → **الإعدادات** إلى مضيف مُدار تحت **التدقيق**. جنبًا إلى جنب مع أفعال البوابة، مما يربط بين نشاط الشخص في البوابة والمضيف

تدقيق الأوامر

تيارين مكملين، OmniWeb لحصول على رؤية على مستوى الأوامر على المضيفين، تجمع
وقابلين للتصفح تحت **الإعدادات** → **الأوامر** مع تبديل المصدر Loki يتم شحن كلاهما إلى:

تيار Loki	يلتقط	المصدر
`job="cmdaudit"`	خطوط الأوامر الدقيقة التي يكتبها المستخدم في قشرة تفاعلية، **بما في ذلك الأوامر المدمجة في القشرة** مثل `echo`، `cd`، `export`	**الأوامر المكتوبة**
`job="auditd"`	كل ثنائي تم تشغيله فعليًا على المضيف (البرامج النصية، الأدوات، الأتمتة)	**تنفيذ الثنائيات**

لا يحل أحدهما محل الآخر: الأوامر المدمجة لا تشغل ثنائيًا منفصلًا، لذا فقط تيار الأوامر المكتوبة يراها؛ والأتمتة/البرامج النصية التي لا تجلس أبدًا عند موجه تفاعلي تظهر فقط في تيار تنفيذ الثنائيات. معًا، يغطيان *ما كتبه الشخص وما تم تنفيذه فعليًا*.



الأوامر المكتوبة يتم التقاطها بواسطة خطاف قشرة تفاعلية خفيفة الوزن يسجل كل أمر يقوم المستخدم بتشغيله في المستخدم، الدليل العامل، و) TTYمع). هذه هي الطبقة التي تلتقط الأوامر المدمجة التي لا يمكن لمتعقب الثنائيات رؤيتها هيكليًا.

تنفيذ الثنائيات يأتي من عميل مضيف خفيف الوزن يسجل كل ثنائي يتم تشغيله على المضيف. دون دعم تدقيق النواة. كل LXC نظرًا لأنه يعمل في مساحة المستخدم، فإنه يعمل داخل حاويات إدخال يلتقط:

الحقل	المعنى
`login`	المستخدم الذي سجل الدخول في الأصل؛ **يستمر** لذا لا تخفي `sudo`/`su`، تغييرات الامتياز من هو الذي يتصرف
`uid`	UID الفعلي الذي تم تشغيل الأمر به
`filename`	الثنائي الذي تم تنفيذه
`cwd`	الدليل العامل في وقت التنفيذ
(بعد `]:`)	سطر الأوامر الكامل

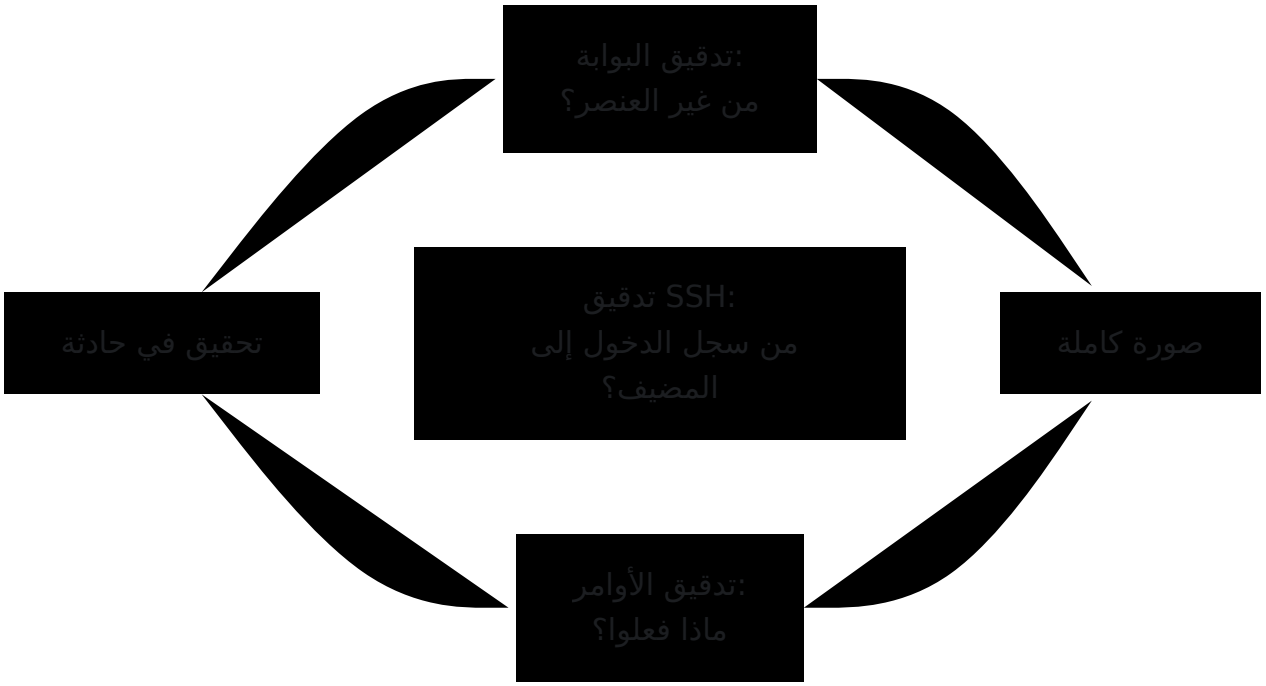
إدخال تنفيذ تمثيلي:

```
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
```

تظهر عرض **الإعدادات ← الأوامر** بشكل افتراضي تيار الأوامر المكتوبة وتتيح لك التصفية حسب المضيف، والبحث حسب المستخدم أو الأمر، ومتابعة النشاط عبر الأسطول، مع تبديل المصدر للتبديل إلى عرض تنفيذ الثنائيات الخام عندما تريد رؤية ما تم تشغيله بالضبط.

> **ملاحظة:** تيارات الأوامر هي أداة لرؤية المشغل يتم التقاطها في مساحة المستخدم. يمكن لمستخدم الجذر المصمم تجاوزها؛ يعد التدقيق على مستوى النواة خطوة تعزيز إذا كنت بحاجة إلى التقاط غير قابل للتجاوز. بالنسبة للسجل الهيكلي ذي الصلة بالأمان (تسجيل الدخول، تغييرات الأذونات، الرفض)، اعتمد على **تدقيق البوابة** و**تدقيق تسجيل الدخول عبر SSH** الخاصة OmniWeb أعلاه، والتي تُكتب في قاعدة بيانات.

كيف تتناسب الطبقات معًا



- تدقيق طلب البوابة ← تغيير تكوين تم **من خلال** **OmniWeb**.
- تدقيق + (من دخل) SSH تغيير تم **يدويًا على مضيف** ← تدقيق تسجيل الدخول عبر الأوامر (ماذا فعلوا).

معًا، لا تترك أي منطقة عمياء بين "تم تغييره في واجهة المستخدم" و"تم تغييره على الجهاز".

ذات صلة

- السجلات وتتبع المشتركين: مستكشف السجلات العام وراء تيارات الأوامر.
- تسجيل الدخول SSH باستخدام مفتاح: الجانب الخاص بالوصول لنشاط المضيف.
- RBAC: الأذونات التي يسجل استخدامها تدقيق البوابة.

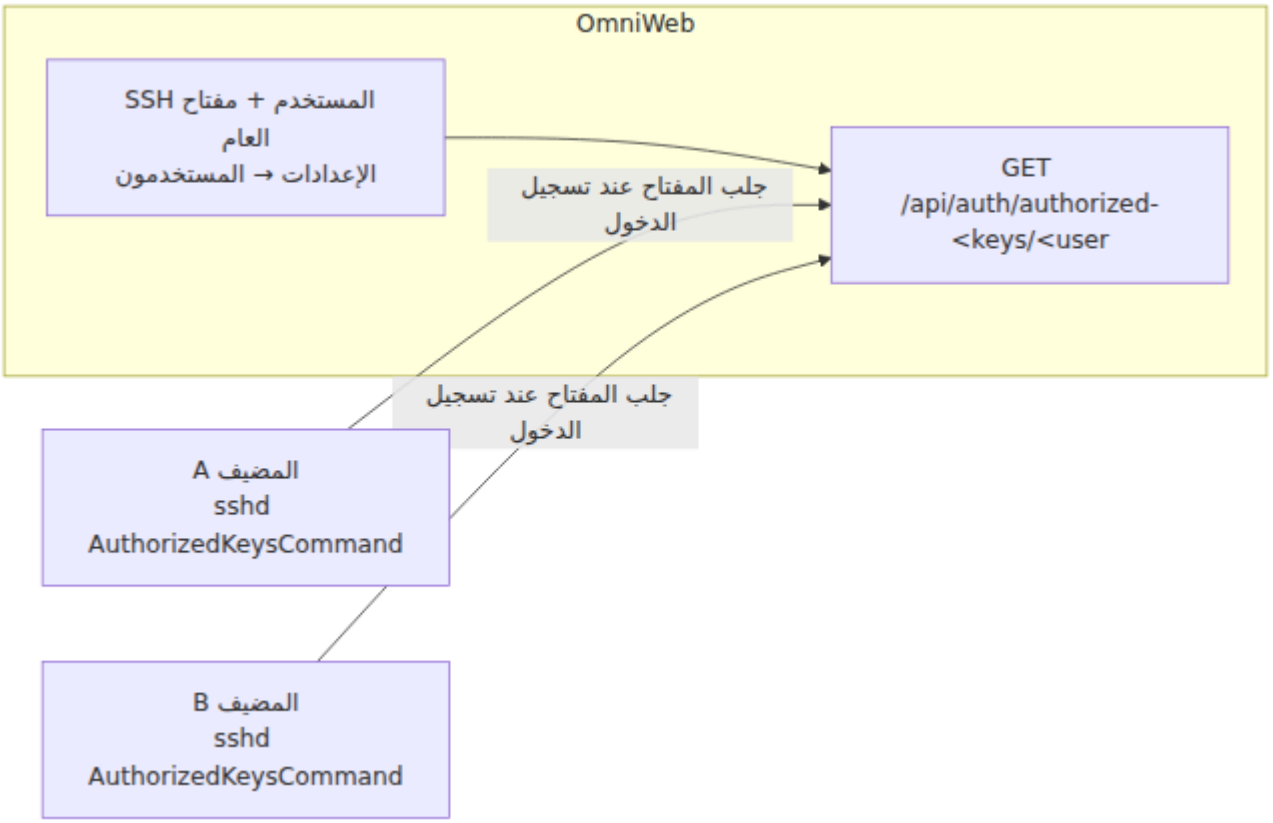
تسجيل الدخول باستخدام مفتاح SSH (الوصول إلى المضيف)

يمتد التحكم في الوصول في OmniWeb إلى **المضيفين** الذين يديرون الشبكة. يمكن لكل مستخدم حمل **مفتاح SSH** **بشكل مباشر**، وتقوم المضيفات المدارة بجلب تلك المفاتيح في وقت تسجيل الدخول. لذا فإن OmniWeb هو المكان الوحيد لإدارة من **يمكنه الوصول إلى *SSH* من فعل ذلك بالفعل**، ومع تسجيل التدقيق *أين*.

(هذا يحل .لكل مضيف للحفاظ عليها `authorized_keys` لا يوجد خادم دليل للتشغيل ولا ملفات السابق؛ الدليل غير موجود، وتُقدم المفاتيح عند الطلب عبر OpenLDAP محل تصميم مزامنة HTTPS.)

المصادقة والتحكم في الوصول · ← دليل العمليات ←

ما الذي يفعله



لكل `sshd` مرة واحدة. يتم تكوين OmniWeb عام في SSH تقوم بإعطاء المستخدم مفتاح عبر (**في لحظة تسجيل الدخول** OmniWeb مضيف مُدار لطلب مفتاح ذلك المستخدم من ويمكن للمستخدم OmniWeb أضف مفتاحًا في `AuthorizedKeysCommand` في OpenSSH). إلى كل مضيف مسجل؛ قم بتعطيل المستخدم وستفقد تلك الوصول في كل مكان في SSH محاولتهم **التالية** لتسجيل الدخول، دون مزامنة، دون انحراف، ودون ملفات مفاتيح لتنظيفها.

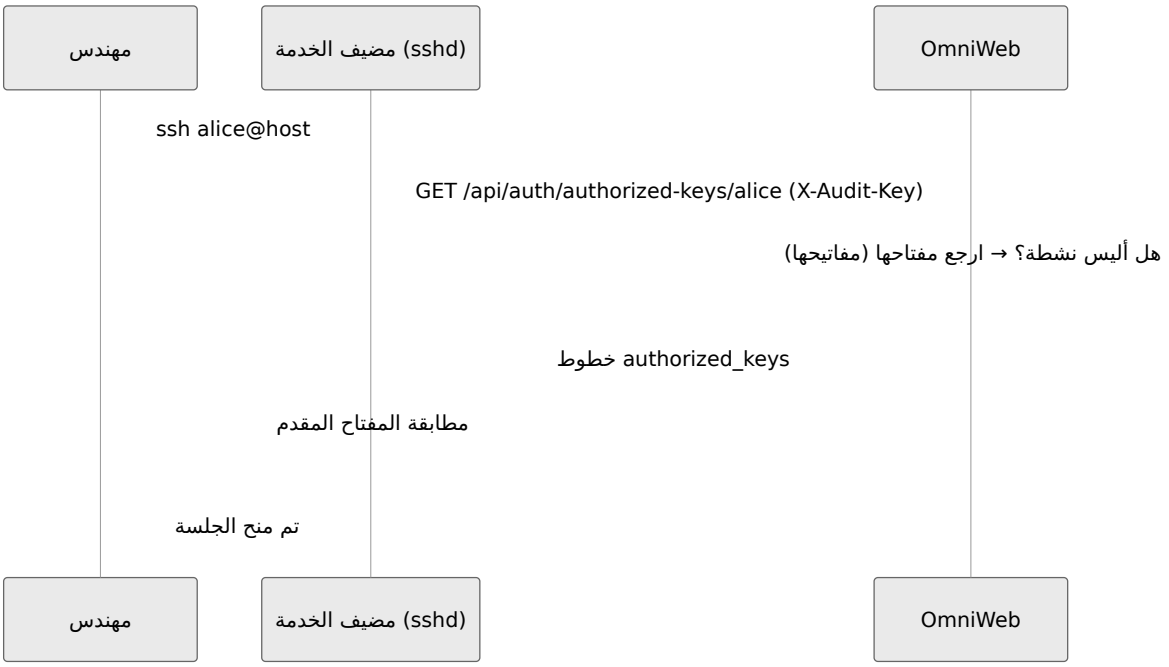
تعيين مفتاح المستخدم

تُدار المفاتيح في **الإعدادات → المستخدمون**، نفس الشاشة التي تدير حسابات البوابة RBAC، مُعدًا؛ أنشئ أو حرر SSH وحالة النشاط/التعطيل. تُظهر كل صف مستخدم ما إذا كان مفتاح مستخدمًا للصق واحد.

العام مُعدًا. المفتاح الذي تلصقه SSH الإعدادات ← المستخدمون: كل مستخدم مع ما إذا كان مفتاح هنا هو المفتاح الذي يمنح الوصول إلى المضيف؛ لا يوجد مكان آخر للحفاظ عليه.

كيف تستهلك المضيفات ذلك

تقوم كل مضيف مُدار بتشغيل مساعد صغير موصول بـ `sshd` كـ `AuthorizedKeysCommand`. عندما يتصل شخص ما، يقوم `sshd` بتشغيل المساعد، الذي يجلب مفاتيح ذلك المستخدم المصرح بها من OmniWeb عبر HTTPS ويعيدها للمطابقة:



الخصائص الرئيسية لهذه العملية:

- **حي**: يتم جلب المفتاح لكل تسجيل دخول، لذا فإن التغييرات تدخل حيز التنفيذ على الفور.
- **مستخدمون نشطون فقط**: تعيد OmniWeb المفاتيح فقط للمستخدمين **النشطين**. عندما تقوم بتعطيل أو حذف مستخدم في OmniWeb، فإن ذلك يمنع تسجيل دخوله التالي على كل مضيف مرة واحدة. هذه هي زر الإلغاء.
- **لا تعداد**: المستخدم غير المعروف أو المعطل، أو الذي ليس لديه مفتاح، يعيد نتيجة فارغة. ببساطة لا يجد تسجيل الدخول مفتاحًا ويتم رفضه، لذا فإن نقطة النهاية لا تكشف عن أسماء المستخدمين الموجودة.
- **OmniWeb تنجو من انقطاع**: يقوم المساعد بتخزين آخر نتيجة جيدة لكل مستخدم. لا يغلق الجميع OmniWeb على المضيف، لذا فإن انقطاعًا قصيرًا في

بواسطة إدارة التكوين جنبًا إلى (دليل المنزل، قشرة Unix، مستخدم) يتم توفير الحساب نفسه **الهوية والمفاتيح**، وتمتلك أتمتة الأسطول **وجود** OmniWeb تمتلك. `sshd` جنب مع مساعد **الحساب** على كل مضيف.

التكوين

تُحرس نقطة النهاية الخاصة بتقديم المفاتيح بنفس السر المشترك مثل استدعاء التدقيق:

المتغير	القيمة الافتراضية	الوصف
`AUDIT_API_KEY`	`omniweb-audit-key`	السر المشترك الذي يقدمه مساعد `AuthorizedKeysCommand` لكل مضيف (كـ `X-Audit-Key`) عند جلب المفاتيح. **قم بتغيير هذا**، واضبط القيمة المطابقة على كل مضيف.

هو الشيء الوحيد الذي يجب استعلامه ويعمل المساعد على المضيفين OmniWeb نظرًا لأن والسر هو بوابة ثانية فوق مسار الشبكة HTTPS الموثوقين، يتم تقديم نقطة النهاية عبر.

لماذا يهم هذا

- عبر الأسطول بأكمله: حالة المستخدم **SSH مكان واحد لمنح/إلغاء الوصول إلى** النشطة هي وصوله إلى المضيف.
- **لا ملفات مفاتيح متفرقة** تنحرف عن التزامن على المضيفين الفرديين، ولا خادم دليل للتشغيل والنسخ الاحتياطي.
- ومن خلال تسجيل SSH، **هوية واحدة** تربط وصول الشخص إلى البوابة، وصوله إلى التدقيق، نشاطه المسجل.

ذات صلة

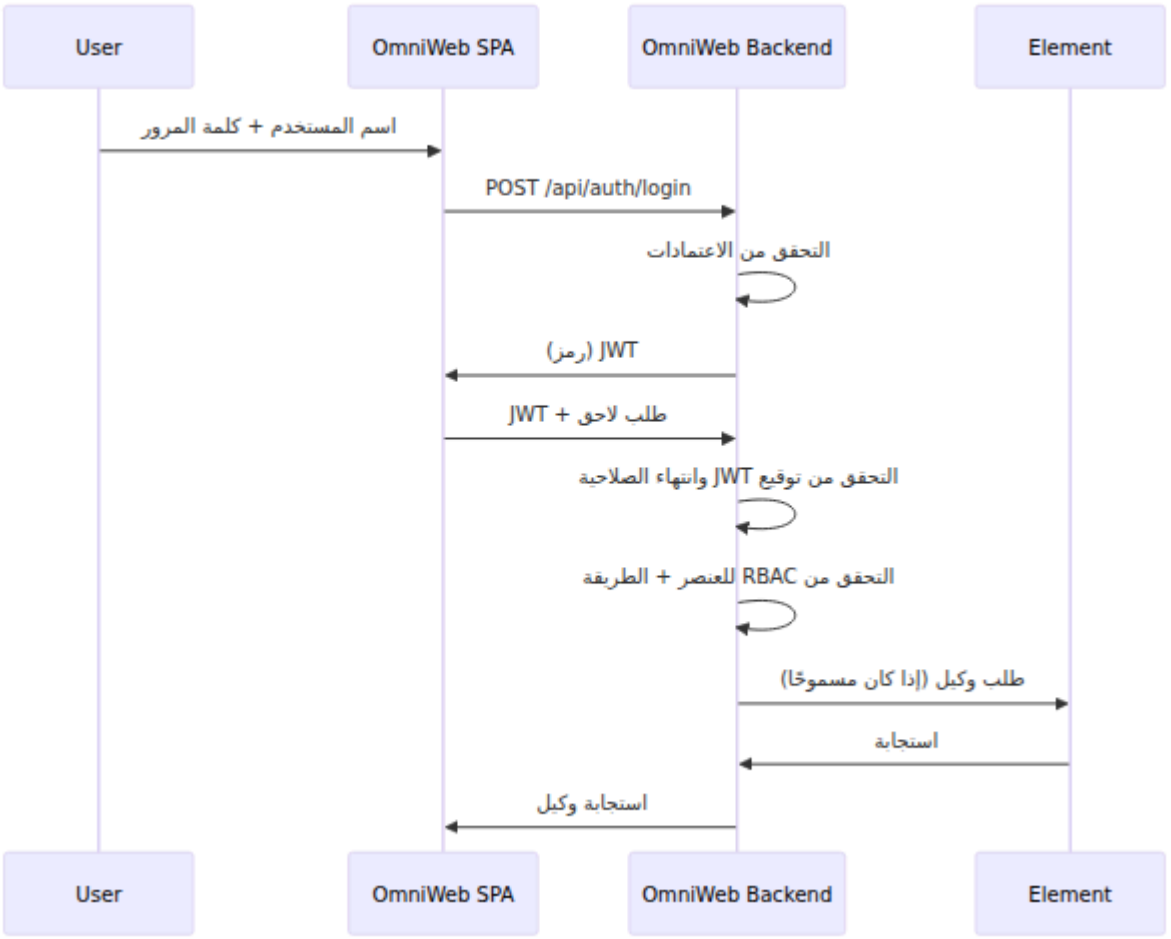
- وكل أمر يتم تشغيله على المضيفات SSH تسجيل التدقيق: سجل تسجيلات دخول.
- RBAC: *داخل* التحكم فيما يمكن أن يفعله نفس المستخدمين OmniWeb.

تسجيل الدخول وجلسات JWT

تقوم OmniWeb بمصادقة المشغلين باستخدام اسم المستخدم وكلمة المرور وتصدر رمز ويب يثبت هذا الرمز من أنت في كل طلب لاحق. والأهم من ذلك، أنه هو *نفس* الاعتماد الذي يخول Grafana وLoki وHomer النظام بأكمله. تسجيل دخول واحد يغطي كامل المدمجة.

المصادقة والتحكم في الوصول · ← دليل العمليات ←

تدفق تسجيل الدخول



يتم إصدار الرمز بواسطة `POST /api/auth/login`. يقوم SPA بتقديمه بمجرد الحصول عليه، ويتحقق الخلفية من التوقيع وانتهاء الصلاحية قبل القيام بأي شيء آخر، في كل استدعاء API.

الذي يحكم كامل النظام: JWT شاشة تسجيل الدخول. المصادقة هنا تؤدي إلى الحصول على واجهات برمجة التطبيقات للعناصر، Loki، Grafana، وHomer.

كيفية نقل الرمز

يقبل الخلفية JWT في ثلاثة مواقع، مما يسمح لنفس الرمز بالعمل لاستدعاءات API XHR، والتنقلات في المتصفح، و iframes المدمجة على حد سواء:

الموقع	الاستخدام
رأس التفويض	طلبات API القياسية (XHR/fetch) من SPA
ملف تعريف الارتباط (`access_token`, HttpOnly)	التنقلات في المتصفح والمحتوى المدمج (iframe علامة Homer، Grafana)
سلسلة الاستعلام	الحالات التي لا يمكن فيها تعيين رأس أو ملف تعريف ارتباط

ملف تعريف الارتباط هو **HttpOnly** (لا يمكن قراءته بواسطة JavaScript) ويستخدم `SameSite=Lax`، مما يحمي الرمز من السرقة عبر الوصول إلى النصوص البرمجية عبر المواقع بينما لا يزال يسمح بالتنقلات على المستوى الأعلى إلى الأدوات المدمجة.

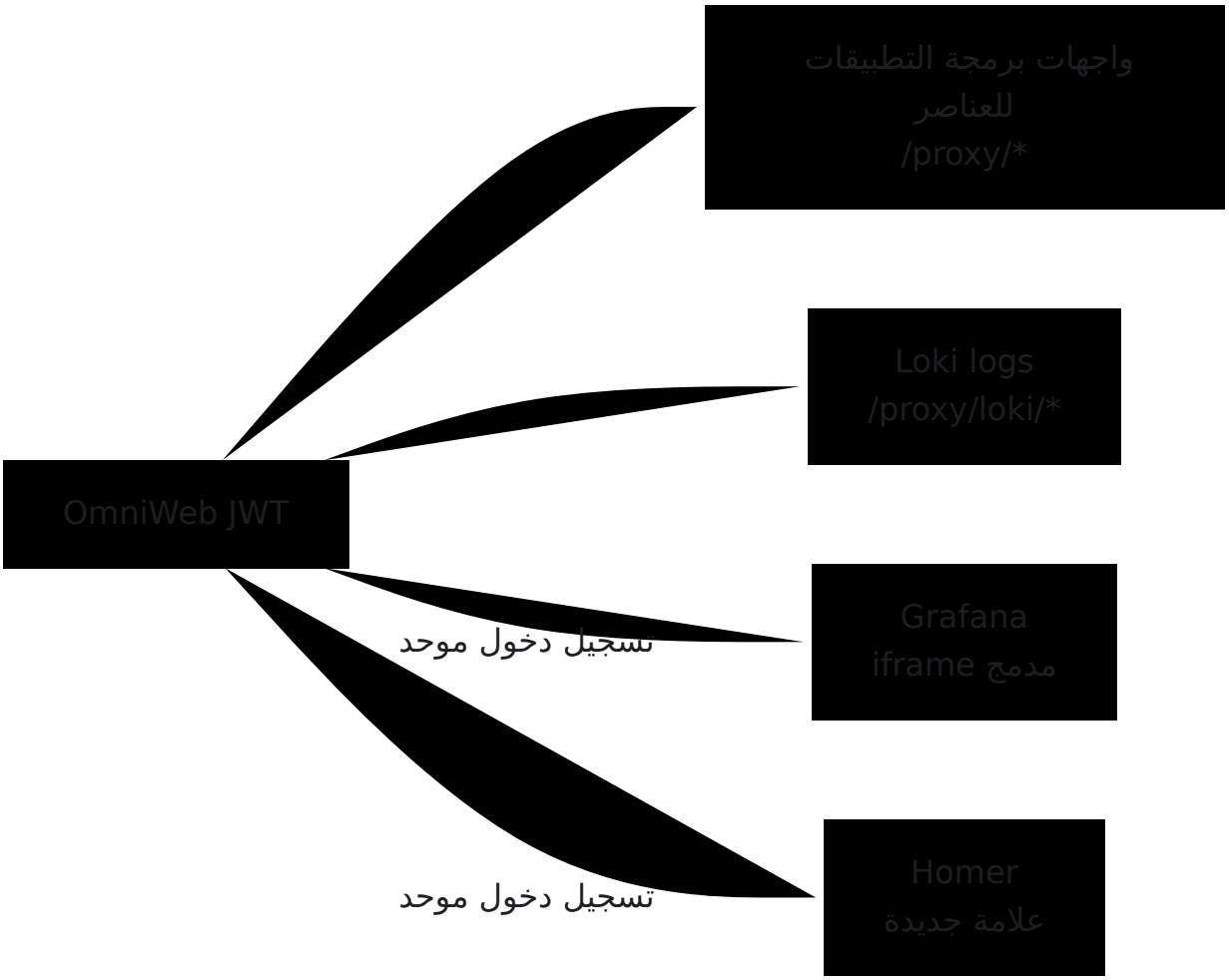
مدة صلاحية الرمز

يمتلك رمز الوصول انتهاء صلاحية قابل للتكوين، **24 ساعة بشكل افتراضي** (`JWT_ACCESS_TOKEN_EXPIRES`، بالثواني). عند انتهاء صلاحيته، يتم إعادة المشغل إلى شاشة تسجيل الدخول ويقوم بإعادة المصادقة. لا توجد جلسة صامتة غير محددة؛ مدة الصلاحية هي حدود أمان مقصودة.

الإعداد	الافتراضي	الوصف
`JWT_ACCESS_TOKEN_EXPIRES`	`86400` (24 ساعة)	مدة صلاحية رمز الوصول بالثواني. قللها لجلسات أكثر صرامة؛ ارفعها لتقليل إعادة تسجيل الدخول.
`JWT_SECRET_KEY`	*(تم إنشاؤه)*	السر المستخدم لتوقيع والتحقق من الرموز. يتم تعيينه صراحة في الإنتاج بحيث تبقى الرموز قائمة بعد إعادة تشغيل الخلفية وتكون متسقة عبر الحالات.

تسجيل دخول واحد، كامل النظام

يخول أدوات المراقبة المتكاملة، لذا لا يقوم المشغلون بتسجيل الدخول مرتين JWT نفس:



- يتم الوصول إليها من خلال وكيل **Lokiواجهات برمجة التطبيقات للعناصر و** الخلفية، الذي يتحقق من JWT مباشرة.
- يتم الوصول إليهما من خلال بوابة مصادق عليها، تتحقق من **Homer وGrafana** الخاص بك قبل الوكالة، دون الحاجة إلى كلمة مرور ثانية. OmniWeb تسجيل دخول انظر Grafana وHomer.

واحدة في كامل السطح التشغيلي: لوحات المعلومات، OmniWeb لهذا السبب، تتحكم جلسة السجلات، التتبع، وإدارة العناصر جميعها تعتمد على نفس الرمز.

تسجيل الدخول الأول وتغيير الاعتمادات

قم بتغيير هذا على الفور. (`admin` / `admin`) تأتي النشر الجديد مع حساب مسؤول افتراضي بعد تسجيل الدخول الأول، عبر الإعدادات. الوجود الافتراضي موجود فقط لتشغيل النظام ولا يجب أن يبقى في الإنتاج.

تسجيل الخروج وانتهاء الصلاحية

تسجيل الخروج يتخلص من الرمز. يؤدي الرمز المنتهي الصلاحية أو غير الصالح إلى رفض الطلب إلى شاشة تسجيل الدخول. نظرًا لأن إجراءات العناصر تتم فقط من خلال SPA التالي وعودة RBAC، استدعاء وكيل مصادق عليه ومتحقق منه. لا يمكن لجلسة منتهية الصلاحية تنفيذ إجراء مميز.

ذات صلة

- التحكم في الوصول القائم على الدور: ما يُسمح للمستخدم المسجل الدخول بالقيام به.
- تسجيل التدقيق: يتم تسجيل كل إجراء مصادق عليه.

التحكم في الوصول القائم على الدور (RBAC)

ما يمكنك فعله. يتم منح الوصول RBAC يحدد .OmniWeb تخبرك عملية المصادقة من هو *أنت* في والتي تتطابق مباشرة مع العمليات الحقيقية التي ،**HTTP** بدقة، **لكل نوع عنصر، لكل طريقة** يقوم بها المشغل: عرض، تعديل، أو حذف. بالإضافة إلى ذلك، تحدد نطاقان *أين*: أي **مواقع** يمكن للمشغل الوصول إليها، وأي **أجهزة اختبار** يمكنهم استخدامها. يجب أن تمر كل طلب عبر جميعها.

المصادقة والتحكم في الوصول · ← دليل العمليات ←

مستويات الإذن

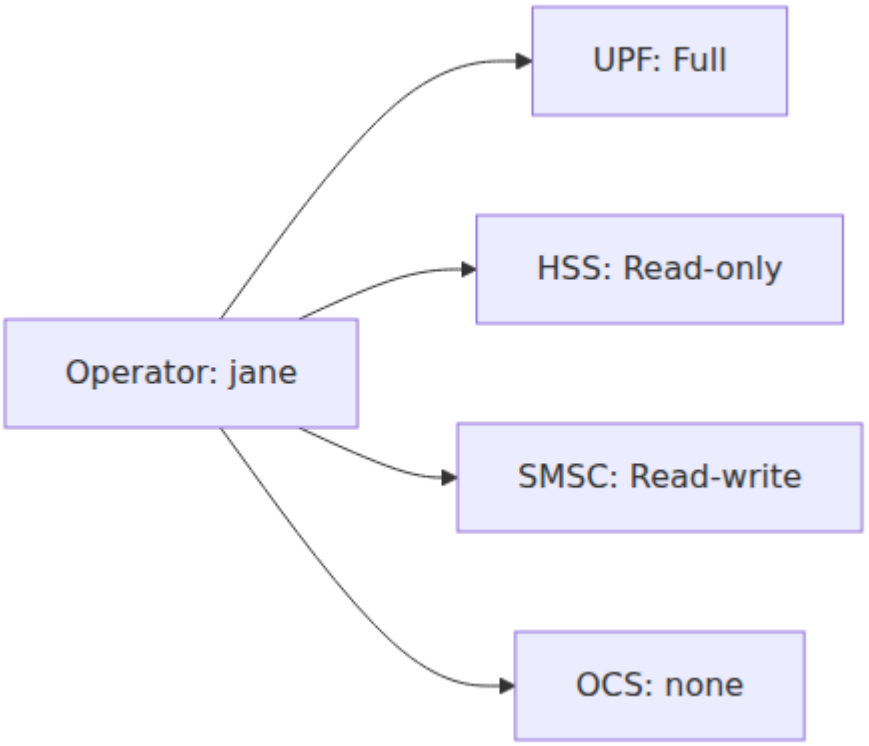
يمكن منح كل نوع عنصر لمستخدم على أحد ثلاثة مستويات. يتم التعبير عن المستوى كمجموعة التي يمكن للمستخدم استخدام ا ضد ذلك العنصر من خلال الوكيل HTTP من طرق:

الإذن	الطرق المسموح بها	ما يمكن للمشغل القيام به
للقراءة فقط	`GET`	عرض البيانات فقط، بدون تغييرات
للقراءة والكتابة	`GET`, `POST`, `PUT`, `PATCH`	عرض وتعديل: على سبيل المثال، إضافة QoS مشترك، تحرير مسار، تغيير قاعدة
كامل	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	كل شيء، بما في ذلك الحذف ومسح الجلسات

فإنها تتماشى تمامًا مع نموذج التحرير العام: نموذج HTTP، نظرًا لأن الأذونات مرتبطة بطرق `POST` هو "إضافة"، `PUT`/`PATCH` هو "تحرير"، و`DELETE` هو "حذف"/"مسح".

دقة لكل عنصر

تُمنح الأذونات **بشكل مستقل لكل نوع عنصر**. يمكن أن يحمل المستخدم مستويات مختلفة على عناصر مختلفة:

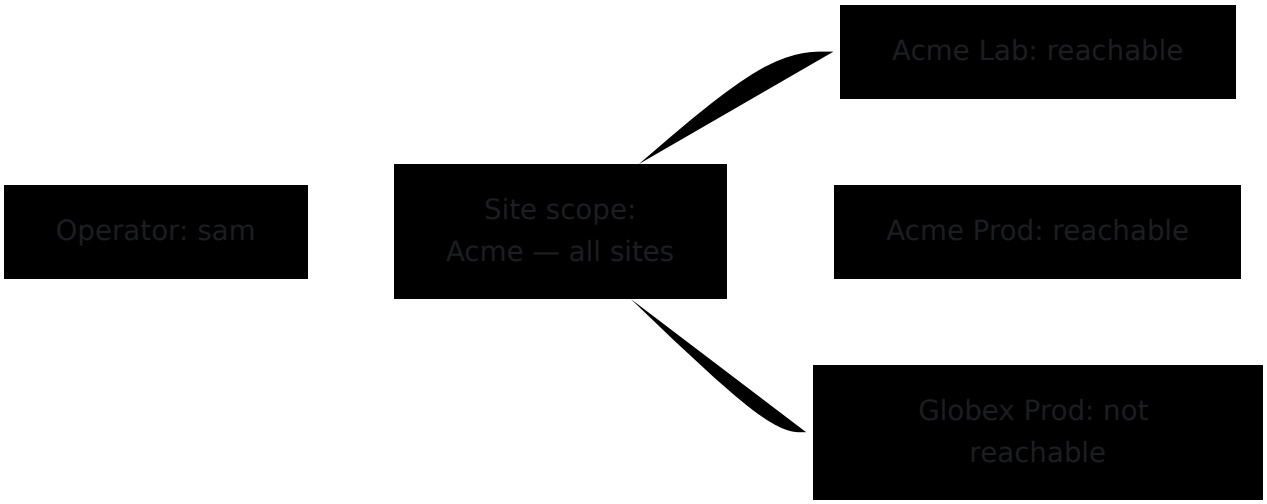


في هذا المثال، يمكن لجين مسح جلسات UPF، يمكنها عرض HSS ولكن لا يمكنها تغييره، يمكنها على الإطلاق. هذا يتيح لك منح، على سبيل المثال، OCS ولا يمكنها رؤية SMSC، إضافة مسارات مع الحفاظ على بيانات المشتركين للقراءة فقط UPF مهندس بيانات التحكم الكامل في.

نطاق الموقع (نشر متعدد المواقع)

تجيب أذونات العناصر على *ما* يمكن للمشغل القيام به. في أسطول يتكون من أكثر من موقع واحد، يجيب محور ثانٍ مستقل على *أين*: مجموعة المواقع التي يمكنهم الوصول إليها على الإطلاق. يجب أن تلبي الطلبات كلا الشرطين.

بشكل افتراضي، يكون المستخدم **غير مقيد** — يمكنه الوصول إلى كل موقع، بما في ذلك المواقع التي تمت إضافتها لاحقًا. يضيق نطاق المستخدم إلى موقع واحد أو أكثر ليشمل تلك المواقع فقط، ويمكن منح عميل كامل دفعة واحدة بحيث يتم تضمين المواقع الجديدة لذلك العميل تلقائيًا.



يرى المشغل ذو النطاق المحدد مواقعهم الخاصة فقط في قائمة المواقع؛ المواقع الأخرى غير مدرجة، والعناصر، والسجلات، والقياسات، ومخزون البرمجيات وأثر المكالمات خلفها مرفوضة من جانب الخادم. يصل المسؤولون إلى كل موقع بغض النظر عن النطاق.

يتم إدارة نطاق الموقع تحت **الإعدادات ← المستخدمون**، من إجراء الكرة الأرضية على صف المستخدم. حدد المواقع التي يمكنهم الوصول إليها، أو اترك كل شيء غير محدد ليظل غير مقيد.

نطاق جهاز الاختبار (مزرعة الهواتف)

مزرعة الهواتف هي نوع عنصر واحد — **أجهزة الاختبار** — تغطي كل مقعد، هاتف ومودم، أدواتها والاختبارات المجدولة لها. يتبع منحها نفس قاعدة الطريقة لكل عنصر آخر:

الإذن	ما يمكن للمشغل القيام به مع الهواتف
للقراءة فقط	قائمة بالمقاعد والأجهزة، مشاهدة شاشة الهاتف، قراءة السجلات، تحميل الملفات وعرض نتائج الاختبار
للقراءة والكتابة	تحميل الملفات وتشغيل SMS، وAT أيضًا الكتابة على الهاتف، إرسال أوامر نص اختبار
كامل	أيضًا إزالة سجل جهاز ومسح بياناته الوصفية المعينة

تُعتبر مشاهدة شاشة الهاتف **قراءة**، وليس تغييرًا — يمكن للمشغل الذي يمكنه المراقبة فقط أن يرى ما يفعله المقعد. الكتابة على الهاتف هي إجراء منفصل على مستوى الكتابة.

نظرًا لأن المزرعة بأكملها هي نوع عنصر واحد، فإن المنح تكون بشكل عام إما كاملة أو لا شيء. لمنح شخص ما *بعض* الهواتف فقط، قم بتعيين **نطاق الجهاز**: حدد الأجهزة الفردية التي يمكنهم استخدامها، مجمعة حسب المقعد. ترك كل شيء غير محدد يتركهم غير مقيدين — كل جهاز، بما في ذلك الأجهزة التي تمت إضافتها لاحقًا.

يرى المشغل ذو النطاق المحدد أجهزته الخاصة فقط في قائمة الأسطول، ويرى كل مقعد مقيدًا بتلك الأجهزة (والمقاعد التي لا تحتوي على أي منها على الإطلاق)، ويتم رفضه إذا ذكر جهازًا آخر مباشرة. يتم رفض تشغيل نص عبر عدة هواتف بشكل قاطع إذا كان أي واحد منها خارج نطاقهم، بدلاً من تشغيله بهدوء على المجموعة الفرعية — ستقرأ التشغيل الجزئي كنجاح كامل. يؤدي تحرير قائمة الجدول الزمني إلى استبدال المجموعة بأكملها، بحيث تبقى مع المشغلين الذين يحملون كل جهاز.

نطاق الموقع ونطاق الجهاز مستقلان: مزرعة الهواتف مستقلة عن الموقع عن عمد، حيث إن المقعد ليس جزءًا من نشر الشبكة.

يتم تعيين كلاهما تحت **الإعدادات → المستخدمون**، من إجراء الكرة الأرضية على صف المستخدم.

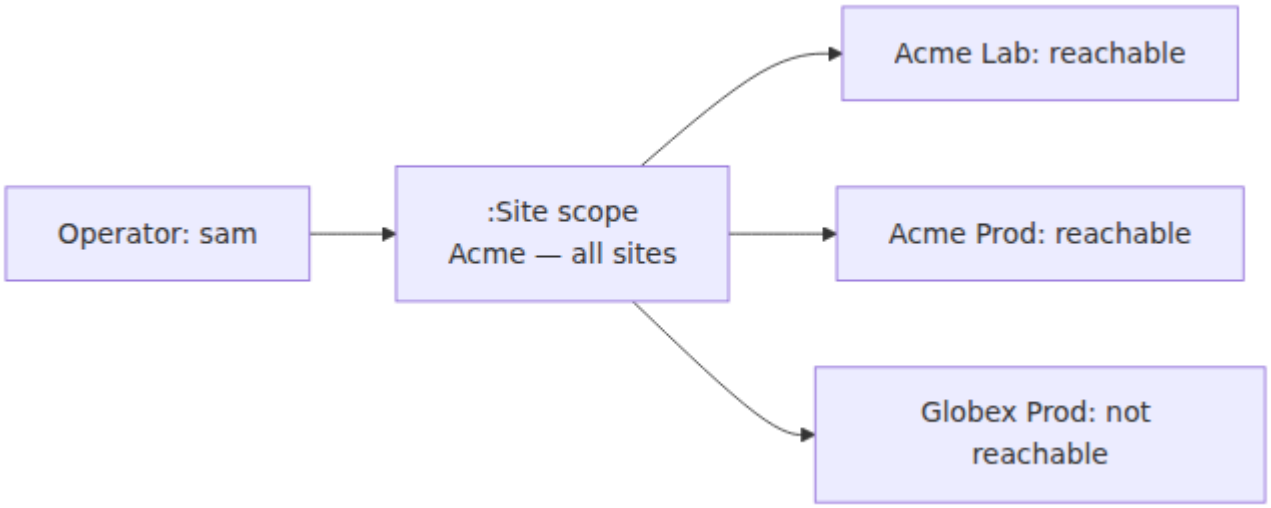
> **عند الترقية:** كانت مزرعة الهواتف تحتاج سابقًا فقط إلى تسجيل دخول، لذا يحتفظ كل حساب موجود قبل هذا التغيير بالوصول الكامل إلى أجهزة الاختبار، مسجلًا كمنح عادية. قم بتشديدها بنفس الطريقة مثل أي عنصر آخر: إلغاء **أجهزة الاختبار** من أي شخص لا ينبغي أن يمتلك الهواتف، وتعيين نطاق جهاز لمن ينبغي أن يمتلك فقط بعضًا منها. تبدأ الحسابات التي تم إنشاؤها بعد ذلك بدون وصول حتى يتم منحها.

المسؤولون

لدى المسؤولين وصول كامل إلى جميع أنواع العناصر تلقائيًا. دور المسؤول هو أيضًا ما يمنح الوصول إلى إدارة المستخدمين والأذونات. احتفظ بعدد المسؤولين قليلًا، ويفضل منح أذونات محددة لكل عنصر للجميع الآخرين.

إدارة الأدوار والأذونات

تتم إدارة الأذونات تحت **الإعدادات → الأذونات**. لكل مستخدم تختاره، حسب نوع العنصر، سواء كان لديهم وصول للقراءة فقط، أو للقراءة والكتابة، أو كامل.

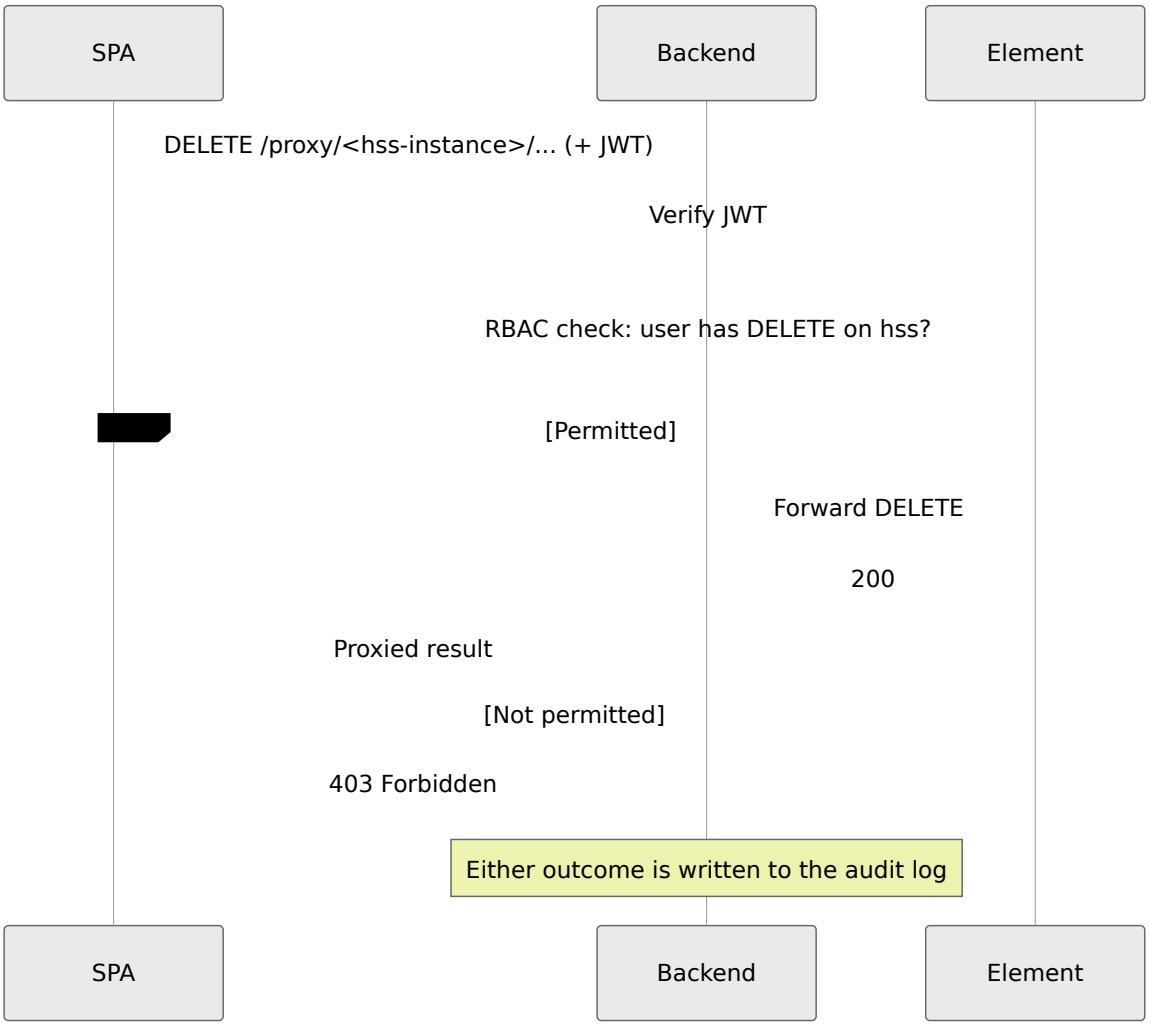


كيفية عمل التنفيذ

يتم تنفيذ RBAC في مكانين متكاملين:

1. **في واجهة المستخدم**: لا يتم عرض عناصر التحكم للإجراءات التي لا يمكنك تنفيذها. إذا كان لديك وصول للقراءة فقط إلى HSS، هناك، حذف/تحرير/إضافة أزرار ترى فلن.
2. **في الخلفية**: يتم إعادة التحقق من كل طلب تم توجيهه ضد أذوناتك *من جانب الخادم*. حتى الطلب المصمم لتجاوز واجهة المستخدم يتم رفضه إذا لم يسمح دورك بذلك العنصر/الطريقة — أو إذا ذكر عنصرًا في موقع خارج نطاق موقعك. يتم أخذ الموقع الذي يعمل عليه الطلب من الطلب نفسه، لذا يتم التحقق منه بدلاً من الوثوق به.

يعني هذا "الدفاع في العمق" أن واجهة المستخدم هي وسيلة راحة، وليست حدود الأمان. الوكيل الخلفي هو الحدود.


SPA
Backend
Element
DELETE /proxy/<hss-instance>/... (+ JWT)
Verify JWT
RBAC check: user has DELETE on hss?
[Permitted]
Forward DELETE
200
Proxied result
[Not permitted]
403 Forbidden
Either outcome is written to the audit log
SPA
Backend
Element

الإعدادات → الأذونات: اختر مستخدمًا، ثم منح مستوى (للقراءة فقط، للقراءة والكتابة، أو كامل) لكل نوع عنصر.

الممارسات الجيدة

- **أقل امتياز**: منح أدنى مستوى يسمح لشخص ما بأداء عمله؛ توسيع فقط عند الحاجة.
- **للقراءة فقط بشكل افتراضي** للعناصر التي يحتاج المشغل فقط لمراقبتها.
- **احتفظ بكامل (حذف)** لأولئك الذين يحتاجون حقًا إلى مسح الجلسات أو إزالة السجلات.
- **عدد قليل من المسؤولين**: استخدم منحًا مستهدفة لكل عنصر بدلاً من توزيع صلاحيات المسؤول.
- **نطاق حسب الموقع** في أسطول متعدد المواقع: امنح مشغلي العميل مواقعهم الخاصة، بحيث لا يمكن أن تصل الخطأ إلى نشر آخر.
- **نطاق أجهزة الاختبار** إلى الهواتف التي يكون شخص ما مسؤولًا عنها، بحيث لا يمكن أن يزعج تشغيل نص مقعد فريق آخر.
- **تثبيت بيانات اعتماد الخدمة**: يمكن تقييد مفتاح API إلى مواقع أقل من مالكه، بحيث لا يمكن لمفتاح صادر لنشر واحد أن يعمل على آخر. يمكن أن يكون المفتاح أضيق دائمًا من الحساب الذي ينتمي إليه، وليس أوسع.

ذات صلة

- JWT تسجيل الدخول وجلسات: المصادقة التي يعتمد عليها RBAC.
- العمليات الشائعة: كيف تشكل الأذونات واجهة المستخدم اليومية.
- تسجيل التدقيق: يتم تسجيل كل من الإجراءات المسموح بها والمرفوضة.

المصادقة والتحكم في الوصول

يعتبر OmniWeb هو المدخل الوحيد إلى الشبكة بأكملها، لذا فإن التحكم في الوصول هو واحدة من أهم مسؤولياته. يستخدم تسجيل الدخول المعتمد على JWT، والتحكم في الوصول القائم على الأدوار (RBAC) للوصول إلى SSH بدقة على كل عنصر، وتسجيل الدخول باستخدام مفتاح المضيفين، وسجل تدقيق موحد يمتد عبر البوابة والمضيفين الذين يديرهم.

تم تقسيم هذه المنطقة إلى صفحات مركزة:

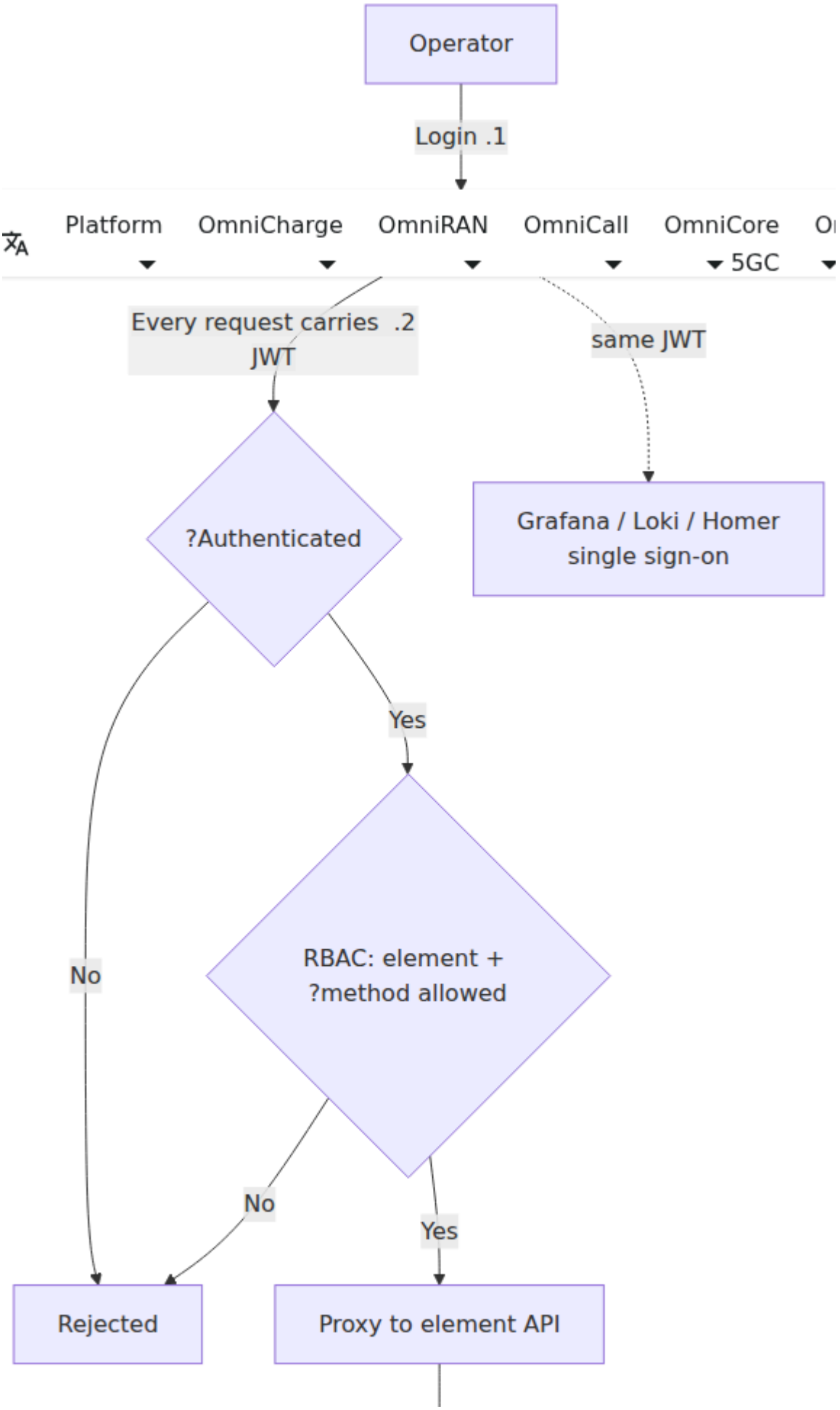
← العودة إلى دليل العمليات

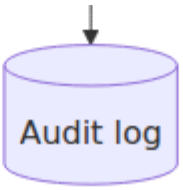
في هذا القسم

- **تسجيل الدخول وجلسات JWT**: كيفية تسجيل دخول المشغلين، كيفية عمل JWT، مدة صلاحية الرمز، وكيف تمتد جلسة تسجيل الدخول الواحدة عبر Grafana وLoki وHomer.
- **التحكم في الوصول القائم على الأدوار (RBAC)**: أذونات لكل عنصر، لكل طريقة؛ كيفية منحها؛ وكيف يتم تنفيذها.
- **تسجيل الدخول باستخدام مفتاح SSH**: يقوم المضيفون المدارة بجلب مفتاح OmniWeb (AuthorizedKeysCommand) العمومي لكل مستخدم مباشرة من، لذا يتم منح/إلغاء الوصول إلى المضيفين مركزيًا.
- **تسجيل التدقيق**: ثلاث طبقات من التدقيق: تدقيق طلبات البوابة، تدقيق تسجيل الدخول عبر SSH، وتدقيق الأوامر.

نموذج التحكم في الوصول

يضع OmniWeb أربعة تحكمات. يجب أن تمر الطلبات بكل واحدة قبل أن تصل إلى عنصر، ويتم تسجيل السلسلة بالكامل.


Operator
Login .1
Platform
OmniCharge
OmniRAN
OmniCall
OmniCore
5GC
Every request carries .2 JWT
same JWT
?Authenticated
Grafana / Loki / Homer single sign-on
Yes
No
RBAC: element + ?method allowed
No
Yes
Rejected
Proxy to element API



الصفحة	ما تتحكم فيه	الطبقة
تسجيل الدخول وJWT	موقع JWT من أنت، مثبت بواسطة	**المصادقة**
RBAC	ما يمكنك القيام به، حسب نوع العنصر وطريقة HTTP	**التفويض (RBAC)**
تسجيل الدخول باستخدام مفتاح SSH	إلى أين؛ المفاتيح مقدمة SSH من يمكنه مباشرة من OmniWeb	**وصول المضيف**
تسجيل التدقيق	ما حدث فعليًا، عبر البوابة والمضيفين	**التدقيق**

لماذا هذا مهم

نظرًا لأن OmniWeb يتوسط كل عنصر، لوحة معلومات Grafana، استعلام Loki، وجلسة Homer، هناك. للشبكة *السطح التشغيلي بالكامل* تحكم هذه الوصول في فإن سلسلة التحكم مكان واحد لمنح الوصول، ومكان واحد لإلغائه، ومسار واحد يسجل من قام بماذا، على البوابة وعلى المضيفين الأساسيين.

وتغييرات SSH، تسجيلات الدخول، تسجيلات الدخول عبر API، مسار واحد لكل شيء: طلبات المصدر. انظر تسجيل التدقيق IP الأذونات، مع المستخدم، العنصر، الطريقة، النتيجة، وعنوان.

ابدأ مع تسجيل الدخول وجلسات JWT.

تتبع المكالمات (SIP)

تتبع المكالمات هو أداة SIP لاستكشاف أخطاء المكالمات الصوتية. يسجل إشارات OmniWeb للمكالمات التي تعبر IMS. وفتح تقرير كامل ووسائط RTP التي تعبر ثم يتيح لك البحث عن تلك المكالمات، لكل مكالمة، ومتابعة المكالمة كدرج إشارات عبر الشبكة، وقياس جودة الصوت، والاستماع إلى الصوت، وتنزيل التقاط الحزم الخام (PCAP).

تتبع المكالمات هو أداة على مستوى الموقع. يظهر في الشريط الجانبي تحت **تتبع الجلسة** كـ **تتبع SIP**. تظهر الأداة فقط عندما يتم تكوين خدمة الالتقاط وقابليتها للوصول للموقع المحدد.

← دليل العمليات

المحتويات

- ما هو
- الهيكلية
- البحث
- تفاصيل المكالمة
- الدرج (تتبع الجلسة)
- علامة QoS
- استمع
- تنزيل PCAP
- المكالمات النشطة
- المراقب المباشر
- وكلاء الالتقاط عن بُعد
- قواعد التسجيل والاحتفاظ
- الخصوصية والتنصت القانوني
- كيف يقارن تتبع المكالمات مع هومر وتتبع الجلسة

ما هو

تتبع المكالمات يجيب على سؤال واحد بعمق: **ماذا حدث لهذه المكالمة؟** بالنسبة لأي مكالمة مسجلة، فإنه يقدم لك:

- الطرفان، أرقامهما، مجالات SIP الخاصة بهما، واسم العرض.
- عنوان IP SIP لكل طرف، مرتبط بعنصر الشبكة OmniWeb الخاص به.
- الاستجابة النهائية لـ SIP وسبب الانفصال SIP (SIP وQ.850).
- جودة الصوت لكل اتجاه وسائط: MOS، تذبذب، فقدان الحزم، وتأخير الذهاب والإياب.
- تدفق رسائل SIP عبر كل عنصر (الدرج) الكامل IMS الذي لمس المكالمة.
- الصوت المسجل وIPCAP الخام.

تتبع المكالمات يسجل المكالمات من المصدر. لأنه يلتقط SIP Call-ID والوسائط على السلك، فإن المكالمة تتطابق مع التقاط الحزم الخاص بها دون أي تخمين.

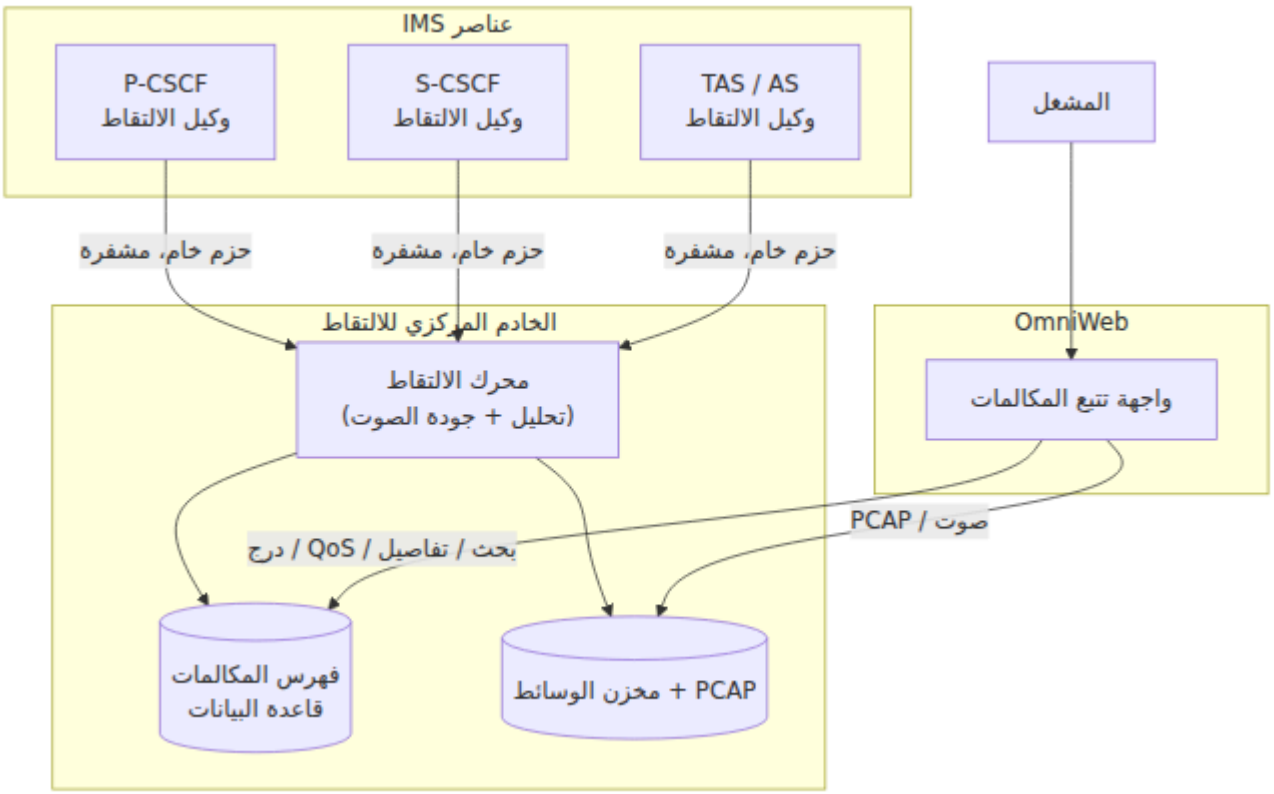
تُبلغ جودة الصوت كـ **MOS** (متوسط تقييم الرأي). MOS هو تقييم من 1 إلى 5. تقييم 4.0 أو أعلى: الأخضر للجيد، جيد، 3.0 إلى 4.0 عادل، وأقل من 3.0 ضعيف. OmniWeb يلون قيم MOS في شبكة صحية تسجل (عالية النطاق) AMR-WB والعنبر للعادل، والأحمر للضعيف. مكالمات حوالي 4.5.

الهيكلية

تتبع المكالمات يستخدم جزئين:

1. **وكلاء الالتقاط** يعملون على عناصر IMS (P-CSCF، S-CSCF، وTAS). كل وكيل يراها على مضيفه. الوكلاء لا يخزنون أو يحللون الحزم محليًا. RTP وSIP يلتقط حزم التي يقومون بإعادة توجيه الحزم الخام إلى الخادم المركزي للالتقاط عبر قناة مشفرة.
2. **الخادم المركزي للالتقاط** يحلل كل حزمة، يحسب جودة الصوت، ويكتب فهرسًا إلى قاعدة بياناته. يحتفظ بمخزن التقاط الحزم والوسائط المسجلة. OmniWeb يقرأ هذا الخادم الواحد للبحث، تفاصيل المكالمة، الدرج، وQoS، الصوت وIPCAP.

لا تحتفظ بأي IMS هذا التصميم يحتفظ بكل البيانات المسجلة على خادم مركزي واحد. عناصر بيانات التقاط خاصة بها.



توفر وكلاء الالتقاط لتتبع المكالمات رؤية من العديد من النقاط في الشبكة. يتم تجميع مكالمة متعدد القفزات عبر SIP واحدة من كل وكيل رأى المكالمة. هذا هو ما يسمح للدرج بإظهار تدفق P-CSCF وS-CSCF وTAS.

البحث

افتح تتبع المكالمات للوصول إلى عرض **البحث**. البحث يجد المكالمات المكتملة في فهرس المكالمات المركزي.

عرض البحث. كل صف يراص المتصل والمستقبل (الاسم، المجال، الرقم، IP SIP، وعميل المستخدم) بجانب خلايا RTP تظهر IP لكل اتجاه التي تقديرات ثلاثة الترميز، المصدر، MOS، التذبذب، والفقد.

المرشحات

قم بتعيين مرشح واحد أو أكثر، ثم اختر **بحث**. جميع المرشحات تتجمع مع AND.

المرشح	ما يتطابق
الرقم	رقم المتصل أو رقم المستقبل.
نطاق الوقت	نافذة مسبقة (آخر 15 دقيقة إلى آخر 7 أيام) أو بداية ونهاية مخصصة.
الاتجاه	وارد، صادر، أو داخلي. يأتي الاتجاه من دور المتصل و IP المستقبل.
أدنى MOS	احتفظ فقط بالمكالمات التي يكون فيها أسوأ اتجاه MOS عند أو فوق هذه القيمة. استخدم هذا للعثور على المكالمات الجيدة، أو عكس قراءتك للعثور على السيئة.
أقصى فقدان	احتفظ فقط بالمكالمات التي يكون فيها أسوأ اتجاه فقدان الحزم عند أو أقل من هذه القيمة.

شبكة النتائج

كل صف من النتائج يظهر:

- **الوقت**: بداية ونهاية المكالمة.
- **المتصل** و**المستقبل**: خلية متراصة مع الرقم والمجال (`num@domain`)، اسم العرض، IP SIP (رابط إلى ذلك العنصر في OmniWeb)، علامة. وعميل المستخدم. BYE تشير إلى الطرف الذي أرسل **معلقة**.
- **النتيجة**: رمز الاستجابة النهائية لـ SIP والنص.
- **RTP A** و**RTP B**: خلية واحدة لكل اتجاه وسائط. كل خلية تظهر IP المصدر، الترميز، التذبذب، وعدد الحزم المفقودة. (ثابت 50 | ثابت 200 | متكيف) ثلاثة تقديرات MOS ملونة القيم الثلاثة لـ MOS.
- **المدة (ث)**: مدة المكالمة بالثواني.
- **PCAP**: زر تنزيل لكل صف لتق التقاط الحزم لتلك المكالمة.

اختر صفًا لفتح تفاصيل المكالمة.

تفاصيل المكالمة

عرض تفاصيل المكالمة هو التقرير الكامل لمكالمة واحدة. يفتح عند اختيار نتيجة بحث. يحمل عنوان URL معرف المكالمة، بحيث يمكنك وضع إشارة مرجعية أو مشاركة المكالمة.

عرض تف��صيل المكالمة. يظهر الرأس Call-ID، المدة، والسياق. يظهر شريط الملخص البداية، الرنين، الاتصال، آخر استجابة SIP، الهوية، العمودين ذو الجدول يظهر. وأسباب الانفصال PDD، وجودة الصوت للمتصل (A) والمستقبل (B).

الرأس والسياق

يظهر الرأس **Call-ID** (وكيل المالك **المستشعر**، **الاتجاه** تظهر أدناه السياق كتلة. السلك على الالتقاط)، أي طرف **أغلق**، وقت **الانتهاء**، و**اسم المتصل**.

شريط الملخص

شريط الملخص هو نظرة عامة من سطر واحد على المكالمة:

الحقل	المعنى
البداية	متى بدأت المكالمة.
المدة	إجمالي طول المكالمة.
PDD	تأخير ما بعد الطلب: الوقت من INVITE إلى أول إشارة رنين.
الرنين	كم من الوقت رن الهاتف قبل الإجابة.
الاتصال	كم من الوقت كانت المكالمة متصلة (تدفق الوسائط).
آخر استجابة SIP	رمز الاستجابة النهائية لـ SIP والنص.
سبب SIP	سبب الانفصال في SIP، عندما يسجل محرك الالتقاط واحدًا.
سبب Q.850	سبب الانفصال في Q.850 موجودًا، والنص.
المتصل و**المستقبل**	الطرفان كـ `num@domain`.

جدول الهوية وجودة الصوت

الجدول الرئيسي يحتوي على عمودين: **المتصل (A)** و**المستقبل (B)**. كل IP يرتبط بعنصر الخاص به عندما يكون العنصر معروفًا. يحتوي الجدول على ثلاث مجموعات OmniWeb الشبكة.

الهوية:

الصف	المعنى
IP SIP	عنوان IP لإشارات SIP للطرف.
IP RTP	عنوان IP لوسائط RTP للطرف.
منفذ RTP	منفذ وسائط RTP.
عميل المستخدم	عميل SIP للطرف.
الترميز	الترميز الصوتي، مثل AMR-WB.
الحزم المستلمة	عدد حزم RTP المستلمة.
الحزم المفقودة	عدد حزم RTP المفقودة.

MOS: ثلاثة مقدرات MOS، كل منها يظهر كـ `متوسط | الحد الأدنى`:

الصف	المعنى
MOS 50 ثابت	MOS على نافذة ثابتة من 50 حزمة.
MOS 200 ثابت	MOS على نافذة ثابتة من 200 حزمة.
MOS 500 متكيف	MOS على نافذة متكيفة تصل إلى 500 حزمة.

RTCP: عدد الفقد والجزء المفقود، RTCP تذبذب، RTP تذبذب (الأقصى والمتوسط)**التذبذب و** RTCP وتأخير الذهاب والإياب في RTCP، في (الأقصى والمتوسط).

الدرج (تتبع الجلسة)

علامة SIP **الدرج** ترسم المكالمة كتدفق إشارات مرتبة زمنياً. يقوم تتبع المكالمات بتجميع رسائل IMS: على معًا من كل وكيل التقاط رأى المكالمة. النتيجة هي درج متعدد القفزات عبر عناصر سبيل المثال من P-CSCF إلى S-CSCF إلى TAS.

يظهر الدرج SIP. التي عبرتها المكالمة. كل درجة هي رسالة IMS علامة الدرج. الأعمدة هي عناصر مع دلتا زمنية لكل رسالة ووقت، BYE إلى ACK إلى 100 إلى 180 إلى 200 إلى INVITE تدفق الذهاب والإياب من الطلب إلى الاستجابة.

كل عمود هو عنصر IMS مأخوذة من SIP واحد، معنون بدوره واسم المضيف. كل درجة هي رسالة المصدر إلى الوجهة. يظهر الدرج:

- **دلتا زمنية لكل رسالة** (الفجوة منذ الرسالة السابقة).
- **وقت الذهاب والإياب من الطلب إلى الاستجابة** لكل استجابة، مرتبطة مرة أخرى بطلبها.
- أوضاع زمنية **مطلقة**، **نسبية**، و**منذ** لعمود الوقت.
- **فك تشفير الحزم في السطر**: اختر درجة لرؤية نص رسالة SIP الكامل وعرض سداسي.

تحتوي لوحة **تفاصيل الجلسة** على قائمة الجلسات في الدرج. لمكالمة واحدة، هناك جلسة واحدة، لذا تبقى اللوحة مطوية.

يستخدم الدرج نفس العرض مثل تدفقات تتبع الجلسة الحية على مستوى الشبكة. انظر السجلات وتتبع المشتركين لأداة تتبع الجلسة الأوسع.

علامة QoS

علامة **QoS** تظهر جودة الصوت على مدار حياة المكالمة.

علامة QoS. تظهر الجداول توزيع PDV (التأخير) والفقدان المتتالي لكل اتجاه. يتم رسم رسم بياني تفاعلي لجودة التأخير و MOS على طول المكالمة أدناه الجداول.

تحتوي علامة QoS على ثلاثة أجزاء:

- رسم بياني تفاعلي **MOS للتأخير / التذبذب وجودة** على مدار المكالمة. الرسم البياني لكل اتجاه وسائط MOS، مما يمكنك قراءة التأخير و في أي نقطة في المكالمة. يظهر أين انخفضت الجودة.
- **توزيع PDV (التأخير)**: عدد الحزم التي وقعت في كل دلو تأخير (على سبيل المثال: 50 إلى 70 مللي ثانية، 70 إلى 90 مللي ثانية، وهكذا حتى أكثر من 300 مللي ثانية). توزيع يبقى في الدلاء المنخفضة يعتبر صحيًا.
- تحليل **الفقدان المتتالي**: عدد المرات التي فقدت فيها 1، 2، 3، وما يصل إلى 10 حزم بشكل متتالي. الفقدان الفردي المعزول أقل وضوحًا بكثير من الفقدان الطويل.

يتم عرض كلا التحليلين لكل اتجاه (المتصل والمستقبل)، بحيث يمكنك معرفة أي الساقين كانت بها المشكلة.

استمع

تقوم لوحة RTP **استمع** بتشغيل المكالمة المسجلة في المتصفح. يتم فك تشفير الصوت من الملتقط. المتصل هو القناة اليسرى والمستقبل هو القناة اليمنى، بحيث يمكنك سماع كل جانب بمفرده.

تعمل ميزة الاستماع فقط عندما تم تسجيل وسائط المكالمة ويمكن فك تشفير الترميز الخاص بها. انظر قواعد التسجيل والاحتفاظ لمعرفة كيفية تسليح التقاط الوسائط.

تنزيل PCAP

في كل من شبكة البحث ورأس تفاصيل المكالمة، كل مكالمة تحتوي على زر **تنزيل PCAP**. التنزيل هو التقاط الحزم الخام (SIP و، عند التسجيل RTP) لتلك المكالمة الواحدة. استخدم PCAP لفحص المكالمة في أداة خارجية مثل Wireshark.

المكالمات النشطة

عرض **المكالمات النشطة** يظهر المكالمات التي هي قيد التقدم الآن. يقرأ قائمة المكالمات الحية من وكلاء الالتقاط ويقوم بتحديثها على فترات قصيرة، بحيث تظهر الصفوف وتختفي مع إعداد المكالمات وإغلاقها.

عرض المكالمات النشطة. كل صف هو مكالمة حية مع حالتها (متصلة أو قيد الإعداد)، الطرفان الحي، ووكيل الالتقاط المالك MOS ،الخاصة بهما، الاتجاه، المدة المتزايدة، الترميز IP وعناوين.

من المتصل إلى IP كل صف يظهر **الحالة** (متصلة، قيد الإعداد، أو فاشلة)، الطرفان، مسار و**المستشعر** ،SIP الحي، آخر استجابة **MOS** ،المستقبل، **الاتجاه**، **المدة** المتزايدة، **الترميز** المالك (وكيل الالتقاط). قم بإيقاف **التحديث التلقائي** للاحتفاظ بالقائمة الحالية.

المراقب المباشر

عرض **المراقب المباشر** يظهر صحة الخادم المركزي للالتقاط ووكلاء الالتقاط الخاصين به.

عرض المراقب المباشر. تظهر لوحة الخادم المركزي النسخة، وقت التشغيل، عدد المكالمات النشطة، معدل التدفق، فقدان الحزم، ومتوسط الحمل. جدول وكلاء الالتقاط عن بُعد يسرد كل وكيل. تظهر لوحة إدخال وإخراج القرص للمخزن الاستخدام ومعدل التدفق.

يعرض العرض:

- **الخادم المركزي**: النسخة والبناء، وقت التشغيل، عدد المكالمات النشطة، معدل الالتقاط، فقدان الحزم، متوسط الحمل، وآخر مرة تم فيها كتابة سجل مكالمة.
- **وكلاء الالتقاط عن بُعد**: الوكلاء لكل عنصر وحالتهم (انظر وكلاء الالتقاط عن بُعد).
- **إدخال وإخراج القرص للمخزن**: الاستخدام، معدل القراءة والكتابة، IOPS، زمن الانتظار، السعة المستخدمة، ومستوى المخزن المؤقت لقرص المخزن.
- تغذية نشاط حية للمكالمات الجارية.

راقب هذا العرض لتأكيد أن محرك الالتقاط صحي، ولا يفقد الحزم، ولديه مساحة كافية على القرص.

وكلاء الالتقاط عن بُعد

جدول **وكلاء الالتقاط عن بُعد** (في عرض المراقب المباشر) يسرد وكلاء الالتقاط الذين يعملون على عناصر IMS. كل صف يظهر:

العمود	المعنى
الوكيل	اسم مضيف الوكيل. اختره لفتح ذلك المضيف في قائمة المضيفين.
معرف المستشعر	المعرف الرقمي للوكيل في فهرس الالتقاط.
الحالة	نشط، خامل، أو غير معروف، مستمد من المكالمات الحية وسجلات المكالمات الأخيرة.
المكالمات النشطة	عدد المكالمات التي يقوم الوكيل بالتقاطها الآن.
CDRs	عدد سجلات المكالمات التي أنتجها الوكيل.
آخر ظهور	متى كان آخر مرة أنتج فيها الوكيل سجل مكالمة.

استخدم هذا الجدول لتأكيد أن كل عنصر IMS الذي يجب أن يلتقط يقوم بالتقاط. وكيل يكون خاملًا أو مفقودًا بشكل غير متوقع يعني أن حركة المرور لذلك العنصر لا يتم تسجيلها.

قواعد التسجيل والاحتفاظ

عرض **قواعد التسجيل** يتحكم في أي المكالمات يتم تسجيل **وسائطها**، ويظهر الاحتفاظ بمخزن الالتقاط وقاعدة بيانات الفهرس.

عرض قواعد التسجيل. يتم تجميع القواعد حسب نوع المطابقة: حسب الرقم، وحسب IP، حسب مجال SIP (رأس SIP). يوجد أيضًا مجموعة حسب كل قاعدة تسلح التقاط وسائط، تتخطى RTP هدفًا، أو تحفظ بيانات الرسم البياني لجودة الخدمة.

قواعد التسجيل

لكل مكالمة، لكنه لا يسجل **وسائط** SIP بشكل افتراضي، يسجل ��حرك الالتقاط إشارات **RTP**. تسلح قاعدة التسجيل التقاط الوسائط لهدف محدد. يقوم محرك الالتقاط بإعادة قراءة القواعد مباشرة، دون الحاجة لإعادة التشغيل.

تُجمع القواعد حسب كيفية مطابقتها لمكالمة:

المجموعة	تتطابق مع
حسب IP	عنوان IP المصدر أو الوجهة وقناع.
حسب الرقم	بادئة رقم المتصل أو المستقبل.
حسب مجال SIP	مجال SIP.
حسب رأس SIP	قيمة رأس SIP عشوائية.

كل قاعدة تحمل مجموعة من العلامات:

العلامة	التأثير
RTP	تسلح التقاط وسائط RTP إلى الاستماع للهدف المتطابق. هذا هو ما يسمح لك بـ مغلفًا عالميًا RTP الوسائط الكامل. احتفظ بـ PCAP المكالمة والحصول على وسلحه لكل هدف.
تخطي	إسقاط الهدف المتطابق تمامًا: لا سجل مكالمة ولا التقاط. استخدم هذا لحركة المرور الاختبارية المعروفة.
رسم بياني	حفظ بيانات الرسم البياني لجودة الخدمة الدقيقة للهدف المتطابق، والتي تدفع رسم بياني QoS.
rtcp	تسجيل تقارير جودة RTCP للهدف المتطابق.
مفعل	تشغيل القاعدة أو إيقافها دون حذفها.

لتسليح الالتقاط لهدف واحد، أضف قاعدة في مجموعة المطابقة، املأ قيمة المطابقة، وقم بتشغيل **RTP**. مفعل **تخطي** مع قاعدة أضف المعروفة، الاختبارية المرور حركة تسجيل لإيقاف.

الاحتفاظ

تظهر لوحة الاحتفاظ مدة الاحتفاظ بالبيانات المسجلة. يتم تعيين الاحتفاظ مركزيًا على الخادم المركزي للالتقاط. اللوحة للقراءة فقط في OmniWeb.

تتحكم إعدادات الاحتفاظ في شيئين: حدود الحجم والعمر لمخزن القرص (مقسم حسب SIP وRTP)، وبيانات الرسم البياني (QoS)، وحدود العمر لفهرس المكالمات وصفوف الجودة لكل تدفق في قاعدة البيانات. الجدول أدناه يسرد الإعدادات التي تبلغ عنها اللوحة:

الإعداد	المعنى
`maxpoolsize_gb`	الحد الأقصى لحجم المخزن الإجمالي، بالجيجابايت. تتم إزالة أقدم البيانات عند الوصول إلى هذا الحد.
`maxpooldays`	الحد الأقصى لعمر أي بيانات مخزن، بالأيام.
`maxpoolsipsize_gb`	الحد الأقصى لحجم مخزن SIP، بالجيجابايت.
`maxpoolsipdays`	الحد الأقصى لعمر مخزن SIP، بالأيام.
`maxpoolrtpsize_gb`	الحد الأقصى لحجم مخزن RTP (الوسائط)، بالجيجابايت.
`maxpoolrtpdays`	الحد الأقصى لعمر مخزن RTP، بالأيام.
`maxpoolgraphsize_gb`	الحد الأقصى لحجم مخزن رسم بياني QoS، بالجيجابايت.
`maxpoolgraphdays`	الحد الأقصى لعمر مخزن رسم بياني QoS، بالأيام.
`cleandatabase_cdr_days`	الحد الأقصى لعمر سجلات المكالمات في قاعدة بيانات الفهرس، بالأيام.
`cleandatabase_rtp_stat_days`	الحد الأقصى لعمر صفوف الجودة لكل تدفق في قاعدة البيانات، بالأيام.

احتفظ بفترة احتفاظ RTP كبيرة. وسلح التقاط SIP، أقصر من فترة احتفاظ بيانات الوسائط (RTP) فقط للأهداف التي تحتاجها RTP.

الخصوصية والتنصت القانوني

تسجيل **وسائط** المكالمات هو قرار تنصت قانوني. تسجل التقاط الإشارات من اتصل بمن ومتى. (**RTP** قاعدة تسجيل) تسجيل الوسائط يسجل **محتوى** المكالمة: الصوت. تسلح التقاط الوسائط فقط للأهداف التي لديك إذن بتسجيلها، وفقط للمدة التي لديك إذن بها.

لأقصر RTP مغلقًا بشكل افتراضي وسلحه لكل هدف. قم بتعيين فترة احتفاظ RTP احتفظ بالتقاط فترة يسمح بها سياستك. اتبع قوانين الخصوصية المحلية وقواعد الموافقة لكل من التقاط الإشارات والوسائط.

كيف يقارن تتبع المكالمات مع هومر وتتبع الجلسة

ثلاث طرق للنظر إلى الإشارات. اختر الأنسب OmniWeb لدى:

	تتبع المكالمات (تتبع SIP)	التقاط هومر (SIP)	تتبع الجلسة
النطاق	SIP ووسائط RTP لمكالمات IMS	SIP فقط	الشبكة بأكملها: Diameter، GTP-C، PFCP، SIP، MAP
السؤال الذي يجيب عليه	"ماذا فعلت هذه المكالمة، وما مدى جودة الصوت؟"	"ماذا فعل تدفق SIP لهذه المكالمة؟"	"ماذا حدث لهذا المشترك عبر كل عنصر؟"
جودة الصوت (MOS)	نعم	لا	لا
الصوت المسجل	نعم	لا	لا
تنزيل PCAP	نعم، لكل مكالمة	لا	لا
الأفضل لـ	تشخيص جودة المكالمة VoLTE، الوسائط، والتدفق	نظرة سريعة على تدفق SIP	متابعة مشترك واحد من البداية إلى النهاية

اختر تتبع المكالمات عندما تحتاج إلى تقييم **جودة الصوت** للمكالمة، سماع الصوت، أو الحصول على PCAP الوسائط. اختر تتبع الجلسة عندما تريد متابعة مشترك عبر كامل المكدس.

ذات صلة

- السجلات وتتبع المشتركين: تتبع الجلسة على مستوى الشبكة والدرج المشترك.
- هومر: التقاط SIP: أداة التقاط SIP فقط.
- الهيكل الشبكي: قائمة المضيفين التي ترتبط بها وكلاء الالتقاط.

العمليات الشائعة

كل عنصر في الشبكة في OmniWeb مختلف من الداخل، لكن الطريقة التي *تعمل* بها معهم متعمدة لتكون متشابهة. توثق هذه الصفحة الأنماط المشتركة بين جميع العناصر: عرض البيانات، قراءة التكوين، تشغيل الإجراءات، مشاهدة السجلات، وفهم الاستطلاع، تحرير وتغيير إعدادات NF. تعلم هذه مرة واحدة وستطبق على كل NF آخر، MSC، SMSC، UPF، HSS، والأذونات.

تأتي لقطات الشاشة أدناه من عناصر محددة، لكنها توضح النمط *العام*: تظهر نفس عناصر التحكم، مع حقول مختلفة، على كل عنصر.

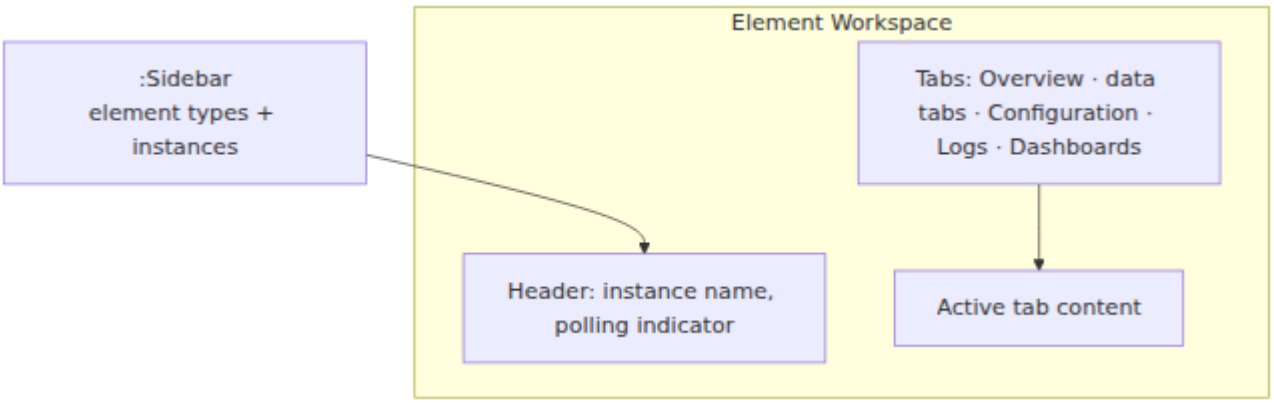
← العودة إلى دليل العمليات

جدول المحتويات

- تشريح الصفحة
- عرض البيانات
- عرض التفاصيل
- تحرير وتغيير إعدادات NF
- تشغيل الإجراءات (ping، مسح، تحرير، اختبار)
- عرض التكوين
- السجلات على كل عنصر
- لوحات المعلومات على كل عنصر
- الاستطلاع في الوقت الحقيقي
- الأذونات وما يمكنك تغييره
- عرض متعدد الحالات والأسطول

تشريح الصفحة

اختيار مثيل عنصر في الشريط الجانبي يفتح مساحة عمله. تشترك كل مساحة عمل عنصر في نفس التخطيط:



- **نظرة عامة**: علامة التبويب الرئيسية: الصحة، العدادات الرئيسية، وحالة المكونات لذلك المثيل.
- **علام��ت تبويب البيانات**: العروض الخاصة بالعنصر (الجلسات، المشتركين، الأقران، التوجيه، إلخ).
- **التكوين**: عرض منظم لتكوين العنصر في وقت التشغيل (حيث يتم الكشف عنه).
- **السجلات**: عارض سجلات Loki مباشر مخصص لذلك العنصر.
- **لوحات المعلومات**: لوحات Grafana المدمجة لذلك العنصر (عندما تتطابق علامات Grafana).

أو النقر الأوسط، أو) **Ctrl/Cmd-click** تكون إدخالات الشريط الجانبي روابط عادية، لذا يمكنك أي منها لفتح تلك المساحة في علامة تبويب جديدة في (النقر الأيمن → *فتح في علامة تبويب جديدة* المتصفح. هذا مفيد لمشاهدة عنصرين في وقت واحد.

عرض البيانات

تُعرض البيانات التشغيلية في جدول متسق وقابل للفرز في جميع أنحاء OmniWeb. توفر الجداول:

- **الفرز** حسب العمود.
- **التقسيم** لمجموعات النتائج الكبيرة.
- **البحث / التصفية** حيث تدعم واجهة برمجة التطبيقات للعنصر ذلك (على سبيل المثال، البحث حسب IMSI/MSISDN أو UE IP).
- **تحميل هيكلي** أثناء جلب البيانات، وحالة **فارغة واضحة** عندما لا يوجد شيء للعرض.
- **النقر على الصف** للانتقال إلى عرض التفاصيل حيثما وُجد.

تكون القيم مُنسقة لسهولة القراءة: الطوابع الزمنية كوقت محلي، المدد كـ `h m s`، عدد البايتات كـ KB/MB/GB، والأرقام الكبيرة مع فواصل الآلاف.

النمط العام للقائمة (هنا، قائمة مشتركي): قابلة للبحث، قابلة للفرز، مقسمة، مع إمكانية النقر والتحرير داخل الصفوف. نفس الجدول يقود الجلسات، الأقران، المسارات، وكل قائمة أخرى.

يمكن أن تعرض الجداول خلايا أغنى: هنا، أشرطة الاستخدام لكل صف. النمط هو نفسه؛ فقط الأعمدة تختلف.

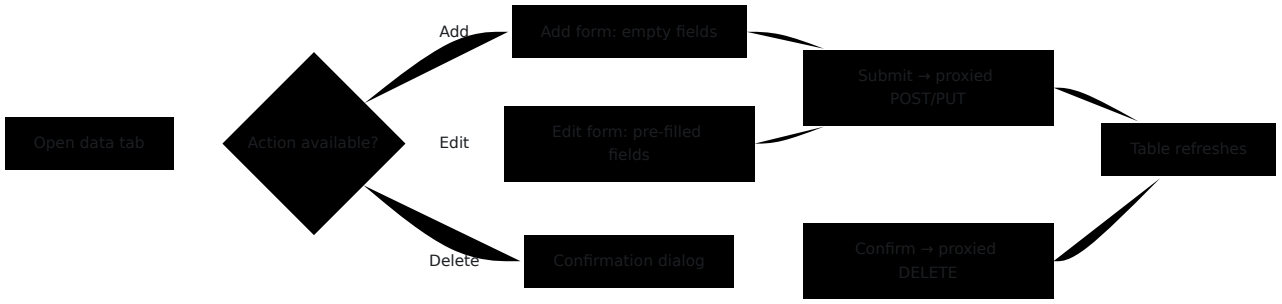
عرض التفاصيل

حيث يحتوي الصف على المزيد ليظهر، انقر عليه لفتح عرض التفاصيل. تعيد هذه استخدام نفس التصميم (الرأس، الاستطلاع، الإجراءات) ولكن تقدم السجل الفردي بعمق، على سبيل المثال، خريطة علاقات تفاعلية لكائن معقد:

عرض تفاصيل مفتوح من صف جدول: هنا، خريطة تفاعلية لقواعد داخلية لجلسة واحدة. يتم الوصول إلى عروض التفاصيل بنفس الطريقة في كل مكان: انقر على الصف.

NF تحرير وتغيير إعدادات

ذلك من خلال **نموذج** OmniWeb أينما تدعم واجهة برمجة التطبيقات للعنصر التعديل، تعرض **إجراء** متسق. نفس مكون النموذج يقود "إضافة مشترك"، "إضافة مسار"، "تحرير قاعدة QoS"، و"تغيير ملف تعريف". تختلف الحقول فقط.



تدعم نماذج الإجراءات هذه الأنواع من الحقول: **نص**، **رقم**، **اختيار** (قائمة منسدلة)، **منطقي** (تبديل)، **كلمة مرور** (مخفاة، مع تبديل عرض/إخفاء)، و**نص متعدد الأسطر**. يمكن تمييز كل حقل على أنه مطلوب، يحمل عنصر نائب، ويظهر نص مساعد. يظهر النموذج حالة تحميل أثناء الإرسال ويبلغ عن النجاح أو الفشل عبر إشعار على الشاشة.

ترتبط طريقة HTTP الأذونات انظر إذن. بمستوى إجراء كل وراء.

نفس النمط، ثلاثة عناصر

توضح هذه *نفس* الآلية المطبقة على NFs مختلفة:

المهمة	المكان	ماذا يحدث
إضافة/تحرير مشترك	HSS → → المشتركين إضافة	املأ النموذج (IMSI، MSISDN، ملف تعريف، مفاتيح) → `POST`/`PUT` عبر الوكيل → تحديث القائمة
إضافة/تغيير مسار	SMSC → → التوجيه إضافة (أو MSC → التوجيه)	املأ القاعدة (النمط، الوجهة، الأولوية) → كتابة عبر الوكيل → تحديث الجدول
مسح/إطلاق جلسة	UPF → الجلسات (أو MSC → المكالمات)	اختر السجل → تأكيد → `DELETE` عبر الوكيل → تحديث القائمة

الآليات متطابقة: نموذج أو حوار تأكيد، كتابة عبر الوكيل، تحديث الجدول. فقط العنصر والحقول تتغير.

تغيير التوجيه هو نفس نمط التحرير: جدول التوجيه هو قائمة تضيف إليها وتحررها؛ بعض العناصر تقوم أيضًا بتحليل الوجهات إلى شرائح قابلة للقراءة وتقدم محاكي لاختبار تغيير قبل أن يصبح ساري المفعول.

تشغيل الإجراءات

تعرض العديد من العناصر **إجراءات تشغيلية** لا تناسب نموذجًا بسيطًا. يتم عرضها بجانب CRUD، كأزرار تقوم بتفعيل استدعاء عبر الوكيل وتظهر النتيجة في الداخل. أمثلة على نفس نمط الزر-ال��جراء:

التأثير	العنصر	إجراء المثال
إنهاء مكالمة نشطة	MSC → المكالمات	إطلاق مكالمة قسرية
اختبار إمكانية الوصول إلى خط SIP	MSC → جيران SIP	اختبار ping لجار SIP
إرسال طلب Multimedia-Auth-Request تجريبي	TWAG → Diameter	اختبار MAR لجار Diameter
إعادة توجيه أو استعادة مشترك	UPF → الحديقة المسورة	تفعيل/إلغاء تفعيل إعادة التوجيه
تشغيل ping من العنصر نفسه	UPF → التشخيصات	ping من العقدة
إنهاء جلسة مصدقة WiFi	TWAG → الجلسات	فصل جلسة
تفعيل طلب نداء	MSC → النداءات	النداء اليدوي

تتطلب الإجراءات المدمرة (الإطلاق، الحذف، الإلغاء) دائمًا تأكيدًا صريحًا قبل أن تعمل.

تظهر الإجراءات التشغيلية كأزرار بجانب البيانات التي تؤثر عليها: هنا، تفعيل/إلغاء تفعيل إعادة توجيه المشتركين وإدارة عناوين IP المسموح بها. تطلب الإجراءات المدمرة التأكيد أولاً.

عرض التكوين

تحتوي العناصر التي تكشف عن تكوينها في وقت التشغيل على علامة تبويب **التكوين**. تعرض **الخام** للمستند الأساسي **JSON** ذلك في تخطيط منظم وسهل القراءة مع تبديل OmniWeb الكامل.

هناك سلوكان يستحقان المعرفة:

- **تتم مواءمة تنسيقات التكوين المختلطة.** بعض العناصر تعيد تكوينها كقواميس صارم. تقوم JSON بدلاً من (`'key': True`, `None`) على نمط بايثون OmniWeb بتحليل هذه تلقائيًا إلى عرض نظيف وتعود بسلاسة إذا لم تتمكن من تحليل قيمة.
- **يتم إخفاء الأسرار.** أي حقل يبدو حساسًا (يتطابق مع `password`, `secret`, `token`, أو `credential`) يتم عرضه كـ `***` بدلاً من قيمته الحقيقية، سواء في عروض التكوين أو في حقول النموذج.

عرض التكوين العام: الإعدادات في تخطيط منظم، مع تبديل JSON الخام والقيم الحساسة مخفية. تستخدم العناصر التي تكشف عن التكوين (UPF، TAS، ePDG، واجهات SMSC، OCS، RAN

Monitor) جميعها هذا النمط.

السجلات على كل عنصر

تستعلم عن سجلات الخدمة لذلك .Loki كل عنصر لديه علامة تبويب **السجلات** مدعومة من العنصر حسب المضيف/التسمية، تدعم التصفية المنظمة، وتبث الأسطر الجديدة عند وصولها. نظرًا لأن نموذج السجل متطابق عبر العناصر، يتم توثيقه بالكامل في صفحة خاصة به:

➡ **السجلات وتتبع المشتركين**

المنظمة، الملونة، والبث Loki تستخدم علامة تبويب السجلات لكل عنصر نفس العارض: سجلات المباشر مع تصفية الخدمة والشدة.

لوحات المعلومات على كل عنصر

لوحات OmniWeb علامة تبويب **لوحات المعلومات**. تكتشف Grafana تظهر العناصر المميزة لـ المعلومات المطابقة حسب العلام�� وتعرضها في الداخل، بحيث يمكنك رؤية الإحصائيات لعنصر دون مغادرة مساحة عمله. انظر:

➡ **لوحات معلومات Grafana والإحصائيات**

الاستطلاع في الوقت الحقيقي

تقوم الصفحات التشغيلية بالتحديث التلقائي. يظهر **مؤشر الاستطلاع** في رأس كل صفحة:

- **نشط (نقطة خضراء)** أو **مؤجل**.
- **الفترة** (الافتراضي 5 ثوانٍ، يتم تعيينه لكل عنصر عبر `pollIntervalMs`).
- **دوار** أثناء جلب البيانات.
- **الطابع الزمني** لآخر تحديث ناجح.

يمكن تبديل الاستطلاع لكل صفحة. الصفحات المبنية حول الإجراءات التفاعلية أو ذات الاستخدام الواحد (منفذي، التشخيصات، الأجهزة، JSON) لا تقوم بالاستطلاع بشكل افتراضي ويتم تحديثها يدويًا. أوقف الاستطلاع عندما تريد عرضًا ثابتًا أثناء قراءة جدول كبير أو أثناء تقدم تتبع.

الأذونات وما يمكنك تغييره

ما يمكنك *فعله* على عنصر يعتمد على دورك. يتم منح الوصول **لكل نوع عنصر، لكل طريقة HTTP**:

الاستخدام النموذجي	الطرق المسموح بها	الإذن
عرض البيانات، بدون تغييرات	`GET`	قراءة فقط
عرض وتعديل (إضافة مشترك، تحرير مسار)	`GET`, `POST`, `PUT`, `PATCH`	قراءة وكتابة
كل شيء، بما في ذلك الحذف / المسح	`GET`, `POST`, `PUT`, `PATCH`, `DELETE`	كامل

ولكن قراءة فقط UPF تُخصص الأذونات بشكل مستقل لكل عنصر: قد يكون لديك وصول كامل إلى إذا لم يكن الإجراء مسموحًا لدورك، فإن تحكمه غير متاح. يتمتع المسؤولون بوصول HSS. على كامل إلى جميع العناصر. انظر المصادقة والتحكم في الوصول لإدارة الأدوار، ولاحظ أن **كل طلب عبر الوكيل يتم تسجيله في السجل** بغض النظر عن الدور.

عرض متعدد الحالات والأسطول

تشغل العديد من أنواع العناصر كحالات متعددة: عدة UPFs خلف PGW-C، زوج من SMSCs، مع ذلك على مستوى نوع العنصر: النوع الذي يحتوي على أكثر من OmniWeb زائدة. تتعامل STPs حالة واحدة مُعَدّة يحصل على وضعي تنقل.

الشريط الجانبي واختيار الحالة

عندما يحتوي نوع على حالات متعددة، يتوسع إدخال الشريط الجانبي لعرض كل واحدة بالاسم. انقر على حالة مسماة لفتح مساحة عمل تلك الحالة مباشرة. يظهر أيضًا قائمة منسدلة للحالة في رأس مساحة العمل. يتيح لك ذلك التبديل بين الحالات دون العودة إلى الشريط الجانبي، وهو مفيد عند مقارنة السلوك عبر العقد دون فقدان موقعك على علامة تبويب معينة.

محدد الحالة في أعلى يمين رأس مساحة العمل. فتحه يظهر كل حالة مُعَدّة بالإضافة إلى "جميع الحالات" للعودة إلى عرض الأسطول، دون مغادرة علامة التبويب الحالية.

عرض الأسطول

انقر على اسم نوع العنصر في الشريط الجانبي (بدلاً من حالة معينة)، أو اختر **جميع الحالات** من القائمة المنسدلة، لفتح **عرض الأسطول** لذلك النوع. يظهر عرض الأسطول بطاقة ملخص لكل

حالة مع حالة الصحة ومقاييس رئيسية، بحيث يمكنك تقييم الأسطول بالكامل بنظرة واحدة قبل التعمق في عقدة معينة.

عرض أسطول UPF: بطاقة واحدة لكل حالة، جميعها يتم استطلاعها بالتوازي. انقر على أي بطاقة حالة أو استخدم القائمة المنسدلة للتعمق.

متى تستخدم كل عرض

الاستخدام	الحالة
عرض الأسطول: جميع الحالات في لمحة	التحقق من صحة الأسطول العامة
قائمة منسدلة للحالة أو عنصر فرعي في الشريط الجانبي	التحقيق في عقدة معينة
افتح كل منها في القائمة المنسدلة للحالة بالتناوب	مقارنة عدد جلسات UPFs اثنين
انتقل إلى ��لك الحالة، ثم الجلسات	مسح جلسة على UPF معين

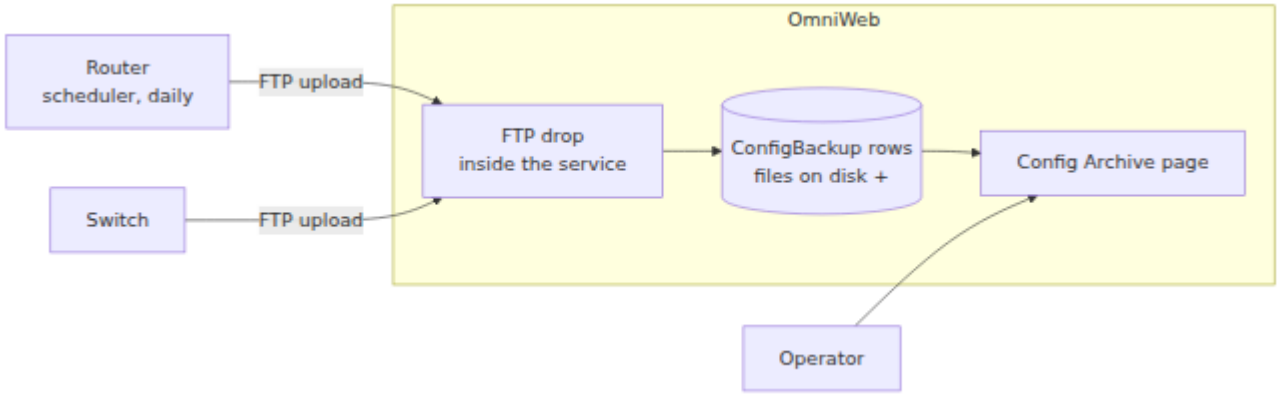
أرشيف التكوين: نسخ احتياطية لتكوين الجهاز

أرشيف التكوين يحتفظ بتكوين كل جهاز شبكة يقوم بتحميل واحد، ويجعل المجموعة قابلة للبحث والترتيب والمقارنة. يقوم جهاز التوجيه بتصدير تكوينه الخاص وفقًا لجدوله الخاص ويدفعه إلى OmniWeb الأخيرة منذ المرة ما وصل، وما بداخله، وما تغير ؛. تعرض الصفحة.

← دليل العمليات

ما هو

لا يمكن لجهاز التوجيه والمفاتيح تشغيل وكيل سجل أو عميل نسخ احتياطي، ولكن يمكنهم جميعًا تحميل ملف. لذا فإن الأرشيف يحول تلك القدرة الوحيدة إلى سجل لكل تكوين تم تشغيله في العقار.



لا توجد عملية جانبية، ولا حزمة إضافية، ولا شيء لتثبيته. **OmniWeb** يعمل السقوط **داخل خدمة** المستمع هو جزء من التطبيق، مكتوب ضد مكتبة بايثون القياسية على المضيف:.

لماذا FTP

يقوم RouterOS `/tool fetch` بتحميل ملف عبر FTP أو SFTP. يمكنه أيضًا إرسال HTTP POST، ولكن الجسم يأتي من متغير RouterOS، وهو، ويحتوي المتغير على 4 كيلوبايت كحد أقصى، وهو وسيلة النقل الوحيدة التي تتحدث بها الأجهزة FTP أقل بكثير من تصدير التكوين. لذلك، يعد OmniWeb و لملف بهذا الحجم.

كلمة المرور والتكوين بنص واضح. قم بتشغيله على شبكة إدارة، وقم بتقييد عناوين FTP يحمل المصدر عند جدار الحماية.

ما الذي يقبله السقوط

الذي يحتاجه الجهاز لتسليم ملف، ويرفض الباقي FTP يطبق المستمع الجزء من.

الإجراء	النتيجة
`STOR` ملف	مقبول، أينما وضعه الجهاز.
`RETR`، `LIST`، `NLST`، `MLSD`	مرفوض. السقوط للكتابة فقط: لا يمكن قراءة أي شيء منه عبر FTP.
`DELE`، `RMD`، `RNFR`، `RNTO`	مرفوض. يمكن للجهاز إضافة نسخة احتياطية ولا يمكنه أبدًا إزالة أو إعادة تسمية واحدة.
`CWD` إلى دليل غير موجود	مقبول. الشجرة افتراضية، ويصبح المسار اسم الجهاز.
`MKD`	مقبول، ولا ينشئ شيئًا. يتم استنتاج الدلائل من التحميلات.
`..` مسار يحتوي على	يتم تطبيعه قبل أن يلمس أي شيء القرص. يتم تحميله داخل الأرشيف.
تحميل يتجاوز حد الحجم	مرفوض بـ `552`، ولا يتم كتابة أي شيء.

يتم دعم كلا نوعي الملفات، ويعامل الأرشيفهما بشكل مختلف:

- **نص**، مثل `/export` من RouterOS (`.rsc`)، أو أي `.txt`، `.conf` أو `.cfg`. يتم فهرسة النص، بحيث يمكن البحث عنه ومقارنته.
- **ثنائي**، مثل `/system backup` من RouterOS. يتم الاحتفاظ بالملف بايتًا بايتًا لاستعادته، ويتم تمييزه كملف ثنائي في القائمة.

الهوية: العنوان، وليس الاسم

عنوان المصدر هو الهوية. كل شيء يعتمد على العنوان الذي جاءت منه البايتات بالفعل: أي سلسلة ينضم إليها التحميل، مع ما يتم مقارنته، وعدد الاحتفاظ به. هذا هو TCP، لذا لا يمكن للمرسل تزوير العنوان دون الاحتفاظ به: يجب أن يكتمل المصافحة.

العنصر الأول `dst-path=<identity>/<file>` يعطي RouterOS **الاسم هو مجرد ادعاء.** يمكن لأي `edge-rtr09`. `edge-rtr09-20260910.rsc` من المسار، ويعطي اسم بسيط مثل مرسل الادعاء بأي اسم، لذا يخزن الأرشيفه، ويعرضه ويبحث عنه، ولا يعتمد على أي شيء منه.

هذا هو ما يجعل السقوط المفتوح آمنًا للتشغيل:

ماذا يحدث	شخص ما يقوم بالتحميل
ينضم إلى سلسلة ذلك الجهاز، كنسخة احتياطية التالية له.	من عنوان جهاز التوجيه الخاص
يبدأ سلسلته الخاصة بجانب السلسل�ة الحقيقية. لا يمكنه تزوير تغيير على جهاز التوجيه الحقيقي، ولا يمكنه إغراق تاريخ جهاز التوجيه الحقيقي حتى يتقدم الاحتفاظ بالنسخ الاحتياطية الأصلية.	من عنوان مختلف، يدعي اسم جهاز التوجيه
لذا فإن مرسل Slack، سلسلة جديدة، تم الإعلان عنها مرة واحدة في غير متوقع يكون مرئيًا بدلاً من أن يكون صامتًا.	من عنوان جديد

تبدأ علامة المصدر كأي شيء تسميه التحميلات الخاصة به، وهو أمر ملائم وغير موثوق. قم بتثبيت اسم صحيح على المصدر لإيقاف التحميلات عن تحريكه.

تكلفة هذا النموذج: جهاز يغير عنوانه بالفعل يبدأ سلسلة جديدة، لذا ينفصل تاريخه. قم بتثبيت علامات على كلاهما، أو اعتبر السلسلة القديمة مغلقة.

التكوين

لا يوجد شيء لتكوينه. يعمل السقوط على المنفذ 2121، مفتوح، بمجرد بدء OmniWeb. وجه جهازًا نحوه وسيقوم بتحميله.

ذلك بوضوح، FTP هذا مقصود، وليس اختصارًا. كلمة المرور ليست ما يحمي الأرشيف: يرسل ويحتفظ أجهزة التوجيه بها في التكوينات التي يقومون بتحميلها، لذا فإن أي شخص يمكنه قراءة الأرشيف أو التنصت على شبكة الإدارة لديه بالفعل. ما يحمي الأرشيف هو أن المرسل يكتب فقط يحتفظ به حقًا. جدار الحماية هو TCP في السلسلة الخاصة بالعنوان الذي يحتفظ به، والذي يجعل التحكم الذي يهم؛ قم بتقييد المنفذ لأجهزتك.

قم بتعيين كلمة مرور للمطالبة بواحدة بالإضافة إلى فحص العنوان، أو للحفاظ على صفحة الأرشيف بدون مستمع على الإطلاق. `OMNIWEB_CONFIG_ARCHIVE_FTP=0` بقية الجدول موجودة للموقع غير المعتاد، وكل قيمة أدناه هي قيمة افتراضية معقولة لا تحتاج إلى إعداد.

متغير البيئة	الافتراضي	صف
OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD	(فارغ)	م بتعيين واحدة لمطالبة مة مرور افة إلى العنوان. فارغ هو الطريقة العادية للتشغيل
OMNIWEB_CONFIG_ARCHIVE_FTP_OPEN	1	قبول تحميلات ون كلمة رور. قم ين 0 **و** مة مرور لمطالبة بواحدة.
OMNIWEB_CONFIG_ARCHIVE_FTP_USER	devbackup	اسم ستخدم ي تصادق الأجهزة
OMNIWEB_CONFIG_ARCHIVE_FTP_PORT	2121	التحكم. خدم 21 إذا كانت ة يمكن ن ترتبط فذ مميز
OMNIWEB_CONFIG_ARCHIVE_FTP_HOST	0.0.0.0	العنوان اع عليه

متغير البيئة	الافتراضي	صف
OMNIWEB_CONFIG_ARCHIVE_PASV_MIN	40000	ول منفذ ب سلبية. فتح هذه نطاقات للأجهزة.
OMNIWEB_CONFIG_ARCHIVE_PASV_MAX	40100	خر منفذ ت سلبية
OMNIWEB_CONFIG_ARCHIVE_ROOT	backend/data/config-archive	حيث يتم لاحتفاظ لملفات، احد لكل جهاز.
OMNIWEB_CONFIG_ARCHIVE_MAX_BYTES	33554432	م رفض ل الأكبر من هذا.
OMNIWEB_CONFIG_ARCHIVE_MAX_TEXT_BYTES	4194304	حتى هذا حجم يتم فهرسته للبحث رنة. يتم لاحتفاظ س الأكبر القرص فقط.
OMNIWEB_CONFIG_ARCHIVE_RETENTION_DAYS	365	تم إزالة النسخة طية بعد ذا العمر

متغير البيئة	الافتراضي	صف
OMNIWEB_CONFIG_ARCHIVE_KEEP_MINIMUM	10	ث النسخ طية لكل هاز التي هما كان .عمرها
OMNIWEB_CONFIG_ARCHIVE_FTP	1	ينها إلى للحفاظ ى صفحة ف ولكن لا تفتح تمع أبدًا
OMNIWEB_CONFIG_ARCHIVE_TIMEOUT	120	قبل أن إسقاط ى التحكم نشط أو متوقف
OMNIWEB_CONFIG_ARCHIVE_RETRY_SECONDS	20	ة يحاول مل فقد يط مرة . هذا هو ا كم من ت يمكن ن يكون وط غير خدم بعد دة تدوير مل الذي تفظ به
OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK	(فارغ)	Sl رابط . الفارغ ني عدم

متغير البيئة	الافتراضي	صف
		وجود شعارات
`OMNIWEB_PUBLIC_URL`	(فارغ)	ا عنوان عام لهذا OmniW م لربط S رسالة ودة إلى لأرشيف
`OMNIWEB_CONFIG_ARCHIVE_MAX_DIFF_BYTES`	`262144`	ر اختلاف زن. يتم يم تغيير كبر على الصف.
`OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN`	(فارغ)	ر حاملي ب على Prome ه لجمع قاييس. غ يتركها مفتوحة.

ويبدأ كل عامل السقوط. يفوز واحد فقط بالربط ويخدم؛ gunicorn، عدة عمال OmniWeb تشغل الآخرون يقفون على أهبة الاستعداد ويحاولون مرة أخرى، لذا يبقى المستمع على قيد الحياة بعد في طلب `false` لكل عملية، لذا فإن `listening_here` إعادة تدوير عامل. تبلغ الصفحة عن واحد ليس خطأ.

Slackتتبع التغييرات و

يتم مقارنة كل تحميل مع التحميل السابق **من نفس المصدر**، من نفس النوع، عند وصوله. نفس النوع يعني نفس الامتداد، لذا فإن الجهاز الذي يرسل تصدير نصي ونسخة احتياطية ثنائية كل ليلة يقارن كل منهما مع سابقتها بدلاً من التناوب بينهما واعتبار كل شيء تغييرًا. تعني البايتات المتطابقة

عدم وجود تغيير، بغض النظر عن الملف. تنتج البايتات المختلفة في ملف نصي اختلافًا موحدًا وعدد الأسطر، يتم تخزين كلاهما على الصف، لذا لا تعيد الصفحة والإشعار حسابهما أبدًا. يتم تسجيل ملف ثنائي يختلف على أنه تغير بدون اختلاف، لأنه لا يوجد شيء قابل للقراءة لعرضه.

ما لا يعتبر تغييرًا

يختم الجهاز تصديره بالوقت الذي تم تشغيله فيه. يفتح RouterOS كل `/export` مع

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

لذا فإن تصديرين لجهاز توجيه غير متأثر يختلفان بتلك السطر ولا شيء آخر، ويكتب الملف تحت اسم جديد في كل تشغيل. بالمقارنة بشكل خام، سيبلغ كل جهاز عن تغيير كل ليلة، ويرسله إلى Slack، ويخفي الإشارة الوحيدة التي تستحق الحصول عليها تحت إيجابية زائفة يومية لكل جهاز.

لذا تتم إزالة هذه الأسطر قبل مقارنة أي شيء، وفقط للمقارنة: يحتفظ الملف المخزن والنص القابل للبحث بما أرسله الجهاز بالضبط.

تم تجاهله	لماذا
`# <date> <time> by RouterOS <version>`	رأس تصدير RouterOS. يكتب `2026-09-10 11:39:35` (تاريخ ISO 7 RouterOS)، بينما يكتب RouterOS 6 `sep/10/2026` ؛ يتطابق النمط مع الشكل الذي يشاركونه بدلاً من أي منهما.
`# software id = ...`	موجود في بعض تصديرات RouterOS.
`! Last configuration change at ...`	يتغير عند كتابة أي شيء، بما في ذلك بواسطة Cisco IOS. الجهاز.
`! NVRAM config last updated at ...`	Cisco IOS.
`ntp clock-period ...`	ينحرف بمفرده، دون تدخل من المشغل Cisco IOS.

اسم الملف ليس جزءًا من المقارنة على الإطلاق: يتم مطابقة تحميل مع التحميل السابق من نفس المصدر بنفس الامتداد، لذا فإن اسمًا يحتوي على طابع زمني لا يغير شيئًا.

قم بتعيين `OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS` إلى قائمة من التعبيرات العادية مفصولة بـ `|||` لاستبدال هذه القائمة لبائع يقوم بختم شيء آخر.

بعد تغيير الأنماط، أعد تجزئة الأرشيف. كل نسخة احتياطية تخزن تجزئة تكوينها العادي، لذا فإن نمطًا جديدًا يترك كل تجزئة مخزنة غير صالحة: لن يتطابق التحميل التالي من كل جهاز مع تاريخه الخاص، مما يخزن ملفًا مكررًا ويبلغ عن تغيير لم يحدث أبدًا.

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

تدفع تلك المقارنة شيئان:

- عندما يتحرك التكوين، أو علامة عندما يرسل الجهاز `+N/-N` **الصفحة.** يظهر كل صف نفس الملف مرة أخرى. **التغييرات فقط** تضيق القائمة إلى التحميلات التي غيرت شيئًا بالفعل.
- **Slack.** يتم نشر تغيير إلى رابط وارد، مع المصدر، وعدد الأسطر، وأول 40 سطرًا من الاختلاف ورابط للعودة إلى الأرشيف. يتم نشر عنوان تم سماعه لأول مرة مرة واحدة أيضًا، مع ذكر العنوان أولاً وما يدعي أنه ثانياً.

لا ينشر النسخ الاحتياطية الليلية غير المتغيرة شيئًا. ستملأ العقار الذي يقوم بعمل نسخ احتياطية كل ليلة قناة بـ "لم يحدث شيء"، وسيمتنع الجميع عن ذلك. ما يصل بدلاً من ذلك هو فقط ما يرغب المشغل في أن يتوقف من أجله.

```
*core-rtr01 (10.64.10.1)* (1-/3+) تم تغيير التكوين
`core-rtr01-2026-09-10-0215.rsc` 02:15 10-09-2026 تم استلامه في
02:15 09-09-2026 :النسخة الاحتياطية السابقة
```

تليها الاختلاف، ورابط إلى الأرشيف.

قم بتعيين `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK` إلى رابط Slack الوارد لتفعيل ذلك، مع عدم تعيين أي OmniWeb. لجعل الرسالة ترتبط بالعودة إلى هذا `OMNIWEB_PUBLIC_URL` و رابط، لا يزال الأرشيف يتتبع التغييرات وتظهر الصفحة ذلك؛ لا يتم نشر أي شيء.

تكون عملية POST بطيئة أو غير قابلة Slack سريعة وتنسى في خيط خلفي، لذا لا يمكن أن تؤخر للوصول تحميلًا أو تفقد نسخة احتياطية.

تسجيل الوصول والمقاييس

حقيقتان، وتحتاج المراقبة إلى كليهما:

ماذا يعني الصمت	الحقل	الحقيقة
خطأ. توقف الجهاز أو جدوله أو المسار هنا عن العمل.	يتم رفعه في **كل** `last_upload_at`، تحميل، سواء كان متغيرًا أم لا	سمعنا منه
لا شيء. الجهاز الذي لا يتغير تكوينه هو جهاز صحي.	يتم رفعه فقط عند `last_change_at`، حدوث تغيير	تحرك تكوينه

قم بتنبيه على الأول وليس الثاني، أو جهاز توجيه مستقر يرسل لك رسالة كل ليلة.

على المصدر بدلاً من أن يتم عدها من (`upload_count`، `change_count`) تعيش العدادات الصفوف، لذا فإن الاحتفاظ بالنسخ الاحتياطية القديمة لا يمكن أن يجعلها تسقط. يتم ملء الأرشيف الذي يسبق هذه الحقول من النسخ الاحتياطية التي يحتفظ بها بالفعل عندما تعمل الهجرة.

جمع البيانات

`GET /api/config-archive/metrics` يعيد عرض نص Prometheus. إنها نقطة نهاية بسيطة بدون اعتماد، ولا تستخدم الجلسة: قم بتعيين `OMNIWEB_CONFIG_ARCHIVE_METRICS_TOKEN` ويقدمه Prometheus كحامل. تركه فارغًا يتركه مفتوحًا، ويعرض العرض أسماء الأجهزة والعناوين، لذا قم بتعيينه على أي شيء يمكن الوصول إليه.

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

المقياس	النوع	الوصف
`config_archive_last_upload_timestamp_seconds`	Gauge	آخر تحميل من هذا المصدر، سواء كان متغيرًا أم لا. **هذا هو الذي يجب التنبيه عليه.** `0` عندما لم يتم تحميله أبدًا، لذا فإن نفس التنبيه يلتقط جهازًا لم يبدأ أبدًا.
`config_archive_last_change_timestamp_seconds`	Gauge	آخر تحميل يختلف تكوينه. `0` عندما لم يتغير أبدًا.
`config_archive_uploads_total`	Counter	التحميلات المستلمة منذ أن تم رؤية المصدر لأول مرة. لا يقلل الاحتفاظ منها.
`config_archive_changes_total`	Counter	التحميلات التي غيرت التكوين.
`config_archive_retained_backups`	Gauge	النسخ الاحتياطية المحتفظ بها بعد الاحتفاظ.

المقياس	النوع	الوصف
`config_archive_retained_bytes`	Gauge	البايتات المحتفظ بها بعد الاحتفاظ.
`config_archive_sources`	Gauge	المصادر التي سمعها الأرشيف على الإطلاق.
`config_archive_ftp_enabled`	Gauge	ما إ��ا كان السقوط مُعدًا للتشغيل.
`config_archive_ftp_bound`	Gauge	ما إذا كان مقبس السقوط يقبل الاتصالات على المضيف. **قم بالتنبيه على هذا.** يمكن لأي عامل الإجابة عليه، لأنه يتم قياسه مع اتصال محلي.
`config_archive_ftp_listening_here`	Gauge	ما إذا كان العامل الذي أجاب على هذا الجمع هو الذي يحمل المقبس. للتصحيح فقط: يجلب الجمع عبر

الوصف	النوع	المقياس
على nginx عامل عشوائي من المجموعة، لذا فإن هذه هي رمية عملة. لا تنبه على ذلك أبدًا.		

اسم العرض، الذي هو فقط ما تدعيه (`label`) و(العنوان، الهوية) `source` تحمل كل سلسلة التحميلات حتى يثبته المشغل).

التنبيهات التي تستحق الحصول عليها

```
# توقف جهاز عن القيام بالنسخ الاحتياطي، أو لم يبدأ أبدًا. جدول يومي
بالإضافة إلى Slack.
(time() - config_archive_last_upload_timestamp_seconds) > 172800

# لا أحد يخدم السقوط.
config_archive_ftp_bound == 0 and config_archive_ftp_enabled == 1

# جهاز يتغير فجأة في كل تشغيل، مما يعني عادة أن تصديره
# يحمل طابع زمني بدلاً من أن يقوم أي شخص بتحريره.
increase(config_archive_changes_total[1d]) > 3
```

الاحتفاظ

يعمل الاحتفاظ **لكل مصدر**، وهو النقطة: لا يمكن لمرسل واحد يملأ سلسلته الخاصة أن يتجاوز نسخ احتياطية لمرسل آخر. يتم إزالة النسخة الاحتياطية التي تزيد عن نافذة الاحتفاظ، باستثناء أن أحدث القليل من كل مصدر تبقى دائمًا. لذا يحتفظ الجهاز الذي يتوقف عن التحميل بتكوينه الأخير المعروف الجيد إلى الأبد، ولا يفرغ عمره وحده تاريخ الجهاز.

تشارك التحميلات من نفس **التكوين** ملفًا واحدًا على القرص، مقارنة بنفس الطريقة التي يتم بها مقارنة التغييرات: مع إزالة طابع التصدير الخاص بها والأسطر المتقلبة الأخرى. هذا الأمر أكثر أهمية بختم الوقت الذي تم تشغيله في سطره الأول، لذا تختلف RouterOS مما يبدو. يقوم تصدير

البايتات الخام في كل ليلة؛ سيؤدي الاعتماد على التخزين منها ��لى كتابة نسخة جديدة من تكوين جهاز توجيه غير متأثر كل ليلة إلى الأبد.

لذا، فإن جهاز التوجيه الذي يقوم بتحميل تكوين غير متغير كل ليلة يحصل على صف كل ليلة، وهو ما يجعل "سمعنا منه" مرئيًا، بينما يتم تخزين البايتات مرة واحدة.

تكوين MikroTik

أمران، يتم تشغيلهما على جهاز التوجيه. قم بتعيين `<omniweb-host>` إلى عنوان OmniWeb الخاص بك. لا حاجة لكلمة مرور، ويتم تجاهل بيانات الاعتماد أدناه: يحدد السقوط جهازًا بواسطة العنوان الذي يقوم بالتحميل منه.

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

/system scheduler add name=config-backup interval=1d start-
time=02:15:00 on-event="/system script run config-backup"
policy=read,write,ftp,test comment="Nightly config export to
OmniWeb Config Archive"
```

قم بتشغيله مرة واحدة يدويًا لإثبات المسار قبل الوثوق بالجدول:

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

مع حجم التحميل، ويظهر الجهاز في `status: finished` تشير عملية تشغيل ناجحة إلى الأرشيف خلال ثوانٍ.

لماذا تم كتابته بهذه الطريقة

السبب	التفاصيل
يرفض CLI الخاص بـ RouterOS الاستمرار باستخدام الشرطة المائلة عند وصول أمر عبر SSH. يتم لصق نص مكتوب عبر عدة أسطر بشكل جيد في الطرفية ويفشل من الأتمتة، مع خطأ بسيط `syntax error (line 1 column N)`.	النص الكامل هو **سطر واحد**
بدونها، تفشل `test` و`ftp` إلى `fetch` يحتاج `policy=read,write,ftp,test` العملية بخطأ في السياسة ولا يتم تحميل أي شيء.	
المنفذ `/tool fetch` الافتراضي للسقوط. يأخذ بشكل منفصل عن العنوان.	`port=2121`
عناصر نائبة. يقبل السقوط أي بيانات اعتماد، لأن يريد وجود `fetch` عنوان المصدر هو الهوية. لا يزال المعاملات.	`user=omniweb password=x`
معرفًا داخليًا، وليس اسمًا. `/file remove` تأخذ تمرير الاسم مباشرة يفشل ويترك التصدير على جهاز التوجيه، مما يملأ تخزينه بمرور الوقت.	`[find name=...]` في `/file remove`
يكتب التصدير بشكل غير متزامن. يمكن أن يؤدي التحميل الفوري إلى التقاط ملف جزئي.	`/export` بعد `:delay 5s`
بعرض التاريخ كـ `2026-09-` يقوم RouterOS 7 `10`، لذا يتم فرز الملف بشكل طبيعي. يتغير الاسم في كل تشغيل وهذا جيد: يتطابق الأرشيف مع التحميل ضد السابق من نفس المصدر، وليس بواسطة اسم الملف.	في اسم الملف `$d`

قم بتوزيع `start-time` عبر أجهزة التوجيه حتى لا يقوموا جميعًا بالتحميل مرة واحدة.

وقم `/system backup save name=$base` للحفاظ على نسخة احتياطية ثنائية أيضًا، أضف بنفس الطريقة. التصدير النصي هو الذي يتم مقارنته؛ النسخة الثنائية هي `$base.backup` بتحميل

التي يتم استعادتها على الأجهزة المماثلة.

يعمل بنفس الطريقة: وجهه إلى المضيف والمنفذ ودعه يسمي FTP أي جهاز يمكنه التحميل عبر ملفه الخاص.

استخدام الصفحة

موجود في الشريط الجانبي، تحت قائمة المضيف **أرشيف التكوين**.

التحكم	ماذا يفعل
لافتة صامتة	تسمي كل مصدر لم يقم بالتحميل لمدة 48 ساعة، مع كم من الوقت مضى. هذا هو تسجيل الوصول، لذا يتم تشغيله لجهاز يرسل نسخ احتياطية غير متغيرة فقط إذا توقف عن إرسالها.
المصدر	تصفية إلى عنوان مصدر واحد. يظهر كل إدخال متى دفع آخر مرة، ويشير إلى واحد صامت.
الاسم أو العنوان أو الملف	بحث عن جزء من الاسم المدعى، وعلامة المصدر، والعنوان واسم الملف.
نص داخل التكوين	ابحث في التكوينات نفسها، على سبيل المثال عنوان IP، `ospf`، أو اسم مستخدم. هذه هي أسرع طريقة للعثور على الأجه��ة التي تحمل إعدادًا.
رؤوس الأعمدة	ترتيب حسب الجهاز، الملف، وقت الاستلام أو الحجم.
تغييرات فقط	تضييق القائمة إلى التحميلات التي غيرت التكوين، مخفية النسخ الليلية غير المتغيرة.
عمود التغيير	`+N/-N` عندما يتحرك التكوين، علامة عندما يعيد الجهاز إرسال نفس الملف.
صف	يفتح التكوين، مع اختلاف ضد النسخة الاحتياطية السابقة لذلك الجهاز.
تحميل	الملف تمامًا كما أرسله الجهاز.
إضافة ملف	تحميل تكوين يدويًا، لجهاز لا يمكنه الدفع.

The diff هو الجزء الذي يكسب قوته: يجيب على "ما الذي تغير في هذا الموجه، ومتى" دون الحاجة إلى تسجيل دخول الجهاز.

API

جميع نقاط النهاية تحتاج إلى جلسة مصادق عليها.

الطريقة والمسار	الوصف
`GET /api/config-archive/backups`	قائمة، مع `source`، `address`، `q`، `content`، `changed`، `ordering`، `limit` و `offset`.
`POST /api/config-archive/backups`	إضافة نسخة احتياطية يدويًا: multipart `file`، `device` اختياري.
`GET /api/config-archive/backups/<id>`	نسخة احتياطية واحدة، مع نصها.
`GET /api/config-archive/backups/<id>/download`	الملف المخزن.
`GET /api/config-archive/backups/<id>/diff`	فرق موحد مقابل النسخة الاحتياطية السابقة، أو `?against=<id>`.
`GET /api/config-archive/sources`	صف واحد لكل عنوان مصدر: عدد النسخ الاحتياطية، التغييرات، أحدث تحميل، الحجم، وكل اسم ادعت تحميلاته.
`PATCH /api/config-archive/sources/<id>/label`	تثبيت اسم صحيح على مصدر، بحيث تتوقف التحميلات عن تحريكه.
`GET /api/config-archive/status`	حالة السقوط وإجمالي الأرشيف.
`GET /api/config-archive/metrics`	عرض نصي لـ Prometheus. انظر Check-in and metrics.

`changed=1` يعيد تغذية التغييرات: التحميلات التي تختلف عن النسخة الاحتياطية السابقة للجهاز.

`ordering` يقبل `received_at`، `claimed_name`، `filename` و `size_bytes`، في `-` مع البداية لعكس الترتيب. أي قيمة أخرى تعود إلى الأحدث أولاً.

استكشاف الأخطاء وإصلاحها

العرض	تحقق
الصفحة تحذر من أن السقوط غير مفعل	`OMNIWEB_CONFIG_ARCHIVE_FTP_PASSWORD` غير محدد. قم بتعيينه وأعد تشغيل OmniWeb.
الجهاز يبلغ عن فشل تسجيل الدخول	`config archive` تأكد من اسم المستخدم وكلمة المرور، ثم ابحث عن `ftp: login failed` في سجل OmniWeb.
النقل يبدأ ويتوقف	النطاق السلبي غير قابل للوصول. افتح `OMNIWEB_CONFIG_ARCHIVE_PASV_MIN` إلى `..._MAX` من الجهاز.
التحميلات تصل باسم غريب مدعى	أرسل الجهاز اسم ملف عاري لا يبدأ بهويته. قم بتعيين `dst-path` إلى `<identity>/<file>`، أو قم بتثبيت تسمية على المصدر.
يظهر جهاز واحد كمصدرين	تغير عنوانه، لذا بدأ سلسلة جديدة. قم بتثبيت تسميات على كلاهما لجعل العلاقة واضحة.
يظهر عنوان غير متوقع	يمكن لشخص ما أو شيء آخر الوصول إلى المنفذ. تحقق من رسالة Slack "الآن يتم النسخ الاحتياطي" لمعرفة متى بدأ، وقيّد المنفذ.
جهاز مفقود من القائمة	لم يكمل أبداً تحميل. قم بتشغيل البرنامج النصي يدويًا على الجهاز وراقب سجله.
لا شيء يصل إلى Slack	تأكد من تعيين `OMNIWEB_CONFIG_ARCHIVE_SLACK_WEBHOOK`، ثم تحقق مما إذا كانت التحميلات هي تغييرات: النسخة الاحتياطية غير المتغيرة صامتة عن عمد. يتم تسجيل الفشل كـ `Slack post failed`.
ينشر Slack في كل نسخة	يقوم الجهاز بختم شيء ما في كل تصدير غير مشمول في قائمة التجاهل. قارن بين نسختين احتياطيتين لمعرفة ما يتحرك، ثم أضف نمطًا إلى

العرض	تحقق
احتياطية	`OMNIWEB_CONFIG_ARCHIVE_VOLATILE_PATTERNS`.

DRA: وكيل توجيه القطر

DRA هو محور توجيه القطر في النواة. بدلاً من أن يحتفظ كل عقدة بشبكة كاملة من اتصالات القطر، تتصل وظائف IMS و EPC بـ DRA، وهو يقوم بإعادة توجيه وإرسال إشاراتهم: **S6a** بين MME و HSS، **Gx/Gy** إلى PCF/PCRF و OCS، **Cx/Dx** و **Sh** لـ IMS، وهكذا. يختار المكان الذي تذهب إليه كل رسالة من **قواعد التوجيه** (AVP المطابقة على تطبيق القطر، المجال أو وخوارزمية اختيار النظير، ويمكنه إعادة كتابة الرسائل باستخدام **قواعد التحويل**. إنه النظير القطر الوحيد الذي يمكن الوصول إليها من نفس Grafana عرض مخططات الإنتاجية والاتجاهات على لوحات الصفحة.

← دليل العمليات

هو صفحة عنصر لكل مثيل DRA في مخزون الموقع، مع عرض أسطول (خريطة الشبكة) حيث تم نشر عدة منها. تمر جميع الحركة المرورية عبر DRA، لذا تبقى خلف البوابة، إلى واجهة برمجة التطبيقات الخاصة بـ OmniWeb وكيل خلفية المعتمدة الوحيدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. يتم تنظيمها في علامات تبويب.

خريطة الشبكة

وكل نظير قطر يعرفه، مع عدد الاتصالات في لمحة (على سبيل المثال DRA عرض محور وسبوك لـ باللون الأخضر. يتم عرض نظير **معطل** أو DRA *5/6 متصل*). يتم ربط النظراء المتصلين بـ **منفصل** إدارياً باللون الرمادي وبخط متقطع. إنها أسرع طريقة ��رؤية، في صورة واحدة، أي جيران الإشارات متاحون.

الحالة

تقرير علامة **الحالة** عن هوية DRA الخاصة به وتكوينه: **Origin-Host**، **المجال**، **IP والمنفذ للاستماع** (عادةً ما يكون القطر 3868)، **اسم المنتج** المبلغ عنه، و **خوارزمية اختيار النظير** المستخدمة (على سبيل المثال، جولة دائرية). هنا تؤكد أن DRA يعمل ومكون كما هو متوقع.

النظراء

كل نظير قطر، كل صف يظهر **Origin-Host** للنظير، **النقل IP** المبلغ عنه، **المنتج والمنفذ**، **تطبيقات القطر** المتفاوض عليها، و **حالة الاتصال** الخاصة به. يمكن (TCP أو SCTP)، **المجال**، تصفية النظراء حسب الاسم، التطبيق، المجال أو الحالة. لكل نظير زر **تفعيل/تعطيل**. تعطيل نظير إدارياً يخرجه من التوجيه دون تفكيك تكوينه، وهذه هي الطريقة ��لتي تقوم بها بتفريغ جار للصيانة.

القواعد

قواعد التوجيه النشطة و **قواعد التحويل**، و **خوارزمية التوجيه** التي تعمل تحتها. تتطابق كل قاعدة توجيه على مرشح (أو كل الحركة المرورية، AVP، تطبيق قطر) وتحل إلى وجهة: إما مجموعة صريحة من النظراء أو استراتيجية مسماة مثل *destination-host* أو *destination-realm*. هنا تؤكد، على سبيل المثال، أن S6a يتم توجيهه إلى HSS و Gx إلى PCF.

السجلات

تقوم علامة DRA بعرض سجل **السجلات** الحي لمساعدتك في استكشاف الأخطاء وإصلاحها لوكيل OmniWeb. توجيه واحد دون مغادرة

لوحات المراقبة

يتم تقديم معدلات الرسائل، والإنتاجية لكل واجهة، وسلاسل زمنية أخرى لـ DRA كلوحات Grafana، لا تقوم بتكرار تلك المخططات OmniWeb يمكن الوصول إليها من صفحة العنصر. بشكل أصلي.

ذات صلة

- **MME** و **HSS**: يقوم DRA بإعادة توجيه **S6a** بينهما.
- **PCF/PCRF** (**Gx**) و **OCS** (**Gy**): نظراء السياسة والرسوم التي يتم توجيهها عبر DRA.
- **CSCF** و **HSS**: إشارات **Cx/Dx** IMS.
- **STP**: النظير القطر لـ DRA في مستوى الإشارات.

OmniSEP: خادم الحقوق

خادم الحقوق (**OmniSEP**) يقرر الخدمات التي يُسمح للمشترك وجهازه باستخدامها. عندما يسأل الهاتف المحمول عما إذا كان يمكنه تشغيل **Wi-Fi Calling**، أو **VoLTE** أو **VoWiFi**، يقوم **ODSA** بتشغيل لتوفير الجهاز لإضافة أو تفعيل جهاز، فإنه يتحقق من خادم الحقوق. يقوم الخادم بتفويض الطلب عبر واجهة **الحقوق (TS.43)**، ويحلل بيانات المشترك عبر **Diameter**، حقوقها الحية، OmniWeb الخاصة بالمشترك. تعرض ويطبق ملفات تعريف خدمة **XCAP** على صفحة عنصر XCAP وملفات تعريف Diameter والنشاط، والجلسات، والرموز، ونظراء التي يمكن الوصول إليها من نفس Grafana واحدة؛ وتعيش مخططات الحجم والاتجاه على لوحات الصفحة.

← دليل العمليات

يعد OmniSEP صفحة عنصر لكل مثيل يتم الوصول إليها من الشريط الجانبي عند تشغيله في إلى واجهة برمجة تطبيقات OmniWeb مخزون الموقع. تمر جميع حركة المرور عبر وكيل خلفية خادم الحقوق، لذا تبقى خلف بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

تعد علامة التبويب الرئيسية قراءة صحية على شاشة واحدة لخادم الحقوق: **حالة النظام**، عدد **الجلسات** و**الرموز** النشطة، المشتركين الذين يحملون **حقوق مخصصة**، وصحة نظراء **Diameter**. إنها أسرع طريقة لتأكيد أن الخادم يعمل ويقوم بتفويض الأجهزة.

الحقوق

المشتركون الذين يحملون **حقوق مخصصة**: تعديلات على مجموعة الخدمات الافتراضية، لكل مشترك. افتح مشتركًا لرؤية الخدمات المفعلة لهم. يمكن لمشغل الشبكة **حذف جميع الحقوق** لمشترك لإعادته إلى الإعداد الافتراضي للشبكة. هذا مفيد لمسح تعديل خاطئ أثناء حدوث عطل.

النشاط

سجلات **النشاط** الأخيرة: تغذية لطلبات الحقوق التي تعامل معها الخادم، كل منها يظهر المشترك أو الجهاز، الخدمة المطلوبة والنتيجة. افتح سجلًا للحصول على تفاصيله. هذه هي مسار التدقيق لتأكيد ما إذا كان الهاتف المحمول قد طلب فعلاً VoWiFi/VoLTE وما هي الإجابة التي تم إعطاؤها.

الجلسات

النشطة التي يحتفظ بها الخا��م لمصادقة الجهاز، كل منها مع هوية **EAP-AKA جلسات** المشترك وحالته. يمكن **إنهاء** جلسة فردية من هنا لإجبار الجهاز على إعادة المصادقة. هذه هي أسرع طريقة لمسح جلسة عالقة.

الرموز

رموز المصادقة النشطة التي أصدرها الخادم للأجهزة بعد مصادقتها. يمكن **إلغاء** كل رمز بشكل فردي، مما يسحب تفويض الجهاز ويتطلب منه المصادقة مرة أخرى. هذا هو ما يعادل الحقوق لإجبار إعادة تسجيل الدخول.

Diameter

نظراء Diameter لكل **حالة الاتصال** مع، المشترك لبيانات الحقوق خادم بهم يتصل الذين نظير. عندما تبدأ قرارات الحقوق في الفشل لأسباب تبدو مثل بيانات المشترك المفقودة، هذه علامة التبويب هي المكان الذي تؤكد فيه أن مسار Diameter يعمل.

ملفات تعريف XCAP

ملفات تعريف XCAP: إعدادات الخدمة لكل مشترك (مثل تكوين الخدمة الإضافية) التي يطبقها خادم الحقوق. افتح ملف تعريف لقراءته. يمكن **حذف** ملف تعريف لمسح إعدادات المشترك المخزنة والعودة إلى الإعداد الافتراضي.

السجلات

تقوم علامة تبويب **السجلات** بتتبع مخرجات سجل خادم الحقوق الحية لاستكشاف الأخطاء وإصلاحها لخادم واحد دون مغادرة OmniWeb.

لوحات المراقبة

تُعرض معدلات الطلب، وعدد الخدمات، وسلاسل زمنية أخرى لخادم الحقوق كلوحات Grafana، بتكرار تلك المخططات بشكل OmniWeb التي يمكن الوصول إليها من صفحة العنصر. لا تقوم أصلي.

ذات صلة

- يحتفظ **HSS** ببيانات المشترك التي تحل طلبات Diameter الخاصة بخادم الحقوق.
- يقدم **CSCF** و**TAS** خدمات VoLTE/VoWiFi التي يفوضها خادم الحقو��.
- يحمل **ePDG** و**TWAG** الوصول إلى Wi-Fi Calling الذي يمكّنه خادم الحقوق.
- يقوم **DRA** بنقل إشارات Diameter الخاصة بخادم الحقوق إلى نظرائه.

ePDG: بوابة بيانات الحزمة المتطورة

تُعتبر **ePDG** **الوصول إلى** البوابة الآمنة لـ **Wi-Fi** العقدة وراء مكالمات Wi-Fi **غير الموثوق**: عبر ePDG إلى IPsec/IKEv2 وبيانات WLAN غير الموثوقة. يقوم الهاتف بإنشاء نفق (VoWiFi) Diameter عبر AAA/HSS بمصادقة المشترك ضد ePDG أي اتصال بالإنترنت؛ تقوم (SWm/SWx)، وتطبيق حدود معدل لكل (S2b إلى PGW)، وترسيخ الجلسة في نواة الحزمة Diameter، ونظرائها في ePDG، الأنفاق الحية لـ OmniWeb تعرض .geo-IP مشترك وسياسة وتكوينgeo-IP، وإعدادات وقت التشغيل؛ الاتجاهات طويلة الأمد موجودة على و تحديد المعدل لوحات Grafana التي يمكن الوصول إليها من نفس الصفحة.

← دليل العمليات

تُعتبر ePDG عنصر صفحة لكل مثيل يمك�ن الوصول إليه من الشريط الجانبي عند تشغيله في الخلفي، لذا تبقى خلف البوابة OmniWeb مخزون الموقع. يمر كل حركة المرور عبر وكيل المعتمدة الوحيدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

حالة: قراءة صحة على شاشة واحدة لـ ePDG، **الجلسات النشطة** عدد (أنفاق IPsec)، وملخص تعمل وتحمل أنفاق مكالمات ePDG لحالة تشغيل البوابة. هذه هي أسرع تأكيد على أن Wi-Fi.

الجلسات

التي تم إنشاؤها حاليًا، مفاتيحها حسب المشترك، مع حالة IPsec/IKEv2 كل جلسة نشطة: أنفاق Wi-Fi النفق والحامل. يمكنك فحص جلسة لرؤية تفاصيلها. هنا يمكنك تأكيد أن نفق مكالمات لمشترك معين يعمل.

Diameter

اتصالات الأقران Diameter إلى AAA/HSS التي تحمل المصادقة (SWm/SWx)، مع حالة اتصال كل نظير. هذا هو المكان الأول الذي تبحث فيه عندما تفشل مصادقات مكالمات Wi-Fi.

محدد المعدل

تقوم ePDG بإنهاء أنفاق IPsec/IKEv2 غير الموثوقة بـ (SWu) وتربطها بـ EPC عبر S2b، مما يجعلها معرضة لأي هاتف (أو أي مصدر) على الإنترنت المفتوح. **محدد المعدل** هو الدفاع ضد هجوم العميل على إعداد النفق IKE بحيث لا يمكن لهاتف واحد يتصرف بشكل غير صحيح أو مصدر مهاجم استنفاد البوابة. تعرض علامة التبويب الحدود **المفروضة** جنبًا إلى جنب مع عدد حي لعدد **IPs** و**IMSIs لكل** طلبات ا��. الحدود هي حدود **لكل IP المحجوبة حاليًا**. يتم التعبير عنها كعدد من محاولات المصادقة ضمن **نافذة** متحركة، و**مدة الحظر** المطبقة، **IMSI** بمجرد تجاوز الحد.

لرؤية ما إذا كان محجوبًا وعدد الفشل الذي IMSI أو IP أسفل الحدود يمكنك **البحث** عن أي عنوان تراكم، و**إزالة** ذلك الحظر حتى تُسمح محاولات المصادقة المستقبلية منه مرة أخرى؛ إجراء **مسح الكل** الواحد يزيل كل الحظر ويعيد تعيين جميع عدادات الفشل دفعة واحدة. هنا يؤكد المشغل لماذا يتم رفض نفق مكالمات Wi-Fi المسبب المصدر أن يستقر بمجرد الحظر ويزيل لمشترك.

GeoIP

GeoIP القائم على البلدان: كيف يقيد المشغل إنشاء أنفاق ePDG هو التحكم في دخول VoWiFi المصدر لكل نفق وارد مع قاعدة بيانات IP إلى البلدان المسموح بها من خلال مطابقة عنوان GeoIP. تعرض علامة التبويب ما إذا كانت التصفية **مفعلة** وما إذا كانت قاعدة البيانات **جاهزة** (محملة وقابلة للاستخدام)، و**الوضع**، و**قائمة البلدان** التي ينطبق عليها الوضع. الوضع إما **قائمة بيضاء** (فقط البلدان المدرجة يمكنها الاتصال) أو **قائمة سوداء** (البلدان المدرجة مرفوضة). كما **IPs المستخدمة** مسموح **GeoIP** تظهر **قاعدة بيانات من دول غير معروفة** بها أو محجوبة. هذه هي عناوين المصدر التي لا يمكن للقاعدة البيانات حلها إلى دولة.

على القرص، يمكن لعلامة التبويب **إعادة تحميل**ها حتى GeoIP بمجرد تحديث ملف قاعدة بيانات تدخل التعيينات الجديدة حيز التنفيذ دون إزعاج الأنفاق القائمة. هذا هو التحكم الذي يحافظ على إعداد نفق VoWiFi محصورًا في المناطق التي يخدمها المشغل.

ا��تكوين

في وقت التشغيل، وقواعد **تحديد المعدل** (حدود لكل مشترك / لكل مصدر تحمي ePDG **تكوين** هذه هي الضوابط .(أي المناطق المصدرية مسموح لها بإنشاء الأنفاق) **geo-IP** البوابة)، و**سياسة** التي تحدد من يمكنه الاتصال ومدى العدوانية.

السجلات

لاستكشاف الأخطاء وإصلاحها في ePDG تقوم علامة **السجلات** بعرض مخرجات السجل الحية لـ بوابة واحدة دون مغادرة OmniWeb.

لوحات المراقبة

تُعرض معدلات الأنفاق، ومعدل النقل وغيرها من السلاسل الزمنية لـ ePDG كلوحات Grafana، بتكرار تلك الرسوم البيانية بشكل OmniWeb التي يمكن الوصول إليها من صفحة العنصر. لا تقوم أصلي.

ذات صلة

- **PGW** يرسخ خطة مستخدم ePDG عبر **S2b**.
- **AAA/HSS** يحتفظ ببيانات مصادقة المشترك التي تحل طلبات Diameter الخاصة بـ ePDG.
- TWAG: نظير Wi-Fi *الموثوق*.

نواة 5GC

قسم **نواة 5G** يوفر لكل وظيفة شبكة 5GC (NF) لوحة تحكم حية خاصة بها. تظهر كل لوحة تحكم NF (سياقات UE، جلسات PDU، مجمعات IP، الحالة، التسجيل، وبيانات التشغيل التي تمتلكها ولكل عنصر لمسح NF كما يوفر إجراءات لكل (السياسات، جلسات الشحن، NRF تسجيلات EPC/IMS. تقرأ كل NF واجهة برمجة الحالة. إنها تعادل صفحات العناصر لكل من وظائف التطبيقات OAM الخاصة بها من خلال وكيل OmniWeb الخلفي.

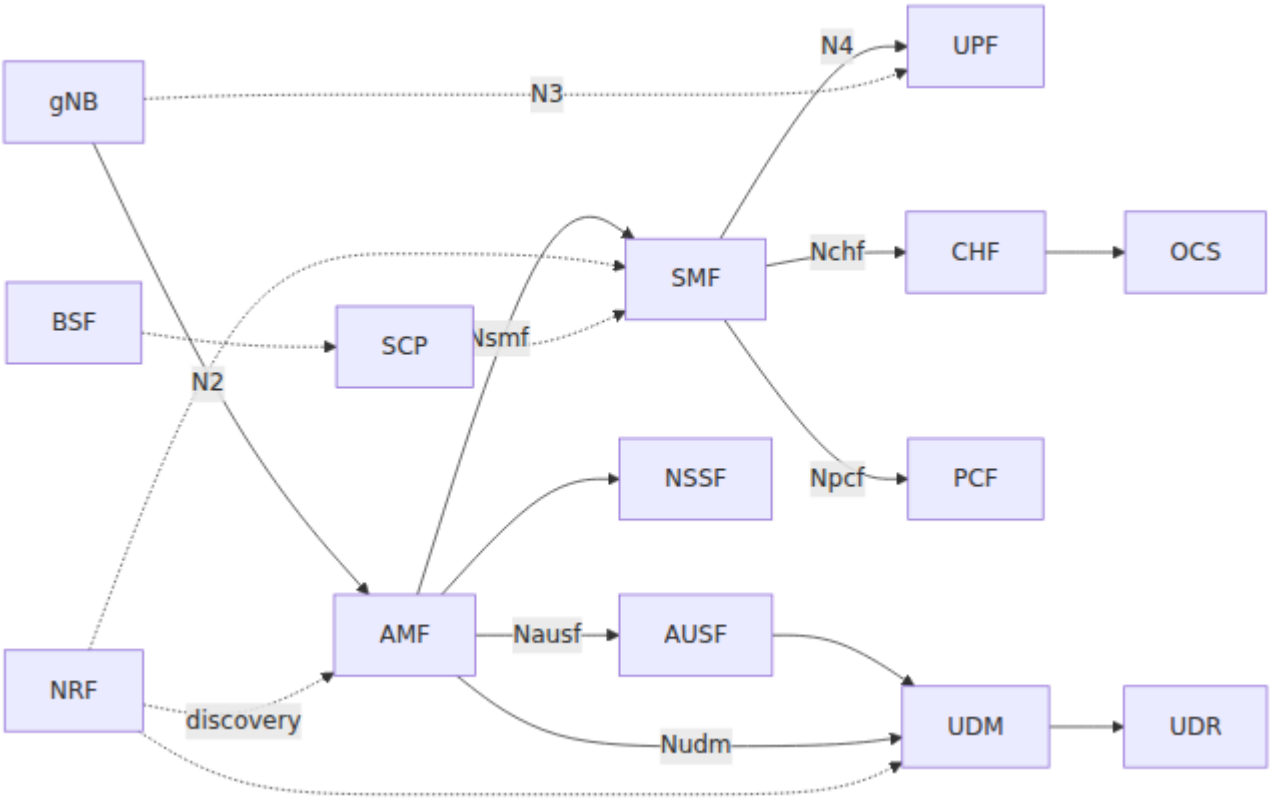
← دليل العمليات

متى تظهر

تظهر مجموعة **نواة 5G** فقط في الشريط الجانبي عندما يكون الموقع المحدد يعمل فعليًا على مستوى التحكم في 5GC. يعتمد OmniWeb على وجود **SMF و/أو AMF** في جرد الموقع. UPF وحيد مشترك مع CHF أو EPC 5GC ليس هذا القسم يظهر ا��و.

مباشرة من NF، لكل OAM تظهر، وعنوان واجهة برمجة التطبيقات NFs أي يستمد OmniWeb المعرفة في ملف المضيف. لذلك، فإن NF 5GC **الخاص بالموقع**: مجموعات **Ansible جرد** يتم حله إلى تسمية، NF هو تغيير في الجرد دون الحاجة إلى قالب يدوي. كل NF إضافة أو نقل ومنفذ. يقدم IP، وصف، ثم تستعلم `/api/5gc/nf-registry`. السجل المحل عبر OmniWeb من خلال الوكيل NF لكل OAM لوحات التحكم عن واجهة برمجة التطبيقات (`/api/5gc/nf/<id>/…`)، نموذج انظر لذا تبقى كل حركة المرور خلف البوابة المعتمدة الواحدة. التكوين. التوزيعات التي لا تعمل على أي جرد (مثل الخدمة المستضافة) تعود إلى كتلة ثابتة `fivegc` في تكوين OmniWeb.

NFs



لكل NF لوحة تحكم خاصة بها:

NF	الوظيفة	البيانات الرئيسية المعروضة
NRF	وظيفة مستودع الشبكة	المسجلة (مجمعة حسب النوع)، الخدمات NF حالات المسجلة، الاشتراكات: انظر أدناه
AMF	إدارة الوصول والتنقل	قائمة UE، gNodeBs المتصلة (مع فك تشفير gNB-ID / TAC / PLMN / SST)، الإحصائيات، وضع الصيانة
SMF	إدارة الجلسات	جلسات PDU، **مجمعات IP**، ارتباط UPF، الإحصائيات
UDM	إدارة البيانات الموحدة	قائمة UE، الإحصائيات
UDR	مستودع البيانات الموحد	صحة HSS، المشتركين
AUSF	خادم المصادقة	جلسات AUSF (المصادقة)، الإحصائيات
PCF	التحكم في السياسات	سياسات AM، سياسات SM، الإحصائيات
CHF	وظيفة الشحن	جلسات الشحن، صحة CGrateS، سجلات CDR
NSSF	تيار شريحة ا الشبكة	الشرائح، توفر NSSAI، الإحصائيات
BSF	دعم الربط	ربطات PCF، الإحصائيات
SCP	وكيل الاتصالات الخدمية	صحة NF، الإحصائيات، ذاكرة التخزين المؤقت للاكتشاف

صفحة NF المعرفة في جرد الموقع. لكل NFs تظهر فقط NF. ليس كل توزيع يعمل على كل مرجعية خاصة بها. اتبع الروابط أعلاه.

SMF الخاصة بـ IP علامة تبويب مجمعات

على علامة SMF التي تظهرها هذه اللوحات: تحتوي لوحة تحكم NF كمثال على البيانات المملوكة لـ إلى جانب UE، لـ IP عناوين SMF تظهر مجمعات العناوين التي يخصص منها **IP** تبويب **مجمعات** إلى مستوى المستخدم N4/PFCP حالة رابط) **UPF** الحية الخاصة به و**ارتباط PDU جلسات**). الخاص به، ما هي الجلسات النشطة، وهل تنفذ UPF متصل بـ SMF معًا، تجيب هذه على "هل العناوين؟" دون مغادرة OmniWeb.

لوحة تحكم في لمحة

نفس التخطيط NF تتبع كل لوحة تحكم:

1. هل تم) NRF **بطاقات الصحة** عبر الأ��لى: صحة واجهة برمجة التطبيقات، تسجيل والترخيص. كل منها يستعلم على فترات. استخدم NF، حالة NF، تسجيل هذه NF مع NRF؟)، **مؤشر الاستعلام** في الرأس لإيقاف أو رؤية وقت آخر تحديث (الاستعلام هو نمط مشترك: انظر العمليات الشائعة).
2. عمليات على مستوى NF (انظر أدناه): **الإجراءات**.
3. تفاصيل حالة واجهة برمجة التطبيقات، تفاصيل تسجيل NRF، **أقسام البيانات**: من الجدول أعلاه، كل منها يتم تحديثه تلقائيًا. تقوم الجداول NF والجداول المحددة لـ Erlang، المشفرة بـ S1AP من مصطلحات PLMN/TAC/SST: بفك تشفير ما يمكنها الطوابع الزمنية إلى الوقت النسبي، الحالات إلى رقائق ملونة، والروابط المتقاطعة NF). ترتبط بلوحة التحكم الخاصة بتلك NF قيمة نوع

الإجراءات

كل منها يطلب تأكيدًا أولاً، لأنها مدمرة. NF تظهر لوحات التحكم إجراءات لمسح حالة:

NF	إجراءات على مستوى NF	إجراءات لكل صف
AMF	مسح الذاكرة المؤقتة · UE مسح جميع سياقات	إلغاء تسجيل UE
SMF	مسح الذاكرة المؤقتة · · PDU تحرير جميع جلسات إعادة ارتباط PFCP (إعادة إنشاء ارتباط UPF)	تحرير جلسة PDU واحدة
NRF	إلغاء تسجيل جميع NFs	إلغاء تسجيل NF · واحد إزالة اشتراك
AUSF	مسح جميع جلسات المصادقة	مسح جلسة واحدة
UDM	مسح ذاكرة التخزين المؤقت للمشتركين	-
PCF	-	إزالة سياسة AM أو SM

SMF تتيح هذه الإجراءات للمشغل التعافي من حالة متوقفة. على سبيل المثال، فرض إعادة ارتباط قديم من NF الذي لن يتم مسحه، أو إلغاء تسجيل UE الخاص به، إسقاط سياق UPF الذي فقد NRF.

NRF لوحة تحكم

تحصل NRF 5 كل تكتشفه الذي السجل أنها لأن أغنى عرض على GCمن خلاله:

- **بطاقات القياس**: أنواع NF، إجمالي الحالات، المسجلة (مع شريط النسبة المئوية من الإجمالي)، والخدمات/الاشتراكات.
- **المسجلة NF حالا��**: مجمعة حسب نوع NF. تقوم لوحة التحكم بتشفير كل بطاقة حالة بالألوان. تظهر البطاقة حالة التسجيل، مؤقت نبض القلب، عدد الخدمات، و PLMN. انقر على حالة للحصول على ملفها الشخصي الكامل (مع رابط **فتح لوحة التحكم** وزر **إلغاء التسجيل** لتلك NF).
- **الخدمات المسجلة**: جدول مسطح لكل خدمة تعلن عنها كل حالة، إصداراتها، وحالتها.
- **إلغاء تسجيل جميع NFs**: يمسح كل تسجيل (بعد ذلك إعادة NF يجب على كل التسجيل).

النشطة، هل تم تسجيلها جميعًا، وما هي الخدمات NFs المكان للإجابة على "ما هي NRF هذا يجعل التي تقدمها؟"

ذات صلة

- توبولوجيا الشبكة: وجهات النظر التوبولوجية التي ترتبط بهذه اللوحات.
- العمليات الشائعة: أنماط الاستعلام، التكوين، و RBAC المشتركة مع كل صفحة عنصر.
- UPF و PGW-C / SMF: صفحات الجلسات/مستوى المستخدم من جانب EPC المتقارب JEPC+5GC.

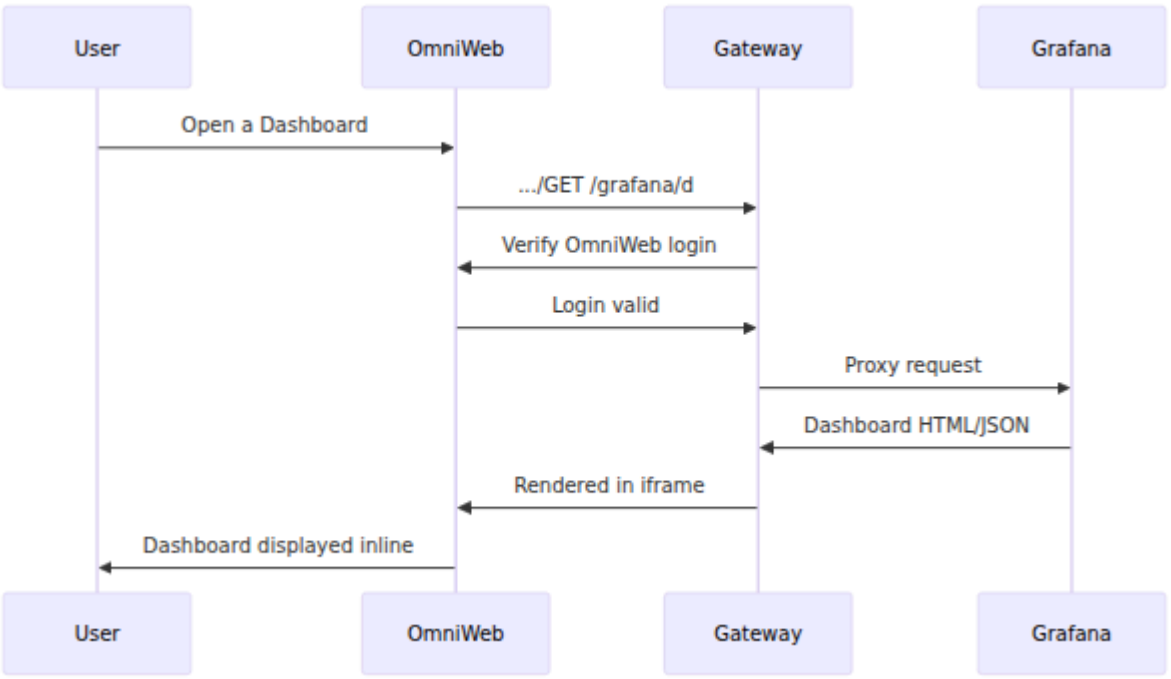
لوحات معلومات جرافانا والإحصائيات

تقوم OmniWeb بتضمين جرافانا مباشرة في البوابة. يمكن للمشغلين رؤية لوحات المعلومات والإحصائيات لأي عنصر، وللشبكة ككل، دون الحاجة إلى تسجيل دخول منفصل أو علامة تبويب متصفح.

← العودة إلى دليل العمليات

كيف يعمل

يتم تقديم جرافانا خلف البوابة المعتمدة على المسار `/grafana/` ومضمونة كإطار iframe داخل OmniWeb. تكون المصادقة شفافة: عندما تكون مسجلاً دخولك إلى OmniWeb، يتم تفويض الوصول إلى جرافانا تلقائيًا ضد تسجيل دخولك إلى OmniWeb. لا يوجد كلمة مرور ثانية.



تم تكوين مثيل جرافانا الذي تقوم OmniWeb بتمريره بواسطة متغير البيئة `GRAFANA_URL` (الافتراضي `http://localhost:3000`). تتولى البوابة التعامل مع التمرير والتحقق من تسجيل الدخول الأحادي بشكل شفاف.

طريقتان للوصول إلى لوحات المعلومات

1. علامة تبويب لوحات المعلومات لكل عنصر

تظهر العناصر التي تم وضع علامة عليها لجرافانا علامة تبويب **لوحات المعلومات** في مساحة عملها. تقوم OmniWeb باستعلام جرافانا عن لوحات المعلومات التي تتطابق مع علامات ذلك العنصر وتعرض اللوحة المعنية بشكل متداخل. هذا يحافظ على إحصائيات العنصر بجانب بياناته التشغيلية.

تطابق العلامات غير حساس لحالة الأحرف. مجموعات العلامات التمثيلية:

العنصر	العلامات المتطابقة في جرافانا
UPF	`upf`
P-CSCF	`pcscf`, `cscf`
I-CSCF	`icscf`, `cscf`
S-CSCF	`scscf`, `cscf`
PGW-C, MME, SMSC, DRA, OCS, TAS	علامات محددة للعنصر

لجعل لوحة المعلومات تظهر تحت عنصر، ضع علامة عليها في جرافانا بعلامة ذلك العنصر (على سبيل المثال، ضع علامة على لوحة معلومات UPF بـ `upf`).

2. الشريط الجانبي لجرافانا

تدرج إدخال **جرافانا → لوحات المعلومات** في الشريط الجانبي جميع لوحات المعلومات المتاحة. يؤدي اختيار واحدة إلى فتحها بشكل متداخل داخل OmniWeb، ويتم تحديث عنوان URL ليعكس مسار لوحة المعلومات بحيث يمكنك الارتباط العميق بلوحة معلومات معينة.

الإحصائيات

تعتبر لوحات المعلومات المضمنة هي المكان الذي تعيش فيه **الإحصائيات** على مستوى الشبكة وعلى مستوى كل عنصر: عدد الجلسات ومعدلاتها، الإنتاجية، الكمون، معدلات السقوط، صحة

عدد التسجيلات، واتجاهات السعة. تمنحك CDR، بمرور الوقت، أحجام Diameter/PFCP ظير الحالة *الحالية* (وتتيح لك التصرف بناءً عليها)؛ بينما تقدم OmniWeb صفحات العناصر الخاصة بـ جرافانا الصورة *التاريخية* والاتجاهات. تم تصميمها لتستخدم معًا. تحقق من تنبيه جرافانا من خلال الانتقال إلى صفحات التشغيل الخاصة بالعنصر، والسجلات، والتتبع.

التنبيه

يتولى محرك التنبيه المدمج في جرافانا جميع التنبيهات المعتمدة على العتبات. يتم تعريف قواعد التنبيه في جرافانا ويمكن أن تُخطِر عبر البريد الإلكتروني، Slack، PagerDuty، أو webhook. لا تقوم OmniWeb بتكرار التنبيه. إنها توفر السياق التشغيلي (صفحات العناصر، السجلات، التتبع) اللازمة للتحقيق عند حدوث تنبيه.

فئات التنبيه الشائعة:

الفئة	الأمثلة
التوفر	PFCP معطل، فقدان ارتباط Diameter العنصر غير قابل للوصول، نظير
السعة	عتبة عدد المشتركين في eBPF > 80%، استخدام خريطة IP، تنفاد مجموعة VLR
الأداء	فشل نبضات القلب XDP، كمون إعداد الجلسة، معدل سقوط
الحركة	حجم CDR غير الطبيعي، معدل سقوط المكالمات، فشل تسليم SMS

التحقيق في تنبيه: التدفق الموصى به



1. تأكيد الاتجاه في جرافانا (لوحات المعلومات).
2. التحقق من الحالة الحالية في نظرة عامة على العنصر.
3. قراءة سجلات العنصر حول وقت التنبيه.
4. إذا كان خاصًا بالمشترك، قم بتشغيل تتبع الجلسة. انظر السجلات وتتبع المشتركين.

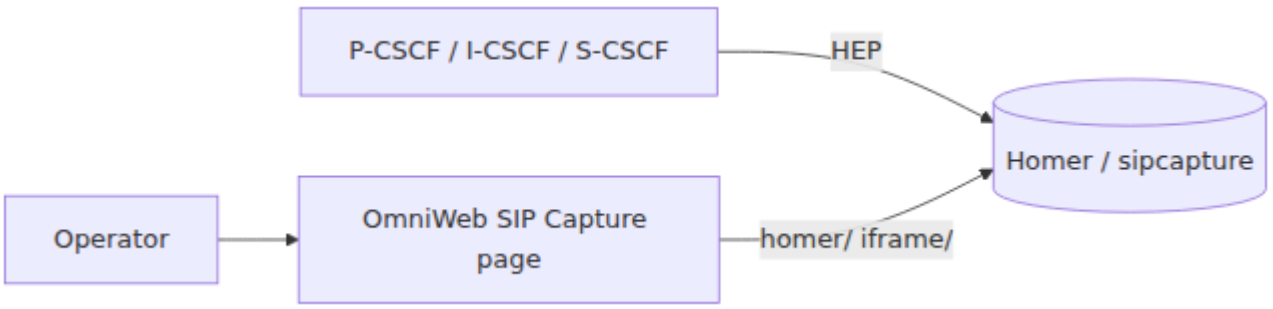
SIP هومر: تحليل التقاط وتدفق المكالمات

بتضمين OmniWeb يقوم. (HEP / sipcapture) والبحث عنها SIP هو نظام لتقاط رسائل **هومر** الملتقطة وإعادة SIP واجهة المستخدم الخاصة بهومر مباشرة، بحيث يمكنك البحث في حركة مرور بناء سلم الإشارات لمكالمة دون مغادرة البوابة أو تسجيل الدخول بشكل منفصل.

← دليل العمليات

ما هو

ويخزنها بحيث يمكن البحث عنها بواسطة (HEP عبر بروتوكول) IMS من SIP يجمع هومر رسائل معرف المكالمة، رقم من/إلى، الوقت، والمزيد. تتيح لك واجهة المستخدم على الويب العثور على بين النقاط النهائية و SIP مكالمة ورسم **مخطط التدفق** الكامل لها: كل رسالة CSCFs، مع تنفيذ أي من هذا. إنه **يضم تطبيق** OmniWeb التوقيتات وأي سبب لفشل/إنهاء المكالمة. لا يعيد (مدرج تحت تتبع الجلسة في الشريط الجانبي) **SIP** تحت **التقاط** iframe في **هومر**.



تسجيل الدخول الموحد

بتمرير تطبيق هومر عند OmniWeb لا تحتاج إلى تسجيل الدخول إلى هومر بشكل منفصل. يقوم في الطريق، لذا فإن واجهة المستخدم المضمنة **مُعتمدة** auth-proxy ويحقن رؤوس `/homer/` **مسبقًا**، دون ظهور مطالبة تسجيل دخول هومر. يتم الوصول إليها من خلال نفس بوابة يحكمها OmniWeb لذا فإن تسجيل دخول واحد إلى Loki،و Grafana المعتمدة مثل OmniWeb أيضًا.

فقط في الشريط الجانبي عندما يكون هومر **مكونًا وقابلًا للوصول SIP** تظهر إدخال **التقاط** بفحصه ويخفي الإدخال إذا لم يكن موجودًا، لذا لن تضطر أبدًا للنقر على OmniWeb للنشر. يقوم صفحة ميتة.

هومر مقابل تتبع الجلسة

يمتلك OmniWeb طريقتين مكملتين للنظر في الإشارات، ومن المفيد معرفة أي منهما يجب الوصول إليه:

	هومر (التقاط SIP)	تتبع الجلسة
النطاق	SIP فقط، بعمق	الشبكة بأكملها: Diameter، GTP-C، PFCP، SIP، MAP
السؤال الذي يجيب عليه	"ماذا فعل SIP لهذه *المكالمة*، رسالة تلو الأخرى، مع التوقيت وسبب إنهاء المكالمة؟"	"ماذا حدث لهذا *المشترك* عبر كل عنصر؟"
الأفضل لـ	تسجيل VoIP/VoLTE، تشخيص مكالمة فاشل، إنهاء محدد	متابعة IMSI/MSISDN واحد من النهاية إلى النهاية عبر النواة

استعن بهومر عندما يكون لديك مكالمة لتفكيكها؛ واستعن بتتبع الجلسة عندما تتابع مشتركًا عبر السجلات وتتبع المشتركين. كما يرتبط هومر من دليل كامل المكدس.

ذات صلة

- السجلات وتتبع المشتركين: تتبع الجلسة عبر ��لشبكة وأين يتناسب هومر.
- والإحصائيات: الأداة الأخرى للمراقبة المضمنة، التي يتم Grafana لوحات معلومات الوصول إليها بنفس الطريقة المعتمدة.

HSS: خادم المشترك المنزلي

HSS (خادم المشترك المنزلي) هو قاعدة بيانات المشتركين الرئيسية للنواة المحمولة. يحتفظ بهويات كل مشترك (IMSI، MSISDN وSIM/ICCID)، ومادة مفتاح المصادقة التي تثبت من هم، والتجوال التي تحدد ما يمكن لكل مشترك القيام به PCRF وIMS وEPC وملفات تعريف خدمات لمصادقة وتحديد موقع جهاز ما ولتعلم اشتراكه في S6a بقراءته عبر MME على الشبكة. يقوم EPC. يقوم CSCF بقراءته عبر Cx لتسجيل IMS وتحفيز خدمات iFC. يستمد PCRF قواعد سياسته وشحنه منه. يستخدم المشغل لوحة التحكم الخاصة به لتوفير والبحث عن المشتركين، وتنظيم ملفات تعريف الخدمة المشتركة، والتحقق من صحة HSS الخاصة به.

← دليل العمليات

في جرد HSS عد لوحة التحكم صفحة عنصر لكل مثيل. تفتح من الشريط الجانبي عندما يعمل إلى واجهة برمجة التطبيقات OmniWeb الموقع. تمر جميع الحركة المرورية عبر وكيل خلفي الخاصة بـ HSS، لذا تبقى خلف بوابة مصدقة واحدة. تأتي الردود في ظرف `{status, response}`. يوفر رابط الوثائق في رأس الصفحة مساعدة في السياق. تحتوي الصفحة على علامات تبويب.

المشتركين

للعثور **ICCID أو MSISDN أو IMSI** تعد علامة التبويب الرئيسية دليل المشتركين. ابحث **حسب** عندما تتتبع جلسة حية إلى مالكها. **IP** على سجل. يقوم البحث أيضًا بحل مشترك **حسب عنوان** وحالته، **(IMSI)** افتح سجلًا لعرض نظرة عامة على المشترك: مخطط علاقة يربط المشترك بهويته و**التجوال** المعينة له. تظهر **IMS**و **EPC** وملفات تعريف، **(مفعلًا IMS مفعل، وما إذا كان)** بقيم المفتاح HSS يحتفظ .EPC الخاصة بالملف الشخصي تحت ملف تعريف APNs الصف��ة الحساسة ولكنه لا يعرضها. يمكنك تحديثها، ولكن يتم قراءتها مرة أخرى كمحررة.

التوفير

قم بإنشاء أو تحرير مشترك من نموذج التوفير. يجمع النموذج الهوية، والاعتمادات، و SIMوالملفات الشخصية في مكان واحد:

- **هوية المشترك**: IMSI، **مفعل** و**مفعل** اسم المشترك، ومفاتيح **IMS**.
- **مجموعة مفتاح المصادقة**: خوارزمية المصادقة، **Ki** و**OPc** (أو **OP**)، **AMF**، **SQN**، وكلمة مرور SIP المستخدمة لـ IMS.
- **بطاقة SIM**: **ICCID**، وما إذا كانت eSIM، وقيم PIN/PUK وتفاصيل الدفعة والبائع.
- **أرقام الهواتف MSISDNs**: قم بتعيين واحد أو أكثر من الأرقام الموجودة. ابحث عن أثناء الكتابة حتى لا تقوم بإنشاء رقم مرتين.
- **تعيين الملفات الشخصية EPC** و**IMS** و**التجوال** التي تمنح المشترك خدمته.

يمكنك تحديث المشتركين الحاليين بنفس الطريقة. يمكنك حذف مشترك من سجله.

بطاقات SIM

يحتفظ مخزون SIM بكل **SIM** يعرفه HSS. **حسب** ابحث عنه **ICCID**. تحمل كل SIM **ICCID**، ومجموعة كاملة من **LPA**، eSIM وeSIM (**KIC**، **KID**) اسم الدفعة والبائع، قيم المفتاح النقل، علم eSIM. يمكنك إنشاء، تحرير وحذف SIMs. يتم إدارة **مجموعة مفاتيح** المصادقة التي **مفاتيح ADM**. في علامة تبويب خاصة بها SIM تتزاوج معها سجلات.

MSISDNs

يحتوي دليل MSISDN للحصول **حسب الأرقام** ابحث. على مجموعة أرقام الهواتف المخصصة. يمكنك إنشاء، تحرير وحذف الأرقام. على تطابق جزئي للعثور على رقم أو التحقق منه قبل تعيينه. تقوم بإرفاق الأرقام بالمشتركين أثناء التوفير.

مجموعات المفاتيح

دليل مجموعة المفاتيح هو مخزن بيانات اعتماد المصادقة الذي تشير إليه كل سجل مشترك. تحتوي كل إدخالة على **الخوارزمية**، مادة المفتاح (Digest-MD5 أو Milenage)، وعداد **SQN**، وعداد **AMF**. يمكنك **حسب** **AMF أو الخوارزمية أو ID** الاختياري. قم بتصفية الصفحة وعداد SIM OTA إنشاء، تحرير وحذف مجموعات المفاتيح.

لا تظهر أبدًا - يتم قراءتها مرة SIP وكلمة مرور **Ki**، **OPc**، **OP**. مادة المفتاح قابلة للكتابة فقط أخرى كمحررة، وتحرير يترك واحدة فارغة يحتفظ بالقيمة المخزنة بدلاً من مسحها. حذف مجموعة مفاتيح لا يزال يشير إليها مشترك يمنع ذلك المشترك من المصادقة، لذا تحقق قبل إزالة واحدة.

ملفات تعريف الخدمة

ملفات تعريف الخدمة هي اللبنات القابلة لإعادة الاستخدام التي تحدد ما يمكن أن يفعله المشترك. يشير المشترك إليها بدلاً من حمل نسخته الخاصة. لذا فإن التغيير في ملف تعريف ينطبق على الجميع الذين يستخدمونه.

ملفات تعريف EPC

وضع الوصول إلى EPC يحدد **ملف تعريف** MME. الاشتراك في حزمة البيانات الذي يفرضه وقائمة ،**TAU فترة** ،UE-AMBR **الشبكة**، عرض النطاق الترددي المجمع **للتحميل/الرفع الافتراضي**. **APN** هي APN التي يمكن للمشترك استخدامها. واحدة من **APN ملفات تعريف** و**ملف تعريف QoS APN** إلى **ملف تعريف APN** يربط **معرف APN** كل **ملف تعريف** EPC كافتراضي. يجب أن يشير ملف تعريف APN يمكنك وضع علامة على ملف تعريف **PCRF**. المعينة APNs الافتراضي واحدًا من APN يجب أن يكون .APN إلى الأقل واحد من ملفات تعريف

APN يربط **APN** الخاصة به. **إضافة** APN لقائمة ملفات تعريف EPC قم بتوسيع ملف تعريف **EPC** على كل صف **لإزالته من هذا الملف الشخصي** unlink بالملف الشخصي. تعمل عملية نفسه. يمكنك إعادة إضافته لاحقًا، أو يمكن أن تعيد APN بملف تعريف HSS **فقط**. يحتفظ واحد، APN الأخرى. يجب أن يحتفظ الملف الشخصي بحد أدنى من EPC استخدامه ملفات تعريف الذي كان APN الافتراضي تلقائيًا إذا قمت بإزالة APN بإزالة HSS لذا لا يمكنك إزالة الأخير. يقوم يشير إليه.

ملفات تعريف APN

بشكل مستقل عن ملفات تعريف APN كل ملف تعريف APN تسرد علامة تبويب ملفات تعريف **PCRF**. و**ملف تعريف QoS APN** و**ملف تعريف APN** التي تستخدمه. يظهر EPC **معرف**

يتم وضع علامة .APN الذي يشير إلى EPC تسرد عمود **المستخدم من قبل** كل ملف تعريف إلى هذه الحالة بمجرد APN يصل .EPC **يتيم** عندما لا يشير إليه أي م��ف تعريف APN على الذي استخدمه. يقوم مفتاح **يتيم فقط** بتصفية القائمة لتلك، حتى EPC إزالته من آخر ملف تعريف غير المستخدمة وتنظيفها APNs تتمكن من العثور على.

يمكنك إنشاء ملفات تعريف هنا، تحريرها، وحذفها. يبدأ ملف تعريف جديد غير مرتبط. لربطه بخدمة لا يزال مرتبطًا بواحد أو APN لا يمكنك حذف ملف تعريف .EPC مشترك، أضفه إلى ملف تعريف أولاً أزلها من تلك الملفات، ثم احذفها من هذه العلامة .EPC أكثر من ملفات تعريف.

ملفات تعريف QoS APN

القابلة لإعادة APN على مستوى QoS قوالب QoS APN تدير علامة تبويب ملفات تعريف الخاص به إلى APN يحصل كل مشترك يشير .APNو EPC الاستخدام التي تشير إليها ملفات تعريف معرف فئة) **QCI**قالب على نفس جودة الخدمة على حامله الافتراضي. يحمل كل قالب **اسم** و ،(أولوية التخصيص/الاحتفاظ) **ARP** يحمل أيضًا .(الذي يربط الحامل بسلوك تأخير وفقد موحد QoS مع **قدرة التقديم** و**هشاشة التقديم**. تحدد هذه الأعلام ما إذا كان يمكن للحامل أن يتجاوز، أو APN-AMBR يتم تجاوزه من قبل، الآخرين عندما تكون الموارد نادرة. يحمل كل قالب أيضًا معدلات للرفع والتحميل، وما إذا كانت **الشحن عبر الإنترنت** و**الشحن غير المتصل** مفعلتين.

يمكنك إنشاء، تحرير، وحذف القوالب. يمكنك أيضًا استنساخ قالب للحصول على نسخة جديدة. بدلاً من حمل نسخته الخاصة. إذا قمت بتحرير قالب، فإنك QoS إلى قالب APN يشير ملف تعريف يستخدمه. لا يمكنك حذف قالب لا يزال يشير إليه ملف تعريف APN لكل QoS تعيد تشكيل APN. أولاً أعيد تعيين تلك APNs.

ملفات تعريف QoS APN

يشير إليها ملف تعريف APN إعدادات جودة الخدمة لكل APN: **QCI**، **ARP** و**قدرة/هشاشة** وما إذا كانت **الشحن عبر** APN-AMBR، عرض النطاق الترددي **التقديم**، **للتحميل/الرفع** تنطبق. يمكنك استنساخ ملف تعريف للحصول **(Rf)** و**الشحن غير المتصل (Gy) الإنترنت** على نسخة جديدة من واحد موجود.

ملفات تعريف IMS

معايير **iFC**: **قالب IMS** يحمل **ملف تعريف** عبر Cx. CSCF الذي يقرأه IMS الاشتراك في لمشترك. يمكنك إنشاء، تحرير SIP التصفية الأولية التي تحدد أي خوادم تطبيقات تتلقى حركة وحذف الملفات الشخصية.

عناوين IP الثابتة

تخصيصات IP الثابتة للمشتركين الذين يجب أن يتلقوا دائمًا نفس العنوان، تُدار جنبًا إلى جنب مع بيانات اشتراك EPC.

PCRF

طبقة السياسة التي يطبقها PCRF. تت��رض رؤية العلاقة الأجزاء الثلاثة:

- **ملفات تعريف PCRF**: لمشترك، تتكون من APN السياسة المسماة التي يشير إليها مجموعة من قواعد الشحن.
- **قواعد الشحن**: كل منها مع **نوع القاعدة** و**الأولوية** حدود **التحميل/ ARP**، و**QCI**، **مجموعة تصنيف** و**معرف الخدمة** للشحن. يحمل حامل MBR/GBR، و**الرفع** مخصص قاعدة مع GBR أو MBR.
- **قواعد معلومات التدفق**: قوالب تدفق الحركة المرتبطة بقاعدة شحن تحدد أي حزم تتطابق معها.

يمكنك إنشاء، تحرير وحذف الثلاثة. إذا قمت بتحرير قاعدة شحن، فإنك تؤثر على كل ملف تعريف يستخدمها.

التجوال

على المشتركين الواردين والصادرين. يحدد **ملف تعريف** HSS سياسة التجوال التي يطبقها **الافتراضي**، وقائمة **قواعد التجو��ل**. **IMS التجوال إجراء البيانات الافتراضي**، **إجراء** لتلك الشبكة. يمكنك **IMS** وتحدد **إجراء البيانات** و**إجراء MCC/MNC** تعتمد كل قاعدة على بالتالي السماح أو حظر شبكات معينة أثناء تغطي ملف التعريف الافتراضي الباقي. لإضافة قاعدة، القواعد .(IR.21 من) لشبكة من اسم مشغل MCC/MNC استخدم بحث المشغل للعثور على مشتركة. إذا قمت بتحرير قاعدة، فإنك تؤثر على كل ملف تعريف يستخدمها.

EIR

بواسطة تعبير عادي وتحدد **إجراء**: السماح **IMEI** مع **EIR** سجل هوية المعدات. تتطابق كل **قاعدة** أو الحظر. يمكنك بالتالي حظر نموذج جهاز أو هاتف محدد من الشبكة. تساعدك عملية بحث نموذج الجهاز في بناء نمط IMEI. يمكنك إنشاء، تحرير وحذف القواعد.

الحالة

وقاعدة البيانات والترخيص، وأعداد API نفسه: صحة HSS قراءة صحة شاشة واحدة لـ IMS وملفات تعريف EPC الكيانات للمجموع الكلي من المشتركين وملفات تعريف يعمل وكم HSS وملفات تعريف التجوال. إنها أسرع تأكيد على أن MSISDNsو SIMsو المدمجة لوحات المراقبة والإحصائيات Grafana يحمل. توفر رسومات.

نظيرة. تتبع علامة تبويب HSS تظهر علامة تبويب التكرار حالة تكرار قاعدة البيانات إلى أي مثيلات الحية. استخدمها لاستكشاف الأخطاء في مثيل واحد دون مغادرة HSS السجلات مخرجات سجل OmniWeb.

التكرار

HSS لقاعدة بيانات المشتركين في عقدة PostgreSQL تقرأ علامة تبويب التكرار صحة تكرار وترسمها كطوبولوجي�؟ حية. تظهر كل عقدة ما إذا كانت قاعدة بياناتها **رئيسية** أو **نسخة احتياطية**. النسخة الاحتياطية هي عقدة في حالة استرداد. تعيد تشغيل تغييرات الرئيسية بدلاً من قبول الكتابات الخاصة بها. بالنسبة للرئيسية، ترسم علامة التبويب كل نسخة احتياطية متصلة كرابط أسفل المنبع. يظهر الرابط **عنوان العميل** للنسخة الاحتياطية، و**فتحة التكرار** التي تتدفق من الحالي للرئيسية. تظهر علامة WAL خلالها، و**حالة البث**، و**تأخر التكرار** المقاس مقابل موقع التبويب التأخر بالبايت، لذا فإن النسخة الاحتياطية التي تتأخر تبرز في لمحة. يحدد ما إذا كانت كل فتحة تكرار **نشطة** حاليًا ما إذا كان رابطها يقرأ كصحي أو معطل.

يستخدم المشغل هذه العلامة لتأكيد أن قاعدة بيانات المشتركين تتكرر عبر مجموعة HSS: أن تغييرًا تم توفيره على عقدة واحدة سيصل إلى الآخرين، وأن هناك نسخة احتياطية موجودة للتبديل إليها. تظهر النسخة المتأخرة رقم تأخر متزايد. تسقط النسخة المعطلة أو المنفصلة رابطها. إذا تعمل ولكن لا تتكرر أي منها، فإن علامة التبويب تشير HSS كانت هناك اثنتان أو أكثر من مثيلات إلى المجموعة بأكملها كفجوة في التكرار. صحح ذلك قبل أن يصبح خطر فقدان البيانات.

العمليات

تعمل عمليتان على مستوى المشترك على جلسة حية بدلاً من السجل المخزن:

- **إلغاء الموقع (CLR)**: إرسال طلب إلغاء الموقع S6a إلى MME. هذا الخادم لمشترك يفصل المشترك، لذا يعيد الاتصال ويستلم بيانات الاشتراك المتغيرة.
- **إعادة مصادقة PCRF**: طلب أن يعيد PCRF مصادقة مشترك لجلسة PDN معينة. هذا يدفع قواعد السياسة أو الشحن المحدثة إلى جلسة نشطة.

ذات صلة

- **MME**: يقرأ بيانات مصادقة المشترك وبيانات اشتراك EPC عبر **S6a**. إنه الهدف من إلغاء الموقع.
- **CSCF**: يقرأ ملف تعريف IMS وiFC عبر **Cx** لتسجيل IMS وتحفيز الخدمة.
- **PCRF / PCF**: يطبق ملفات تعريف PCRF وقواعد الشحن وقواعد التدفق المحتفظ بها هنا. إنه الهدف من إعادة المصادقة.
- **UDR**: مخزن بيانات المشتركين المشتركة الذي يواجهه HSS 5 في نواة 5G.
- العودة إلى فهرس العناصر: دليل العمليات.

LCS: خدمات الموقع (OmniLCS)

توفر **خدمات الموقع** للنواة. إنها تجيب على سؤال "أين هو هذا المشترك؟" وتدفع **LCS** وظيفة من الخلية الخدمية (ومعلمات الخلية المكونة) ، وتلبي UE تحذيرات البث الخلوي. تقوم بتحديد موقع طلبات الموقع من الشبكة (الفورية والمتأخرة) ، وتدفع تحذيرات **تنبيهات الهاتف المحمول** مخزون الخلايا الخاص بـ OmniWeb LCS ، **التجارية / البث الخلوي** إلى منطقة معينة. تعرض والبث؛ الاتجاهات CAP والتحديثات الحية والماضية للموقع ، وطلبات الموقع المؤجلة ، وتنبيهات التي يمكن الوصول إليها من نفس الصفحة Grafana طويلة الأمد موجودة على لوحات.

← دليل العمليات

يعتبر LCS صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيلها في مخزون لذا يبقى خلف بوابة مصدقة واحدة. ، OmniWeb الموقع. يمر كل حركة المرور عبر وكيل خلفية يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

حالة: قراءة صحة على شاشة واحدة للموقع ، عدد ، LCS **الجلسات النشطة** و **المكتملة**. هذه هي أسرع تأكيد على أن LCS يعمل ولديه معلمات **الخلايا المحملة** ، ونتيجة **مزامنة الخلايا** خلية حالية.

تظهر النظرة العامة أيضًا كل اتصال يحتفظ به LCS أو **متصل** (مع بقية النواة ، كل منها بحالته **منفصل**)، العنوان و، بالنسبة لارتباطات SCTP، ظهوره ووقت معرف الارتباط:

- **أقران SBc-AP**: 4 لكل MME. 4 ارتباط البث الخلوي لكل eNB يمكن أن تصل بث تحذير eNB الخاص بها متصلًا، لذا فإن هذا هو أول SBc-AP التي يكون ارتباط MME فقط إلى خلايا شيء يجب التحقق منه عندما لا يصل البث إلى الهواتف المحمولة.
- **أقران SLs**: ارتباط **LCS-AP** لكل MME، الذي يحمل تحديد الموقع (E-CID، OTDOA، A-GNSS) بين LCS و MME الخدمية.
- **أقران Diameter**: اتصالات SLg/SLh Diameter (على سبيل المثال إلى DRA)، مع معرفات المنتج والتطبيق الخاصة بالند.
- **تغذيات CAP**: كل اتصال بمصدر تنبيه (انظر تغذيات CAP)، مع وقت آخر نبضة أو استعلام له.

تعدّ البلاطات في الأعلى عدد الأقران المتصلة من كل نوع مقابل الإجمالي المكون، وتتحول إلى اللون الأحمر عندما يكون أي منها غير متصل.

الخلايا

ضده: معرف كل خلية، خط العرض/خط الطول، نصف القطر، LCS **مخزون الخلايا** الذي يحدد يمكنك إضافة وتحرير وإزالة الخلايا هنا. هذه .RAT الاتجاه و ،EARFCN ،PCI ،TAC/LAC ،الارتفاع المعلمات هي ما يحول معرف الخلية الخدمية إلى موقع.

إضافة أو تحرير خلية

1. **الراديو** اختر (2G، 3G، 4G أو 5G). تظهر النافذة الحقول التي يستخدمها هذا الراديو: LAC لـ 2G/3G، TAC لـ 4G/5G، ورقم القناة المطابق (ARFCN، UARFCN، EARFCN أو NR-ARFCN) وهوية الخلية الفيزيائية.
2. **ECI من بناء** يعمل، أدخل **معرف الخلية** بالضبط كما تقارير الشبكة. بالنسبة لـ 4G، ورقم الخلية eNB من معرف ECI على حساب **معرف eNB**.
3. أدخل **LAC** أو **TAC** لهذه الخلية إلى رمز المنطقة هذا. تذهب بث الخلايا.
4. ضع الخلية: انقر على الخريطة، اسحب العلامة، أو اكتب أو ألصق خط العرض وخط الطول (`lat, lon`). و، اضبط **نصف القطر** (الملصوق في أي صندوق يملأ كلاهما). بالنسبة لهوائي مقسم، **الاتجاه**؛ تظهر الخريطة التغطية الناتجة.

يتم التحقق من كل قيمة مقابل نطاقها الصالح قبل أن يمكن حفظ الخلية. يصل تنبيه CAP إلى خلية عندما يكون موقع الخلية داخل منطقة التنبيه، لذا فإن الخلية التي ليس لديها موقع، أو مع TAC أو LAC خاطئ، لا تتلقى أي تنبيهات.

الموقع

تحديثات **الموقع الأخيرة**: مشترك كل تحديث، خلية الحل، الموقع المحسوب، الدقة والطريقة. يمكن **طلب** موقع لمشترك من هنا، وفتح تحديث يظهر موقعه المعروف الأخير بشكل موثوق. هنا يؤكد المشغل نتيجة تحديد الموقع.

المؤجل

حيث تجيب علامة التبويب الموقع على LCS. **طلبات الموقع المؤجلة المعلقة** التي يحتفظ بها **المؤجل** (طلب تحديد موقع موجه للجوّال مؤجل) **MT-LR** "أين هو هذا المشترك *الآن*" ، فإن يطلب من الشبكة الإبلاغ عن موقع المشترك **لاحقًا، عندما يتم تشغيل الزناد**، بدلاً من الفور: **UE** بتسليح الطلب ويعود التقرير عندما يتم استيفاء الشرط. الزناد الشائع هو **توفر** GMLC يقوم الإبلاغ في المرة القادمة التي يصبح فيها الجهاز قابلًا للوصول، بعد أن كان غير نشط أو غير قابل للوصول عند تقديم الطلب)، **الموقع الدوري** (الإبلاغ في **فترة** ثابتة لعدد **التقارير** المحدد)، وأحداث المنطقة/الحركة (الإبلاغ عندما يدخل UE أو يغادر أو يتحرك داخل منطقة معينة). هذه هي الطريقة التي يحدد بها المشغل الموقع لمشترك لا يمكن العثور عليه في الوقت الحالي أو يحتاج إلى تتبعه على مر الزمن.

تسرد كل صف المشترك في الجلسة المؤجلة حسب **IMSI**، **طريقة** (**دوري** أو **مُشغل**)، نوعه التحديد، جدولها (فترة التقرير لجلسة دورية؛ حدث المنطقة وفترة الاستعلام لجلسة مُشغلة)، **التقارير المتبقية** من الإجمالي، **الحالة**، العميل المطلوب، متى **بدأت** ووقت **آخر تحديث**. تظهر الجلسة المُشغلة التي ليس لديها حد للتقارير *لانهائي* من التقارير المتبقية.

يمكن للمشغل **إنشاء** طلب مؤجل جديد من هنا، مع تحديد IMSI المستهدف، النوع وطريقة التحديد (خلية، E-CID، GNSS أو OTDOA):

- **دوري**: فترة التقرير بالثواني وعدد التقارير التي سيتم إرسالها.

- **مُشغل**: حدث المنطقة (**الدخول**، **المغادرة** أو **التواجد داخل**)، المنطقة نفسها (دائرة محددة بمركزها ونصف قطرها بالأمتار، أو مضلع مكون من ثلاث نقاط على الأقل من خطوط العرض/الطول)، الحد الأقصى لعدد التقارير (0 لغير المحدود) ومدى تكرار LCS لاستعلام موقع المشترك.

يمكن للمشغل أيضًا **إلغاء** جلسة معلقة في أي وقت، مما يؤدي إلى إلغاء الطلب المسلح بحيث لا يتم إنتاج المزيد من التقارير. يتم استعلام القائمة بحيث يتم تحديث حالة الجلسة مع تسليح الشبكة لها وتشغيل الزناد.

تنبيهات CAP

تنبيهات **بروتوكول التنبيه المشترك (CAP)** التي قبلها LCS للبث الخلوي، في ثلاث مجموعات:

- **في انتظار الموافقة**: تنبيهات تنتظر مشغل. **الموافقة** تبث التنبيه إلى الخلايا داخل منطقة التحذير الخاصة بها؛ **رفض** يسقطها.
- **نشطة**: تنبيهات يتم بثها. **إيقاف البث** يوقف تنبيهًا عن الهواء على كل شبكة تم إرساله عليها.
- **التاريخ**: تنبيهات تم إرسالها، رفضها، **إلغاؤها** (من قبل السلطة المصدرة أو مشغل) أو **انتهت صلاحيتها**.

والمرسل، وسطر واحد CAP معرف ،(أو تقديم يدوي CAP تغذية) تظهر كل تنبيه من أين جاءت لكل **لغة**: اللغة، **معرف الرسالة** للبث الخلوي الذي يتم إرساله عليه والنص المرسل إلى الهواتف المحمولة. عندما يتم إرسال تنبيه، يظهر كل سطر أيضًا الرقم التسلسلي ونتيجة كل شبكة. يعطي المستهدفة، عدد الخلايا التي تطابقت مع منطقة التحذير، ومتى TACs/LACs، التذييل رمز الشبكة تم استلام التنبيه، إرساله، الموافقة عليه، انتهاء صلاحيته وانتهائه.

ليس كل CAP XML. أو يمكن لمشغل **تقديم تنبيه** مع ،CAP تصل التنبيهات تلقائيًا من تغذيات قواعد التنبيه أدناه، ويتم الإبلاغ عن تقديم لا LCS مخصصة للهواتف المحمولة. يطبق CAP رسالة يتأهل بدلاً من وضعه في قائمة الانتظار:

- فقط التنبيهات **الحقيقية** ذات النطاق **العام** يتم بثها. يتم تجاهل الرسائل الاختبارية التي لا تهدف إلى البث؛
- يتم بث فقط كتل المعلومات المعلمة للتوزيع (CAP-CP)، بالنسبة لتنبيهات كندا اللاسلكي، باستخدام نصوصها اللاسلكية؛
- تخرج كل لغة كبث خاص بها: اللغة الرئيسية على معرف الرسالة المكون (4370 بشكل افتراضي) وكل لغة أخرى على معرف اللغة الإضافية المطابقة (4383)؛
- **إلغاء** أو **تحديث** من السلطة المصدرة يوقف بث التنبيه السابق، ويتوقف التنبيه عن البث عندما **تنتهي صلاحيته**؛
- يتم معالجة نفس التنبيه (نفس المرسل والمعرف) مرة واحدة فقط.

تغذيات CAP

تغذيات CAP التي يتلقى منها LCS التنبيهات. يتم دعم نوعين:

- **تدفق NAAD (كندا)**: نظام تجميع وتوزيع التنبيهات الوطنية (NAAD) من Pelmorex. يتصل LCS من كل موقع بث في وقت واحد (الموقعان يوفران تكرارًا) ويتوقع نبضة منهما كل دقيقة؛ يتم إعادة الاتصال بموقع يسكت. تسرد كل نبضة أحدث التنبيهات، وأي منها لم يصل إلى التدفق يتم جلبه من أرشيف NAAD، لذا يتم استلام تن��يه تم إصداره أثناء انقطاع الاتصال.
- **تغذية CAP Atom**: تغذية CAP بتنسيق Atom، يتم استعلامها في فترة محددة.

تظهر كل تغذية ما إذا كانت مفعلة، إعداد الموافقة الخاص بها، ولكل موقع أو عنوان URL، **حالة الاتصال**، وقت آخر نبضة (أو استعلام) وعدد: التنبيهات والنبضات المستلمة، التنبيهات **المقدمة** للبث، **المتجاهلة** (غير مخصصة للهواتف المحمولة)، **المُلغاة**، **المكررة** (نفس التنبيه من الموقع الآخر) والتنبيهات **المسترجعة** من الأرشيف.

كلا من موقعي البث NAAD **Pelmorex NAAD - إضافة تغذية** تنشئ تغذية. يملأ زر **كندا** ما إذا كانت مفعلة وسلوك URL، وعنواني الأرشيف. لكل تغذية، تحدد اسمها، نوعها، عناوين LCS، يتطلب من مشغل الموافقة على كل **الموافقة** الخاص بها: استخدام الإعداد على مستوى تنبيه، أو البث دون موافقة. يمكن تعديل التغذيات المضافة هنا، وتفعيلها أو تعطيلها، وحذفها. يتم تمييز التغذيات المعرفة في تكوين LCS وهي للقراءة فقط هنا بـ **من التكوين**.

البث

صف واحد لكل شبكة: معرف LCS، تظهر علامة التبويب **البث** رسائل **البث الخلوي** التي يدفعها عبر 2G) الرسالة واسمها (تُعلم معرفات الاختبار والتمرين بـ **اختبار**)، الرقم التسلسلي، الشبكة نص الرسالة، حالتها ومتى تم إرسالها. تعرض عرض (SBc-AP عبر 4G، SABP عبر 3G، CBSP **التاريخ** البث السابق، بما في ذلك نوع تحذيرها.

يتم عرض الرقم التسلسلي في صيغة سداسية عشرية مع **رمز الرسالة** و**رقم التحديث**؛ مرر فوقه لرؤية النطاق الجغرافي. تظهر الهواتف المحمولة الرسالة مرة واحدة فقط لكل معرف رسالة ورقم تسلسلي. يتم تمييز الصف الذي تم إرسال نفس المعرف ورقم التسلسل أكثر من مرة بـ **مكرر - الهواتف المحمولة تتجاهل**: الهواتف المحم��لة التي تلقت الإرسال الأول لم تعرض الإرسال اللاحق.

يمكن للمشغل **إيقاف** بث نشط من صفه؛ ينطبق الإيقاف على شبكة هذا الصف فقط، لذا يتم إيقاف الرسالة المرسلة على كل من 3G و4G بشكل منفصل.

إرسال بث يبدأ بثًا جديدًا:

- **معرف الرسالة**: اختر من قائمة 3GPP (ETWS/تسونامي، الزلزال، CMAS/WEA، الرئاسية، AMBER، اختبار شهري، تمرين، معرف محدد من المشغل، الشديدة، الحادة ETWS، أو أدخل قيمة مخصصة. بالنسبة لمعرفات (سلامة عامة، اختبار حكومي/محلي ETWS. اختر **نوع التحذير**
- **اللغات**: نص الرسالة، بالإضافة إلى أي عدد من **اللغات الإضافية**. يتم إرسال كل لغة إضافية على معرف اللغة الإضافية الذي يتطابق مع المختارة (على سبيل المثال 4370 → 4383)، بنفس الرقم التسلسلي، ويتم الإبلاغ عن نتيجة كل لغة. لا تحتوي معرفات ETWS والمعرفات المخصصة على معرف لغة إضافية. تحت كل نص، يظهر عداد يوضح عندما يحتوي النص على أحرف مثل بعض الحروف UCS-2 بت، أو-7 GSM) الترميز (المشددة 15 حتى، المستخدمة الصفحات وعدد.
- **الرقم التسلسلي**: مبني من **النطاق الجغرافي**، **رمز الرسالة** (0–1023) و**رقم التحديث** (0–15). يحصل التنبيه الجديد على رمز الرسالة التالي الذي لم يُستخدم بعد لذلك المعرف. **إرسال كتحديث لـ...** يختار بثًا سابقًا ويحتفظ برمزه مع زيادة رقم التحديث بواحد، لذا تستبدل الهواتف المحمولة الرسالة السابقة. يظهر تحذير عندما تم إرسال المعرف والرقم التسلسلي بالفعل، لأن الهواتف المحمولة ستتجاهل الرسالة.
- **MNC** و **MCC** للشبكة التي يتم البث إليها (مطلوب دائمًا، لذا لا يخرج البث تحت رمز الشبكة الخاطئ)، الشبكات التي سيتم الإرسال عليها، و **TACs** المستهدفة (4G)، **LACs** (2G/3G) و **SACs** (3G) للشبكات المحددة.

- مدى تكرار الرسالة وعدد مرات تكرارها (0 تكرارات حتى يتم إيقافها).

السجلات

المباشرة لاستكشاف الأخطاء وإصلاحها دون LCS تظهر علامة التبويب **السجلات** مخرجات سجل مغادرة OmniWeb.

لوحات المراقبة

تُعرض معدلات طلب الموقع وغيرها من السلاسل الزمنية كلوحات Grafana، يمكن الوصول إليها بتكرار تلك الرسوم البيانية بشكل أصلي OmniWeb من صفحة العنصر. لا تقوم.

ذات صلة

- **MME** تطلب تحديد الموقع عبر واجهات الموقع وهي نظير Diameter لـ LCS.
- **تنبيهات CAP** تغذي نظام تحذير البث الخلوي و **البث**.

خادم الترخيص: ترخيص أومنيتوتش

خادم الترخيص هو السلطة المسؤولة عن ترخيص أومنيتوتش التي تتحقق منها وظائف الشبكة. كل منتج من منتجات أومنيتوتش (MME، HSS، DRA، PGW-C، UPF، SGW-C، SMSC، CSCF وغيرها) يتحقق من استحقاقه مقابل خادم الترخيص قبل أن يعمل، سائلاً عما إذا كان **المرخص له** معينًا مرخصًا لذلك **المنتج** وما إذا كانت الرخصة لا تزال ضمن نافذة صلاحيتها. يحتفظ الخادم برخص **موقعة تشفيرياً**، كل منها يمنح مرخصًا مجموعة من المنتجات مع فترة صلاحية وبيانات وصفية، ويجيب على استفسارات الاستحقاق ويسجل كل طلب يُطلب منه. نظرًا لأن الرخصة لا تكون ذات معنى إلا مقابل ساعة موثوقة، فإن الخادم يتتبع أيضًا مصدر **الوقت الموثوق** حتى لا يمكن إحياء الرخصة من خلال إعادة ضبط ساعة العقدة. تعرض OmniWeb ما هو مرخص وصحته، سجل طلبات الاستحقاق التي قدمتها وظائف الشبكة، أداة استعلام عند الطلب، وسجلات الخادم الحية.

← دليل العمليات

خادم الترخيص هو صفحة عنصر لكل مثيل يتم الوصول إليها من الشريط الجانبي عند تشغيلها في مخزون الموقع، مع عرض أسطول حيث يتم نشر عدة منها. يمر كل حركة المرور عبر وكيل خلفي إلى واجهة برمجة تطبيقات خادم الترخيص، لذا يبقى خلف بوابة مصدقة واحدة. يفتح OmniWeb لـ رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة / الحالة

قراءة من شاشة واحدة لما يقوم الخادم بترخيصه وما إذا كان صحيًا. تعطي بطاقات الملخص عدد **المنتجات الإجمالية**، وعدد **الصالح** و**غير الصالح**، وعدد **المرخصين** المتميزين. تعرض لوحة **الوقت الموثوق** حالة مصدر ساعة الخادم: **صالح**، **فترة السماح** أو **غير صالح**. عندما يكون الوقت الموثوق غير متاح، لا يمكن للخادم التحقق من صحة الرخصة بأمان على الإطلاق، مما يرفع صحة الصفحة إلى تحذير أو خطأ.

جدول **المنتجات المرخصة** يسرد صفًا واحدًا لكل منتج مرخص، كل منها يظهر **المنتج**، مع مؤشر "الأيام) و**المرخص له** الذي مُنح له، ومتى تم **إصداره**، وتواريخ **البداية** و**الانتهاء** يومًا" الذي يتحول إلى اللون الكهرماني خلال 30 يومًا من انتهاء الصلاحية N المتبقية" أو "انتهت منذ وحالته **صالح/غير صالح**. فتح صف يوسع التفاصيل الكاملة: الطوابع ،(والأحمر بمجرد تجاوزه الزمنية الدقيقة للصلاحية، وما إذا كانت **لتوقيع التشفي** صالحًا، وأي بيانات وصفية للمنتج، والتوقيع نفسه. هذه هي أسرع تأكيد على أن وظائف الشبكة كلها مرخصة وأنه لا شيء على وشك الانتهاء.

سجلات الطلبات

سجل تدقيق لطلبات **الاستحقاق** التي قدمتها وظائف الشبكة ضد الخادم. يسجل كل صف **الطابع** **المصدر** الذي جاء منه الطلب (أي مضيف وظيفة شبكة طلب)، و**المرخص IP الزمني**، و**عنوان** **له** و**المنتج** الذي سأل عنه، و**القرار** (**مسموح** أو **مرفوض**)، وللرفض، **السبب**. يمكن تصفية **المصدر** أو **المرخص له**، **IP** القائمة حسب القرار، حسب المنتج، ووفقًا لبحث جزئي عن **عنوان** وهي مقسمة إلى صفحات. هنا يمكنك أن ترى، على سبيل المثال، أن وظيفة جديدة تم نشرها يتم رفضها لأن منتجها لم يتم ترخيصه أبدًا، أو تأكيد أن وظيفة تتحقق بنجاح.

استعلام الرخصة

تحقق من **الاستحقاق** عند الطلب. أدخل **المرخص له** و**المنتج** والأداة تسأل الخادم نفس السؤال الذي قد تسأله وظيفة الشبكة (هل هذا المرخص له له الحق في هذا المنتج الآن) وتعيد الحكم: **صالح** أو **غير صالح**، تاريخ **صالح حتى** للرخصة، **الطابع الزمني** للاستجابة، أي **بيانات وصفية**، و**التوقيع**. إنها الطريقة المباشرة لتأكيد استحقاق معين دون انتظار وظيفة المالك (على سبيل المثال `omnihss`، `omniupf`، `omnimme`) للتحقق، وتدرج معرفات المنتجات المعروفة حتى تتمكن من استعلام المنتج المحدد.

السجلات

علامة **السجلات** تتابع مخرجات السجل الحي لخادم الترخيص لاستكشاف الأخطاء وإصلاحها لمثيل واحد دون مغادرة OmniWeb.

ذات صلة

- **كل وظيفة شبكة أومنيتوتش**: MME، HSS، DRA، PGW-C، UPF، SGW-C، SMSC، CSCF وغيرها تتحقق من استحقاقها هنا؛ تظهر علامة **نظرة عامة / الحالة** الخاصة بكل منتج شارة صحة الرخصة المستمدة من هذا التحقق.

- العودة إلى فهرس العناصر: دليل العمليات.

السجلات وتتبع المشتركين

يوفر OmniWeb للمشغلين عدة طرق مكملة، في الوقت الحقيقي، لرؤية ما تفعله الشبكة:

1. **السجلات**: سجلات خدمة منظمة، حية لأي عنصر واحد، مدعومة من Loki.
2. **تتبع الجلسة**: عرض عبر الشبكة يتتبع مشتركًا واحدًا عبر كل بروتوكول وعناصر (Diameter، GTP-C، PFCP، SIP، MAP).
3. **Homer**: التقاط حزم SIP/VoIP وتحليل تدفق المكالمات.

← العودة إلى دليل العمليات

الانتقال إلى مشترك من NF

تظهر العديد من وظائف الشبكة مشتركًا أو جلسة بواسطة UE أو IMSI. تشمل هذه **MME** (UEs)، **SGW-C**، **PGW-C** و **ePDG** (الجلسات)، **MSC** و **TAS** (المشتركين)، و **SMSC** (الموقع). في كل حالة، تظهر صف من أزرار الروابط السريعة التي تت**ح لك الانتقال مباشرة إلى ذلك المشترك في مكان آخر، دون الحاجة لنسخ IMSI:

- **الذهاب إلى سجل HSS** يفتح سجل إعدادات المشترك على HSS (يتم حله بواسطة IMSI عبر مثيلات HSS المكونة).
- **عرض تتبع الجلسة** يفتح سلم الإشارة الحي للمشترك في تتبع الجلسة، محددًا لذلك IMSI.
- **عرض السجلات** يفتح علامة تبويب السجلات *لهذا* العنصر مسبقًا مصفاة لذلك IMSI، بحيث ترى فقط خطوط السجل لذلك المشترك.

أو تتبع الجلسة للموقع. لذلك، HSS وتم تكوين IMSI، تظهر كل زر فقط عندما ينطبق: يتم معرفة يتكيف هذا المجموعة مع النشر.

سلم الإشارة الحي، HSS، نقرة واحدة إلى سجل MME UE): روابط المشتركين السريعة (هنا على أو سجلات هذا العنصر المصفاة للمشترك.

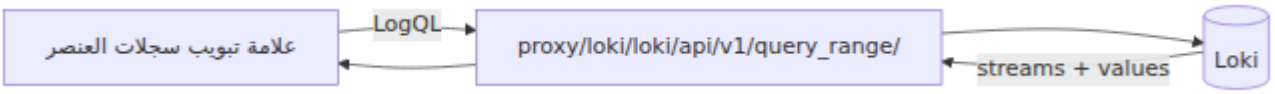
السجلات في الوقت الحقيقي (Loki)

وتبث خطوط Loki كل عنصر لديه علامة تبويب **السجلات**. تستعلم عن سجلات الخدمة للعنصر من جديدة عند وصولها، بحيث يمكنك مشاهدة عنصر حي أثناء إجراء تغيير أو إعادة إنتاج مشكلة.

مع فلاتر Loki، خطوط سجل منظمة، ملونة تم بثها من (UPF هنا على): علامة تبويب السجلات (IMSI). الخدمة، الشدة، البروتوكول، والمشترك. كل عنصر يكشف نفس العرض.

كيفية عمل استعلامات السجل

في الخلفية. لا يستعلم أي شيء عن Loki ويرسله عبر بوابة LogQL يبني الواجهة الأمامية استعلام Loki مباشرة من المتصفح. يتم توجيهه (وبالتالي يتم التحقق من هويته وتدقيقه) مثل أي طلب آخر.



الافتراضي) `LOKI_URL` في الخلفية بواسطة متغير البيئة Loki يتم تعيي هدف `http://localhost:3100`). تستخدم الاستعلامات واجهة برمجة التطبيقات للاستعلام عن LogQL، مع تعبير Loki النطاق في نافذة زمنية، حد نتائج، واتجاه (الأحدث أولاً أو الأقدم أولاً).

المحددات مقابل فلاتر الأنابيب

يبني OmniWeb استعلامات منظمة من نوعين من الفلاتر:

مكان الفلتر	موقع LogQL	مثال	الاستخدام
محدد	داخل محدد التدفق `{ … }`	`{hostname="omni-eval-upf01"}`	اختر أي التدفقات (أي مضيف/خدمة) للقراءة. مفهرسة وسريعة.
أنبوب	بعد `|`	`| level="error"`	تصفية الخطوط المطابقة بواسطة حقل منظم.

تثبّت علامة تبويب سجلات العنصر النموذجية المضيف/الخدمة كمحدد وتتيح لك إضافة فلاتر أنابيب تصدر **خطوط** Omnitouch (الشدة، المكونات، معرفات المشتركين) فوقها. نظرًا لأن خدمات **سجلات منظمة**، يمكنك التصفية على حق��ل حقيقية بدلاً من البحث في نصوص حرة.

بيانات السجلات المنظمة

تشحن المضيفات سجلات منظمة إلى Loki (مكونة بواسطة دور Ansible الشائع). مصدران منظمين مفيدان بشكل خاص:

- **سجلات الخدمة**: الإخراج المنظم الخاص بكل NF، معنون بواسطة `hostname`/الخدمة، متاح في علامة تبويب سجلات ذلك العنصر.
- **تدقيق الأوامر**: كل أمر تم تنفيذه على مضيف، بما في ذلك من قام بتسجيل الدخول الفعلي، الثنائي، الدليل العامل، والسطر UID، `sudo`/`su` البقاء على قيد الحياة). انظر تسجيل التدقيق للحصول على مرجع الحقول الكامل للأمر. تم شحنه إلى Loki.

استخدام علامة تبويب السجلات

1. افتح أي عنصر واختر **السجلات**.
2. يقوم العارض بتحميل الخطوط الحديثة لذلك العنصر ويبدأ في الاستعلام عن خطوط جديدة.
3. إذا كانت IMSI/MSISDN مثل الشدة، أو) قم بتضييق العرض باستخدام فلاتر الأنابيب سجلات الخدمة تتضمنها).
4. اضبط نافذة الوقت للرجوع إلى حدث سابق.
5. أوقف الاستعلام (مؤشر الرأس) للحفاظ على عرض ثابت أثناء القراءة.

> **نصيحة:** عند التحقيق في مشترك واحد، فإن تصفية سجلات العنصر بواسطة IMSI/MSISDN هي الخطوة السريعة الأولى؛ لرؤية المشترك عبر *عناصر* متعددة في وقت واحد، استخدم تتبع الجلسة أدناه.

تتبع الجلسة: متابعة مشترك عبر الشبكة

محرك **تتبع الجلسة** يربط الإشارات لمشترك واحد عبر عناصر وبروتوكولات متعددة، مما يوفر جدول زمني موحد من الاتصال اللاسلكي إلى المصادقة، إنشاء الجلسة، وتسليم المكالمات/SMS. هذه هي الأداة للإجابة على "ماذا حدث لهذا المشترك؟" دون القفز بين واجهات سطر الأوامر للعناصر.

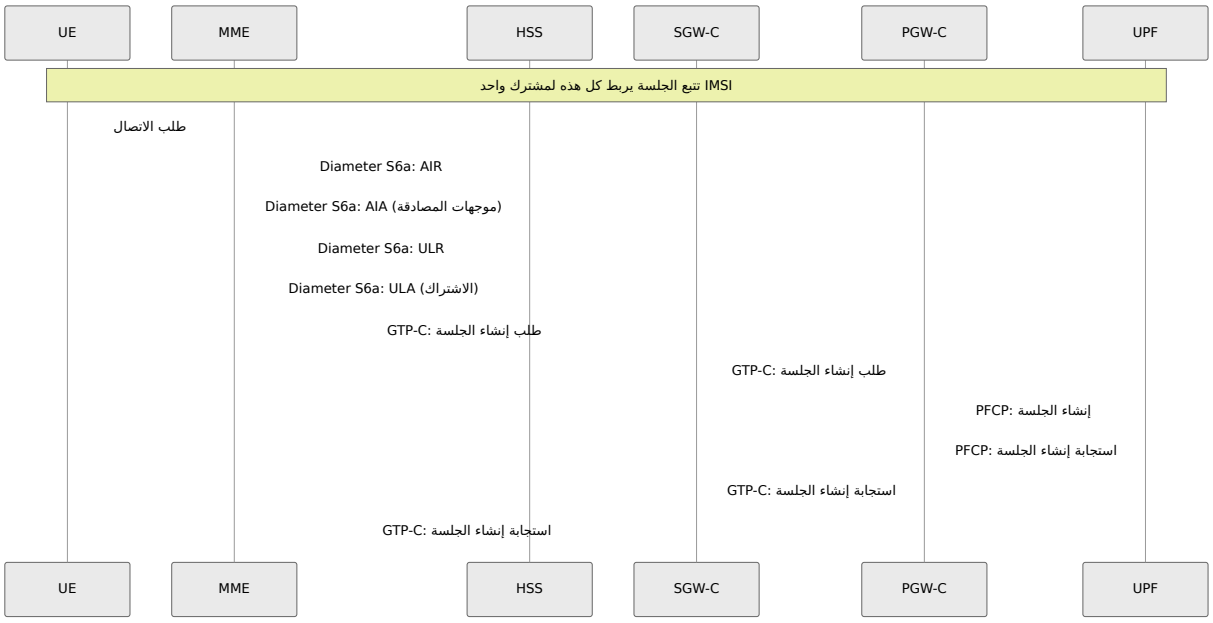
تتبع الجلسة: البحث بواسطة IMSI أو MSISDN وربط نشاط المشترك عبر Diameter، GTP-C، PFCP، SIP، و MAP، مع علامات تبويب لكل بروتوكول عبر الأعلى.

البروتوكولات المدعومة

البروتوكول	ما يظهره	العناصر المعنية
Diameter	المصادقة، السياسة، الشحن	HSS، DRA، PGW-C، PCRF، OCS، CSCF (Cx/Dx/Rx)
GTP-C	إدارة الجلسة (S5/S8، S11)	SGW-C، PGW-C، MME
PFCP	قواعد جلسة المستخدم (N4)	PGW-C/SMF ↔ UPF
SIP	التحكم في مكالمات IMS	P-CSCF، I-CSCF، S-CSCF، TAS
MAP	الموقع SS7، المصادقة، SMS	MSC، HLR، CAMEL GW، IP-SM-GW

تتبع المستخدم

ورؤية كل تفاعل بروتوكولي **MSISDN** أو **IMSI** تتيح لك عرض **تتبع المستخدم** البحث بواسطة مرتبط لذلك المشترك عبر الشبكة. على سبيل المثال، يكشف الاتصال الواحد عن المصادقة Diameter، وإنشاء جلسة GTP-C، وتثبيت قاعدة PFCP كسلسلة متماسكة واحدة:



علامات تبويب محددة للبروتوكول

يمتلك كل بروتوكول علامة تبويب خاصة به (**Diameter، GTP-C، PFCP، SIP، MAP**)، بالإضافة إلى نظرة عامة **على جميع البروتوكولات**. تعتبر علامات التبويب الخاصة بالبروتوكول لمكالمة SIP مثل فقط تبادل) وجهات نظر مصفاة. تساعد عندما تتعقب مشكلة محددة بالبروتوكول VoLTE) بدلاً من متابعة مشترك واحد عبر كل شيء.

سلم PCAP

التقاط الحزم إلى سلم: رسم بياني متسلسل زمني للإشارات. **PCAP** تحول علامة تبويب **سلم** على سبيل المثال من جهاز شبكة أو تتبع على مستوى) PCAPNG أو PCAP ق�ّ بتحميل التقاط والدور المستنتج IP بتحليل الحزم، وتحديد عقد الإشارة بواسطة عنوان OmniWeb و يقوم (العنصر ويربط الطلبات باستجاباتها في جلسات. يتم رسم ،(وما إلى ذلك ،S-CSCF ،HSS ،MSC/VLR) النتيجة كسلم رسائل عبر تلك العقد، مرتبة زمنياً، بحيث يمكنك قراءة تبادل كامل من الأعلى إلى الأسفل بنظرة واحدة.

التقاط تم تحميله تم عرضه كسلم عبر العقد المكتشفة. انقر على أي رسالة لرؤية :PCAP سلم إطارها المفكك والهيكس.

انقر على رسالة في السلم لفتح فكها الكامل والهيكس الخام، نفس التفاصيل التي ستحصل عليها من محلل البروتوكولات. تتعرف الأداة على عائلات الإشارات التي تواجهها عبر نواة الهاتف

المحمول: MAP، CAMEL، TCAP، Diameter، SIP، GTP-C، PFCP، و GSM SMS. يتم سرد كل التقاط تقوم بتحميله على علامة التبويب بحيث يمكن إعادة فتحه أو مشاركته مع زميل بدلاً من تمرير الملف.

التدفقات الحية

تظهر علامة تبويب **التدفقات الحية** نفس عرض السلم، ولكن مصدرها مباشرة من سجلات الإشارات المنظمة للشبكة (عبر Loki) بدلاً من ملف تم تحميله. مع إصدار عناصر الشبكة لبيانات IMSI، دون الإشارات، تظهر تدفقات المكالمات الحديثة لكل مشترك هنا تلقائيًا، مجمعة حسب PCAP، بحيث تكون التدفق الحاجة لتحميل أي التقاط. اختر تدفقًا لإعادة بنائه إلى نفس السلم مثل الحي غنية مثل واحدة تُقرأ من ملف، حتى إلى فك الرسالة والهيكس.

التدفقات الحية: تدفقات المكالمات الحديثة المستمدة مباشرة من بيانات الإشارات للشبكة. قم بالتصفية حسب IMSI، العقدة، أو البروتوكول، ثم افتح تدفقًا لرسم سلمها الحي.

ولكن من بيانات الشبكة، PCAP بإعادة بنائه إلى نفس السلم مثل OmniWeb افتح تدفقًا و يقوم لمشترك واحد، مرتبط عبر كل LTE الخاصة، دون الحاجة لالتقاط أو تحميل. المثال أدناه هو اتصال وتحديث الموقع ضد Diameter S6a المصادقة، **eNodeB** مع S1AP/NAS عنصر لمسه: تبادل كل هذا يظهر على سلم واحد مرتب زمنياً، **PGW-C** و **SGW-C** عبر GTP-C وإعداد جلسة **HSS**، مع أوقات جولة الطلب/الاستجابة لكل رسالة وفك كامل على بعد نقرة واحدة.

تدفق حي تم فتحه إلى سلم: اتصال LTE لمشترك واحد عبر eNodeB و MME و HSS و SGW-C، انقر على أي رسالة لفكها والهيكس، GTP-C. و Diameter S6a و S1AP مرتبط بين PGW-C و أو أي عقدة للتركيز على تبادلاتها.

إذا لم يكن هناك بيانات إشارات تتدفق بعد، تظهر علامة التبويب حالة فارغة؛ تتعبأ التدفقات تلقائيًا عندما تبدأ عناصر الشبكة في إصدار بيانات الإشارات.

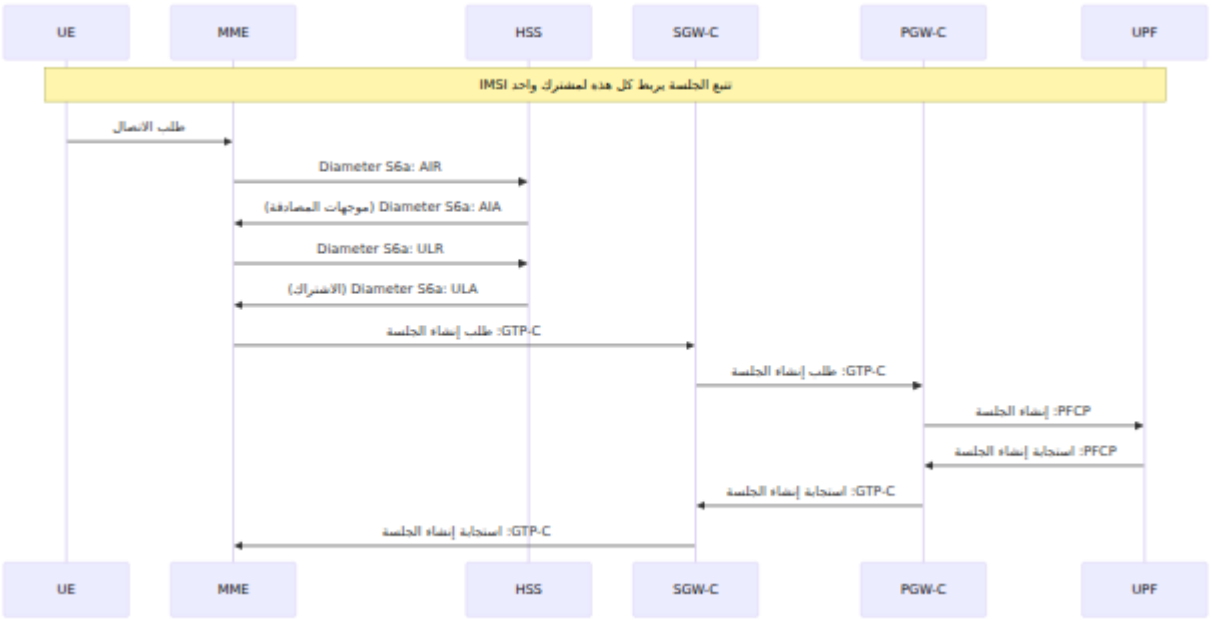
Homer: التقاط SIP وتحليل تدفق المكالمات

يتكامل OmniWeb مع Homer، منصة التقاط SIP مفتوحة المصدر وتحليل VoIP، لتصور تدفق المكالمات SIP الملتقطة. حيث يقدم تتبع الجلسة بعمق، فك البروتوكولات، والبحث عبر إشارات التفاصيل الكاملة، رسالة تلو الأخرى، لحزم Homer *ملخصًا* عبر البروتوكولات لمشترك واحد، يقدم SIP.

التوفر والوصول

Homer من OmniWeb هو **اختياري** ويتم اكتشافه تلقائيًا. عند بدء التشغيل، يتحقق `/api/homer/status`:

- إذا تم تكوين Homer (`HOMER_URL` تم تعيينه في الخلفية) وقابل للوصول، تظهر إدخال **Homer** في الشريط الجانبي.
- إذا لم يتم نشر Homer، يتم ببساطة إخفاء الإدخال، ولا يتغير ي آخر.



في علامة تبويب متصفح جديدة. المصادقة شفافة: Homer يفتح واجهة ويب **Homer** النقر على الخاص بك عبر نفس تسجيل الدخول الموحد OmniWeb تتحقق البوابة من تسجيل دخول المستخدم لـ Grafana، يتم تكوين `HOMER_URL` في الخلفية و) لذا لا يوجد تسجيل دخول ثانٍ. `HOMER_PROXY_SECRET`، عند تعيينه) للتكامل.

حالات الاستخدام

Homer هو الأداة التي يجب الوصول إليها عندما تكون المشكلة في طبقة SIP نفسها:

- **تحليل تدفق مكالمات VoLTE**: تتبع تسلسلات SIP `INVITE`/`BYE` عبر P-CSCF، I-CSCF، S-CSCF، و TAS.
- **استكشاف أخطاء VoWiFi**: تحليل تفاعلات SIP بين ePDG ↔ P-CSCF.
- **تصحيح تسجيل IMS**: فحص تبادلات `REGISTER` / `401` / `REGISTER` / `200 OK`.
- **مشكلات الاتصال**: التقاط إشارات SIP-trunk بين MSC ونظراء SIP.

Homer تتبع الجلسة مقابل

كلاهما يساعد في استكشاف الأخطاء، لكنهما يجيبان على أسئلة مختلفة. هما تكميليان، وليس بدائل:

الأداة	الأفضل لـ	النطاق	أين تفتح
تتبع الجلسة	"اتبع هذا المشترك عبر الشبكة بأكملها"	Diameter، GTP-C، PFCP، SIP، MAP مرتبطة بواسطة IMSI/MSISDN	داخل OmniWeb
Homer	"أرني الرسائل SIP الدقيقة لهذه المكالمة"	إشارات SIP/VoIP، فك كامل للحزم (VoLTE/VoWiFi/IMS)	علامة تبويب جديدة (اكتشاف تلقائي)

للحصول Homer في تتبع الجلسة، ثم الانتقال إلى SIP تدفق شائع هو اكتشاف شذوذ متعلق بـ على تدفق المكالمات التفصيلي.

استكشاف الأخطاء

لا تظهر السجلات في علامة تبويب سجلات عنصر

الأعراض: علامة تبويب السجلات فارغة أو تظهر "ل�� توجد نتائج".

الأسباب المحتملة:

- لا يمكن الوصول إلى Loki من الخلفية (`LOKI_URL` غير مكون بشكل صحيح).
- شحن السجلات غير قيد التشغيل / غير مكون (المضيف لا يشحن السجلات إلى Loki بشكل صحيح).
- نافذة الوقت المحددة سابقة للسجلات المتاحة، أو لا يتطابق تسمية المضيف.

الحل:

1. تأكد من أن `LOKI_URL` يشير إلى مثيل Loki يمكن الوصول إليه.

2. تحقق من أن مضيف العنصر يشحن السجلات (تحقق من وكيل شحن السجلات على ذلك المضيف).
3. قم بتوسيع نافذة الوقت وإزالة فلاتر الأنابيب للتأكد من وصول أي خطوط.

لا يعيد تتبع الجلسة أي شيء لمشترك

الأعراض: يظهر تتبع المستخدم بواسطة IMSI/MSISDN عدم وجود أحداث.

الأسباب المحتملة:

- كان المشترك غير نشط في النافذة المحددة.
- تم كتابة المعرف بشكل خاطئ (IMSI مقابل MSISDN).
- مصادر التتبع للبروتوكول المعني لا تغذي المحرك.

الحل:

1. تحقق مرة أخرى من المعرف وحاو�ّ البديل (IMSI ↔ MSISDN).
2. قم بتوسيع نافذة الوقت.
3. تأكد مع علامة تبويب سجلات العنصر الخاصة أن المشترك كان نشطًا على الإطلاق.

مفقود من الشريط الجانبي Homer إدخال

الأعراض: لا يظهر رابط **Homer**.

الأسباب المحتملة:

- لم يتم نشر Homer، أو لم يتم تعيين `HOMER_URL` في الخلفية.
- Homer غير قابل للوصول، لذا فإن `/api/homer/status` يبلغه بأنه غير متاح.

الحل:

1. تأكد من نشر Homer و `HOMER_URL` تم تعيينه في خلفية OmniWeb.
2. تحقق من أن الخلفية يمكنها الوصول إلى Homer، ثم أعد تحميل OmniWeb (يتم تشغيل الاكتشاف عند بدء التشغيل).

MME: كيان إدارة الحركة

الـ **MME** هو نقطة التحكم في شبكة EPC. ينهي **S1AP** مع eNodeBs، وينفذ إجراءات الاتصال، والمصادقة، والحركة لكل جهاز مستخدم (UE)، ويحتفظ بسجل **سياق** لكل مشترك متصل. **UE** يقوم بجلب بيانات الاشتراك والمصادقة من HSS عبر **S6a** (Diameter)، ويقوم بإعداد الدوائر والأنظمة الأخرى عبر MME وينسق عمليات الانتقال بين **S10/N26**. على بوابة الخدمة عبر **S11**. باختصار، هو العقدة التي تقرر أين وكيف يتصل كل مشترك، وكيف يتم استدعاؤه ويتنقل عبر الشبكة. تعرض OmniWeb eNodeBs الحية لـ MME، وسياقات UE، وSGW، ونظراء Diameter، وحالات الواجهة، وحالة الانتقال. الاتجاهات طويلة الأمد متاحة على لوحات Grafana التي يمكن الوصول إليها من نفس الصفحة.

← دليل العمليات

هو صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيله في جرد MME الـ الموقع، وعندما يتم نشر عدة منها، يتم عرض حالة الأسطول بشكل مجمع. كل حركة المرور تمر عبر وكيل الخلفية OmniWeb إلى واجهة برمجة التطبيقات (API) الخاصة بـ MME، لذا تبقى خلف البوابة المعتمدة الوحيدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

وملخص لحملها الحي، بما في ذلك MME لـ **API** قراءة صحة على شاشة واحدة: **حالة** **Diameter** (S6a). إنها وحالة نظراء **SGW** المتصلة، و**نظراء UEs** المتصلة، و **eNodeBs** يعمل ورؤية مقدار الشبكة التي يخدمها MME أسرع طريقة لتأكيد أن.

eNodeBs

كل eNodeB يرتبط به MME عبر S1AP، **معرف** كل صف يظهر **eNB حالة** و**العالمي**، الاسم المتصلة به. يمكن UEsو TACsلعرض سياقه: الخلايا والخدمات المقدمة و eNodeB الاتصال. افتح MME عبر مجموعة UEs مما يعدل كيفية توزيع eNodeB، المعلنة لـ **MME** للمشغل **تحديث سعة** (للصيانة أو إعادة التوازن MME يستخدم لتفريغ أو وزن).

UEs

مع حالة الاتصال والحركة **GUTI**و **IMSI** لكل مشترك متصل، كل صف مفاتيح بواسطة **UE** سياق UE: يظهر سياقه الكامل. تتوفر مجموعة من الإجراءات لكل UE الخادم. فتح eNodeBو

- **استدعاء** UE.
- **إرسال إلى وضع الخمول**: تحرير الاتصال اللاسلكي مع الاحتفاظ بالسياق.
- **تفريغ** UE إلى MME آخر.
- **طلب إعادة الاتصال**: إجبار UE على إعادة الاتصال.
- **إرسال SMS** إلى UE.
- **حذف** سياق UE: مسح مشترك عالق أو قديم.

لتحديد المشتركين المحليين مقابل IMSI لـ **PLMN** / يمكنك أيضًا **البحث عن المشغل** المشتركين المتجولين.

نظراء S-GW

للنظير، و**حالة IP** كل صف يظهر، (GTP-C) **S11** عبر MME بوابات الخدمة التي يتحدث إليها و**عدد الجلسات** المرتبطة بتلك **(الاسترداد) GTP النشاط / الوصول**، وعداد **إعادة تشغيل** بإعادة إنشاء الجلسات التي كان MME مما يخبر، S-GW البوابة. يتم زيادة العداد عند إعادة تشغيل **S-GW** أو كان إدخالًا **ثابتًا** يظهر بجانب **طريقة اختيار DNS** يحتفظ بها. سواء تم تعلم نظير عبر للمشتركين المحليين والمتجولين. افتح نظيرًا لسرد **الجلسات** التي يحملها، كل MME التي يطبقها MME نقاط نهاية النفق على جانب) الخاصة به **TEIDs S11** مع **IMSI** منها معرف بواسطة عبرها. يساعد ذلك UE تعمل ويرى كيفية توزيع جلسات S-GWs هنا يؤكد المشغل أي .(S-GWو عند موازنة الحمل أو تشخيص سبب انقطاع الدوائر لمجموعة من المشتركين مع بوابة واحدة.

S10 وتفريغ GUTI إعادة تخصيص

بدلاً من كل صف IMSI تُدفع عمليتان للحركة بواسطة:

- **إعادة تخصيص GUTI**: إعادة تخصيص **GUTI** لمشترك متصل لتحديث الهوية المؤقتة التي يقدمها UE (تستخدم عند تدوير المعرفات أو مسح عدم تطابق الهوية).
- **تفريغ S10**: إجبار تفريغ مشترك محدد من **MME** إلى **آخر**. هذا ينقل سياق مشترك عبر S10، هذا MME ويكمل التحكم في سعة eNodeB عند تفريغ MME.

S10

عند انتقاله بين UE هي المسار الذي يتم من خلاله نقل سياق **MME بين S10/N26** واجهة للتشغيل البيني بين AMFو MME بين ،**N26** وعبر) أو **الانتقال TAU** في مجموعة خلال MMEs تحتوي علامة التبويب على جزئين. تسرد **الانتقالات النشطة** عمليات النقل قيد .(EPC 5وGC الذي يتم نقله، بحيث يمكن **IMSIالهدف** و **MMEالمصدر** و **MME** التنفيذ، كل منها يظهر **النظير** كيف يجد **MME** للمشغل متابعة حدث الحركة أو اكتشاف حدث عالق. تعرض **اكتشاف** التي يجريها وأي نظراء **ثابتين** تم **DNS / NAPTR** نظراءه في المجموعة: عمليات البحث MME صحية MME وعنوان كل نظير. هنا تؤكد أن الحركة بين (FQDN) تكوينهم، مع اسم المجال المؤهل يمكنه فعلاً الوصول إلى الجيران الذين يحتاجهم لنقل السياقات. يكمل ذلك إجراء **تفريغ** MME وأن **S10** لكل مشترك المدفوع من علامة تبويب UEs.

Diameter

كل صف يظهر **مضيف** النظير، **S6a** عبر HSS بشكل رئيسي، Diameter لـ MME نظراء و**النطاق** و**حالة** الاتصال. افتح نظيرًا لعرض تفاصيله. هنا تؤكد أن مسار المصادقة والاشتراك إلى HSS يعمل عندما تفشل الاتصالات.

الواجهات

عرض MME في مكان واحد: **S1AP** إلى eNodeBs، **GTP-C** (S11) إلى SGW، **Diameter** لـ **S6a** (HSS) و**SLg** (خدمات الموقع)، **SGsAP** (إلى MSC لاحتياطي CS وSMS)، **LCS-AP / SLs** (خدمات الموقع)، و**S10/N26** (الانتقال بين MME والتشغيل البيني بين EPC 5وGC). إنها الشاشة الوحيدة لتأكيد أي من مسارات الإشارة الخاصة بـ MME تعمل وأيها معطلة.

السجلات

تعرض سجل **السجلات** علامة تبويب MME الحي لتشخيص MME واحد دون مغادرة OmniWeb.

لوحات المراقبة

تُعرض MME ومعدلات الانتقال وغيرها من السلاسل الزمنية لـ UEs، معدلات الاتصال، وعدد كلوحات Grafana، لا تقوم OmniWeb يمكن الوصول إليها من صفحة العنصر. بتكرار تلك الرسوم البيانية بشكل أصلي.

ذات صلة

- يحتفظ **HSS** ببيانات الاشتراك والمصادقة التي يجلبها MME عبر **S6a**.
- **SGW-C** هو النظير التحكم عبر **S11**. يدير MME إعداد الجلسات والدوائر عليه.
- يتم الوصول إلى **MSC** عبر **SGsAP** لاحتياطي CS وSMS.
- يتم الوصول إلى **MMEs** الأخرى عبر **S10** للحركة بين MME، و**AMF** عبر **N26** للانتقال من EPC 5 إلىGC.

مرجع أوامر AT لجهاز Quectel EP06 (اختبار الشبكة الخلوية)

مرجع لوحدة التحكم في مودم أجهزة الاختبار. يستهدف **Quectel EP06** (البرمجيات الثابتة `EP06ELAR04A05M4G`، IMEI `868186042000040`) على حاوية المختبر، ولكنه ينطبق على عائلة EP06 الحي؛ استجابات الأمثلة هي تم اختبار كل أمر أدناه ضد EC25 / EG06 / EG06 / EM06. كان في حالة `NO SERVICE / SEARCH` (**استجابات حقيقية تم التقاطها من ذلك المودم** في ذلك الوقت، لذا كانت حقول الإشارة فارغة، ويجب أن تتعامل المحللات مع ذلك).

التحويل هو طلب/استجابة: `sendModemAt(serial, command, readMs, timeoutMs)` → backend `modem_at` → agent `modem.run_at(serial, command, min_read, timeout)`. `min_read` يستمر في قراءة المنفذ لمدة لا تقل عن ذلك حتى يتم التقاط URCs غير المتزامنة قبل أن تعود المكالمة. لا يوجد **تدفق** **URC** أدناه "تسجيل الأحداث". انظر **دائم**.

معلومات الجهاز / SIM

الأمر	الغرض	الاستجابة الحية
`ATI`	الشركة المصنعة / الطراز / البرنامج الثابت	`Quectel` / `EP06` / `Revision: EP06ELAR04A05M4G`
`AT+CGMM`	الطراز	`EP06`
`AT+CGMR`	إصدار البرنامج الثابت	`EP06ELAR04A05M4G`
`AT+CGSN`	IMEI	`868186042000040`
`AT+CIMI`	IMSI	(SIM IMSI)
`AT+QCCID`	ICCID	(SIM ICCID)
`AT+CPIN?`	حالة PIN لـ SIM	`+CPIN: READY`

الإشارة / القياس

الأمر	الغرض	الاستجابة الحية
`AT+CSQ`	RSSI/BER (قديم)	`+CSQ: 99,99` (99 = لا إشارة). dBm = `-113 + 2*rssi`.
`AT+QCSQ`	إشارة لكل RAT	`+QCSQ: "NOSERVICE"`. عند الاتصال: `+QCSQ: "LTE",<rssi>,<rsrp>,<sinr>,<rsrq>`.
`AT+QNWINFO`	RAT الحالي / النطاق / القناة	`+QNWINFO: No Service`. عند الاتصال: `+QNWINFO: "FDD LTE","<mccmnc>","LTE BAND 3",1850`.
`AT+QENG="servingcell"`	قياسات الخلية الخدمية الكاملة	`+QENG: "servingcell","SEARCH"` (خامل). انظر التنسيق أدناه.
`AT+QENG="neighbourcell"`	خلايا الجوار	`OK` (لا شيء عند عدم التخييم).

تنسيق LTE لـ `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 (جميعها أعداد صحيحة موقعة).
- `SINR` **محولة** هو قيمة: dB `(1/5)` = الفعلي`*SINR - 20` (→ النطاق 0..250 dB).
- `cellID`/`PCI`/`EARFCN` عادة ما تكون بالصيغة السداسية العشرية/العشرية لكل حقل؛ `band` هو مؤشر نطاق LTE.

تنسيق LTE لـ `AT+QENG="neighbourcell"`

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

التسجيل / الاتصال

الأمر	الغرض	الاستجابة الحية
`AT+CFUN?`	وظيفة الراديو	`+CFUN: 1` (كامل). وضع الحد الأدنى/الطائرة = `0`.
`AT+CEREG?`	تسجيل EPS	`+CEREG: 2,2` (2 = البحث).
`AT+CEREG=2`	تمكين URC التسجيل **مع الموقع** (TAC/cellID)	`OK`
`AT+CGATT?` / `AT+CGATT=1` / `=0`	حالة الاتصال PS / الاتصال / فصل الاتصال	`+CGATT: 0`
`AT+COPS?`	اختيار المشغل الحالي	`+COPS: 0` (تلقائي، غير مسجل).
`AT+COPS=?`	**مسح الشبكة** (بحث عن المشغل، بطيء)	قائمة من `(stat,"long","short","numeric",AcT)` tuples.
`AT+COPS=0`	اختيار المشغل تلقائيًا	`OK`
`AT+COPS=1,2,"<mccmnc>"[,<AcT>]`	اختيار يدوي حسب المعرف الرقمي	`OK`

RAT / قفل الخلايا / النطاقات

الأمر	الغرض	الاستجابة الحية
`AT+QNWLOCK=?`	القدرات	`+QNWLOCK: "common/4g",<num of cells>,[[<freq>,<pci>],...]` و `+QNWLOCK: "common/lte"[,<action>[,<EARFCN>,<PCI>[,<status>]]]`
`AT+QNWLOCK="common/4g"`	استعلام عن قفل الخلية	`+QNWLOCK: "common/4g",0` (O بعد القفل(خلايا = لا قفل ؛ `+QNWLOCK: "common/4g",1,1850,0`.
`AT+QNWLOCK="common/4g",<n>,<EARFCN>,<PCI>[,<EARFCN>,<PCI>...]`	**قفل** على n خلايا (يعمل على هذا البرنامج الثابت)	`OK`
`AT+QNWLOCK="common/4g",0`	**فتح القفل**	`OK` (يمسح القفل).
`AT+QNWLOCK="common/lte"`	استعلام عن قفل LTE لخلية واحدة (للقراءة فقط)	`+QNWLOCK: "common/lte",0,0,0,0`.

سلوك البرنامج الثابت (تم التحقق منه مباشرة على `EP06ELAR04A05M4G`):
الشكل `common/4g` هو الشكل الذي يقبل *إجراء* قفل على هذه الوحدة. `AT+QNWLOCK="common/4g",1,<EARFCN>,<PCI>` يقفل (يعود `OK`، و (يستمر القفل `common/lte` (`...,1,` يمسحه. الأشكال *المجموعة* لـ `AT+QNWLOCK="common/4g",0`

على هذا البرنامج الثابت، لذا فإن `ERROR` جميعها تعود (و `0,...` `<EARFCN>,<PCI>` لكل من `common/4g` `common/lte` هنا للقراءة فقط. لذلك، تستخدم واجهة المستخدم القفل وفتح القفل. | `AT+QCFG="band"` | استعلام عن قناع النطاق | `+QCFG: "band",0x8d0,0x1a0880800d5,0x0` = (قناع GSM، قناع LTE، قناع TDS). | | `AT+QCFG="band",0,<lte_hex_mask>,0` | **قفل النطاق** (LTE). `0x0` قناع LTE = جميع النطاقات. | `OK` | | `AT+QCFG="nwscanmode"` | وضع مسح RAT | `+QCFG: "nwscanmode",0` (0 = تلقائي، 1 = GSM، 2 = WCDMA، 3 = LTE). | | `AT+QCFG="nwscanmode",<m>[,1]` | تعيين تفضيل RAT (`,1` = ساري المفعول على الفور) | `OK` | | `AT+QCAINFO` | معلومات تجم��ع الناقل | `OK` (لا شيء مجمع عند الخمول). |

قناع نطاق LTE: بت (`band-1`)، أي النطاق N → `1 << (N-1)`. على سبيل المثال، B3 = `0x4`، B7 = `0x40`، B28 = `0x8000000`. `0x0` (أو جميع الأحاد) = جميع النطاقات مفعلة.

> **ملاحظة البرنامج الثابت:** `AT+QCFG="nwscanseq"` تعود `ERROR` على هذا البرنامج الثابت EP06 (`EP06ELAR04A05M4G`). واجهة المستخدم لا تعرضه. `AT+QSCAN` أيضًا غير مدعوم على هذا البرنامج الثابت EP06 (إنه أمر من سلسلة RG/RM 5G). يستخدم مسح الشبكة `AT+COPS=?` بالإضافة إلى `AT+QENG` بدلاً من ذلك.

المكالمات الصوتية (VoLTE / IMS)

صوت EP06 هو **VoLTE**: يحتاج إلى تسجيل **فقط** IMS عبر LTE. `AT+QCFG="ims"` على هذه الوحدة تعود `+QCFG: "ims",1,0` (تم تمكين IMS 0 بواسطة الإعداد، الحالة الحالية).

الأمر	الغرض
`AT+QCFG="ims"`	استعلام/تمكين IMS. `AT+QCFG="ims",1` لتمكينه بالقوة.
`ATD<number>;`	إجراء مكالمة صوتية (علامة `;` = صوت، وليس بيانات).
`ATA`	الرد على مكالمة واردة.
`ATH` / `AT+CHUP`	إنهاء المكالمة.
`AT+CLCC`	قائمة المكالمات الحالية: `+CLCC: <id>,<dir>,<state>,<mode>,<mpty>,"<number>",<type>`. فارغ `OK` = لا توجد مكالمات.
`AT+CLIP=1`	تمكين URC معرف رقم المتصل (`+CLIP:`) عند `RING`.

`AT+CLCC`: 0 في نشطة، 1 محتفظ بها، 2 في الاتصال، 3 في التنبيه، 4 واردة، 5 في حالات مكالمات الانتظار.

الرسائل القصيرة (وضع النص)

الأمر	الغرض	الاستجابة الحية
`AT+CMGF=1`	وضع النص (مقابل PDU)	`OK`
`AT+CPMS?`	مناطق التخزين / العد	`+CPMS: "ME",0,255,"ME",0,255,"ME",0,255`
`AT+CMGL="ALL"`	قائمة الرسائل (وضع النص)	لكل رسالة: `+CMGL: <index>,"<stat>","<sender>",,"<timestamp>"` ثم سطر الجسم.
`AT+CMGR=<index>`	قراءة رسالة واحدة	`+CMGR: "<stat>","<sender>",,"<timestamp>"` + الجسم.
`AT+CMGS="<number>"` ثم الجسم + Ctrl-Z	إرسال (يتم التعامل معه بواسطة الوكيل `send_sms`).	`+CMGS: <mr>`
`AT+CMGD=<index>[,<delflag>]`	حذف الرسالة (`delflag` 4 = الكل).	`OK`
`AT+CNMI?` / `AT+CNMI=2,1,0,0,0`	إعدادات مؤشر الرسائل الجديدة	`+CNMI: 2,1,0,0,0`

البيانات / PDP

الأمر	الغرض	الاستجابة الحية
`AT+CGDCONT?`	قائمة سياقات PDP (APNs)	`+CGDCONT: 1,"IPV4V6","ims",...`
`AT+CGDCONT=<cid>,"<type>","<apn>"`	تعيين السياق. الأنواع: IP، IPV6، IPV4V6، Non-IP.	`OK`
`AT+CGACT=1,<cid>` / `=0,<cid>`	تفعيل / إلغاء تفعيل السياق.	`OK`
`AT+CGPADDR[=<cid>]`	عرض IP المعين.	`+CGPADDR: 1,"<ip>"`
`AT+CGCONTRDP=<cid>`	DNS / بوابة / PCO.	`+CGCONTRDP: ...`
`AT+QPING=1,"<host>"`	Ping من المودم (يحتاج URC استجابات؛ إلى `min_read`).	`+QPING: ...`

وقيود التحويل :(URCs) تسجيل الأحداث

التحويل عبر الوكيل هو **طلب/استجابة مع منفذ مفتوح لكل مكالمة**. يفتح المنفذ التسلسلي، ثم يغلق. لا يحتفظ بالمنفذ, (`min_read` أو تنقضي) يرسل أمرًا واحدًا، يقرأ حتى OK/ERROR مرة أخرى إلى المتصفح. لذا، فإن تدفق الأحداث (URCs) مفتوحًا لبث أكواد النتائج غير المطلوبة الحي الحقيقي غير ممكن من خلال هذا المسار دون تغ��يرات في الوكيل.

URCs التي تستحق التمكين (لمرة واحدة `OK` كل منها أمر):

الأمر	URC يمكّن
`AT+CEREG=2`	`+CEREG:` تغييرات التسجيل (مع TAC/cellID).
`AT+CGEREP=2,1`	`+CGEV:` أحداث PS/حامل.
`AT+CLIP=1`	`+CLIP:` معرف المتصل عند `RING`.
`AT+CNMI=2,1,0,0,0`	`+CMTI:` مؤشر SMS جديدة.
`AT+QINDCFG="all",1`	`+QIND:` مؤشرات Quectel.

النهج العملي المستخدم في واجهة المستخدم: علامة التبويب الأحداث تمكّن URCs أعلاه، ثم **تستعلم** المودم على فترات (`AT+CEREG?`, `AT+CLCC`, `AT+QENG`, `AT+CSQ`, `AT+CMGL`) قصيرة حتى `min_read` وتعرض تغييرات الحالة في سجل مؤرخ. كل استعلام يستخدم أيضًا نافذة التسجيل) يحدث أثناء القراءة بشكل عرضي. هذا يلتقط انتقالات الحالة URC يتم التقاط أي بتواتر الاستعلام، وهو كافٍ (جديدة، تغيير الإشارة SMS، المكتسب/المفقود، بدء/إنهاء المكالمة للاختبار في المختبر. تم توثيق القيد في واجهة المستخدم.

MSC: مركز التحويل المحمول

إن **MSC** هو قلب التحكم في المكالمات في النواة المعتمدة على الدوائر. يحتفظ بسجل موقع الزائر (VLR) للمشتركين الموجودين حاليًا في منطقة خدمته، ويقوم بإعداد وإلغاء **المكالمات** ويدير **الحركة** (تحديثات الموقع، النداءات، **الرسائل القصيرة (SMS)** الصوتية، وينقل والتحويلات) لهؤلاء المشتركين. يصل إلى الجانب الإذاعي عبر اتصالات **RAN/BSC** (واجهة A، ويوجه الوسائط، **SIP** ويتصل عبر **أقران** IMS ويربط الصوت بـ M3UA/SS7)، مدفوعة عبر MSC، المشتركين النشطين في OmniWeb الفعلية من خلال بوابات وسائط واحدة أو أكثر. تعرض جدول التوجيه والصفحات المعلقة. الاتجاهات طويلة، SIP وأقران RAN، SMS، المكالمات، معاملات التي يمكن الوصول إليها من نفس الصفحة Grafana الأمد موجودة على لوحات.

← دليل العمليات

إن MSC هو صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيلها في مخزون الموقع، وحيث يتم نشر عدة عناصر، عرض أسطول للحالة الإجمالية. يمر كل حركة المرور لذا تبقى خلف، MSC الخاصة بـ (API) إلى واجهة برمجة التطبيقات OmniWeb عبر وكيل خلفي بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

وملخص لما يتعامل معه حاليًا، بما في ذلك MSC لـ **API** قراءة حالة شاشة واحدة: **حالة** قيد التنفيذ، **اتصالات SMS المكالمات النشطة**، معاملات VLR، **المشتركين** المسجلين في يعمل ورؤية، MSC إنها أسرع طريقة لتأكيد أن .**STP** ووصلة إشارة **SIP** الحية وحالة **أقران RAN** في لمحة، الحمل الحي له.

المشتركين

كل مشترك يحتفظ به VLR حاليًا، كل صف مفاتيح بواسطة **IMSI** و **MSISDN** مع حالة تسجيله وموقعه. افتح مشتركًا لعرض سياقه الكامل في VLR. من هنا يمكن للمشغل:

- **إزالة** مشترك من VLR لمسح تسجيل قديم أو عالق حتى يعيد المشترك التسجيل بشكل نظيف.
- تشغيل **إجراء مشترك** ضد مشترك معين.
- إدارة **الخدمات التكميلية**: فحص وتغيير تحويل المكالمات، الحظر والخدمات ذات الصلة النشطة للمشترك.
- **إشعار بالرسوم (AoC)** إرسال إلى المشترك.
- **رسالة SMS** إرسال **مكالمة صامتة**: استقصاء الموقع/ **صامتة (النوع 0)** أو بدء القابلية للوصول الذي لا ينبه الهاتف.

المكالمات

كل مكالمة نشطة، كل صف يظهر **الأطراف المتصلة** و **الأطراف المتلقية**، **حالة** المكالمة و الخادم ومسار الوسائط. يمكن RAN **مدتها**. افتح مكالمة لعرض تفاصيلها الكاملة: الأرجل، اتصال للمشغل **إجبار على إنهاء** مكالمة لمسح مكالمة عالقة أو غير مرغوب فيها.

الرسائل القصيرة

حاليًا، كل منها يظهر **المرسل**، **المستلم** و **حالة** MSC التي يتعامل معها SMS معاملات **التسليم**، حتى يمكنك تأكيد أن الرسائل يتم نقلها ورؤية تلك التي عالقة.

RAN

الحية التي A جمعيات واجهة) **النشطة RAN** تسرد **ات��الات** .MSC الجانب الإذاعي من على روابط RESET المعروفة، التي تم تعلمها من تبادل **BSCs** و (تحمل إشارة المشترك SS7/M3UA. هنا يمكنك تأكيد أن وحدات التحكم في المحطات الأساسية متصلة ورؤية أي المشتركين على أي اتصال.

أقران SIP

مفاتيح البرامج ووصلة التوصيل، كل صف ،IMS الصوت من خلالها هي MSC التي يربط SIP أقران يظهر **عنوان** النظير وحالة **قابلية الوصول**. افتح نظيرًا لعرض تفاصيله. يمكن للمشغل **تشغيل اختبار OPTIONS** على نظير لاختبار قابلية الوصول بشكل نشط، وهو أسرع طريقة لإثبات أن مسار SIP إليه يعمل عندما تفشل المكالمات.

بوابات الوسائط

من خ��الها حوامل الصوت، كل صف يظهر البوابة و **حالتها**، MSC بوابات الوسائط التي يوجه حتى يمكنك تأكيد أن مستوى الوسائط متاح لإعداد المكالمات.

التوجيه

بالقواعد التي تحدد، حسب بادئة الرقم المدعو، أين يتم MSC تحتفظ جدول توجيه الأرقام في إرسال المكالمة. كل قاعدة تظهر **البادئة** و **الوجهة**. يمكن للمشغل:

- **إضافة مسار**: بادئة جديدة ووجهتها.
- **إزالة مسار** حسب البادئة.
- **اختبار بحث المسار** لرقم: أدخل رقمًا وانظر أي مسار يتم حله إليه، لتأكيد خطط الاتصال قبل أو بعد التغيير.

الصفحات

حاليًا تحديد موقعهم عبر الشبكة MSC طلبات الصفحات المعلقة هي المشتركين الذين يحاول الإذاعية لمكالمة وا��دة أو SMS. مباشرة من **إرسال صفحة لمشترك** يمكن للمشغل أيضًا هنا.

السجلات

لاستكشاف مشكلة في مفتاح MSC تقوم علامة تبويب **السجلات** بعرض مخرجات السجل الحية لـ واحد دون مغادرة OmniWeb.

لوحات المراقبة

أعداد المشتركين وغيرها من السلاسل الزمنية لـ MSC، تُعرض معدلات المكالمات، أحجام SMS، بتكرار تلك OmniWeb التي يمكن الوصول إليها من صفحة العنصر. لا تقوم Grafana، كلوحات الرسوم البيانية بشكل أصلي.

ذات صلة

- يحتفظ **HSS** ببيانات المشتركين التي يتم حلها ضد VLR وأين يسجل MSC كنقطة خدمة.
- يتم ربط **CSCF / IMS أقران** عبر **SIP** الخاصة بـ MSC للصوت.
- تتصل **BSCs** على الجانب الإذاعي عبر واجهة A، تحمل على روابط إشارة SS7/M3UA.

اختبار الشبكة (اختبار التحميل)

اختبار الشبكة يدفع حمل الإشارة الاصطناعية في نواة حية حتى تتمكن من قياس كيفية تصرفها الافتراضية التي تمارس المسار UEs و eNodeBs: RAN تحت الضغط. يتم تشغيله بواسطة محاكي بدلاً من واجهة واحدة (S1AP/NAS، GTP-U، IMS) الكامل من الراديو إلى النواة.

← دليل العمليات

تجمع مجموعة RAN: **اختبار الشبكة** في الشريط الجانبي أدوات اختبار تحميل محاكي

علامة فرعية	ما تفعله
اختبار تحميل RAN	وظائف اختبار تحميل حديثة — عمليات الاتصال، جلسات البيانات قابل pcap التي تتم ضد النواة، مع نتائجها وملف IMS وتسجيلات للتنزيل.
جدول السيناريوهات	تعريف عمليات السيناريو المتكررة (مثل دفعة اتصال كل ساعة)، تشغيل واحدة الآن، وتصفح تاريخ التشغيل. يتم تصدير النتائج إلى Prometheus للتنبيه.
محاكي RAN	إعداد eNodeBs/gNodeBs و UEs الافتراضية وقيادتها مباشرة.
راديو RAN	التحكم في الراديو متعدد RAT (5G NR / 2G GERAN / 3G UTRAN).
RANsimware — IMS	تسجيل IMS وحمل VoLTE عبر الأسطول المحاكي.

كل هذه موثقة بالتفصيل في **RAN** محاكي.

توجيه عملية إلى نواة

قائمة منسدلة بعقد النواة التي يمكنه الاتصال بها — كل OmniWeb عند تشغيل خلية، يقدم **MME**، **AMF** و **STP** التي يجدها عبر جرد موقعك — بحيث يمكنك توجيه العملية إلى النواة الصحيحة (`mme_ip` / `amf_ip` / `stp_ip`) بدلاً من كتابة عنوان IP. يعود مع عدم تكوين أي جرد، الحقل إلى نص حر.

الاستخدام النموذجي

1. افتح **محاكي RAN**، قم بتشغيل eNodeB/gNodeB ووجهه إلى النواة للاختبار.
2. قم بتوصيل دفعة من UEs وتشغيل سيناريو (اتصال، بيانات، تسجيل IMS، VoLTE، أو سيناريو انقطاع).
3. راقب النتائج، ولتفاصيل الإشارة، قم بتنزيل ملف pcap للعملية.
4. احفظ السيناريو كجدول **سيناريو** بحيث يعمل على فترات ويصدر للتغطية الروتينية، النجاح/الفشل إلى Prometheus.

ذات صلة

- محاكي RAN: eNodeBs/UEs الافتراضية للاختبار الوظيفي واختبار التحميل عبر المسار الكامل من الراديو إلى النواة.
- لوحات معلومات Grafana والإحصائيات: يتم تصدير نجاح/فشل السيناريو والتوقيت إلى Prometheus؛ استخدم Grafana للحصول على الصورة الكاملة أثناء الاختبار.

OmniRoam: اتفاقيات التجوال وأتمتة البريد الإلكتروني

بتحويل الأعمال الورقية اللازمة لإعداد شريك تجوال OmniRoam تقوم جانب **الاتفاقيات** في إلى سجل واحد (وأعمال التزويد SIM، تبديل IOT، أسعار AA.12/AA.13، البريد الإلكتروني، نماذج) متعقب لكل شريك. إنها تقوم بأتمتة الأجزاء التي كانت تتطلب النسخ واللصق. حيلتها الرئيسية: **قم وسيقوم بقراءة السلسلة، واستخراج OmniRoam بإعادة توجيه بريد شريك إلى الحقائق، وتحديث الاتفاقية لك**. ثم تقوم بإنشاء وتوقيع العقود إلكترونيًا، وتخزينها، ورفع أوامر العمل لإطلاق الشريك.

← العودة إلى دليل العمليات

> هذه الوثيقة تتعلق بجانب **الاتفاقيات / هناك نوعان مختلفان من "OmniRoam".** OmniRoam (الدورة التجارية والتزويد مع شريك تجوال). **البريد الإلكتروني / الوثائق** من اختبار توافق (IR.38 / IR.48) إنها **ليست** نفس الشيء كما في **كتب اختبار التجوال** أتمتة اختبار التجوال. منتج واحد، OmniRoam: يتم تغطيتها بشكل منفصل في VoLTE). وظيفتان: *احصل على الاتفاقية موقعة* (هنا) و*أثبت أن التجوال يعمل* (هناك).

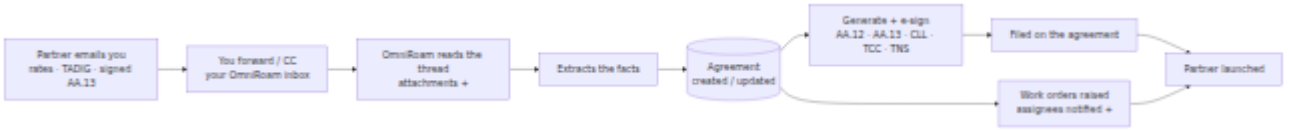
جدول المحتويات

- الصورة الكبيرة
- 1. استيعاب البريد الإلكتروني الوارد: "استخراج البيانات"
- 2. الاتفاقيات والشركاء
- 3. إنشاء وتوقيع الوثائق تلقائيًا
- 4. التخزين والأرشفة
- 5. أوامر العمل وإشعارات المعينين
- الدورة الكاملة، من البداية إلى النهاية
- ما تقوم بإعداده مرة واحدة

الصورة الكبيرة

يعتمد على سجل واحد: **الاتفاقية**، واحدة لكل ��ريك تجوال. تحمل OmniRoam كل شيء في حالة **الدورة**، جهات الاتصال، **الأسعار** التجارية، TADIG(s)/PLMN، الاتفاقية اسم الشريك، البلد المتبادلة، **الوثائق** المولدة والمستلمة، **جدول زمني** للأنشطة، و**أوامر** SIMs، المتفق عليها التي تجعل الشريك نشطًا **العمل**.

هو أن معظمها يصل OmniRoam يمكنك بناء كل ذلك يدويًا في واجهة المستخدم. لكن الهدف من *عن طريق البريد الإلكتروني*، و OmniRoamيقوم بتخزينه لك.



الجهة التي تعمل بها هي **مشغل** (شبكتك الخاصة، الجانب "المنزلي"). كل شيء مرتبط بها: رأس خطابك وتوقيعك يملأ الوثائق المولدة، عنوانك الوارد يقود أتمتة البريد الإلكتروني، وفرقك هم المعينون لأوامر العمل.

---

1. استيعاب البريد الإلكتروني الوارد: استخراج البيانات""

ما تفعله

عليك القيام بشيء، OmniRoam التفاوض مع شريك هو محادثة عبر البريد الإلكتروني. لإدخالها في **الوارد على OmniRoam عنوان CC** واحد: **إعادة توجيه البريد الإلكتروني، أو السلسلة**. هذا كل شيء. عنوانك المخصص الوارد (على سبيل المثال `roaming@yourdomain`) يتم تكوينه مرة واحدة لكل مشغل (الإعدادات → تفاصيل الأوراق، `البريد الإلكتروني الوارد`).

- يقوم ببناء الاتفاقية من OmniRoam**قم بإعادة توجيه سلسلة كاملة** مرة واحدة و التاريخ المدفون في الرسائل المقتبسة.
- **العنوان في مفاوضة جارية** وكل بريد إلكتروني جديد يبقي السجل محدثًا. تتقدم **CC** تصل الأسعار، وتُخزن الأوراق المرفقة، بريدًا تلو ،TADIGsالحالة، تملأ جهات الاتصال و الآخر.

أنت لا تملأ نموذجًا للقيام بذلك. البريد الإلكتروني هو المدخل.

ما يفعله OmniRoam

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

المحاولة مجددا

خطوة بخطوة، بمجرد وصول البريد إلى OmniRoam:

1. مع To/Cc **يحدد أي مشغل (مستأجر) يتعلق البريد به** من خلال مطابقة عنوان عنوان الوارد المكون للمشغل. إذا لم يتطابق شيء، يتم تسجيل البريد الإلكتروني كـ `no-operator` عملية آمنة: *لا يتم تغيير أي شيء*.
2. **يقرأ المرفقات، وليس فقط الجسم.** غالبًا ما تكون الأسعار المتفق عليها أو الشروط الموقعة داخل مرفقة، أو **ورقة أسعار AA.13** أو جدول بيانات. لذا، **IOT** يقوم OmniRoam باستخراج النص من مرفقات PDF وWord وExcel وCSV ويغذي ذلك إلى المستخرج أيضًا. يتم تجاهل شعارات توقيع الكتل (PNG/JPG).
3. **يستخرج الحقائق** باستخدام واجهة برمجة تطبيقات ChatGPT. يتم إخبار المستخرج بشكل محدد أن المرسل الخارجي عادةً ما يكون *يُعيد توجيه* السلسلة (غالبًا مدير التجوال الخاص بك) وأن يقرأ **التاريخ المقتبس بالكامل**. ينسب الأسعار، جهات الاتصال، العناوين و SIMs إلى من ذكرها فعليًا، وليس إلى المُعيد التوجيه. يُرجع سجلًا منظمًا: اسم الشريك، البلد، العنوان، TADIG(s)/PLMN، أفضل حالة دورة حياة مناسبة، الأسعار المتفق عليها (فقط إذا *اتفق الطرفان* بشكل صريح)، جهات اتصال الشريك المتبادلة/المطلوبة، ما إذا كانت اتفاقية موقعة مرفقة، وملخص من سطر واحد.
4. **يجد الاتفاقية الصحيحة، أو ينشئ واحدة.** المطابقة متسامحة عمدًا بحيث لا تتولد سلسلة مكررة: اسم الشريك الدقيق، ثم مطابقة "الاسم المنظم" (لذا *AT&T Mobility* تنضم إلى *AT&T*)، ثم مطابقة **PLMN المشتركة** (MCC+MNC). هذه إشارة عالية الدقة جدًا، حيث أن PLMN يحدد شبكة بشكل فريد. لا مطابقة → اتفاقية جديدة تمامًا.
5. **يمزج فقط ما هو جديد.** بالنسبة لكل من الاتفاقيات الجديدة والقديمة، يقوم OmniRoam بتطبيق ما يكشفه هذا البريد الإلكتروني حديثًا و**لا يتجاوز** القيم الموجودة:
   - **الحالة** تتحرك دائمًا *إلى الأمام* عبر دورة الحياة (لا تتراجع أبدًا).
   - **البلد / العنوان** يتم تعيينه إذا كان فارغًا أو تم تغييره.
   - **TADIGs** تُضاف، ولكن فقط الرموز التي توجد في كتالوج IR.21 (لذا لا يمكن للذكاء الاصطناعي اختراع واحدة، وأبدًا رموز شبكتك المنزلية).
   - **جهات الاتصال** تُضاف، أو يتم *تعزيز* الموجودة (تعبئة الحقول الفارغة).
   - **SIMs** تُسجل (SIMs التجريبية التي شاركها الشريك) و**طلبات SIM** (دفعات طلب شخص ما شحنها إلى عنوان).

- **الأسعار المتفق عليها** تصبح شريحة سعر، فقط عندما يتفق الطرفان بشكل صريح، وأبدًا لا تكون مكررة لشريحة موجودة.
- **الموقعة AA.12/AA.13** (مرفقة، أو مذكورة في البريد) ترفع الحالة إلى *موقعة IRA*.

6. **يكتب سجلين.** إدخال **سجل النشاط** الودي على جدول الزمن الخاص بالاتفاقية (معاد توجيهه): سعر البيانات المتفق عليه؛ الحالة "تمت إضافة جهة الاتصال جين، تم تسجيل الأسعار المتفق عليها"، → rates_agreed و**سجل تدقيق وارد** خام (انظر أدناه).

المعالجة **غير قابلة للتكرار**: يتم معالجة نفس البريد الإلكتروني (حسب معرف الرسالة) مرة واحدة فقط، لذا فإن CC'ing عدة أشخاص أو إعادة توجيه سلسلة لا يعد أبدًا مرتين.

ثلاث طرق لدخول البريد الإلكتروني

تحتاج فقط إلى واحدة. جميعها تنتهي بالاتصال بنفس منطق المعالجة:

المسار	كيف يعمل	متى تستخدمه
Cloudflare Email Worker	يقوم توجيه البريد الإلكتروني من Cloudflare بإعادة توجيه الرسالة الخام إلى عامل صغير مباشرة إلى واجهة برمجة `.eml` يقوم بتدفق التطبيقات الخاصة بـ OmniRoam.	المجالات التي تستخدم بالفعل؛ لا Cloudflare يوجد صندوق بريد للاستطلاع.
IMAP poller	يقوم OmniRoam بتسجيل الدخول إلى صندوق بريد حقيقي كل ~60 ثانية، ويعالج الرسائل غير المقروءة، ويعلمها بأنها مقروءة.	أي صندوق بريد قياسي (TLS ضمني، STARTTLS، أو عادي).
Provider inbound-parse	يقوم مز��د البريد (Mailjet/SendGrid) بإرسال الرسالة المفسرة + المرفقات إلى واجهة برمجة التطبيقات.	إذا كنت تقوم بتشغيل inbound-parse بالفعل.

واجهة برمجة التطبيقات (`/api/roaming/inbound-email`) محمية بواسطة **سر مشترك**، لذا يمكن فقط لمسار البريد المكون الخاص بك النشر إليها.

سجل البريد الإلكتروني الوارد: أثر التدقيق الخاص بك

كل بريد إلكتروني تمت معالجته، سواء كان ناجحًا *أو* فاشلاً، يكتب صفًا في **سجل البريد الإلكتروني الوارد** (في واجهة المستخدم تحت عرض رسائل البريد الإلكتروني الخاصة بالمشغل). يظهر كل صف المرسل، المستلمين، الموضوع، المرفقات، ما إذا كانت **استخراج الذكاء الاصطناعي قد نجح**، بالضبط ما تم استخراجه، وما الذي **تغير** في البريد الإلكتروني (أو لماذا لم يتغير شيئًا: `no-operator`, `no-partner`). هذه هي نافذتك إلى الأتمتة: إذا لم يتم التقاط سعر، يخبرك السجل بما رآه المستخرج بالفعل.

سجل البريد الإلكتروني الوارد: صف واحد لكل بريد إلكتروني تمت معالجته، مع نتيجة الاستخراج والتغييرات التي أجراها. هذه هي أثر التدقيق لكل أتمتة البريد الإلكتروني←الاتفاقية.

---

2. الاتفاقيات والشركاء

قائمة **الاتفاقيات** هي كتابك لشركاء التجوال للمشغل الحالي. كل صف هو شريك واحد، مع حالة **الدورة**، TADIG/("نحن" أو "هم")، البلد، الأولوية، ومن ينتظر الإجراء التالي.

قائمة الاتفاقيات. الحالات تمتد من اليسار إلى اليمين عبر الدورة؛ شريط الفلترة يضيق حسب الحالة. يمكنك إنشاء الاتفاقيات هنا يدويًا، أو تصل تلقائيًا من بريد إلكتروني وارد.

دورة الحياة (الحالة)

تتحرك الاتفاقية للأمام عبر هذه المراحل. الأتمتة البريدية لا تتقدم الحالة أبدًا، لذا يعكس السجل أبعد نقطة وصلت إليها المحادثة:

`في المفاوضات → في IRA → في انتظار التوقيع IOT → IOT استفسار → مفاوضة موقعة → الأسعار المتفق عليها → تبادل IRA → IRA انتظار توقيعات → SIM` (بالإضافة إلى `إطلاق افتراضي`، `معلق`، `ملغى`).

`اختبار → إطلاق`.

فتح شريك

انقر على شريك لفتح صفحة **التفاصيل** الخاصة به: مجموعة من علامات التبويب/الأقسام تغطي كل شيء عن العلاقة:

- **نظرة عامة وجدول زمني**: الحالة، الأولوية، الملاحظات، وسجل النشاط (كل بريد إلكتروني، وثيقة مولدة، توقيع، وملاحظة يدوية مرتبة حسب التاريخ).
- **TADIGs**: رموز شبكة الشريك (مع MCC/MNC، نوع الاتصال والاتجاه). يمكن أن تسحب إجراء **"البحث عن المرشحين"** TADIGs الأخرى لمشغل الشريك من كتالوج

لمراجعتها وإضافتها IR.21.

- **جهات الاتصال**: الأشخاص التجاريون/التقنيون في الشريك.
- **الأسعار**: شرائح الأسعار التجارية المتفق عليها (صوت، عملة، وحدة/SMS/بيانات).
- **SIMs وطلبات SIM**: SIMs التجريبية المتبادلة، والدُفعات المطلوبة للشحن.
- **الوثائق**: الأوراق المولدة والمستلمة (انظر أدناه).
- **التوجيه**: مسارات DRA، عناوين SS7، ونطاقات DNS العالمية وIP للتزويد (الكثير منها مُعبأ مسبقًا من IR.21 الخاص بالشريك).

كل شيء في صفحة التفاصيل **قابل للتعديل**. تمنحك الأتمتة بداية، وتقوم بتصحيح أو إضافة يدويًا حسب الحاجة.

IR.21 كتالوج

تستند عمليات البحث عن TADIG إلى **كتالوج عالمي لمشغلي IR.21** مفاتيحها بواسطة TADIG (الشبكة، المنظمة، MCC/MNC، DNS، نطاقات IP، عقد SS7، جهات الاتصال). هذه هي الطريقة التي يتحقق بها OmniRoam من TADIG الذي استخرجه الذكاء الاصطناعي، ويكتشف الشقيقة لشريك، ويقوم بتعبئة بيانات التوجيه مسبقًا TADIGs.

---

3. إنشاء وتوقيع الوثائق تلقائيًا

إنشاء وثيقة

بإنشاء OmniRoam في قسم **الوثائق** للاتفاقية، تختار نوع الوثيقة وتضغط على **إنشاء**. يقوم النموذج الحقيقي لـ Word، جاهزًا للتوقيع، مليئًا بتفاصيل كلا الجانبين:

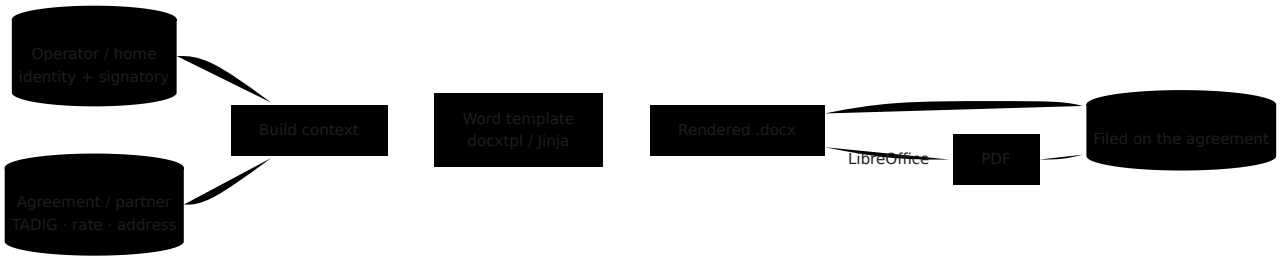
النوع	ما هو	التنسيق
AA.12	اتفاقية التجوال GSMA AA.12 IREG (النموذج الحقيقي، مليء مسبقًا من كلا الجانبين)	.docx / PDF
AA.13	الملحقات الشائعة GSMA AA.13، بما في ذلك ملحق الفوترة/التسوية (انظر خيارات تسوية AA.13)	.docx / PDF
CLL	خطاب الإطلاق التجاري (عام)	.docx / PDF
CLL (/ ثنائي أحادي، بعد الاختبار)	خطاب الإطلاق يؤكد تاريخ البدء **بعد اختبار IREG وTADIG الناجح**	.docx / PDF
CLL (/ ثنائي أحادي، افتراضي)	خطاب الإطلاق لإطلاق **افتراضي، دون إكمال اختبار IREG/TADIG**	.docx / PDF
TCC (VoLTE)	إكمال اختبار مكالمة VoLTE	.docx / PDF
استكمال TADIG	نموذج استكمال TADIG	.docx / PDF
نموذج اتفاقية التجوال TNS	طلب clearing-house TNS (يتم تسليمه كـ .doc قديم)	.doc
طلب TNS 3G-4G	طلب clearing-house TNS	.docx

كل وثيقة هي قالب Word مع عناصر نائبة (docxtpl / Jinja). يقوم **كيف يتم ملء الحقول.** بملئها من OmniRoam:

- **الجانب المنزلي**: من سجل **المشغل** الخاص بك: اسمك، الاسم القانوني، TADIG، البلد، **التوقيع واللقب**، المكان، والعنوان. لأن هذا يأتي من المستأجر، يحصل كل مشغل مستضاف على *رأس خطابه* وتوقيعه تلقائيًا.
- **جانب الشريك**: من **الاتفاقية**: اسم الشريك، اختصاره القصير المستخدم في نص العقد، TADIG(s)، PLMN(s)، البلد والعنوان. يتم ترك توقيع الشريك/لقبه فارغًا، لذا

تظل تلك السطر جاهزة لتوقيعهم.

- **القيم المشتقة**: تاريخ ا��سريان، الاتجاه (ثنائي/وارد/صادر)، شركة المحور، مجالات Diameter، وسعر العملة، المؤكد IOT.



تنسيق الإخراج: Word بشكل افتراضي، PDF للتوقيع

بشكل افتراضي. هذه هي النسخة `.docx` **قابلة للتعديل Word** تنتج عملية الإنشاء **نسخة** فقط عندما تحتاج فعليًا PDF العملية التي تقوم بمراجعتها وتحريرها يدويًا إذا لزم الأمر. تحصل على إلى عرض ثابت نهائي:

- **إخراج** قم بتحديد خانة **PDF** قبل النقر على إنشاء لتوليد PDF بدلاً من `.docx`.
- **التوقيع الإلكتروني** يستخدم دائمًا PDF (يجب ألا يتغير العنصر الموقّع).
- **قم بتنزيل / معاينة** وثيقة مخزنة كـ *PDF* عند الطلب.

قابلة للتعديل حتى يتمكن الشريك `.docx` كـ AA.12/AA.13 تقوم رسالة **حزمة التجوال** بإرفاق من مراجعتها والتعليق عليها. هذه ليست خطوة التوقيع، لذا لا يتم إرسالها كـ PDF.

خيارات تسوية AA.13 (الملحق C.3.2)

هو **قائمة من الخيارات** يتفاوض عليها كل (الفوترة والتسوية) GSMA AA.13 من C.3.2 الملحق شريك: أي نموذج فاتورة، أي طريقة دفع، حد التسوية والفترة، شروط الدفع، والفائدة. بدلاً من عنها كلوحة خيارات تسوية في OmniRoam قفل مجموعة واحدة من الخيارات في القالب، يكشف واضبط القيم لهذا الشريك، ثم انقر على **AA.13**، قسم **الوثائق**: قم بتوسيع **خيارات تسوية وهي) يحتوي الملحق المولد فقط على الخيارات التي اخترتها. يتم إسقاط البدائل .**AA.13 إنشاء** تلقائيًا (GSMA "حذف تلك التي لا تنطبق" من.

كل حقل له قيمة افتراضية معقولة، لذا فإن الإنشاء دون لمس اللوحة ينتج الشروط القياسية؛ غير فقط ما يختلف لشريك معين.

الخيار	الافتراضي	الوصف
نوع الفاتورة	فاتورة شبكة واحدة (SNI)	يحدد الملحق التسويتي: **شبكة واحدة (SNI)** ← الملحق C.3.2 H، أو **شبكة متعددة (MNI)** ← الملحق C.3.2 I. يتم إزالة الملحق غير المستخدم.
طريقة الدفع	التسوية الصافية	آلية التسوية: **التسوية الصافية**، **الدفع الكامل المباشر (بدون تحويل)**، **الدفع الكامل المباشر (مع تحويل)**، أو **التسوية بدون تحويل**. يتم الاحتفاظ فقط بفقرة الطريقة المختارة.
حد التسوية	الخيار 1 (التسوية)	**الخيار 1 (التسوية)** يطبق حدًا منخفضًا متفقًا عليه؛ **الخيار 2 (الدفع المباشر)** يستخدم حدودًا لكل طرف (الطرف A / الطرف B).
الحد	50	مبلغ حد التسوية المنخفض، في عملة التسوية للاتفاقية (مثل SDR). تحت هذا المجموع الشهري، قد يتم تأجيل التسوية.
بداية الفترة / نهاية الفترة	يناير / ديسمبر	الفترة غير التسوية للأرصدة التي تقل عن الحد، عادةً لسنة المالية��.
أيام الدفع	60	الأيام من تاريخ الفاتورة التي يجب على المدين الدفع خلالها.
نسبة الفائدة المنزلية %	8	الفائدة السنوية التي يمكن للدائن فرضها على الأرصدة المتأخرة عندما يكون **المشغل** المنزلي هو الدائن.
نسبة الفائدة الشريكة %	8	الفائدة السنوية عندما يكون **المشغل** الشريك هو الدائن.
إرسال فواتير بقيمة صفرية	إيقاف	عند الإيقاف، ينص الملحق على أن كل طرف **لن** يرسل فواتير شهرية بمبلغ صفر (0.00).

الخيار	الافتراضي	الوصف
على BCE فاتورة TAP	إيقاف	**لن** BCE عند الإيقاف، ينص الملحق على أن استخدام TAP يتم تضمينه في فاتورة التجوال.

كيف يعمل. يتم تمرير الخيارات إلى الإنشاء كاستبدالات فوق القيم الافتراضية المدمجة. يقوم بحلها في الملحق النهائي: يحدد كتل الخيارات الصحيحة، يملأ المبالغ/الفترات/الأسعار، AA.13 قالب ويصوغ التبديلات. تأتي عملة التسوية نفس��ا من العملة المكونة للاتفاقية، وليس من هذه اللوحة.

وسنة مالية من أبريل إلى SDR **حالة الاستخدام.** يصر شريك على شروط 90 يومًا، وحد 100 مارس: افتح اللوحة، اضبط **أيام الدفع** 90، **الحد** 100، **بداية الفترة** أبريل، **نهاية الفترة** مارس، وأنشئ. تبقى كل فقرة أخرى على الشروط القياسية.

> **نموذج TNS للـ clearing-house** الطلبان **خاص.** قوالب TNS *ليسا* docxtpl. إنها نماذج TNS الحقيقية للمشغل مع تغيير فقط الحقول القابلة للتعبئة وتحديد المربعات الصحيحة، لذا يتلقى TNS بالضبط التخطيط الذي يتوقعه. إنها **مقيدة بـ IOT**: لا يقوم بإنشائها حتى تحتوي الاتفاقية على **سعر مؤكد (متفق عليه)**. محاولة القيام بذلك في وقت سابق تعيد رسالة واضحة "مطلوب سعر مؤكد". يتم اشتقاق حالات المربعات IOT تلقائيًا من الاتفاقية، وجميع الحقول (LTE، GRX نوع الاتفاقية، الاتجاه، الخدمات، واجهات) قابلة للاستبدال في وقت الإنشاء.

يقوم LibreOffice بإجراء توليد PDF (و`.doc` القديم لـ TNS) بدون واجهة على الخادم. تحصل فقط على الملف النهائي.

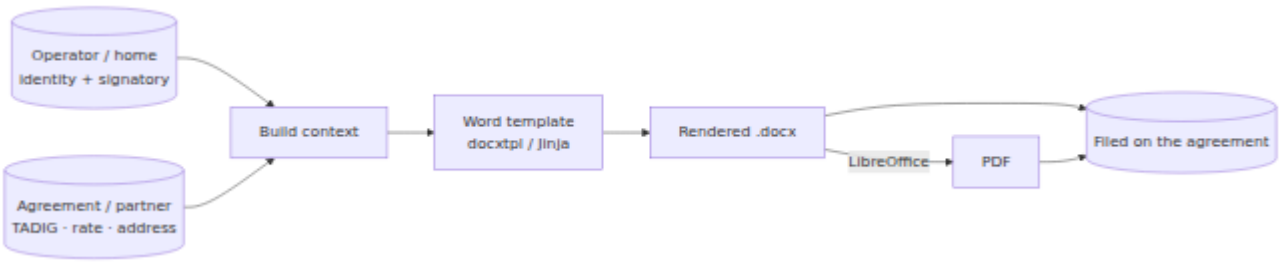
قسم الوثائق للاتفاقية. قم بإنشاء عقد على اليسار؛ الوثائق المولدة والمستلمة (مع حالة التوقيع) مدرجة أدناه، كل منها قابلة للتنزيل.

التوقيع: عبر الإنترنت أو خارج الإنترنت

يدعم OmniRoam مسارين للتوقيع:

التوقيع الإلكتروني عبر الإنترنت (يوقع الشريك في المتصفح، بدون تسجيل دخول). من AA.12/AA.13 المولدة، انقر على **إرسال للتوقيع**، سمِّ الموقّع وبريده الإلكتروني، وOmniRoam:

1. ينشئ طلب توقيع برمز غير شفاف ويرسل بريدًا إلكترونيًا إلى الشريك برابط **آمن** (لا حاجة لحساب).
2. بتحديد الطلب *المشاهد* و��سجله في الجدول OmniRoam عندما يفتحونه، يقوم الزمني. يقومون بمراجعة الوثيقة، وتصحيح اسم/لقب/شركة الموقّع إذا لزم الأمر، و**يوقعون** بكتابة اسمهم و/أو رسم توقيع.
3. يقوم OmniRoam بإنتاج **PDF** (الموقّع + صندوق البريد العائد لمشغل الخاص بك)، ويخزنه في الاتفاقية، ويسجل "تم التوقيع بواسطة ... في ...".
4. يمكن للشريك أيضًا **رفض** (مع سبب)، والذي يتم تسجيله أيضًا.



التوقيع خارج الإنترنت. تفضل التوقيع بالطريقة القديمة؟ قم بتنزيل الوثيقة المولدة، ووقعها خارجيًا، وقم بتحميل النسخة الموقعة مرة أخرى على الاتفاقية. يتم التعرف على ا��م ملف يحتوي على *موقع/مُنفذ/موقع من قبل* كنسخة موقعة. البريد الإلكتروني الوارد الذي يرفق واحدة *موقعة IRA* يرفع الحالة تلقائيًا إلى.

حزمة التجوال: أول اتصال بنقرة واحدة

بدلاً من إنشاء كل نموذج بشكل منفصل، تقوم **إرسال حزمة التجوال** بإرسال بريد إلكتروني إلى جهة اتصال شريك مع **عرض IOT + AA.12 + AA.13** معًا في رسالة واحدة. تقوم بإنشاء لك. اختر جهة اتصال (أو اكتب اسم + بريد IOT على الفور وتلحق أحدث عرض PDFs العقود كـ الحزمة مع نص القالب المحفوظ OmniRoam إلكتروني، والذي يتم ملؤه كجهة اتصال)، ويرسل OmniRoam لديك. هذه هي رسالة "دعونا نقوم بصفقة تجوال" الافتتاحية، المرسلة من داخل.

قوالب البريد الإلكتروني القابلة للتعديل

تستخدم رسائل البريد الإلكتروني الثلاثة المؤتمتة (**طلب التوقيع**، **نسخة موقعة**، و**حزمة التجوال**) قوالب قابلة للتعديل (استبدال لكل مشغل، وإلا فافتراضي عالمي)، مع عناصر نائبة مثل `{{ signer_name }}`، `{{ partner }}`، `{{ operator }}`، `{{ sign_url }}` و `{{ document_name }}`. قم بضبط النص مرة واحدة في الإعدادات وكل إرسال يستخدمه.

> **فعليًا.** يتم إرسال جميع الرسائل الصادرة **كيف يغادر البريد الإلكتروني OmniRoam** عبر **Mailjet HTTPS Send API**، وليس SMTP. تمنع منصات الاستضافة (Railway) منافذ SMTP الصادرة، لذا يقوم OmniRoam بإرسال POST إلى Mailjet عبر HTTPS بدلاً من ذلك. تكون الإرسال **بأفضل جهد وغير حاصرة**: تعود زر واجهة المستخدم على الفور ويخرج البريد على خيط خلفي، لذا لا يمكن لخادم بريد بطيء أن يوقف التطبيق.

التخزين والأرشفة

يتم تخزين كل وثيقة **مباشرة على الاتفاقية** التي تنتمي إليها. يغطي هذا **الوثائق المولدة** (AA.12، AA.13، CLL، TCC، TNS...) و**الوثائق المستلمة** نسخة موقعة مرفقة ببريد

لا يوجد متجر وثائق منفصل لإدارته. (IOT تم تحميله، ورقة IR.21، إلكتروني):

- يتم تخزين الوثائق كـ blobs **نوع** مع وضع علامة **في قاعدة البيانات**، (`aa12`, `aa13`, `aa12_signed`, `iot`, `ir21`, `cll`, `other`, ...)، اسم الملف، نوع المحتوى، الحجم، وما إذا كان OmniRoam **قد أنشأها**.
- **يتم إزالة المرفقات الواردة المكررة**: لا يتم إعادة تخزين نسخة متطابقة (نفس اسم الملف + طول البايت) تصل مرة أخرى.
- تكتب **إدخالًا زمنيًا**، لذا فإن سجل نشاط IOT كل عملية إنشاء، تحميل، توقيع، وتصدير الاتفاقية هو مسار ورقي كامل لما تم إنتاجه واستلامه، ومتى.

لاسترجاع وثيقة، افتح قسم **الوثائق** للاتفاقية وقم بتنزيلها (Word/PDF الأصل أو المولدة). يتم تخزين PDFs على طلب المستلم (المستلم الموقعة التي تم إنتاجها من خلال تدفق التوقيع عبر الإنترنت. التوقيع ويتم إرسالها أيضًا إلى كلا الطرفين عبر البريد الإلكتروني.

من **XML GSMA RAEX IOT 5.0** يمكنك أ��ضًا **تصدير السعر المتفق عليه كملف** المصدرة والنماذج IOT لذا فإن TNS، الاتفاقية. هذا هو نفس اختيار السعر الذي تستخدمه نماذج المولدة تتفق دائمًا.

أوامر العمل وإشعارات المعينين

عمل: شحن جعل شريك نشط هو SIMs، إجراء اختبارات، تغيير التوجيه، IREG/TADIG، تدقيق، يتم تتبع هذا العمل كـ **أوامر العمل**: الوحدة المتعقبة الوحيدة، OmniRoam متابعة القضايا. في للعمل التجوالي. يمكن أن تتعلق أمر العمل باتفاقية (شريك) أو أن تكون قائمة بذاتها.

عرض أوامر العمل. كل أمر له نوع، أولوية، حالة، رابط شريك اختياري، ومعين: الطرف الذي يتم إخطاره عند تعيينه.

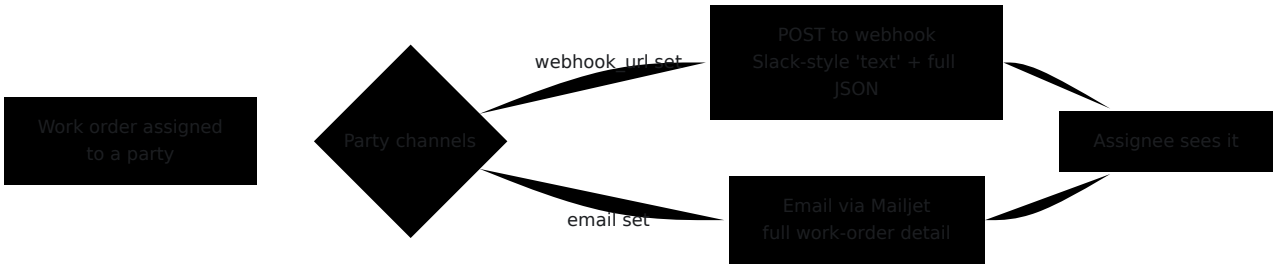
إنشاء وتعيين

لأمر العمل نوع (شحن SIM، اختبار توجيه، IREG، اختبار TADIG، مشكلة، ،(تدقي��، عنوان، أولوية، حالة (مفتوح / قيد التقدم / محجوز / مكتمل / ملغى)، رابط شريك (اتفاقية) اختياري، على سبيل المثال، يحمل شحن) تفاصيل نصية حرة، تاريخ استحقاق، وحقول هيكلية خاصة بالنوع SIM (الكمية، العنوان البريدي، الناقل والتتبع).

تقوم بتعيين أمر العمل إلى **طرف**: فريق داخلي مسمى أو جهة اتصال خارجية (مثل "Roaming مدير" ،"TADIG") **معين افتراضي** في **الإعدادات**. يمكنك تعيين يتم إدارتها لكل مشغل NOC"، لذا يتم تعيين شحن SIM ما **لكل نوع من أوامر العمل**، جديد تلقائيًا إلى من يتعامل مع الشحن لم تقم بتجاوز ذلك.

الإشعار: webhook + بريد إلكتروني

عندما يتم **تعيين** أمر العمل (تم إنشاؤه مع معين، أو أعيد تعيينه إلى طرف جديد)، يقوم OmniRoam من خلال أي قنوات قام الطرف بتكوينها **بإخطار ذلك المعين**:



- **Webhook**: إذا كان لدى الطرف عنوان URL webhook (مثل **webhook الوارد لـ Slack**)، يقوم OmniRoam بإرسال رسالة مع كتلة `text` قابلة للقراءة من قبل الإنسان JSON، الشريك، الحالة، الأولوية، منظم (النوع، الحمولة الخاصة بالنوع، رابط العودة إلى صفحة أوامر العمل) *وأيضًا* أمر العمل الكامل كـ.
- **البريد الإلكتروني**: إذا كان لدى الطرف عنوان بريد إلكتروني، يقوم OmniRoam بإرسال نفس التفاصيل كرسالة بريد إلكتروني (عبر Mailjet)، الموضوع `[Work Order] <title> assigned to you`.

الطرف الذي ليس لديه **أي من** القنوات المحددة هو ببساطة معين صامت (لا عملية). كلا الإشعارين هما أفضل جهد وغير حاصرة، لذا لا يمكن لخادم webhook أو بريد بطيء أن يوقف التطبيق. إعادة التعيين تخطر فقط عندما **يتغير** المعين فعليًا إلى طرف جديد (لذا فإن تحرير الحقول الأخرى لا يعيد تنبيه الأشخاص).

> في اللحظة التي تصل (أو بريد إلكتروني) Slack **من كرسي المعين:** تحصل على رسالة فيها مهمة إلى فريقك، مع كل ما تحتاجه: ماذا تفعل، لأي شريك، عدد SIMs وعنوان الشحن (أو تغيير التوجيه، أو نطاق الاختبار)، الأولوية وتاريخ الاستحقاق، ورابط مباشر إلى أمر العمل.

الدورة الكاملة، من البداية إلى النهاية

جمع كل شيء معًا، هذه هي الرحلة من "شريك أرسل لنا بريدًا إلكترونيًا" إلى "الشريك نشط":

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



في كل خطوة، يسجل **الجدول الزمني** للاتفاقية ما حدث، ويحتفظ **سجل البريد الإلكتروني** بالأدلة الخام لما ساهمت به كل رسالة بريد إلكتروني **الوارد**.

ما تقوم بإعداده مرة واحدة

تحتاج معظم الأتمتة فقط إلى تكوين صغير لمرة واحدة لكل مشغل (في **الإعدادات**):

أين يتم استخدامه	لماذا	الإعداد
إنشاء الوثائق	يملأ الجانب المنزلي من كل وثيقة مولدة	**تفاصيل الأوراق** (الاسم القانوني، البلد، **التوقيع واللقب**، PLMN، TADIG، المكان، العنوان)
استيعاب البريد الإلكتروني	العنوان الذي تقوم بإعادة توجيه/CC إليه بريد الشريك	**عنوان البريد الإلكتروني الوارد**
التوقيع	حيث تذهب الرسائل الموقعة خارجيًا ورسائل النسخ الموقعة	**صندوق البريد العائد الموقّع**
البريد الإلكتروني الصادر	نصك للبريد الإلكتروني المؤتمت	**قوالب البر��د الإلكتروني** (طلب التوقيع، النسخة الموقعة، حزمة التجوال)
أوامر العمل	من يتم إخطاره لكل نوع من العمل	**أطراف أوامر العمل** + المعينون الافتراضيون لكل نوع

مع وجود هذه الأمور في مكانها، يصبح إعادة توجيه بريد شريك فعليًا: *البريد الإلكتروني الوارد → الاتفاقية الصادرة → العقود المولدة والموقعة → أوامر العمل المرفوعة وإخطار فريقك*.

انظر أيضًا

- OmniRoam: أتمتة اختبار التجوال: *الآخر* OmniRoam. يقوم بتشغيل كتب اختبار التجوال GSMA (IR.38 / IR.48 / VoLTE) ضد شبكة حية. هذا تكميلي: وقع الاتفاقية هنا، أثبت أنها تعمل هناك.
- العمليات الشائعة: أنماط العرض/التحرير المشتركة عبر جميع OmniWeb.

أومني روم: أتمتة اختبار التجوال

أومني روم هي ميزة أتمتة كتيبات اختبار التجوال في أومني ويب. تقوم بتشغيل كتيبات اختبار ضد شبكة حية. تقوم بتشغيل حالات الاختبار الفردية تلقائيًا من GSMA الامتثال للتجوال الخاصة بـ GSMA جهاز اختبار. تسجل حكم النجاح/الفشل مع الأدلة الداعمة لكل حالة. ثم تنتج كتيب اختبار مكتمل جاهز للإرسال إلى شريك أو مركز تجوال.

باختصار: أومني روم تحول تمرين الامتثال للتجوال اليدوي الذي يستغرق عدة ساعات إلى ضغطة زر (أو وظيفة مجدولة). تعيد نفس جدول بيانات GSMA الرسمي الذي كان سيقوم المختبر بملئه يدويًا.

> **لدى أومني روم جانبين.** تغطي هذه الوثيقة **كتيبات اختبار التجوال** (IR.38 / IR.48 / اختبار توافق VoLTE: *هل يعمل التجوال فعلاً؟*). الجانب الآخر هو **اتفاقيات التجوال وأتمتة البريد الإلكتروني**. تحول بريد شريك إلى اتفاقية موقعة، وتولد أوراق وأوامر العمل لجعل الشريك نشطًا. يتم توثيق ذلك بشكل AA.12/AA.13/CLL/TCC/TNS، منفصل في **اتفاقيات التجوال وأتمتة البريد الإلكتروني**. منتج واحد، وظيفتان: *احصل على الاتفاقية موقعة* (هناك) و*أثبت أن التجوال يعمل* (هنا).

شاشة كتيبات اختبار التجوال. كل صف هو كتيب تم تشغيله ضد شريك تجوال، مع حالته الحالية.

روابط سريعة

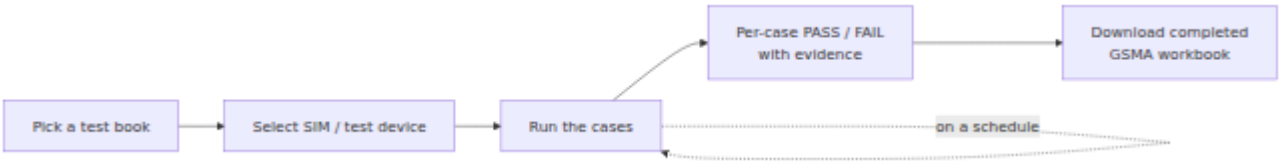
- **كتيبات الاختبار**: الكتيبات المتاحة (IR.38، IR.48، VoLTE) وكل حالة اختبار تحتويها
- **تشغيل الاختبارات**: كيفية إنشاء كتيب، تشغيله، تخصيص مجموعة الحالات، وجدولة التشغيلات الروتينية
- **مستكشف كتيب الاختبار**: كيفية فحص ما تختبره كل كتيب وكيف يتم تشغيل كل حالة
- **مستندات كتيب الاختبار المكتملة**: كيفية توليد أومني روم لكتيب GSMA المملوء
- **اتفاقيات التجوال وأتمتة البريد الإلكتروني**: الجانب *الآخر* من أومني روم. أرسل بريد شريك ← تم إنشاء الاتفاقية، تم توليد العقود وتوقيعها إلكترونيًا، وتم حفظها، وتم رفع أوامر العمل

ما تفعله أومني روم

قائمة بحالات الاختبار التي تثبت أن كتيب اختبار التجوال هو قائمة تحقق محددة من قبل GSMA: يتلقى الخدمات المتوقعة أثناء ("PLMN(a)")، الـ **PLMN المنزلي** مشتركًا من شبكة واحدة تاريخيًا، يتم تنفيذ كل حالة يدويًا ويتم التجوال على شبكة أخرى (الـ **PLMN الزائر**، "PLMN(b)"). كتابة النتيجة في جدول بيانات.

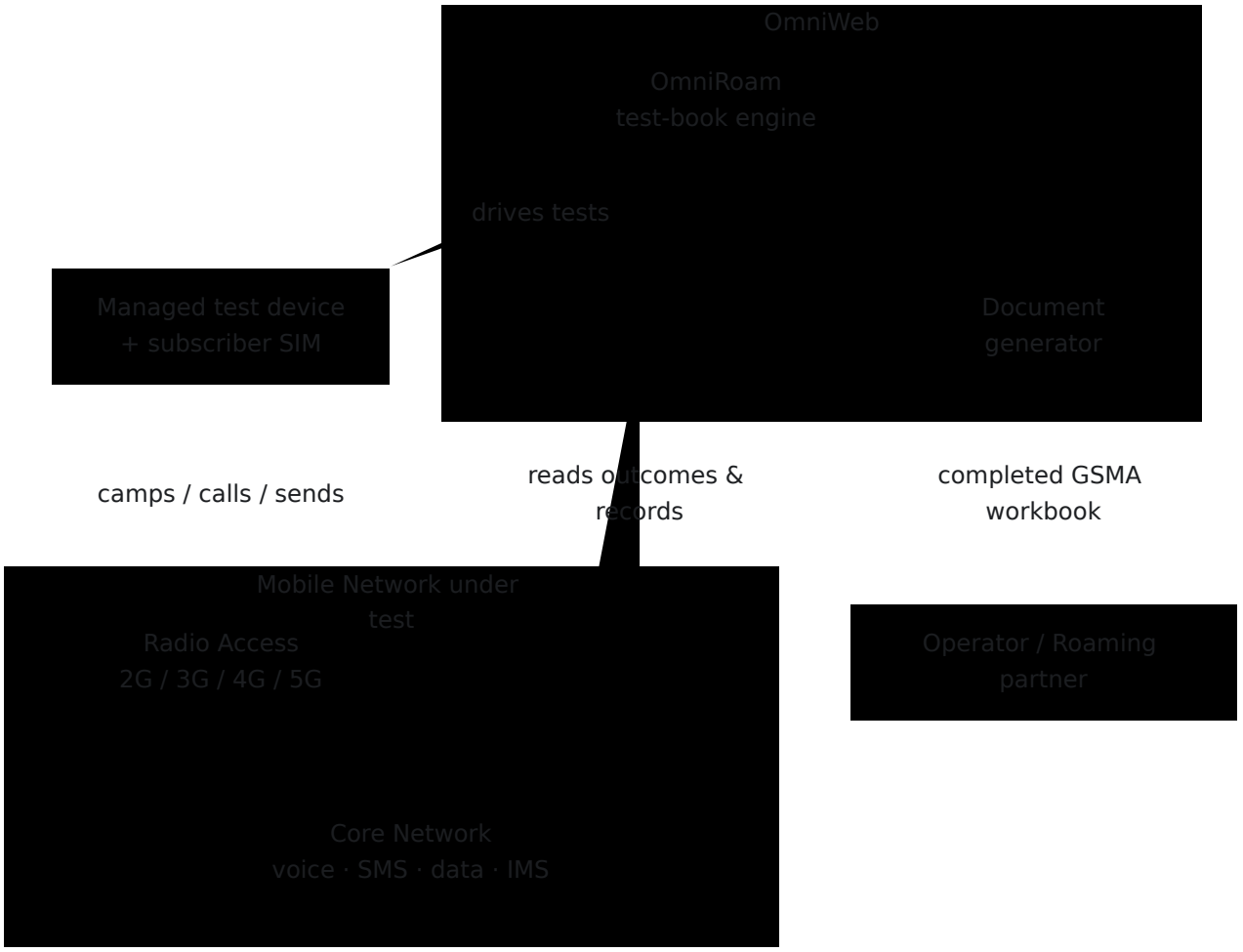
تقوم أومني روم بأتمتة ثلاثة أشياء:

1. **تشغيل الاختبار**: تقوم بإجراء المكالمة، إرسال الرسالة النصية، تشغيل جلسة البيانات، أو توفير الخدمة التكميلية على جهاز اختبار.
2. **تقييم النتيجة**: تقارن ما حدث مع النتيجة المتوقعة من GSMA. تسجل **نجاح**، **فشل** أو **لم يتم التنفيذ**، مع الأدلة الداعمة (الأوقات، معدل النقل، أسباب إصدار الشبكة، وما إلى ذلك).
3. **إنتاج المستند**: تملأ كتيب GSMA الرسمي بالنتائج وجميع البيانات الوصفية المحيطة (الهويات، التواريخ، تفاصيل المختبر).



أين تتناسب

تقوم أومني روم باختبار مشترك حقيقي على الشبكة الحقيقية باستخدام جهاز اختبار مُدار. كل حالة مؤتمتة تقود الجه��ز، ثم تقرأ النتيجة مرة أخرى من الجهاز وأينما كان ذلك مناسبًا، من سجلات الشبكة الخاصة (على سبيل المثال، سجلات الشحن الخاصة ببوابة الخدمة لجلسة البيانات). لا شيء يتم محاكاته: المكالمة التي يتم الإبلاغ عنها على أنها متصلة قد اتصلت فعلاً.



المفاهيم الرئيسية

المصطلح	المعنى
كتيب الاختبار	مجموعة من حالات الاختبار المحددة من قبل GSMA (مثل IR.38، IR.48، VoLTE). انظر كتيبات الاختبار.
حالة اختبار	فحص فردي داخل كتيب، يتم تحديده برقم GSMA الخاص به (مثل حالة "حظر جميع المكالمات الصادرة"، `2.3` IR.48).
تشغيل	تنفيذ واحد لكتيب (أو مجموعة مختارة من حالاته) ضد جهاز و SIM.
الحكم	النتيجة المسجلة لحالة: `نجاح`، `فشل`، أو `لم يتم التنفيذ`.
الأدلة	التفاصيل الداعمة الملتقطة للحكم: الأوقات، أرقام معدل النقل، أسباب الشبكة، قراءات الاستجواب، إلخ.
PLMN المنزلي (أ)	الشبكة التي تمتلك المشترك الذي يتم اختباره.
PLMN الزائر (ب)	الشبكة التي يتجول عليها المشترك.

الحالات المؤتمتة مقابل اليدوية

تكون معظم الحالات في كل كتيب **مدفوعة تلقائيًا**: تقوم أومني روم بتنفيذها من البداية إلى النهاية وتسجل الحكم دون تفاعل من المشغل. تعتمد بعض الحالات على ظروف الشبكة التي لا يمكنك تحفيزها من جهاز اختبار بمفرده (على سبيل المثال، اختبارات CAMEL المدفوعة سلبًا). تظل هذه **يدوية**. لا تزال أومني روم تسردها في الكتيب ويسجل المشغل النتيجة يدويًا، لذا فإن المستند النهائي مكتمل.

يظهر مستكشف كتيب الاختبار بالضبط أي الحالات في كتيب مؤتمتة وكيف يتم تشغيل كل واحدة منها.

المعايير المرجعية

تتبع أومني روم مستندات GSMA 3 لـ المرجعية الدائمة والمواصفات الأساسيةGPP:

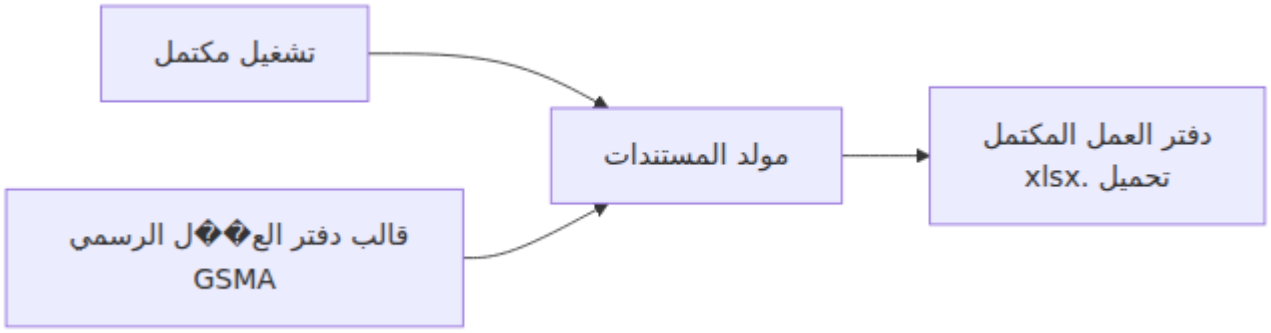
المرجع	ينطبق على
GSMA IR.38	كتيب اختبار بيانات التجوال LTE
GSMA IR.48 / IR.24	كتيب اختبار التجوال الثنائي (صوت / SMS / MMS / بيانات)
GSMA BA.65	اختبار التجوال VoLTE
GSMA IR.92	ملف IMS و للصوتSMS (سلوك VoLTE)
GSMA IR.88	إرشادات التجوال LTE (أسباب رفض الاتصال)
3GPP TS 22.011	إمكانية الوصول إلى الخدمة (الحظر المحدد من قبل المشغل)
3GPP TS 23.011	حالة الخدمة التكميلية (نشط/مسجل/مُزود/خامل)
3GPP TS 22.082	خدمات الحظر المكالمات التكميلية
3GPP TS 22.088	خدمات الحظر المكالمات التكميلية

مستندات اختبار الكتاب المكتملة

المكتمل: الجدول الرسمي لـ **GSMA** هو **دفتر اختبار** OmniRoam المنتج النهائي لتشغيل للكتاب، مليء بنتائج التشغيل وجميع التفاصيل المحيطة، جاهز للإرسال إلى شريك تجوال أو GSMA بإنتاجه من خلال إجراء **تحميل دفتر الاختبار** واحد. لا يحتاج إلى نسخ OmniRoam مركز. يقوم يدوي.

ما ستحصل عليه

للكتاب ويملأه في مكانه، لذا فإن النتيجة هي نفس GSMA القالب الرسمي لـ OmniRoam يأخذ دفتر العمل الذي يتوقع الشريك استلامه (نفس الأوراق، نفس ترقيم الحالات، نفس التخطيط)، ولكن معبأ بنتائج حقيقية بدلاً من حقول فارغة.



ما الذي يتم ملؤه

تتم كتابة ثلاث فئات من المعلومات في دفتر العمل.

1. نتائج لكل حالة

لكل حالة في الكتاب، يتم تعيين خلية النتيجة في دفتر العمل إلى الحكم المسجل (**نجاح**، **فشل**، أو **لم يتم الأداء**). يتم ملء خلية التعليقات الخاصة بالحالة بالأدلة الداعمة التي تم التقاطها خلال التشغيل.

في المستند	يأتي من
نتيجة حالة الاختبار (نجاح / فشل / لم يتم الأداء)	حكم الحالة
تعليقات حالة الاختبار	الأدلة: التوقيتات، السعة، أسباب الشبكة، قراءات الاستجواب، إلخ.

2. الهويات والبيانات الوصفية

يتم ملء قسم الرأس ومعلومات المشغل من التشغيل:

في المستند	يأتي من
IMSI	الاختبار SIM بطاقة
MSISDN	الاختبار SIM بطاقة
PLMN (أ) المنزل / PLMN (ب) الزائر	لمختارة للكتاب PLMNs / شريك التجوال
تاريخ الاختبارات	تاريخ التشغيل
اسم المختبر، الهاتف، البريد الإلكتروني	تفاصيل المختبر في الكتاب
APN (حيثما ينطبق)	تكوين البيانات المستخدم

3. القيم المقاسة

بالنسبة لحالات البيانات والخدمات الإضافية، يتم كتابة القيم المقاسة المحددة التي يطلبها ورقة GSMA في خلاياها المخصصة:

يأتي من	في المستند
جلسة البيانات	أوقات بدء / انتهاء جلسة البيانات
سجلات شحن البوابة الخدمية	أحجام البيانات المرسلة / المستلمة
جلسة البيانات	مدة الجلسة
قياس السعة	السعة / متوسط معدل البيانات
نتيجة الحالة	مؤشرات نجاح الخدمة (نعم / لا)

إخراج نظيف وقابل للتقديم

الفارغة مع محتوى أمثلة ومحتوى نائب في خلايا الملء: توقيتات نموذجية GSMA تشحن قوالب بإزالة م��توى نائب ذلك OmniRoam وملاحظات مرجعية تهدف إلى توجيه مختبر يدوي. يقوم عند إنشاء المستند، لذا يظهر دفتر العمل المكتمل فقط نتائجك الحقيقية وحقول فارغة حيث لم يتم التقاط قيمة. لا يحمل أبداً بيانات نموذج البائع إلى تقريرك المقدم، ولا يكتب أبداً على تسميات أو العناوين أو الهيكل GSMA.



removed



متى يتم الإنشاء

يمكنك تنزيل المستند في أي وقت. إنه يعكس دائماً الحالة الحالية للتشغيل. التدفق النموذجي هو تشغيل الكتاب (أو الروتين المجدول)، مراجعة أحكام كل حالة، إعادة تشغيل أي حالات تحتاج إلى

اهتمام، ثم تنزيل دفتر العمل النهائي بمجرد أن تبدو النتائج صحيحة. لأن التصدير يعكس التشغيل المباشر، فإن إعادة التصدير بعد إعادة التشغيل ببساطة ينتج مستنداً محدثاً.

الحالات اليدوية في المستند

تظهر الحالات التي لا يمكن لـ OmniRoam قيادتها تلقائياً في دفتر العمل مع رقم الحالة وعنوانها، جاهزة للمختبر لتسجيل نتيجة يدوياً. هذا يحافظ على اكتمال المستند المقدم: يتم ملء الحالات الآلية بأدلة حقيقية، وتُعرض الحالات اليدوية في المكان الصحيح ليقوم المختبر بإكمالها.

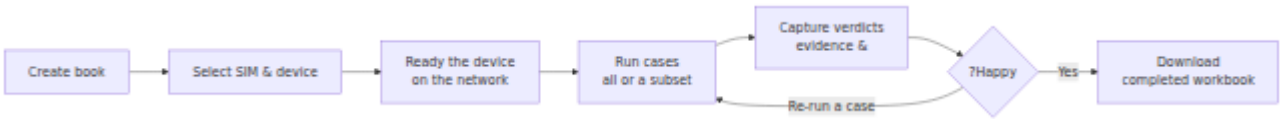
للحصول على تخطيط Test Book Explorer راجع تشغيل الاختبارات لمعرفة كيفية إنتاج الأحكام و دقيق خلية بخلايا لما يتم ملؤه.

تشغيل اختبارات OmniRoam

تغطي هذه الدليل دورة حياة اختبار التجوال بالكامل: إنشاء كتاب، تشغيله، مراقبة تنفيذ الحالات، تخصيص الحالات التي يتم تشغيلها، إعادة تشغيل حالة واحدة، وجدولة عمليات تشغيل روتينية غير مراقبة.

- دورة حياة الاختبار
- إنشاء كتاب اختبار
- تشغيل كتاب
- كيفية تشغيل الحالات الآلية
- تخصيص عملية التشغيل
- إعادة تشغيل حالة واحدة
- تشغيلات روتينية ومجدولة
- قراءة النتائج

دورة حياة الاختبار



إنشاء كتاب اختبار

تعرض شاشة كتب اختبار التجوال كل كتاب مع نوعه، الشبكات المنزلية والزائرة، هوية المشترك، المختبر، والحالة الحالية.

يتم إنشاء كتاب اختبار من شاشة **كتب اختبار التجوال**. عند إنشاء كتاب، تختار:

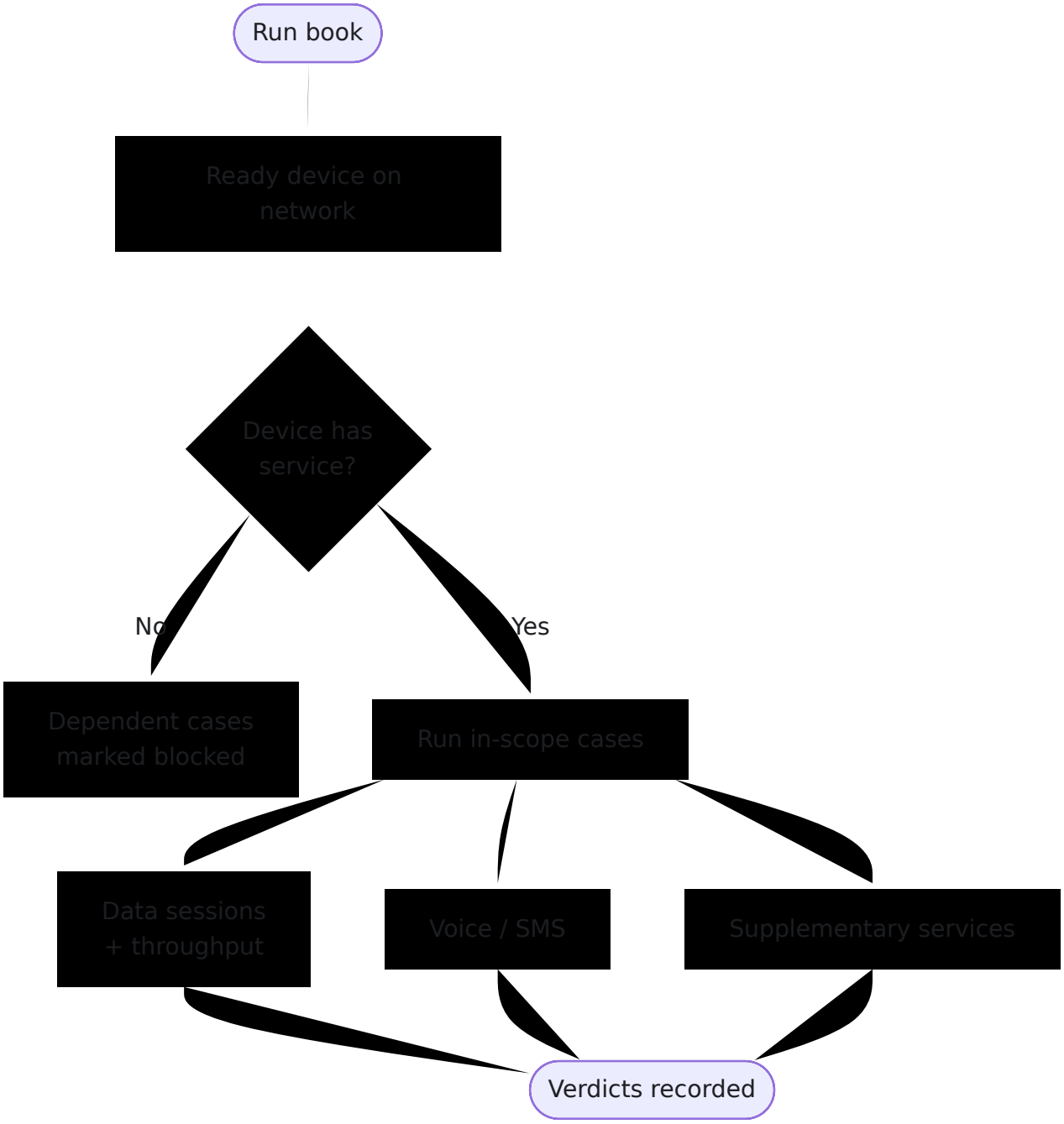
الحقل	الغرض
نوع الكتاب	أي كتاب GSMA لتشغيله: IR.38، IR.48، أو VoLTE. هذا يحدد مجموعة الحالات.
شريك التجوال / PLMNs	الشبكات المنزلية (PLMN a) والزائرة (PLMN b). تستخدم لملء رأس الوثيقة ولتحديد عتبة الإنتاجية الصحيحة.
SIM	بطاقة SIM يتم قراءة MSISDN و IMSI الخاصة بالمشترك لاختبارها. الخاصة بها واستخدامها طوال فترة التشغيل وفي الوثيقة النهائية.
تفاصيل المختبر	اسم، هاتف، وبريد إلكتروني للشخص المسؤول، مكتوب في دفتر العمل المكتمل.

المختار، كل منها تبدأ في حالة "لم يتم GSMA بمجرد إنشائه، يسرد الكتاب كل حالة من الكتاب تنفيذها بعد".

تشغيل كتاب

يؤدي تشغيل كتاب إلى تنفيذ كل حالة ضمن النطاق بالتتابع. قبل تشغيل حالات الاختبار، يقوم OmniRoam بتحضير جهاز الاختبار على الشبكة. يعرض بطاقة SIM ويؤكد أن الجهاز قد اتصل وتوفر الخدمة. هذه هي **بوابة المتطلبات**: إذا لم يتمكن الجهاز من الحصول على الخدمة، يتم الإبلاغ عن الحالات المعتمدة على أنها محجوزة بدلاً من فاشلة، لأنه لا فائدة من اختبار البيانات أو الصوت بدون حامل.

بقراءة هوية المشترك من المودم وملء OmniRoam كجزء من تحضير الجهاز، يقوم ويتم ا��تقاق **الشب���ة المنزلية** SIM، من بطاقة **الكتاب تلقائيًا IMSI**: يتم قراءة من الشبكة التي يتواجد عليها الجهاز **(VPLMN)** منها، ويتم قراءة **الشبكة الزائرة (HPLMN)** حاليًا. هذه تملأ رأس الكتاب، وبالتالي الوثيقة المكتملة، بما تم اختباره فعليًا، بدلاً من القيم التي تم كتابتها يدويًا.



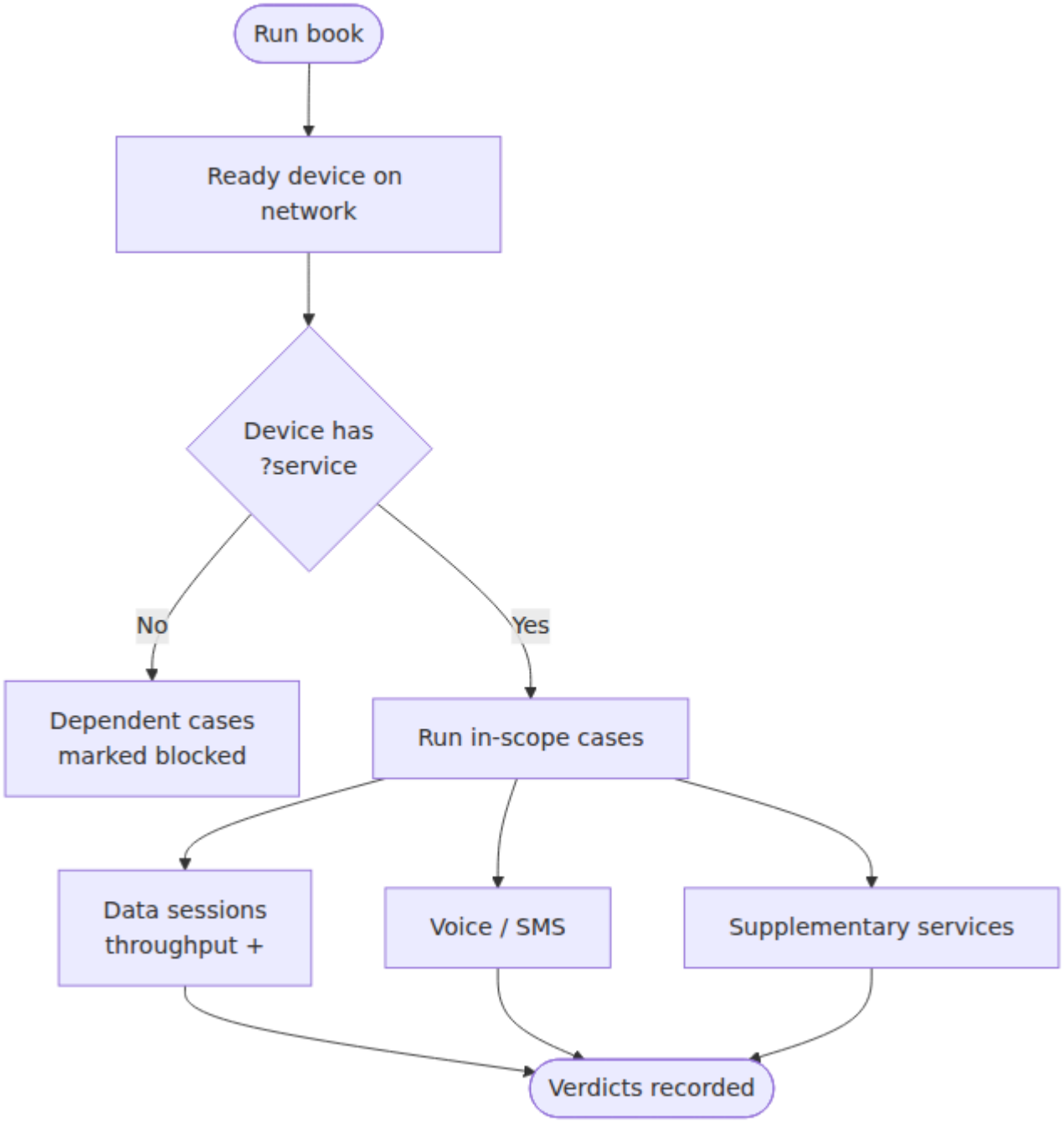
أثناء تشغيل الكتاب، تعرض الشاشة كل خطوة كما تحدث، مع تسليط الضوء على الخطوة الحالية وإشارة حية للنجاح/الفشل لكل حالة.

كيفية تشغيل الحالات الآلية

تقوم كل حالة آلية بتوجيه جهاز الاختبار، تراقب ما تفعله الشبكة، وتقارن النتيجة مع النتيجة المتوقعة من GSMA. تمر الحالة فقط عند وجود دليل إيجابي. ��تم تسجيل خطوة لا يمكن تأكيدها كفشل مع السبب، وليس كنجاح صامت.

جلسات البيانات والإنتاجية

بإنشاء جلسة بيانات حزم، ويقوم بتشغيل حركة المرور OmniRoam بالنسبة لحالات البيانات، يقوم لقياس معدل التنزيل/التحميل المحقق والكمون، ثم يفصل الاتصال حتى تكتب الشبكة سجل شحن نظيف للجلسة. يتم قراءة أحجام البيانات والتوقيتات من سجلات شحن بوابة الخدمة. بالنسبة لحالة IR.38، يتم التأكيد على المعدل المقاس مقابل الحد الأدنى للإنتاجية للمسافة المنزلية/ سرعة الزائرة.



المكالمات الصوتية

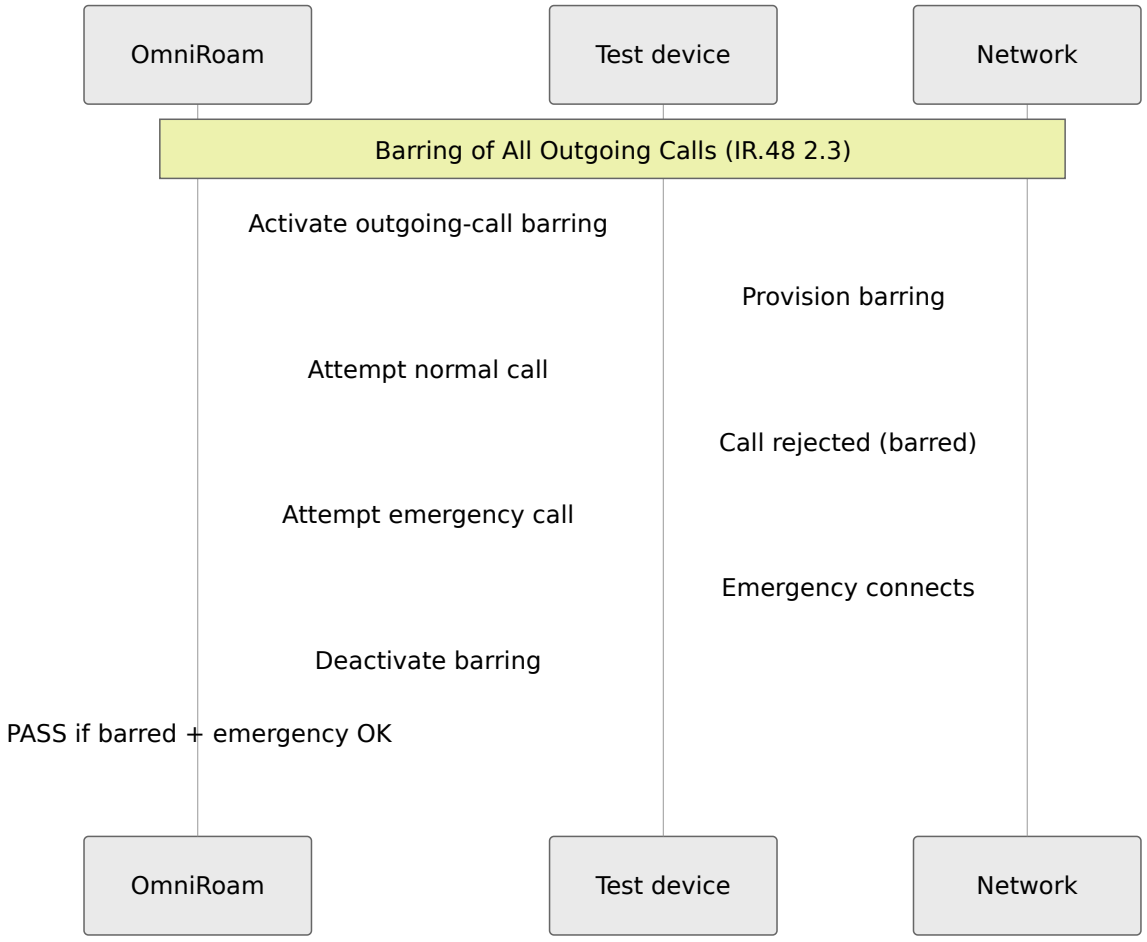
يقوم OmniRoam بإجراء مكالمة من الجهاز إلى خدمة الرد في المختبر، ويؤكد أن المكالمة وصلت إلى الحالة النشطة (المستجيبة)، ويحتفظ بها اختياريًا لتأكيد الاستقرار، ثم يقوم بإلغائها. تسجل النتيجة الوقت المستغرق للاتصال وما إذا كانت المكالمة قد استمرت.

الرسائل القصيرة

يقوم OmniRoam بإرسال رسالة تحتوي على نص فريد إلى خدمة الرد في المختبر وينتظر الرد. تؤكد تسليم الرد على الرسائل القصيرة المرسلة من الهاتف المحمول والمستلمة من الهاتف المحمول من النهاية إلى النهاية. يعد الرد المفقود فشلًا واضحًا مع السبب، وليس انهيارًا.

الخدمات التكميلية (حظر المكالمات وإعادة التوجيه)

يقوم OmniRoam بتوفير الخدمات التكميلية عبر الهواء من جهاز الاختبار نفسه، تمامًا كما يفعل المشترك مع رموز التحكم في الخدمة القياسية، ثم يقوم بتجربتها:



بتسجيل إعادة التوجيه OmniRoam بالنسبة لـ **إعادة توجيه المكالمات عند عدم الرد**، يقوم إلى رقم مستهدف مع مؤقت رنين، ثم يستجوب الخدمة ويؤكد أن الشبكة قد خزنت رقم إعادة

التوجيه والموقت الذي تم تسجيله.

إلغاء الموقع (IR.38 3.1.2)

يطلب LTE، تُدار بعض الحالات من جانب الشبكة بدلاً من الجهاز. بالنسبة لـ **إلغاء الموقع** من خادم المشترك المنزلي إلغاء موقع المشترك على الشبكة الزائرة، ويسجل OmniRoam النجاح عندما يتم قبول الطلب. هذا يؤكد أن الشبكة المنزلية يمكنها سحب تسجيل التجوال.

تسجيل IMS (VoLTE)

بالنسبة لـ VoLTE، يؤكد OmniRoam أولاً أن الجهاز مسجل في IMS. هذه هي بوابة الحالات والرسائل VoLTE إذا لم يتم تأكيد التسجيل، يتم الإبلاغ عن حالات مكالمات IMS: المعتمدة على IMS القصيرة عبر على أنها محجوزة.

تخصيص عملية التشغيل

لا يتعين أن تغطي عملية التشغيل الكتاب بالكامل. باستخدام **محدد الاختبار**، يختار المشغل بالضبط الحالات التي سيتم تشغيلها. هذا مفيد لـ:

- إعادة التحقق فقط من الحالات التي فشلت سابقًا.
- تشغيل حالات الصوت فقط، أو حالات البيانات فقط، أثناء البحث عن الأخطاء.
- تخطي الحالات التي تعتمد على ترتيب لم يتم وضعه بعد (على سبيل المثال، اتفاقية CAMEL).

تحتفظ الحالات التي تم استبعادها من النطاق بالحكم الحالي الخاص بها ولا تتأثر.

إعادة تشغيل حالة واحدة

تمتلك كل حالة تحكم لإعادة التشغيل. يؤدي اختيارها إلى تشغيل تلك الحالة مرة أخرى فقط، ضد نفس الجهاز وبطاقة SIM، ويقوم بتحديث حكم تلك الحالة فقط. هذه هي أسرع طريقة لتأكيد إصلاح (على سبيل المثال، إعادة تشغيل حالة الإنتاجية بعد تغيير النقل) دون تكرار الكتاب بالكامل.

تشغيلات روتينية ومجدولة

يمكن لـ OmniRoam تشغيل الاختبارات **غير المراقبة وفقًا لجدول زمني** بحيث يتم التحقق من علاقة التجوال باستمرار بدلاً من التحقق منها مرة واحدة.

- **التحقق الروتيني** يقوم بتشغيل مجموعة مضغوطة من اختبارات الصحة ضد جهاز (بيانات، سرعة، صوت، ورسائل قصيرة) ويبلغ عن نجاح/فشل مجمع. هذه هي نفس المحركات المستخدمة من قبل الكتب الكاملة، معبأة كاختبار ثقة سريع متكرر.
- **الجدول الزمني** يقوم بتشغيل روتين مختار على فترات متكررة تلقائيًا. يسجل كل تشغيل مجدول نتائجه الخاصة، مما يبني تاريخًا بمرور الوقت بحيث يتم اكتشاف التراجع (على سبيل المثال، انخفاض الإنتاجية دون الحد الأدنى، أو فشل تسليم الرسائل القصيرة) ويكون مرئيًا دون الحاجة إلى أي شخص لتشغيل اختبار يدويًا.



إعداد جدول زمني

تُدار الجداول الزمنية على شاشة **الجداول الزمنية** تحت اختبارات التجوال. يعرف الجدول الزمني:

الإعداد	الغرض
الاسم	يحدد الجدول الزمني (ويضع علامات على مقاييسه وتاريخه).
المودم (مودمات)	جهاز الاختبار (الأجهزة) التي يتم تشغيل الروتين ضدها.
التحقق	أي التحقق الذي يقوم به الروتين: بيانات، اختبار سرعة، صوت، رسائل قصيرة.
الفترة	كم مرة يتم تشغيل الروتين (على سبيل المثال، كل ساعة).

بمجرد حفظه، يتم تشغيل الجدول الزمني تلقائيًا في فترته دون أي تفاعل إضافي. تعرض شاشة **اختبار الروتين** تاريخ التشغيل: نجاح/فشل كل تشغيل مجمع، السرعات المقاسة، وتفاصيل كل تحقق. يظهر التشغيل الفاشل نفس الأدلة مث�� التشغيل التفاعلي.

مراقبة Prometheus

يتم تصدير نتائج الروتين المجدولة كـ **مقاييس Prometheus**، بحيث يمكن تنبيه صحة التجوال ومراقبتها جنبًا إلى جنب مع بقية الشبكة، بنفس الطريقة التي تتم بها مراقبة الاختبارات المجدولة (يقرأ أحدث تشغيل `/api/ir38/routine/metrics` على أجهزة الاختبار. يتم تقديم العرض في مجدول لكل جدول زمني ومودم):

المقياس	النوع	المعنى
`omniweb_ir38_routine_pass`	gauge	أحدث نتيجة روتين مجدولة (1 = نجاح، 0 = فشل)
`omniweb_ir38_routine_check_pass`	gauge	نتيجة كل تحقق من أحدث تشغيل (التسمية `check`: بيانات/اختبار سرعة/ صوت/ رسائل قصيرة)
`omniweb_ir38_routine_download_mbps`	gauge	معدل التنزيل المقاس في أحدث تشغيل
`omniweb_ir38_routine_upload_mbps`	gauge	معدل التحميل المقاس في أحدث تشغيل
`omniweb_ir38_routine_latency_ms`	gauge	الكمون المقاس في أحدث تشغيل

المعنى	النوع	المقياس
وقت Unix لأحدث تشغيل مجدول	gauge	`omniweb_ir38_routine_last_run_timestamp_seconds`

على `check` بالإضافة إلى) `imsi` و ،`modem` ،`serial` ،`schedule` تحمل كل سلسلة تسميات بحيث يمكنك تنبيه حسب الجدول الزمني، حسب الجهاز، أو حسب المشترك ،(المقياس لكل تحقق المنزلي. لا يحتاج نقطة النهاية إلى تسجيل دخول (لا يمكن للبرامج النصية حمل واحد) ويمكن أن يتم تأمينها باستخدام رمز حامل عند الحاجة.

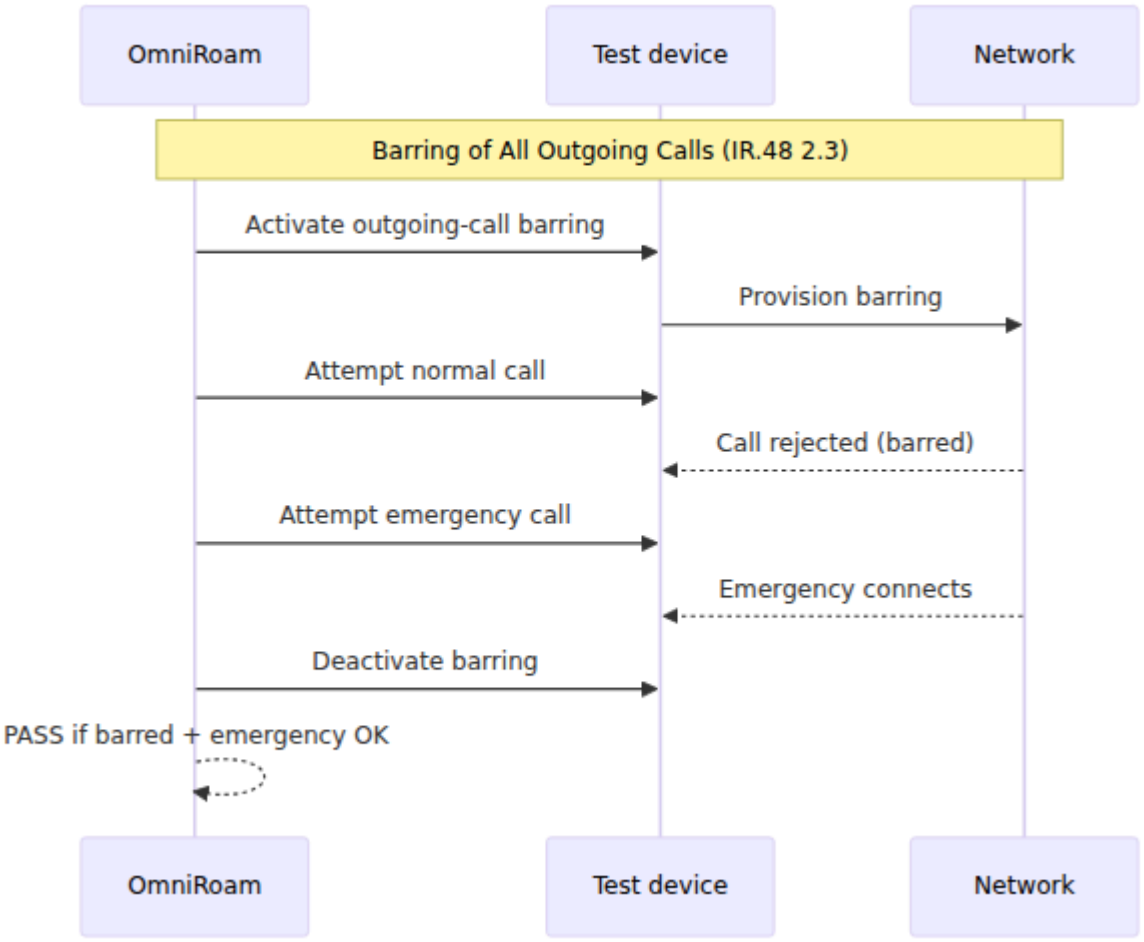
مثال على تنبيه: فشل الصوت التجوال على جهاز لمدة 15 دقيقة:

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

تتراكم النتائج المجدولة في تاريخ يمكن مراجعته في أي وقت، ويظهر التشغيل الفاشل نفس الأدلة مثل التشغيل التفاعلي.

قراءة النتائج

تظهر كل حالة حكمها (**نجاح**، **فشل**، أو **لم يتم التنفيذ**) مع الأدلة وراء ذلك:



- **نجاح**: تم تأكيد النتيجة المتوقعة من GSMA، مع الأرقام الداعمة.
- **فشل**: لم يتم تحقيق النتيجة المتوقعة؛ يتم تسجيل السبب (على سبيل المثال، "الإنتاجية أقل من الحد الأدنى"، "لا رد صدى"، أو سبب تحرير الشبكة لمكالمة لم تتصل).
- **لم يتم التنفيذ**: لم يتم تشغيل الحالة، أو هي حالة يدوية تنتظر مختبرًا.

عندما تبدو النتائج صحيحة، قم بإنشاء الوثيقة المكتملة. انظر وثائق كتاب الاختبار المكتمل.

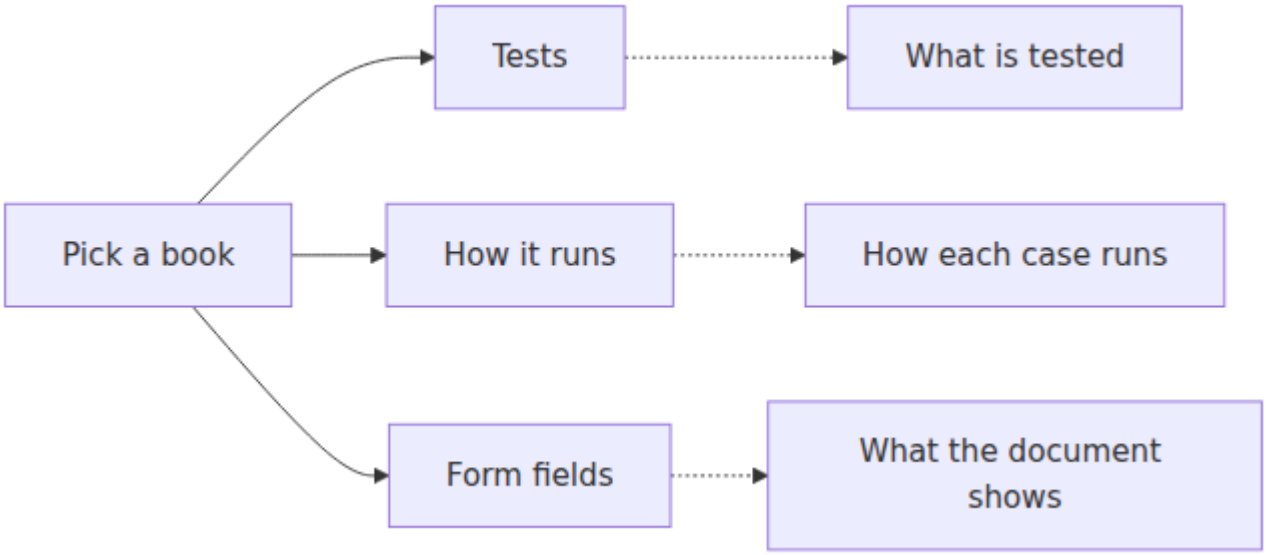
مستعرض كتاب الاختبار

مستعرض كتاب الاختبار هو عرض مرجعي للقراءة فقط يُظهر، لكل كتاب اختبار، بالضبط ما الذي يتم اختباره وكيف. يجيب على ثلاثة أسئلة عادةً ما يسألها المشغل قبل الوثوق بتشغيل آلي:

1. **ما الحالات الموجودة في هذا الكتاب، وأيها مؤتمت؟**
2. **كيف يتم تنفيذ كل حالة فعليًا؟**
3. **ما الذي يظهر في الوثيقة المكتملة، ومن أين يأتي؟**

يمكن الوصول إلى المستعرض من شاشة كتب الاختبار المتجولة عبر **استكشاف الكتب**، ويسمح لك بالتبديل بين IR.38 و IR.48 و VoLTE.

كل حالة مدرجة مع ما إذا كانت مؤتمتة أو يدوية ووصف لكيفية تشغيلها.



الاختبارات

عرض **الاختبارات** يسرد كل حالة في الكتاب مع:

- **رقم الحالة** و **العنوان** (مطابق لمواصفة GSMA)،
- ما إذا كانت الحالة **مؤتمتة** أو **يدوية**، و
- وصف بسيط لـ **كيفية تشغيلها**: على سبيل المثال "جلسة بيانات + تحقق من سجل الشحن"، "مكالمة صوتية"، "تفعيل الحظر ومحاولة الاتصال"، أو "المختبر يسجل النتيجة" للحالات اليدوية.

هذه هي أسرع طريقة لرؤية، بنظرة سريعة، مقدار ما يقوم به OmniRoam من كتاب معين وما يبقى كتحقق يدوي.

كيفية التشغيل

عرض **كيفية التشغيل** يُظهر **تسلسل الخطوات** الذي ستقوم به عملية تشغي كاملة للكتاب، بالترتيب: تجهيز الجهاز، جلسات البيانات، تحقق من معدل النقل، محركات الصوت والرسائل القصيرة، محركات الخدمات الإضافية، وهكذا. يعكس الحالات الموجودة حاليًا في النطاق، لذا فهو معاينة دقيقة لما ستفعله عملية التشغيل قبل أن تبدأها.

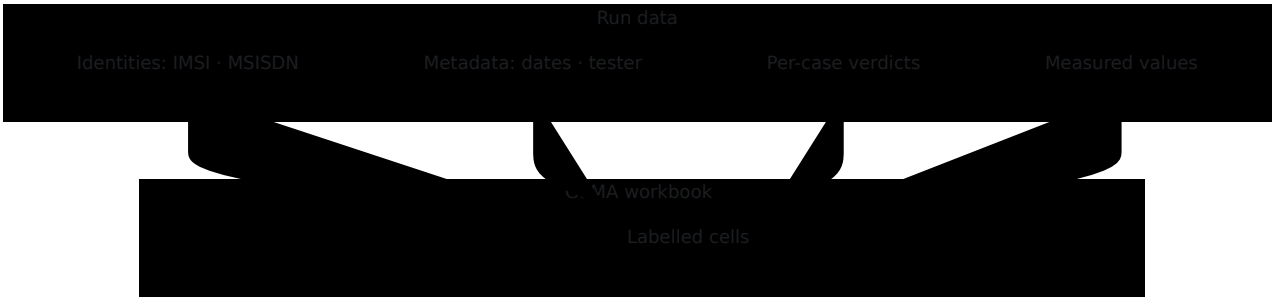
هذا العرض مفيد لفهم شكل عملية التشغيل ولتأكيد أن النطاق المخصص سيؤدي الخطوات التي تتوقعها.

حقول النموذج

عرض GSMA الذي يملأه **حقول النموذج** يسرد كل خلية في دفتر العمل المكتمل من OmniRoam، كل منها مشروح بـ:

- GSMA في قالب **الورقة والخلية**،
- **تسمية حقل GSMA** (مقروءة من القالب نفسه)، و
- **مصدر** القيمة: على سبيل المثال رقم MSISDN /حكم النجاح، تاريخ الاختبار، للمشترك الفشل لكل حالة، أو قيمة مقاسة مثل حجم البيانات.

نظرًا لأن هذه القائمة مستمدة من نفس المنطق الذي ينتج الوثيقة، فلا يمكن أن تنحرف عن الخطوة الفعلية مع التصدير: ما يقوله المستعرض بأنه سيتم ملؤه هو بالضبط ما يتم ملؤه. انظر وثائق كتاب الاختبار المكتمل للحصول على الوثيقة نفسها.



تنزيل القالب

يقدم المستعرض أيضًا إجراء **تنزيل القالب**، والذي يقوم بتنزيل دفتر العمل الفارغ من GSMA للكتاب المحدد: القالب الرسمي مع محتوى المثال/المكان المحجوز الخاص بالبائع تمت إزالته، جاهز للتعبئة يدويًا إذا لزم الأمر. هذا هو النظير الفارغ للوثيقة المكتملة التي تنتجها عملية التشغيل (انظر وثائق كتاب الاختبار المكتمل).

لماذا الأمر مهم

شريك التجوال الذي يقبل كتاب اختبار مكتمل يحتاج إلى الثقة بأن النتائج حقيقية وأن الوثيقة تمثل بدقة ما تم اختباره. يجعل المستعرض التخطيط شفافًا: يمكن تتبع كل حالة مؤتمتة من رقم الحالة في GSMA، من خلال الطريقة التي يتم تشغيلها بها، إلى الخلية الدقيقة التي تصل إليها في الوثيقة النهائية.

OmniRoam كتب اختبار

تقوم OmniRoam بشحن ثلاثة كتب اختبار تجوال GSMA. كل كتاب هو مجموعة الاختبار الرسمية الخاصة بها بحيث تتطابق الوثيقة GSMA مع تحديد الحالات بواسطة أرقام حالات GSMA، المكتملة واحد لواحد مع المواصفة المنشورة.

- IR.38: اختبار بيانات تجوال LTE
- IR.48: التجوال الثنائي (صوت / SMS / MMS / بيانات)
- VoLTE: اختبار تجوال VoLTE

لرؤية كيفية تشغيل كل حالة آلية وتقييمها، انظر تشغيل الاختبارات. لتصفح حالات الكتاب بشكل تفاعلي، استخدم مستكشف كتاب الاختبار.

تقوم بتنفيذ الحالة تلقائيًا (**آلي**) أو OmniRoam في الجداول أدناه، **مدفوع** يشير إلى ما إذا كانت تتركها للمختبر لتسجيلها (**يدوي**).

IR.38: اختبار بيانات تجوال LTE

يثبت أن المشترك المتجول يمكنه الاتصال بالبيانات على شبكة **GSMA IR.38 v3.0** استنادًا إلى الزائرة، والوصول إلى الخدمات من خلال الشبكة المنزلية، واستقبال معدل نقل مقبول. كما LTE حيثما تكون ضمن النطاق، 2G/3Gوبيانات، SMSيثبت أيضًا الصوت الاحتياطي عبر الدائرة و.

الحالة	العنوان	مدفوع	ما يثبته
`3.1.1`	اختبار سرعة LTE (البيانات + معدل النقل)	آلي	يتم إنشاء جلسة بيانات من خلال بوابة المنزل، تحمل حركة المرور، وتفي بحد معدل النقل.
`3.1.2`	إلغاء الموقع LTE	آلي	يمكن للشبكة المنزلية إلغاء موقع المشترك على الشبكة الزائرة (تم تفعيله من خادم المشترك المنزلي).
`3.1.3`	حظر محدد من المشغل LTE	يدوي	يتم احترام الحظر المحدد من المشغل لمطبق في سجل المشترك المنزلي.
`3.2.2`	الصوت الاحتياطي عبر الدائرة: مكالمة صوتية منشأة من الهاتف المحمول	آلي	تنجح مكالمة صوتية منشأة من المشترك عبر الصوت الاحتياطي.
`3.2.3`	الصوت الاحتياطي عبر الدائرة: مكالمة صوتية متجهة إلى الهاتف المحمول	يدوي	تنجح مكالمة إلى المشترك عبر الصوت الاحتياطي.
`3.2.4`	SMS عبر SGs	آلي	تعمل SMS المنشأة من الهاتف المحمول والمتجهة عبر واجهة SGs.
`3.3.1`	الوصول إلى البيانات من 2G/3G باستخدام PGW في HPLMN	آلي	تصل جلسة بيانات 2G/3G إلى الخدمات من خلال بوابة المنزل.
`3.4`	الوصول إلى البيانات من 4G + 5G NSA عبر S8	آلي	تتوفر بيانات الحزمة وتصل إلى الإنترنت (تم تأكيدها من خلال جلسة بيانات مع فحص الاتصال).

إلغاء الموقع (3.1.2)

تقوم OmniRoam بأتمتة إلغاء الموقع من خلال طلب من خادم المشترك المنزلي لإلغاء موقع المشترك على الشبكة الزائرة، ثم أكيد قبول الطلب. هذا هو الإزالة التي تبدأها الشبكة

المنزلية لتسجيل التجوال (3 وفقًا لإجراء إلغاء الموقع في GPP TS 29.272).

معدل النقل KPI

الحالة `3.1.1` تفعل أكثر من تأكيد جلسة البيانات. إنها تقيس معدل التنزيل المحقق وتؤكد ذلك مقابل حد معدل النقل في IR.38. يعتمد الحد على المسافة الجغرافية بين الشبكات المنزلية والزائرة (تسمح المسارات الأطول بمعدلات أقل):

البروتوكول	المسافة > 4000 كم	المسافة ≤ 4000 كم
HTTP	≥ 11 Mbit/s	≥ 5 Mbit/s
FTP	≥ 13.5 Mbit/s	≥ 6 Mbit/s

تقوم OmniRoam بتقدير المسافة من هويات الشبكة المنزلية والزائرة وتختار العتبة الصحيحة تلقائيًا؛ يمكن للمشغل تجاوز المسافة أو البروتوكول عندما لا تتطابق الافتراضات مع إعداد الاختبار. لا يتم اعتبار تسجيل السرعة دون اختبارها مقابل الحد كنجاح.

IR.48: التجوال الثنائي (صوت / SMS / MMS / بيانات)

الكتاب الكلاسيكي للتجوال (IR.24). داخليًا مجموعة اختبار **GSMA IR.48 v2.1** استنادًا إلى 2G/3G: و الثنائيالمكالمات الأساسية، والخدمات التكميلية، SMS، وبيانات الحزمة، تم اختبارها لمشترك تجول إلى الشبكة الزائرة.

الحالة	العنوان	مدفوع	ما يثبته
2.1	MS2(a)، يتصل بـ MS1(a) كلاهما تجول في VPLMN(b)	آلي	يتم إنشاء مكالمة صوتية أساسية وتستمر.
2.2	اختبار سلبي CAMEL (MOC، مسبق الدفع، لا يوجد اتفاق)	يدوي	يتم حظر مكالمة مسبقة الدفع بشكل صحيح CAMEL حيث لا يوجد اتفاق نشط.
2.3	حظر جميع المكالمات الصادرة (BAOC)	آلي	مع تفعيل حظر المكالمات الصادرة، تفشل المكالمات العادية بينما لا تزال المكالمات الطارئة تنجح.
2.4	إعادة توجيه المكالمات عند عدم الرد (CFNRY)	آلي	يمكن تسجيل إعادة توجيه المكالمات عند عدم الرد واستجوابها، مع تأكيد التكوين المخزن.
2.5	SMS المنشأة / المتجهة من الهاتف المحمول	آلي	يتم تسليم SMS المرسلة من المشترك المتجول ويتم استلام رد.
2.6	اختبار سلبي CAMEL (SMS-MO، مسبق الدفع)	يدوي	سلوك SMS مسبق الدفع حيث لا يوجد اتفاق CAMEL نشط.
2.7	الوصول إلى الشبكة الداخلية / مزود خدمة الإنترنت باستخدام بوابة المنزل	آلي	تصل جلسة بيانات إلى الإنترنت / الشبكة الداخلية من خلال بوابة المنزل.
2.8	MMS باستخدام بوابة المنزل وMMSC	يدوي	يتم تسليم رسالة وسائط متعددة عبر MMSC المنزلية.

الخدمات التكميلية في IR.48

حالتان من الخدمات التكميلية مؤتمتة بالكامل:

- **BAOC (2.3):** تقوم **حظر جميع المكالمات الصادرة.** بتفعيل حظر OmniRoam المكالمات الصادرة على المشترك الاختباري، وتؤكد أن مكالمة صادرة عادية تم رفضها

من قبل الشبكة، وتؤكد أن مكالمة طارئة لا تزال تتصل (الاستثناء الم��لوب)، ثم تزيل الحظر ليبقى بطاقة SIM نظيفة.

- **CFNRY (2.4): إعادة توجيه المكالمات عند عدم الرد.** تقوم OmniRoam بتسجيل إعادة توجيه المكالمات عند عدم الرد إلى رقم مستهدف مع مؤقت رنين، ثم تستجوب الخدمة (ما يعادل طلب رمز الحالة `*#61#`) وتؤكد أن الشبكة خزنت رقم إعادة التوجيه والموقت الذي تم تسجيله. يتطلب ملاحظة التحويل المباشر مكالمة واردة من طرف ثالث، لذا تُترك تلك المرحلة الأخيرة للتحقق اليدوي؛ يتم أتمتة الت provision والاستجواب.

تقوم OmniRoam بالإبلاغ عن حالة كل خدمة تكميلية باستخدام الأعلام الأربعة القياسية من 3GPP: **مُزود**، **مسجل**، **نشط**، و**خامل** (انظر 3GPP TS 23.011).

VoLTE: اختبار تجوال VoLTE

يثبت أن المشترك **GSMA IR.92** وفقًا لـ VoLTE، مع سلوك **GSMA BA.65 §5.3** استنادًا إلى IMS. يمكنه التسجيل في IMS وإجراء / استقبال مكالمات VoLTE وSMS عبر IMS أثناء التجوال.

الحالة	العنوان	مدفوع	ما يثبته
`ims_reg`	تسجيل IMS عبر التجوال	آلي	يقوم الجهاز بالتسجيل في IMS أثناء التجوال (المتطلب الأساسي لجميع خدمات VoLTE).
`mo_call`	مكالمة منشأة من الهاتف المحمول VoLTE	آلي	يتم إنشاء مكالمة منشأة من VoLTE وتستمر المشترك.
`mt_call`	مكالمة متجهة إلى الهاتف المحمول VoLTE	يدوي	يتم إنشاء مكالمة إلى المشترك عبر VoLTE.
`sms_ims`	SMS عبر IMS (SMSoIP)	آلي	يتم تسليم SMS عبر شبكة IMS.
`emergency`	مكالمة طارئة VoLTE	يدوي	تعمل المكالمات الطارئة عبر VoLTE (لا يتم الاتصال بها تلقائيًا).

بوابة تسجيل IMS

أولاً كـ **بوابة**: إذا `ims_reg` بتشغيل OmniRoam تقوم .IMS على تسجيل VoLTE تعتمد خدمات IMS (`mo_call`، لم يكن الجهاز مسجلاً في IMS، يتم الإبلاغ عن الحالات المعتمدة على `sms_ims`) عندما يكون VoLTE على أنها محجوبة بدلاً من الفشل. لا قيمة في الاتصال بمكالمة معطلاً، وتخبر النتيجة المحجوبة المشغل بالضبط لماذا IMS.

كيفية مقارنة الكتب



الكتاب	المجال الرئيسي	الأفضل لـ
IR.38	بيانات LTE / EPC	التحقق من علاقة بيانات التجوال LTE الجديدة ومعدل النقل
IR.48	2G/3G + عبر الدائرة حزمة	التحقق من الصوت، والخدمات التكميلية، و SMS والبيانات الأساسية
VoLTE	IMS	التحقق من تجوال VoLTE بمجرد أن تكون الربط بين في مكانه IMS

إدارة SIM عبر الهواء: RFM/RAM

عبر الهواء: تقرأ وتعدل الملفات على بطاقة بعيدة. ترسل **حزم** SIM تدير بطاقات **OTA** وحدة تحمل أوامر إدارة (ETSI TS 102 225 / 3GPP TS 31.115، "03.48" / SCP80) **مؤمنة** تتحقق البطاقة من كل حزمة وتفك (RAM). وإدارة التطبيقات عن بُعد (RFM) الملفات عن بُعد تشفيرها، وتنفيذ الأوامر، وتعيد **إثبات الاستلام (POR)** الموقع.

في الممارسة العملية، تعطيك نفس مستوى تحرير الملفات كما هو الحال في مستكشف نظام ملفات SIM: تصفح شجرة الملفات، فك تشفير EF، تعديل الحقول، وإعادة كتابتها. الفرق هو أن تصل إلى البطاقة PC/SC في المضيف المركزي، أو قارئ OTA **عن بُعد**: من خلال قارئ في الميدان. SIM إلى **SMPP** وكيل بعيد، أو عبر

يحدد الملف *أي* SIM. كما هو الحال في مخزن مفاتيح ICCID تستند إلى نفس مخزن المفاتيح لكل الفعلي لتلك البطاقة. لا يقوم **KIC/KID** *مجموعة مفاتيح وخوارزميات*، ويحتفظ مخزن المفاتيح بـ المحرك بتسجيل أو إعادة المفاتيح. إنه يعيد فقط النص المشفر الناتج و POR.

ما هي الحزمة المؤمنة

تحمي الحزمة المؤمنة أوامر APDUs من النهاية إلى النهاية، بغض النظر عن الناقل (العادي). تم التحقق من المحرك ضد بطاقات ISIM الفعلية.

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

CPL تحسب كل بايت بعد نفسها؛ **CHL** تحسب من SPI حتى بما في ذلك RC/CC/DS. عند تشغيل التشفير، يتم تشفير كل شيء من CNTR إلى النهاية ويتم إضافة أصفار إلى حجم كتلة التشفير، مع تسجيل **PCNTR** عدد البايتات التي تمت إضافتها.

- **TAR** (3 بايت، مرجع تطبيق مجموعة ال��دوات) يوجه الحزمة إلى خدمة على البطاقة: تطبيق RFM أو محدد RAM (مدير البطاقة).
- **SPI** يحدد خيارات التشفير، والتحقق من السلامة، وسياسة العداد، وما يجب أن يحتوي عليه PoR.
- **KIc / KID** تشير إلى أي مجموعة مفاتيح (تشفير) ومجموعة مفاتيح مصادقة تستخدمها البطاقة؛ **القيم** تأتي من مخزن المفاتيح لكل ICCID.

إعدادات الأمان بالكامل

يمكن ضبط كل مفتاح أدناه على ملف، وتم تنفيذ كل مجموعة. يقتبس بائع البطاقة هذه كأربعة بايت سداسية عشرية — MSL، PoR، KIc، KID — في `15213505` ويقبل الملف هذه الطريقة: ألصق ويتم ضبط كل مفتاح من ذلك. يعمل الحقل أيضًا بالعكس، حيث يظهر الأربعة بايت حقل **SPI** تتحدث بينما تقوم بتغيير مفتاح، بحيث يمكن قراءة الإعداد مقابل ورقة التخصيص.

بايت SPI	الإعداد	الخيارات
MSL	السلامة	تجزئة تشفيرية (CC)، لا شيء (RC)، تحقق من التكرار
MSL	التشفير	تشغيل / إيقاف
MSL	العداد	لا عداد؛ موجود ولكن غير محدد؛ يجب أن يكون أعلى؛ يجب أن يكون أعلى بواحد
PoR	المتطلبات	أبداً؛ دائماً؛ فقط عند الخطأ
PoR	سلامة الاستجابة	CC، RC، لا شيء
PoR	التشفير	تشغيل / إيقاف
PoR	الناقل	SMS-SUBMIT أو SMS-DELIVER-REPORT
KIc	خوارزمية التشفير	DES-CBC، triple DES-CBC 2-key، triple DES-CBC 3-key، DES-ECB، AES-CBC
KIc	إصدار المفتاح	1–3
KID	خوارزمية التجزئة	DES-CBC، triple DES-CBC 2-key، triple DES-CBC 3-key، AES-CMAC
KID	خوارزمية التكرار	CRC 16، CRC 32
KID	إصدار المفتاح	1–3

يعني بايت KID أشياء مختلفة على جانبي MSL: عندما يكون خيار السلامة هو **CC**، فإنه يسمي خوارزمية تجزئة، وعندما يكون **RC**، فإن نفس البتات تسمي CRC. يقوم محرر الملف بتبديل الخيارات لتتناسب، ويتبع طول RC — بايتين لـ CRC 16، وأربعة لـ CRC 32.

نفسه SPI تتوقف إصدارات المفاتيح عند 3 لأن سجل البطاقة يحمل ثلاث مجموعات مفاتيح؛ يسمح 15–1 ـ��.

المعلمات لكل مجموعة مفاتيح

1 يتم تخصيص بطاقة بخوارزمية **لكل مجموعة مفاتيح** — قد تكون مجموعة المفاتيح triple DES مع CRC بينما مجموعة المفاتيح 3 هي AES مع CMAC. هذا ينتمي إلى المفاتيح، وليس إلى الملف الذي يختارها، لذلك تحمل كل مجموعة مفاتيح في مخزن مفاتيح SIM SPI الخاص بها.

عندما تسجل مجموعة مفاتيح واحدة، يتم استخدام **الخوارزميات وإصدارات المفاتيح** بدلاً من تلك الخاصة بالملف، لأن الحزمة المبنية بأي شيء آخر يتم رفضها من قبل البطاقة. كل ما هو حقًا خيار المشغل — TAR، سياسة PoR، لا يزال — تنسيق الأمر، تنسيق التشفير، ما إذا كان يجب سياسة العداد، يأتي من الملف. تقارير المعاينة توضح أي الإعدادات جاءت من أين، بحيث يظهر الملف الذي يتعارض مع البطاقة قبل إرسال أي شيء بدلاً من أن يكون تسليمًا فاشلاً بعد ذلك.

مجموعة مفاتيح بدون SPI مسجلة لا تغير شيئًا: يظل الملف كما هو مكتوب.

يتم CC. أو RC يتم فك تشفير **إثبات الاستلام** مقابل نفس الإعدادات، بما في ذلك التحقق من الإبلاغ عن بايت الحالة بكلمات المواصفات الخاصة به — *PoR OK، RC/CC/DS فشل، CNTR محجوز، خطأ في التشفير، خطأ أمني غير معروف، ذاكرة غير CNTR، مرتفع CNTR، منخفض غير معروف، مستوى أمان غير كاف TAR، كافية، مزيد من الوقت مطلوب*.

تنسيق الأمر عن بُعد

مضغوط تكون نصوص الأوامر افتراضيًا في تنسيق :C-APDUs واحدًا تلو الآخر. يمكن للملف في C-APDU والذي يلتف حول كل ،(ETSI TS 102 226) اختيار التنسيق **الموسع** بدلاً من ذلك كخيار. ترد البطاقة (`AE`) مع ترميز غير محدد الطول، `AA` داخل قالب برمجة الأوامر TLV `22` واحد لكل أمر، بحيث يمكن تتبع نص فاشل إلى الأمر الذي فشل R-APDU يحمل `AF` أو `AB` بقالب بدلاً من مجرد آخر TARs لا تقبل أي شيء آخر. بعض ��لمة حالة.

APDUs الداخلية هي نص عادي C-APDU: `SELECT` + `READ BINARY` لقراءة RFM، `SELECT` + `UPDATE BINARY` للكتابة، GlobalPlatform `DELETE` / `INSTALL` لـ RAM.

على السلك (SMS-PP)، تحمل الحزمة في TP-User-Data مع معرف حزمة الأمر UDH (IEI `0x70`)، PID `0x7F` (تنزيل بيانات SIM)، DCS `0xF6` (8 bit، فئة الرسالة 2). يتم تسليمها داخل القالب كـ APDU CAT `ENVELOPE(SMS-PP-Download)` ويعود PoR بشكل متزامن.

تُقسم الحزمة الطويلة جدًا لرسالة قصيرة واحدة تلقائيًا، إما مع رأس التجميع 8 بت أو — عبر SMPP — مع معلمات `sar_*` بحيث يعيد SMSC تجميعها.

الملفات الشخصية، السياقات، والتوجيه التلقائي

ملف **OTA** **أي مواد مفتاحية** لا يحمل. إعداد أمان قابل لإعادة الاستخدام هو:

الحقل	المعنى
`tar`	مرجع تطبيق مجموعة الأدوات 3 بايت (الخدمة المستهدفة).
`kic_index` / `kid_index`	(1/2/3) أي مجموعة مفاتيح ← `KIC{n}`/`KID{n}` من صف مخزن مفاتيح البطاقة.
`cipher_algo` / `cc_algo`	خوارزمية التشفير والتجزئة (`triple_des_cbc2`، `aes_cbc`، ...).
`ciphering`، `rc_cc_ds`، `counter_mode`	SPI: هل يتم التشفير؟ CC مقابل RC؟ مقابل لا شيء؟ سياسة العداد.
`por`، `por_ciphered`، `por_rc_cc_ds`	هل يتطلب PoR؟ موقع؟ مشفر؟ ؟

تم تزويد ملفين، يتطابقان مع القيم التي تم التحقق منها على sysmoISIM:

- **RFM-USIM-3DES-keyset3**: TAR `B00011`، 3 ،3مجموعة المفاتيح DES، التشفير + CC، PoR مشفر + مطلوب + CC. يعمل داخل **ADF.USIM**.
- **RFM-SIM-3DES-keyset2**: TAR `B00010`، يعمل على 2. مجموعة المفاتيح شجرة **MF-rooted** 2G (DF.GSM / DF.TELECOM).

تحتاج التطبيقات المختلفة إلى خدمات مختلفة، لذا يقوم المستكشف **بتوجيه الملف الشخصي وسياق SELECT تلقائيًا لكل ملف**، من تطبيق الملف:

تطبيق الملف	السياق	الملف الشخصي (حسب TAR)	قبل Pre-SELECT ENVELOPE
`ADF.USIM`	`usim`	TAR `B00011`	`SELECT ADF.USIM` (حسب AID)
`DF.GSM`، `DF.TELECOM`	`sim`	TAR `B00010`	لا شيء (MF-rooted)
`ADF.ISIM`	`isim`	TAR `B00013`	`SELECT ADF.ISIM` (حسب AID)

قابلة للتجاوز في TAR، المفترضة من خلال مطابقة) يتوافق كل سياق مع أحد ملفاتك الشخصية (المستكشف). يقوم OmniWeb باختر بطاقة وانقر على أي ملف (USIM، GSM أو TELECOM). يعمل SELECT بتطبيق الملف الشخصي الصحيح، مجموعة المفاتيح و ISIM دون تبديل أي شيء. تختلف TAR حسب البطاقة) بمجرد أن تقوم بإنشاء ملف شخصي له (الخاصة به.

وسائل النقل

تشارك المحولات POR. تقوم وسيلة النقل بتوصيل الحزمة المؤمنة، وحيثما يسمح الناقل، تجمع القابلة للتوصيل واجهة واحدة:

النوع	يصل إلى	POR	ملاحظات
`local_pcsc`	بطاقة في قارئ PC/SC **على المضيف المركزي**	متزامن	مسار التحقق المتصل مباشرة.
`agent_reader`	بطاقة في قارئ **عند وكيل بعيد**	متزامن	الوكيل مثل WebSocket يركب نفس أجهزة الاختبار SIM / بنك (`session_apdu` relay).
`smpp`	**SIM ميداني** عبر SMPP `submit_sm`	غير متزامن	PoR ؛ يعود SMSC إلى MT SMS، أو على نفس MO SMS لاحقًا كـ الاتصال عند ربطه كمرسل. انظر **معلمات SMPP** أدناه.
`http_admin`	**SIM ميداني** عبر **HTTP (SCP81)**	غير متزامن	البطاقة المحفزة SMS تجعل رسالة تتصل بخادم الإدارة عن بُعد عبر TLS-PSK ؛ تتدفق النصوص + الاستجابات هناك. انظر **HTTP OTA** أدناه.

؛ يمكن أن(متزامن PoR يحتاج إلى) يستخدم **المستكشف** فقط وسائل النقل داخل القالب تستخدم SMPP. **الحملات** أيًا منها، بما في ذلك

معلمات SMPP

تختلف رسالة OTA القصيرة عن العادية في عدد قليل من المعلمات، وسيتقبل SMSC رسالة تحتوي على أخطاء فيها بصمت ولن يقوم بتسليمها إلى البطاقة. يمكن ضبط جميعها:

المعلمة	الافتراضي	لماذا هي مهمة
`esm_class`	`0x40`	يحدد بيانات المستخدم على أنها تبدأ برأس. بدونها، لا ترى البطاقة معرف حزمة الأمر.
`protocol_id`	`0x7F`	تنزيل البيانات (U)SIM.
`data_coding`	`0xF6`	بت، فئة الرسالة 2 8 — ما يوجه الرسالة إلى SIM بدلاً من صندوق الوارد.
`dest_addr_subunit`	`0x02`	الوحدة الفرعية المستهدفة هي SIM. المعلمة الأكثر شيوعًا التي تكون مفقودة عندما يتم قبول حزمة ولا تصل أبدًا.
`user_message_reference`	غير محدد	يتم تمريرها إلى MO PoR بواسطة معظم SMSCs، وهو ما يطابق غير المتزامن مع PoR وظيفته.
`registered_delivery`، `validity_period`، `priority_flag`، `service_type`، `schedule_delivery_time`، `replace_if_present_flag`، `sm_default_msg_id`	إعدادات SMSC الافتراضية	عناصر تحكم submit_sm العادية.

تقوم الحزم الطويلة بالتجزئة بثلاث طرق: رأس التجميع 8 بت في بيانات المستخدم (الافتراضي)، بحيث يعيد `sar_segment_seqnum` / `sar_total_segments` / `sar_msg_ref_num` معلمات

SMSC تجميعها، أو `message_payload` واحدة حيث يدعمها SMSC. يمكن إضافة أي معلم�ة اختيارية أخرى بالاسم.

SIM قبل الإرسال، ستقوم وسيلة النقل بالإبلاغ عن الإعدادات التي تكون صالحة ولكن لن تصل إلى SIM — علم رأس مفقود، ترميز بيانات يؤدي إلى صندوق الوارد، وحدة فرعية مستهدفة ليست.

اكتشاف معلمات بطاقة

لا يمكن طلب من البطاقة أي TAR وإعدادات أمان تم تخصيصها بها. عندما تصل دفعة مع مفاتيح ولكن بدون وثائق، فإن **الملفات الشخصية ← اكتشاف المعلمات** تجدها من خلال الاستكشاف: تحاول كل مجموعة مفاتيح في البطاقة ضد مساحة المعلمات المحتملة وتبلغ عما تقبله البطاقة. يمكن تحويل النتيجة مباشرة إلى ملف شخصي باستخدام **استخدام**.

تحتاج هذه إلى وسيلة نقل داخل القالب — لا يمكن أن تجيب وسيلة نقل تخزين وإعادة توجيه على كل استكشاف.

تجعل شيئان المسح الساذج غير مفيد، وتتعامل عملية الاكتشاف مع كلاهما:

- **يتم رفض العداد المنخفض جدًا بصمت.** حيث يقول مستوى الأمان يجب *أن يكون العداد أعلى*، تعيد البطاقة عدادًا عند أو أقل من قيمتها المخزنة ولا تعيد شيئًا على الإطلاق TAR — لا خطأ، لا إثبات استلام. هذا لا يمكن تمييزه عن المفاتيح الخاطئة أو خاطئة. لذلك، يبدأ الاكتشاف بالعداد مرتفعًا؛ نظرًا لأن العداد يزيد فقط، فإن البدء مرتفعًا لا يكلف شيئًا.
- **يحدد بايت PoR مكان عودة الإجابة.** مع وجود البت 6 واضح، تجيب البطاقة في استجابة ENVELOPE رسالة SEND SHORT MESSAGE ؛ مع تعيينه، ترفع البطاقة استجابة ENVELOPE استباقية بدلاً من ذلك وتكون استجابة فارغة. راقب مسارًا واحدًا فقط، وإجابة صحيحة غير مرئية، لذا يتم البحث عن كلاهما.

يتم التعامل مع حالة TAR **منخفض** على أنها نجاح بدلاً من فشل: فهذا يعني أن المفاتيح و **CNTR** والخوارزميات ومستوى الأمان كلها مقبولة، وكان العداد فقط هو الخطأ. يتوقف الاكتشاف هناك ويحل العداد عن طريق مضاعفته، مما يستغرق عددًا قليلاً من الرحلات بدلاً من مواصلة المسح.

إذا لم يتم قبول أي شيء، فإن ذلك لا يخبرك حقًا بأي معلمة كانت خاطئة — الصمت هو استجابة البطاقة لكل نوع من الأخطاء.

> كل استكشاف مقبول يزيد من عداد البطاقة، ولا ينخفض العداد أبدًا.

التسليم عبر EF_SMS

على بطاقة في قارئ، (`3F00/7F10/6F3C`) `EF_SMS` يمكن أيضًا كتابة حزمة مباشرة في سجل مع وضع علامة على السجل بأنه غير مقروء. تعالج البطاقة ذلك تمامًا كما لو كانت قد وصلت عبر الهواء — لا SMSC ولا راديو. هذه هي الطريقة العملية لاختبار نص ضد بطاقة على مكتب أو في بنك.

المستكشف

`src/pages/ota/OtaExplorer.tsx`: محرر ملفات SIM عن بُعد.

1. اختر **ICCID المستهدف** (من مخزن مفاتيح SIM) و**وسيلة النقل**.
2. تصفح **كتالوج الملفات**: كل EF معروف من نموذج الملف غير المتصل (ADF.USIM، ADF.ISIM، DF.GSM، DF.TELECOM)، مجمعة حسب التطبيق وقابلة للبحث حسب الرمز / الاسم / الوصف.
3. اختر ملف ← **قراءة عبر** **OTA**. يتم تسليم القراءة المؤمنة RFM، ويتم فك تشفير ونموذج **حقل مطبوع** + ASCII، نص خام، SW آخر، حالة POR، ويتم عرض EF: (تم فك تشفيره إلى حقول مسماة).
4. يتم تعديل **الحقول** (يتم إعادة ترميزها تلقائيًا) أو **النص الخام**، ثم **اكتب عبر** **OTA**. إرسال RFM `UPDATE` المؤمنة ويتم **قراءة الملف مرة أخرى** تلقائيًا حتى ترى الحالة على البطاقة بعد الكتابة.

تكون عمليات القراءة / الكتابة مقيدة بإذن التحكم **وظيفة** `ota`؛ يتم تسجيل كل شيء كـ.

الحملات

`src/pages/ota/OtaCampaigns.tsx`: عملية محفوظة موزعة عبر مجموعة من بطاقات SIM: **استعلام مستهدف → ملف شخصي → عملية → وسيلة نقل**.

- في وقت التشغيل: قائمة SIM بنك **الاستعلام المستهدف** يتم تقييمه مقابل مخزون بادئة أو نطاق، وكيل، بنك. يتطابق استعلام فارغ عمدًا مع لا شيء IMSI، بادئة / ICCID (لا تفريغ عرضي).
- حذف / الحصول على GP، قراءة / تحديث ثنائي أو سجل RFM/RAM هي أمر **العملية** الحالة / التثبيت).
- هي إطلاق SMPP **التشغيل** ينشئ واحدة **وظيفة** لكل بطاقة متطابقة. الحملات عبر MO SMS) لاحقًا كـ POR يصل) ونسيان.

بحيث لا يمكن لاستعلام ذو أصابع سمينة أن (`CAMPAIGN_MAX_TARGETS`) يكون التشغيل محدودًا يطلق آلاف البطاقات في طلب واحد.

الوظائف

`src/pages/ota/OtaJobs.tsx`: كل تسليم OTA (قراءات / كتابات المستكشف وتشغيل) تعرض درج التفاصيل **حزمة الطلب المؤمنة** (النص المشفر)، و .POR مع حالتها و (الحملات أسرار البطاقة **لا** .(بيانات الاستجابة، SW الأوامر المنفذة، آخر) **إثبات الاستلام**، والنتيجة المفككة POR. **يتم تخزينها أبدًا** في وظيفة: فقط النص المشفر و

REST واجهة برمجة التطبيقات

(`/api/ota`، JWT، نوع عنصر RBAC `ota`)

الطريقة	المسار	الغرض
GET	`/profiles` · POST · `/profiles/<id>` PUT/DELETE	ملفات تعريف أمان OTA.
GET	`/campaigns` · POST · `/campaigns/<id>` GET/PUT/DELETE	الحملات.
GET	`/campaigns/<id>/targets`	معاينة بطاقات SIM التي يتطابق معها الاستعلام حاليًا.
POST	`/campaigns/<id>/run`	تنفيذ: وظيفة واحدة لكل بطاقة متطابقة.
GET	`/jobs`، `/jobs/<id>`	تاريخ الوظائف (تصفية حسب `campaign_id` / `iccid`).
GET	`/files/catalog`	كتالوج EF القابل للتصفح (نموذج الملف غير المتصل).
POST	`/explore/read`	قراءة EF واحد عبر OTA؛ تعيد الوظيفة + EF المفكك.
POST	`/execute`	تشغيل عملية واحدة (تحديث RFM، RAM، خام) ضد بطاقة واحدة.
POST	`/preview`	بناء الحزمة المؤمنة **بدون** إرسال — تعيد النص المشفر، إطارات SMS، العداد المستخدم والعداد التالي، تفصيل SPI.
POST	`/spi`	فك تشفير أربعة بايت إلى SPI الإعدادات المسماة، أو بناء البايتات

الطريقة	المسار	الغرض
		من الإعدادات. حسابات رياضية بحتة؛ لا تتضمن بطاقة أو مواد مفتاحية.
POST	`/discover`	التي SPI و TAR استكشاف بطاقة لـ تقبلها، مع إعطاء مفاتيحها فقط. تحتاج إلى وسيلة نقل داخل القالب؛ تزيد من عداد البطاقة.
POST	`/decode` · `/encode`	حقول مطبوعة ↔ EF فك تشفير بايت (غير متصلة).

مع JWT يمر المسؤولون دائمًا؛ بخلاف ذلك، يمنح إذن `simbank`/`ir38`: تعكس RBAC في طرقه يمنح التحكم. تُعتبر عمليات القراءة `POST` عرضًا، و `element_type == "ota"` كتحكم (تقوم بنقل حزمة إلى البطاقة). يتم توثيق المسارات تلقائيًا في مرجع API.

مخطط قاعدة البيانات

الجدول	الصف	أعمدة المفتاح
`ota_profiles`	إعداد أمان واحد	`name`، `tar`، `kic_index`/`kid_index`، الخوارزميات، أعلام SPI.
`ota_campaigns`	تفريغ محفوظ واحد	`name`، `profile_id`، `target_query` (JSON)، `operation` (JSON)، `transport` (JSON)، `status`.
`ota_jobs`	تسليم واحد إلى بطاقة واحدة	`iccid`، `operation`، `request_hex` (النص المشفر)، `response_hex` (POR)، `por_status`، `result` (JSON)، `status`.

المشار إليها لكل SIM)، مخزن مفاتيح) الموجود `simbank_keys` تعيش المفاتيح في جدول بواسطة فهرس مجموعة المفاتيح الخاصة بالملف الشخصي. **لا** يتم تكرارها هنا ICCID.

كيف يعمل

يتعامل محرك OTA ونموذج الملف غير TLVs CAT/SMS، مع التشفير، هيكل الحزمة المؤمنة RFM/RAM 03.48/SCP80. المتصل المطلوب لبناء وفك تشفير حزم يعمل في خدمة الخلفية. التسليم قابل للتوصيل عبر القارئ لدور الوكيل ويشارك الاتصال الوكيل لوسيلة النقل داخل القالب. SMPP، وقارئ الوكيل البعيد، ووسائل النقل المحلي.

ملاحظات الأمان

- من مخزن المفاتيح لبناء الحزم ولكن **لا يتم** كتابتها (KIC/KID) يتم قراءة أسرار البطاقة أبدًا في سجل التدقيق أو إعادتها في أ�� استجابة. يتم تخزين فقط طلب النص المشفر و POR.
- كتابة ملف مدمرة؛ يؤكد المستكشف قبل كل كتابة ويعيد قراءة النتيجة.
- يفشل) الحزمة المؤمنة هي 03.48 حقيقية: إذا تم العبث ببايت، ترفض البطاقة ذلك النصية أبدًا على السلك APDUs ؛ مع تشغيل التشفير، لا تظهر(CC.

HTTP OTA (SCP81 / RAM-over-HTTP)

بجانب SCP80 عبر SMS / تتحدث، القارئ OmniWeb **SCP81** — OTA المعتمد على HTTP وفقًا لـ **GlobalPlatform Card Spec v2.3 Amendment B**. بدلاً من SMS، مؤمن واحد، تفتح البطاقة **جلسة إدارة** **HTTP عبر TLS-PSK** وتقوم بتشغيل نص كامل.

```
 trigger SMS (SCP80) ─▶ card ─BIP OPEN CHANNEL─▶ TLS-PSK ─▶ Remote
Admin Server
                        RAS serves command scripts, collects
responses, ends with 204
```

- مؤمن يحمل *محفز جلسة الإدارة* SMS بإرسال `http_admin` — تقوم عملية **المحفز** ثم SMPP، عبر نفس الناقل (سياسة إعادة المحاولة، `psk_id`، URI / RAS مضيف) تقوم بجدولة **جلسة الإدارة**.

- **TLS-PSK — مشتق من مجم��عة مفاتيح OTA** مفتاح مسبق المشاركة **KIC/KID** وفقًا لـ TLS للبطاقة؛ لا شهادات. ملف تعريف **GlobalPlatform Amendment B §3.3.2** (تؤجل المواصفة ETSI TS 102 226 إلى): TLS 1.2 مع `TLS_PSK_WITH_AES_128_CBC_SHA256` / `TLS_PSK_WITH_NULL_SHA256`، مع `NULL` تعتبر مجموعات TLS 1.0/1.1. لبطاقات RFC 4279 الرجوع إلى مجموعات SCP80. صالحة هنا — النص مؤمن بالفعل تحت (فقط سلامة)
- **حلقة الإدارة** — تقوم البطاقة بعمل POST إلى RAS، الذي يقدم نص الأمر المجدول، ويجمع كل استجابة حتى تكتمل الجلسة.
- كل جلسة مباشرة: الحالة، تقدم (`/ota/admin-sessions`) تعرض جلسات الإدارة النص، وسلسلة الأمر→الاستجابة. تحمل **الوظيفة** النتيجة النهائية، تمامًا مثل وسائل النقل الأخرى.

يبقى التشفير (PSK، مشتقة) في جانب OTA (محفز مؤمن، لا تحمل **RAS** العامة ؛ `omniweb-ota-scp81`، خدمة Elixir/OTP) تنهي — أي مفاتيح TLS-PSK عبر وتسحب النصوص من الخلفية localhost. يعمل مع RFM/RAM UICC و الكلاسيكي eUICC (SGP.02). انظر `docs/ota-specs/HTTP_OTA_PLAN.md`.

PGW-C: بوابة بيانات الشبكة (طبقة التحكم)

تعتبر **PGW-C** في **بوابة بيانات الشبكة** من EPC. إنها نقطة النصف الخاص بطبقة التحكم. وتقوم بإعداد والحفاظ على كل SGW-C، إلى **S5/S8** الارتكاز لكل جلسة بيانات مشترك: تنهي الخاصة بالمشغل، وتختار **IP** من **مجموعة** IP وتخصص لجهاز المستخدم عنوان، **اتصال PDN**. كما أنها تدير سياسة الجلسة والرسوم عبر **Sx/PFCP**. وتتحكم في طبقة المستخدم (**UPF**) عبر للرسوم عبر الإنترنت. OCS إلى **Gy**للسياسة وجودة الخدمة، و PCF/PCRF إلى **Gx** :Diameter تعرض **SMF**. الوظيفة المعادلة هي G، للرسوم غير المتصلة. في النواة 5 **CDRs** كما أنها ترفع Diameter، وخريطة UPF، ونظراء IP، ومجموعات PGW-C، الجلسات الحية لـ OmniWeb التي يمكن الوصول Grafana الطو��ولوجيا وتاريخ الجلسات، وأدوات التشخيص. تحتوي لوحات إليها من نفس الصفحة على الاتجاهات طويلة الأمد.

← دليل العمليات

تعتبر PGW-C صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيلها في جرد الموقع، مع عرض أسطول حيث يتم نشر عدة منها. تمر جميع حركة المرور عبر وكيل الخلفية لذا تبقى خلف بوابة مصدقة واحدة. PGW-C، إلى واجهة برمجة التطبيقات الخاصة بـ OmniWeb لـ يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

حالة قراءة صحة على شاشة واحدة: **API** لـ PGW-C الحية وملخص لحالتها (عدد الجلسات، استخدام مجموعة IP النشطة، نظراء UPF ونظراء Diameter). إنها أسرع طريقة لتأكيد أن العقدة تعمل وت��مل الجلسات.

الجلسات

كل جلسة PGW هو مفتاحه **لجهاز IP** للمشترك مع **عنوان MSISDN**و **IMSI** نشطة، كل صف مفتاحه لجهاز IP عنوان، IMSI المخصص له. يمكن البحث عن الجلسات حسب **APNالمستخدم** و SGW، والناقلات PDN فتح جلسة يظهر حالتها الكاملة: اتصال .APN أو MSISDN، المستخدم يمكنك تعديل جلسة هنا. يمكن .Gx/Gy المختار، وسياق السياسة والرسوم الحية UPFالخادم و (UPF جديد إلى APN-AMBR الذي يدفع) للجلسة **AMBR** للمشغل ضبط الحالة الحية مثل المطلوبة التي تتحكم في تقارير تغيير الموقع. يمكن للمشغل أيضًا **حذف Gx** و**محفزات أحداث** جلسة لإجبار إطلاق مشترك عالق أو غير متعاون. نظرًا لأن المشغل يطبق التعديلات مباشرة على الحالة الحية، فإنها تدخل حيز التنفيذ على الفور.

تسرد نفس علامة ال��بويب في **عرض الأسطول** كل جلسة، PGW-Cs عندما يتم نشر عدة الخادم مقابل كل صف. يتم تمرير البحث إلى كل PGW-C عبر جميعها في جدول واحد، مع عرض يربطهم؛ فتح صف ينتقل إلى PGW-C مثيل، لذا يمكن للمشغل العثور على مشترك دون معرفة أي تلك الجلسة على مثيلها الخاص. يتم تسمية المثيل الذي لا يمكن الوصول إليه فوق الجدول، لذا لا يتم الخلط بين القائمة القصيرة وشبكة هادئة.

مجموعات IP

عناوين لجهاز المستخدم منها، كل منها يظهر PGW-C الخاصة بالمشغل التي تخصص IP مجموعات **حجمها**، وعدد **العناوين المخصصة** و**الاستخدام**. فتح مجموعة يسرد العناوين الفردية المخصصة. هنا تؤكد أن المجموعة ليست مستنفدة (المجموعة المستنفدة هي سبب شائع لفشل إعداد الجلسات) وترى أي مشترك يحمل عنوانًا معينًا.

نظراء UPF

كل منها يظهر **عنوان** ،**Sx/PFCP** عبر PGW-C الذين تتحكم فيهم (UPF) نظراء طبقة المستخدم التي تحمل طبقة PFCP فتح نظير يظهر تفاصيله. هنا تؤكد أن ارتباطات .PFCP و**حالة الارتباط IP** المستخدم لكل جلسة تعمل.

Diameter

نظراء Diameter الذين تتحدث إليهم PGW-C (الـ **PCF/PCRF** عبر **Gx** للسياسة و **OCS** عبر كل منها مع **اسم المضيف** و**حالة الاتصال**. فتح نظير يظهر تفاصيله. ،(للرسوم عبر الإنترنت **Gy** عندما يتم رفض الجلسات أو تقليلها، هنا تؤكد أن مسارات السياسة والرسوم تعمل.

التاريخ

سجل قابل للبحث ومقسم لأحداث دورة حياة الجلسة **: تم الإنشاء�� تم التعديل**، **تم الحذف**، **النقل** و**الفشل**. يمكنك تصفية الأحداث حسب النوع والبحث عنها حسب IMSI، MSISDN، عنوان IP أو TEID. هنا تعيد بناء ما حدث لجلسة مشترك معين مع مرور الوقت، بما في ذلك الفشل.

الطوبولوجيا

خريطة لـ PGW-C والجيران الذين تعمل معهم SGWs، و UPFsالتي تربط الجلسات لها: والجيران الذين يتصل بهم العقدة في Diameter. تتحكم فيها، ونظراء تعطي رؤية واحدة عن الإشارات وطبقة المستخدم.

اختيار UPF

مرشح UPF يتم وضع جلسة جديدة عليه، مع **حالة الصحة** الحالية لكل UPF القواعد التي تقرر أي إلى جهاز المستخدم. هنا تؤكد PGW-C التي تعيدها (خيارات تكوين البروتوكول) **PCO** و**تكوين** معين وتتحقق من أن جميع المرشحين في حالة صحية UPF لماذا تهبط ال��لسات على.

بحث UE

يعيد معلومات ذلك الجهاز، **IP** أو **عنوان MSISDN**، **IMSI** بحث مباشر عن مشترك واحد حسب إنها أسرع طريقة للعثور على جلسة مشترك واحد دون التمرير في قائمة الجلسات .PGW-C على الكاملة.

الرسوم

IMSI الحية لكل جلسة نشطة، كل صف مفتاحه هو **(Gy/OCS)** حالة **الرسوم عبر الإنترنت** للرسوم **Gy** وقابل للبحث بواسطة أي منهما. في لمحة، تظهر كل جلسة ما إذا كانت **MSISDN**و وما إذا ،(و**المجال** الذي تتحدث إليه **OCS** مع **معرف الجلسة**، و**مضيف**) عبر الإنترنت مفعل قد دفع المشترك إلى إعادة توجيه OCS تعمل أيضًا، وما إذا كان **(Gz)** كانت محاسبة **غير متصلة** URR **في حديقة مسورة**. فتح جلسة يوسع تفاصيل الرسوم الكاملة: الحصص **الممنوحة** لكل مقابل الحجم **المستخدم** (الرفع، التنزيل وإجمالي البايتات)، **إجراء الوحدة النهائية** الذي حدده وأي هدف إعادة توجيه. هذه هي الطريقة ،(Gz) عندما تنفد الرصيد، العدادات غير المتصلة OCS التي تقرأ بها حالة التحكم في الائتمان الحية لمشترك: ما إذا كان لديهم رصيد، وكم من منحهم قد استهلكوه، ولماذا قد تم تقليلهم أو إعادة توجيههم.

كسر الزجاج: تعليق الرسوم عبر الإنترنت. في أعلى علامة التبويب يوجد مفتاح على مستوى الإجابة OCS بالكامل. استخدمه عندما لا يمكن لـ PGW-C العقدة يعلق الرسوم عبر الإنترنت عبر وإلا سيفقد المشتركون الخدمة.

على الجلسات الحية. CCR-U عند الاتصال ولا CCR-I أي PGW-C أثناء تسليح المفتاح، لا ترسل لا تتأثر .OCS. يحرر الحدائق المسورة ويفتح الناقلات المقيدة، لذا يتم نقل الحركة بدون إذن ويمكن تقييمه لاحقًا CDRs الرسوم غير المتصلة: لا يزال يتم كتابة الاستخدام إلى.

لتسليح المفتاح، أعطه شيئين:

الحقل	مطلوب	الوصف
التعليق لمدة	نعم	المدة التي يبقى فيها المفتاح مسلحًا. يقوم بإلغاء تسليحه عندما تنتهي المدة. تحدد العقدة أطول قيمة تقبلها.
السبب	نعم	لماذا تم تعليق الرسوم. يتم تسجيله ضد التجاوز.
المسلح بواسطة	لا	من قام بتسليحه. الافتراضي هو عنوانك.
إرسال CCR-T على فصل	لا	معطل بشكل افتراضي. قم بتشغيله للإبلاغ عن الاستخدام الذي لم يوافق عليه OCS.

قدم سببًا حقيقيًا. يتم تسجيل السبب والمشغل، ويستمران بعد التحول الذي قام بتسليح المفتاح.

تظهر اللوحة الوقت المتبقي أثناء تسليح المفتاح. اضغط على **استئناف الرسوم** لإلغاء تسليحه على الفور. يقوم المفتاح أيضًا بإلغاء ت��ليحه عندما تنتهي مدته، وهو ما يمنع التجاوز المنسي من أن يصبح خدمة مجانية دائمة.

CDRs

للفوترة: صف واحد لكل **بدء** جلسة، **مؤقت** PGW-C سجلات **الرسوم غير المتصلة** التي تكتبها **IMSI** يحمل كل سجل .**MSISDN** أو **IMSI** و**توقف**، الأحدث أولاً، وقابل للتصفية حسب و**معرف الرسوم** الذي يربط سجلات جلسة معينة، ،**QCI**و **APN**للمشترك، و **IMEI**و **MSISDN**و و**ملف** ،**UE**و **PGW**و **S-GW** لـ IP و**بايتات الرفع/التنزيل** التي تم عدها لتلك الفترة، وعناوين **المصدر** الذي تم قراءة السجل منه. هنا تقوم بمصالحة استخدام البيانات لمشترك مقابل محاسبة التي يقوم المشغل بالفوترة بناءً عليها، وتتبع أي ملف سجل هبطت فيه جلسة (Gz) غير متصلة معينة.

اختبار Gy

للتحقق من مسار الرسوم عبر OCS ضد **Gy Credit-Control** أداة للمشغل تصدر **طلب** الإنترنت من النهاية إلى النهاية. تقوم بتزويد **IMSI** (مستخدم MSISDN/ وعدد بايتات مطلوب وخياراً) لفتح جلسة وطلب وحدات، وتختار نوع الطلب. استخدم **الأولي (CCR-I)** **تحديث** للإبلاغ عن الاستخدام النهائي **(CCR-T)** للإبلاغ عن الاستخدام وطلب المزيد، أو **إنهاء (CCR-U)** بتعيين مجموعة التصنيف، ومعرف سياق الخدمة، ومعرف PGW-C وإغلاقه. ثم أرسله. تقوم التطبيق المصرح به بشكل افتراضي. تأتي **إجابة التحكم في الائتمان** المحللة مرة أخرى على نفس الشاشة. على عكس علامات التبويب الأخرى، هذه **لا تسترد أي شيء عند التحميل**: إنها نموذج تقوم بتقديمه. عندما تتصرف الرسوم عبر الإنترنت بشكل غير صحيح، إنها أسرع طريقة لإثبات أن OCS قابل للوصول ويمنح الائتمان.

مراقب P-CSCF

أثناء VoLTE إلى أجهزة P-CSCF عنوان PGW-C تعيد .P-CSCF حالة وقياسات مراقب اكتشاف IMS. وتؤكد هذه العلامة أن الاكتشاف صحي حتى يمكن أن تستمر تسجيل PDN، إعداد

السجلات

لاستكشاف أخطاء عقدة PGW-C تقوم علامة التبويب **السجلات** بتتبع مخرجات السجل الحية لـ OmniWeb. دون مغادرة (Diameterو PFCP فشل إعداد الجلسات، أخطاء) واحدة

المراقبة

كلوحات PGW-C تُعرض اتجاهات عدد الجلسات، ومعدل النقل وغيرها من السلاسل الزمنية لـ Grafana، لا تقوم .OmniWeb يمكن الوصول إليها من صفحة العنصر بتكرار تلك الرسوم البيانية بشكل أصلي.

ذات صلة

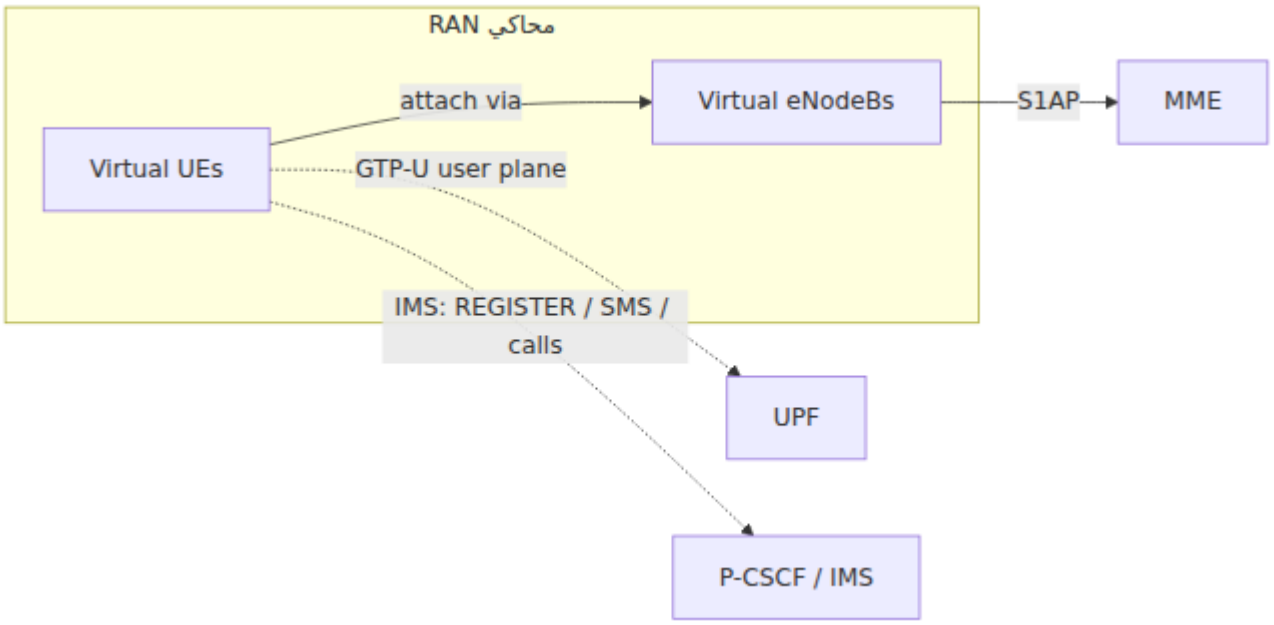
- الـ **SGW-C** هو نظير التحكم عبر **S5/S8** التي يربط الناقلات على جانب الوصول ؛ تتصل بها PGW-C بـ PDN.
- الـ **UPF** هو طبقة المستخدم التي تختارها PGW-C وتتحكم فيها عبر **Sx/PFCP**.
- الـ **PCF/PCRF** يوفر السياسة وجودة الخدمة عبر **Gx**.
- الـ **CHF/OCS** يقوم بالرسوم عبر الإنترنت عبر **Gy** كما ترفع ؛ PGW-C CDRs للرسوم غير المتصلة.

RAN محاكي

ممارسة شبكة النواة الحية بدون أجهزة راديو أو هواتف فعلية. يقوم بإنشاء **RAN** يتيح لك **محاكي** إلى البوابات، بحيث GTP-U و MME حقيقية إلى S1AP/NAS افتراضية تتحدث **UEs** و **eNodeBs** الرسائل القصيرة والمكالمات. IMS، يمكنك تشغيل عمليات الاتصال، جلسات البيانات، تسجيلات استخدمه للاختبار الوظيفي، اختبار التحميل، أو إعادة إنتاج سيناريوهات ميدانية، كل ذلك من OmniWeb.

← دليل العمليات

ما هو



يظهر كمنطقة **محاكي**، OmniWeb يعمل المحاكي جنبًا إلى جنب مع النوا�ة التي يستهدفها. في **RAN** خاصة به (خريطة الشبكة، eNodeBs، UEs، IMS، جداول السيناريو، اختبار التحميل). نظرًا الخاصة به تظهر أيضًا في **أجهزة الاختبار** بحيث UEs المحاكي يتصرف مثل جهاز، فإن UE لأن يمكنك التحكم فيها من نفس المكان مثل الهواتف الحقيقية.

بشكل افتراضي، يبدأ بدون **eNodeBs**. يمكنك إنشاء التوبولوجيا التي تريدها بالضبط.

eNodeBs

عند تشغيل eNodeB، يتم توصيله بـ MME (إعداد S1). يمكن توصيل eNB بـ **أكثر من MME** **واحد** (مجموعة MME). تظهر خريطة الشبكة مجموعة MMEs الكاملة التي ينتمي إليها eNB.

ويعود؛ يتم إنشاء رابط eNB من المحاكي تشغيل OmniWeb البدء هو **إطلاق ونسيان**: يطلب eNodeBs راقب خريطة الشبكة / قائمة) في الخلفية S1 (لتأكيد أنه تم تشغيله).

فصل eNodeB

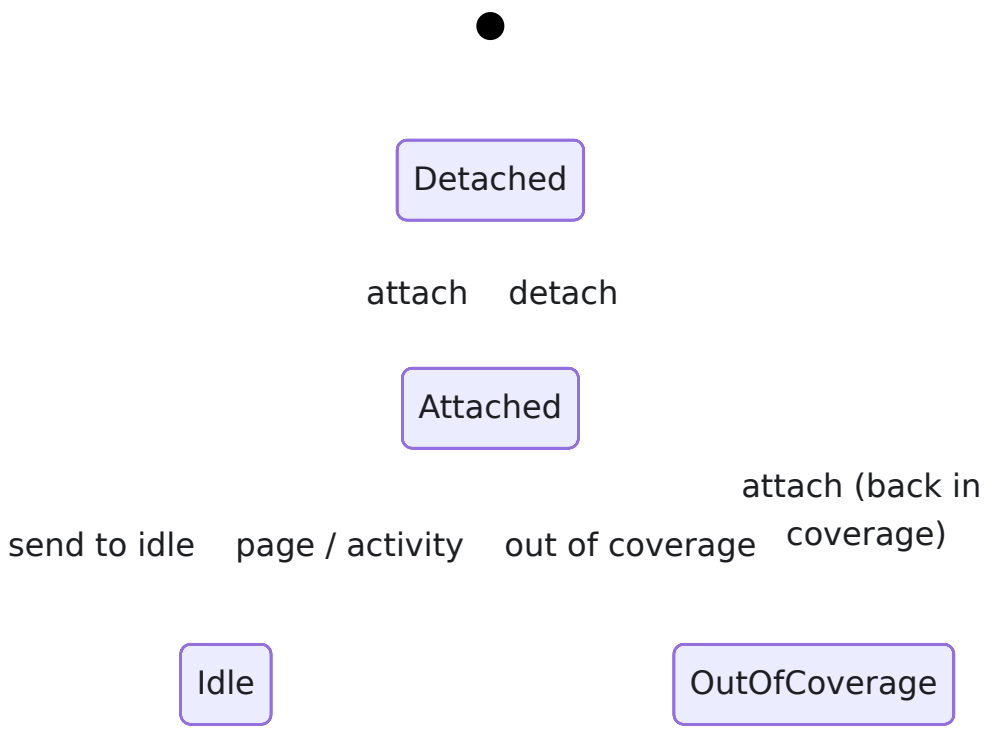
يمكنك إيقاف eNB بطريقتين، مما يمثل أحداثًا مختلفة في العالم الحقيقي:

الإجراء	النماذج	التأثير على UEs
فصل S1 النظيف	إيقاف تشغيل eNB بشكل منظم / إعادة تعيين S1	يتم تحرير UEs. **تنجو** و بشكل نظيف يعيدون الاتصال عندما يكون الرابط متاحًا
فصل الرابط	فقدان eNB لـ S1 المفاجئ (قطع الألياف، فقدان الطاقة)	يتم إلغاء ارتباط S1؛ UEs من **تنجو** وتعيد الاتصال بدلاً من أن يتم eNB مغادرة تدميرها

من المهم أن أخذ eNB **يدمر** لا لأسفل تستمر UEs الخاصة به. لذا يمكنك محاكاة انقطاع النقل دون إعادة بناء أسطول المشتركين لديك.

UEs

يمتلك كل UE محاكي دورة حياة يمكنك التحكم فيها مباشرة:

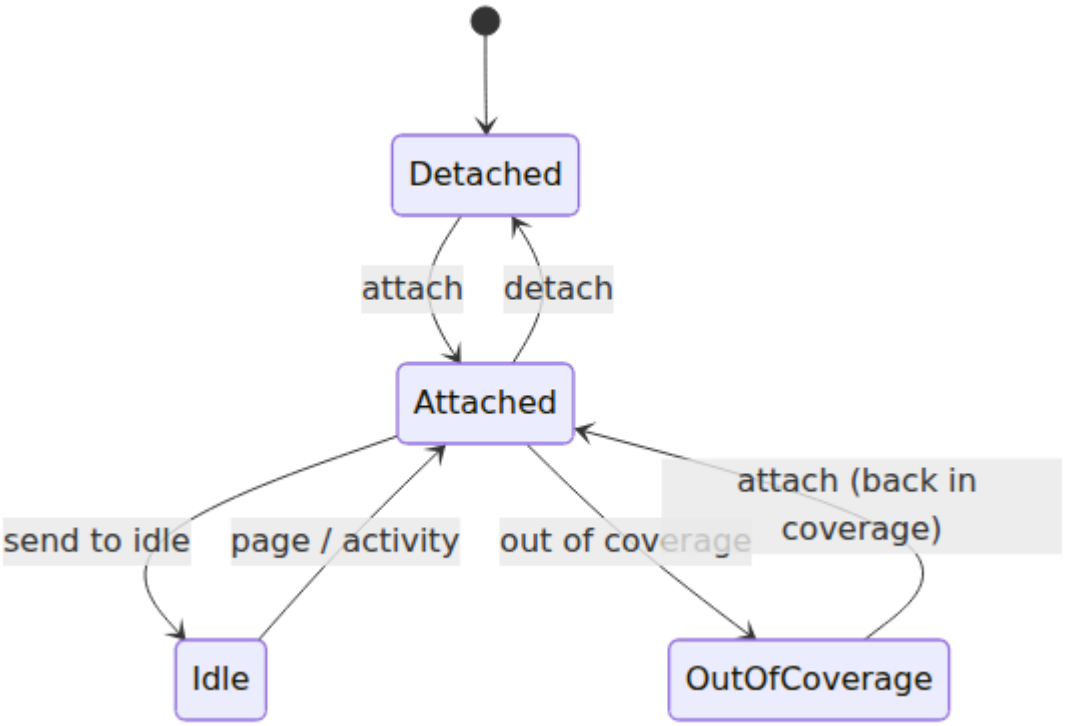


- **الاتصال / الفصل**: الانضمام أو مغادرة الشبكة.
- **إرسال إلى وضع الخمول**: الانتقال ECM-IDLE (كما يفعل UE الحقيقي بين الأنشطة). يجلبه الإشعار أو النشاط الجديد مرة أخرى.
- **خارج التغطية**: فقدان *غير نظيف* للإشارة (بدون إشارة يترك UE)، لاختبار كيفية تعامل UE النواة مع الذي يختفي ببساطة. يعيد الاتصال به إلى التغطية.

بالنسبة لكل UE، يظهر المحاكي **MME** الذي يتصل به: معرف مجموعة MME ورمز MME **الخادم** (الخاص بـ UE). لذا في نشر مجموعة، يمكنك رؤية أي MME استقبل كل GUTI المفكك من مشترك.

تسجيل IMS والموقع

عند التسجيل، يتضمن UE في المحاكي IMS وإجراء مكالمات SMS. **موقع الخلية** الخاص به (`P-Access-Network-Info` مع `utran-cell-id-3gpp` لخليته الخادمة)، ينقل هذا الموقع إلى S-CSCF من REGISTER الحقيقي. لذا فإن تسجيل UE تمامًا كما يفعل IMS المعتمد على الموقع من IMS وخوادم التطبيقات الأخرى. هذا يتيح لك اختبار سلوك TAS و SMSc النهاية إلى النهاية دون أجهزة راديو حقيقية.



من الأجهزة UEs التحكم في

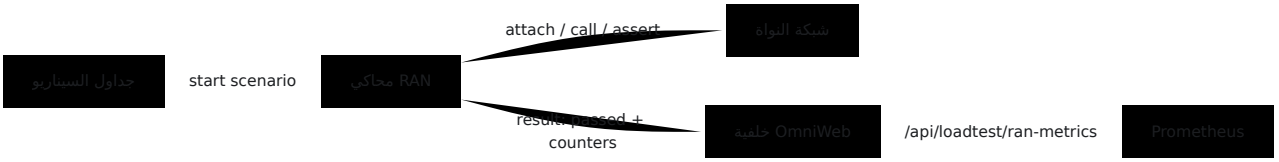
المحاكي هو مجرد جهاز آخر، فإنه يظهر في **أجهزة الاختبار** مع علامة كمحاكي، UE نظرًا لأن من خريطة شبكة UE سواء فتحت **UE** ويمكن تصفيته هناك. تستخدم **نفس لوحة التحكم لـ** أو من أسطول الأجهزة. إنه مكان واحد للاتصال / الفصل، وضع الخمول، التحكم في RAN محاكي أو إجراء مكالمة، ومراقبة سجل SMS إرسال رسالة، IMS الخروج من التغطية، التسجيل في الأحداث.

للتحكم في المشتركين المحاكيين جنبًا RAN الخاصة بمحاكي UEs قم بتصفية أجهزة الاختبار إلى إلى جنب مع الهواتف الحقيقية.

السيناريوهات المجدولة

الاتصال، وضع الخمول،) UE الـ **سيناريو** هو وصفة اختبار محفوظة: تسلسل مسمى من إجراءات التي يقوم المحاكي (ال��كالمة، الرسائل القصيرة، التحويل، الفصل، IMS الاستيقاظ، تسجيل على) بتشغيلها ضد النواة. يقوم المحاكي بشحن مكتبة من الإعدادات المسبقة، مجمعة حسب الفئة قم بتشغيل سيناريو مرة واحدة. (وحالات الرفض السلبية، VoLTE، سبيل المثال دورة حياة الاتصال من عرض اختبار التحميل، أو قم بتشغيله على جدول متكرر لمراقبة النواة باستمرار.

تدير صفحة **جداول السيناريو** (الشريط الجانبي: اختبار التحميل ← جداول السيناريو) عمليات التشغيل المتكررة. لكل جدول، تختار سيناريو وكم مرة لتشغيله. يسجل OmniWeb نتيجة النجاح أو الفشل لكل تشغيل ويصدرها إلى Prometheus، بحيث يمكنك التنبيه عليها ورسمها.



تشغيل سيناريو مجدول واحد في كل مرة، لأن OmniWeb تكون العمليات **متسلسلة**. يقوم ويضع حملًا حقيقيًا على النواة. إذا كانت عملية التشغيل لا UEs السيناريو يمكن أن يبدأ العديد من ويبدأها في الدورة الحرة التالية. OmniWeb تزال نشطة عندما يحين موعد الجدول التالي، ينتظر استخدم زر **تشغيل الآن** على جدول محفوظ لبدءه على الفور.

معلمات الجدول

الحقل	النوع	مطلوب	الافتراضي	الوصف
الاسم	سلسلة	نعم	-	تسمية فريدة للجدول. أيضًا تسمية `schedule` على المقياس المصدر.
السيناريو	سلسلة	نعم	-	السيناريو المسبق للتشغيل. يقوم المحدد بتجميع السيناريوهات حسب الفئة.
كل (ث)	عدد صحيح	لا	3600	كم مرة لتشغيل السيناريو، بالثواني. الحد الأدنى 60.
عدد UE	عدد صحيح	لا	100	عدد المشتركين الذين يعمل السيناريو عليهم.
RPS	عدد	لا	10	العدد المستهدف من السيناريوهات الجديدة في الثانية.
التزامن	عدد صحيح	لا	50	الحد الأقصى لعدد السيناريوهات النشطة في وقت واحد.
APNs	قائمة	لا	الافتراضي للسيناريو	APNs للاتصال، كقائمة مفصولة بفواصل. تتجاوز الافتراضي للسيناريو.

النجاح والفشل

تمر عملية التشغيل المجدولة **عندما** يبلغ المحاكي أن كل تأكيد قد نجح ولا يوجد سيناريو مشترك تم إلغاؤه. تفشل عملية التشغيل **إذا** فشل أي تأكيد أو تم إلغاء أي سيناريو. يمر السيناريو الذي لا يحتوي على تأكيدات طالما لم يتم إلغاء أي سيناريو. إذا لم يتمكن OmniWeb من بدء التشغيل، أو لم تنته العملية في الوقت المحدد، يسجل OmniWeb **خطأ** كـ العملية.

تظهر الصفحة جدول **التشغيلات الأخيرة** مع النتيجة، عدد التأكيدات، عدد السيناريوهات الملغاة، ومدة كل عملية تشغيل.

المقاييس

يكشف OmniWeb في Prometheus عن أحدث نتيجة لكل جدول بتنسيق `/api/loadtest/ran-metrics`. يقوم Prometheus بجمعها كوظيفة `ransim_scenarios`، والتي يتم تكوينها تلقائيًا من قبل دور المراقبة.

النوع: مقياس **الوصف**: نتيجة أحدث عملية تشغيل `ransim_scenario_pass` **المقياس**: مجدولة: `1` للنجاح، `0` لعدم النجاح **التسميات**:

- `schedule`: اسم الجدول
- `scenario`: معرف السيناريو الذي تم تشغيله
- `category`: فئة السيناريو
- `status`: نتيجة التشغيل (`passed`، `failed`، أو `error`)

تشارك المقاييس المصاحبة نفس التسميات:

المقياس	الوصف
`ransim_scenario_duration_ms`	مدة آخر عملية تشغيل، بالمللي ثانية
`ransim_scenario_assertions_passed`	التأكيدات التي نجحت في آخر عملية تشغيل
`ransim_scenario_assertions_failed`	التأكيدات التي فشلت في آخر عملية تشغيل
`ransim_scenario_scenarios_aborted`	السيناريوهات المشتركة الملغاة في آخر عملية تشغيل
`ransim_scenario_last_run_timestamp`	الوقت اليوني الخاص بآخر عملية تشغيل

استعلامات المثال:

```
# السيناريوهات التي لم تنجح آخر عملية تشغيل لها
ransim_scenario_pass == 0

# إجمالي فشل التأكيدات عبر جميع السيناريوهات المجدولة
sum(ransim_scenario_assertions_failed)

# جدول لم يتم تشغيله في الساعتين الماضيتين
time() - ransim_scenario_last_run_timestamp > 7200
```

لوحة معلومات Grafana

يشحن دور المراقبة لوحة معلومات **RAN** (مجلد Grafana **RAN**). تقرأ **سيناريوهات محاكي** المقاييس أعلاه وتظهر خط زمني للنجاح أو الفشل، أحدث نتيجة لكل جدول، فشل التأكيدات، نضارة السيناريو، ومدة التشغيل. قم بالتصفية حسب الفئة أو السيناريو أو الجدول في الأعلى. انظر Grafana.

الاستخدامات النموذجية

- **الاختبار الوظيفي**: تشغيل UE، eNB و الاتصال، بدء جلسة بيانات، التسجيل في IMS، إرسال رسالة SMS، ثم تأكيد سلوك كل عنصر نواة.
- **اختبار التحميل**: تشغيل العديد من UEs الجلسة / الاتصال / لتوليد حمل IMS ضد النواة (انظر عرض اختبار التحميل).
- **إعادة إنتاج السيناريو**: نمذجة الانقط��عات (فصل الرابط، خارج التغطية) وسلوك مجموعة MME لإعادة إنتاج وتشخيص المشكلات الميدانية.
- **المراقبة المستمرة**: جدولة سيناريو للتشغيل على مؤقت والتنبيه على مقياس النجاح أو الفشل (انظر السيناريوهات المجدولة).

ذات صلة

- أجهزة الاختبار: الهواتف الحقيقية و UEs واحد من مكان فيها التحكم يتم المحاكية،.
- تتبع الجلسة: ربط الإشارات التي يولدها المحاكي.

عن بُعد وبطاقة SIM بطاقة SIM افتراضية

يمكن لـ OmniWeb تقديم بطاقة **SIM** **لأي مودم عبر الشبكة**. يمكنه أيضًا تقديم **أي بطاقة** بمحاكاتها من صورة بطاقة محفوظة بالإضافة إلى مفاتيح OmniWeb **لا توجد فعليًا**: يقوم SIM ومحاكيات البطاقات SIM هذا يحول مجموعة من قراء بطاقات .HSS المشترك المحتفظ بها في والمودمات في موقع أو أكثر إلى مجموعة مشتركة. يمكن لأي مختبر تشغيل أي ("cardems") بلاستيكية إلى فتحة SIM ملف تعريف مشترك ضد أي مودم دون الحاجة إلى السير لحمل بطاقة بطاقة.

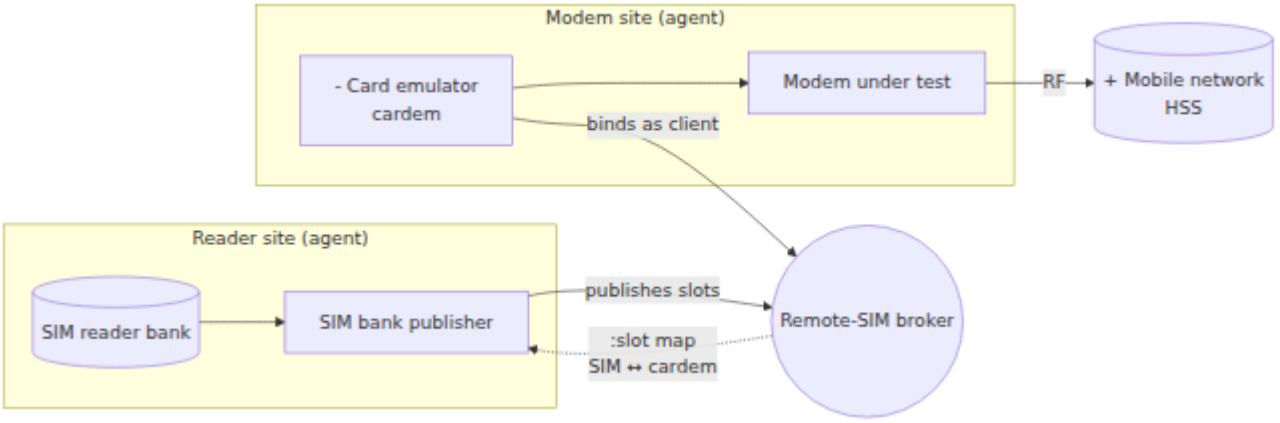
موجودة SIM تعد هذه الصفحة دليل العمليات لهذه القدرة. نصف **المخزون** يكتشف أي بطاقات SIM ��هذا النصف. تغطي هذه الصفحة كيفية **تقديم** بطاق SIM Bank في أي قراء. تغطي حزم ملفات تعريف SIM) إلى مودم واستخدامها في اختبار. تغطي صور (حقيقية أو افتراضية كيفية حفظ نظام ملفات بطاقة كحزمة ملف تعريف محمولة وكيفية استخدام واحدة لدعم SAIP) بطاقة SIM افتراضية.

جدول المحتويات

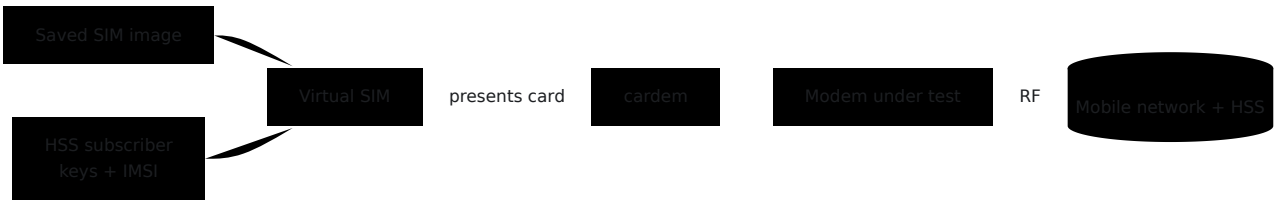
- نظرة عامة على المعمارية
- المفاهيم
- ما هو وأين :SIM بنك
- ربط بطاقة SIM عن بُعد: SIM بـ cardem
- وحدة تحكم Cardem
- SIM افتراضية: مشترك بدون بطاقة فعلية
- في كتاب اختبار التجوال SIM استخدام بطاقة
- استكشاف الأخطاء وإصلاحها

نظرة عامة على المعمارية

تتصل مجموعة قارئات بطاقة SIM، ومحاكيات بطاقات واحدة أو أكثر، والمودمات قيد الاختبار بـ cardem المختارة بـ SIM من خلال وكلاء الأجهزة. يقوم وسيط مركزي بربط فتحة OmniWeb تلك البطاقة إلى المودم المتصل به cardem المختار؛ ثم يق��م.



بناء OmniWeb **الافتراضية**، تحل بطاقة برمجية محل مجموعة القراء. يقوم SIM بالنسبة لبطاقة محفوظة ومفاتيح المشترك. كل شيء آخر متطابق SIM هذه البطاقة البرمجية من صورة:



المفاهيم

المصطلح	المعنى
بنك SIM	مجموعة من قارئات بطاقات الذكية على وكيل�� منشورة بحيث يمكن تقديم بطاقاتها في مكان آخر. كل قارئ مزدحم هو **فتحة** واحدة.
cardem	تجاه مودم متصل بها. SIM تتظاهر بأنها بطاقة (USB) لوحة محاكي بطاقة تقوم بتشغيل أي بطاقة تم ربطها بها.
خريطة الفتحة	إنشاؤها يربط الاثنين عبر "تقديم الربط cardem". **هذه** الفتحة إلى **تلك** الشبكة؛ وإزالتها تفصل بينهما.
المودم قيد الاختبار	المودم خلف cardem. يتصل SIM بالشبكة الحية باستخدام أي بطاقة تقدمها cardem.
SIM الافتراضية	محفوظة بالإضافة إلى مفاتيح SIM بطاقة برمجية مبنية من صورة SIM تمامًا مثل بطاقة cardem إلى OmniWeb المشترك. يقدمها حقيقية. لا تتطلب بطاقة فعلية.

بنك SIM: ما هو وأين

بإدراج كل فتحة قارئ على كل وكيل متصل، مجمعة حسب الوكيل. تخطيط **SIM** تقوم صفحة **بنك** البنك هو الحقيقة: الفتحات الفارغة وغير القابلة للقراءة والمستخدمة جميعها تظهر، وليس فقط المزدحمة.

*كل صف هو قارئ بطاقة فعلية واحدة. تُظهر شريحة الحالة ما إذا كانت بطاقة موجودة وقابلة للقراءة. ثم يُظهر الصف هوية SIM (ICCID، IMSI، MCC/MNC، اسم المشغل، البلد). تُظهر القراء المحفوظة التي SIM المحتفظ بها بجلسة محاكاة نشطة على أنها **قيد الاستخدام**. تظهر بطاقات قارئها غير متصل حاليًا تحت **تم رؤيتها سابقًا**. تعود للظهور عندما يعيد الوكيل الاتصال مع إدخال بطاقة SIM.*

شريحة الحالة	المعنى
SIM	بطاقة موجودة وتم قراءة هويتها.
البطاقة موجودة	بطاقة موجودة فعليًا ولكن لم يمكن قراءة هويتها (مثل توافق غير متوافق بين القارئ/البطاقة).
قيد الاستخدام	القارئ SIM محتفظ به بواسطة جلسة عن بُعد/محاكاة في الوقت الحالي.
فارغ	لا توجد بطاقة في الفتحة.

لتلك الفتحة بالضبط، **APDU** أو **محطة SIM** تفتح الإجراءات لكل صف مستكشف **نظام ملفات** وإعادة **المسح** تعيد قراءة قراء الوكيل عند الطلب.

cardem بـ SIM عن بُعد: ربط بطاقة SIM

تعد صفحة **SIM** المكان الذي تربط فيه بطاقة **عن بُعد** SIM بـ cardem. تعمل الروابط **عبر** cardem/mode في قارئ في موقع واحد و SIM **الوكلاء والمواقع**: يمكن أن تكون بطاقة موقع آخر.

الخطوات

1. **بدء بنك SIM** بدء (**bankd**). هذا ينشر فتحات قارئه.
2. **بدء عميل cardem** (**بدء العميل**). هذا يربط لمحاكي البطاقة الذي تريد استخدامه به. بحيث يمكن ربط بطاقة cardem SIM.
3. **ربط بطاقة** تحت **SIM**، اختر فتحة منشورة واختر cardem لربطها به. يتم إنشاء الربط ويظهر تحت **الربط النشط** كـ **نشط**.
4. ا��ظر وحدة تحكم) تلك البطاقة إلى مودمه. أعد ضبط المودم cardem الآن يقدم cardem) المقدمة حديثًا ويتصل SIM حتى يقرأ بطاقة.

إلى حالة الخمول. استخدمها cardem **إعادة تعيين عالمية** تقوم بتفكيك جميع الروابط وتعيد كل للتعافي من منصة اختبار مشوشة.

الحقل (الروابط النشطة)	المعنى
الحالة	`ACTIVE` بمجرد أن يقدم cardem بطاقة SIM.
SIM (البنك/الفتحة)	بنك أي وكيل والفتحة التي تعيش فيها البطاقة.
ICCID	بطاقة SIM المقدمة.
cardem (العميل/الفتحة)	أي cardem (وأي وكيل) يقدمها.
بواسطة	المشغل الذي أنشأ الربط.

وحدة تحكم Cardem

بجانب ،(`ngff-cardem`) محاكي بطاقة كنوع جهاز خاص به OmniWeb في **الأجهزة**، يظهر بتسمية أنواع الأجهزة غير OmniWeb المودمات والهواتف. لا يتم فتحه أبدًا كجهاز هاتف. يقوم المعروفة بوضوح بدلاً من تخمينها.

للحصول على وحدة تحكم مخصصة للمحاكي ومودمه cardem افتح.

التحكم	ماذا يفعل
بدء العميل	يربط cardem كعميل SIM عن بُعد بحيث يمكن ربط بطاقة SIM به.
إعادة ضبط المودم	يعيد تقديم البطاقة المحاكية، مما يجعل المودم يعيد قراءة بطاقة SIM ويعيد تشغيل الاتصال. هذه هي الطريقة التي "تبدل بها بطاقة SIM" دون لمس الأجهزة.
SIM عن بُعد	الاتصال أو فصل أي SIM هذا إلى يتم تقديمه عن بُعد cardem.

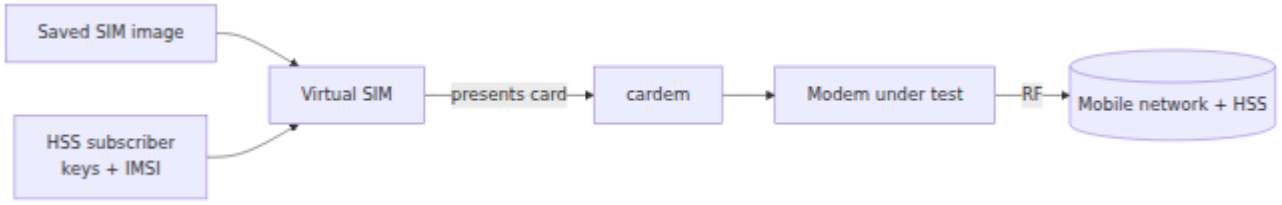
توضح لوحة **مصدر SIM** المودم بطاقة cardem بصراحة ما هو متاح وما ليس متاحًا: تغذي بطاقة SIM *محلية* موضوعة على لوحة المحاكي. تقول *عن بُعد*. لا تقدم وحدة التحكم بعد خيار تقديم بطاقة وحدة التحكم ذلك بدلاً من عرض تحكم لا يفعل شيئًا.

افتراضية: مشترك بدون بطاقة SIM فعلية

تتيح OmniWeb **له**. يقوم **SIM الافتراضية** للمودم الاتصال كمشترك **ليس لديك بطاقة SIM** ببنائها من شيئين لديك بالفعل:

1. **صورة SIM الأساسية**: لقطة محفوظة لبنية ملف بطاقة حقيقية (أي بطاقة اختبار متوافقة تعمل كقاعدة؛ انظر **صور SIM**).
2. **هوية المشترك ومفاتيحه من HSS**: IMSI ومفاتيح المصادقة لمشترك تم توفيره بالفعل في الشبكة.

يجمع OmniWeb بينهما في بطاقة برمجية. تستجيب هذه البطاقة لقراءات ملفات المودم من الصورة وتستجيب لتحدي المصادقة من الشبكة بمفاتيح HSS. إنها تضع IMSI المختار. للمشترك ويجري المصادقة، IMSI، بلاستيكية: يقرأ SIM لا يمكن للمودم أن يميزها عن بطاقة cardem، خلال **ويتصل بالشبكة الحية**.



متى تستخدمها

- إعادة إنتاج سلوك مشترك محدد في التجوال أو الاتصال دون مصدر لبطاقة SIM الفعلية الخاصة بهم.
- اختبار العديد من المشتركين المجهزين ضد مودم واحد، واحدًا تلو الآخر.
- اختبار الملفات الشخصية التي توجد فقط في HSS (تم تجهيزها حديثًا، قبل الشحن).

لا HSS **ما تثبته.** لقد اتصل مودم على المنصة بالشبكة الحية (`مسجل، شبكة منزلية`) كمشترك لذلك المشترك وأكمل المصادقة على الشبكة بالكامل IMSI بلاستيكية. لقد قرأ SIM توجد له بطاقة من البطاقة الافتراضية.

> **الافتراضي** المخصص هو الخطوة التالية في هذه القدرة. هناك يمكنك **قارئ SIM** عنصر افتراضية من صورة ومشترك مختارين وتقديمها مثل أي فتحة قارئ SIM "تحميل" بطاقة عن SIM بتوصيل البطاقة الافتراضية عبر ن��س وسيط OmniWeb أخرى. اليوم، يقوم بُعد ومسار cardem الموصوف أعلاه.

في كتاب اختبار SIM استخدام بطاقة التجوال

كجزء من عملية SIM تقديم بطاقة (GSMA IR.38 / IR.48) يمكن أن تدفع **كتب اختبار التجوال** التشغيل. في لوحة **تشغيل الاختبارات** لكتاب الاختبار يمكنك اختيار:

- **SIM (حسب ICCID / IMSI)**: تتبع حسب الهوية، يتم حل قارئها الحالي تلقائيًا في وقت التشغيل، و
- **مودم Cardem**: cardem الذي يتم محاكاة بطاقة SIM له.

يحدد الربط قبل أن تختبر. **اذهب: تشغيل جميع الاختبارات** يقدم **تقديم SIM إلى cardem** ويجري حالات البيانات. IMSI ثم يقرأ ،(cardemو SIM عند اختيار كل من بطاقة) أولاً بطاقة SIM إذا لم تكن بطاقة قيد التشغيل، توضح cardem موجودة حاليًا في قارئ، أو لم يكن عميل SIM اللوحة بالضبط السبب. لا تعمل ضد البطاقة الخطأ بصمت.

انظر أجهزة الاختبار ووثائق كتاب الاختبار لبقية تدفق IR.38.

استكشاف الأخطاء وإصلاحها

لا تظهر في البنك SIM بطاقة

الأعراض: تم توصيل قارئ ولكن لا تظهر أي فتحة (أو فتحة فارغة).

الأسباب المحتملة والحل:

- البطاقة غير موضوعة، أو لا يمكن أن يمد القارئ/البطاقة الطاقة للبطاقة. تظهر الفتحة **البطاقة موجودة** أو **فارغة**. أعد وضع بطاقة SIM.
- بإعادة مسح القراء عند التوصيل الساخن، OmniWeb تم توصيل القارئ للتو. يقوم ولكن يمكنك فرض ذلك باستخدام **إعادة المسح** في مجموعة الوكيل.

المودم لا يتصل بعد ربط بطاقة SIM

الأسباب المحتملة والحل:

- استخدم **إعادة ضبط المودم** في وحدة تحكم cardem لإعادة تقديم البطاقة. لم يعيد المودم قراءة بطاقة SIM.
- عن بُعد أن بطاقة SIM الربط ليس **نشطًا**. تأكد تحت **الروابط النشطة** في صفحة cardem الصحيح مرتبطة بـ SIM.
- في (أو محظور) مزود غير المشترك HSS للشبكة الخدمية.

البطاقة موجودة (غير قابلة للقراءة)" على قارئ"

الأعراض: تم اكتشاف بطاقة ولكن لم يمكن قراءة هويتها.

الحل: لا يمكن لذلك القارئ التحدث إلى تلك البطاقة (عادةً ما يكون هناك عدم توافق في الجهد/البروتوكول على القراء الرخيصة). انقل بطاقة SIM إلى قارئ مختلف في البنك.

الافتراضية: المودم يقرأ البطاقة ولكن لا يتصل SIM

الأسباب المحتملة والحل:

- يجب أن يكون المشترك المختار **مفعلًا** ومجهزًا بالكامل (مع ملف تعريف بيانات) في HSS للشبكة الخدمية.
- يجب أن تأتي الصورة الأساسية من نوع بطاقة متوافق. إذا توقفت البداية، أعد التقاط الصورة الأساسية من بطاقة SIM معروفة أنها جيدة.

وظيفة كشف قدرة SCEF: الخدمة

هو **البوابة الشمالية** لـ Omnitouch، **OmniSCEF** (وظيفة كشف قدرة الخدمة) **SCEF**. إنه يكشف عن قدرات الشبكة الأساسية لخوادم التطبيقات الخارجية **للشبكة لإنترنت الأشياء**، بحيث يمكن لمنصة **واجهة برمجة التطبيقات** عبر **RESTful T8** المحددة في TS 29.122 الآلة إلى الآلة الاشتراك في الأحداث المتعلقة بأسطول من الأجهزة وتبادل كميات صغيرة من البيانات معها دون الحاجة للتحدث بـ GTP أو Diameter. إنه يتعامل مع عائلتين من الخدمات. **أحداث المراقبة** تطلب من الشبكة الإبلاغ عندما تصبح الأجهزة قابلة للوصول، تفقد الاتصال، تغير الموقع، وما إلى ذلك. **تسليم البيانات غير IP (NIDD)** يحمل حمولات صغيرة غير IP من وإلى أجهزة NB-IoT عبر واجهة MME إلى SCEF المقيدة عبر طبقة التحكم. داخليًا، يصل Diameter **T6a** (TS 29.128). تعرض OmniWeb حالته، والموارد T8 التي أنشأها خادم التطبيقات، وجلسات NIDD الحية التي يحملها.

← دليل العمليات

تعتبر لوحة المعلومات صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عندما يعمل SCEF في مخزون الموقع. تمر جميع حركة المرور عبر وكيل خلفية OmniWeb إلى واجهة برمجة التطبيقات T8 الخاصة بـ SCEF، لذا تبقى خلف البوابة المعتمدة الوحيدة. يوفر رابط الوثائق في رأس الصفحة مساعدة في السياق. يتم تنظيم الصفحة في علامات تبويب.

نموذج SCS/AS ID

التي سجل تحتها **SCS/AS** هو **محدد لهوية** (كل اشتراك مراقبة وكل تكوين NIDD) كل مورد T8 خادم التطبيقات (خادم قدرة الخدمات / خادم التطبيقات). لا تحتوي واجهة برمجة التطبيقات المستخدمة، لذا لا يمكن لـ OmniWeb اكتشافها لك: **SCS/AS** على **نقطة نهاية تعدد هويات** ذلك **عبر علامات تبويب** على الصفحة، ويتذكر OmniWeb **SCS/AS ID** يقوم المشغل **بتعيين** حتى NIDD. بحيث تقوم بتعيينه مرة واحدة وينتقل من نظرة عامة إلى أحداث المراقبة إلى **SCEF** تطلب علامات التبويب المحددة واحدة بدلاً من عرض قائمة فارغة. توجد، يتم تعيين SCS/AS ID الذي تم تسجيل خادم التطبيقات به SCS/AS ID الموارد تحت هوية يجب عليك تسميتها. أدخل للعمل مع اشتراكات وتكوينات تلك (`iot-platform-01@omnitouch` على سبيل المثال) المنصة.

نظرة عامة

نفسه: **حالته**، اسم **المنتج**، حالة **الرخصة** و**المضيف** SCEF قراءة صحية لشاشة واحدة لـ SCS/AS ID حقل) أسفله هو **سياق التطبيق** .MME نحو T6a الذي يستخدمه لـ **Diameter** عدد **اشتراكات المراقبة** و**تكوينات** ،SCS/AS ID و، بمجرد تعيين (الموصوف أعلاه **NIDD** يعمل وكم يحمل منصة SCEF المحتفظ بها حاليًا لذلك خادم التطبيقات. إنها أسرع تأكيد على أن يمكن الوصول إليها، Grafana معينة. يتم توفير لوحات معلومات المراقبة والإحصائيات كإدراجات من نفس الصفحة.

أحداث المراقبة

يطلب كل SCS/AS. **اشتراكات أحداث المراقبة** التي أنشأها خادم التطبيقات للهوية الحالية إلى خادم التطبيقات؛ كل صف POST اشتراك من الشبكة الإبلاغ عن فئة من الأحداث وإرسالها عبر يظهر:

- **نوع الحدث**: نوع المراقبة، مثل **قابلية الوصول**، **فقدان الاتصال**، **تقرير UE**، **في منطقة UEs** أو **عدد حالة التجوال**، **الموقع DDN**، **التوفر بعد فشل**.
- **الهدف**: الجهاز أو المجموعة التي يراقبها الاشتراك، محددة بواسطة **معرف خارجي**، أو **معرف مجموعة خارجية** لأسطول كامل **MSISDN**.
- **وجهة الإشعار**: **رابط الاستدعاء** الذي يرسل SCEF كل تقرير حدث إليه. يجب أن يكون عنوان `http(s)` مطلقًا يكشفه خادم التطبيقات.
- **الحد الأقصى للتقارير** و، بالنسبة للاشتراك القابلية للوصول، **نوع القابلية للوصول** (`SMS` أو `DATA`). تحدد هذه عدد الأحداث مع **مدة/انتهاء المراقبة**، المرسلة ومدة حياة الاشتراك.

يمكن إنشاء الاشتراكات وتعديلها وحذفها؛ حذف واحدة يوقف خادم التطبيقات عن تلقي تقارير تلك الأحداث.

NIDD

التي أنشأها خادم التطبيقات للهو��ة الحالية IP هي روابط تسليم البيانات غير **تكوينات NIDD** مع جهاز عبر طبقة التحكم. كل صف يظهر IP يصرح تكوين بتبادل حمولات صغيرة غير SCS/AS.:

- **معرف مجموعة خارجية MSISDN**، **الهدف**: الجهاز بواسطة **معرف خارجي** أو.
- **DNN / APN**: اسم شبكة البيانات (APN) الذي يستخدمه اتصال NIDD PDN (على سبيل المثال `nidd.iot.omnitouch`).
- **الحالة**: `ACTIVE`، أو مُنهى (`TERMINATED`، `TERMINATED_UE_NOT_AUTHORIZED`).
- **الحد الأقصى للحزمة**: **الحد الأقصى لحجم الحزمة** بالبايت الذي قد تصل إليه الحمولة غير IP.
- **RDS**: ما إذا كانت **خدمة البيانات الموثوقة** مفعلة. تضيف وسيلة نقل معترف بها خفيفة مع منافذ المصدر/الوجهة عبر الرابط غير IP.

الذي يحدد ما يحدث عندما تصل بيانات سفلية بينما لا يكون **PDN** يحمل التكوين أيضًا **خيار إنشاء** عن **PDN** لإنشاء واحد، **أشر إلى خطأ**، أو **أنشئ اتصال UE انتظر** للجهاز اتصال NIDD PDN: طريق استدعاء الجهاز.

تسليم البيانات السفلية

يمكنك SCEF **تسليم حمولة سفلية** إلى الجهاز. أدخل الحمولة كنص. يقوم NIDD من تكوين ويمكن أن تحمل كل تسليم **أولوية**، NIDD قبل إرسالها عبر **base64 بتشفيرها باستخدام وزمن تأخير أقصى**. تُدرج التسليمات الأخيرة مع **حالة التسليم**: `SUCCESS`، `BUFFERING`، `SENDING`، أو أحد أسباب الفشل مثل `FAILURE_UE_NOT_REACHABLE`. يمكنك إلغاء تسليم مؤجل أو مخزن. هذه هي الطريقة التي تدفع بها منصة أمرًا أو دفعة برمجية لجهاز مقيد ليس لديه عنوان IP.

جلسات NIDD

جلسات NIDD T6a النشطة التي يحتفظ بها SCEF مع IP **الحية** هي روابط تسليم البيانات غير محددة بهوية T8 التي هي موارد NIDD، في الوقت الحالي. على عكس تكوينات SCS/AS، فإن هذه هي **حالة وقت التشغيل العالمية للخادم**: فهي **للقراءة فقط** وليست محددة بهوية SCS/AS، لذا تظهر هذه العلامة كل جلسة نشطة بغض النظر عن سياق التطبيق الذي تشاهده. كل صف يظهر **معرف حامل EPS (EBI)**، NIDD PDN الذي يستخدمه اتصال **APN**، للجهاز **IMSI**، **MME**، **ومجال MME مضيف**، **معرف جلسة T6a**، **حالة الجلسة** (`ACTIVE`، `IDLE`)، **ومعرف التكوين** الذي تم إعداد الجلسة ضده. إنها أسرع طريقة لرؤية الأجهزة التي لديها فعلاً رابط غير حي، ومن خلال أي IP MME.

السجلات

السجلات علامة SCEF تعرض مخرجات السجل الحية لـ لاستكشاف الأخطاء وإصلاحها لمثيل واحد دون مغادرة OmniWeb.

لوحات معلومات المراقبة

كلوحات SCEF لـ NIDD وعرض تقارير الأحداث، وعدد تسليمات T8، تُعرض معدلات طلب بتكرار تلك OmniWeb يمكن الوصول إليها من صفحة العنصر. لا يقوم Grafana، معلومات الرسوم البيانية بشكل أصلي.

ذات صلة

- **MME**: يصل SCEF إليه عبر **T6a** لإعداد اتصالات NIDD PDN ولجمع أحداث المراقبة والمجال الذي يستخدمه كل جلسة على علامة MME المبلغ عنها هنا. يتم عرض مضيف جلسات NIDD.
- **HSS**: يحتفظ ببيانات الاشتراك (المعرفات الخارجية، تفويض NIDD) التي تعتمد عليها خدمات المراقبة و NIDD لـ SCEF.
- **PGW-C / SMF** و**UPF**: تحمل طبقة بيانات IP. يتجاوز NIDD العادية. عمدًا هذه لنقل حمولات صغيرة غير IP عبر طبقة التحكم بدلاً من ذلك.
- العودة إلى فهرس العنصر: دليل العمليات.

SGW-C: بوابة الخدمة (طبقة التحكم)

تعتبر **SGW-C** النصف الخاص بطبقة التحكم من بوابة الخدمة EPC. إنها تربط بين حاملي كل مشترك والشبكة الوصول وبوابة الحزمة: تنهي **S11** إلى MME (إشارات الجلسة والحامل)، التي تقوم بتحويل (SGW-U) وتبرمج طبقة المستخدم، PGW-C (اتصال PDN) إلى **S5/S8**و باختصار، هي العقدة التي تحتفظ بحالة الحامل الحية لكل eNodeB إلى **S1-U** الحركة على الجلسات OmniWeb وطبقة المستخدم. تعرض PGWو MME مشترك متصل وتحافظ على تزامن وعدد الجلسات والسجلات؛ الاتجاهات طويلة الأمد (معدل النقل، نمو الجلسات) لـ SGW-C، الحية التي يمكن الوصول إليها من نفس الصفحة Grafana موجودة على لوحات.

← دليل العمليات

تعتبر SGW-C صفحة عنص�ّ لكل مثيل يتم الوصول إليها من الشريط الجانبي عند تشغيلها في مخزون الموقع. حيث يتم نشر عدة منها، توفر أيضًا عرض أسطول للحالة الإجمالية. تمر جميع الحركة عبر وكيل خلفي OmniWeb إلى واجهة برمجة التطبيقات SGW-C، لذا تبقى خلف بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. إنها منظمة في علامات تبويب.

نظرة عامة

قراءة صحة على شاشة واحدة: **حالة واجهة برمجة التطبيقات** لـ SGW-C، **عدد الجلسات** الفريدة (المتميزة S11 أقران)، **MMEs النشطة**، وملخص مستمد من الجلسات الحية: عدد **PGWs** الفريدة (المتميزة S5/S8 أقران)، **وإجمالي الحوامل** المتاحة حاليًا. إنها أسرع طريقة لتأكيد أن SGW-C وMMEs وPGWs التي تتعامل معها تعمل، وعدد الجلسات التي تحتفظ بها، وعدد.

الجلسات

للمشترك مع **حالة** الاتصال الخاصة به. **MSISDN**و **IMSI** كل جلسة مربوطة، كل صف مفتاحه هو SGW-sideو MME-side نقاط نهاية) **S11** فتح جلسة يظهر حالتها الكاملة للحامل: نقاط التحكم F-TEIDs)، **اتصال** كل **PDN** (APN، ونقاط نهاية التحكم F-TEIDs S5/S8 إلى حامل افتراضي، وجودة الخدمة، S5/S8و S1-U لطبقة المستخدم F-TEIDs نقاط نهاية، EBI) وكل **حامل** PGW)، تخدمهم PGWو MME هنا يمكنك تأكيد أن حوامل مشترك معين قد تم إنشاؤها ورؤية أي QoS).

تسرد نفس علامة التبويب في **عرض الأسطول** كل جلسة عبر SGW-Cs، حيث يتم نشر عدة الخادم مقابل كل صف، بحيث يمكن للمشغل العثور SGW-C جميعها في جدول واحد، مع عرض تقوم بتثبيته. فتح صف ينتقل إلى تلك الجلسة على مثيلها SGW-C على مشترك دون معرفة أي الخاص. يتم تسمية المثيل الذي لا يمكن الوصول إليه فوق الجدول، وكذلك حد الصف لكل مثيل عندما يحمل مثيل واحد المزيد من الجلسات مما تسحبه الرؤية المجمعة.

السجلات

لاستكشاف الأخطاء وإصلاحها في SGW-C تقوم علامة **السجلات** بعرض مخرجات السجل الحية لـ OmniWeb بوابة واحدة دون مغادرة.

لوحات المراقبة

كلوحات SGW-C تُعرض اتجاهات معدل النقل وعدد الجلسات وغيرها من السلاسل الزمنية لـ Grafana، لا تقوم بتكرار تلك المخططات التي يمكن الوصول إليها من صفحة العنصر. OmniWeb بشكل أصلي.

ذات صلة

- MME: نظير التحكم عبر **S11** على الحامل والجلسة إعداد يقود ؛ SGW-C.
- **PGW-C** يثبت اتصال PDN عبر **S5/S8**.
- **SGW-U / UPF** هي طبقة المستخدم التي يبرمجها SGW-C على التحويل الحركة لـ S1-U.

أدوات بطاقة SIM: نظام الملفات، APDU و eSIM

تقوم OmniWeb بأكثر من اكتشاف وتقديم بطاقات SIM. **أدوات البطاقة منخفضة المستوى** التي تصل عبر أي قارئ على أي وكيل للتحدث إلى البطاقة الخام يدويًا، مشاهدة تتبع APDUs مباشرة. يمكنك تصفح وتحرير نظام الملفات الخاص بها، إرسال APDU المباشر لجلسة SIM هذه الصفحة هي eUICC. على eSIM عن بُعد، وإدارة ملفات تعريف دليل العمليات لتلك الأدوات.

← دليل العمليات

تجلس هذه الأدوات بجانب ميزات SIM الحالية وتعيد استخدامها. ابدأ هنا للحصول على الصورة الأكبر:

- **بنك SIM**: موجودة في أي قارئ عبر كل وكيل. تستهدف كل SIM الجرد: أي بطاقات SIM أداة في هذه الصفحة قارنًا من ذلك الجرد، وتقوم إجراءات بنك لكل فتحة بربط مباشر إليها.
- **صور SIM (حزم ملفات تعريف SAIP)**: كيفية حفظ نظام الملفات المقروء كصورة محمولة، وكيفية تصفح أو مقارنة الصور المحفوظة.
- **SIM عن بُعد و SIM افتراضي**: كيفية تقديم SIM (حقيقية أو افتراضية) إلى مودم عبر الشبكة من خلال محاكيات البطاقة.
- **إدارة SIM عبر OTA**: نفس تحرير مستوى الملف، ولكنه يصل إلى بطاقة **عبر الهواء** (03.48 / SCP80) بدلاً من قارئ محلي مع حزم مؤمنة.

تعيش جميع الأدوات الأربعة أدناه في الشريط الجانبي تحت مجموعة **SIMs**.

قارئ واحد، مستهلك واحد في كل مرة

يمكن لشيء واحد فقط في كل مرة تشغيل قارئ PC/SC في هذه الصفحة فعلي. قد تحتاج أداة إلى قارئ يحتفظ به شيء آخر: مشغل آخر يقوم بقراءته، أو جلسة مصرفية عن بُعد حية SIM تقدمها إلى مودم. ثم تظهر الأداة **من يحتفظ بها ولماذا**، وتقدم **استحواذًا صريحًا**. لا يوجد طرد صامت: عندما تستحوذ، تقوم OmniWeb بإلغاء الجلسة الأخرى (جلسة مصرفية، تفصل). بدون رابط SIM↔cardem). للتحرير أو الإرسال هو إجراء تحكم محجوز خلف إذن تحكم بنك SIM. ذلك يمكنك عرض القراء ولكن لا يمكنك تشغيل البطاقات.



مستكشف نظام ملفات SIM

اختر قارئًا و**اقرأ شجرة الملفات الكاملة** لبطاقته: MF، DF.GSM / DF.TELECOM، الخاصة بهم، مع كل ملف قابل للقراءة مفكوك إلى حقول EFs وجميع ADF.ISIM و ADF.USIM مسماة. قراءة كاملة تلمس العديد من الملفات، لذا تظهر شريط تقدم يعرض المشي X قراءة") من Y ملفات: EF....").

- **ابحث** في الشجرة حسب رمز الملف (FID)، بحث عن الاسم القصير، أو الوصف. يجد "رموز الاتصال الطارئ" EF.ECC، `6` وليس فقط `FB7`.
- **مُعلمة، لا تُقرأ أبدًا لملفات المحمية برمز PIN**: لن يحرق المستكشف محاولات PIN.
- **تحرير EF** (مع إذن التحكم): يقدم جزء التفاصيل نموذجًا مدفوعًا بالمخطط (حقول مفككة، مكتوبة) حيثما كان ذلك متاحًا، ويعود إلى الهيكس الخام. الكتابة مدمرة وتطلب أولاً. يقوم باختبار **CHV/ADM** إلى مصادقة، استخدم **تحقق** EF تأكيدًا. حيث تحتاج ضد البطاقة (يبلغ عن المحاولات المتبقية ولا يحرق المحاولة الأخيرة). PIN/ADM مفتاح مفاتيح SIM بمجرد إثباته، يعيد المستكشف استخدامه للكتابة. يقدم مخزن مفاتيح محفوظة لرقم ICCID الخاص بالبطاقة تلقائيًا.
- **مقارنة بالصورة** مسماة. **حفظ الصورة** يلتقط الشجرة المفككة كـ صورة SIM تقارن البطاقة الحية مع واحدة محفوظة. **الصور المحفوظة** تفتح مكتبة الصور. يمكنك لتصفح بطاقة لم تعد لديك في (`?image=<id>`) أيضًا فتح صورة محفوظة كـ شجرة قارئ.

أو يمكنك الاستحواذ كما هو، (عن بُعد SIM غير محتجز بواسطة جلسة) يجب أن يكون القارئ مجانيًا مذكور أعلاه.

محطة APDU

خام بالهيكس، أرسلها إلى البطاقة APDU هي **وحدة تحكم يدوية للبطاقة**: اكتب محطة APDU للأمر، كلمة الحالة ومعناها، في قارئ مختار، وشاهد الاستجابة مفككة. يظهر التفكيك اسم INS مفككة، أو نتيجة EF حقول FCP TLV، شجرة) وتفسير موسع لأي بيانات استجابة AUTHENTICATE). تملأ الأزرار الجاهزة (SELECT MF، STATUS، READ BINARY، GET

RESPONSE، ...) بايتات) الأوامر الشائعة. الإدخال متسامح مع الفراغات/النقط ويتم التحقق منه كاملة، على الأقل CLA/INS/P1/P2).

وضعان:

الوضع	السلوك	الاستخدام لـ
طلقة واحدة	بين MF مكتفية ذاتيًا؛ تعيد البطاقة تعيينها إلى كل APDU الإرسال.	استفسارات لمرة واحدة.
جلسة	يفتح جلسة بطاقة دائمة وحصرية بحيث **تستمر** الحالة عبر APDUs: يعمل SELECT ثم READ BINARY، ويشارك VERIFY مصادقته مع UPDATE لاحق. (التحديد، المصادقة) يبقى القارئ محتجزًا حتى تغلق الجلسة.	تسلسلات ذات حالة.

بربط مباشر هنا مع ذلك القارئ المحدد مسبقًا. تنطبق SIM لكل فتحة في بنك **APDU** تقوم إجراء نفس قواعد المستهلك الواحد/الاستحواذ.

سجل APDU

هو **تتبع حي** سلبي لأوامر/ **APDU** حيث تكون المحطة هي قيادتك لبطاقة واحدة، فإن **سجل** عن بُعد / cardem. عبر سلسلة SIM **(عن بُعد) SIM**المتبادلة بين **مودم و** APDUs استجابات مع كلمة الحالة `modem→card` قم بتشغيل **التقاط** وسيقوم بتتبع التبادل: كل صف يربط أمر شجرة) المفككة الخاصة به، بالإضافة إلى نفس تفكيك الاستجابة مثل المحطة FCP، حقول EF، يمكنك إيقاف العرض (يستمر الالتقاط في العمل)، تصفية حسب الأمر/ .(ATR/reset أحداث والتمرير التلقائي، الهيكس/SW.

أي: IR.38 أثناء عملية الاتصال أو تشغيل اختبار SIM استخدمه لرؤية ما يسأله المودم فعليًا من تنجح. لا تحتاج إلى تجهيز AUTHENTICATE وما إذا كانت VERIFY، الملفات يختارها، أين يفشل الذي يتتبعه السجل SIM↔عن بُعد، الذي ينشئ رابط المودم SIM المودم. يتزاوج بشكل طبيعي مع بعد ذلك.

---

eSIM (LPA)

تدير أداة **eSIM eUICC مساعد الملف المحلي** من خلال **(LPA)** للوكيل. eUICC هو شريحة فعلية في أحد قرائك. تحتوي على عدة ملفات تعريف، ولكن واحدًا فقط نشط في كل مرة eSIM.

- **بطاقة eUICC**: تظهر **EID** للشريحة.
- **الملفات التعريفية المثبتة**: كل ملف تعريف على البطاقة: حالته (نشط/معطل)، ICCIDاللقب، المزود، الاسم، و جعلها) لكل ملف تعريف يمكنك **تمكين** eSIM). الحذف يزيل الملف التعريفي من **حذف**، أو (لقب) **تسمية إعادة**، **تعطيل** (النشطة، وهو غير قابل للتراجع، لذا يتم تأكيده أولاً eUICC.
- **تنزيل ملف تعريف**: سحب ملف تعريف جديد من SM-DP+ لمشغل وتثبيته على البطاقة. استخدم **رمز تفعيل** كامل (`LPA:1$smdp.example.com$MATCHING-ID`) أو عنوان **SM-DP+** مع رمز تأكيد اختياري، **مقسم + معرف مطابق**.

هذا مخصص لبطاقات eSIM (eUICC) بشكل محدد. لاستخدام تحرير ملفات SIM/UICC الكلاسيكية، استخدم مستكشف نظام الملفات أعلاه. لتحرير بطاقة **عن بُعد**، استخدم OTA.

مجموعة أدوات SIM (STK)

مجموعة أدوات تدفع عميل **SIM** تطبيقات STK على بطاقة SIM. ترسل ملف تعريف محطة إلى البطاقة، ثم تقدم كل أمر استباقي كشاشة تفاعلية: قوائم، عرض نص، إدخال مفتاح واحد، وإدخال نص. استخدمها للتنقل في خدمات المقيم لدى المشغل، بدء تدفقات تكوين OTA، أو اختبار منطق تطبيقات المقيم على SIM.

للحصول على دليل العمليات الكامل انظر **مجموعة أدوات** **SIM**.

ذات صلة

- بنك SIM: جرد القارئ/SIM الذي تستهدفه هذه الأدوات.
- صور SIM: حفظ، تصفح ومقارنة أنظمة الملفات المقروءة.
- SIM عن بُعد و SIM افتراضي: تقديم SIM إلى مودم عبر الشبكة (الرابط الذي يتتبعه سجل APDU).
- إدارة SIM عبر OTA: نفس تحرير الملفات، عبر الهواء.
- مجموعة أدوات SIM: التفاعل مع تطبيقات STK على بطاقة في قارئ.

صور SIM: حزم ملف تعريف SAIP

كل صورة كـ OmniWeb هي لقطة محفوظة لنظام الملفات الكامل لبطاقة. تخزن **صورة SIM** هذا هو نفس التنسيق القابل .DER بتشفير **حزمة ملف تعريف SAIP غير محمية (UPP)** والذي تم تعريفه بواسطة *مواصفات* eUICC، للتشغيل المتبادل الذي تستخدمه ملفات تعريف تصبح بطاقة واحدة .TCA من *eUICC التقنية للتنسيق القابل للتشغيل المتبادل لحزمة ملف تعريف* قراءته SAIP محمول يمكن لأي أداة تدعم `.der` تم التقاطها ملف.

SIM، تعتبر هذه الصفحة دليل العمليات. تغطي كيفية التقاط، تصدير، رفع، تصفح ومقارنة صور جرد القارئ المباشر SIM Bank افتراضية. يغطي SIM وكيفية استخدام صورة محفوظة لدعم.

جدول المحتويات

- لماذا SAIP UPP
- نظرة عامة على ا��عمارة
- ما هو موجود في صورة
- التقاط صورة
- تصدير صورة
- رفع صورة
- تصفح صورة في المستعرض
- مقارنة صورتين
- دعم SIM افتراضية بصورة
- مرجع عنصر الملف الشخصي
- استكشاف الأخطاء وإصلاحها

لماذا SAIP UPP

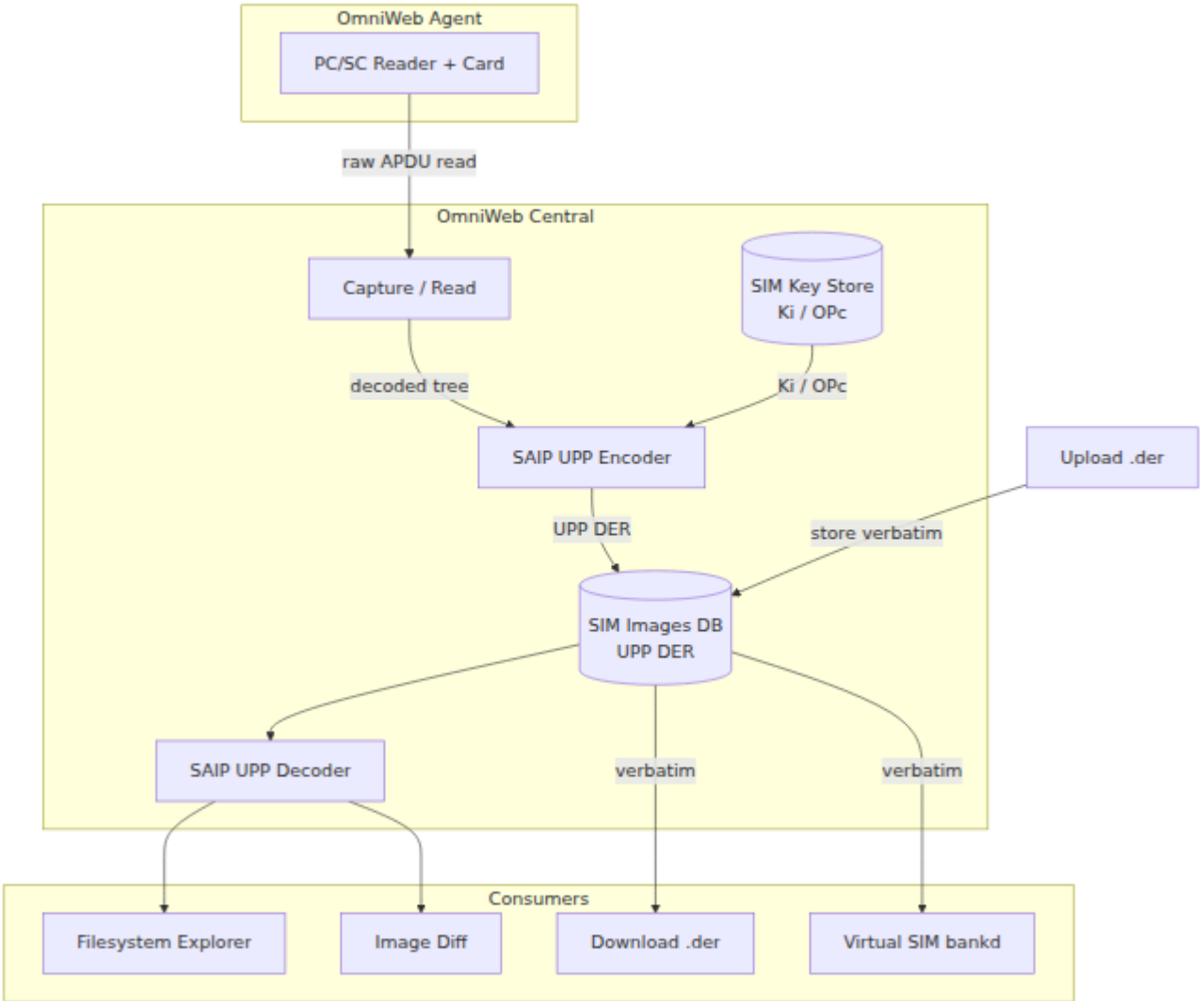
مفككة تستخدم فقط للمقارنة. كان هذا JSON كشجرة SIM كانت الإصدارات السابقة تخزن صورة ولم يكن بإمكان أي أداة خارجية استهلاكه OmniWeb التنسيق خاصًا بـ.

بدلاً من ذلك، تحصل على **SAIP UPP** الصورة كـ OmniWeb عندما تخزن:

- **قابلية النقل**: الملف `.der` المصدّر هو حزمة ملف تعريف قياسية. يتم تحميله في أي مجموعة أدوات متوافقة مع SAIP وأي مدققات ملفات تعريف SAIP.
- **تنسيق واحد في كل مكان**: نفس الملف `.der` الذي يقوم المشغل بتنزيله هو ما يدعم SIM افتراضية وما يقوم مستعرض نظام الملفات بعرضه. لا يوجد تمثيل ثانٍ مختلف.
- **إعادة التكوين**: عندما تكون مفاتيح مصادقة البطاقة معروفة (انظر التقاط صورة)، تصف الحزمة بعد ذلك OPc. و Ki الذي يحمل `PE-AKAParameter` عنصر UPP تتضمن ملف تعريف كامل وقابل للتثبيت بدلاً من تفريغ للقراءة فقط.

إنها **ليست** مشفرة (إنها DER. الحزمة هي تجميع خام لعناصر الملف الشخصي المشفرة بتنسيق المصدّر بنفس العناية التي تتعامل بها مع أي `.der` حزمة ملف تعريف *غير محمية*). تعامل مع ملف ملف يحمل Ki/OPc. استكشاف الأخطاء وإصلاحها انظر.

نظرة عامة على العمارة



من مخزن مفاتيح Ki/OPc يضم) UPP تقوم عملية الالتقاط بقراءة البطاقة، ويقوم المشفر بإنتاج الحزمة. كل مستهلك يقرأ من تلك الحزمة المخزنة OmniWeb وتخزن ،(إذا كان متاحًا SIM الوحيدةSIM. يقوم المستعرض والمقارنة بفك تشفيرها إلى شجرة عند الطلب. يستخدم التنزيل و الافتراضية البايتات كما هي.

ما هو موجود في صورة

تحتوي الصورة الملتقطة على، بالنسبة لتخطيط MF القياسي / ADF.USIM للبطاقة:

العنصر	عنصر ملف تعريف SAIP	المحتويات
نظام الملفات	`PE-GenericFileManagement`	يمكن الوصول إليه: معلمات التحكم EF كل (EFs ومحتوى خام (FCP) في الملف (EFs الخطية/الدائرية) أو كل سجل (الشفافة
الهوية	`PE-Header`	ICCID الخاص بالبطاقة
المصادقة	`PE-AKAParameter`	Ki و OPc لـ Milenage. **موجودة فقط عندما تكون مفاتيح البطاقة في مخزن مفاتيح SIM**

(DF مجموعة عمليات واحدة لكل) `PE-GenericFileManagement` يتم إنشاء الملفات باستخدام تستعيد قراءة البطاقة البايتات الخام، وليس القالب SAIP: بدلاً من قوالب نظام الملفات القياسية الذي استخدمه منشئ الملف الشخصي في الأصل، لذا فإن التمثيل العام دائمًا دقيق.

التقاط صورة

يحدث الالتقاط من مستعرض نظام ملفات أو إجراءات فتحة SIM SIM:

1. قراءة نظام ملفات البطاقة في المستعرض.
2. اختيار **حفظ الصورة** وإعطائها تسمية.

يتم ترميز نظام الملفات المفكك إلى UPP وتخزينه. إذا كان هناك مدخل في مخزن مفاتيح لـ SIM بحيث `PE-AKAParameter` يتم كتابة تلك المفاتيح في، **OPc** و **Ki** البطاقة مع كل من ICCID تكون الحزمة الناتجة قابلة للتثبيت بالكامل. بدون إدخال في مخزن المفاتيح، لا تزال الحزمة تلتقط نظام الملفات الكامل؛ فقط عنصر المصادقة يتم حذفه.

أعمدة الهوية تُشتق (ICCID، IMSI، عدد الملفات، نوع البطاقة) من نظام الملفات في وقت الالتقاط بحيث لا تحتاج قائمة الصور ورأس المقارنة أبدًا إلى إعادة فك تشفير الحزمة.

تصدير صورة

كل صف في قائمة الصور المحفوظة يحتوي على إجراء **تنزيل** يقدم الحزمة المخزنة كما هي كـ `UPP_<iccid>.der`.

الملف `.der` الذي تم تنزيله هو قياسية UPP SAIP ويمكن فحصه باستخدام أي أداة ملف تعريف متوافقة مع SAIP.

كيف يعمل: الملف هو بالضبط البايتات المخزنة عند الالتقاط (أو الرفع)، دون إعادة ترميز عند التنزيل، لذا فإن تنزيل الجولة هو مطابق بالبايت لما هو مخزن.

رفع صورة

رفع تحتوي صفحة الصور المحف**ظة على إجراء **.der** يقبل ملف SAIP UPP ويخزنه كصورة جديدة. استخدمه لإدخال ملفات تعريف تم إنشاؤها في أماكن أخرى: على سبيل المثال حزم *ملف تعريف اختبار eUICC من العامة* GSMA TS.48، أو UPP أو ملفات SAIP أخرى تم إنتاجها بواسطة أداة.

عند الرفع، تقوم OmniWeb:

1. بالتحقق من أن الملف يبدأ بعلامة عنصر ملف تعريف SAIP (علامة تم بناؤها من فئة السياق: `A0`، `A1` أو `B0`).
2. تخزين الحزمة كما هي.
3. فك تشفير `PE-Header` لملء عمود ICCID حيثما كان موجودًا.

الصورة المرفوعة هي صورة من الدرجة الأولى: يمكن تنزيلها، وتصفحها في المستعرض، ومقارنتها، وتحريرها، واستخدامها لدعم SIM افتراضية تمامًا مثل صورة ملتقطة.

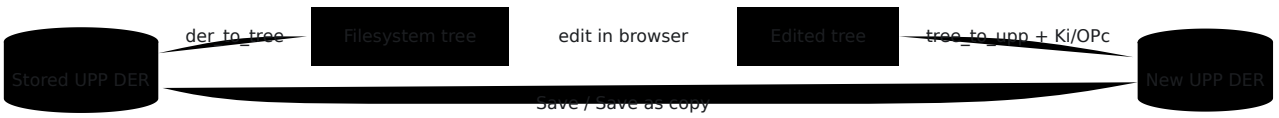
تحرير صورة

الصورة المحفوظة هي **ملف**، وليست بطاقة. لتعديل واحدة، يتم تغيير حزمة الملف الشخصي المخزنة فقط و **لا تكتب أبدًا إلى أي SIM**. من قائمة الصور المحفوظة، يفتح إجراء **تحرير** (`?image=<id>&edit=1`) في وضع التحرير SIM **نظام الملفات** مستعرض نظام ملفات. لا يتم استخدام قارئ ولا يتم الوصول إلى بطاقة الوكيل.

يمكنك:

- كما هو الحال مع بطاقة حية، يقدم المحرر EF. **تحرير محتوى ملف**: تغيير أي بايتات كخيار **Raw hex** لكامل السجل، و **JSON** وعرض **Form**، نموذجًا مدفوعًا بالهيكل لا يحتوي الملف على شروط وصول يجب الوفاء (PIN/ADM هروب. لا يوجد مطالبة بـ بها).
- إنشاء **إضافة ملف**: أو EF جديد (شفاف أو هيكلي) تحت أي DF DF/MF/ADF، وإعطائه FID، وهيكل ومحتوى أولي.
- إزالة أي **حذف ملف**: EF أو DF (الجذر MF لا يمكن حذفه هو الصورة الكاملة).
- **إعادة تسمية** الصورة (بيانات التعريف فقط) من القائمة.

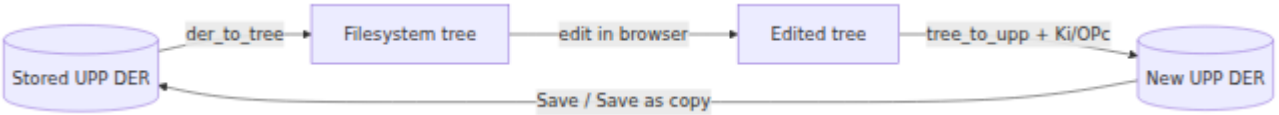
يحتفظ المستعرض بالتغييرات حتى تقوم بـ **حفظ الصورة** (استبدال في المكان) أو **حفظ كنسخة** (إنشاء صورة جديدة وترك الأصل دون تغيير). عند الحفظ، تقوم OmniWeb بإعادة ترميز عندما تكون SIM من مخزن مفاتيح Ki/OPc إنها تضم SAIP UPP. شجرة نظام الملفات المعدلة إلى مجال (PIN، PUK، معروفة. إنها تحافظ على أي عناصر ملف تعريف لا تمثلها الشجرة كما هي الأمان، القوالب)، لذا فإن التعديل لا يسقط بقية الملف الشخصي.



إلى EF **في وضع عدم الاتصال.** لفك تشفير **JSON / تحرير الحقول باستخدام النموذج** حقول مسماة وإعادة ترميزها، يتم استخدام نفس نموذج الملف الذي يستخدمه المحرر الحي، ويتم تشغيله على أي وكيل متصل، ولكن بدون **بطاقة**: الصورة تحتوي بالفعل على البايتات، لذا يقوم الوكيل بتشغيل برنامج الترميز فقط. إذا لم يكن هناك وكيل متصل، فإن التحرير يتراجع إلى Raw hex، الذي لا يحتاج إلى أي شيء خارجي.

تصفح صورة في المستعرض

كل صورة مح��وظة تحتوي على إجراء **تصفح في مستعرض نظام الملفات**. يفتح ضد الحزمة المخزنة. **لا حاجة إلى بطاقة مادية ولا قارئ**. تقوم SIM مستعرض نظام ملفات بفك تشفير الحزمة مرة أخرى إلى نفس شجرة نظام الملفات التي يعرضها OmniWeb الخام دون اتصال EF المستعرض لبطاقة حية، بحيث يمكنك فحص كل محتوى.



مقارنة صورتين

تتيح لك صفحة الصور المحفوظة اختيار صورتين ومقارنتهما. يتم فك تشفير كلا الحزمتين إلى أشجار نظام الملفات ويتم محاذاتهما حسب مسار EF، لذا فإن المقارنة تكون ملفًا بملف بغض النظر عن ترتيب الالتقاط:

الحالة	المعنى
`same`	EF موجود في كلاهما بمحتوى متطابق
`changed`	EF موجود في كلاهما، المحتوى مختلف
`only_a`	EF موجود فقط في الصورة الأولى
`only_b`	EF موجود فقط في الصورة الثانية

المتغيرة EF بالنسبة لـ هيكل ملفات لكل سجل (ودلتا لكل بايت المختلفة) تُبلغ المقارنة عن نطاقات البايت المختلفة، بحيث يمكنك رؤية بالضبط أي بايتات تحركت: على سبيل المثال، السجل، SIM قبل وبعد اختبار تغيير التخصيص، أو SIMs جنب إلى جنبًا لمشغلين اثنين.

دعم SIM افتراضية بصورة

الافتراضية، SIM يمكن أن تمثل صورة محفوظة بطاقة مادية عند تقديم SIM افتراضية. في مؤلف الملتقطة كمصادر نظام ملفات قابلة للاختيار. rspro تظهر الصور المحفوظة جنبًا إلى جنب مع صور `bankd` بإطلاق OmniWeb وتقوم (SIM أو مخزن مفاتيح HSS من) قم بربط واحدة بهوية مشترك Ki/OPc افتراضية مدعومة بنظام الملفات لتلك الصورة، مع للمشترك مضافًا للمصادقة.



نظام الملفات الذي يقرأه المودم يتم إعادة تشغيله من الصورة؛ الهوية والمفاتيح تضاف من المشترك المختار، لذا يمكن لصورة واحدة دعم العديد من المشتركين.

مرجع عنصر الملف الشخصي

تعتبر UPP سلسلة من عناصر الملف الشخصي، كل منها عبارة عن TLV بتنسيق DER حيث تحدد وتقرأ المجموعة الفرعية أدناه؛ يتم الحفاظ على العناصر OmniWeb علامة فئة السياق نوعه. تكتب عند التخزين ويتم (مجال الأمان، قوالب نظام الملفات، PUK، PIN) الأخرى في حزمة مرفوعة تخطيها عند فك التشفير إلى شجرة نظام الملفات.

العلامة	عنصر الملف الشخصي	OmniWeb يستخدمه
`A0`	`PE-Header`	بيانات ال��عريف للملفICCID ؛ الشخصي
`A1`	`PE-GenericFileManagement`	نظام الملفات (FCP + المحتوى)
`A4`	`PE-AKAParameter`	Ki و OPc (Milenage)
`AA`	`PE-End`	علامة نهاية الحزمة
`B0`	`PE-MF`	مُعد مسبقًا: يُقرأ عند الرفع، لا يتم (MF إصداره)

لحزمة ملف تعريف TCA للحصول على كتالوج العناصر الكامل وقواعد التشفير، انظر مواصفات eUICC: المواصفات التقنية للتنسيق القابل للتشغيل المتبادل.

استكشاف الأخطاء وإصلاحها

الصورة المصدرة لا تحتوي على مفاتيح المصادقة

الأعراض: ملف `.der` الذي تم تنزيله لا يحتوي على `PE-AKAParameter` ؛ لا يمكن لـ SIM الافتراضية المدعومة بالصورة المصادقة بدون المفاتيح المقدمة بشكل منفصل.

الأسباب المحتملة:

- لم يكن هناك إدخال في مخزن مفاتيح ICCID لـ SIM البطاقة في وقت الالتقاط.
- كان الإدخال في مخزن المفاتيح يفتقر إلى Ki أو OPc.

الحل:

1. أضف Ki و OPc للبطاقة إلى مخزن مفاتيح SIM، معتمدًا على ICCID الخاص بها.
2. أعد التقاط الصورة. يدمج الالتقاط الجديد المفاتيح في `PE-AKAParameter`.
3. بدلاً من ذلك، قدم المفاتيح في وقت تقديم SIM الافتراضية (من HSS أو تجاوز صريح).

الرفع مرفوض كـ "لا يبدو كـ SAIP UPP"

الأعراض: يؤدي رفع ملف إلى ظهور خطأ في التحقق.

الأسباب المحتملة:

- الملف ليس SAIP UPP: لا يبدأ بعلامة عنصر ملف تعريف (`A0`، `A1` أو `B0`).
- الملف هو حزمة ملف تعريف *محمية* (مشفرة)، وليس *غير محمية*.

الحل:

1. تأكد من أن الملف هو حزمة ملف تعريف **غير محمية** بتشفير DER.
2. تحقق من أنه يبدأ بـ `PE-Header` (`A0`). معظم UPPs المنسقة بشكل جيد تفعل ذلك.
3. إذا كانت الحزمة محمية/مشفرة، فلا يمكن تخزينها أو تصفحها؛ فقط الحزم غير المحمية مدعومة.

تصفح صورة مرفوعة يظهر الملفات حسب FID، وليس بالاسم

الأعراض: يتم تسمية ملف EFs في المستعرض بواسطة معرف ا��ملف (مثل `EF.6FXX`) بدلاً من اسم ودود.

الأسباب المحتملة:

- تستعيد قراءة البطاقة معرفات الملفات والمحتوى الخام، وليس الأسماء الرمزية التي استخدمها منشئ الملف الشخصي. تقوم OmniWeb بتعيين EFs المعروفة في USIM الخاص به FID خارج تلك الخريطة يتم عرضه بواسطة EF إلى أسماء ودية؛ أي هو المعرف الرسمي والمحتوى الخام دقيق. هذا متوقع للملفات غير القياسية أو الخاصة بالبائع.

الحل: لا حاجة لأي إجراء.

التعامل مع الحزم المصدرة بأمان

تعتبر UPP تحتوي على Ki و OPc المصدرة **غير مشفرة**، وعندما كانت المفاتيح متاحة عند الالتقاط، تعامل مع ملف `.der` الذي تم تنزيله كمادة مفاتيح حساسة:

- لا ترسله عبر قنوات غير موثوقة.
- احذف النسخ المحلية عندما لا تكون مطلوبة بعد الآن.
- يفضل الاحتفاظ بالصور داخل OmniWeb (حيث يتم التحكم في الوصول بواسطة إذن SIM Bank) على توزيع ملفات `.der`.

بنك SIM: جرد SIM الموزع

بنك يظهر **SIM** كل SIM في كل قارئ بطاقات ذكية عبر كل وكيل OmniWeb. يقوم كل وكيل ويبلغ الجرد إلى المركز تمامًا كما، SIM المحلية الخاصة به، ويقرأ هوية كل PC/SC بمسح قارئات يبلغ عن المودمات/الهاتف كأجهزة. يقوم المركز بتجميع الجرد لكل وكيل ويحتفظ بقاعدة بيانات من وأين" قائمة حتى مع انقطاع الاتصال SIMs بحيث تبقى رؤية "ما هي، ICCID مفاتيحها SIMs بالقارئ والوكيل.

SIM عن بُعد موزعة. تتيح لك طبقة محاكاة/بنك بطاقة SIM هذه هي نصف الجرد من منصة اختبار عن بُعد هذه الطبقة بشكل SIM **بأي بطاقة عبر الشبكة**. توثق **SIM** عن بُعد **الاتصال بأي** حزم ملفات تعريف SIM (SAIP) منفصل. تغطي هذه الصفحة الاكتشاف والجرد. تغطي صور كيفية حفظ وتصدير وإعادة استخدام نظام ملفات البطاقة كحزمة ملف تعريف محمولة.

الصفحة **مركزية حول القارئ**: صف واحد لكل فتحة قارئ فعلية، مجمعة حسب الوكيل. تظهر الفتحات الفارغة وغير القابلة للقراءة والمستخدمة جميعها. تصميم البنك هو الحقيقة، وليس فقط الفتحات المملوءة.

SIM كيف يقرأ الوكيل

يعكس ماسح الوكيل ماسح المودم: التعداد بطيء، لذا يتم تخزين النتائج مؤقتًا وإعادة مسحها على فترات.

لكل قارئ PC/SC على المضيف:

1. تعداد **قارئات** PC/SC المتصلة بالمضيف.
2. **استكشاف** كل قارئ مع اتصال حصري.
   - لا توجد بطاقة → `present=false`.
   - القارئ محجوز بواسطة عملية أخرى (مثل `bankd` SIM بطاقة محاكاة جلسة أو بُعد عن) → `present=true, in_use=true`، لا يؤدي **انتهاك المشاركة** إلى رفع الاتصال و**لا يتم محاولة القراءة**. القارئ المشغول أبدًا إلى تعطل المسح.
   - البطاقة موجودة ومجانية → اقرأها.
3. **اقرأ** هوية SIM من مجموعة مستقلة من APDUs الخام:
   - كشف UICC مقابل SIM الكلاسيكي (اختر `3F00` `6E00`؛ → GSM ووضع الاختيار الكلاسيكي `CLA=A0`)، لذا استخدم الكلاسيكي،
   - EF.ICCID (`2FE2`)، EF.IMSI (`6F07`)، EF.SPN (`6F46`)،
   - `EF.AD` (`6FAD`) لطول MNC (بشكل صحيح MCC/MNC لذا يتم تقسيم)،
   - (`0000`) **آمن** افتراضي **رقم تعريف شخصي** VERIFY على بطاقة مقفلة. **ويرفض** (فارغ غير متناقص VERIFY) يقوم بفحص عداد إعادة المحاولة أولاً إذا بقيت محاولة واحدة فقط، لذا فإنه **لا يحرق** أبدًا آخر محاولة أو يلمس PUK (في تعطل البطاقات SIM يجب ألا يتسبب بنك)،
   - ATR البطاقة.

يصبح كل قارئ قاموسًا:

```
{
  "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…"
}
```

عند التسجيل وعندما تتغير؛ (بجانب قائمة الأجهزة) `sims` يتم إرسال القائمة إلى المركز كرسالة أمر `simbank_rescan` يجبر على مسح غير مخزن مؤقتًا على الفور.

قدرة قراءة البطاقة

يقرأ المضيف SIMs الذكية الخاصة به. حيثما كانت هناك حاجة PC/SC من خلال مجموعة بطاقات إلى فك تشفير أعمق للبطاقة، يستخدم الوكيل مكتبة بطاقات ذكية اختيارية، مرخصة بشكل منفصل، محفوظة بمعزل عن بقية الوكيل (لم يتم دمجها في كود OmniWeb الخاص). يعمل المضيف SIMs **بدون** مجموعة بطاقات ذكية بشكل جيد ويبلغ ببساطة عن عدم وجود SIM هو بنك SIMs. قدرة اختيارية لكل مضيف، مثل المودمات.

القارئ المرجعي هو SCM/Identiv SCR35xx. يتم دعم عدة قراء لكل مضيف.

تدفق الجرد → المركز → واجهة المستخدم

```
agent host                              central (android-role process)
browser
──────►──────                            ──────────────────────────────
──────

simbank.list_sims()  ──sims──►     android agent_socket
  (PC/SC read)                       └─
registry.update_sims(agent_id, …)   GET /api/simbank/sims
                                     └─ simbank.record_sims(…)  ──►
DB       GET /api/simbank/readers

POST /api/simbank/agents/<id>/rescan
                        ◄──simbank_rescan──  (forces an uncached
scan)
```

- يقوم الوكيل بالاتصال WebSocket الذي يستخدمه للهواتف **بالمركز** عبر نفس (`/api/android/agent`). يركب جرد SIM على هذا الاتصال. لا يوجد نقل جديد.
- يحتفظ المركز بلقطة **حية** لكل قارئ لكل وكيل في `android.Registry` في الذاكرة (`update_sims` / `all_sims`)، ويعكس كل ICCID في جدول `simbank_sims` الدائم عبر `simbank.record_sims`.
- نظرًا لأن هذا يعتمد على سجل الوكيل أحادي العملية، يتم تقديم واجهة برمجة تطبيقات **فقط بواسطة عملية الخلفية الخاصة بدور الوكيل** (نفس القيود مثل SIM بنك أجهزة الاختبار).

واجهة برمجة التطبيقات REST (`/api/simbank`، JWT، نوع عنصر RBAC `simbank`)

الطريقة	المسار	الغرض
GET	`/sims`	كل SIM عبر جميع الوكلاء (بما في ذلك فقط المخزنة غير المتصلة)، مع وجود حالي/مستخدم فوقها.
GET	`/readers`	كل قارئ PC/SC على كل وكيل **متصل** (حي)، بما في ذلك القراء الفارغين والمستخدمين.
GET	`/sims/<iccid>`	SIM واحدة.
PATCH	`/sims/<iccid>`	تحرير الحقول المعينة من قبل المشغل (ملاحظات اليوم). ينشئ الصف إذا كان ICCID غير مرئي.
DELETE	`/sims/<iccid>`	نسيان SIM (يسقط السجل المخزن؛ يظهر مرة أخرى في المسح التالي إذا كانت لا تزال مدخلة).
POST	`/agents/<id>/rescan`	إجبار مسح PC/SC غير مخزن مؤقتًا على الفور على وكيل واحد وإرجاع جرده الجديد.

مع JWT يمر المسؤولون دائمًا؛ بخلاف ذلك، يمنح إذن RBAC يعكس `ir38`/`android-control`: العرض، و `element_type == "simbank"` في طرقه يمنح التحكم `POST`.

الواجهة الأمامية

`src/pages/simbank/SimBank.tsx`: جدول قابل للبحث، قابل للتصفية لجميع الحالة: SIMs، البلد، MCC/MNC، IMSI، ICCID، (موجودة / مستخدمة / غير متصلة)، الوكيل/الموقع، القارئ، SPN، ملاحظات قابلة للتحرير، آخر ظهور. زر **إعادة المسح** لكل وكيل. يتم توجيهه إلى `/simbank` ويرتبط من الشريط الجانبي تحت **اختبارات التجوال** › **بنك** **SIM**.

مخطط قاعدة البيانات

`simbank_sims`: صف واحد لكل ICCID تم رؤيته على الإطلاق:

العمود	الملاحظات
`iccid` (PK)	الرقم التسلسلي لـ SIM.
`imsi`, `mcc`, `mnc`, `country`, `spn`, `atr`	الهوية الأخيرة المعروفة (تُستبدل فقط بالقراءات غير الفارغة).
`notes`	مخصصة من قبل المشغل، قابلة للتحرير.
`last_agent_id`, `last_site`, `last_reader_name`, `last_reader_index`	حيث تم رؤيته آخر مرة (أو يتم رؤيته حاليًا).
`first_seen`, `last_seen`	الطوابع الزمنية (UTC).
`remsim_bank_id`, `remsim_slot_nr`, `remsim_mapped_cardem`	**محجوز للمرحلة الث��نية** (قابل للإلغاء، غير مستخدم).

تظهر فقط في SIMs. لذا فهي لا تُخزن كـ ICCID، لا تحمل القراء الفارغين والمستخدمين **أي** الحية لقطة `/readers`.

المستقبل: SIM عن بُعد

في موقع SIM عن بُعد بحيث يمكن تقديم SIM فعلي في بنك SIM/تقوم المرحلة 2 بربط قارئ واحد إلى مودم/هاتف في موقع آخر (SIM عن بُعد). ابحث في الكود عن تم وضع الخطافات بالفعل. `# TODO remsim`:

- `simbank_sims.remsim_bank_id` / `remsim_slot_nr` / `remsim_mapped_cardem` أعمدة قابلة للإلغاء، تظهر في `to_dict` ونوع TS `SimRow` كـ `null`),

- علم `in_use` لكل قارئ في الوكيل يميز بالفعل قارئًا محجوزًا بواسطة جلسة `bankd`/ محاكاة. هذا هو القارئ الذي ستقوم المرحلة 2 بربطه،
- `PATCH /api/simbank/sims/<iccid>` هو المكان الذي سيتم فيه توصيل تحرير خريطة remsim.

اليوم؛ الشكل محجوز بحيث يمكن أن تتناسب خريطة المربعات دون remsim لا شيء هنا يدفع إعادة العمل على مسار الجرد الساخن.

محرر الموقع: عارض إعدادات الموقع

يعرض **محرر الموقع** ملف الإعدادات الخام للموقع المحدد حاليًا: ملف YAML الخاص بالمضيف/ الجرد الذي يحدد وظائف الشبكة والبنية التحتية والإعدادات لهذا النشر. إنه عرض للقراءة فقط مع تمييز نحوي، لذا يمكنك رؤية بالضبط ما يعمل عليه OmniWeb لموقع دون فتح نافذة سطر الأوامر على مضيف.

← دليل العمليات

ما يعرضه

كل موقع من ملف إعدادات خاص بكل موقع. يسرد هذا الملف عناصر الموقع (ما يدفع OmniWeb هي الوظائف الشبكية الموجودة وعناوينها)، مضيفي البنية التحتية، دوره في المراقبة، كتلة `fivegc` الخاصة به (انظر 5G Core)، وهكذا: كل ما تستمده الشريط الجانبي، وا��توبولوجيا، وصفحات العناصر، ولوحات المعلومات.

يقوم محرر الموقع بتحميل هذا الملف للموقع المختار من القائمة المنسدلة في شريط العنوان ويعرضه في لوحة محرر كاملة (Monaco، نفس المحرر الذي يستخدمه VS Code) مع تمييز YAML، وأرقام الأسطر، والطي، وخريطة مصغرة. يظهر العنوان العميل، والموقع، واسم الملف المصدر.

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'

المحاولة مجددا

إذا لم يتم اختيار أي موقع، ستطلب منك الصفحة اختيار واحد من القائمة المنسدلة أولاً.

للقراءة فقط عن تصميم

محرر الموقع هو **عارض**: اللوحة للقراءة فقط (مميزة بشريحة **للقراءة فقط** في العنوان). إنه موجود لفحص الإعدادات الفعالة، وليس لتغييرها.

لا يتم تحرير إعدادات الموقع من المتصفح. كما هو مذكور في جميع أنحاء ذا الدليل، يتم إدارة OmniWeb عبر **Ansible**. لا تقم بتحرير ملفات الإعدادات مباشرة على المضيفين، وإضافة أو تغيير عنصر هو تغيير في الإعدادات يتم من خلال تلك القناة (انظر نموذج الإعدادات). يتيح لك محرر الموقع قراءة نتيجة تلك القناة للموقع المحدد.

متى تستخدمه

- **تأكيد ما تم إعداد الموقع به**: ما هي العناصر، والمضيفين، ووظائف 5GC التي يعتقد أنها موجودة، وفي أي عناوين OmniWeb.
- **استكشاف الأخطاء في واجهة المستخدم مقابل الإعدادات**: إذا كان عنصر، أو إدخال في الشريط الجانبي، أو قسم 5GC مفقودًا أو يشير إلى مضيف خاطئ، فإن الملف الخام هو مصدر الحقيقة للتحقق منه.
- **الرجوع إلى اسم الملف والمحتويات الدقيقة** عند إعداد تغيير في Ansible.

ذات صلة

- الهندسة المعمارية: نموذج الإعدادات: كيف تدفع إعدادات الموقع OmniWeb وكيف يتم إدارتها.
- 5G Core: كتلة `fivegc` وما تعرضه من إعدادات الموقع.
- توبولوجيا الشبكة: عرض التوبولوجيا وقائمة المضيفين المبنية من نفس إعدادات الموقع.

بوابة SMPP

بوابة تعمل **SMPP** كحلقة وصل بين نظراء SMPP الخارجيين ونواة الرسائل. تتصل التطبيقات إما عبر SMPP، (كيانات الرسائل القصيرة الخارجية) **ESMEs**، الخارجية والشركاء المتعاونون كعملاء تتصل بهم البوابة أو كخوادم تقبل البوابة الاتصالات منها، وتقوم البوابة بنقل رسائلهم القصيرة إلى ومن SMSC. **ربط** كل اتصال هو SMPP (مرسل، مستقبل أو جهاز إرسال واستقبال). تحافظ البوابة على هذه الروابط، وتقوم بالتحقق منها وتنظيمها، وتقوم بنقل الحركة إلى نواة الرسائل. تعرض OmniWeb حالة الربط الحية، والأقران المكونين من العملاء والخوادم، وسجلات البوابة.

← دليل العمليات

تعتبر بوابة SMPP صفحة عنصر لك�� مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيلها في جرد الموقع، مع عرض أسطول حيث يتم نشر عدة منها. تمر جميع الحركة عبر وكيل OmniWeb الخلفي إلى واجهة برمجة التطبيقات الخاصة بالبوابة، لذا تبقى خلف البوابة الوحيدة المعتمدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

قراءة صحية على شاشة واحدة لإحصائيات الربط الإجمالية: **إجمالي** عدد الروابط و**التقسيم المتصل / غير المتصل** مقسومًا عبر روابط **العملاء** (الصادرة) و**الخوادم** (الواردة). إنها أسرع طريقة لتأكيد أن البوابة تعمل وأن نظراءها متصلون، ولرؤية لمحة سريعة إذا كان هناك أي اتصال متوقع قد انقطع.

حالة الربط

كل ربط مفعل، سواء كان عميلًا أو خادمًا، مع **حالة الاتصال** الحالية، و**تفاصيل الجلسة** الأساسية و**القياسات** لكل ربط. هذه هي الرؤية الحية لمن هو متصل الآن. من هنا يمكن للمشغل اتخاذ إجراء على الربط:

- **إسقاط** ربط نشط. بالنسبة لربط العميل، فإن ذلك ينهي الاتصال الصادر. بالنسبة لربط الخادم، فإنه يفصل جميع اتصالات العملاء النشطة. استخدمه لمسح اتصال عالق أو غير متصرف.
- **إعادة الاتصال** برابط عميل. هذا يجبر ربط العميل (الصادر) على إعادة الاتصال بمضيفه البعيد، وهي أسرع طريقة لإعادة شريك خارجي بعد انقطاع الشبكة.

نظراء العملاء

العميل الصادرة المكونة هي الأقران التي تتصل بها البوابة. يظهر كل منها SMPP اتصالات **اسمها**، **المضيف** البعيد و**المنفذ**، و**معرف النظام** الذي تتصل به، و**نوع الربط** (مرسل، مستقبل أو جهاز إرسال واستقبال). يمكن تعديل نظراء العملاء بالكامل هنا: يمكن للمشغل **إضافة** TPS المضيف، المنفذ، بيانات الاعتماد، نوع الربط، فترة الاستعلام، حد) نظير، **تعديل** واحد موجود و**حذف** واحد لم يعد مطلوبًا. تمكين نظير يجلب ربطه الصادر إلى ،(والمعلمات الأخرى للربط الخدمة. تعطيله يخرج النظير دون التخلص من تكوينه.

نظراء الخوادم

الخادم الواردة المكونة هي بيانات الاعتماد والقواعد للأقران التي تتصل *بالبوابة*. SMPP تفويضات كل إدخال يحدد **معرف النظام** وكلمة المرور، و**أنواع الربط المسموح بها**، والقيود التي تنظم لعناوين المصدر المسموح بها و**قائمة بيضاء لعنوان IP** الربط الوارد: **قائمة بيضاء لعنوان المصدر TPS**. يمكن تعديل نظراء الخوادم لأنماط العناوين الأصلية المسموح بها، بالإضافة إلى **حد** هنا بنفس الطريقة (**إضافة**، **تعديل** و**حذف**)، لذا يمكن للمشغل إدخال شريك وارد جديد، أو تشديد قوائم بيضاء، أو إلغاء تفويضه. التحكم في تمكين وتعطيل التفويض يحدد ما إذا كان يُسمح لذلك الشريك بالربط.

السجلات

تقوم علامة **السجلات** بعرض مخرجات السجل الحية للبوابة لاستكشاف الأخطاء وإصلاحها في بوابة OmniWeb واحدة (فشل الربط، رفضات المصادقة والاتصالات المقطوعة) دون مغادرة.

المراقبة

كلوحات SMPP تُعرض معدلات الرسائل، وسرعة النقل وغيرها من السلاسل الزمنية لبوابة بتكرار تلك OmniWeb مكن الوصول إليها من صفحة العنصر. لا تقوم�، Grafana معلومات

الرسوم البيانية بشكل أصلي.

ذات صلة

- **SMSC** هي نواة الرسائل التي تسلم إليها البوابة الرسائل القصيرة.
- **IP-SM-GW** تحمل SMS عبر IMS لأجهزة VoLTE، وتكمل مسار SMPP إلى الأقران الخارجيين.

SMSC: مركز خدمة الرسائل القصيرة

إن **SMSC** (مركز خدمة الرسائل القصيرة) هو قلب التخزين والإرسال للرسائل القصيرة في Diameter، من الجانب المحمول، عبر SS7 (MAP) عبر النواة. إنه **يقبل** الرسائل من الشبكة ثم **يوجه**، **يترجم** و **يسلم**ها. يحتفظ بأي رسالة لا يمكنه .(من واجهات التطبيقات SMPP وعبر تسليمها على الفور ويعيد المحاولة حتى يتم تسليم الرسالة، أو تنتهي صلاحيتها، أو يتم إسقاطها. على طول الطريق، يتتبع حالة تسليم كل رسالة، يترجم الأرقام المتصلة والمستقبلة، يتعاون مع SMSCs النظيرة حتى يمكن تسليم الرسالة إلى أي عقدة يمكنها الوصول إلى المستلم، ويقود كل هذا من صفحة واحدة لكل مثيل: حالة OmniWeb حملات الرسائل القصيرة **الجماعية**. تعرض الرسائل الحية، مواقع المشتركين، تسجيلات الواجهة الأمامية، صحة Diameter والفيدرالية، مجموعات قواعد التوجيه والترجمة، وإدارة الحملات.

← دليل العمليات

إن SMSC هو عنصر صفحة لكل مثيل يمكن الوصول إليه من الشريط الجانبي عند التشغيل في مخزون الموقع، مع عرض أسطول حيث يتم نشر عدة منها. يمر كل حركة المرور عبر وكيل خلفية SMSC، إلى واجهة برمجة تطبيقات OmniWeb لذا يبقى خلف بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

تعد علامة التبويب الرئيسية قراءة صحية على شاشة واحدة للعقدة: عدد الرسائل الحالية وحالة التسليم، صحة الواجهة الأمامية والنظير في لمحة، و **بحث حسب MSISDN** يبحث عبر كل من الرسائل المخزنة و��واقع المشتركين. إنها أسرع طريقة للإجابة على "ما الذي يحدث لرسالة SMS لهذا المشترك الآن" من صندوق واحد.

الرسائل

أو قام بمعالجتها، كل صف يظهر الأرقام المرسلة والمستقبلة، **حالة** SMSC كل رسالة يحتفظ بها الرسالة (معلقة، مسلمة، فاشلة، منتهية، مسقطة أو رد تلقائي)، عدد **محاولات التسليم**، وعمرها. ولتضمين حركة المرور **المتوفاة** أو **غير** ،**SMSC** يمكنك تصفية الرسائل حسب الحالة، حسب اسم العقدة أو معرف الرسالة. اختر رسالة لفتح تفاصيلها، ،MSISDN **الموجهة**، والبحث حسب بما في ذلك النص العادي المفكك. يمكن للمشغل **إعادة توجيه** رسالة لإجبارها على العودة عبر التوجيه، على سبيل المثال بعد إصلاح قاعدة التوجيه.

الواجهات الأمامية

هي العملاء الذين يقدمون ويتلقون SMSC **المسجلة** حاليًا مع SMPPالواجهات الأمامية للتطبيق و الرسائل. كل إدخال يظهر اسم المضيف، متى تم **رؤيته آخر مرة**، ومتى **تنتهي** تسجيله، لذا يمكنك تأكيد أن واجهات معالجة الرسائل متصلة وتسجيلاتها نشطة.

المواقع

مواقع المشتركين SMSC حسب و **IMSI** هي آخر موقع معروف يخدم كل مشترك التي تعلمها IMSI هذه المعلومات للوصول إلى المستلم. يمكنك البحث عنها حسب SMSC يستخدم **MSISDN**. يعرف SMSC وتصفيتها لتضمين الإدخالات المنتهية. إنها المكان الذي تؤكد فيه أن MSISDN أو مكان المشترك قبل أن يتمكن من التسليم إليهم.

Diameter

للرسائل، كل صف يظهر **مجال** النظير، SMSC التي يستخدمها Diameter اتصالات الأقران **النقل**، اتجاه بدء الاتصال، **اسم المنتج** المبلغ عنه، **معرفات التطبيقات** المتفاوض ،**IP عنوان** يعمل SMSC الذي يعتمد عليه Diameter عليها و**حالة الاتصال**. هنا تؤكد أن مسار.

الفيدرالية

النظيرة حتى يمكن تسليم رسالة إلى أي SMSCs مع SMSC تظهر **عرض الفيدرالية** كيف يتعاون عقدة يمكنها الوصول إلى المستلم. إنها تبلغ عن **هذه العقدة**، عدد الأقران **الصحيين**، **المتدهورين** و**غير الصحيين**، عدد **الرسائل الفيدرالية المخزنة** (مميزة عندما تكون غير صفرية)، طريقة **الاكتشاف** المستخدمة (أو أقران ثابتة DNS نطاق) وجدول لكل نظير يحتوي على اسم العقدة، الحالة، الفشل الأخير، آخر فحص صحي ناجح وواجهات كل نظير. إنها أسرع طريقة لرؤية ما إذا كانت SMSCs في الفيدرالية تصل إلى بعضها البعض.

التوجيه

قواعد توجيه SMS التي تقرر أين تذهب كل رسالة، مدرجة حسب **الأولوية**. كل قاعدة تتطابق مع نمط الرقم **المتصل** و**المستقبل** (وبشكل اختياري SMSC المصدر أو نوع المصدر مثل SS7 المصدر أو بحث SMSC مستهدف أو **ENUM**) مع وصف وحالة تمكين. القواعد قابلة للتعديل بالكامل: يمكن للمشغل إضافة، تعديل، تمكين، تعطيل أو حذفها، وتصدير وإعادة استيراد مجموعة القواعد.

الترجمات

قواعد ترجمة الأرقام التي تعيد كتابة الأرقام المتصلة والمستقبلة أثناء مرور الرسائل: تقوم بتطبيع التنسيقات، وتطبيق البادئات وما إلى ذلك. يتم سرد كل قاعدة حسب **الأولوية** مع مطابقة المصدر الاختياري، علامة **استمرار** (حتى يمكن تطبيق عدة قواعد SMSC، الاتصال والمستقبل بالتسلسل)، وصف وحالة تمكين. كما هو الحال مع التوجيه، القواعد قابلة للتعديل (إضافة، تعديل، تمكين، تعطيل، حذف)، ويمكنك تصديرها وإعادة استيرادها.

الحملات

الجماعية من هذه العلامة. يتم تعريف **حملة جديدة** باسم ووصف، ورقم SMS تُنشأ وتُدار حملات المصدر، وقائمة **المستلمين**، و**الجمهور** (المستلمون النشطون فقط أو الجميع SMSC**مرسل**، و في القائمة)، ومعدل **التقطير** بالرسائل في الثانية، ونافذة **صلاحية** الرسالة، ووقت **التسليم بعده** اختياري وقالب **الرسالة**. بمجرد إنشائها، يتم التحكم في الحملة من هنا (**بدء**، **إيقاف مؤقت**، **استئناف** أو **إلغاء**). يمكنك فحص **الأهداف** الخاصة بها لرؤية حالة الإرسال والتسليم لكل مستلم مع تقدم الحملة.

قوائم الحملات

قوائم المستلمين التي ترسل إليها الحملات. يتم إدارة القوائم بالكامل هنا: إنشاء **قائمة مستلمين جديدة** باسم، وصف ومجموعة أولية من المستلمين، **إضافة** المزيد من المستلمين لاحقًا، تعديل، أو حذف قائمة. يتم تزويد المستلمين كـ **CSV**، لذا يمكنك استيراد قائمة جهات اتصال موجودة مباشرة بدلاً من إدخالها يدويًا.

اختبار NAPTR

اختبار علامة تبويب **NAPTR** هي أداة للمشغل تحل رقم **E.164 (أو نطاق)** عبر DNS بتوجيه رسالة نحوه. أدخل رقم الهاتف و **نطاق** SMSC لرؤية كيف سيقوم ENUM/NAPTR وقدم. لا يتم جلب أي شيء حتى تفعل ذلك. (بشكل افتراضي `e164.arpa`) للاستعلام **ENUM** المنشورة هناك، **NAPTR** يبحث عن سجلات ENUM، بعكس أرقام الرقم إلى منطقة SMSC يقوم لإعادة الكتابة **regexp**، ويعيدها بترتيب و**تفضيل**. تحمل كل سجل **علاماتها**، **الخدمة** و**الاستبدال**، و **النطاق الناتج** المحلول الذي تشير إليه السجل. إنها المكان الذي تؤكد فيه أن أو مسار تتوقعه، قبل الاعتماد عليها في URI وراء قاعدة التوجيه تحل فعلاً رقمًا إلى ENUM بيانات الإنتاج.

MWI

ترسل تحديث **إشارة انتظار الرسالة** لمشترك: الإشعار الذي يحدد أو يزيل **MWI** علامة تبويب علامة "الرسائل المنتظرة" على جهاز الهاتف، عادة بعد ترك رسالة صوتية أو جمعها. قدم **المصدر** الذي تأتي منه، اختر **نوع الإشارة** (البريد **MSISDN الوجهة** للإخطار و **MSISDN** الصوتي، الفاكس، البريد الإلكتروني أو غيره)، وحدد ما إذا كان يجب أن يكون المؤشر **نشطًا** المنشئ. إنها نموذج تقديم: يتم **SMSC** (تشغيل) أو مسح (إيقاف)، مع نص **رسالة** اختياري و إرسال التحديث فقط عندما تقوم بنشره. هذه هي الطريقة المباشرة لرفع أ�ً مسح مؤشر الرسالة المنتظرة لمشترك يدويًا.

سجلات النظام

الخاصة المدعومة بواجهة برمجة SMSC علامة تبويب **سجلات النظام** هي عرض سجلات التطبيقات. يمكنك تصفيتها حسب **المستوى** (تصحيح، معلومات، تحذير، خطأ) وحسب **حد** على عدد الأسطر المعادة، لذا يمكنك سحب الأخطاء الحديثة فقط أو تتبع أكثر شمولاً عند التحقيق في مشكلة معينة، دون مغادرة OmniWeb.

المزيد من الأدوات

بعض الأدوات المركزة SMSC بجانب علامات التبويب أعلاه، تقدم صفحة:

- **إرسال**: نموذج يرسل رسالة SMS لمرة واحدة مباشرة من OmniWeb (من، إلى، ونص الرسالة)، لاختبار التسليم لمستلم معين.
- **العمليات**: إجراءات صيانة على مستوى العقدة، بما في ذلك مسح **الواجهات الأمامية** المسجلة، **الرسائل ��**لمخزنة، قواعد **التوجيه** وقواعد **الترجمة**. كل منها هو إجراء مدمر ويطلب تأكيدًا أولاً.

السجلات

الحية لاستكشاف مشكلة في عقدة ��احدة SMSC علامة تبويب **السجلات** تتبع مخرجات سجل للحصول على عرض مصفى مدعوم بواجهة برمجة التطبيقات لنفس .OmniWeb دون مغادرة العقدة، استخدم **سجلات النظام** أعلاه.

المراقبة

يتم تقديم معدل مرور الرسائل، ومعدلات نجاح التسليم، وعمق الطابور وغيرها من السلاسل الزمنية لـ SMSC يمكن الوصول إليها من صفحة العنصر. لا تقوم Grafana، كلوحات معلومات بتكرار تلك الرسوم البيانية بشكل أصلي OmniWeb.

ذات صلة

- **HSS**: يحتفظ ببيانات المشترك ومعلومات التوجيه التي تعتمد عليها تسليمات SMSC.
- **DRA**: ينقل إشارات Diameter التي يستخدمها SMSC للرسائل.
- **STP**: مسار إشارات SS7 الذي يتبادل SMSC رسائل MAP مع الشبكة المحمولة.
- **CSCF/TAS**: الجانب IMS الذي ينشئ وينهي الرسائل لمشتركي VoLTE.

إدارة البرمجيات ودورة حياتها

يوفر OmniWeb مكانًا واحدًا لرؤية وإدارة البرمجيات التي تعمل عبر الأسطول: إصدارات الحزم، التحديثات المتاحة، والتراخيص. دورة حياة البرمجيات في الشبكة مرئية من نفس البوابة المستخدمة لتشغيلها.

← العودة إلى دليل العمليات

صفحة البرمجيات (مستودع APT)

تعتبر صفحة APT لحزم Omnitouch **البرمجيات** متصفحًا لمستودع APT تتصل بخادم مستودع Omnitouch. المكون وتظهر، للحزم التي تديرها:

- **الحزم المتاحة** في المستودع.
- **الإصدارات** المعروضة، بما في ذلك أحدث إصدار متاح.
- **حالة التحديث**: ما إذا كان هناك إصدار أحدث موجود مقارنةً بما هو مُنشر.

هذا يسمح للمشغلين برؤية لمحة سريعة عن مكونات Omnitouch التي لديها تحديثات معلقة وأي الإصدارات هي الحالية، مما يوفر الجانب المخزني لدورة حياة البرمجيات. يتم تثبيت/ترقية الحزم على المضيفين من خلال أدوات APT/`dpkg` القياسية (عبر Ansible وغالبًا ما يتم أتمتتها)؛ يوفر طبقة الرؤية على ما هو منشور وحالي OmniWeb.

صفحة البرمجيات: كل حزمة Omnitouch مع أحدث إصداراتها من المستودع والذاكرة المؤقتة `omni-upf` *و* `omni-msc` *هنا) ومؤشر المزامنة الذي يوضح أين تم نشر إصدار أحدث مما هو مخزن/مُنفذ (غير متزامنين).*



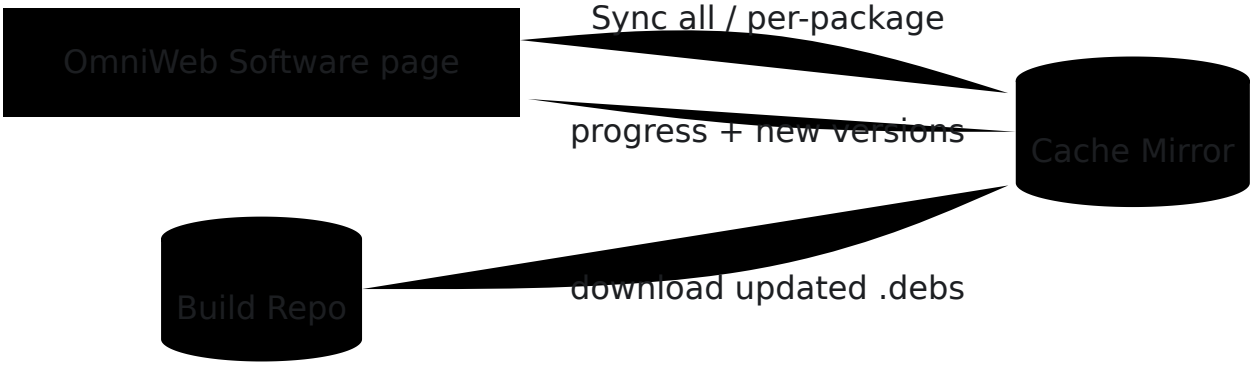
مزامنة الحزم إلى الذاكرة المؤقتة

في الموقع (للمواقع المعزولة أو ذات **APT** تقوم عمليات النشر التي تعمل على **مرآة ذاكرة** النطاق ا��ترددي المحدود) بالاحتفاظ بنسخة محلية من الحزم المنشورة على مستودع البناء. مع مرور الوقت، تتأخر الذاكرة المؤقتة. تشير صفحة البرمجيات إلى كل حزمة تكون **غير متزامنة** (تم نشر إصدار أحدث مما هو مخزن). من نفس الصفحة يمكنك سحب تلك التحديثات إلى الذاكرة المؤقتة دون الانتقال بعيدًا عن OmniWeb:

- **مزامنة الكل**: سحب كل حزمة محدثة من المستودع إلى الذاكرة المؤقتة.
- **مزامنة** (لكل صف): سحب حزمة واحدة فقط. انقر على عدة حزم وستكون في **قائمة الانتظار** OmniWeb بإعادة توليد فهرس الحزم: يتم تنزيلها واحدة تلو الأخرى، ويقوم **مرة واحدة** في النهاية (ليس لكل حزمة)، بحيث لا تترك الذاكرة المؤقتة نصف محدثة.

أثناء تشغيل المزامنة، تعرض الصفحة تقدمًا مباشرًا (أي حزمة يتم تنزيلها، وعدد الحزم في قائمة الانتظار، وسجل مباشر). يتم تحديث مقارنة الإصدارات عند الانتهاء.

في قائمة الانتظار، لافتة المرحلة، `omni-upf` يتم تنزيلها مع `omni-msc` :مزامنة قيد التنفيذ والسجل المباشر. عندما تفرغ قائمة الانتظار، يتم إعادة توليد فهرس الذاكرة المؤقتة مرة واحدة وتحديث حالة المزامنة.



تسحب(بتحفيزها وبث التقدم OmniWeb يقوم) تعمل المزامنة على مرآة الذاكرة المؤقتة نفسها ؛ المحدثة من مستودع البناء وتعيد توليد فهرسها. ثم يقوم المضيفون في `.deb` المرآة ملفات الموقع بتثبيت الحزم المحدثة من الذاكرة المؤقتة كما هو معتاد.

إصدار البرمجيات

يبلغ OmniWeb عن إصدار البناء الخاص به (الإصدار، الالتزام، وتاريخ البناء) حتى يتمكن المشغلون من تأكيد بال��بط أي إصدار من البوابة يعملون عليه. هذه هي نقطة المرجع عند الإبلاغ عن المشكلات أو تنسيق ترقية البوابة نفسها.

إدارة التراخيص

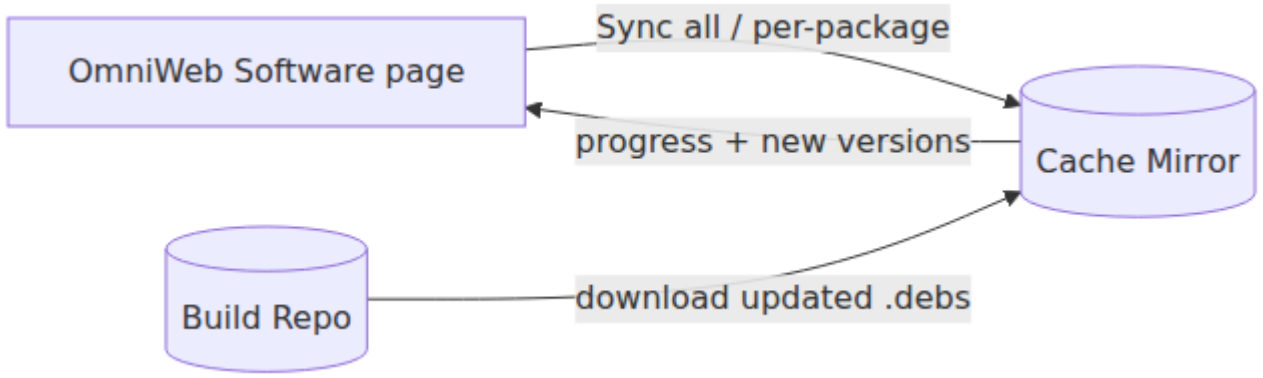
يتم إدارة OmniWeb مثل أي عنصر آخر، باستخدام نفس الأنماط العامة (انظر العمليات الشائعة). يظهر **خادم الترخيص** من خلال:

نظرة عامة على خادم الترخيص: حالة الترخيص الحالية وصلاحيته، بما في ذلك حالة الوقت الموثوق به.

العرض	الوصف
نظرة عامة	حالة الترخيص الحالية، تواريخ الصلاحية، وحقوق الميزات.
سجلات الطلبات	طلبات الترخيص التاريخية، مع تصفية. هذا مفيد لتدقيق ما تم التحقق منه ومتى.
استعلام	البحث عن حالة الترخيص لمرخص محدد/منتج عند الطلب.

ترتبط الترخيص بدورة حياة البرمجيات: تحدد الحقوق المنتجات والميزات ا��تي يُسمح للنشر بتشغيلها، وتوفر سجلات الطلبات مسار تدقيق لنشاط الترخيص على مر الزمن.

دورة الحياة في لمحة



1. **رؤية ما هو متاح**: تظهر صفحة البرمجيات التحديثات المعلقة.
2. **تأكيد الحقوق**: يظهر خادم الترخيص ما هو مرخص للنشر.
3. **تطبيق**: يتم تشغيل الترقيات عبر APT/Ansible على المضيفين.
4. **التحقق**: تأكيد الإصدارات، ثم مراقبة السجلات ولوحات المعلومات لتأكيد نتيجة صحية.

SS7: كومة الإشارات (STP / HLR / IP-SM-GW / CAMEL-GW)

كومة SS7 (OmniSS7) تقوم بإنهاء نقل SIGTRAN (جمعيات SCTP التي تحمل **M3UA**) وتوجيه حركة مرور SS7/MAP عبر شبكة الإشارات. توفر خدمة واحدة الكومة بالكامل، وتعرض OmniWeb المختلفة نقطة نقل الإشارات، جهاز توجيه (**STP**: ذلك كأربع وجهات عناصر لأدوارها SS7)، **HLR** (سجل الموقع المنزلي)، **IP-SM-GW** (بوابة الرسائل القصيرة IP) و **CAMEL-GW** (بوابة CAMEL). جميع الأربعة مدعومة من نفس العميل المشترك، لذا فإن نقل SIGTRAN والتوجيه الذي يتشاركون فيه هو نفس الكومة الأساسية التي تُرى من زوايا مختلفة.

← دليل العمليات

كل وجهة هي صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عندما عمل إلى واجهة OmniWeb في مخزون الموقع. تمر جميع حركة المرور عبر وكيل خلفي SS7 كومة برمجة التطبيقات الخاصة بالكومة، لذا تبقى خلف البوابة المعتمدة الواحدة. تأتي الردود في ظرف `{status, response}`. يفتح رابط الوثائق في رأس كل صفحة عنصر (زر المساعدة في السياق) هذه الصفحة. كل وجهة منظمة في علامات تبويب. يتم تقديم معدلات الرسائل وسلاسل الزمن الأخرى كلوحات معلومات Grafana. لا تقوم يمكن الوصول إليها من صفحة العنصر. بتكرار تلك الرسوم البيانية بشكل أصلي OmniWeb.

نظرة سريعة على الكومة

في **SCTP** تحت كل دور هو نفسه، لذا تظهر علامات التبويب **الأقران** و **اتصالات** نقل SIGTRAN جميع الوجهات الأربع وتقرأ نفس البيانات.

كل جار (`/api/m3ua-status`) تبلغ علامة التبويب M3UA عن حالة الأقران **الأقران**، **حالة الجمعية**، **النقاط النهائية** المحلية والبعيدة، **سياق** ،**ASP** مع **حالة** ،M3UA/M2PA **التوجيه**، البروتوكول والوضع، وإحصائيات **مدة التشغيل** لكل جار. هنا يمكنك تأكيد أن عملية خادم التطبيق لكل جار إشارات تعمل وتكون في الخدمة.

كل جمعية (`/api/sctp-connections`): النقل الأساسي **SCTP** تسرد علامة التبويب **اتصالات** المحلية والبعيدة، عدد **التدفقات** الواردة والصادرة، **البايتات** **IP/port**، مع **الحالة**، **الدور** SCTP و **الرسائل** المرسلة والمستلمة، **آخر نشاط**، وأي خطأ أخير، بالإضافة إلى المجموعات التراكمية عبر جميع الاتصالات. عندما يظهر جار على أنه غير متصل، تحقق من هذه الطبقة لمعرفة ما إذا كانت جمعية SCTP قد تم إنشاؤها بن��سها.

STP: التوجيه

عرض **STP** هو جهاز توجيه SS7. إلى جانب علامات التبويب المشتركة للنقل، تحمل علامة التبويب **SS7 التوجيه**، بالإضافة إلى **خريطة الشبكة**، **نظرة عامة** و **تغذية أحداث**.

الأقران (`/api/routing`): تظهر علامة التبويب M3UA **التوجيه** التكوين الكامل لتوجيه **(GT)** و **طرق العنوان العالمي (PC)** المكونة، و **طرق رمز النقطة**.

- عبر **جار** (`dest_pc`) **طرق رمز النقطة** توجه حركة المرور إلى رمز نقطة وجهة مستهدف، مع **مؤشر الشبكة**، **قناع** رمز النقطة و **أولوية**. يمكن للمشغلين **إضافة** طريق PC (`POST /api/routing/pc-routes`، مع إعطاء رمز النقطة الوجهة والجار المستهدف) و **حذف** واحد (`DELETE /api/routing/pc-routes/{dest_pc}-{peer_id}`).

- توجه إلى **جار** مستهدف مع **أولوية**** GT **طرق العنوان العالمي** تطابق **بادئة** نوع الترجمة وطبيعة العنوان ووصف. يمكن للمشغلين **إضافة** SSN، وتفاصيل اختيارية لـ طريق GT (`POST /api/routing/gt-routes`، مع إعطاء البادئة والجار المستهدف) و **حذف** واحد (`DELETE /api/routing/gt-routes/{prefix}:{peer_id}`).

هنا يمكنك تأكيد وضبط كيفية توجيه STP لرسائل SS7 نحو كل وجهة.

HLR

عرض **HLR** يعرض المشتركين النشطين في السجل والرابط إلى الخلفية HLR، إلى جانب علامات التبويب المشتركة للنقل، و **نظرة عامة** و علامة التبويب **عميل** **SS7**.

كل (`/api/subscribers`): تسرد علامة التبويب **المشتركين** سجل المشتركين النشطين **IMSI**، كل صف يظهر مشترك أرسل **UpdateLocation** ولم يرسل بعد **CancelLocation**، الفريدة. يمكن MSCs و VLRs الخادم، وقت التسجيل و **المدة**، مع عدادات لـ **MSC**، **VLR** لإعادة (`DELETE /api/subscribers`) للمشغل **مسح** جميع المشتركين النشطين المتعقبين تعيين عرض السجل.

المكونة HLR من الاتصال مع واجهة برمجة التطبيقات **HLR** تتحقق علامة التبويب **روابط** (`/api/hlr-links`): **الحالة** (مرفوعة، متدهورة أو غير متصلة)، **الكمون** المقاس، **الإصدار** المبلغ عنه و **المضيف** المستهدف. إنها أسرع طريقة لتأكيد أن الكومة يمكنها الوصول إلى الخلفية HLR.

IP-SM-GW

IP-SM-GW هو بوابة الرسائل القصيرة. يحمل متتبع المشتركين SMSc والرابط إلى الخلفية SMSc، عرض **نظرة عامة** للنقل و إلى جانب علامات التبويب المشتركة.

المكونة SMSc من الاتصال مع واجهة برمجة التطبيقات **SMSc** تتحقق علامة الت��ويب **روابط الحالة** (مرفوعة، متدهورة أو غير متصلة)، **الكمون**، **الإصدار** المبلغ عنه :(`/api/smsc-links`) SMS. في مسار HLR و **المضيف** المستهدف. إنها تعادل فحص رابط

SMSc تسرد علامة التبويب **مشتركي** SMSc المشتركين المتعقبين بواسطة متتبع المشتركين (`/api/smsc-subscribers`): كل منهم مع **MSISDN**، **IMSI**، **HLR GT** و **VLR GT**، **الرسائل المرسلة** و **المستلمة**، الحالة وآخر تحديث، بالإضافة إلى عدادات نشطة/فاشلة و **مسح** جميع مشتركي HLRS المتعقبين SMSc الفريدة. يمكن للمشغل (`DELETE /api/smsc-subscribers`).

CAMEL-GW

CAMEL-GW يعرض جلسات CAMEL التي تعمل بها البوابة، إلى جانب علامات التبويب عرض **نظرة عامة** و للنقل المشتركة.

CAMEL تسرد علامة التبويب **جلسات** جميع جلسات CAMEL النشطة التي تديرها البوابة (`/api/camel-sessions`): كل جلسة، **إصدار CAP**، **حالة الخدمة**، **مفتاح IMSI**، **أرقام الاتصال** و **المتصل**، وقت البدء و **المدة**، مع عدادات للجلسات التي تم بدءها والإجابة عليها. هنا يمكنك مشاهدة معالجة مكالمات CAMEL الحية في الوقت الحقيقي.

الحالة

الحالة تبلغ نقطة النهاية (`/api/status`) عن صحة العقدة العامة التي تلخصها علامات التبويب **نظرة عامة**: هوية العقدة و **الدور**، ما إذا كانت الخدمة **جيدة**، **مدة التشغيل**، وملخص للأقران حول عدد أقران الإشارات النشطة من الإجمالي. هذه هي القراءة الأولى لتأكيد أن الكومة تعمل وأن أقرانها في الخدمة.

ذات صلة

- **STP**: عنصر توجيه SS7 (طرق رمز النقطة وطرق العنوان العالمي).
- **HLR**: عنصر سجل الموقع المنزلي (سجل المشتركين النشطين ورابط HLR).
- **IP-SM-GW**: عنصر بوابة الرسائل القصيرة IP (مشتركي SMSc والرابط).
- **CAMEL-GW**: عنصر بوابة CAMEL (جلسات CAMEL الحية).
- **MSC/VLR** التي تقوم هذه الكومة CAMEL وإشارات UpdateLocation يرفع بتوجيهها وتتبعها.
- **SMSc** هو الخلفية التي يتم حل رابط SMSc في IP-SM-GW لمتتبع المشتركين ضدها.
- ← دليل العمليات

عميل مجموعة أدوات SIM (STK)

يتضمن OmniWeb عميل **مجموعة أدوات SIM** تفاعلي. استخدمه للتنقل وتشغيل تطبيقات STK ملف STK لجهاز متصل. يرسل عميل PC/SC فعلية تم إدخالها في قارئ SIM على أي بطاقة تعريف طرفي إلى البطاقة، ثم يقدم كل أمر استباقي كشاشة تفاعلية. تستجيب كما يفعل الطرف، لذا يتقدم التطبيق إلى خطوته التالية.

مجموعة أدوات SIM - توجد هذه الأداة في الشريط الجانبي تحت **بطاقات**، جنبًا إلى جنب مع محطة ومستكشف نظام ملفات APDU SIM.

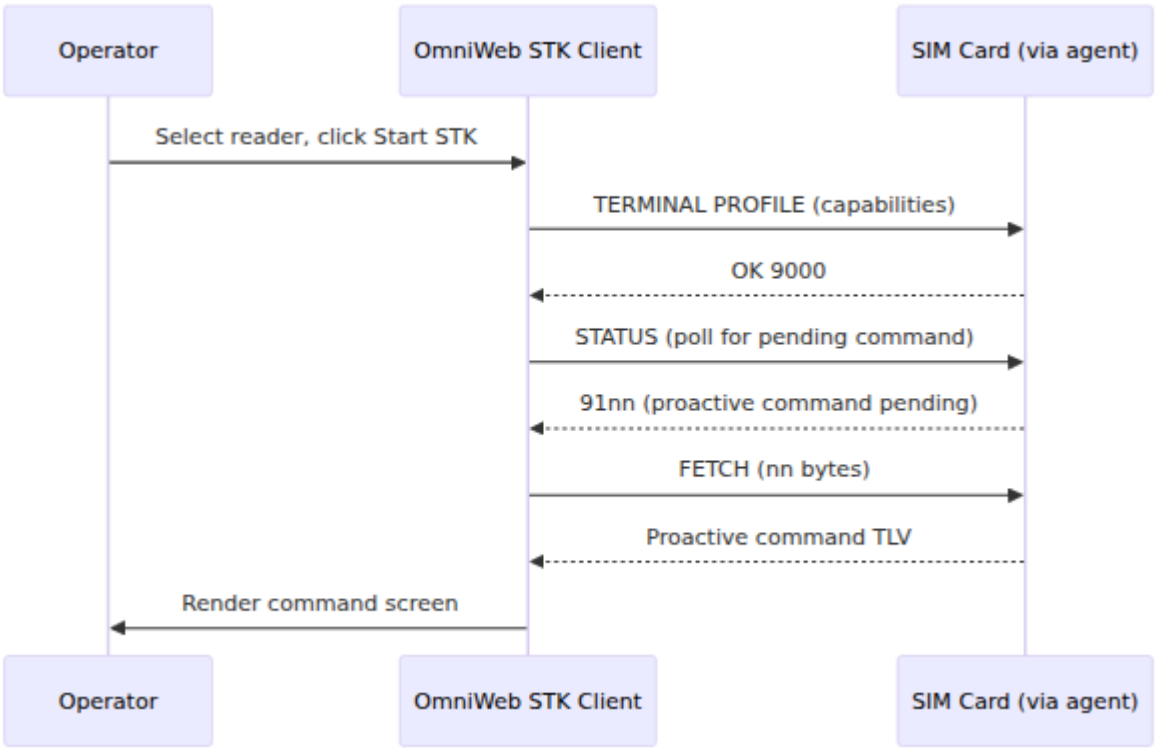
ما هي مجموعة أدوات SIM؟

مجموعة أدوات تطبيق SIM (STK) هي معيار محدد في ETSI TS 102.223 يسمح لبطاقة SIM ببدء إجراءات على الطرف. تصدر تطبيقات SIM طلبات مثل "عرض هذا النص" - **أوامر استباقية** أو "عرض هذه القائمة" - ويستجيب الطرف باختيار المستخدم أو إدخاله. تشمل حالات الاستخدام الشائعة قوائم شحن المشغل، استفسارات الرصيد، مشغلات تكوين OTA، وبوابات الخدمات المقيمة على SIM.

المتطلبات

- قارئ SIM مع بطاقة تحتوي على تطبيق STK.
- **تحكم بنك SIM** إذن. بدون ذلك، يمكنك رؤية القارئات ولكن لا يمكنك فتح جلسات أو تشغيل بطاقات.
- يجب ألا يكون القارئ محتجزًا بواسطة أداة أخرى. إذا كان كذلك، يظهر OmniWeb من يحتفظ به ويقدم خيار **استحواذ**. يؤدي الاستحواذ إلى إلغاء الجلسة الأخرى.

فتح جلسة



1. اختر القارئ من قائمة **القارئ** المنسدلة. تظهر فقط القارئات التي تحتوي على بطاقة.
2. انقر على **بدء** **STK**. يفتح OmniWeb جلسة حصرية على البطاقة، ويرسل ملف تعريف طرفي، ويستعلم عن أول أمر استباقي.
3. تفاعل مع كل شاشة كما تظهر. يرسل OmniWeb استجابة طرفية بعد كل خطوة ويستخرج الأمر التالي تلقائيًا.
4. تنتهي الجلسة عندما تصدر البطاقة أمر إنهاء الجلسة، أو عندما تنقر على **إنهاء** **الجلسة**.

شاشات الأوامر

يقدم OmniWeb كل أمر استباقي كشاشة تفاعلية. الجدول أدناه يوضح أنواع الأوامر المدعومة.

الأمر	الوصف	إجراء المستخدم
عرض النص	تعرض البطاقة رسالة.	انقر على **موافق** للاعتراف، أو **رجوع** للعودة إلى الخطوة السابقة.
تحديد عنصر / إعداد القائمة	تقدم البطاقة قائمة مرقمة من الخيارات.	انقر على العنصر الذي تر��د تحديده.
الحصول على مفتاح	تطلب البطاقة ضغطة مفتاح واحدة.	اكتب حرفًا واحدًا وانقر على **إرسال**، أو اختر **نعم** / **لا** لطلبات نعم-لا.
الحصول على إدخال	تطلب البطاقة سلسلة نصية بطول محدد.	اكتب النص وانقر على **إرسال**. يظهر الحقل الحد الأدنى والحد الأقصى لعدد الأحرف.

إذا أصدرت البطاقة نوع أمر لا يعرضه العميل بشكل تفاعلي (على سبيل المثال، إرسال رسالة بيانات الأمر الخام ويرسل استجابة **موافق** تلقائيًا حتى OmniWeb قصيرة أو إعداد مكالمة)، يظهر تتمكن الجلسة من الاستمرار.

تاريخ الجلسة

يظهر لوح **تاريخ الجلسة** على الجانب الأيمن من الشاشة بمجرد أن تبدأ في التفاعل. يسجل كل نوع أمر والاستجابة التي قدمتها (العنصر المحدد، نص الإدخال، أو موافق/رجوع). استخدمه لتتبع المسار عبر شجرة القائمة.

إنهاء الجلسة

تنتهي الجلسة بإحدى الطرق الثلاث:

- **إنهاء من قبل البطاقة**: يصدر التطبيق أمر إنهاء الجلسة الاستباقي. يغلق OmniWeb الجلسة تلقائيًا ويظهر رسالة إكمال.
- **إنهاء من قبل المشغل**: انقر على **إنهاء الجلسة** في أي وقت. يرسل OmniWeb نتيجة انتهاء الجلسة إلى البطاقة ويغلق جلسة القارئ.

- **التنقل للخلف بعد الجذر**: النقر على **رجوع** في الشاشة الأولى يرسل نتيجة حركة للخلف إلى البطاقة. تتحكم البطاقة في كيفية الاستجابة - قد تعرض شاشة سابقة أو تنهي الجلسة.

بعد انتهاء الجلسة، يصبح القارئ متاحًا مرة أخرى لأدوات أخرى.

العلاقة مع أدوات SIM الأخرى

الأداة	الغرض
مجموعة أدوات SIM (هذه الصفحة)	تشغيل تطبيقات STK بشكل تفاعلي.
محطة APDU	إرسال APDUs خام يدويًا، واحدة تلو الأخرى أو في جلسة مستمرة.
مستكشف نظام ملفات SIM	تصفح وتحرير نظام ملفات البطا��ة.
سجل APDU	تتبع الأوامر بشكل سلبي بين مودم وبطاقة SIM عن بُعد.

استكشاف الأخطاء وإصلاحها

فشل بدء STK مع "فشل ملف تعريف الطرف"

رفضت البطاقة ملف التعريف الطرفي أو لم يتمكن الوكيل من الوصول إلى البطاقة. تحقق من:

- أن البطاقة مثبتة بشكل صحيح في القارئ.
- عدم احتجاز أداة أخرى للقارئ. إذا كان كذلك، استخدم **استحواذ**.
- أن الوكيل الذي يمتلك القارئ متصل بالإنترنت (تحقق من صفحة بنك SIM).

تتوقف الجلسة بعد الأمر الأول

بعض تطبيقات SIM تنهي الجلسة على الفور إذا لم يعلن ملف التعريف الطرفي عن القدرات التي يحتاجها التطبيق. يعلن العميل عن مجموعة واسعة من القدرات، لكن بعض البطاقات تتحقق من بتات محددة. إذا حدث ذلك، استخدم APDU في وضع الجلسة لإرسال ملف تعريف الطرف محطة واستخرج الأمر يدويًا وفحص بيانات الأمر الاستباقي الخام.

يعود "رجوع" بشاشة غير متوقعة

تقوم عملية **رجوع** (حركة للخلف) x11 بإرسال رمز نتيجة 0 إلى البطاقة. تتحكم البطاقة في ما يعنيه ذلك. بعض التطبيقات تعود إلى القائمة السابقة؛ والبعض الآخر يعيد بدء الجلسة من القائمة الجذرية؛ وقليل منها يتجاهل الحركة للخلف ويعيد إصدار نفس الأمر.

يرفض "الحصول على إدخال" نصي

تحدد البطاقة الحد الأدنى والحد الأقصى لعدد الأحرف. يظهر حقل الإدخال كليهما. إذا كانت البطاقة تقيد أيضًا بالأرقام فقط، فإن تسمية الحقل تقول **أرقام فقط**. أدخل قيمة ضمن النطاق المطلوب.

TAS: خادم تطبيق الهاتف

TAS (خادم تطبيق الهاتف) هو خادم تطبيق IMS يتعامل مع المشترك. يقدم تجربة الهاتف للمشترك الذي **تحكم المكالمات** و **الخدمات التكميلية** (تحويل المكالمات، الحظر، الانتظار، الانتظار وغيرها)، يدير **المؤتمرات**، يستقبل ويعيد تشغيل **البريد الصوتي**، يسجل **سجلات المكالمات** لكل بحيث يتم احتساب Diameter عبر **OCS** مكالمة، يحل **التوجيه** وترجمة الأرقام، ويتحدث إلى *ماذا* TAS *كيف* يتم الإشارة إلى المكالمة، يقرر CSCF المكالمات في الوقت الحقيقي. حيث يقرر مكالماتها الحية، تسجيلات المشتركين، البوابات، أقران OmniWeb تفعل الخدمة. تعرض والتكوين على صفحة عنصر واحدة. تعيش مخططات حجم المكا��مات والاتجاهات Diameter التي يمكن الوصول إليها من نفس الصفحة Grafana على لوحات.

← دليل العمليات

هو صفحة عنصر لكل مثيل يمكن الوصول إليها من الشريط الجانبي عند تشغيله في مخزون TAS إلى واجهة برمجة التطبيقات الخاصة بـ OmniWeb الموقع. يمر كل حركة المرور عبر وكيل خلفية TAS، لذا يبقى خلف بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

نظرة عامة

علامة التبويب الرئيسية هي قراءة صحة على شاشة واحدة لخادم التطبيق: عدد **المكالمات النشطة**، **المشتركين المسجلين**، المؤتمرات **الجارية** وسجلات **البريد الصوتي** المخزنة، TAS وحالة **الترخيص**. إنها أسرع طريقة لتأكيد أن ،**SIP** و **بوابات Diameter** صحة **أقران** يعمل وينقل الحركة.

المكالمات النشطة

كل مكالمة جارية حاليًا، كل صف يظهر الأطراف المتصلة والمستقبلة، **الاتجاه**، **حالة** المكالمة و **مدتها**. اختر مكالمة لفتح تفاصيلها حتى تتمكن من رؤية كيف تم تقسيم مكالمة معينة وأين تقع في خطة الاتصال. إنها أول مكان يجب النظر إليه عندما يبلغ مشترك عن مكالمة في مشكلة الآن.

سجلات المكالمات

صف واحد لكل مكالمة مكتملة، مع الأطراف، TAS: **سجلات تفاصيل المكالمات** التي كتبها **وقت البدء**، **المدة** و **التصرف**. افتح أي سجل للحص��ل على تفاصيله الكاملة. تعتبر سجلات المكالمات المسار المحاسبي والتصحيح بعد الحدث: استخدمها لتأكيد حدوث مكالمة، ومدة تشغيلها وكيف انتهت.

المشتركين

كل منها مع **هوية** المشترك، **حالة** التسجيل و TAS، **تسجيلات المشتركين** التي يعرفها **الاتصال** الحالي. افتح مشتركًا للحصول على تفاصيل التسجيل الكاملة. هنا يمكنك تأكيد أن المشترك مسجل في خادم التطبيق قبل البحث عن سبب عدم عمل خدمة لهم.

Diameter

أقران Diameter التي يتصل بها TAS، بما في ذلك المسار إلى **OCS** للرسوم و **HSS** لبيانات المستخدم، مع اسم المضيف لكل نظير و **حالة الاتصال**. افتح نظيرًا للحصول على تفاصيله. عندما تفشل ��لرسوم أو عمليات البحث عن المشتركين، هذه علامة التبويب هي المكان الذي تؤكد فيه أن المسارات الأساسية لـ Diameter تعمل.

البوابات

بوابات SIP للوصول إلى الشبكات والأقسام الأخرى، كل منها يظهر اسمه و TAS التي يستخدمها **حالته** الحالية. افتح بوابة للحصول على تفاصيلها. استخدم هذه علامة التبويب لتأكيد أن بوابات الاتصال المسجلة متاحة قبل تشخيص المكالمات الفاشلة خارج الشبكة.

المؤتمرات

المؤتمرات النشطة ومشاركوها. افتح مؤتمرًا لترى من فيه، وتصرف بناءً على ذلك في المكان: **قفل** أو **فتح** الجسر، **طرد** مشارك، تشغيل **الفيديو أو إيقافه**، أو **تدمير** المؤتمر بالكامل. هذه هي السيطرة الحية للمشغل على جسر قيد التشغيل.

البريد الصوتي

سجلات البريد الصوتي المخزنة، لكل مشترك. يمكن **حذف** كل سجل بشكل فردي، على سبيل المثال لمسح رسالة تركت عن طريق الخطأ أو لتحرير صندوق بريد ممتلئ.

اختبار OCS

حتى تتمكن من، TAS النشطة التي يحتفظ بها **جلسات OCS (نظام الشحن عبر الإنترنت)** رؤية أي المكالمات تسحب من رصيد في الوقت الحقيقي. يمكن **إنهاء** جلسة شحن فردية من هنا. هذا مفيد لمسح جلسة عالقة بعد انتهاء مكالمتها.

التوجيه

المكالمات ضدها. تظهر القائمة كل قالب؛ افتح واحدًا TAS **قوالب خطة الاتصال** التي يوجه لقراءة محتواه. هذه هي المرجعية لكيفية مطابقة الأرقام وأين يتم إرسال المكالمات. اقرأها جنبًا إلى جنب مع أداة **ترجمة الأرقام** لتأكيد أن رقمًا معينًا يتم توجيهه كما هو مقصود.

التكوين

مقسم حسب التطبيق. افتح إدخالًا لقراءة إعداداته. هذه هي TAS، **تكوين التطبيق** الذي يعمل به OmniWeb. المرجعية لقراءة تأكيد أن الخادم تم تكوينه كما هو متوقع دون مغادرة

التعليمات

للمتصلين، الإعلانات وتعليمات القائمة، مع حالة TAS **تسجيلات التعليمات الصوتية** التي يشغلها كل منها. استخدم هذه علامة التبويب لتأكيد أن التعليمات المتوقعة موجودة وتم تقديمها.

الأدوات

مجموعة من الأدوات عند الطلب للتحقق من TAS بجانب علامات التبويب أعلاه، تحمل صفحة التوجيه وبيانات المشتركين. كل منها يأخذ نموذجًا صغيرًا، ويشغل الطلب ضد خادم التطبيق عبر OmniWeb، وكيل ويظهر النتيجة في المكان.

محاكي المكالمات

ويمكن اختيار رقم) للتحقق من التوجيه والوسائط. أدخل **وجهة** TAS يضع مكالمة اختبار عبر يقوم المحاكي بتمرير المكالمة عبر خطة الاتصال **دون** .(مصدر وتصرف مفروض IP مصدر، عنوان قرار على/خارج الشبكة، كل ،(أو طارئ MT، MO) **رنين أي شخص**. إنه يعيد نوع المكالمة المحدد **متغيرات خطة الاتصال** التي تم تعيينها، وقائمة خطوة بخطوة من **ملاحظات المعالجة**، حتى تتمكن من رؤية بالضبط كيف سيتم التعامل مع رقم قبل إجراء مكالمة حقيقية. يمكن تخطي تفويض لعزل مرحلة. إجراء **اختبار صدى** منفصل يرن وجهة ويعيد الصوت الخاص بالطرف، HLRو OCS مما يؤكد مسار الصوت الحي إلى الهاتف.

استعلام Sh

يستعلم HSS عبر واجهة **Sh** لبيانات مستخدم المشترك. أدخل **الهوية العامة** للمشترك واختر **مرجع البيانات** IMS، لجلبه، من **بيانات المستودع** الكاملة إلى عنصر محدد مثل حالة مستخدم الخادم، معايير الفلترة الأولية S-CSCF اسم تعيد الأداة بيانات الخدمة الشفافة .IMSI أو MSISDN استخدمها لتأكيد ما يراه خادم التطبيق لمشترك عندما لا تعمل HSS. والمخزنة التي يحتفظ بها خدمة كما هو متوقع.

بحث HLR

لحل حالة توجيه المشترك (طلب معلومات توجيه الإرسال) SS7 MAP عبر **HLR** يجري **بحث** مع **متغيرات خطة** HLR بالتنسيق الدولي وتعيد الأداة استجابة **MSISDN** والتجوال. أدخل **الاتصال** التي ستحددها النتيجة على مكالمة. هذه هي الطريقة التي تؤكد بها الموقع الحالي للشبكة لرقم قبل تشخيص سبب توجيه المكالمات إليه بالطريقة التي تفعلها.

ترجمة الأرقام

أدخل **رمز الدولة**، .TAS يختبر كيف يتم **تطبيع وترجمة** الرقم المتصل بواسطة قواعد توجيه **رقم الهاتف** وتصرف اختياري. تعيد الأداة الرقم المترجم الذي ستستخدمه خطة الاتصال. اقرأها جنبًا إلى جنب مع علامة التبويب **التوجيه** لتأكيد أن رقمًا معينًا يتم مطابقته وإعادة كتابته كم��هو مقصود.

ESL

لأغراض التشخيص. TAS وحدة تحكم **تفاعلية** لإصدار أوامر على طراز خادم الوسائط إلى محرك اكتب أمرًا واضغط على Enter. يتم طباعة المخرجات مرة أخرى في وحدة التحكم، وتسترجع الأسهم لأعلى/أسفل الأوامر السابقة. يتم تقديم أمثلة للأوامر مثل `status`، `sofia status`، `show channels` و `show registrations` كشرائح نقرة واحدة. إنها أقل مستوى عرض للمحرك الجاري، لتأكيد القنوات الحية، حالة البوابة والتسجيلات مباشرة.

السجلات

الحية لاستكشاف أخطاء خادم تطبيق واحد دون TAS تتبع علامة التبويب **السجلات** مخرجات سجل مغادرة OmniWeb.

لوحات المراقبة

كلوحات TAS يتم تقديم أحجام المكالمات، عدادات الخدمة وغيرها من السلاسل الزمنية لـ بتكرار تلك المخططات OmniWeb التي يمكن الوصول إليها من صفحة العنصر. لا تقوم Grafana، بشكل أصلي.

ذات صلة

- **CSCF** يشير إلى المكالمات التي يطبق TAS صوت الخدمات عليها. الاثنان معًا يوفران IMS.
- **HSS** يحتفظ ببيانات المشترك وبيانات المستخدم التي يحلها Sh TAS.
- **OCS** يقوم بتقييم واحتساب مكالمات TAS عبر Diameter في الوقت الحقيقي.
- **DRA** ينقل الإشارات Diameter الخاصة بـ TAS (Sh، Gy) إلى هؤلاء الأقران.

أجهزة الاختبار

أجهزة الاختبار تحول الهواتف الذكية الحقيقية التي تعمل بنظام أندرويد في المواقع البعيدة إلى مزرعة اختبار يمكن التحكم بها عن بُعد. من خلال OmniWeb يمكنك مشاهدة شاشة الهاتف مباشرة، والتحكم به (الضغط، السحب، الكتابة، المفاتيح المادية)، وإجراء المكالمات وإرسال الرسائل النصية، وتشغيل الفحوصات الصحية المجدولة. تغطي هذه الفحوصات تسجيل VoLTE، الإشارة والاتصال. يقوم OmniWeb بتصدير نتائج النجاح/الفشل إلى Prometheus من أجل التنبيهات ولوحات المعلومات.

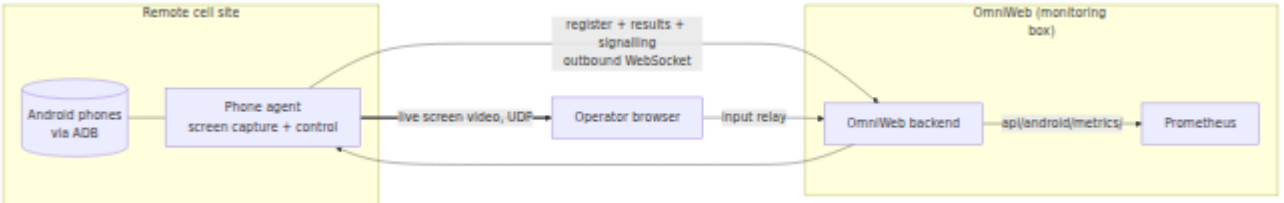
← العودة إلى دليل العمليات

توجد للإجابة على السؤال الذي يطرحه مركز العمليات: *"هل يعمل هاتف حقيقي على هذه الشبكة الآن؟"* يجب أن يكون الهاتف مسجلاً لـ VoLTE وقادراً على إجراء المكالمات، إرسال الرسائل والوصول إلى الإنترنت. لا يحتاج أحد للذهاب إلى الموقع.

الهيكلية

يعمل على تشغيل **وكيل** خفيف الوزن. يقوم ADB كل مضيف يحتوي على هواتف موصولة عبر NAT لذا فإن المواقع خلف OmniWeb، لا تحتاج إلى وصول داخلي. الوكيل بالاتصال بمركز OmniWeb لذا فهي تتحمل الروابط ذات الفقد العالي والكمون (UDP) **WebRTC** تستخدم الفيديو المباشر بشكل أفضل بكثير من مشاركة الشاشة عبر TCP. نتائج الاختبار ونقل المدخلات بالمركز.

> **مسارات الشبكة مهمة.** واجهة الويب، المدخلات وإعداد المكالمات ("الإشارة") تمر عبر HTTPS إلى خادم OmniWeb. ومع ذلك، فإن فيديو الشاشة المباشر مستوى التحكم عبر **UDP يتدفق مباشرة بين متصفح المشغل ووكيل المضيف عبر** الخادم. لا يمر عبر UDP، فإن إذا كان بإمكان المتصفح الوصول إلى الخادم ولكن ليس إلى مضيف الوكيل عبر "Connecting...". وحدة التحكم تتعطل على قاعدة للحصول على **متطلبات الشبكة** راجع جدار الحماية المطلوبة وكيفية التعرف على المشكلة.



المكون	الدور
وكيل الهاتف	يلتقط الشاشة، يحقن المدخلات، يشغل نصوص Ansible، يكتشف أجهزة ADB، واحد لكل موقع؛ يتم تثبيته بواسطة دور اختبار المضيف. `device_tester`.
OmniWeb المركزي	سجل الأجهزة، وسيط إشارة WebRTC، توزيع النصوص، تاريخ النتائج، مقاييس Prometheus.
Prometheus	يجمع نتائج الاختبارات المجدولة من `/api/android/metrics`.

أنواع الأجهزة

لم تعد المزرعة مخصصة للهواتف فقط. كل جها�ز متصل هو واحد من ثلاثة أنواع، يتم اكتشافه تلقائيًا بواسطة الوكيل ويظهر بشارة خاصة به (ورمز الروبوت أندرويد للهواتف) في الأسطول:

النوع	ما هو	وحدة التحكم
هاتف أندرويد	هاتف عادي (5.0 أندرويد+ / API 21+) عبر ADB	شاشة مباشرة + تحكم كامل
مودم USB	وحدة خلوية تعرض منافذ AT (مثل Quectel EP06)	وحدة تحكم خلوية مدفوعة بـ AT: الحالة، المكالمات، الرسائل النصية، VoLTE، قفل الشبكة
دونجل أندرويد قديم	دونجل LTE رخيص يعمل بنظام أندرويد قديم (API < 21، مثل UZ801) قديم جدًا لعرض الشاشة المباشرة	عرض **لقطة الشاشة** المعتمدة على الاستطلاع + التحكم
محاكي RAN UE	UE افتراضي من محاكي RAN، بدون أجهزة	لوحة تحكم UE: إرفاق/فصل، خمول، خارج ��لتغطية، تسجيل IMS، رسائل نصية، مكالمات

النقر على جهاز يفتح وحدة التحكم المناسبة لنوعه. داخل أي وحدة تحكم، زر **تبديل الهاتف** (أعلى اليمين) يبدل إلى جهاز آخر دون العودة إلى شبكة الأسطول.

تظهر في الأسطول مع علامة المحاكيات، لذا يمكنك التحكم في RAN **المحاكية** من محاكي **UEs** المشتركين المحاكيين بجانب الهواتف الحقيقية. يتيح لك فلتر أجهزة الاختبار تضييق نطاق العرض المعروضة في خريطة الشبكة **UE** فقط. تستخدم **نفس لوحة تحكم** RAN من محاكي UEs إلى الخاصة بمحاكي RAN، لذا هناك مكان واحد للإرفاق، الخمول، الخروج من التغطية، التسجيل في IMS، وإرسال الرسائل النصية/المكالمات. راجع محاكي RAN لدورة حياة UE الكاملة.

إضافة جهاز إلى موقع

ينضم الجهاز إلى الأسطول تلقائيًا بمجرد أن يتمكن **مضيف الوكيل** في ذلك الموقع من رؤيته عبر ADB. هناك خطوتان. أولاً، قم بتمكين ADB على الهاتف الفعلي أو VM. ثم، إذا كان الوكيل يعمل في حاوية، قم بتمرير جهاز USB إليه.

1. تمكين ADB على الهاتف

1. على الهاتف، افتح **الإعدادات** ← **حول الهاتف** واضغط على **رقم البناء** سبع مرات لفتح **خيارات المطور**.
2. في **الإعدادات** ← **النظام** ← **خيارات المطور**، قم بتشغيل **تصحيح USB**.
3. قم بتوصيل الهاتف بمضيف الوكيل باستخدام كابل USB **قابل للبيانات**.
4. يظهر الهاتف موجه *"هل تسمح بتصحيح USB* مع مفتاح RSA للمضيف. قم بتحديد *؟"* وقم بالقبول **السماح دائمًا من هذا الكمبيوتر**. (بدون تحديد، يعود الموجه في كل مرة يعيد الاتصال ويظهر الجهاز كـ `unauthorized`.)

الهاتف العادي لا يحتاج إلى أي شيء آخر. تستخدم نصوص الاختبار والشاشة المباشرة فقط ADB القياسي. احتفظ بالشاشة غير مقفلة للاتصال الأول حتى يمكن قبول الموجه.

2. تمرير جهاز USB إلى مضيف الوكيل

تخطى هذه الخطوة إذا كان الوكيل يعمل على المعدن العاري. إذا كان مضيف الوكيل هو آلة افتراضية أو حاوية، فإن hypervisor يمتلك منفذ USB، لذا يجب عليك تمرير الجهاز:

النظام الأساسي	كيفية تمرير الجهاز
Proxmox (VM)	`qm set <vmid> -usbN host=<bus>-<port>` لربط منفذ مادي (تظل الخريطة قائمة عند تبديل الهواتف على ذلك المنفذ)، أو `host=<vendor>:<product>` لمتابعة جهاز محدد. ابحث عن المعرفات باستخدام `lsusb` على مضيف Proxmox.
Proxmox (حاوية LXC)	أضف إلى `/etc/pve/lxc/<ctid>.conf`: سماح USB مجموعة جهاز (`lxc.cgroup2.devices.allow: c 189:* rwm`) وmount-bind لحافلة USB (`lxc.mount.entry: /dev/bus/usb/<bus> dev/bus/usb/<bus> none bind,optional,create=dir`)، ثم أعد تشغيل الحاوية. إعادة توصيل جهاز على حافلة مختلفة تحتاج إلى أن تكون الحافلة المطابقة مركبة.
VMware	مع تشغيل VM، **VM → الأجهزة القابلة للإزالة → <phone> → الاتصال** (وقم بإرفاق الجهاز في إعدادات USB أو أضف وحدة تحكم VM).

> والدونجل ال��ندرويد القديمة بنفس الطريقة. تظهر كفئة جهاز USB يتم تمرير المودمات نفسها، لذا فإن الحافلة التي يتم تمريرها تحمل الهواتف، المودمات والدونجل على حد USB سواء.

3. تأكيد ظهورها

على مضيف الوكيل، يجب أن تسرد `adb devices` الهاتف كـ `device` (ليس `unauthorized` خلال بضع ثوانٍ، يظهر في **عرض الأسطول** لذلك الموقع. إذا لم يظهر، راجع `offline`). أو استكشاف الأخطاء.

عرض الأسطول

تظهر **عرض أجهزة الاختبار** كل هاتف متصل عبر جميع المواقع، مجمعة حسب الموقع. تظهر كل بطاقة النموذج، الشركة المصنعة، إصدار أندرويد، دقة الشاشة، مشغل الشبكة، البطارية والبناء. يمكنك أن ترى بسرعة أي الهواتف متصلة وصحية.

تقوم المزرعة بتجميع الأجهزة حسب الموقع (مثل "موقع الخلية 12"، "المختبر الشمالي"). تظهر كل بطاقة الحالة المباشر��، البطارية والمشغل. اختر الهواتف ونصًا لتوزيع اختبار عبرها. انقر على بطاقة لفتح وحدة التحكم الخاصة بها.

تسمية جهاز. يفتح القلم على بطاقة الأسطول **تحرير بيانات الجهاز**، حيث يمكنك إعطاء الجهاز يخفي) هذه مخصصة من قبل المشغل. **MSISDN** و **IMSI**، **اسمًا** ودون معلومات **المشغل** أندرويد الحديث وتلتصق بالجهاز حتى عندما يكون غير متصل. الاسم هو (ADB من IMSI/MSISDN ما يظهر في رؤوس وحدة التحكم ومختارات الأجهزة.

تتوسع إدخال **أجهزة الاختبار** في الشريط الجانبي لتظهر كل موقع (مع عدد الأجهزة)، عرض **الوكلاء**، مكتبة النصوص، المجدول وأدوات الأجهزة، لذا يمكنك الانتقال مباشرة إلى المكان الذي تحتاجه.

تشغيل الاختبارات عبر الأجهزة

اختر واحدًا أو أكثر من الهواتف، اختر نصًا، و**تشغيل على المحدد** يوزعها بالتوازي. تتدفق النتائج إلى جدول، صف واحد لكل جهاز مع شارة نجاح/فشل، رم�� خروج، مدة وإخراج قابل للتوسيع.

الوكلاء

تظهر **عرض الوكلاء** (الشريط الجانبي ← أجهزة الاختبار ← الوكلاء) كل مقعد متصل بهذا الخادم، الأجهزة التي يحملها، متى تم تسجيله، وإصدار IP، صف واحد لكل مضيف موقع، مع حالته المتصلة برمجياته. يجيب على "أي المواقع تقوم بالتقارير فعلاً، ومن أين؟" بسرعة، وهو المكان الذي تؤكد فيه أن مقعدًا تم تثبيته حديثًا قد اتصل.

وحدة التحكم بالجهاز

النقر على هاتف يفتح **وحدة التحكم** الخاصة به: عرض مباشر للشاشة مع تحكم كامل عن بُعد.

تقوم وحدة التحكم ببث شاشة الهاتف مباشرة. انق�ر للضغط، اسحب للسحب، اكت�ب لإدخال النص. تظهر شارة ***جودة الشبكة*** *(أعلى يمين الشاشة) باللون الأخضر/البرتقالي/الأحمر بسرعة. معدل البت، نسبة فقد الحزمة لمدة ،FPS ،الدقة) انقر عليها للحصول على إحصائيات البت الكاملة شريط المفاتيح المادية (رجوع، الرئيسية، حديث، حجم، طاقة) والإجراءات .(RTT ،5 ثوانٍ، الاهتزاز السريعة (وضع الطيران، لوحة الاتصال، الرسائل، الإعدادات) تقع أدناه. توجد لوحة أدوات مع الملفات والتسجيل ،Logcat ،علامات تبويب بجانبها: التحقق من الشبكة، النصوص، الصدفة.*

> **مشاهد واحد في كل مرة.** يقوم الجهاز ببث إلى مشغل واحد في كل مرة. إذا كان شخص آخر يشاهدها بالفعل، تظهر وحدة التحكم *"مستخدمة بواسطة <user> (<IP>)"*. يتيح لك IP معرفة ما إذا كنت أنت على آلة أخرى أو مشغل مختلف. زر **استيلاء** يطالب بالبث. وحدة التحكم التي تم إسقاطها أو إعادة تحميلها تتصل بجلسة خاصة بها تلقائيًا بد�اً من القتال من أجلها.

التحكم عن بُعد

الإجراء	كيفية
الضغط	انقر في أي مكان على الشاشة
السحب	انقر واسحب
الكتابة	انقر على الشاشة، ثم اكتب على لوحة المفاتيح الخاصة بك
المفاتيح المادية	زر الرجوع، الرئيسية، حديث، حجم ±، زر الطاقة
الإجراءات السريعة	تبديل وضع الطيران بنقرة واحدة، أو فتح تطبيق لوحة الاتصال، الرسائل أو الإعدادات. تعمل هذه في الخلفية. لا تقوم بتشغيل اختبار أو تعيق وحدة التحكم.

تكون الشاشة المتدفقة هي الجهاز المباشر. أي تطبيق أو صفحة ويب يتم عرضها ويمكن التحكم فيها بالكامل من وحدة التحكم. هنا هاتف اختبار لديه صفحة مفتوحة في المتصفح، يتم التحكم بها عن بُعد:

مشاهدة أكثر من هاتف

لمشاهدة عدة هواتف في وقت واحد (كلا طرفي مكالمة اختبار، على سبيل المثال)، افتح وحدة التحكم الخاصة بهاتف واحد وانقر على **هاتف إضافي** (أعلى اليمين). اختر هاتفًا آخر من القائمة وتفتح شاشته المباشرة بجانب الأولى، مع تحكم كامل خاص به: الضغط/السحب/الكتابة، المفاتيح المادية، الإجراءات السريعة، الاستماع إلى الصوت وإحصائيات البث. تبقى القائمة مفتوحة حتى تتمكن من الاستمرار في الإضافة، وتكون الشاشات موزعة عبر الصفحة — لا يوجد حد ثابت، لذا أضف بقدر ما يوجد في المقعد.

لفتح مجموعة كاملة دفعة واحدة، حدد الهواتف التي تريدها في قائمة أجهزة الاختبار وانقر على **عرض المحدد**: يصبح الأول هو الجهاز الرئيسي (الذي تعمل عليه عمود الأدوات) وتبقى البقية موزعة بجانبه.

تحمل كل شاشة إضافية مختارها الخاص لت **تبديل** الهاتف الذي تعرضه و × لإغلاقها. يتم التقاط لذا يمكن حفظ تخطيط متعدد الهواتف المحدد كمفضل أو ،(`?with=…`) الترتيب في عنوان الصفحة مشاركته.

تعمل لوحة الأدوات مع علامات التبويب (التحقق من الشبكة، النصوص، الصدفة، ...) دائمًا على **الهاتف الرئيسي**، الذي فتحته. يسمي رأس اللوحة ذلك بحيث يكون واضحًا أين سيتم تشغيل نص أو أمر.

أدوات وحدة التحكم

بجانب الشاشة، تحتفظ **لوحة أدوات مع علامات تبويب** بأدوات كل جهاز معًا. قم بتبديل علامات التبويب دون فقدان حالة كل أداة:

علامة التبويب	ما تفعله
التحقق من الشبكة	اختبار السرعة / ping / أدوات التحقق من المكالمات / الرسائل النصية (أدناه)
النصوص	تشغيل نص مكتبة على هذا الجهاز ورؤية تاريخ تشغيله الكامل، مع إعادة تشغيل بنقرة واحدة على أي تشغيل سابق
الصدفة	وحدة تحكم تفاعلية للأوامر/الاستجابة للجهاز
Logcat	تدفق سجل الجهاز المباشر مع تصفية النص + المستوى
الملفات	تصفح، تحميل، رفع، إعادة تسمية وحذف الملفات على الجهاز
التسجيل	التقاط تسلسل ضغط/سحب كخطوط نص قابلة لإعادة التشغيل

لوحة التحقق من الشبكة

أدوات مدمجة للفحوصات التي يقوم بها المشغل يدويًا، كل منها يأخذ المدخلات التي تتوقعها:

الأداة	المدخلات	ما تفعله
مكالمة	الرقم، وقت الانتظار	يقوم بالاتصال، يؤكد أن المكالمة قد بدأت، ينتظر، ينهي المكالمة
رسالة نصية	الرقم، الرسالة	يرسل رسالة نصية ويؤكد أنها تركت الجهاز
Ping	المضيف، العدد	يقوم بعمل ping لمضيف عبر اتصال بيانات الجهاز
اختبار السرعة	عنوان URL للاختبار	يقيس معدل نقل البيانات عبر رابط بيانات الجهاز

تتذكر خانة **الرقم** الأرقام التي قمت بالاتصال بها أو إرسال رسائل نصية إليها مؤخرًا (تحتفظ بها في متصفحك فقط، وليس على الخادم) وتقدمها كقائمة منسدلة، لذا فإن إعادة الاتصال برقم اختبار هي نقرة واحدة.

النصوص

تقوم علامة التبويب **النصوص** بتشغيل أي نص مكتبة ضد هذا الجهاز الواحد وتحافظ على تاريخ تشغيله الكامل دون مغادرة وحدة التحكم. يمكنك تصفية ذلك التاريخ حسب المصدر، الحالة والاختبار. كل تشغيل سابق له زر **إعادة التشغيل**، لذا فإن تكرار فحص (أو نص فشل للتو) هو نقرة واحدة. النصوص التي تأخذ مدخلات تعيد طلبها.

الصدفة

تعد علامة التبويب **الصدفة** وحدة تحكم تفاعلية للأوامر/الاستجابة للجهاز. اكتب أمرًا، شاهد مخرجاته ورمز خروجه، م�� ↑/↓ لاسترجاع التاريخ. إنها النسخة المعادلة للجهاز من وحدة تحكم مودم AT، للأوقات التي يكون فيها أمر سريع أسرع من كتابة نص.

Logcat

تقوم علامة التبويب **Logcat** ببث سجل النظام المباشر للجهاز. تصفية حسب النص الحر والمستوى الأدنى (Verbose → Fatal). في تدفق **بدء/إيقاف** تتحكم .المستويات مشفرة بالألوان. البيانات. يوقف الإيقاف ما قمت بالتقاطه على الشاشة حتى تتمكن من التمرير عبره.

الملفات

تعد علامة التبويب **الملفات** مدير ملفات للجهاز. تصفح الدلائل (بدءًا من `/sdcard`)، ملف **تحميل** إلى جهازك، **رفع** ملف إلى الجهاز، و**إعادة تسمية**، **حذف** أو إنشاء مجلدات. مفيد لسحب ملف التقاط أو تشخيص من جهاز، أو لدفع تكوين إليه.

تسجيل الإيماءات

قم بتبديل **التسجيل**، قم بأداء تسلسل ضغط/سحب على الشاشة، وتقوم وحدة التحكم بإصدار `adb input` خطوط المعادلة. ألصقها في نص مجلد لتحويل تدفق واجهة المستخدم اليدوي إلى اختبار قابل للتكرار.

وحدة التحكم بمودم USB

في الأسطول كـ **مودم** ويفتح وحدة تحكم (وما شابه Quectel EP06) الخلوي USB يظهر مودم خلوية بدلاً من الشاشة. يقوم الوكيل بنقل أوامر AT التسلسلي منفذه عبر المودم إلى (AT). يسجل كل أمر واستجابة في علامة التبويب **Terminal** كمسار تدقيق.

علامة التبويب	ما تفعله
الحالة	الإشارة، SIM / IMSI / IMEI / قراءة لمرة واحدة للنموذج / البرنامج الثابت (CSQ + قياس CSQ لكل RAT)، تجيل المشغل، EPS، إرفاق، IMS، IP، APN، DNS/PCO
الإجراءات	إرفاق/فصل البيانات، **PDP / IP** مسبق أو مخصص، مع **نوع** تعيين APN (الراديو (وضع الطيران / إعادة، إرسال SMS، ping، عرض IP + DNS (التشغيل)
الشبكات	مسح المشغل (`AT+COPS=?`) وقياس **الخلايا** الخدمية/الجوار (`AT+QENG`) → جدول EARFCN / PCI / band / RSRP / RSRQ / SINR
قفل الخلية	قفل النطاق (`AT+QNWLOCK`)، القفل على **EARFCN محدد (+PCI)** أو العودة إلى الوضع التلقائي، تفضيل RAT (`AT+QCFG="band"`)
المكالمات	الاتصال / الرد / إنهاء المكالمة، جدول مكالمات (`AT+CLCC`)، **وتفعيل / تعطيل VoLTE** (`AT+QCFG="ims"`)
الرسائل النصية	قراءة صندوق الوارد (`AT+CMGL`)، والإرسال، الحذف
الأحداث	تمكين URCs / مكالمة / (تسجيل / مؤرخ ذات الصلة واستطلاعها في سجل إشارة / تغييرات رسائل جديدة)
Terminal	إدخال AT الكامل الخام بالإضافة إلى سجل الطلب/الاستجابة

المرجع الكامل لأوامر AT، مع استجابات EP06 موجود في الحقيقة، **modem-at-commands.md**.

> **VoLTE:** EP06 هو VoLTE/IMS *تفعيل*. فقط للصوت *VoLTE* يضبط `AT+QCFG="ims",1`؛ ولا يسجل إلا إذا، IMS لـ (إلغاء) تسجيل `AT+CFUN=1,1` قد يكون هناك حاجة لإعادة تشغيل الناقل الصحيح MBN توفره وتم اختيار SIM + كانت الشبكة.

دونجل أندرويد القديمة (وضع لقطة الشاشة)

تشغيل دونجل LTE 10$~ رخيص "MiFi" (مثل UZ801، Qualcomm msm8916) يعمل بنظام **أندرويد 4.4 (API 19)**، وهو قديم جدًا لعرض الشاشة المباشرة. تتراجع هذه الأجهزة إلى وحدة `adb screencap` للإطارات (بضع إطارات في الثانية، لأن `screencap` ويحقن (نفسه هو عنق الزجاجة على هذا الجهاز `adb input` للتحكم. تحكم **لقطة الشاشة**: يقوم الوكيل باستطلاع تحصل على عرض الضغط للضغط، الكتابة للنص. ليس فيديو سلس، لكنه يكفي للتحكم به.

يقوم الوكيل بتنعيم حواف هذه الدونجل على جانب المضيف:

- **فتح ADB**: يتم شحنها في وضع RNDIS. خدمة مدفوعة بـ udev تقوم بـ `curl` لـ `usbdebug.html` للدونجل لتحويله إلى وضع ADB. راجع agent/host-setup/mifi-dongle.
- **الإنجليزية التلقائية**: يتم شحنها باللغة الصينية. يقوم الوكيل بضبط `persist.sys.language` إلى `en-US` في المرة الأولى التي يرى فيها جهاز API-<21 (يمكن تعطيله باستخدام `OMNIWEB_DONGLE_AUTO_ENGLISH=0`).

النصوص

تكون الاختبارات نصوص bash لذا تتوفر أدوات المضيف مثل) تعمل على **مضيف الوكيل** `grep`/`awk`) وتستهدف جهازًا عبر ADB. هناك نوعان:

- **نصوص المجلد**: فحوصات الصحة التي تظهر في المكتبة، وموصل التوزيع، والمجدول. يأخذ (تقرير قوة الإشارة، VoLTE الجهاز متصل، تسجيل) بعضها يعمل مع الجهاز فقط مضيفًا وعددًا. يأخذ اختبار نقل ping يأخذ اختبار (`@param`) البعض مدخلات اختيارية (Ping، إرسال SMS، نقل البيانات، URL. اختبارات الاتصال والصوت عنوان البيانات هي نصوص مجلد، لذا يمكنك جدولتها بالإضافة إلى تشغيلها يدويًا. تؤكد (إجراء مكالمة اختباري استعادة وضع الطيران أن الجهاز يتعافى بعد فقدان الراديو. **استعادة وضع الطيران → Ping** يقوم بتشغيل وضع الطيران، ثم إيقافه، ينتظر لإعادة الاتصال بالبيانات، ثم يقوم بعمل ping. **استعادة → استعادة وضع الطيران IMS** يفعل مرة أخرى VoLTE نفس الشيء، ثم يؤكد تسجيل.
- **الأدوات المدمجة**: اختصارات فتح التطبيقات (لوحة الاتصال، الرسائل، الإعدادات) وزر وضع الطيران العادي في إجراءات وحدة التحكم السريعة. يقوم كل منها بعمل إجراء واجهة مستخدم واحد دون نتيجة نجاح أو فشل، لذا فهي ليست في المكتبة أو المجدول.

تقوم مكتبة النصوص بإدراج نصوص المجلد بدون مدخلات. تظهر كل منها وصفها ووقت انتهاءها. انقر على واحدة لعرض مصدرها (للقراءة فقط). تظهر التشغيلات الأخيرة أدناه.

تقوم النصوص بالإبلاغ عن نتيجت��ا بواسطة **رمز الخروج**: `0` هو نجاح، أي شيء آخر فشل. تظهر مخرجاتها الملتقطة في جدول النتائج.

الاختبارات المجدولة

تُعرف الاختبارات المجدولة بشكل توضيحي في `schedules.json` في دليل النصوص. يتم إعادة قراءة الملف في كل دورة، لذا فإن التعديلات تدخل حيز التنفيذ دون إعادة تشغيل. يتم تشغيل كل إدخال نص مجلد ضد أجهزته المستهدفة على فترات.

التكوين

```
{
  "schedules": [
    {
      "name": "VoLTE Registration",
      "script": "volte_registration.sh",
      "interval_seconds": 120,
      "serials": [],
      "enabled": true
    }
  ]
}
```

المعامل	النوع	مطلوب	الافتراضي	الوصف
`name`	سلسلة	نعم	-	تسمية فريدة للجدول الزمني. تظهر كعلامة على المقياس `schedule` المصدر.
`script`	سلسلة	نعم	-	اسم ملف نص مجلد في دليل النصوص للتشغيل.
`interval_seconds`	عدد صحيح	لا	300	كم مرة يتم تشغيل النص، بالثواني. الحد الأدنى 30.
`serials`	قائمة	لا	`[]`	تسلسلات الأجهزة المستهدفة. تعني **قائمة فارغة جميع الأجهزة المتصلة حاليًا**، لذا يتبع الجدول الزمني تلقائيًا أي هواتف موصولة.
`params`	كائن	لا	`{}`	المدخلات لنص يعلن عن المفاتيح هي `@param`. قيم أسماء المعاملات. على سبيل المثال، يأخذ اختبار Ping `host` و `count`.
`enabled`	منطقي	لا	true	ما إذا كان الجدول الزمني نشطًا. اضبط `false` لإيقافه دون إزالة الإدخال.
`exclusive`	منطقي	لا	false	حجز الهاتف لمدة اختبار هذا. أثناء تشغيل اختبار حصري، لا يبدأ أي اختبار مجدول آخر على ذلك الجهاز، وينتظر الاختبار الحصري نفسه حتى يكون الجهاز مجانيًا قبل أن يبدأ.

الوصف	الافتراضي	مطلوب	النوع	المعامل
استخدمه للاختبارات المدمرة — مثل تقلب وضع الطيران أو إعادة التشغيل — التي قد تفسد اختبارًا آخر (مثل مكالمة VoLTE) تعمل على نفس الهاتف في نفس الوقت.				

مثال: التحقق من VoLTE عبر موقع

```
{
  "name": "VoLTE Registration",
  "script": "volte_registration.sh",
  "interval_seconds": 120,
  "serials": [],
  "enabled": true
}
```

كيف يعمل: كل 120 ثانية يقوم المجدول بتشغيل `volte_registration.sh` ضد كل هاتف متصل. يتحقق السكربت من أن الجهاز مسجل صوتيًا VoPS مع دعم LTE على (`IN_SERVICE`)، وإذا تم تسجيل `0` ويخرج VoLTE. تصبح النتيجة مقياس Prometheus لكل جهاز.

حالة الاستخدام: إثبات باستمرار أن الهواتف الحقيقية في موقع يمكنها التسجيل لـ VoLTE، وتنبيه في اللحظة التي لا يمكن فيها التسجيل.

مثال: اختبار Ping لكل هاتف

```
{
  "name": "Ping Test",
  "script": "ping_test.sh",
  "interval_seconds": 120,
  "serials": [],
  "params": { "host": "8.8.8.8", "count": "5" },
  "enabled": true
}
```

على كل هاتف متصل. توفر `ping_test.sh` **كيف يعمل:** كل 120 ثانية يقوم المجدول بتشغيل لـ `8.8.8.8` خمس مرات عبر رابط ping مدخلات السكربت. يقوم السكربت بعمل `params` لاختبار هدف محدد `host` بيانات الجهاز ويخرج `0` إذا حصل على ردود. قم بتغيير.

حالة الاستخدام: إثبات أن الهواتف الحقيقية في موقع لديها بيانات تعمل، وتنبيه في حالة فقدان الحزم.

التوقف التلقائي أثناء استخدام الهاتف

فتح شاشة الهاتف الحية يوقف الاختبارات المجدولة **لذلك الهاتف**. اختبار يتم تشغيله على هاتف يشاهده شخص ما ويضغط عليه سيقاتلهم من أجل الشاشة ويسجل نتيجة غير ذات معنى، لذا يتخطى المجدول أي هاتف لديه مشاهد حي ويستأنف العمل عليه بمجرد إغلاق العرض.

- التوقف يكون لكل هاتف. كل هاتف آخر يستهدفه الجدول يستمر في العمل على فترته العادية.
- لا يتم احتساب التشغيل المتخطى كمنجز: يتم تشغيل الجدول في دورته التالية بمجرد أن يصبح ال��اتف متاحًا، بدلاً من الانتظار لفترة كاملة.
- يتم ترك اختبار كان قيد التشغيل بالفعل عند فتح الشاشة ليكتمل.
- أغلق عرض الهاتف (أو انتقل بعيدًا) وتستأنف الاختبارات في غضون دقيقة تقريبًا. إذا اختفى المتصفح دون إغلاق نظيف، فإن التوقف ينتهي من تلقاء نفسه.
- **تشغيل الآن** غير متأثر - التشغيل المطلوب صراحة دائمًا ما يستمر.

تظهر علامة التبويب للاختبارات المجدولة للهاتف لافتة أثناء تأثير التوقف، وتحدد الأسطول الهاتف المحتجز **قيد الاستخدام** مع من لديه.

المقاييس

تقوم OmniWeb المركزية بكشف أحدث نتيجة لكل اختبار مجدول، لكل جهاز، بتنسيق Prometheus على `/api/android/metrics`. يقوم Prometheus بجمعه كوظيفة `android_device_tests` (تم تكوينها تلقائيًا بواسطة دور المراقبة).

المقياس: `omniweb_android_test_pass` **النوع**: مقياس **الوصف**: نتيجة التشغيل المجدول الأكثر حداثة: `1` للنجاح، `0` للفشل **التسميات**:

- `phone`: طراز الجهاز (مثل `SM-A536E`)
- `serial`: رقم تسلسلي للجهاز
- `site`: تسمية موقع الوكيل (مثل `Cell Site 12`)

- `agent`: المضيف الذي يتصل به الجهاز
- `script`: السكربت الذي تم تشغيله
- `schedule`: اسم الجدول
- `status`: نتيجة التشغيل (`passed`، `failed`، `timeout`، أو `error`)

تشارك المقاييس المساعدة نفس التسميات:

الوصف	المقياس
مدة التشغيل الأخيرة، بالمللي ثانية	`omniweb_android_test_duration_ms`
الوقت Unix لآخر تشغيل	`omniweb_android_test_last_run_timestamp`

يبلغ مقياس منفصل عن أي الهواتف محتجزة حاليًا بواسطة مشاهد، بحيث يمكن لتنبيه الفساد أن يميز بين الهاتف الموقوف عمدًا واختبار معطل:

التسميات	الوصف	المقياس
`serial`، `phone`، `site`، `agent`	`1` بينما يكون لدى شخص ما شاشة الهاتف مفتوحة (تكون اختباراتهم المجدولة متوقفة)، `0` بخلاف ذلك	`omniweb_android_device_in_use`

استعلامات المثال:

```
# الهواتف VoLTE ال��تي تفشل حاليًا في تسجيل
omniweb_android_test_pass{schedule="VoLTE Registration"} == 0

# الاختبارات الفاشلة مجمعة حسب الموقع
count by (site) (omniweb_android_test_pass == 0)

# اختبار لم يتم تشغيله مؤخرًا (وكيل قديم أو جهاز غير متصل)
time() - omniweb_android_test_last_run_timestamp > 600

# نفس الشيء، متجاهلاً الهواتف التي يمتلكها شخص ما حاليًا (تكون
الاختبارات متوقفة لتلك)
(time() - omniweb_android_test_last_run_timestamp > 600)
  unless on (serial) omniweb_android_device_in_use == 1

# الهواتف التي هي قيد الاستخدام حاليًا
omniweb_android_device_in_use == 1
```

لوحة معلومات Grafana

يشحن دور المراقبة لوحة معلومات Grafana مجلد (**الأجهزة**). تقرأ **اختبارات الهاتف / الجهاز** المقاييس أعلاه وتظهر، لكل هاتف وجدول:

- حالة النجاح أو الفشل على مدى الزمن،
- أحدث نتيجة لكل هاتف واختبار،
- حداثة الاختبار (الوقت منذ آخر تشغيل، لالتقاط وكيل متوقف)،
- مدة التشغيل على مر الزمن.

قم بتصفية لوحة ��لمعلومات حسب الموقع أو الهاتف أو الاختبار في الأعلى. يتم توفير لوحة المعلومات تلقائيًا. انظر Grafana.

استكشاف الأخطاء وإصلاحها

الهاتف لا يظهر في الأسطول

الأعراض: جهاز موصول في موقع ولكنه غير مدرج تحت أجهزة الاختبار.

الأسباب المحتملة:

- على مضيف الوكيل ADB الهاتف غير مصرح له بـ
- الوكيل غير قيد التشغيل أو لا يمكنه الوصول إلى المركز
- غير متصلة/غير مصرح بها ADB الهاتف في حالة
- خدمة أجهزة الاختبار المركزية غير قيد التشغيل (تُقدم أجهزة الاختبار بواسطة خدمة خلفية مخصصة خاصة بها، منفصلة عن مجموعة الطلبات الرئيسية)

الحل:

1. في ADB (ليس `unauthorized`/`offline`) تأكد من أن الهاتف يظهر كـ `device`. على الهاتف إذا لزم الأمر RSA على مضيف الوكيل، وقم بقبول مطالبة.
2. المركزي والتوك�ن المكونين URL تحقق من أن خدمة الوكيل قيد التشغيل وأن عنوان صحيحان.
3. على المركز، تأكد من أن خدمة أجهزة الاختبار قيد التشغيل وأن البوابة توجه إليها. إذا تم تسجيل الوكيل ولكن الأسطول فارغ، فإن هذه الخدمة `/api/android/*` هي السبب المعتاد.
4. تحقق من اتصال USB للهاتف؛ أعد توصيل الكابل إذا كان يظهر كغير متصل.

شاشة وحدة التحكم تبقى على "Connecting"

الأعراض: تفتح وحدة تحكم الجهاز ولكن الشاشة لا تظهر أبدًا، بينما يعمل بقية واجهة المستخدم (قائمة الأسطول، تفاصيل الجهاز، الإدخال) بشكل طبيعي ويظهر الجهاز **متصل**.

الأسباب المحتملة:

- تم حظر UDP من **مباشرة** بين شبكة المتصفح ومضيف الوكيل (تدفقات الفيديو الحية المتصفح إلى مضيف الوكيل، وليس عبر الخادم، وهذا هو السبب الأكثر شيوعًا)
- لا يمكن للوكيل بدء التقاط الشاشة على ذلك الهاتف

تم إثبات عمل TLS (تم تحميل واجهة المستخدم) ومع مشاكل، هذه SSL أو MTU: مشكلة **ليست** ستت�ل الفيديو *ثم* تنقطع بدلاً من عدم البدء أبدًا. العلامة الدالة هي جهاز يظهر **متصل** MTU في الأسطول ومع ذلك لن يبدأ عرض الفيديو الحي وحده.

الحل:

1. تأكد من أن شبكة المتصفح يمكنها الوصول إلى مضيف الوكيل عبر **UDP** (مسار الفيديو). تسمح لشبكة المشغل بالوصول إلى VLAN/يعني هذا عادةً قاعدة جدار ناري مضيفي الطاولة عبر UDP. انظر **متطلبات الشبكة** للحصول على القاعدة الدقيقة التي يجب طلبها وكيفية تأكيد الإصلاح.

2. تحقق من سجل الوكيل بحثًا عن أخطاء التقاط الشاشة. بعض الهواتف لا يمكن التقاط شاشتها عبر ADB.

تقارير VoLTE / "غير قابلة للقراءة "فحوصات الإشارة

الأعراض: تفشل سكربتات VoLTE أو الإشارة مع حالة الهاتف غير قابلة للقراءة.

الأسباب المحتملة:

- يقيد الهاتف حالة الهاتف إلى الوصول المميز

الحل:

1. قد تخفي الأجهزة المقفلة من قبل ADB. استخدم هواتف اختبار تكشف حالة الهاتف لـ البائع ذلك بدون وصول مميز.

أجهزة الاختبار: متطلبات الشبكة

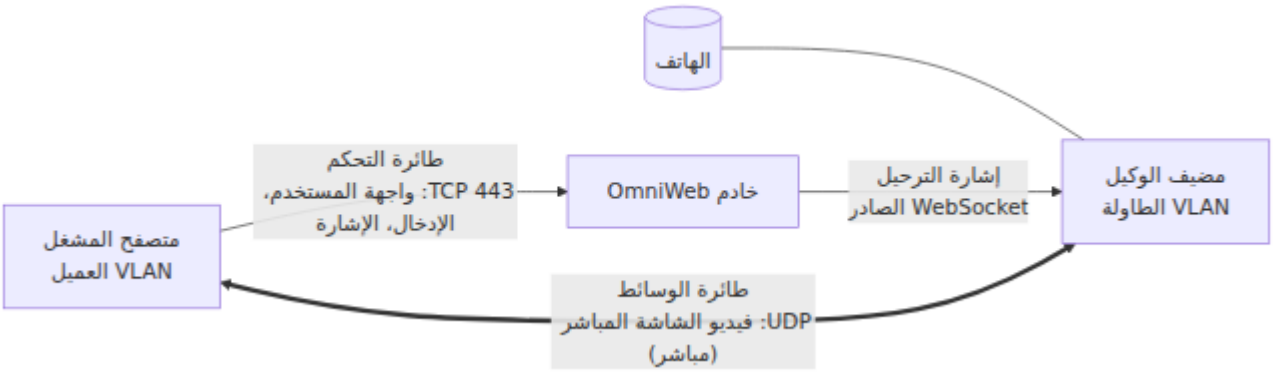
تستخدم مشاهدة الهاتف المباشرة في **أجهزة الاختبار مسارين شبكيين منفصلين**. افهم الانقسام لجعله يعمل عبر الجدران النارية و VLANs. يساعدك الانقسام أيضًا في تشخيص أكثر الأعراض شيوعًا، وهو وحدة التحكم التي تبقى على **"Connecting..."** إلى الأبد.

← العودة إلى أجهزة الاختبار

المساران

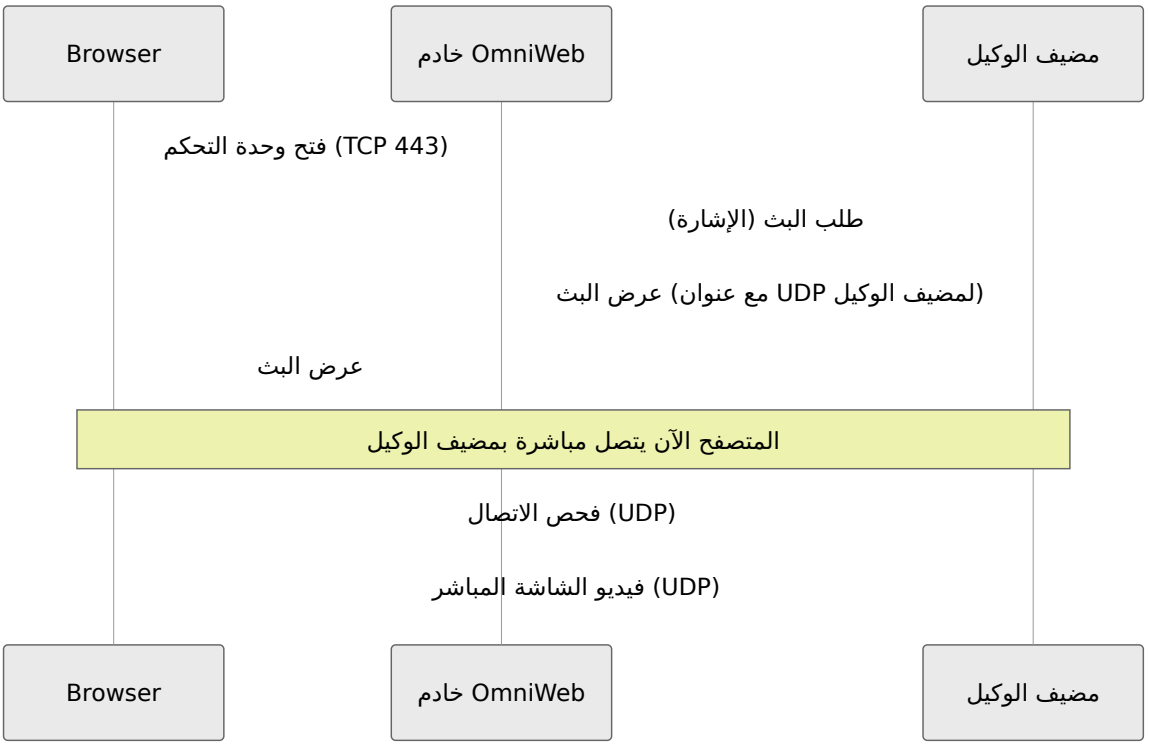
المسار	يحمل	الاتجاه	النقل	نقطة النهاية
طائرة التحكم	واجهة الويب، تسجيل الدخول، قائمة الأجهزة، الإدخال عن بُعد، نتائج الاختبار، وإعداد المكالمة ("الإشارة") لعرض مباشر	المتصفح ↔ خادم OmniWeb	**TCP 443 (HTTPS)**	خادم OmniWeb
طائرة الوسائط	الفيديو المباشر للشاشة نفسها	المتصفح ⇄ **مضيف الوكيل** (الطاولة التي يتم توصيل الهاتف بها)	**UDP** (WebRTC)	مضيف الوكيل، **ليس** الخادم

النقطة الحاسمة: **الفيديو المباشر لا يتدفق عبر خادم OmniWeb.** بمجرد أن يكون الخادم قد وسّط الاتصال، تتدفق الفيديوهات **مباشرة بين متصفح المشغل ومضيف الوكيل** عبر UDP. إذا كانت الشبكة تسمح للمتصفح بالوصول إلى *الخادم* ولكن ليس إلى *مضيف الوكيل*، فإنها تحمل واجهة المستخدم، وتعرض قائمة الأجهزة، ثم تتوقف عند "Connecting...".



لماذا المسار الوسائطي مباشر

بحيث **UDP عبر WebRTC** يتم إرسال فيديو الشاشة المباشر ��ن نظير إلى نظير باستخدام يتحمل الروابط عالية التأخير وفقدان الحزم النموذجية لمواقع الخلايا البعيدة بشكل أفضل من TCP. تمريره عبر خادم مركزي عبر **مباشر UDP** العيب هو أن متصفح المشغل يحتاج إلى **مسار** **إلى مضيف الوكيل**. لا يوجد ترحيل وسائط في المنتصف للعودة إليه.



متطلبات الجدار الناري

لكي يتمكن المشغل من مشاهدة الهواتف في موقع ما، يجب السماح **بكلا** المسارين من شبكة المشغل إلى المضيفين المعنيين.

طائرة التحكم (عادة مفتوحة بالفعل)

الحقل	ا��قيمة
الإجراء	السماح (حالة)
البروتوكول	TCP
المصدر	المشغل / العميل VLANs
الوجهة	خادم OmniWeb
منفذ الوجهة	`443`

على الإطلاق، فإن هذا المسار مفتوح بالفعل. لا حاجة للتغيير OmniWeb إذا تم تحميل واجهة.

طائرة الوسائط (التي عادة ما تكون مفقودة)

الحقل	القيمة
الإجراء	السماح (**حالة**، لذا يُسمح تلقائيًا بفيديو العودة)
البروتوكول	**UDP**
المصدر	المشغل / العميل، حيث تعمل المتصفحات VLANs
الوجهة	**الشبكة الفرعية لمضيف الطاولة** (مضيفي الوكيل)، مثل `10.0.20.0/24`
منافذ الوجهة	الافتراضي المؤقت الذي يستمد منه الوكيل Linux نطاق) `32768–60999` منافذ الوسائط)

يبدأ المتصفح دائمًا الاتصال بالوسائط، لذا فإن السماح **الحالة** على `الـعميل → مضيف الـو��يل` أو غيرها متضمنة STUN/TURN يسمح أيضًا بفيديو العودة للوكيل تلقائيًا. لا توجد منافذ UDP.

> **لا تغير المنفذ 443 من أجل هذا.** الإشارة بالفعل تمر عبر طائرة التحكم. فقط يجب فتح مسار الوسائط UDP إلى مضيفي الوكيل.

موصى به: تثبيت نطاق منفذ الوسائط

فتح النطاق المؤقت بالكامل (`60999–32768`) واسع. يمكنك بدلاً من ذلك تكوين الوكيل لاستمداد منافذ الوسائط الخاصة به من نطاق ثابت صغير. هذا يقلل قاعدة الجدار الناري إلى كتلة مرتبة:

الحقل	القيمة
الإجراء	السماح (حالة)
البروتوكول	UDP
المصدر	المشغل / العميل VLANs
الوجهة	الشبكة الفرعية لمضيف الطاولة
منافذ الوجهة	(نطاق مثبت) `50000–50100`

هذا هو الشكل المفضل لتسليمه إلى فريق الشبكة. 100 منفذ إلى شبكة فرعية واحدة أسهل بكثير للموافقة عليها وتدقيقها من النطاق المؤقت الكامل. يتم تعيين النطاق المثبت على مضيف الوكيل. تنسيق النطاق المحدد مع من يحافظ على الطاولات بحيث تتطابق قاعدة الجدار الناري وتكوين الوكيل.

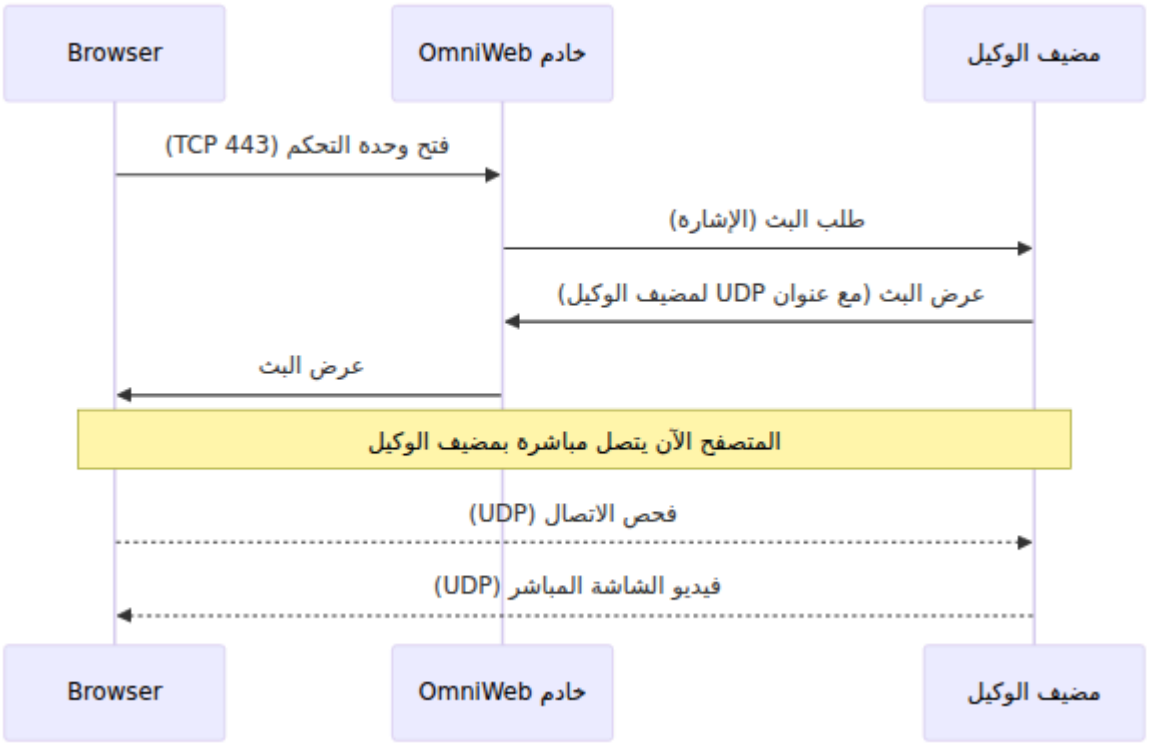
التعرف على المشكلة

الأعراض: تفتح وحدة التحكم للجهاز، لكن الشاشة لا تظهر أبدًا. تبقى على "Connecting..." إلى أجل غير مسمى. كل شيء آخر يعمل: قائمة الأسطول، تفاصيل الجهاز، حتى إعداد الإدخال عن بُعد.

هذا عادة ما يكون بسبب حظر مسار UDP لطائرة الوسائط. **ليس** مشكلة TLS / الشهادة و **ليس** مشكلة MTU:

السبب المشتبه به	لماذا ليس هذا	ماذا سترى فعليًا إذا كان الأمر كذلك
SSL / الشهادة	واجهة المستخدم، تسجيل الدخول، قائمة الأجهزة والإشارة جميعها تنجح عبر HTTPS، لذا فإن TLS يعمل بوضوح	ستفشل الصفحة نفسها في التحميل، أو تظهر تحذير شهادة
MTU / التجزئة	مهم فقط عندما تتدفق حزم MTU الفيديو. هنا **لا** تصل أي ح��م فيديو على الإطلاق	سيتصل الفيديو، ثم يتوقف أو يتمزق، وليس يبقى على "Connecting..."
مضيف / هاتف معطل	يظهر الجهاز **متصل** في الأسطول مع بيانات البطارية / المشغل المباشرة	سيكون الجهاز مفقودًا من الأسطول، أو مُعَلَّمًا كغير متصل
حظر مسار UDP ✓	يمكن للمتصفح الوصول إلى الخادم (تحميل واجهة المستخدم) ولكن ليس UDP إلى مضيف الوكيل عبر	"Connecting..." الدائم، بالضبط هذا العرض

علامة مفيدة: تظهر بلاطة الجهاز الهاتف كـ **متصل** (لذا فإن الوكيل والهاتف في حالة جيدة ويمكن للخادم رؤيتهما)، ومع ذلك لن يبدأ العرض المباشر وحده. تلك المجموعة تشير بوضوح إلى مسار الجدار الناري لطائرة الوسائط.



تأكيد الإصلاح

بعد تطبيق قاعدة الجدار الناري، أعد فتح وحدة التحكم للجهاز. إذا ظهرت الشاشة في غضون ثوانٍ قليلة وذهب شارة **جودة الشبكة** (في أعلى يمين العرض المباشر) إلى اللون الأخضر، فإن مسار الوسائط يعمل. تؤكد إحصائيات تدفق الشارة (الدقة، FPS، الاهتزاز، نسبة فقد الحزم، معدل البت، RTT) أن الفيديو يتدفق من النهاية إلى النهاية.

إذا استمرت في التوقف، تحقق من شيئين مع من يحافظ على الطاولات. أولاً، يجب أن تتطابق **الشبكة الفرعية والمنافذ** لقاعدة الجدار الناري مع مضيفي الوكيل ونطاق منافذ الوسائط المكونة لديهم. ثانيًا، يجب أن تنطبق القاعدة على **VLAN** للمشغل (جهاز **المصدر الفعلي** كمبيوتر محمول على Wi-Fi كمبيوتر محمول على LAN الضيف هو مصدر مختلف عن LAN المؤسسي).

مواقع المشغل المتعددة

يجب أن تحتوي كل شبكة مشغل تحتاج إلى مشاهدة الهواتف على قاعدة طائرة الوسائط لشبكة VLAN الخاصة بها. القاعدة هي لكل شبكة فرعية مصدر ← شبكة فرعية للطاولة، لذا فإن إضافة مكتب جديد، أو مجموعة VPN، على إضافي كمصدر الفرعية شبكتها إضافة تعني موقع أو UDP. نفس السماح لـ LAN المواقع التي لا يشاهد مشغلوها الهواتف إلا من شبكة LAN الخاصة بالطاولة. على الإطلاق VLAN نفسها لا تحتاج إلى قاعدة بين.

تخطيط الشبكة ونافذة واحدة

هي "نافذة واحدة" للدخول إلى الشبكة بأكملها. تظهر كيف تتصل OmniWeb تعتبر وجهات تخطيط العناصر، وأي منها تم نشره، وتتيح لك القفز مباشرة من عقدة على الخريطة إلى مساحة العمل الخاصة بتلك العنصر.

← العودة إلى دليل العمليات

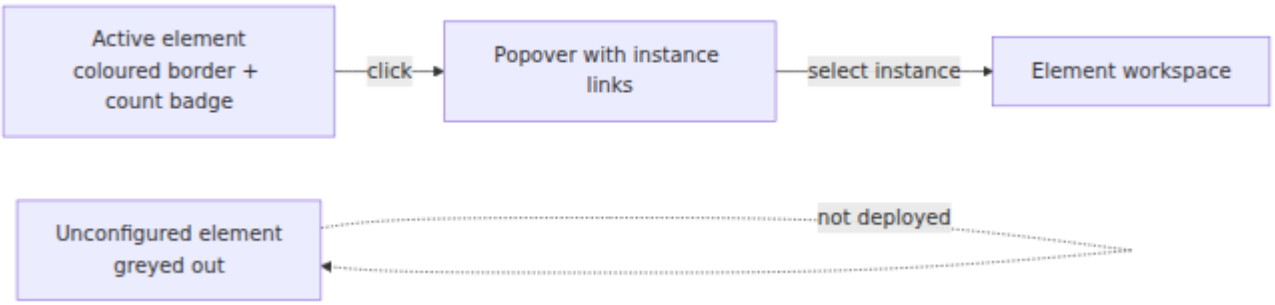
وجهات التخطيط

تقدم صفحة الهبوط/التخطيط الشبكة عبر أربعة علامات تبويب. كل واحدة هي خريطة تفاعلية للعناصر ذات الصلة وواجهاتها.

تخطيط EPC: UE → eNB → MME → SGW-C → PGW-C → UPF، مع إشارات Diameter عبر DRA إلى HSS. تظهر العناصر النشطة بحدود ملونة وشارة عدد ال��الات.

علامة تبويب	العناصر المعروضة
النواة (EPC)	UE → eNB → MME → SGW-C → PGW-C → UPF؛ DRA ↔ HSS؛ OCS؛ TWAG؛ RAN Monitor
IMS	P-CSCF → I-CSCF → S-CSCF؛ DRA ↔ HSS؛ TAS؛ IMS SMSc → SMSC → SMPP GW؛ OCSاستحقاق ؛ (OmniSEP)
نواة CS	BTS → BSC → MSC؛ STP ↔ HLR / CAMEL GW / IP-SM-GW؛ HSS؛ SMSC؛ OCS
نواة 5G	gNB → AMF → SMF → UPF؛ NRF، SCP، AUSF، UDM، UDR، PCF؛ CHF → OCS؛ NSSF؛ BSF

قراءة الخريطة



- تظهر `omniweb.json`. **العناصر النشطة** هي تلك التي تم إعلان حالات لها في بحدود ملونة وشارة تظهر عدد الحالات الموجودة. انقر على واحدة لفتح نافذة منبثقة تحتوي على روابط مباشرة لكل حالة. يمكنك بعد ذلك التنقل من التخطيط مباشرة إلى صفحات العنصر.
- **العناصر غير المكونة** تظهر باللون الرمادي، لذا ت��مل الخريطة كجرد سريع لما هو موجود وما هو غير موجود.
- **الاتصالات** تشير إلى الواجهة بين العناصر (مثل SIP، Diameter، PFCP، GTP-C، SS7)، مميزة أنواع الإشارات.

هذا يجعل صفحة التخطيط هي نقطة البداية الطبيعية: رؤية شكل الشبكة، وتحديد ما تم نشره، والتعمق.

تخطيط مستوى العنصر

التخطيط، ← **PGW-C** تقدم بعض العناصر أيضًا وجهة تخطيط مركزة خاصة بها. علامة تبويب مع ،Diameter ونظرائها من UPF و SGW-C على سبيل المثال، تظهر علاقات تلك العقدة مع توضيح عدد الجلسات الحية والاستخدام. هذا يوفر عرضًا محليًا للنافذة الواحدة لجوار تلك العنصر.

تخطيط PGW-C: علاقات SGW-C و UPF ونظراء Diameter مع توزيع الجلسات لكل نظير.

قائمة المضيفين والبنية التحتية

بجانب وظائف الشبكة نفسها، تعتبر صفحة **قائمة المضيفين** هي النافذة الواحدة للبنية التحتية التي تشغلها. تسرد جميع مضيفي البنية التحتية حسب الفئة، كل منها مع رابط مباشر إلى واجهته على الويب:

الفئة	أمثلة
المراقبة	Grafana، Prometheus، Loki
التقاط SIP	واجهة ويب Homer
الشحن	واجهة ويب OCS
DNS	خوادم DNS
الافتراضية	وحدات التحكم في Proxmox
الإدارة خارج النطاق	إدارة خادم iDRAC
أجهزة التوجيه	MikroTik WebFig، Peplink
الميكروويف	SAF، روابط Ubiquiti AirFiber
NAS	Synology DSM

قائمة المضيفين: كل مضيف للبنية التحتية والعناصر حسب الفئة، كل منها مع رابط مباشر إلى واجهته على الويب (واجهات برمجة التطبيقات للعناصر، والمزيد ،Grafana، Prometheus، Loki).

هذا يوفر للمشغلين مكانًا واحدًا للوصول إلى كل نظام دعم: المراقبة، وحدات التحك
الافتراضية، الإدارة خارج النطاق، والنقل. لا يحتاجون إلى البحث عن الإشارات المرجعية.

TWAG: بوابة الوصول الموثوقة لشبكة WLAN

تقدم **TWAG** (بوابة الوصول الموثوقة لشبكة WLAN) وصول Wi-Fi موثوق إلى النواة المتنقلة. تقوم Wi-Fi باستخدام EAP-AKA/AKA′ ضد AAA/HSS عبر Diameter، وتمنح كل عميل مصادق عليه عنوان IP عبر DHCP، عبر نفق GTP وتربط بياناته مرة أخرى إلى النواة الحزم عبر نفق إلى PGW. كما هو Wi-Fi والسياسة، والرسوم للمشترك على APN، وبالتالي، يتم تقديم نفس الحال في الشبكة الخلوية. لوحة التحكم الخاصة بها هي المكان الذي يمكنك من خلاله رؤية من هو متصل، وما إذا كانت مسارات GTP وDiameter صحية، ومسح الجلسات الفردية.

← دليل العمليات

تعتبر لوحة التحكم عنصر صفحة لكل مثيل يتم الوصول إليها من الشري�ي الجانبي عندما تعمل TWAG في مخزون الموقع. تمر جميع حركة المرور عبر وكيل OmniWeb الخلفي إلى واجهة TWAG، وهي منظمة في TWAG برمجة التطبيقات الخاصة بـ لذا تبقى خلف البوابة الموثوقة الوحيدة. علامات تبويب.

نظرة عامة

تعتبر علامة التبويب الرئيسية قراءة صحية على شاشة واحدة: **الجلسات** النشطة والإجمالية، المتصلة/المنفصلة، **المشتركين** المقبولين، عدد **نقاط الوصول**، عدد عقود **Diameter نظائر** (مثل EAP-AKA)، الخاص به، **وضع المصادقة** المستخدم PGW وعنوان **GTP** حالة نفق ،**DHCP** **حركة المرور** الإجمالية الداخلة والخارجة، وقت التشغيل، وتغذية **النشاط الأخير** الحية للمصادقات وبدايات/توقفات الجلسات.

الجلسات

مصادق عليها، حيث تظهر كل صف هوية **المشترك** (معرف الوصول إلى Wi-Fi كل جلسة الخادم، **مدة** الجلسة، و**البايتات** **NAS IP**، **SSID**، العميل **MAC**، المعين **IP**، الشبكة)، **الحالة** **الداخلة/الخارجة**. يمكن للمشغل **حذف** جلسة لقطع اتصال عميل قسراً، على سبيل المثال لمسح جهاز عالق أو غير متعاون.

نقاط الوصول

نقاط الوصول WLAN (أجهزة NAS) المتصلة حالياً بالبوابة. يمكن **إزالة** كل منها بشكل فردي عندما يتم إلغاء تكليف نقطة وصول أو تحتاج إلى مسح.

المحاسبة

سجلات الاستخدام التي تم رفعها للعملاء المصادق :TWAG جلسات ا��محاسبة التي سجلتها عليهم. يمكن **حذف** جلسات المحاسبة الفردية.

Diameter

التي تحمل المصادقة، مع عدد متصل وغير متصل. تقدم AAA/HSS إلى Diameter اتصالات نظير لاختبار (Multimedia-Auth-Request (MAR ترسل طلب .**Diameter** هذه العلامة أيضاً **اختبار** عندما تفشل Diameter وهو أسرع طريقة لإثبات الاتصال بـ AAA/HSS، مسار المصادقة إلى المصادقات.

DHCP

عقود DHCP التي أصدرتها TWAG لعملاء Wi-Fi، حتى مع العنوان، العميل وحالة العقد لكل منها، تتمكن من تأكيد أن العملاء يتم توجيههم ورؤية مقدار ما يتم استخدامه من المجموعة.

السجلات

تقوم علامة تبويب TWAG فردية دون **السجلات** بعرض سجل المباشر لحل مشاكل بواب�� مغادرة OmniWeb.

الإجراءات

تطلب كل إجراء تأكيد أولاً:

- **حذف جلسة**: قطع اتصال جلسة Wi-Fi (علامة تبويب الجلسات، مصادق عليها قسراً لكل صف).
- **حذف نقطة وصول** / NAS: مسح إدخال نقطة وصول واحدة (علامة تبويب نقاط الوصول، لكل صف).
- **حذف جلسة محاسبة**: إزالة سجل محاسبة واحد (علامة تبويب المحاسبة، لكل صف).

- **اختبار Diameter**: إرسال MAR اختبار للتحقق من مسار Diameter إلى AAA/HSS (علامة تبويب Diameter).

ذات صلة

- **PGW** يربط مستوى المستخدم لـ TWAG عبر GTP. انظر عناصر النواة الحزم.
- **HSS** يحتفظ ببيانات مصادقة المشتركين التي تحل طلبات Diameter الخاصة بـ TWAG.
- ePDG: نظير Wi-Fi غير الموثوق لمكالمات Wi-Fi.

UPF: وظيفة مستوى المستخدم

إن **UPF** (وظيفة مستوى المستخدم) هي عقدة توجيه الحزم في النواة المحمولة. إنها تحمل حركة المرور الفعلية لكل مشترك: تتلقى أنفاق GTP-U من شبكة الوصول على **N3** (S1-U في EPC)، وتوجه الحزم من وإلى شبكة البيانات، وتطبق جودة الخدمة (QoS)، وحساب الحجم لكل تدفق، وتخزن الحزم الهابطة عندما يكون الجهاز في حالة خمول. ليس لديها منطق خاص بها. يقوم مستوى التحكم (وهو **SGW-C** في EPC عبر **Sxa**، أو **SMF** في نواة 5G عبر **N4**) ببرمجتها بالكامل عبر **PFCP**. يقوم مستوى التحكم بتثبيت قواعد الكشف عن الحزم، والتوجيه، وجودة الخدمة، وتقارير الاستخدام التي تصف كيفية تعامل UPF مع حركة مرور كل جلسة. يقوم **OmniUPF** من Omnitouch بتنفيذ مسار التوجيه كـ **eBPF/XDP dataplane** في النواة، بحيث تصبح القواعد التي يثبتها مستوى التحكم إدخالات في خرائط eBPF التي يستشيرها برنامج XDP لكل حزمة. تعرض OmniWeb ارتباطات UPF الخاصة بـ PFCP وخرائط eBPF الحية، والجلسات، ومحتويات ذاكرات التخزين الهابطة، وحالة الحديقة المسورة والتكوين، والتوجيه، وإحصائيات dataplane. تصل إلى مخططات الإنتاجية والاتجاهات على لوحات معلومات Grafana من نفس الصفحة.

← دليل العمليات

تعتبر UPF عنصر صفحة لكل مثيل يمكن الوصول إليه من الشريط الجانبي عند تشغيله في جرد الموقع، مع محدد مثيل حيث يتم نشر عدة منها وعرض أسطول للحالة الإجمالية. تمر كل حركة المرور عبر وكيل خلفية OmniWeb إلى واجهة برمجة تطبيقات UPF، لذا تبقى خلف بوابة مصدقة واحدة. يفتح رابط الوثائق في رأس الصفحة (زر المساعدة في السياق) هذه الصفحة. وهي منظمة في علامات تبويب.

اختيار الأسطول والمثيل

واحد، يسرد **عرض الأسطول** كل مثيل مع صحته في لمحة. UPF عندما يعمل موقع ما بأكثر من .هذه هي أسرع طريقة لتأكيد أن مستوى المستخدم بالكامل يعمل قبل أن تتعمق في عقدة واحدة

تقرأه الصفحة. كل UPF من أي علامة تبويب، يقوم **محدد المثيل** في رأس الصفحة بتبديل أي مرتبط بالمثيل المحدد، لذا تختار (الإحصائيات ،eBPF الجلسات، الارتباطات، خرائط) شيء أدناه العقدة مرة واحدة وتتابع الصفحة بأكملها معها.

نظرة عامة

التي تحتفظ بها مع **PFCP** حالتها **الصحية**، عدد **ارتباطات** :UPF قراءة صحية لشاشة واحدة لـ نظرائها في مستوى التحكم، إجمالي **الجلسات النشطة** عبر هؤلاء النظراء، و**عدادات إجراءات** أو تم إسقاطها، أو إعادة توجيهها، أو نقلها أو إلغاؤها، ،dataplane عدد الحزم التي مرت بها :**XDP** مع حالة ارتباطه، **PFCP** وهو التأكيد الأسرع على أن الحركة تتدفق فعليًا. أدناه، يتم سرد كل **نظير** FARو PDR سعة خرائط **eBPF** وعدد الجلسات وأي نبضات قلب مفقودة، وتظهر **أحجام خرائط** والحد الأقصى لعدد الجلسات. يتيح لك مربع البحث القفز مباشرة إلى جلسة بواسطة URRو QERو إلى أول نظير نشط في PFCP وإجراء **تقرير عقدة** يرسل طلب تقرير عقدة ،**TEID** أو **UE IP** مستوى التحكم.

الجلسات

التي قام مستوى التحكم PDU حالة مستوى المستخدم لكل حامل / جلسة :**PFCP** كل **جلسة** للجلسة، **IMSI المحلي والبعيد** ويظهر **SEID** بتثبيتها. يتم تحديد كل صف بواسطة و**APN/DNN**، **الكشف عن** و**لارتباط** (أي نظير مستوى التحكم يمتلكها)، وعدد قواعد **الحزم**، و**إجراءات التوجيه**، و**فرض جودة الخدمة** و**تقارير الاستخدام** التي تحملها. ابحث للعثور على الجلسة التي تخدم جهازًا أو نفقًا معينًا **TEID أو UE IP حسب**.

عبر PFCP تسرد نفس علامة التبويب في **عرض الأسطول** كل جلسة، UPFs عندما يتم نشر عدة في TEIDو UE IP الحامل موضحًا مقابل كل صف. يتم البحث عن UPF جميعها في جدول واحد، مع في القائمة المجمعة. فتح صف يذهب إلى تفاصيل تلك APN/DNNو IMSI ؛ يتم مطابقةUPF كل الذي لا يمكن الوصول إليه فوق الجدول، لذا لا يتم UPF الجلسة على مثيلها الخاص. يتم تسمية الخلط بين القائمة القصيرة وبين مستوى مستخدم خامد.

تفاصيل الجلسة

فتح جلسة يظهر حالتها الكاملة للقواعد. ترسم **خريطة قواعد الجلسة** كيف تشير كل **قاعدة كشف عن الحزمة (PDR)** إلى **قاعدة إجراء التوجيه (FAR)**، و**قاعدة فرض جودة الخدمة (QER)** و**قواعد تقارير الاستخدام (URR)** التي تطبقها. انقر على أي عقدة لتسليط الضوء فقط على القواعد المرتبطة بها، بحيث يمكنك تتبع مسار تدفق واحد عبر dataplane. تحت الخريطة، تقدم أربع جداول التفاصيل:

- **قواعد كشف الحزم (PDR)**: كيف تصنف UPF الحزم الواردة. يشمل هذا الاتجاه SDF (نطاقات UE IP أو TEID الوارد الذي يتطابقون معه، ومرشحات (صاعد / نازل)، و البروتوكول والمنافذ)، وأي FAR وQER وURRs يتم حلها إليها.
- **قواعد إجراء التوجيه (FAR)**: ما يحدث للحزم المطابقة. الإجراء هو **توجيه**، **إسقاط**، **تخزين مؤقت** أو **إخطار CP**، مع تفاصيل نفق GTP-U الصادر (IP البعيد وTEID). يمكنك تعديل FARs في المكان ومثيل الشبكة.
- **قواعد فرض جودة الخدمة (QER)**: يشمل هذا جودة الخدمة لكل تدفق. **QFI**، حالة **البوابة** (مفتوحة / مغلقة) و**أقصى** و**معدلات البيانات المضمونة**. يمكنك تعديل QERs في المكان.
- **قواعد تقارير الاستخدام (URR)**: عدادات الحجم. هذه هي بايتات الرفع والنزول الحالية والأخيرة المبلغ عنها ورقم تسلسل التقرير، وهو ما تغذيه UPF مرة أخرى إلى مستوى التحكم من أجل الشحن والحصة.

من رأس الجلسة يمكنك أيضًا **تفعيل أو إزالة إعادة توجيه الحديقة المسورة** لتلك الجلسة المحددة (انظر الحديقة المسورة أدناه).

الارتباطات

مع نظرائها في مستوى التحكم UPF التي تحتفظ بها Sxa/N4 العلاقات: **PFCP** إن **الارتباطات البعيد والمنفذ** للنظير، وعدد **الجلسات**، وما إذا كانت **IP** يظهر كل صف (SMF أو SGW-C). **مرتبطة** حاليًا، وعدد **نبضات القلب المفقودة**، ومتى كانت آخر مرة **اتصلت** أو **انفصلت**. هنا تؤكد أن مستوى المستخدم ومستوى التحكم في تناغم. هنا يمكنك أيضًا اكتشاف نظير نبضات قلبه تتلاشى.

الإحصائيات

مدى امتلاء **eBPF** في الوقت الحقيقي. تُظهر **استخدام خريطة** dataplane الأرقام الفعلية لـ كأشرطة استخدام مقابل السعة التي تتحول إلى (URRو QER، FAR، PDR، الجلسات) كل خريطة يقترب من سعته المحددة UPF اللون الكهرماني والأحمر كلما اقتربت من حدها، لذا يمكنك رؤية عدد الحزم المارة / المرفوضة / المعاد **XDP** قبل أن يبدأ في رفض الجلسات. تُظهر **إحصائيات** كأرقام UPF الخاصة بـ Prometheus الملغاة، وقسم **المقاييس** يعرض عدادات / TX / توجيهها فردية.

تقرأ فحص السعة نفس نموذج الاستخدام مقابل السعة. في لمحة، يمكنك أن تخبر ما إذا كانت المورد المقيد هو جدول الجلسات أو واحدة من خرائط القواعد.

التوجيه

UE IP يسرد جدول **مسارات** المسارات التي توجه حركة مرور المشتركين إلى ومن UPF. المخصصة، وإجراء **مزامنة** UE IP حاليًا لمجموعات UPF **النشطة** المسارات التي تحتفظ بها في vtysh محطة **FRR** أدناه، توفر **وحدة التحكم في** dataplane. **المسارات** يوفقها مع السياق ضد خادم توجيه UPF. لفحص حالة التوجيه، اكتب أمر `show` على سبيل المثال) `show ip route` أو `show ip ospf neighbor`)، مع إكمال علامة التبويب وسجل الأوامر. لإجراء تغيير، الخاصة بها إلى UE عن مجموعات UPF انتقل إلى **وضع التكوين**. هذه هي الطريقة التي تعلن بها الشبكة المحيطة دون مغادرة OmniWeb.

الذاكرات

إن **ذاكرات الحزم الهابطة**. عندما تصل بيانات هابطة لجهاز في حالة خمول (لا يوجد نفق نشط)، المعني وتطلب من مستوى التحكم أن يطلب من الجهاز. FAR بتلك الحزم ضد dataplane تحتفظ بتفريغ الحزم المخزنة (هذا هو جانب مستوى المستخدم من UPF بمجرد إعادة إنشاء النفق، تقوم التي **FARs إخطار بيانات هابطة**). تظهر علامة التبويب **إجمالي الحزم المخزنة** و**إجمالي لرؤية عدد **FAR ID** و**إجمالي**، وأداة **بحث بواسطة FAR** تحمل الحزم، و**حدود التخزين لكل معين. يمكن **تفريغ** الذاكرات بشكل فردي أو **مسحها** بكميات كبيرة FAR الحزم التي يحتفظ بها.

خرائط eBPF

متصفح مباشر على **خرائط eBPF** التي هي dataplane الخاصة بـ UPF. هذه هي الإدخالات لكل حزمة، مقسمة عبر علامات تبويب XDP ��لخام على جانب النواة التي يستشيرها برنامج:

- **PDR الصاعدة**: مفاتيح بواسطة TEID الخاص بـ FARو PDR الوارد، الذي يربط نفقه به.
- **PDR الهابطة**: مفاتيح بواسطة UE IP، PDR الذي يربط بيانات هابطة لمشترك بـ FARو الخاص به.
- **FAR**: الصادر وإنشاء الرأس TEID، البعيد IP، إجراءات التوجيه، مع الإجراء المفكك الخارجي.
- **QER**: إدخالات جودة الخدمة، مع QFI، حالة البوابة وحدود معدلات البيانات.
- **URR**: عدادات الاستخدام، مع الأحجام الحالية والأخيرة المبلغ عنها للرفع/النزول.

انقر على أي صف لـ **تعديل إدخال الخريطة الخام**، وهو أداة استكشاف وإصلاح على مستوى الخرائط بالكامل، لذا تقوم بتحرير إدخال للتشخيص بدلاً من التشغيل PFCP منخفض. عادةً ما تقود الروتيني.

التكوين

عرض للقراءة فقط لكيفية تكوين UPF: **الشبكية** هويتها (عنوان، معرف العقدة PFCP والمنفذ، مدير المسار ونوعه، (FTUP، UEIP، **والميزات** التي تم تمكينها (N9و N3 عناوين، منفذ API، ووضع إرفاق XDP: (محلي، عام أو محمل، **وفترة نبض القلب** **PFCP**، وإعدادات المهلة وإعادة المحاولة، و**عناوين dataplane** N3/N9. يظهر تبديل **JSON** الوثيقة الكاملة للتكوين **الخام**. هنا تؤكد أن UPF للدعم وعنوانه كما هو متوقع تم تحديده.

التشخيصات

ping من عقدة UPF تشغل ping إلى مضيف مستهدف. أدخل هدفًا وعدد الحزم، وستعود نتائج لديه إمكانية الوصول إلى شبكة UPF الخام مع حكم النجاح/الفشل. إنها طريقة سريعة لتأكيد أن البيانات (على سبيل المثال إلى خادم DNS أو بوابة علوية) من حيث مغادرة الحزم فعليًا، دون الحاجة إلى الدخول إلى العقدة.

الحديقة ��لمسورة

إن **الحديقة المسورة**: توجيه مقيد للجلسات التي يجب أن تصل فقط إلى بوابة أسرية قبل أن لجلسة، فإنها تعيد كتابة SEID يتم مصادقتها أو منحها الحق. عندما تقوم بتفعيل إعادة توجيه على **البوابة** بدلاً من الإنترنت المفتوح. **IP /** الهابطة بحيث يذهب الجهاز إلى **رابط إعادة التوجيه** IP gNB، البوابة، رابط إعادة التوجيه IP، UE تسرد علامة التبويب كل **إعادة توجيه نشطة** مع المعنية. لإطلاق الجلسة إلى التوجيه العادي، قم بإزالة إعادة التوجيه. قائمة **المسموح بها** TEIDsو تسمي الوجهات التي لا تزال يُسمح لجلسة الحديقة المسورة بالوصول إليها CIDRs أو IPs من مباشرة (على سبيل المثال البوابة وأصولها). يمكنك أيضًا تفعيل وإزالة إعادة التوجيه لكل جلسة من صفحة تفاصيل الجلسة.

السجلات

لاستكشاف الأخطاء وإصلاحها في مثيل واحد UPF تتبع علامة **السجلات** مخرجات السجل الحية لـ OmniWeb دون مغادرة.

لوحات المعلومات للمراقبة

يتم تقديم الإنتاجية، ومعدلات الحزم لكل واجهة، واتجاهات عدد الجلسات وغيرها من السلاسل الزمنية لـ UPF يمكن الوصول إليها من صفحة العنصر. لا تقوم Grafana، كلوحات معلومات OmniWeb بتكرار تلك المخططات بشكل أصلي.

ذات صلة

- **SGW-C**: نظير التحكم في EPC الذي يبرمج هذا UPF (كـ SGW-U) عبر **Sxa/PFCP** ويوجه الحركة على **S1-U / N3**.
- **PGW-C / SMF**: يثبت اتصال PDN، وكما هو SMF، 5 يبرمج مستوى المستخدم عبر G **N4/PFCP**.
- **MME**: يدير إعداد الحامل الذي يقوم في النهاية بتثبيت الجلسات التي تُرى هنا.

- **SCEF**: يحمل حمولات صغيرة غير IP عبر مستوى التحكم، ويتجاوز عمدًا هذا مستوى المستخدم.
- العودة إلى فهرس العنصر: دليل العمليات.