OmniSEPP مرجع تكوين

نظرة عامة | دليل العمليات | المقاييس والمراقبة | استكشاف الأخطاء وإصلاحها

تعيش جميع تكوينات OmniSEPP تحت مفتاح التطبيق `:omnisepp`. يمكن تجاوز مجموعة فرعية من المفاتيح بواسطة متغيرات البيئة، ولكن هذا يسري فقط في **تكوين وقت التشغيل الإنتاجي**. الخرائط المتداخلة (`roaming_partners`، `topology_hiding_map`) وعدد قليل من المفاتيح الأخرى ليس لديها متغير بيئة ويتم تعيينها من خلال ملف تكوين التطبيق فقط.

هيكل التكوين

```
config :omnisepp,
  # هوية مستمع SBI/N32 (إلى المعلن NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.22",
  sbi_port: 7777,

  # مواد TLS لمستمع N32 (تستخدم فقط عندما يكون sbi_scheme "https")
  sbi_certfile: nil,
  sbi_keyfile: nil,
  sbi_cacertfile: nil,

  # تسجيل NRF
  nrf_uri: "http://127.0.0.10:7777",
  heartbeat_interval: 10_000,

  # PLMN (تجاوز لكل نشر) المقدم
  mcc: "999",
  mnc: "70",

  # هوية SEPP الخاصة وقدراتها المتفاوض عليها
  sepp_fqdn: "sepp.5gc.mnc70.mcc999.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],

  # استمرارية سياق ارتباط N32 (ملف التكوين فقط)
  n32_context_path: "<priv>/data/n32_context.dets",

  # (ملف التكوين فقط) التجوال وإخفاء الطوبولوجيا
  roaming_partners: %{},
  topology_hiding_map: %{}
```

كل معلمة أعلاه موثقة أدناه.

المعلمات الأساسية

المعلمة	النوع	مطلوب	الافتراضي
`sbi_scheme`	سلسلة	لا	`http`
`sbi_addr`	سلسلة	لا	`127.0.0.22`
`sbi_port`	عدد صحيح	لا	`7777`
`sbi_certfile`	سلسلة (مسار)	مشروط	(لا شيء)

المعلمة	النوع	مطلوب	الافتراضي
`sbi_keyfile`	سلسلة (مسار)	مشروط	(لا شيء)
`sbi_cacertfile`	سلسلة (مسار)	لا	(لا شيء)
`nrf_uri`	سلسلة	لا	`http://127.0.0.10:777`
`mcc`	سلسلة	لا	`999`

المعلمة	النوع	مطلوب	الافتراضي
`mnc`	سلسلة	لا	`70`
`heartbeat_interval`	عدد صحيح (مللي ثانية)	لا	`10000`
`sepp_fqdn`	سلسلة	لا	مشتقة (انظر أدناه)
`supported_sec_capabilities`	قائمة من السلاسل	لا	`["TLS"]`
`n32_context_path`	سلسلة (مسار)	لا	مشتقة (انظر أدناه)

المعلمة	النوع	مطلوب	الافتراضي
`roaming_partners`	خريطة	لا	`%{}`
`topology_hiding_map`	خريطة	لا	`%{}`

sepp_fqdn

يتم اشتقاقه من `sepp_fqdn`، عندما لا يتم تعيين PLMN المقدم كالتالي:

```
sepp.5gc.mnc<mnc>.mcc<mcc>.3gppnetwork.org
```

بالنسبة لـ PLMN الافتراضي `70-999`، ينتج عن ذلك `sepp.5gc.mnc70.mcc999.3gppnetwork.org`. يتم إرسال هذا FQDN كهوية `sender` في طلبات واستجابات مصافحة N32-c (TS 29.573). تجاوزها بشكل صريح عندما لا يتطابق الشكل المشتق مع FQDN الذي يتوقعه شركاؤك المتجولون.

TLS مستمع N32

بنفسه بدلاً من الاعتماد على مُنهي TLS N32 ينهي مستمع، `https` هو `sbi_scheme` عندما يكون الواجهة SEPPs حيث يحمي اثنان من، (TS 33.501 §13.1) TLS N32-f خارجي. هذا هو وضع باست��دام TLS بينهما.

- `sbi_scheme` هو `https` مطلوبان **كلاهما** عندما يكون `sbi_keyfile` و `sbi_certfile` البدء بدلاً من التراجع بصمت إلى النص SEPP إذا كان أي منهما مفقودًا، يرفض العادي.
- SEPP أيضًا، يتطلب المستمع ويحقق شهادة عميل `sbi_cacertfile` عندما يتم تعيين TLS يتم إنهاء، CA موثوق به متبادل. مع عدم تكوين TLS مما يوفر، CA النظير ضد تلك من جانب الخادم فقط.
- يتم تجاهل هذه المفاتيح ويقدم، (الافتراضي) `http` هو `sbi_scheme` عندما يكون المستمع النص العادي.

لذا فإنه يعكس الآن النقل الفعلي للمستمع، `sbi_scheme` يتبع المخطط المعلن في تسجيل NRF.

supported_sec_capabilities

بترتيب **تفضيل محلي** (الأكثر تفضيلًا أولاً). خلال، SEPP التي يدعمها هذا N32-f قدرات الأمان أول إدخال في هذه القائمة الذي يقدمه النظير أيضًا OmniSEPP تختار، N32-c مصافحة (TS 29.573 §5.2.3.2.2).

القيمة	المعنى	المرجع
`TLS`	حماية طبقة النقل بين SEPPs.	TS 33.501 §13.1
`PRINS`	الحماية مع إدراج الأمان الوسيط (حماية طبقة التطبيق JOSE عبر مركز تجوال).	TS 33.501 §13.2

؛ فقط هذان القيمتان معترف بهما؛ أي إدخال آخر يتم تجاهله. القيمة الافتراضية هي `["TLS"]` احتفظ بها عند `["TLS"]` لعملية تشغيل متوافقة.

قدم قائمة مفصولة بفواصل بترتيب، `SEPP_SEC_CAPABILITIES` عند التجاوز عبر متغير البيئة التفضيل، على سبيل المثال `TLS,PRINS`. يتم تقليم الفراغات حول كل إدخال.

استمرارية سياق N32

تستمر ارتباطات N32 التي تم إنشاؤها إلى ملف DETS في `n32_context_path`، بحيث تبقى عند بدء التشغيل، يعيد المتجر تحميل الارتباطات (TS 29.573). بعد إعادة تشغيل العملية أو العقدة المستمرة، بحيث لا يحتاج الشريك إلى إعادة تشغيل مصافحة N32-c بعد إعادة تشغيل OmniSEPP.

- تحت دليل `n32_context.dets` عندما لا يتم تعيينه، ي��ون المسار الافتراضي هو الخاص بتطبيق OTP. يتم إنشاء الدليل الأب عند بدء التشغيل إذا لم يكن `priv` بيانات موجودًا.
- إذا لم يكن بالإمكان فتح الملف (على سبيل المثال، في حالة الفساد)، يسجل المتجر تحذيرًا ويبدأ بجدول فارغ في الذاكرة بدلاً من تعطل التمهيد؛ ثم يتم إعادة إنشاء الارتباطات من خلال المصافحة.
- هذه المفتاح ليس لديها متغير بيئة ويتم تعيينها من خلال ملف تكوين التطبيق فقط.

الشركاء المتجولون

خريطة `roaming_partners` هي القائمة الثابتة المسموح بها لشركاء المتجولين. يتم PLMN الشريك في شكل `"mcc-mnc"`، وكل قيمة هي مواصفة شريك. تعيينها بواسطة معرف PLMN.

```
config :omnisepp,
  roaming_partners: %{
    "001-01" => %{
      sepp_uri: "https://sepp.partner-a.example:7777",
      sec_capabilities: ["TLS"]
    },
    "310-260" => %{
      sepp_uri: "https://sepp.partner-b.example:7777"
    }
  }
```

الهيكل العلوي:

شكل المفتاح	النوع	الوصف
`"mcc-mnc"`	سلسلة (مفتاح الخريطة)	معرف PLMN الشريك، على سبيل المثال `01-001""`.
القيمة	خريطة	مواصفة الشريك (انظر أدناه).

مواصفة الشريك:

المعلمة	النوع	مطلوب	الافتراضي	
`sepp_uri`	سلسلة	نعم	-	ذر كة
`sec_capabilities`	قائمة من السلاسل	لا	ترث `supported_sec_capabilities`	ان رث يك su ة بـ

الفارغة (القيمة الافتراضية) إلى عدم تكوين أي شركاء `roaming_partners` تشير خريطة غير المعروفة. هذه الخريطة ليس لديها متغير بيئة PLMNs جميع N32-f متجولين، ويرفض توجيه ويتم تعيينها من خلال ملف تكوين التطبيق فقط.

خريطة إخفاء الطوبولوجيا

لإخفاء الطوبو��وجيا FQDN بتنفيذ إعادة كتابة `topology_hiding_map` تقوم خريطة (TS 33.501 §13.2). تقوم بربط كل FQDN NF داخلي بـ FQDN الخارجي المقدم لشركاء التجوال.

```
config :omnisepp,
  topology_hiding_map: %{
    "amf1.5gc.mnc070.mcc999.3gppnetwork.org" =>
      "sepp.5gc.mnc070.mcc999.3gppnetwork.org",
    "udm1.5gc.mnc070.mcc999.3gppnetwork.org" =>
      "sepp.5gc.mnc070.mcc999.3gppnetwork.org"
  }
```

شكل المفتاح	النوع	الوصف
`internal_fqdn`	سلسلة (مفتاح الخريطة)	FQDN NF الداخلي الذي سيتم إخفاؤه، على سبيل المثال FQDN AMF أو UDM.
`external_fqdn`	سلسلة (القيمة)	FQDN الخارجي المقدم للشركاء بدلاً منه.

`gpp-Sbi-Target-apiRoot` يتم تطبيق الربط في الاتجاه الخارجي (من الداخلي إلى الخارجي) على قيم `3` ويتم عكسه في الاتجاه الداخلي (من الخارجي إلى `producer-id`، و`Location` و`apiRoot` الداخلي الحقيقي. FQDN المقدمة من الشركاء مرة أخرى إلى apiRoots الداخلي) بحيث يتم حل تعني الخريطة الفارغة (القيمة الافتراضية) عدم وجود إعادة كتابة. هذه الخ��يطة ليس لديها متغير بيئة ويتم تعيينها من خلال ملف تكوين التطبيق فقط.

ملخص متغير البيئة

تطبق متغيرات البيئة فقط في تكوين وقت التشغيل الإنتاجي. المفاتيح غير المدرجة هنا هي فقط لملف التكوين.

متغير البيئة	المعلمة	الملاحظات
`SEPP_SBI_SCHEME`	`sbi_scheme`	`http` أو `https`.
`SEPP_SBI_ADDR`	`sbi_addr`	
`SEPP_SBI_PORT`	`sbi_port`	يتم تحليله كعدد صحيح.
`SEPP_SBI_CERTFILE`	`sbi_certfile`	مطلوب عندما يكون المخطط هو `https`.
`SEPP_SBI_KEYFILE`	`sbi_keyfile`	مطلوب عندما يكون المخطط هو `https`.
`SEPP_SBI_CACERTFILE`	`sbi_cacertfile`	يتم تعيينه لتمكين TLS المتبادل (تحقق من N32-f شهادة العميل النظير).
`SEPP_NRF_URI`	`nrf_uri`	
`SEPP_MCC`	`mcc`	
`SEPP_MNC`	`mnc`	
`SEPP_FQDN`	`sepp_fqdn`	عند عدم تعيينه، يتم اشتقاق FQDN من PLMN.
`SEPP_SEC_CAPABILITIES`	`supported_sec_capabilities`	مفصولة بفواصل، ترتيب التفضيل.

مثال على التكوين

نشر لـ PLMN `260-310` منزلي مع شريك متجول واحد تجاوز واقعي لك:

```
config :omnisepp,
  sbi_scheme: "https",
  sbi_addr: "10.20.0.5",
  sbi_port: 7777,
  sbi_certfile: "/etc/omnisepp/tls/sepp.crt",
  sbi_keyfile: "/etc/omnisepp/tls/sepp.key",
  sbi_cacertfile: "/etc/omnisepp/tls/partner-ca.crt",
  nrf_uri: "http://10.20.0.1:7777",
  heartbeat_interval: 10_000,
  mcc: "310",
  mnc: "260",
  sepp_fqdn: "sepp.5gc.mnc260.mcc310.3gppnetwork.org",
  supported_sec_capabilities: ["TLS"],
  roaming_partners: %{
    "001-01" => %{
      sepp_uri: "https://sepp.partner-a.example:7777",
      sec_capabilities: ["TLS"]
    }
  },
  topology_hiding_map: %{
    "amf1.5gc.mnc260.mcc310.3gppnetwork.org" =>
      "sepp.5gc.mnc260.mcc310.3gppnetwork.org"
  }
```

كيف يعمل: يعلن OmniSEPP عن نفسه إلى NRF كنوع NF `SEPP` لـ `10.20.0.5:7777` عند `https`، ينهي `sbi_scheme` هو مع نبض القلب كل 10 ثوانٍ. نظرًا لأن PLMN `310-260`، ونظرًا لأن `sbi_cacertfile` تم تعيينه، `sepp.key` / `sepp.crt` باستخدام N32 TLS مستمع (متبادل TLS). يقبل `partner-ca.crt` الشريك ضد SEPP فإنه يتطلب ويحقق شهادة عميل مصافحات N32-c كـ `sepp.5gc.mnc260.mcc310.3gppnetwork.org`، م��فاوضًا على الوحيدة، وعند بدء التشغيل يبدأ المصافحة الصادرة نحو الشريك `01-001`. يتم N32-f كقدرة TLS توجيه حركة N32-f فقط إلى ومن الشريك PLMN `001-01`، ويتم إخفاء FQDN AMF الداخلي خلف FQDN SEPP تجاه ذلك الشريك.

قياسات ومراقبة OmniSEPP

نظرة عامة | دليل العمليات | مرجع التكوين | استكشاف الأخطاء وإصلاحها

القابلية للرصد

تُوفر القابلية للرصد من خلال **سجلات التطبيقات المنظمة** وتسجيل الطلبات القياسي. يقوم المشغلون بمراقبة OmniSEPP من خلال سجلاته، التي تلتقط أحداث المصافحة، وإعادة التوجيه، والطلبات الموصوفة أدناه.

ما يجب مراقبته في السجلات

تعتبر سجلات التطبيق هي الإشارة الأساسية لتشغيل OmniSEPP. الفئات التالية من الأحداث تُسجل وتستحق المراقبة.

نتائج مصافحة N32-c

تسجل كل مفاوضة قدرة SEPP البعيدة والقدرة الأمنية N32-f المختارة، بما في ذلك هوية النظير. راقب هذه لتأكيد أن المصافحة تنجح:

- الشركاء المتوقعون في التجوال يكملون المصافحة.
- القدرة المختارة تتطابق مع نيتك (على سبيل المثال `TLS`).
- لم يتم رفض شريك لأنه لم يتم اختيار أي قدرة مشتركة.

يتم تسجيل نظير يختار قدرة لم تعرضها هذه SEPP (على مسار المُبادر) ويتم رفضه كتحذير.

قرارات وإخفاقات إعادة توجيه N32-f

تسجل N32-f قراراتها وإخفاقاتها، بما في ذلك إعادة توجيه:

- الرفض لإعادة التوجيه إلى PLMN ليس شريك تجوال مُكون. تشير الزيادة في معدل هذه إلى وجود إدخال مفقود أو مُكون بشكل خاطئ لـ `roaming_partners`.

- أهداف إعادة التوجيه الواردة والصادرة (عنوان URL والاتجاه المحلول).
- إخفاقات التوجيه، التي تظهر للشريك كـ `502` وتشير `TARGET_NF_NOT_REACHABLE` إلى أن NF الداخلي المعنون لم يكن قابلاً للوصول.

تسجيل الطلبات

يتم التعامل معه بواسطة المستمع، بما في ذلك SBI يغطي تسجيل الطلبات القياسي كل طلب الشاملة. استخدمه لمراقبة حجم الطلبات، والأساليب، N32-f نقاط نهاية المصافحة وإعادة توجيه والمسارات، و لربط نشاط الشريك بأحداث المصافحة وإعادة التوجيه.

فحص الصحة

يتم تقييم الصحة من خلال الجمع بين:

- **الحيوية:** `GET /n32c-handshake/v1/status` `200` تُرجع `{"status":"UP"}` عندما يكون مستمع SBI قيد التشغيل. انظر دليل العمليات.
- **تسجيل NRF:** تأكد من أن OmniSEPP يظهر في NRF كحالة NF `SEPP` ويقوم بإرسال نبضات. يتم وصف سلوك التسجيل في دليل العمليات.
- **إشارات السجل:** أحداث المصافحة وإعادة التوجيه الموضحة أعلاه.

دليل عمليات OmniSEPP

نظرة عامة | مرجع التكوين | المقاييس والمراقبة | استكشاف الأخطاء وإصلاحها

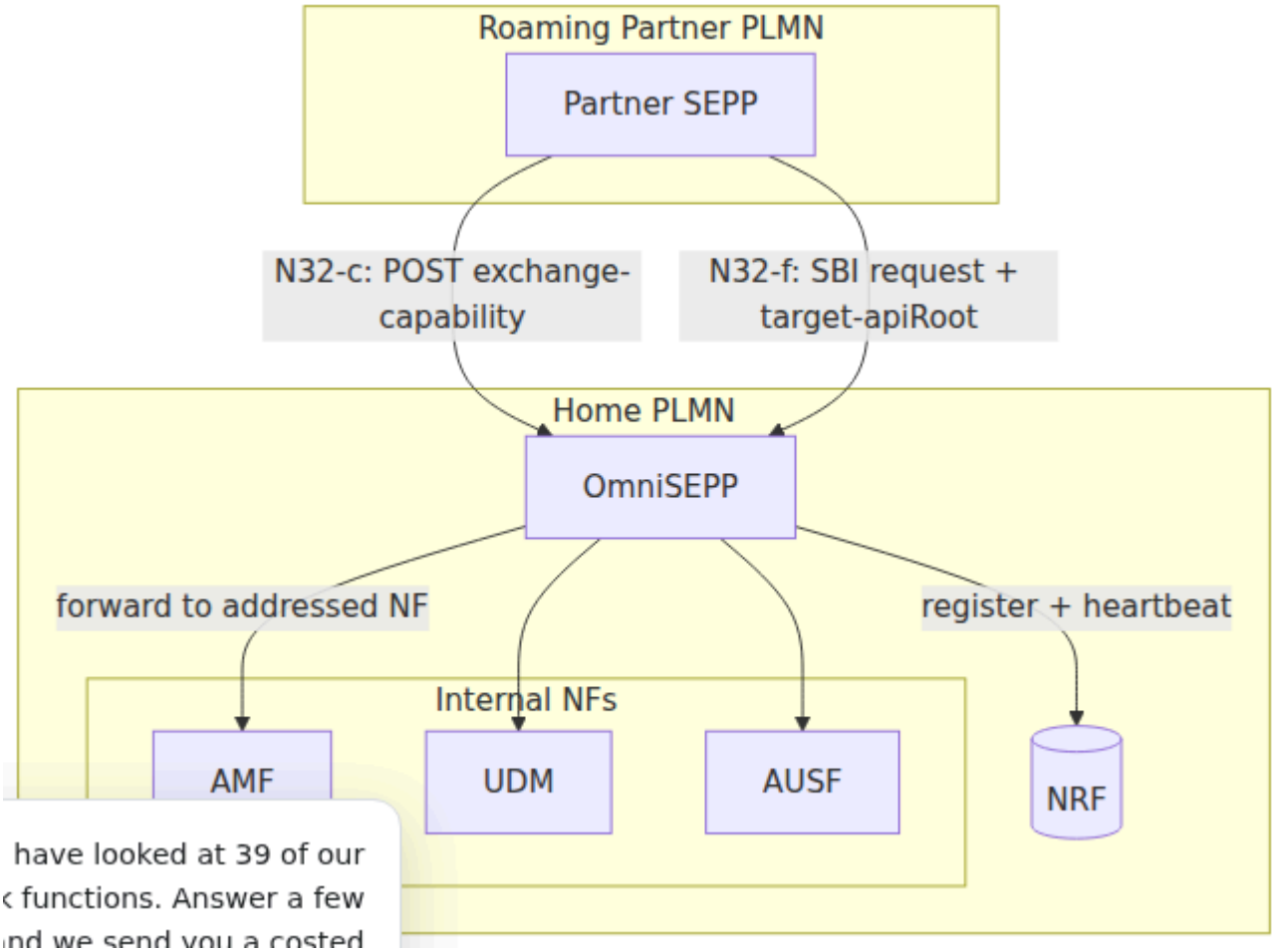
يصف هذا الدليل كيفية تصرف OmniSEPP على واجهة N32 بين PLMN وكيفية تشغيله. OmniSEPP هو وكيل حماية الحافة الأمنية المحدد في 3GPP TS 23.501 §6.2.17، مع سلوك أمني من 3GPP TS 33.501 وواجهة N32 من 3GPP TS 29.573.

جدول المحتويات

- نظرة عامة على العمارة
- واجهة N32
- دورة حياة ارتباط N32
- التفاوض على القدرات
- تحكم شريك التجوال
- إخفاء الطوبولوجيا
- تدفقات الرسائل
- نقاط نهاية SBI
- تسجيل NRF
- ملاحظات تشغيلية

نظرة عامة على العمارة

يقوم OmniSEPP بإنهاء واجهة N32 تجاه SEPPs شريك التجوال وينقل الحركة إلى وظائف NF المحلي كنوع `SEPP` بحيث يمكن المنزلية. يسجل مع NRF الشبكة الداخلية في PLMN النظير البعيد وخريطة إخفاء الطوبولوجيا هما تكوين SEPP اكتشافه؛ SCP للمستهلكين المحليين و SEPPs النظير عبر NRF (لا يتم اكتشاف ثابت حسب اتفاقية التجوال).



واجهة N32

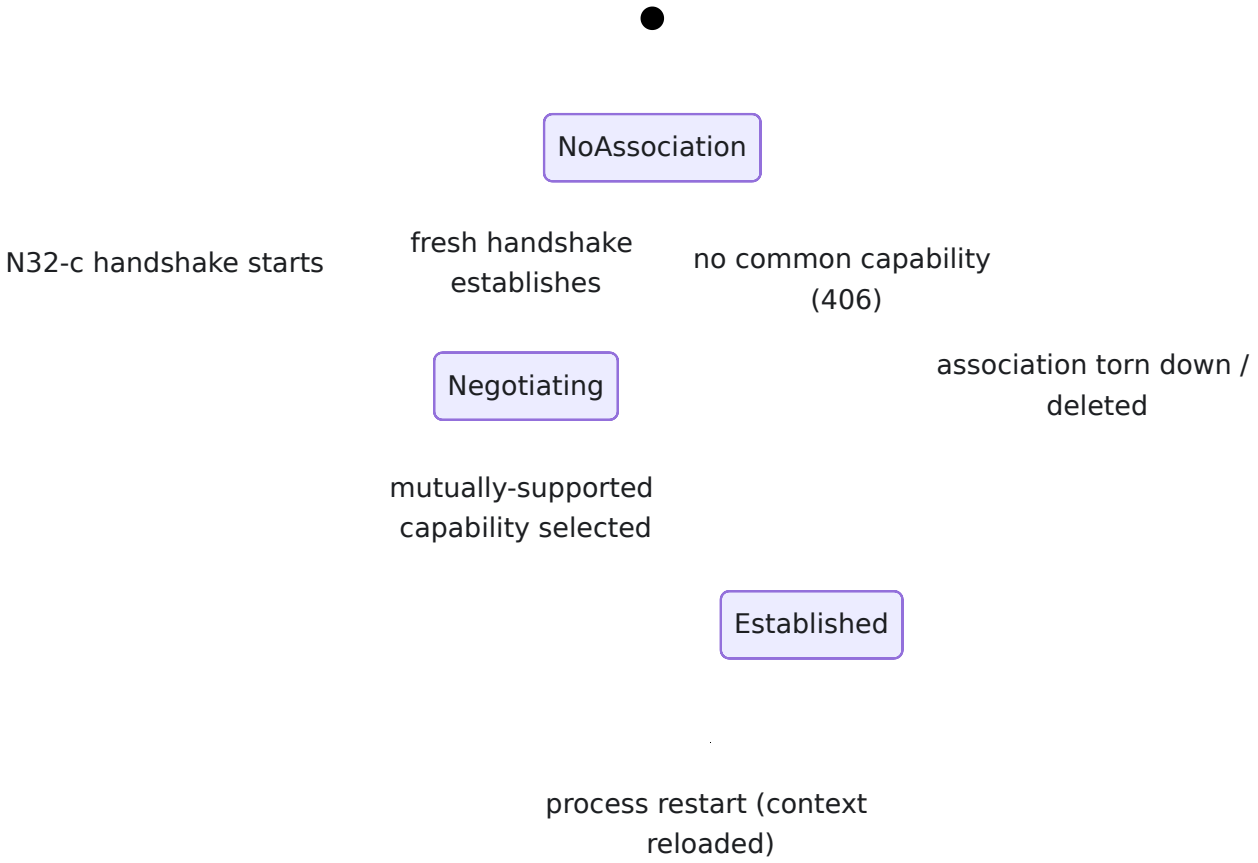
تحتوي N32 على قناتين منطقيتين (TS 29.573):

- **N32-c (قناة التحكم)** - المصافحة المستخدمة للتفاوض على قدرة الأمان N32-f وتأسيس الارتباط بين SEPPs. يقوم OmniSEPP بتعريض هذا كـ `/n32c-handshake/v1/exchange-capability` ويبدأ أيضًا نقطة نهاية (دور المستجيب) المصافحة تجاه كل شريك تجوال مُكون عند بدء التشغيل (دور المُبادر).
- **N32-f (قناة التوجيه)** - تبادل مستمر لرسائل قائمة على الخدمة (SBI) بين PLMNs. يقوم OmniSEPP **وضع** بنقل هذه في **TLS**: يتم توجيه الرسالة بشكل كبير وإخفاء الطوبولوجيا hop-by-hop كما هي، مع تطبيق نظافة رأس.

دورة حياة ارتباط N32

تسجل كل مفاوضة N32-c ناجحة ارتباطًا في **متجر سياق دائم** (جدول DETS مدعوم بذاكرة البعيد. يتضمن السياق المخزن قدرة الأمان FQDN SEPP مفاتيحها بواسطة، (مؤقتة في الذاكرة

N32-f المختارة وقائمة هوية PLMN الشريك.



الخصائص التشغيلية الرئيسية:

- `n32_context_path` في DETS المتجر هو **دائم**: يتم كتابة الارتباطات إلى ملف وإعادة تحميلها عند بدء التشغيل، بحيث تبقى قائمة بعد إعادة تشغيل العملية أو العقدة. لا يتعين على الشريك إعادة المصافحة بعد إعادة تشغيل OmniSEPP.
- **TTL**: لا يوجد. يستمر الارتباط حتى يتم تفكيكه (حذفه) صراحة أو استبداله بمفاوضة جديدة.
- يبدأ المتجر، (على سبيل المثال، بسبب الفساد) DETS إذا لم يكن من الممكن فتح ملف فارغًا ويسجل تحذيرًا؛ ثم يتم إعادة إنشاء الارتباطات بواسطة المصافحة.

التفاوض على القدرات

خلال مصافحة N32-c، يتفق SEPPs مان�� على قدرة N32-f واحدة. القدرات الصالحة هي `TLS` و `PRINS` (TS 33.501 §13.1).

بتمرير OmniSEPP هي **الأولوية المحلية أولاً**: يقوم (TS 29.573 §5.2.3.2.2) قاعدة الاختيار الخاصة به بالترتيب ويختار أول إدخال يقدمه الشريك `supported_sec_capabilities` قائمة

أيضًا. إذا كانت مجموعتا القدرات غير متقاطعتين، تفشل المفاوضة مع `INSUFFICIENT_RESOURCES` (HTTP 406) ولا يتم تسجيل أي ارتباط.

يتم الإعلان عنها. احتفظ بـ (`PRINS`، `TLS`) فقط القدرات المعترف بها والمشكلة بشكل صحيح لتشغيل متوافق. راجع مرجع التكوين لمعرفة `["TLS"]` عند `supported_sec_capabilities` كيفية تعيين ترتيب التفضيل.

تحكم شريك التجوال

سجل PLMN الشريك (`"mcc-mnc"`). إنه **شريك التجوال** هو قائمة سماح ثابتة مفاتيحها بواسطة يحكم توجيه N32-f:

- يتم نقل الحركة فقط بين PLMNs الموجودة في السجل.
- يرفض جميع N32-f يعني سجل فارغ (الإعداد الافتراضي) أن توجيه PLMNs غير المعروفة.
- يحمل كل إدخال شريك جذر API SEPP للشريك، ويفضل، قدرات الأمان N32-f المسموح بها مع ذلك الشريك. عند حذف قائمة القدرات، يرث الشريك `supported_sec_capabilities` لهذا SEPP.

راجع مرجع التكوين - شركاء التجوال لمعرفة هيكل الخريطة.

إخفاء الطوبولوجيا

يخفي إخفاء الطوبولوجيا (TS 33.501 §13.2) هويات NF الداخلية من شركاء التجوال عن طريق إعادة كتابة FQDNs. يقوم OmniSEPP بتطبيق خريطة مكونة بواسطة المشغل من `internal_fqdn => external_fqdn`:

- **خارجية** (نحو شريك): يتم إعادة كتابة FQDNs `3gpp-Sbi-Target-apiRoot` و `Location` و `producer-id` الداخلية في قيم رؤوس إلى نظيراتها الخارجية.
- **داخلية** (من شريك): يتم تطبيق خريطة عكسية بحيث يتم حل apiRoot المعروض الداخلي NF الداخلي الحقيقي قبل توجيه الطلب إلى FQDN خارجيًا مرة أخرى إلى.

رموز تتم إعادة الكتابة مرت**FQDN** **كاملة**: يتم إعادة كتابة FQDN المapped فقط طة بـ `/` و `:` و `@` أو نهاية القيمة URL محدود بواسطة محددات) عندما يظهر كـ مضيف كامل، (مثل وليس كجزء فرعي من اسم مضيف أطول. يمنع هذا التعيين من إفساد مضيف غير ذي صلة يحتوي فقط على الاسم المmapped، ويوقف قيمة واحدة من إعادة المطابقة بواسطة إدخال تعيين آخر.

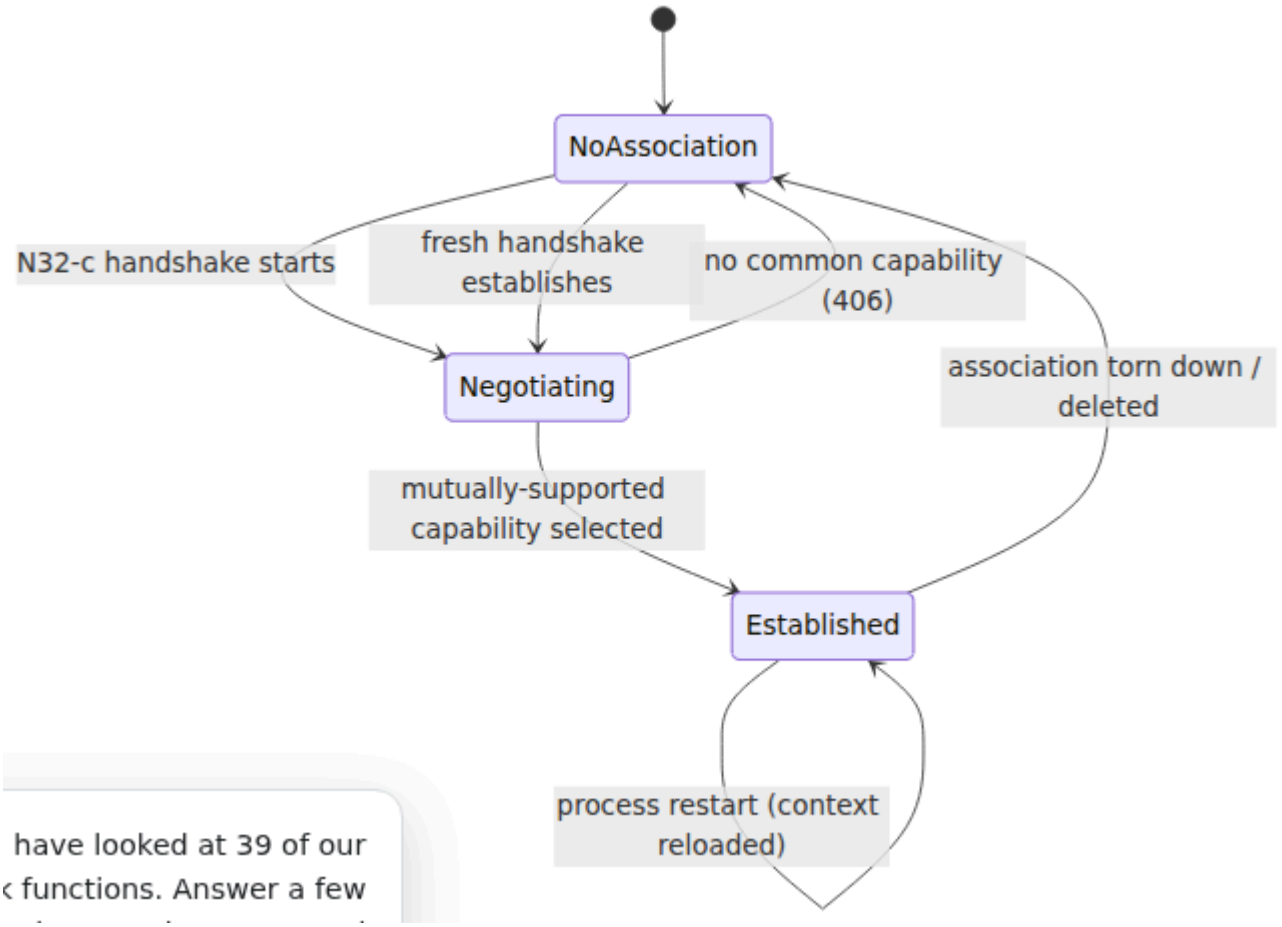
في كل نقل، يتم إزالة رؤوس hop-by-hop (`host` و `content-length` و `connection`). في المسار الداخلي، يتم أيضًا إسقاط رأس `3gpp-Sbi-Target-apiRoot` (الذي تم استهلاكه الآن) قبل أن يصل الطلب إلى NF الداخلي.

يعني خريطة إخفاء الطوبولوجيا فارغة (الإعداد الافتراضي) أنه لا يتم إجراء أي إعادة كتابة. راجع مرجع التكوين - خريطة إخفاء الطوبولوجيا.

تدفقات الرسائل

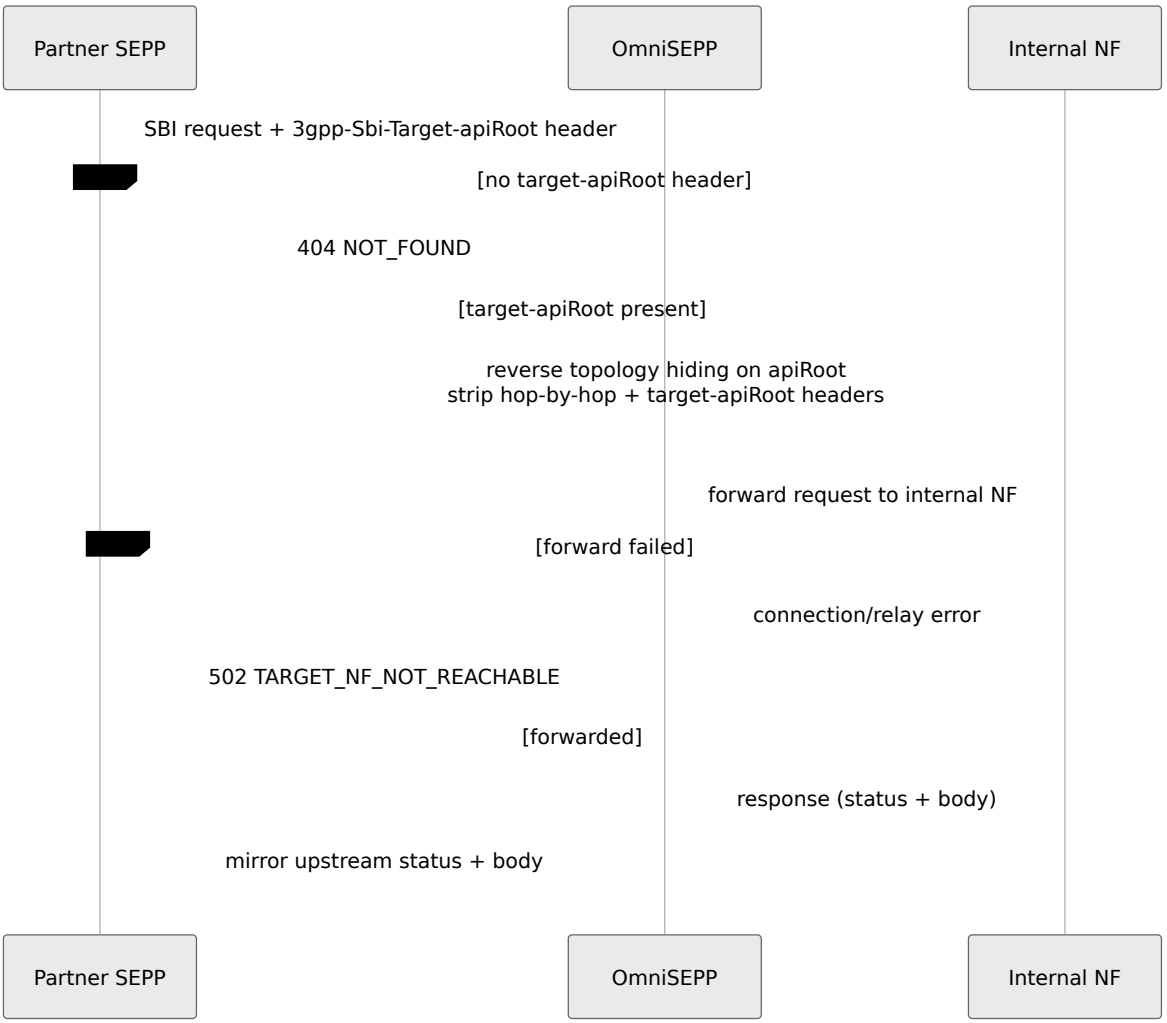
مصافحة N32-c (المستجيب)

يبدأ SEPP شريك التجوال المصافحة عن طريق إرسال طلب تفاوض على القدرة. يقوم OmniSEPP باختيار قدرة مدعومة بشكل متبادل، وتسجيل الارتباط، والرد.



توجيه N32-f الداخلي

يرسل SEPP الشريك طلب SBI يحمل رأس `3gpp-Sbi-Target-apiRoot` الذي يحدد NF الوجهة. يقوم OmniSEPP الداخلي بعكس إخفاء الطوبولوجيا، ويزيل رؤوس hop-by-hop ورؤوس التوجيه، وينقل الطلب، معكوسًا استجابة التيار العلوي.



نقاط نهاية SBI

يعرض OmniSEPP ما يلي عبر مستمع SBI HTTP الخاص به. تعلن مصافحة N32-c عن خدمة واحدة NRF، `n32c-handshake` الإصدار `v1`.

الطريقة	المسار	الغرض
POST	`/n32c-handshake/v1/exchange-capability`	التفاوض على قدرة الأمان N32-c (المستجيب).
GET	`/n32c-handshake/v1/status`	اختبار الحضور.
(أي)	أي مسار آخر	يتم توجيهه خارجيًا إلى N32-f. توجيه شريك التجوال عندما يسمي SEPP الطلب PLMN شريك، وإلا يتم توجيهه الداخلي المسمى بواسطة NF داخليًا إلى `3gpp-Sbi-Target-apiRoot`.

POST /n32c-handshake/v1/exchange-capability

يتفاوض على قدرة الأمان N32-f مع SEPP شريك مُبادر.

الحالة	السبب	الشرط
200	-	نجحت المفاوضة. تحتوي الاستجابة على `sender` و `selectedSecCapability`.
400	`MANDATORY_IE_MISSING`	الطلب مفقود `sender`، أو `supportedSecCapabilityList` غائبة أو فارغة.
406	`INSUFFICIENT_RESOURCES`	لا توجد قدرة أمان N32-f مدعومة بشكل متبادل.

GET /n32c-handshake/v1/status

مناسب كاختبار حضور. يعيد `200` مع الجسم `{"status":"UP"}`.

توجيه N32-f (catch-all)

يتم توجيه N32-f. يتم التعامل مع أي طلب ليس أحد نقاط نهاية المصافحة كحركة مرور توجيه الشريك كاختيار خروج له، وإلا PLMN عندما يسمي (شريك التجوال SEPP إلى) الطلب **خارجيًا** (إلى NF `3` الداخلي المسمى بواسطة `gpp-Sbi-Target-apiRoot`) **داخليًا**.

الحالة	السبب	الشرط
(معكوس)	-	يتم عكس حالة الجسم والتيار العلوي عند النجاح (داخلي أو خارجي).
404	`NOT_FOUND`	`3` رأس `gpp-Sbi-Target-apiRoot` داخلي: غائب، لذا لا يوجد هدف توجيه.
403	`TARGET_PLMN_NOT_A_PARTNER`	خارجي: PLMN الهدف المسمى ليس شريك تجوال مُكون.
502	`TARGET_NF_NOT_REACHABLE`	فشل التوجيه إلى NF (داخلي) الداخلي أو SEPP (خارجي) الشريك.

تسجيل NRF

عند البدء، يسجل OmniSEPP مع NRF كنوع NF `SEPP` (TS 23.501 §6.2.17) ويقوم بإرسال نبضات قلب على الفاصل الزمني المكون. تعلن التسجيل عن عنوان SBI، والمخطط، والمنفذ، وخدمة PLMN المخدوم، `n32c-handshake` `v1` الوحيدة.

يسمح التسجيل مع NRF و SCP المحلي للمستهلكين المحليين باكتشاف هذا SEPP (TS 29.573 cl 4.2.1). يتم حل SEPP حسب الثابت `roaming_partners` النظير **البعيد**، بالمقابل، من تكوين SEPP في حيث لا يمكن لـ PLMN، اتفاقية التجوال: هذا هو النموذج المقصود لحل الأقران بين PLMN آخر. إخفاء الطوبولوجيا هو أيضًا تكوين ثابت NRF PLMN في SEPP واحد البحث عن PLMN.

تتم توثيق معلمات التسجيل ونبض القلب في مرجع التكوين.

المصافحة الخارجية عند بدء التشغيل

المُبادر بالإضافة إلى المستجيب. عند التمهيد، بمجرد أن يصبح **SEPP** كـ OmniSEPP يعم�ي تجاه كل شريك تجوال مُكون N32-c متجر السياق جاهزًا، يبدأ مفاوضة قدرة (`roaming_partners`) لديه `sepp_uri` (TS 29.573 §5.2.3.2). يتم: **أفضل جهد** هذا هو تسجيل الشريك غير القابل للوصول أو الرافض وتخطيه بدلاً من تعطل بدء التشغيل، وتعمل المهمة مرة واحدة دون إعادة تشغيل. يمكن للشريك الذي كان غير قابل للوصول عند التمهيد أن يؤسس الارتباط لاحقًا عن طريق إرسال مصافحة (جانب المستجيب) الخاصة به، أو في إعادة التشغيل التالية.

ملاحظات تشغيلية

- **سلوك إعادة التشغيل:** متجر ارتباط N32 دائم (مدعوم من DETS). يتم إعادة تحميل الارتباطات عند إعادة التشغيل، لذا لا يتعين على الشركاء إعادة تشغيل مصافحة N32-c لاستئناف النقل.
- **PLMNs غير المعروفة:** مع سجل شريك التجوال الفارغ، يرفض توجيه N32-f PLMNs غير المعروفة. قم بملء السجل قبل توقع نقل حركة الشركاء.
- **إنهاء TLS:** عندما يكون `sbi_scheme` هو `https`، يقوم مستمع N32 بإنهاء TLS المتبادل (شهادة العميل) بنفسه باستخدام الشهادة والمفتاح المكونين، ويطبق CA. راجع مرجع التكوين - TLS مستمع N32.
- **PLMN الافتراضي:** PLMN هو قيمة اختبار (`70-999`) المخدوم الافتراضي المرفق ويجب تجاوزها حسب النشر.
- **الرؤية:** العمل ضد سجلات التطبيق الهيكلية؛ راجع المقاييس والمراقبة.

استكشاف أخطاء OmniSEPP وإصلاحها

نظرة عامة | دليل العمليات | مرجع التكوين | المقاييس والمراقبة

يغطي هذا الدليل المشكلات التشغيلية الشائعة وحلولها. يعتمد التشخيص على السجلات المنظمة؛ انظر المقاييس والمراقبة.

المشكلات الشائعة

تم رفض مصافحة N32-c مع 400

الأعراض: يتم الرد على طلب التفاوض على القدرة من شريك SEPP بـ `400` `MANDATORY_IE_MISSING`.

الأسباب المحتملة:

- الطلب يفتقر إلى هوية `sender`.
- قائمة `supportedSecCapabilityList` غائبة أو فارغة.

الحل:

1. تأكد من أن الشريك يرسل `SecNegotiateReqData` بشكل صحيح مع `sender` غير فارغ.
2. تأكد من أن الشريك يتضمن على الأقل قدرة أمان و��حدة من N32-f في `supportedSecCapabilityList`.

تم رفض مصافحة N32-c مع 406

الأعراض: يتم الرد على مصافحة الشريك بـ `406` ولا يتم تسجيل `INSUFFICIENT_RESOURCES` أي ارتباط.

الأسباب المحتملة:

- لا توجد قدرة مشتركة بين `supported_sec_capabilities` الخاصة بهذا SEPP وقائمة الشريك المعروضة. على سبيل المثال، الشريك يعرض فقط `PRINS` بينما هذا SEPP يعرض فقط `TLS`.

الحل:

1. قارن قدرات الشريك المعروضة مع قدرات هذا SEPP `supported_sec_capabilities`.
2. تأكد من أن كلا الجانبين يشتركان في قدرة واحدة على الأقل. في الممارسة العملية، `supported_sec_capabilities` ؛ احتفظ بـ `TLS` يعني هذا أن كلاهما يجب أن يدعم `["TLS"]` عند للتشغيل القابل للتشغيل البيني.

تم رفض حركة مرور N32-f لـ PLMN

الأعراض: تم رفض إعادة توجيه N32-f، وتظهر السجلات رفضًا لإعادة التوجيه إلى PLMN غير الشريك.

الأسباب المحتملة:

- الشريك غير موجود في سجل PLMN `roaming_partners`.
- السجل فارغ (الإعداد الافتراضي)، لذا يتم رفض جميع PLMNs غير المعروفة.

الحل:

1. أضف الشريك إلى PLMN `roaming_partners`، مع مفتاح `"mcc-mnc"`، مع `sepp_uri` لشريك SEPP.
2. تأكد من أن مفتاح PLMN يتطابق تمامًا مع `mcc-mnc` للشريك.

404 إعادة توجيه الوارد تعيد NOT_FOUND

الأعراض: يتم الرد على طلب الشريك بـ `404` `NOT_FOUND` بدلاً من إعادة توجيهه.

الأسباب المحتملة:

- الطلب لا يحمل رأس `3gpp-Sbi-Target-apiRoot`، لذا ليس لدى OmniSEPP هدف توجيه.

الحل:

1. تأكد من أن الشريك يحدد رأس `3gpp-Sbi-Target-apiRoot` الذي يحدد NF الداخلي.
2. إذا كان يتم استخدام إخفاء الطوبولوجيا، تأكد من أن apiRoot الخارجي الذي يقدمه الشريك لديه إدخال عكسي مطابق في `topology_hiding_map`.

502 إعادة توجيه الوارد تعيد TARGET_NF_NOT_REACHABLE

الأعراض: يتم الرد على طلب الشريك بـ `502` `TARGET_NF_NOT_REACHABLE`.

الأسباب المحتملة:

- NF الداخلي المعني متوقف أو غير قابل للوصول من OmniSEPP.
- apiRoot الخارجي إلى FQDN لم يحل إخفاء الطوبولوجيا داخلي قابل للوصول.

الحل:

1. تأكد من أن NF الداخلي الذي تم حله من apiRoot (المعكوس) يعمل ويمكن الوصول إليه.
2. تحقق من أن إدخال `topology_hiding_map` يربط FQDN الخارجي بـ FQDN الداخلي الصحيح والقابل للحل.

تختفي الارتباطات بعد إعادة التشغيل

الأعراض: بعد إعادة تشغيل OmniSEPP، يتم التعامل مع الشركاء الذين تم تأسيسهم سابقًا كما لو لم يكن هناك ارتباط، وتفشل إعادة توجيه N32-f أخرى لهم حتى يصافحوا مرة أخرى.

الأسباب المحتملة:

- لم يكن من الممكن فتح ملف DETS في `n32_context_path` (على سبيل المثال، بسبب الفساد أو مشكلة في الأذونات)، لذا بدأ المتجر فارغًا وسجل تحذيرًا.
- تغير `n32_context_path` المكون بين التشغيلين، لذا لا يتم قراءة الملف السابق.

الحل:

1. عادةً ما تكون الارتباطات دائمة وتُحمّل عند إعادة التشغيل، لذا يجب ألا تؤدي إعادة التشغيل وحدها إلى مسحها. إذا كانت مفقودة، تحقق من سجلات بدء التشغيل بحثًا عن تحذير N32Context حول فتح DETS.

2. تأكد من أن `n32_context_path` يشير إلى موقع مستقر وقابل للكتابة يتم الحفاظ عليه عبر إعادة التشغيل (ليس دليل مؤقت لكل تشغيل).

موثوق به بشكل متبادل TLS الشريك لا يمكنه إنشاء

الأعراض: يتوقع الشريك N32 عبر TLS موثوق به بشكل متبادل ولكن يتم رفض الاتصال، أو يكون HTTP عاديًا، أو لا يتم التحقق من شهادة عميل الشريك.

الأسباب المحتملة:

- `sbi_scheme` هو `http`، لذا يقوم المستمع بتقديم نص عادي.
- `sbi_scheme` هو `https` ولكن لم يتم تعيين `sbi_cacertfile`، لذا يتم إنهاء TLS من جانب الخادم فقط ولا تتطلب شهادة عميل النظير.
- `sbi_scheme` هو `https` ولكن لم يتم تكوين `sbi_certfile` / `sbi_keyfile`، وفي هذه الحالة يرفض OmniSEPP البدء بدلاً من التراجع إلى النص العادي.

الحل:

1. قم بتعيين `sbi_scheme` إلى `https` وقم بتكوين `sbi_certfile` و `sbi_keyfile` بحيث ينهي المستمع TLS بنفسه.
2. قم بتعيين SEPP النظير (TLS المتبادل)، لتطلب والتحقق من شهادة عميل النظير التي توقع شهادة النظير. انظر مرجع التكوين - TLS مستمع N32 إلى CA `sbi_cacertfile`.

المرجع

الموضوع	المواصفة
وظيفة شبكة SEPP	3GPP TS 23.501 §6.2.17
وضع TLS N32-f وإخفاء الطوبولوجيا	3GPP TS 33.501 §13.1, §13.2
مصافحة N32 وإعادة توجيه N32-f	3GPP TS 29.573 §5.2.3, §5.3, §6.1.5.2